15 Salesforce.com SSO

15.1 Description

This tutorial will walk you through using the Gateway to support single sign-on to salesforce.com. It will demonstrate how you are able to login through your browser with one set of credentials and get automatically logged into salesforce.com using a SAML response that is constructed in a Gateway policy. There are two main configurations that will be needed for this tutorial. First, you will need to configure salesforce.com to support Single Sign-on and second a policy will be needed in the Gateway to support this use case.

15.2 Prerequisites

15.2.1 Environment

1. Layer 7 SecureSpan Gateway *(this tutorial was designed using a version 7.0 gateway; it may or may not work with earlier versions; it should work with later versions)*
2. Layer 7 Policy Manager *(this tutorial uses the Policy Manager software installation; the software installation version must match the gateway version; alternatively, users can use the Policy Manager browser-based version which always matches the gateway version that is connected to)*
3. *salesforce.com Developer account – you can obtain a Developer account free of charge from salesforce.com.*
    a. *Go to www.salesforce.com*
    b. *Select Developer Community from the Community menu*
    c. *Click Join Now*
    d. *Complete the necessary information and Submit*

15.2.2 Tutorials

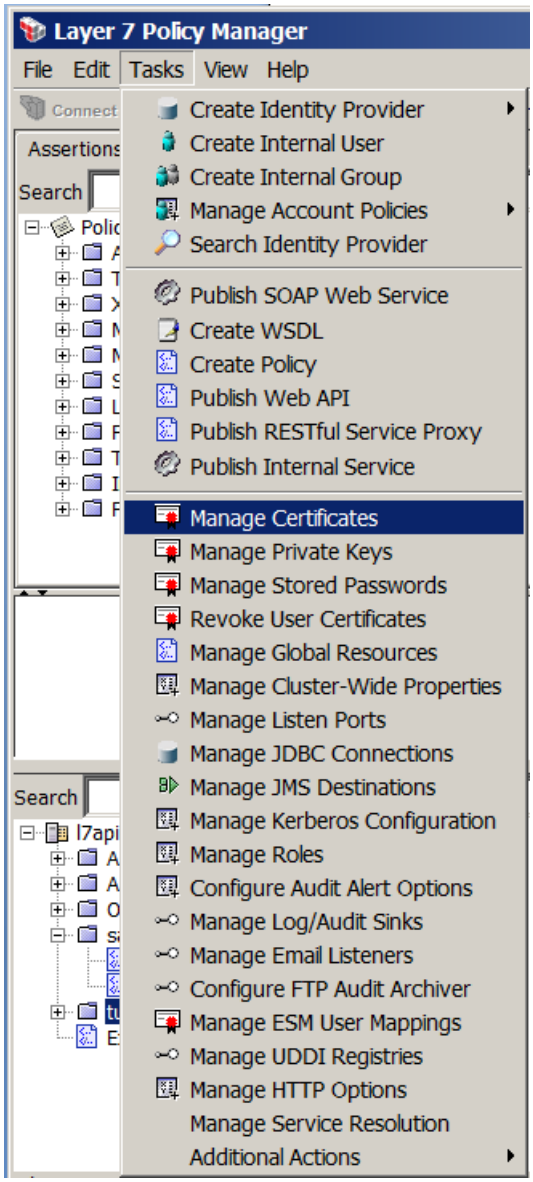
1. Layer 7 Tutorials - Getting Started

15.3 Tutorial Steps

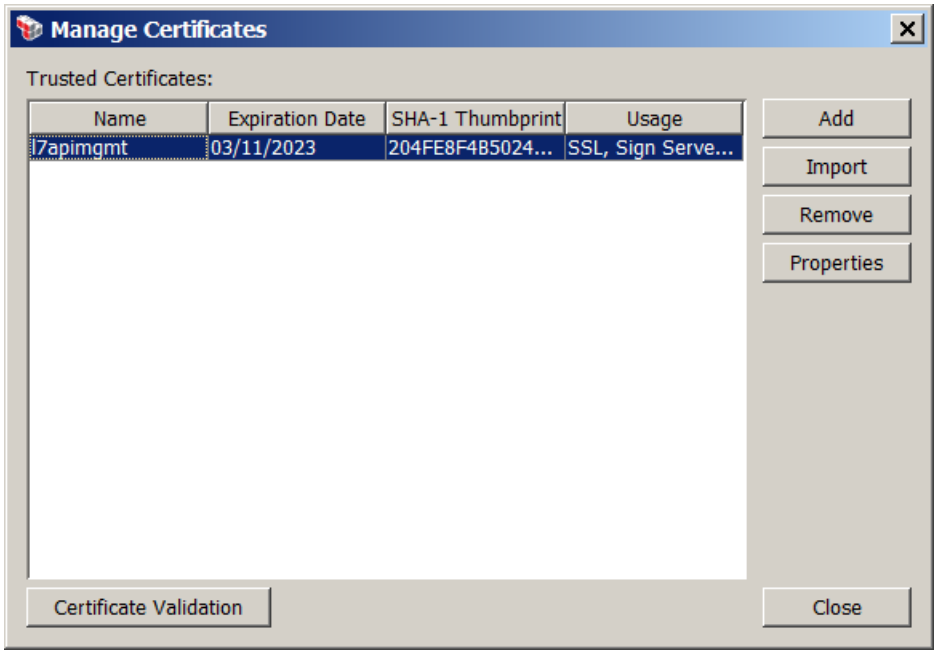
15.3.1.1 Setting up Single Sign-on in salesforce.com

1. You will need to obtain a certificate from the Gateway to be used when configuring salesforce.com.
    a. Connect to your gateway using Policy Manager (see **Layer 7 Tutorials - Getting Started**).

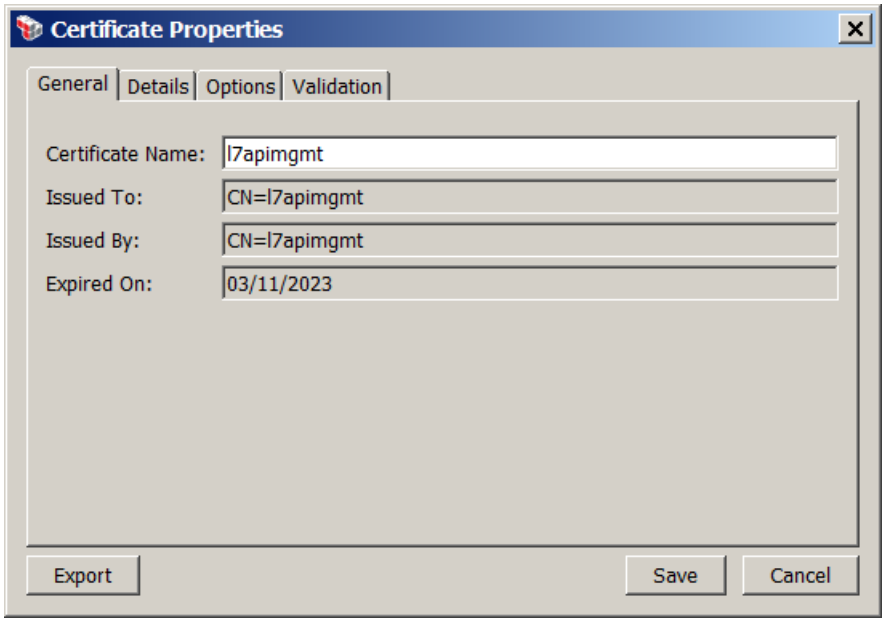
b. In the Policy Manager, select Manage Certificates from the Tasks menu.



c. Select the default SSL certificate from the list. If you are using the standard evaluation image, this certificate is named “l7apimgmt”, otherwise, the certificate name should be the same name as the host of the image. Click the Properties button.

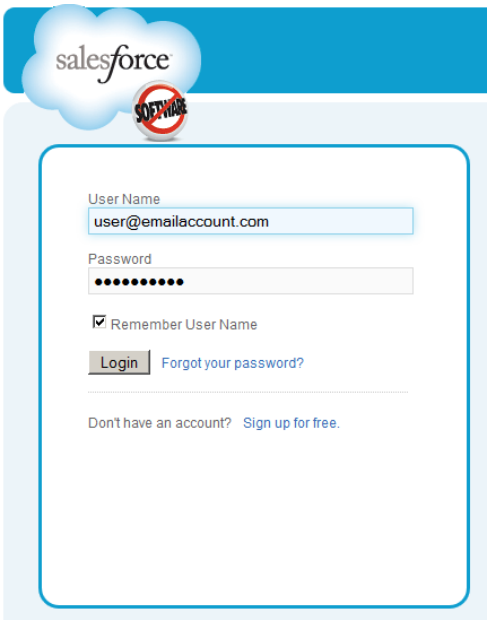


d. Click Export



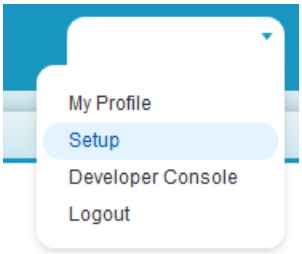
e. Select a location to save the certificate and enter a File name.
f. Click Cancel and then Close.

2. Login to your Salesforce.com Developer account @ https://login.salesforce.com/?lt=de

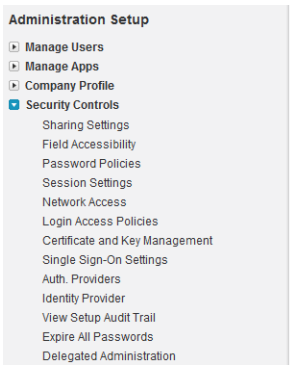


Note that the user name (not the password) provided for this login will also be added to the internal identity provider in the Gateway below.

3. Select Setup from the options underneath your name. If you don't see a Setup item in this menu but already have the Administration Setup section in the left menu pane, skip to step 4.

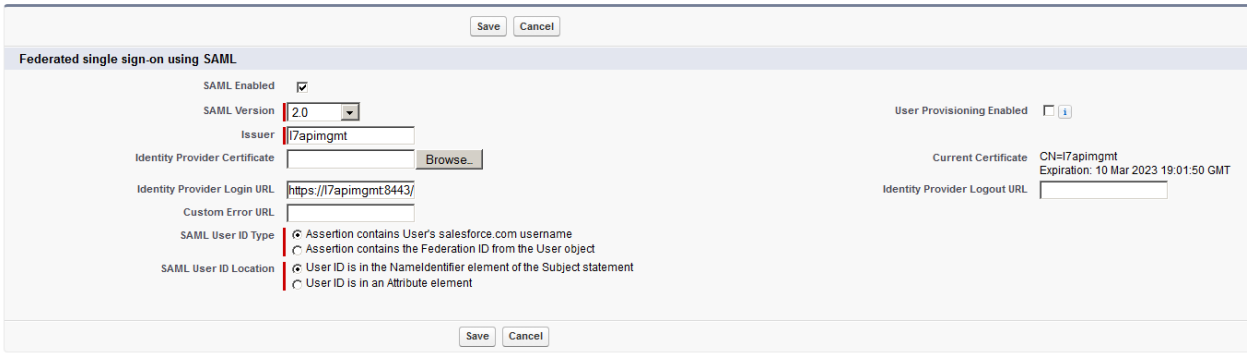


4. From the left hand navigation area, select Security Controls from the Administration Setup section as illustrated below.



5. Select Single Sign-On Settings
6. Enter the following information:
    a. SAML Version: 2.0
    b. Issuer: l7apimgmt (or the name of the SSL cert if different)
    c. Identity Provider Certificate: browse for the certificate that was exported in the steps above
    d. Identity Provider Login URL: https://l7apimgmt:8443/salesforce
    e. Custom Error URL: leave blank
    f. SAML User ID Type: Assertion contains User's salesforce.com username
    g. SAML User ID Location: User ID is in the NameIdentifier element of the Subject statement

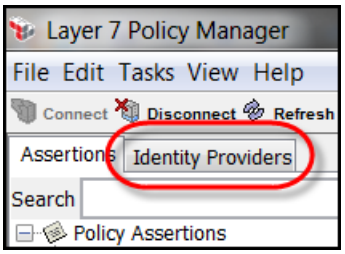
Single Sign-On Settings



7. Click the Save button.

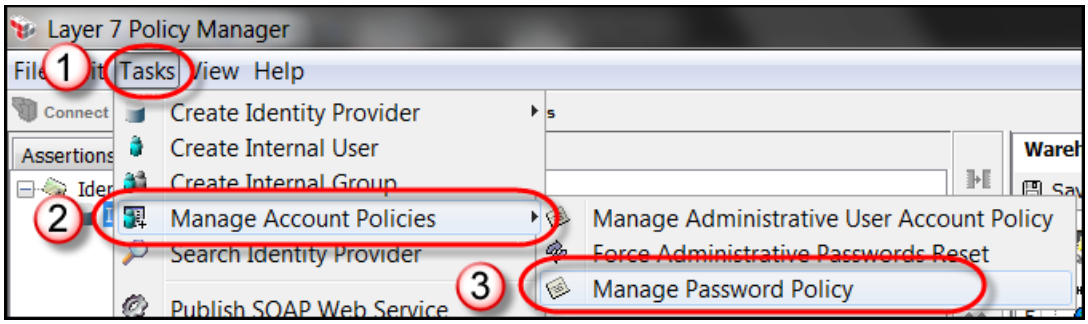
15.3.1.2 Setting up Gateway to Implement SAML-based Federated Authentication

1. Connect to your gateway using Policy Manager (see **Layer 7 Tutorials - Getting Started**).
2. In Policy Manager, select the ***Identity Providers*** tab.
3.

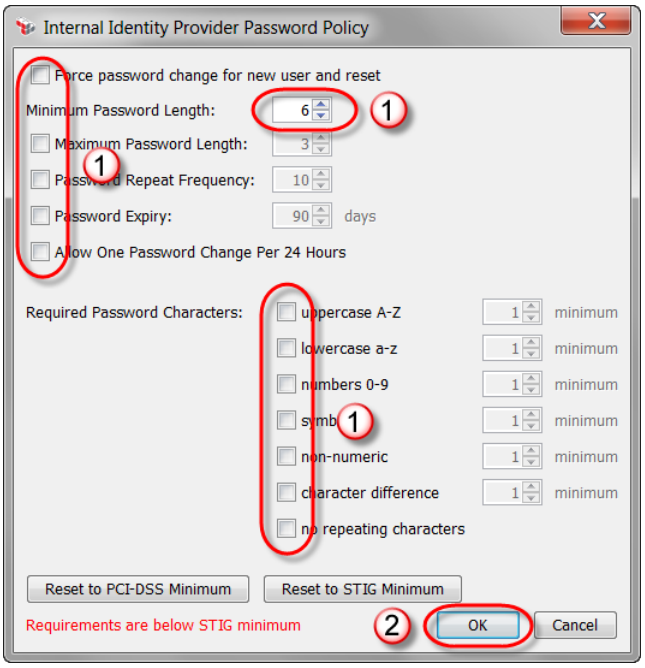


We will now add the user name of the user that was setup in Salesforce.com to the Internal Identity Provider. If this gateway is only being used for evaluation or training purposes, and/or if internal identity provider password policies are not a concern for this gateway, then you may want to relax the gateway's default password policy to allow easier to remember passwords.

To relax the gateway's default password policy, select the ***Tasks/Manage Account Policies/Manage Password Policy*** menu item.

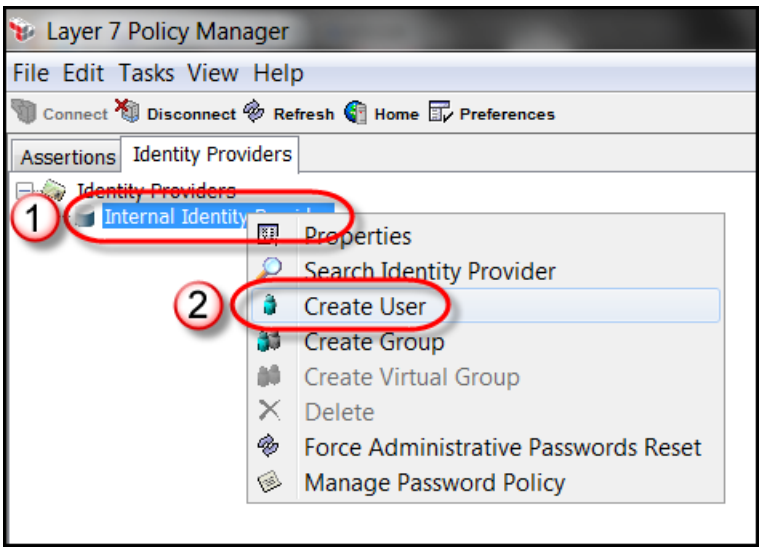


In the Internal Identity Provider Password Policy dialog, uncheck all options and reduce the ***Minimum Password Length*** to a smaller length that suits you, and then click the ***OK*** button.

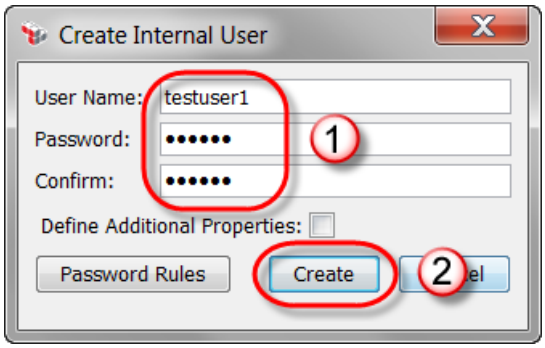


Note: Should you ever want to go back to a higher standard password policy, you can simply return to this dialog and click on either the ***Reset to PCI-DSS Minimum*** *or* ***Reset to STIG Minimum*** *buttons.*

4. In the Identity Providers tree, right click on the ***Internal Identity Provider***, and in the context menu, select the ***Create User*** item.

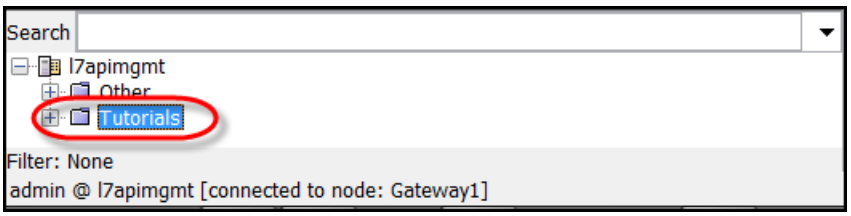


5. In the Create Internal User dialog, in the ***User Name*** field type the user name you supplied when creating your account in Salesforce.com, type and confirm a password of your choice, and click the ***Create*** button. Note that the password entered for this user here should not be the same as the password you used when you created the salesforce.com developer account.

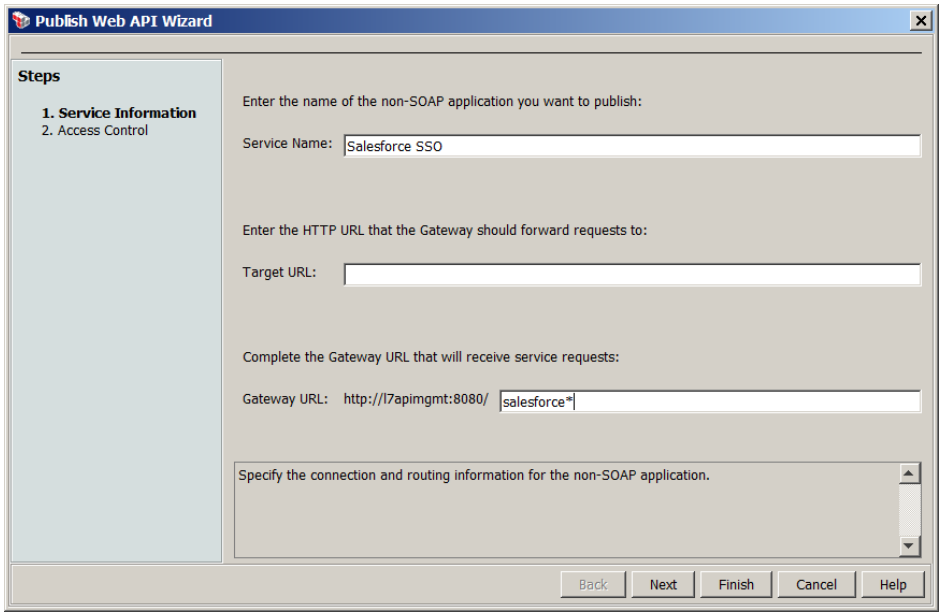


Note: "7layer" is a password that Layer 7 often uses by default. If the Internal Identity Provider's password policy has been relaxed, it's an easy password to remember and one that many Layer 7 employees will think to try first if they help you with your tutorials. You may also want to use "7layer" for this reason. In any case, remember the password you use for this and later tutorials.

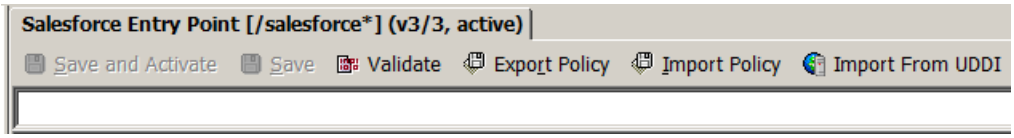
6. In the service and policy tree, right click on the new ***Tutorials*** folder.



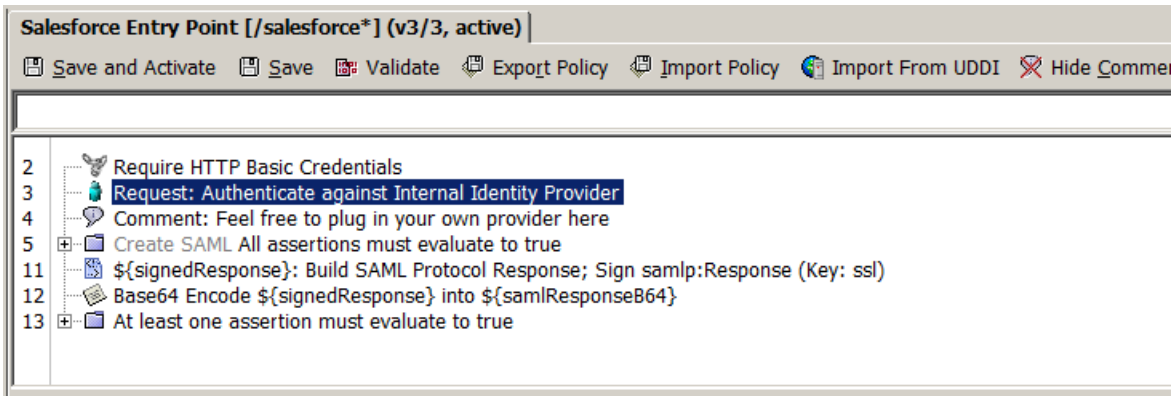
7. In the context menu, select the ***Publish Web API*** context menu item.
8. In the Publish Web API Wizard complete the following property fields:
    a. Service Name: Salesforce SSO
    b. Target URL: Leave blank
    c. Gateway URL: /salesforce*



9. Click Finish
10. In the policy editor toolbar, click the ***Import Policy*** button.

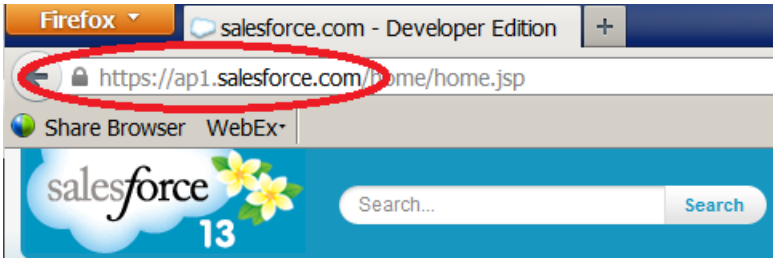


11. In the Import Policy dialog, navigate to the tutorials package folder and the ***Tutorial 15 - Salesforce.com SSO*** subfolder, select the ***Salesforce SSO Policy.xml*** file, and click the ***Open*** button
12. In the policy editor toolbar, click the ***Save and Activate*** button.

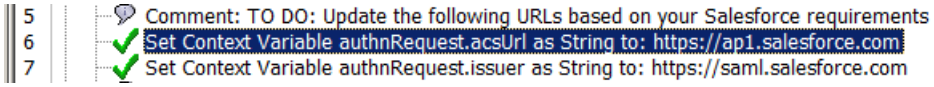


There may be a few updates that will need to be made to the policy to support your particular environment.

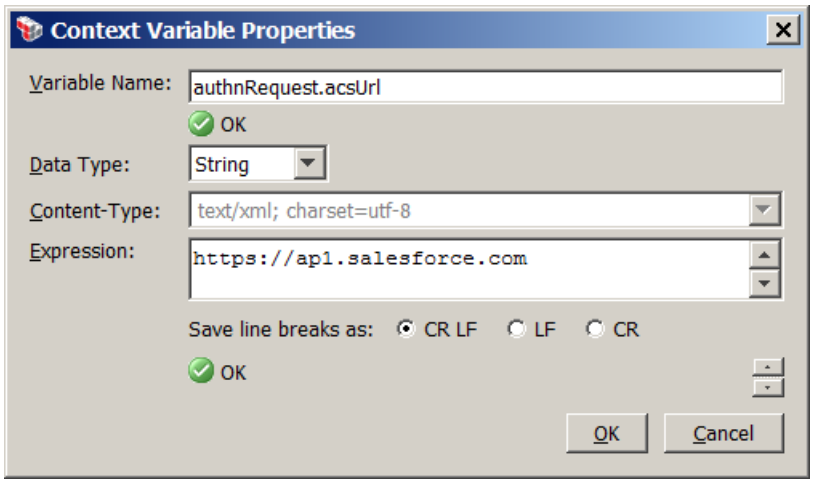
13. Line 6 of the policy stores the Authentication Request URL. The value associated with this URL will be determined by the region that was assigned at the time the Salesforce account was created. The value can be found by looking at the URL when you are logged into Salesforce.com as illustrated below.



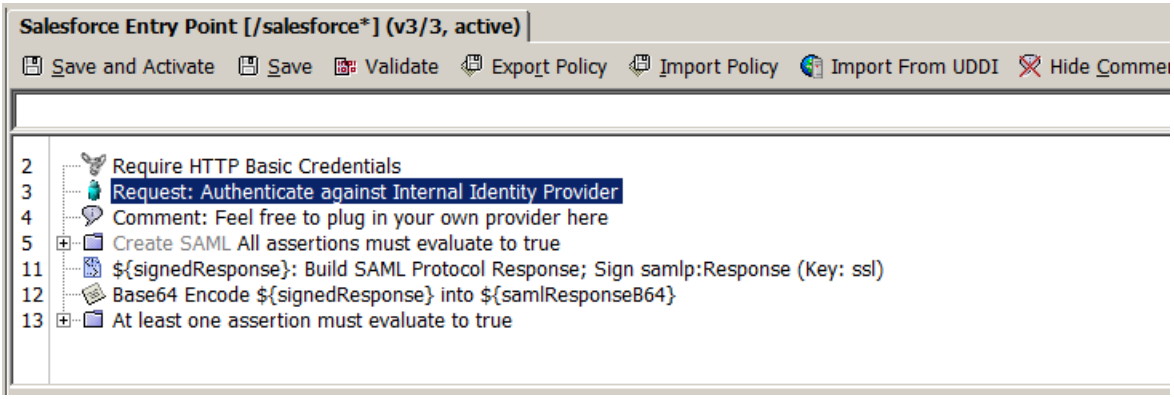
14. To update the value, double click on Line 6 of the policy.



15. Update the Expression field with the value noted above in the URL and click OK.



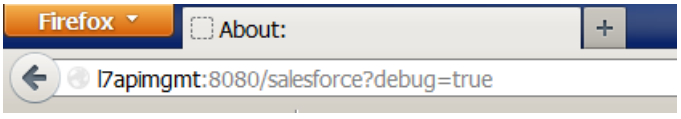
16. In the policy editor toolbar, click the ***Save and Activate*** button.



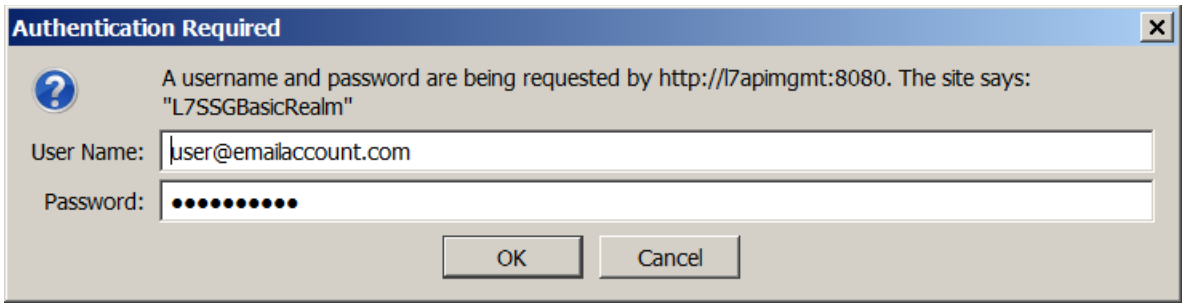
17. Open a browser.

There are two modes available for this service. There is a standard mode which, after you authenticate against the identity provider, will direct you right to salesforce.com and there is a debug mode that will present the resulting base 64 encoded SAML response as well as the un-encoded SAML response for review before logging into salesforce.com.

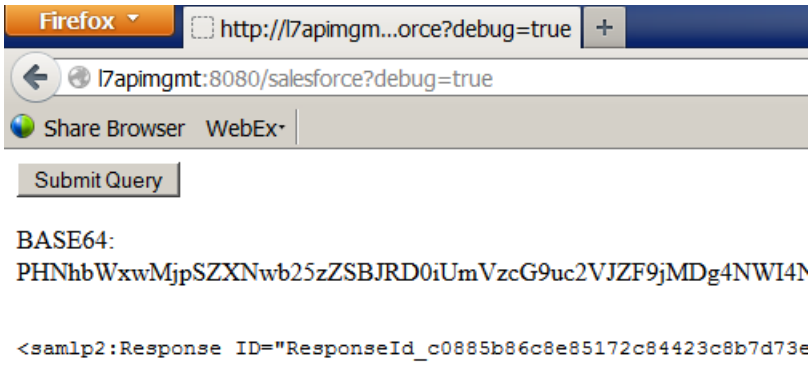
18. Enter http://l7apimgmt:8080/salesforce?debug=true into the browser. This will allow us to see the SAML response before it is passed to salesforce.com.



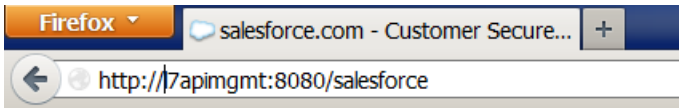
19. Enter the user name and password into the form provided by the browser and then click the OK button. Note that these are the credentials for the account that was created in the gateway's Internal Identity Provider above. The user name will match the user name of your salesforce.com account but the passwords will not.



20. Once authenticated, you will be presented with a page that provides information about the SAML response. Click the Submit Query button to continue to salesforce.com.



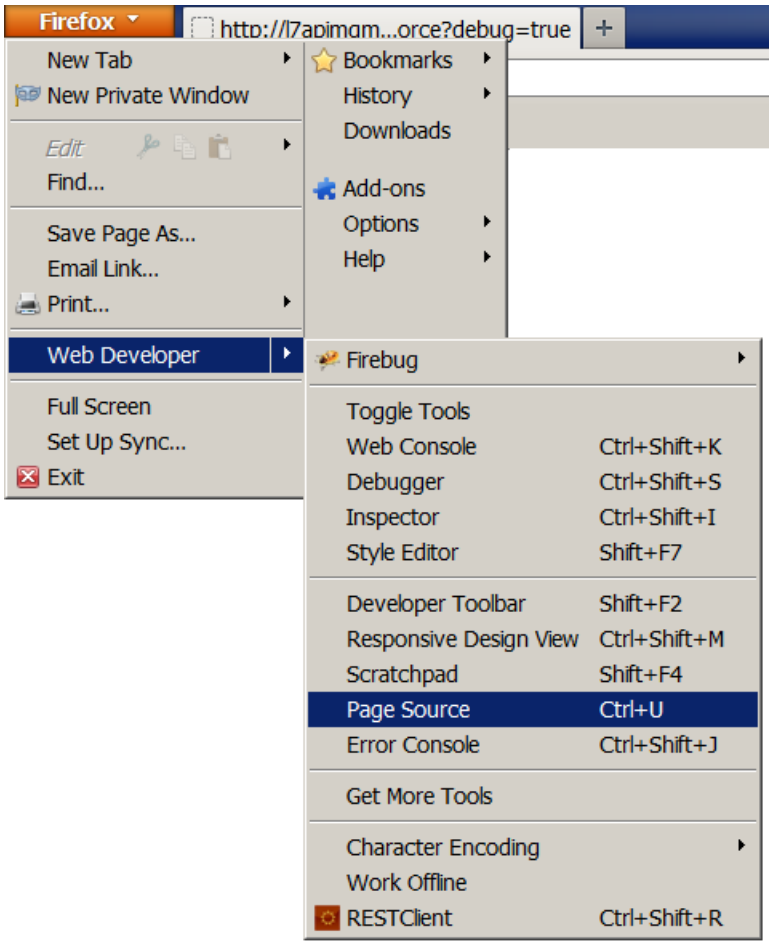
21. If all works correctly, you will be re-directed to salesforce.com and will be logged in automatically using the SAML assertion created in the gateway policy.
22. To avoid the debug page, remove the debug parameter from the URL sent to the Gateway.



15.4 Additional Context

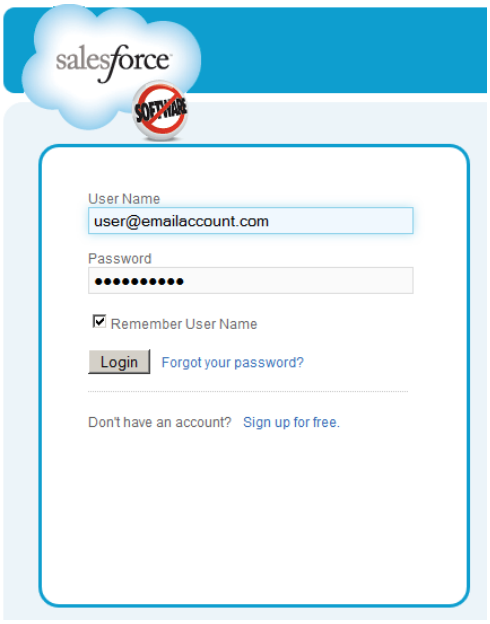
You can test the SAML response (un-encoded) within salesforce.com to ensure that is correct using the following steps.

1. Send the request to the Gateway using debug mode as described above.
2. With the debug page displayed, view the page source using your browser's capabilities. In Firefox, select Web Developer, Page Source from the main Firefox menu.

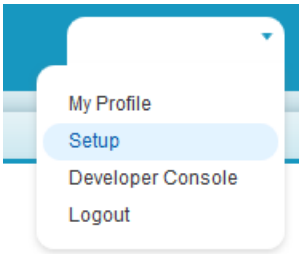


3. Copy the entire line containing the un-encoded SAML response into the Clipboard. In the case below, it is on line 14. Alternatively, you can also copy the Base64 encoded version (located on line 10 below) as long as you do not include the "BASE64: " when you are copying it.

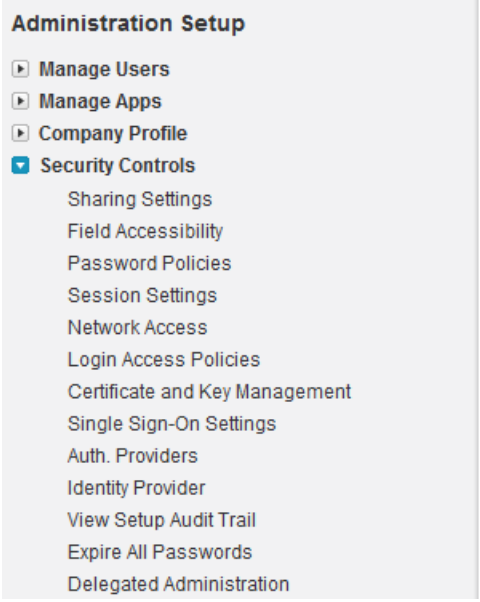
4. Close the Page Source screen down.
5. Login to your Salesforce.com Developer account @ https://login.salesforce.com/?lt=de



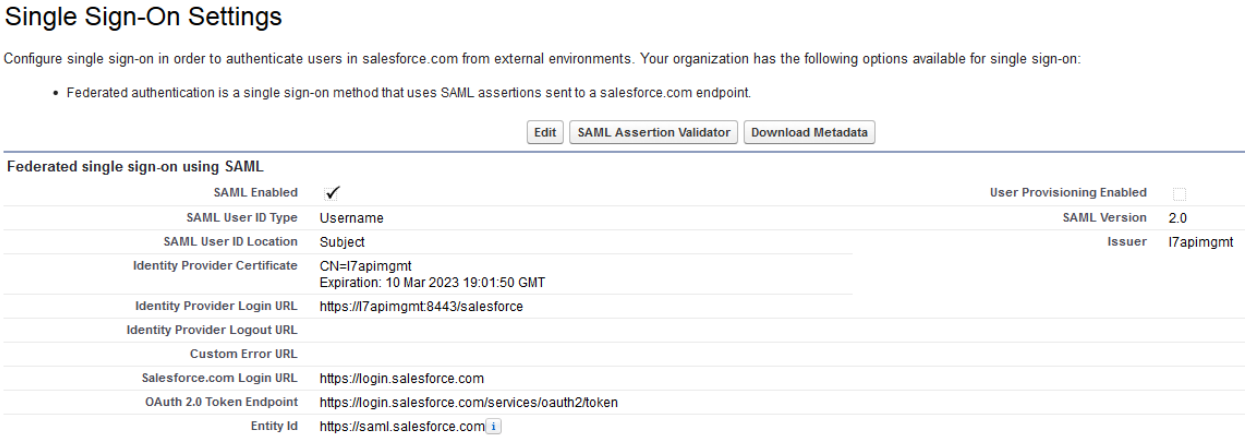
6. Select Setup from the options underneath your name.



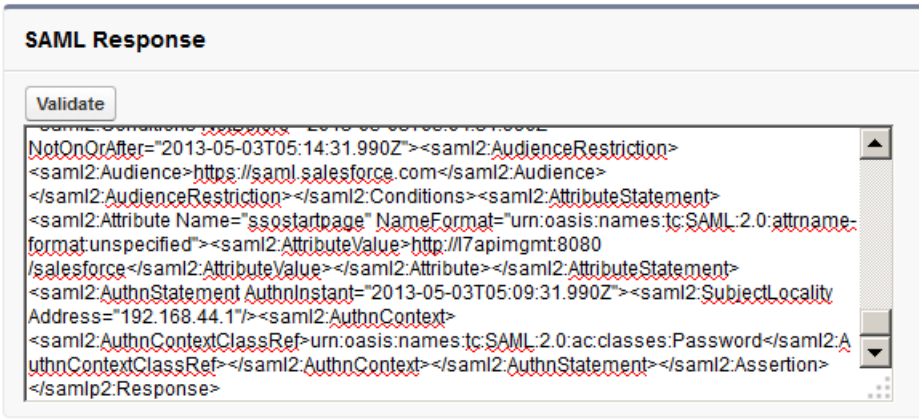
7. From the left hand navigation area, select Security Controls from the Administration Setup section as illustrated below.



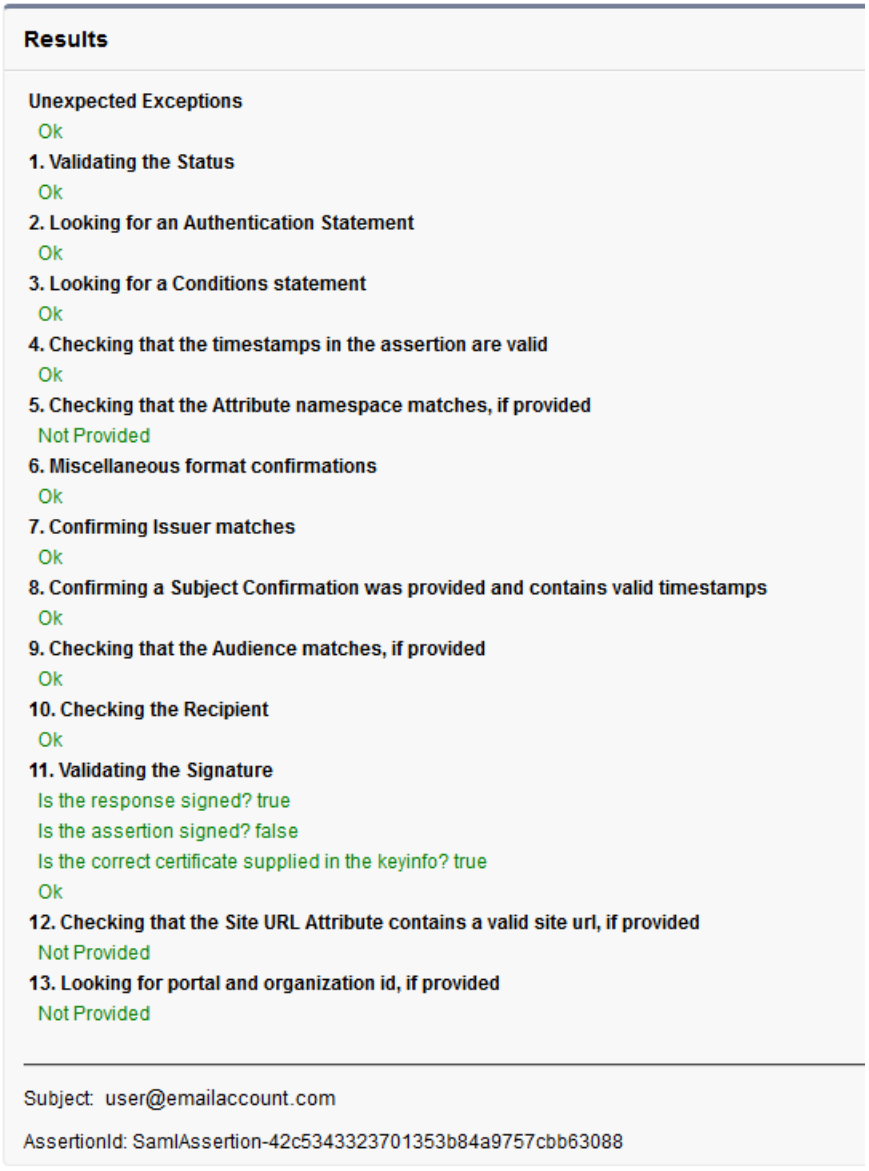
8. Select Single Sign-On Settings.
9. Click on the SAML Assertion Validator button.



10. Paste the SAML response that you captured above into field provided and click the Validate button.

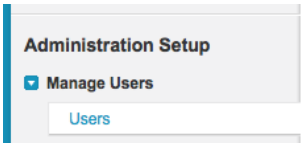


11. salesforce.com will check the SAML response and provide a summary of the check similar to the illustration below. This can be used to debug any problems you may be experiencing.

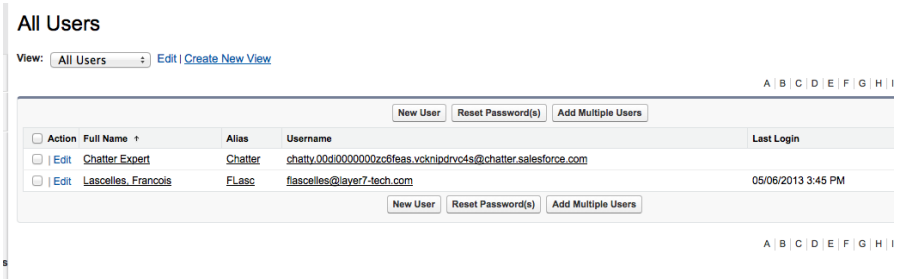


You can also test federated login in your dev Salesforce instance for a different (non administrator) user account which does not have a password on the Salesforce instance.

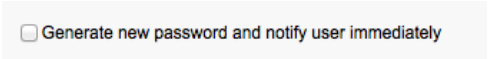
1. Go back to Administration Setup pane and select the Users item.



2. In the All Users, select the New User button.



3. Create a different user name, email (the email does not need to be real) and deselect the bottom option “Generate new password and notify user immediately” and click Save.



4. Add a User in your internal identity provider following step 4 of the main tutorial. Use the same username as used the user created in the Salesforce instance.
5. Clear the history of or restart your browser and repeat steps 17 to 20 of the main tutorial, authenticating with the credentials of the new user.