Single Sign-on to Salesforce.com with CA Federation Manager

TOMMY CHENG, PRINCIPAL ENGINEERING SERVICES ARCHITECT, CA

PETER DAPKUS, FORCE.COM PRODUCT MANAGER, SALESFORCE.COM

Table of Contents

NOTICES

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

Single Sign-on to Salesforce.com with CA Federation Manager

Summary

This document gives SAML 2.0 examples of how CA Federation Manager is configured to help an organization to handle the authentication tasks required to allow their authorized users to single sign-on to the Salesforce.com application.

We start with a brief discussion on the settings needed on the Salesforce.com side and use it to develop a worksheet to allow the single sign on configuration of CA Federation Manager. CA Federation Manager offers two deployment options, as an add-on to CA SiteMinder and/or as a stand-alone or proxy option that does not require CA SiteMinder.

NOTE: If you already own CA SiteMinder with the CA SiteMinder Federation Security Services option and would like to configure it for single sign-on to Salesforce.com; the CA Federation Manager - Add-on to CA SiteMinder option instructions apply.

SECTION 1:

Identity Federation for Single Sign-on

Application developers and IT security people are becoming increasingly aware of the value of using standards-based identity federation to achieve single-sign on to SaaS applications, such as Salesforce.com. This document gives standards-based SAML 2.0 examples of how CA Federation Manager is configured to help an organization to handle the authentication tasks required to allow their authorized users to single sign-on to the Salesforce.com application.

Federated Single Sign-on offers significant benefits, including:

- **Cost Reduction -** IT organizations are looking to control IT costs and gain efficiencies. Federated Single Sign-on targets areas that traditionally require lots of manual processes, including user account management, entitlements management, password management, and access management are a focus of these cost control efforts.
- **Easier Regulatory Compliance** - Expanding regulatory requirements and the increasing rate of compromise of personal information via various types of security breaches have led organizations to place a greater emphasis on data security, and the people, process, and technology that make it up. Standards-based identity federation can increase security enabling an organization to identify and authenticate a user once, and then use that identity information across multiple systems, including external partner websites.
- In this case, CA Federation Manager is used to provides identity federation to allow single sign-on to Salesforce.com

Salesforce.com Single Sign-On Settings and Federation Worksheet

SAML Federation Standards

Salesforce.com supports both SAML 1.1 and SAML 2.0 standards for identity federation. This document focuses on SAML 2.0, although CA supports both SAML 1.1 and SAML 2.0 for single sign-on to Salesforce.com.

CA Federation Manager Federation Deployment Options

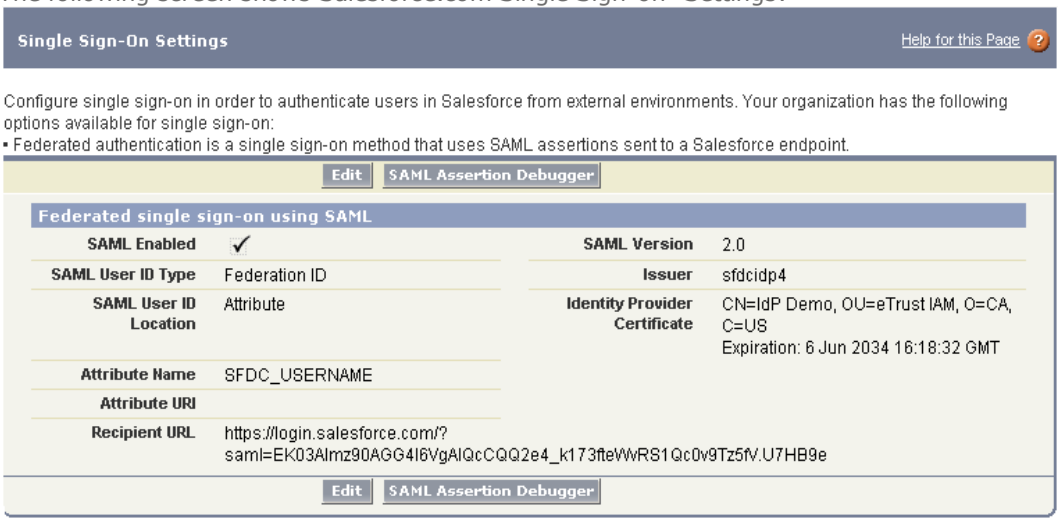
CA Federation Manager offers two deployment options to achieve single sign on to Salesforce.com;

- A Stand-alone option – this option does not require that CA SiteMinder or any other CA software product, be installed.
    a. This option may be deployed in either stand-alone gateway or proxy mode. A connector to CA SiteMinder is provided to easily integrate CA Federation Manager with CA SiteMinder if desired.
- An Add-on to CA SiteMinder option - where federation capabilities are added on to an existing SiteMinder implementation. This option was formerly known as CA SiteMinder Federation Security Services, CA FSS or sometimes called the Web Agent Option Package (WAOP).

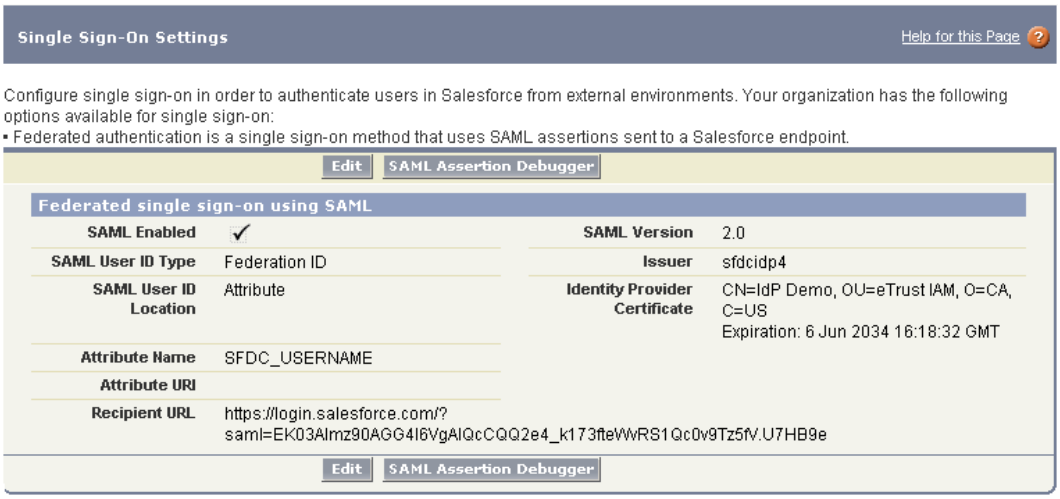
  This paper shows the steps needed to enable single sign-on to Salesforce.com with either CA Federation deployment option; first the "stand-alone' option and then the add-on to Ca SiteMinder option.

Starting at the Saelsorce.com side (the Service Provider or SP-side) of the Federation:

The following screen shows Salesforce.com Single Sign-on- Settings:



Once the settings are saved, the screen becomes:



Using the two screen shots and other SAML 2.0 requirements, develop a Federation Worksheet like the one below to help you gather the information needed to configure CA Federation Manager as an Identity Provider, and provide the identity federation services for your users to access the Salesforce.com. This information will be used throughout the federation partnership configuration process

SFDC Federation Worksheet			
Item	**Description**	**Value**	**Comments**
SAML Enabled	Whether the SAML SSO is enabled on Salesforce.com.		When enabled, Salesforce.com continues to honor the standard ID/password sign on.
SAML Version	The version of the SAML	2.0	
Issuer	The Identity Provider that issues the SAML Assertion		This is known by CA Federation Manager as the IdP ID.
Identity Provider Certificate	The Certificate used to verify the signature of the Identity Provider		The certificate file needs to be uploaded to Salesforce.com.
SAML User ID Type	The SAML User ID can be the Salesforce.com ID or the Federation ID set for a Salesforce.com user object		
SAML User ID Location / Attribute Name	Whether the SAML User ID is the Name ID or exists in the Attribute Statement		If using Attribute Statement is desired, the CA FM needs to use the Attribute Name to provide the SAML User ID.
Recipient URL	This is generated by the Salesforce.com after the SAML User ID Type and Location are determined and saved.		This is known by CA Federation Manager as the Assertion Consumer URL.
Audience	A SAML 2.0 term, used as a shared agreement between IdP and SP.	https://saml.salesforce.com	This is optional by Salesforce.com. When required, always set as this fixed value.
SP ID	A SAML 2.0 used to identify a Service Provider between IdP and SP.		This is used for CA Federation Manager to identify which Service Provider the users are trying to access.

CA Federation Manager: Standalone Option

NOTE: CA FEDERATION MANAGER, THE STAND-ALONE OPTION IS AVAILABLE TO CA SITEMINDER FEDERATION SECURITY SERVICES CUSTOMERS WITH CURRENT MAINTENANCE AT NO ADDITIONAL CHARGE.

SFDC FEDERATION WORKSHEET

To complete the configuration, use the SFDC Federation Worksheet as a guide. From the worksheet, do the following:

- Issuer: Decide the value to be used. This value will be the IdP Entity ID for your configuration.
- Identity Provider Certificate: Obtain and upload the certificate. For CA Federation Manager Standalone, this can be exported from the Admin UI.
- SAML User ID Type: This is set on Salesforce.com.
- SAML User ID Location / Attribute Name: This is set on Salesforce.com.
- Recipient URL: This is generated by Salesforce.com once the SAML User ID Type and SAML User ID Location are determined and saved.
- SP ID: Select an SP ID which will be used to invoke this federation service.

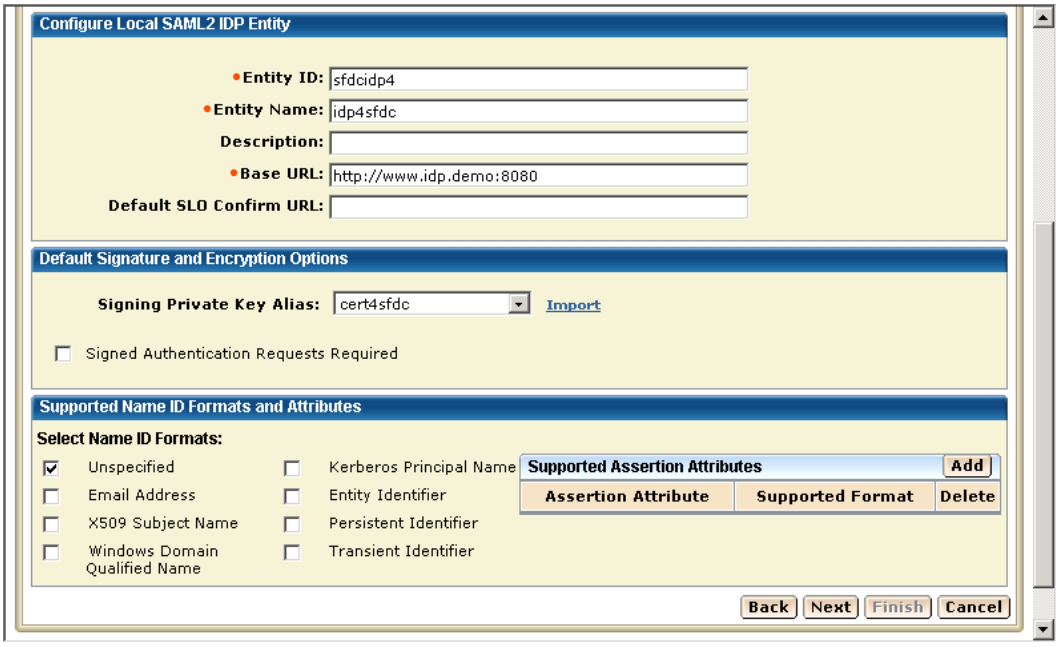
CERTIFICATE TO SIGN SAML ASSERTION

You need to have a certificate to sign the SAML Assertion you are sending to Salesforce.com. For this, you can use the "Request Certificate" button on "Certs and Keys" tab to create a self-signed certificate or to import an existing Certificate that contains both a Private and a Public Key. This type of Certificate is often in PKCS12 format.

With the certificate either created or imported, you can then export it in X509-PEM format and import it into Salesforce.com.

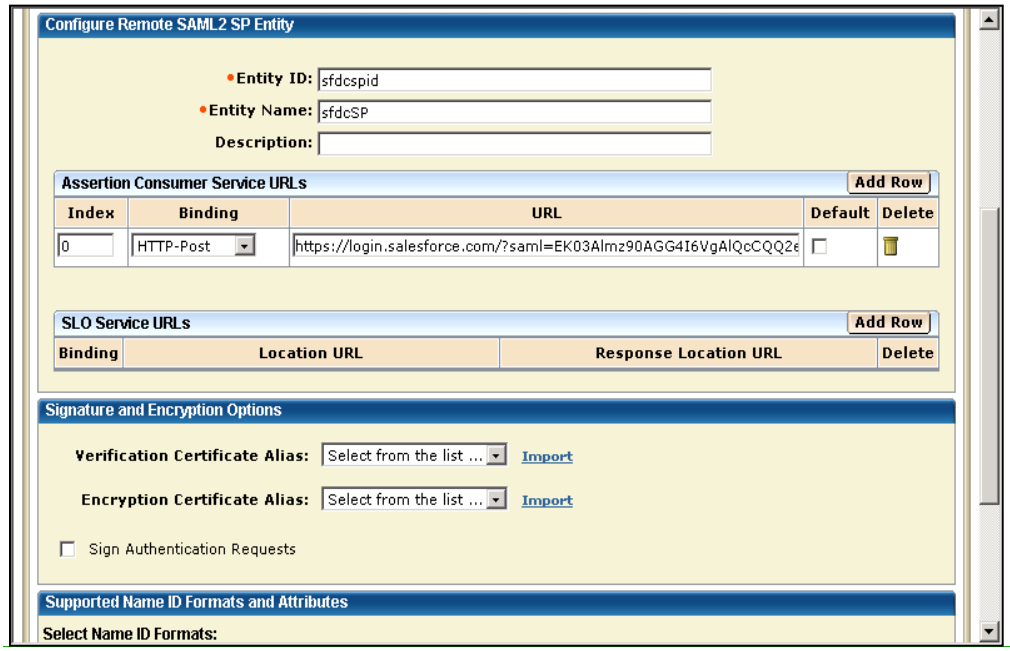
LOCAL SAML 2 IDP ENTITY

To offer federation service using CA Federation Manager- the stand-alone deployment option - as a SAML 2.0 IdP, you now need to define a Local IdP Entity and associate it with the Certificate acquired earlier. The Entity ID needs to be the Issuer from the SFDC Federation Worksheet.



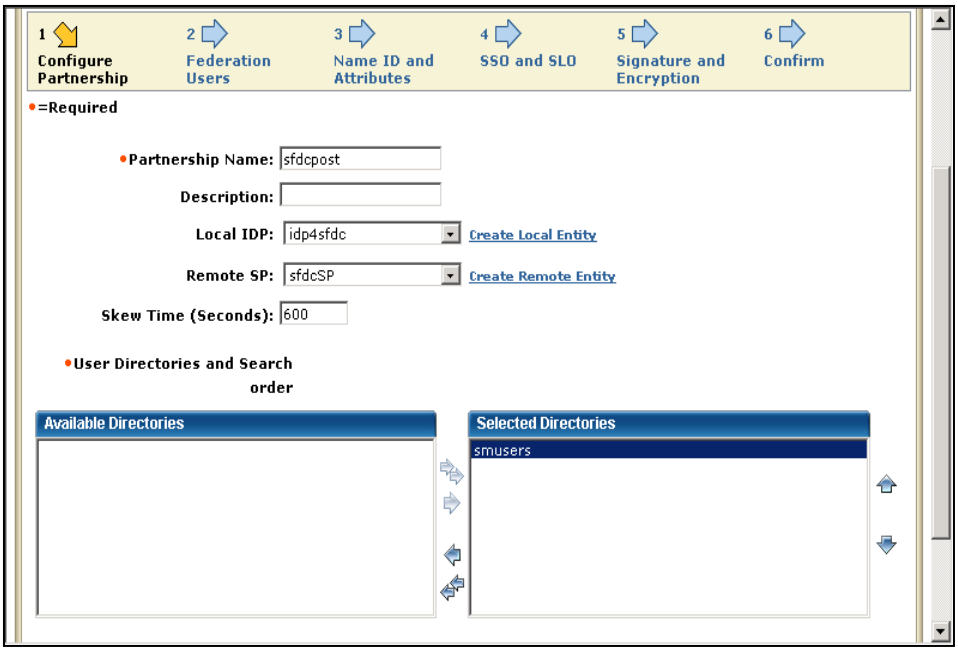
REMOTE SAML 2.0 SP-SIDE ENTITY

You now need to specify a Remote SP Entity to represent Salesforce.com. The Entity ID is the SPID from the SFDC Federation Worksheet. The HTTP-Post Assertion Consumer Service URL needs to define the **Recipient URL** on or SFDC Federation Worksheet.

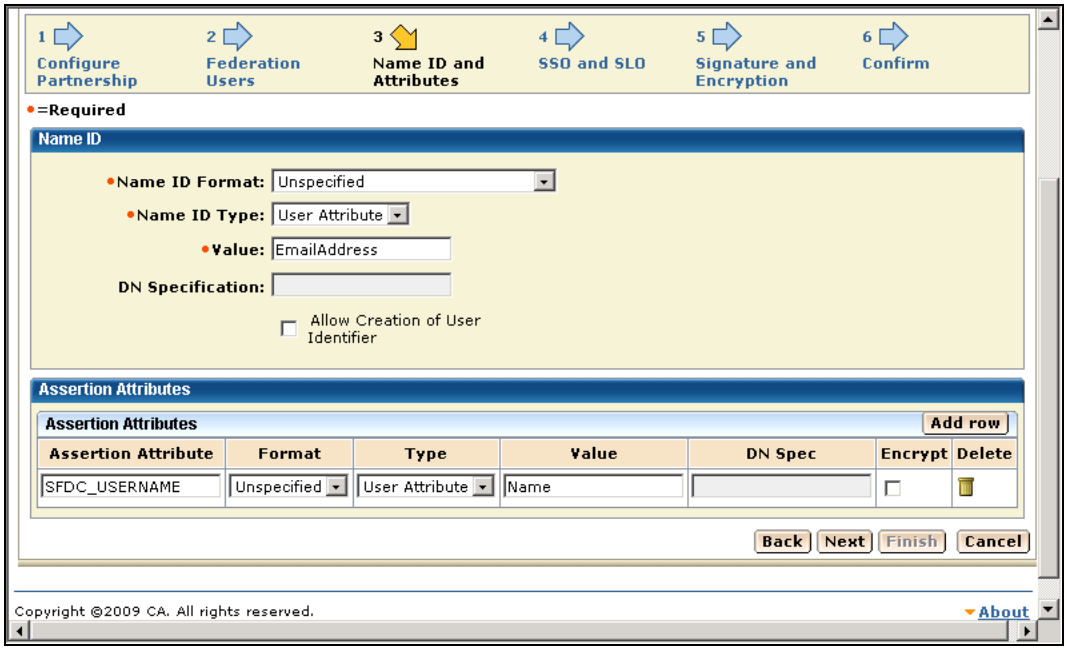


SAML2.0 IDP->SP PARTNERSHIP

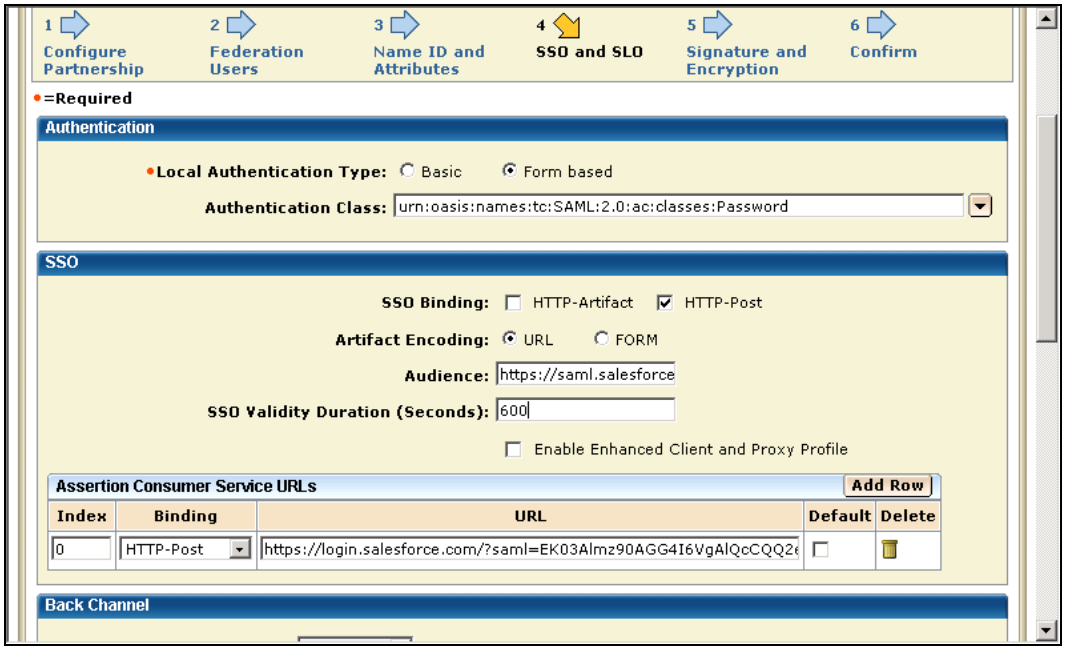
1. With the Local IDP and Remote SP defined, you can now configure and activate a SAML2 IDP->SP Partnership. Choose the Local IDP and Remote SP defined earlier, set an appropriate Skew Time and select an appropriate User Directory.



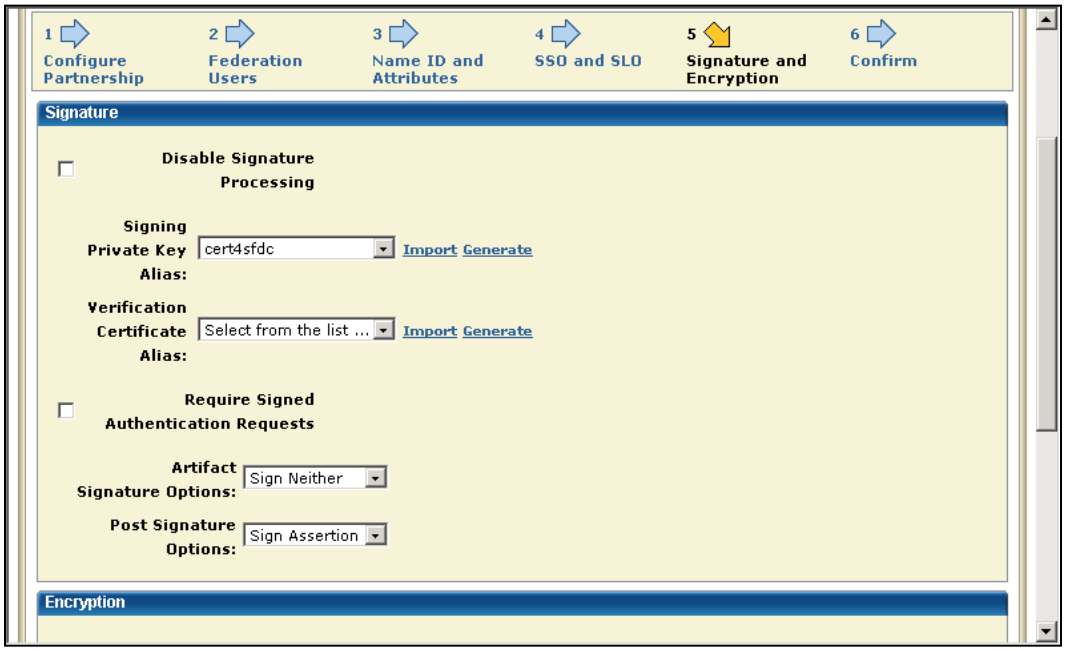
2. Leave the default setting of all users from the User Directory to use the Federation Service.
3. Set the Name ID Value to the appropriate value if the **SAML User ID Location** is the Name ID. If the SAML User ID Location is set to Attribute, add a row and use the **Attribute Name** from the SFDC Federation Worksheet to add an Assertion Attribute:



4. Set the Local Authentication Type of your choice, and check the HTTP-Post for SSO Binding. Use the https://saml.salesforce.com value from the **Audience** value from the SFDC Federation Worksheet and set an appropriate SSO Validity Duration:



5. Leaving the default setting as Federation Manager picks up the correct Signing Private Key Alias from the Local IDP Entity.



6. Save and activate this newly created Federation Partnership.

7. Exercise the Federation Service:

   Once the configuration is done on both Salesforce.com and the CA Federation Manager, you can open a page in the browser to test the federation service. Use a URL similar to the following to invoke the Federation Service to Salesforce.com:
   http://www.idp.demo:8080/affwebservices/public/saml2sso?SPID=sfdcspid

CA Federation Manager Add-on to CA SiteMinder Option

NOTE: IF YOU ALREADY HAVE CA SITEMINDER IMPLEMENTED AT YOUR ORGANIZATION, YOU FIRST NEED TO HAVE THE ADDITIONAL CA FEDERATION MANAGER ADD-ON TO SITEMINDER LICENSE AND SOFTWARE TO USE THE FEDERATION FEATURES.

IF YOU ALREADY HAVE CA SITEMINDER FEDERATION SECURITY SERVICES, THESE INSTRUCTIONS WILL HELP YOU SET UP SINGLE-SIGN ON TO SALESFORCE.COM

SALESFORCE.COM FEDERATION WORKSHEET

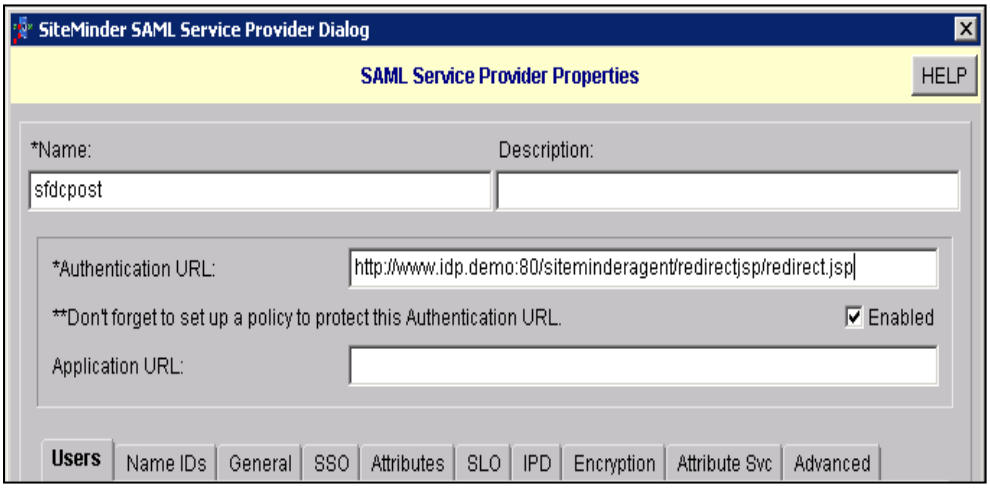
To complete the configuration, use the Salesforce.com Federation Worksheet as a quick guide. From the worksheet, you need to do the following:

- Issuer: Decide the value to be used. This value will be the IdP ID for your configuration.
- Identity Provider Certificate: Obtain and upload the certificate. For CA Federation Manager this can be obtained through the following command:
  a. **smkeytool -export -alias defaultenterpriseprivatekey -outfile smaddon.cer -type cert**
- SAML User ID Type: This is set on Salesforce.com.
- SAML User ID Location / Attribute Name: This is set on Salesforce.com.

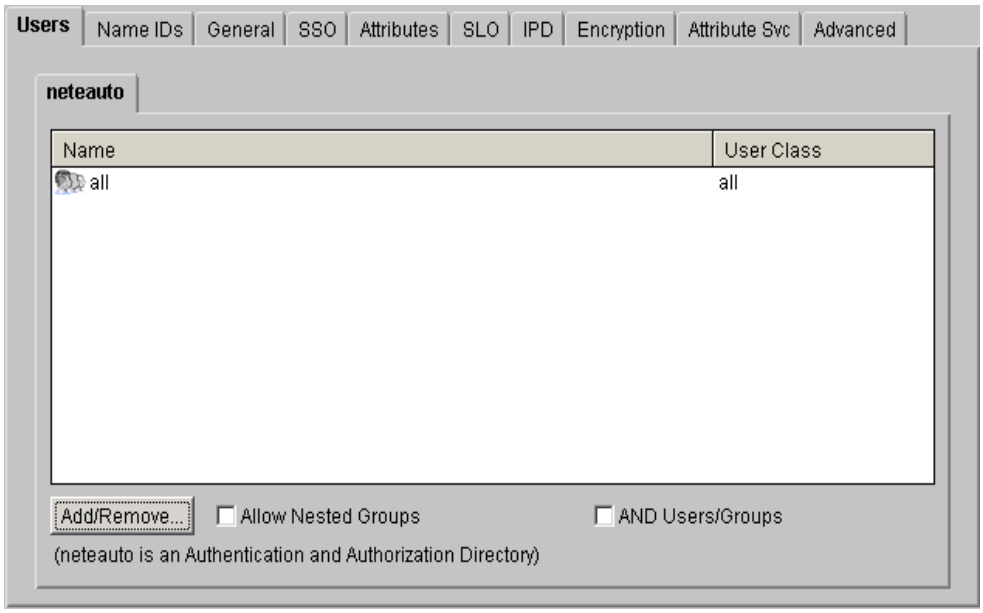
- Recipient URL: This is generated by Salesforce.com once the SAML User ID Type and SAML User ID Location are determined and saved.
- SP ID: Pick an SP ID in order to invoke this federation service.

SERVICE PROVIDER CONFIGURATION

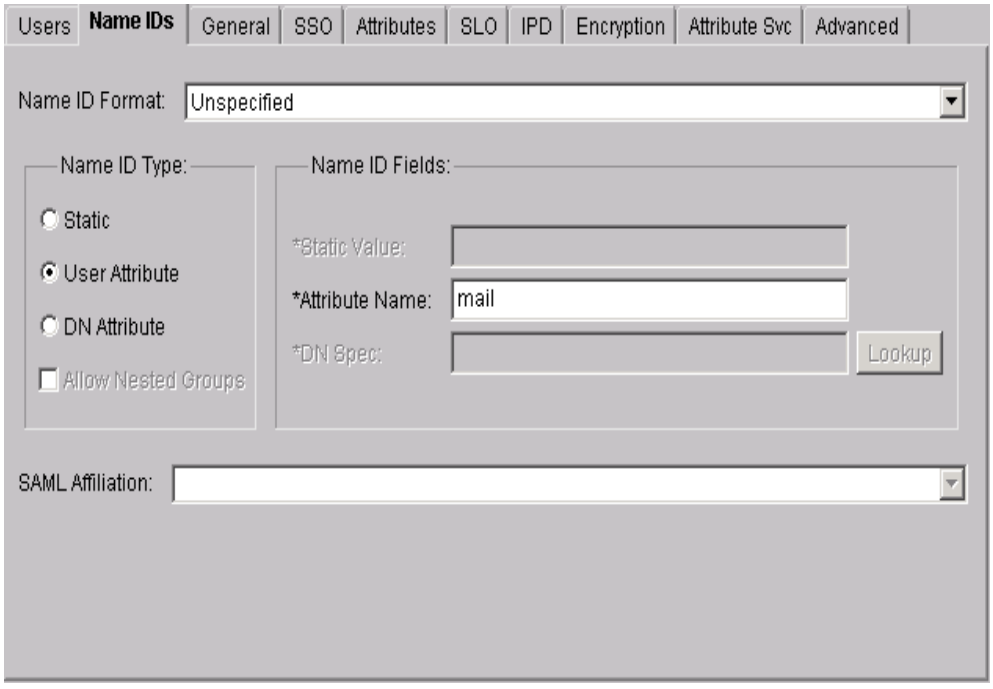
8. To configure the SiteMinder Add-on, you need to create a Service Provider under an Affiliate Domain. Here **sfdcpost** is an example. The Authentication URL is the typical URL that triggers authentication when necessary:



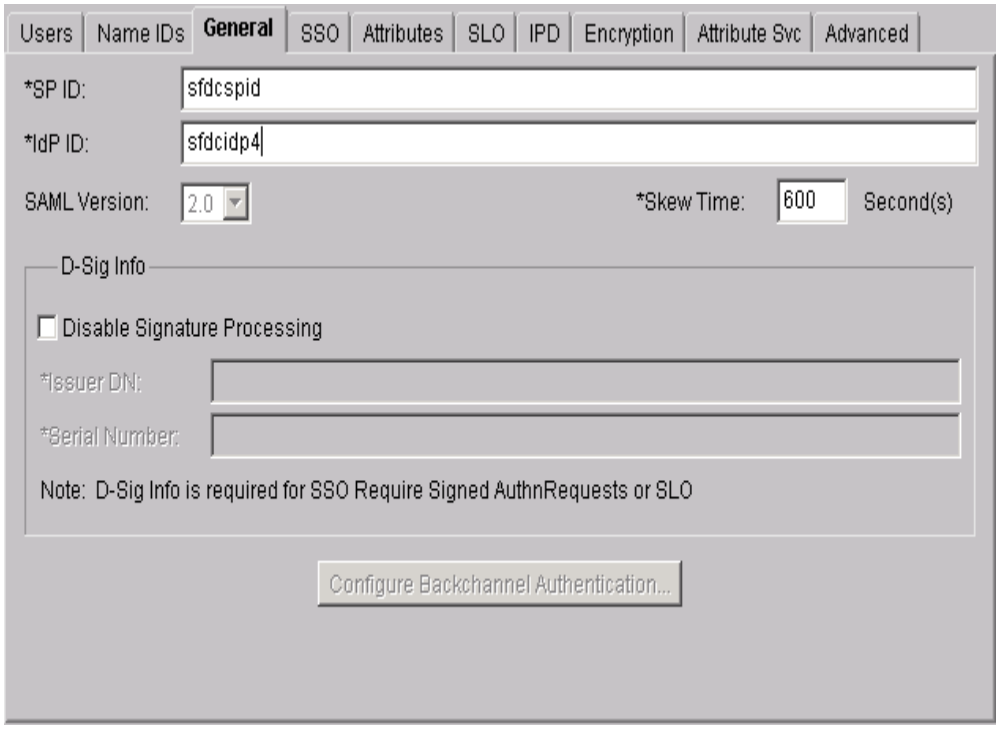
9. Users tab: use "all" to allow all users in the user directory to be able to use this Federation service:



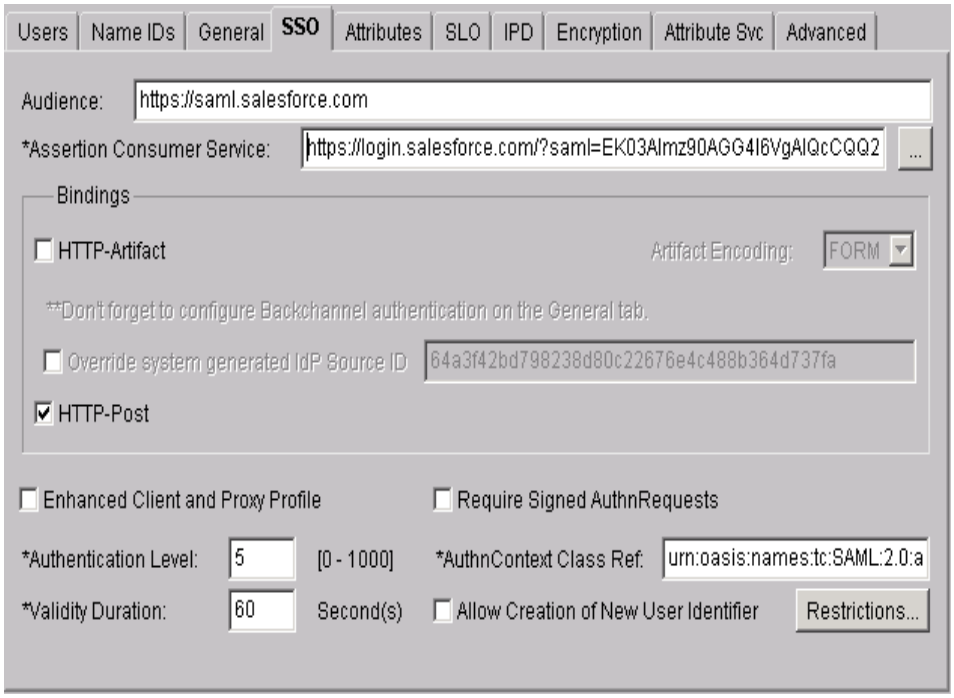
10. Name IDs tab: The Name ID must have a value. If you decided to use the Name ID (SAML User ID Location from the SFDC Federation Worksheet), then this value has to be set as an appropriate attribute name from the user directory that contains the Salesforce.com SAML User ID.



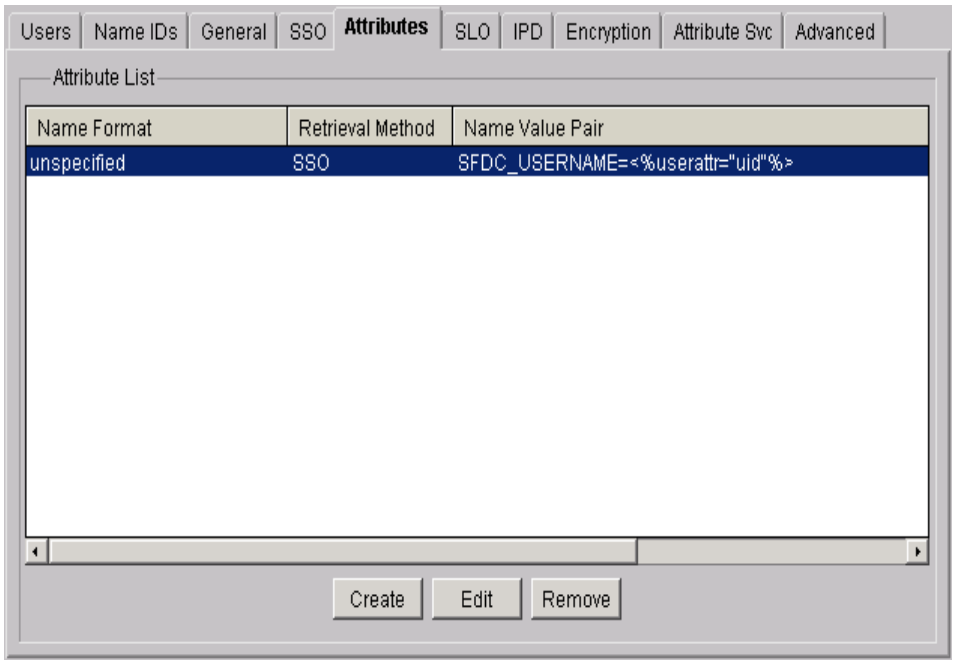
11. General tab: The IDP ID needs to be set as the value of the Issuer from the Federation Worksheet. The SP ID is set to the SP ID from the SFDC Federation Worksheet. Also, set an appropriate Skew Time value to allow a minor time difference between the SiteMinder Policy Server and the Salesforce.com.



12. SSO tab: Set the Audience to "https://saml.salesforce.com" (This value was specified as the Audience value on the Federation Worksheet). The Assertion Consumer Service is set to the value of the Recipient URL from the SFDC Federation Worksheet. The binding needs to have the HTTP-Post checked.



13. Attributes Tab: If the SAML User ID Location from the SFDC Federation Worksheet is set to Name ID, you can leave this tab blank. Otherwise, use the Attribute Name as a Variable Name to configure an attribute:



14. Use the default settings for the remaining tabs.
15. Exercise the Federation Service:

Once the configuration is done on both Salesforce.com and CA SiteMinder Add-on, sides of the federation; open a page in a browser to test the Federation Service.

a. Use a URL similar to the following to invoke the Federation Service to Salesforce.com:
http://www.idp.demo:80/affwebservices/public/saml2sso?SPID=sfdcpost