knowledge14

April 27–May 1, 2014 • Moscone Center • San Francisco, CA

Lab Guide

Integration 201:

Unleash the Power of SAML 2.0

Jason Petty & Jonatan Jardi

Lab instance: https://**<<name>>**.lab.service-now.com

Login / Passwords:

admin / Knowledge14

itil / Knowledge14

employee / Knowledge14

Scenario



IdP



Users

You have been asked to make ServiceNow work with the Single Sign On (SSO) solution that other applications in the company already use so users don't have to login again.

The corporate identity provider already has login credentials stored and your company wants to use the same ones to access ServiceNow



© 2014 ServiceNow All Rights Reserved

SAML 2.0 Browser POST process flow

- Service Provider (SP) Initiated Logon
  - The user goes directly to the ServiceNow instance
  - ServiceNow requests that an authentication takes place
  - ServiceNow authenticates based on a response from the corporate identity provider (IdP)
- Identity Provider (IDP) Initiated Logon
  - The user goes first to a corporate portal or identity store
  - The corporate identity store asks ServiceNow if it can launch and authenticate as a specific person

© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

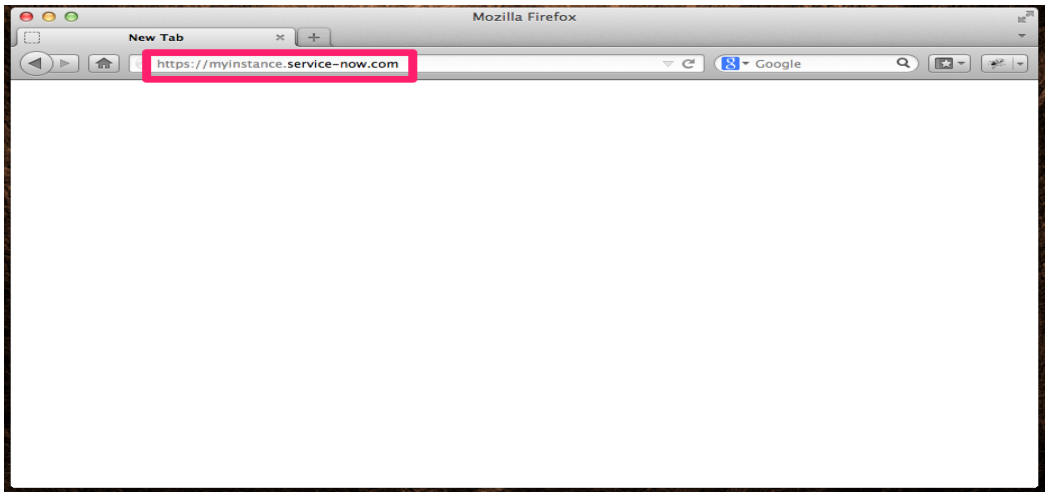
Service Provider Initiated Login

1. User attempts to browse to a ServiceNow instance



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

ServiceNow will..

1. Build an AuthnRequest XML document



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="https://
yourinstance.service-now.com/navpage.do" ForceAuthn="false" ID="SNCb7195eee1fd1b49083cc56cc0d14946d"
IsPassive="false" IssueInstant="2013-03-04T20:14:33.800Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" ProviderName="https://yourinstance.service-now.com/navpage.do" Version="2.0">
 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://yourinstance.service-now.com</saml2:Issuer>
 <saml2p:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"/>
 <saml2p:RequestedAuthnContext Comparison="exact">
  <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:
2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
 </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

ServiceNow will..

1. Build an AuthnRequest XML document
2. Generate a RelayState



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

Your request REQ0010001 has been approved
IT Service Desk
Sent: Friday, March 1, 2013 11:55 AM
To: Jason Petty

Click here to view Reques REQ0010001

Number: REQ0010001
Due date: 2013-03-06 10: 4:45 PST
Opened: 2013-03-01 10:5 :45 PST
Approval: Approved

https://empjpetty.service-now.com/nav_to.do?uri=sc_request.do%3Fsys_id=7cbb14eafcbbbc00e5e3cfe5fabcfc42%26sysparm_stack=sc_request_list.do%3Fsysparm_query=active=true

Requested items:
RITM0010001: Blackberry, Stage: Procure Blackberry Hardware

Ref:MSG0023663

© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

ServiceNow will…

1. Build an AuthnRequest XML Document
2. Generate a RelayState



- Default RelayState will be instance URL
  - RelayState = https://myinstance.service-now.com/navpage.do
- If a deep link is used in "nav_to.do" format, then that will be used as the Relay State instead
  - RelayState = https://myinstance.service-now.com/nav_to.do?uri=sc_request.do

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Build an AuthnRequest XML Document
2. Generate a RelayState
3. Create encoded URL parameters for the AuthnRequest and RelayState
4. Tell client browser to redirect to the IdP URLwith the encoded URL parameters



© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

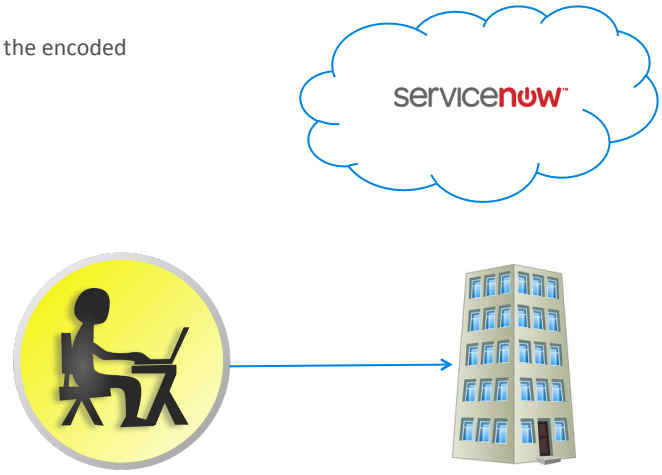
ServiceNow tells the browser to redirect to the IdP with provided AuthnRequest and RelayState parameters



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

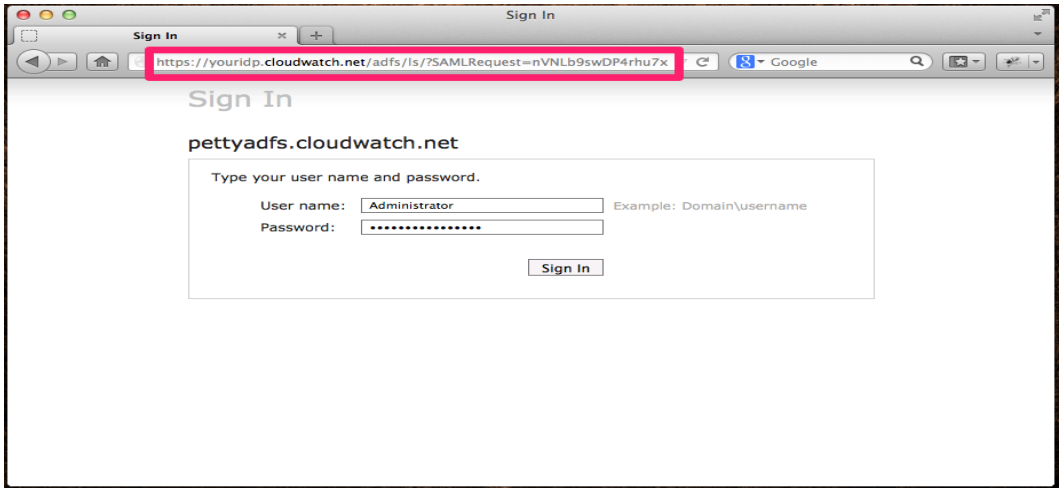
The browser then redirects to the URL and sends the encoded URL parameters provided by ServiceNow



© 2014 ServiceNow All Rights Reserved

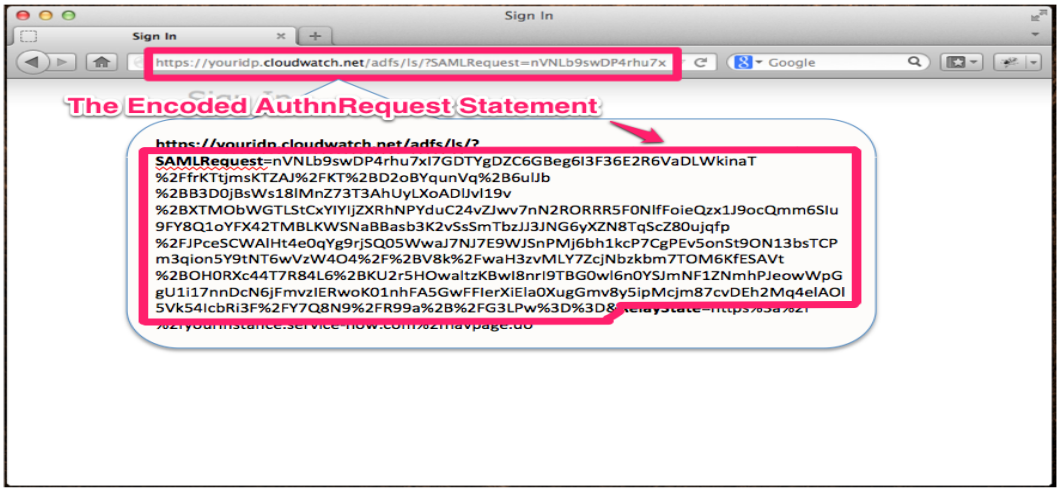
®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

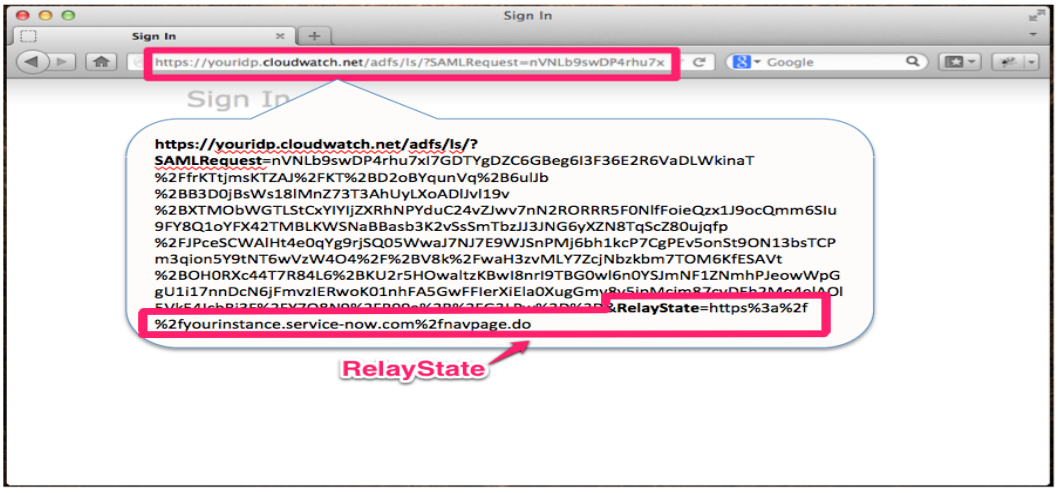
Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



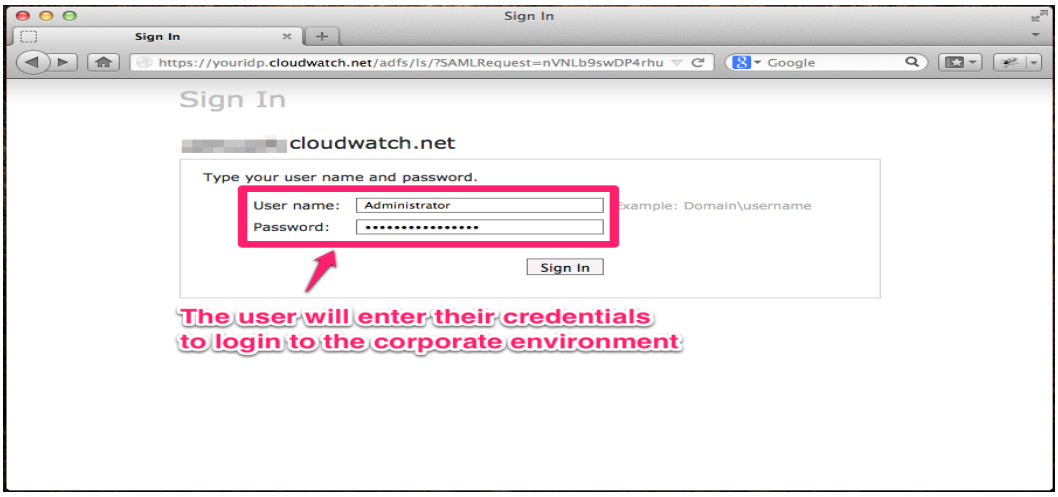
The Corporate Identity Provider (IdP) will then…

1. Decode the AuthnRequest statement
2. Save the RelayState for future use
3. Provide a login page for the user (if they do not already have an active session)

© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



The Corporate Identity Provider (IdP) will then…

1. Decode the AuthnRequest statement
2. Save the RelayState for future use
3. Provide a login page for the user (if they do not already have an active session)
4. Tell the browser to redirect back to ServiceNow with the SAMLResponse and RelayState as POST parameters

© 2014 ServiceNow All Rights Reserved

©2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

The IdP tells the browser to redirect back to ServiceNow with a form POST containing a SAMLResponse & RelayState



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

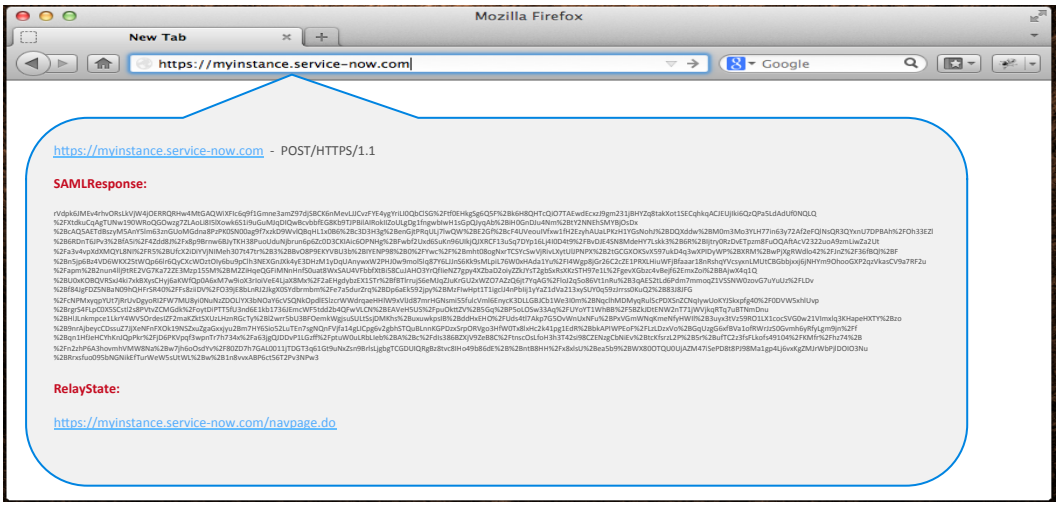
The browser redirects to ServiceNow while POSTing the parameters from the IdP



© 2014 ServiceNow All Rights Reserved

©2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse



© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token



© 2014 ServiceNow All Rights Reserved

©2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

```
<Subject>
      <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">itam@yourcompany.com</
NameID>
      <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm      arer">
        <SubjectConfirmationData InResponseTo="SNCb014ba4cfabf      030357d180e6853"
NotOnOrAfter="2013-03-05T16:34:32.429Z" Recipient="https://yourins      ce.service-now.com/navpage.do" />
      </SubjectConfirmation>
    </Subject>
```

Match NameID token with appropriate field in sys_user table

User ID	Name ▲		
antione.mccleary	Antione Mccleary		tru
antony.thierauf	Antony Thierauf		tru
approver	Approver User	approve ample.com	tru
armando.kolm	Armando Kolm	armand @example.com	tru
armando.papik	Armando Papik	armando. ik@example.com	tru
ashley.leonesio	Ashley Leonesio	ashley.leonesio@example.com	tru
itam	Asset Manager	itam@example.com	tru
athena.fontanilla	Athena Fontanilla	athena.fontanilla@example.com	tru
audra.cantu	Audra Cantu	audra.cantu@example.com	tru
avery.parbol	Avery Parbol	avery.parbol@example.com	tru
barbara.hindley	Barbara Hindley	barbara.hindley@example.com	tru
bart.hachey	Bart Hachey	bart.hachey@example.com	tru

© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table
5. Authenticate as that user



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table
5. Authenticate as that user
6. Redirect to the URL specified in the RelayState parameter



© 2014 ServiceNow All Rights Reserved

©2014 ServiceNow, Inc. All rights reserved.

Lab Goal

Before we set up the SAML 2.0 authentication in ServiceNow we need to have an email and an Identity Provider to do so. This lab steps though the process of setting up those dependencies.

Lab 1
Setup Temp Email and SSOCircle Accounts

Create Temporary Email Address

NOTE: Any email address can be used, however for this exercise you will create a free temporary email address that will be available for 45 minutes and can be used to activate your SSOCircle account.

1. Open a browser, preferably Chrome or Firefox and navigate to one of the following URLs:

   www.explodemail.com
   www.fakeinbox.com
   www.temp-mail.org
   www.getairmail.com

2. Follow instructions from the site you picked to obtain the temporary email.

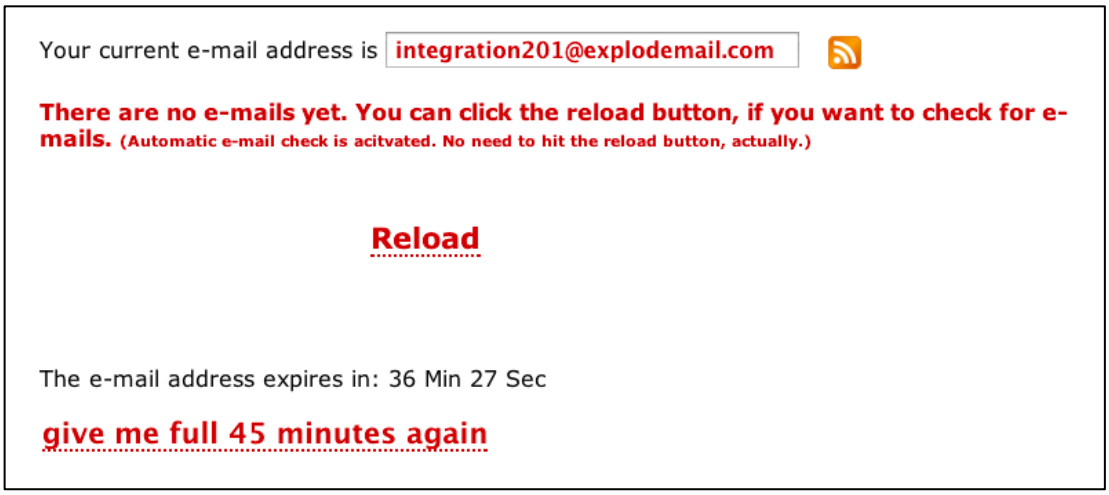
NOTE: The following steps are only valid if you selected **explodemail** as the temporary email address.

©2014 ServiceNow, Inc. All rights reserved.

3. Click **get temporary e-email** or enter your desired prefix and click **set temporary e-email**, as show below.



4. Click **Reload** until your email address account is created.



5. Write down your temporary email here: _____

©2014 ServiceNow, Inc. All rights reserved.

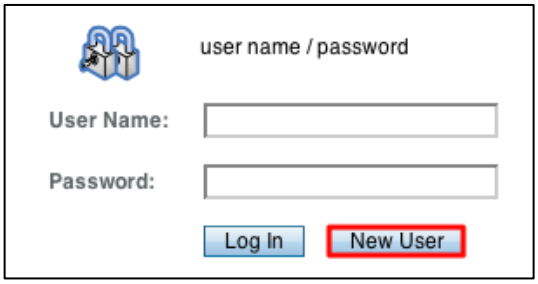
Create SSO Account

1. Open a new tab in the browser and navigate to www.ssocircle.com.

2. Click **Sign In / Register**.

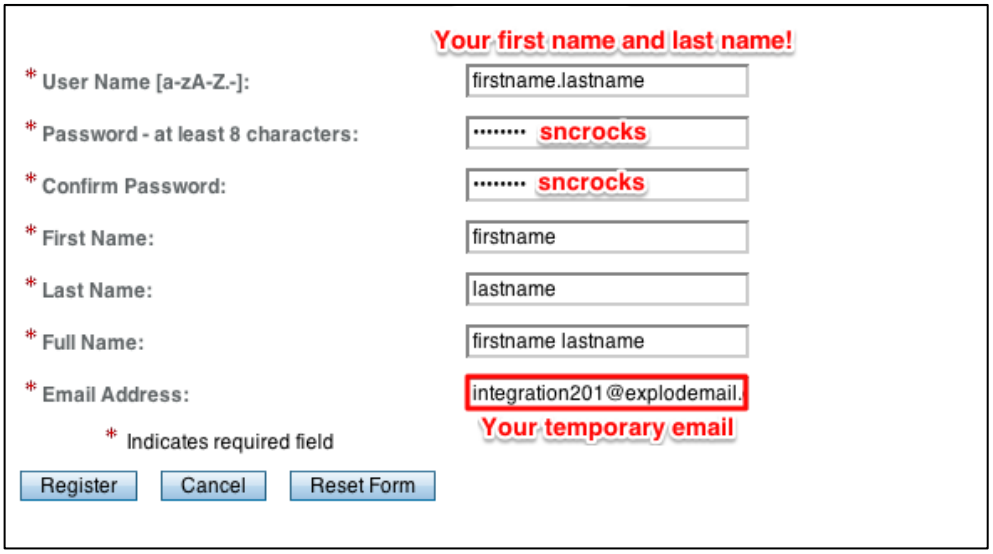


3. Click **New User**.



®2014 ServiceNow, Inc. All rights reserved.

4. Complete the form as shown below.



5. Click **Register**.

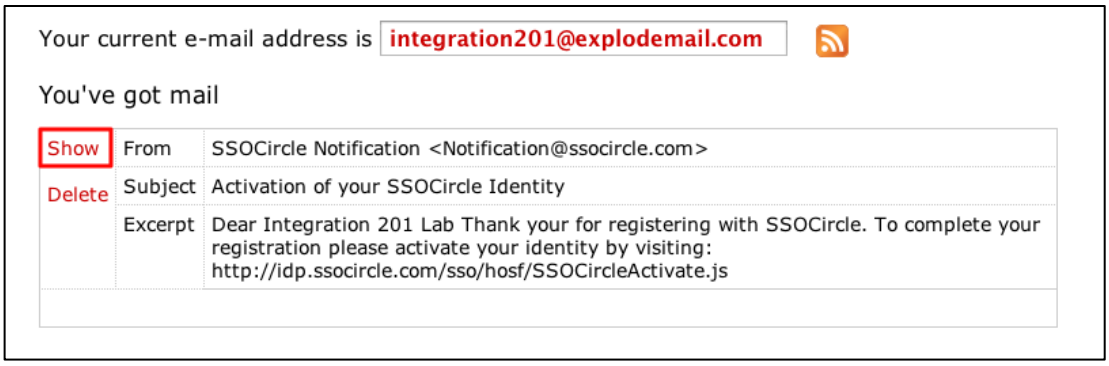
6. Click **Agree**.

7. Go back to your temporary email site and wait for the SSOCircle activation email to arrive.

   NOTE: This may take a few minutes. Depending on your browser, the email may be filtered and not appear. Some browsers may take longer than others. Chrome tends to receive the fastest response.

©2014 ServiceNow, Inc. All rights reserved.

8. After the email arrives, click the **Show** link (Hint: depending on the email service you picked this may look slightly different).



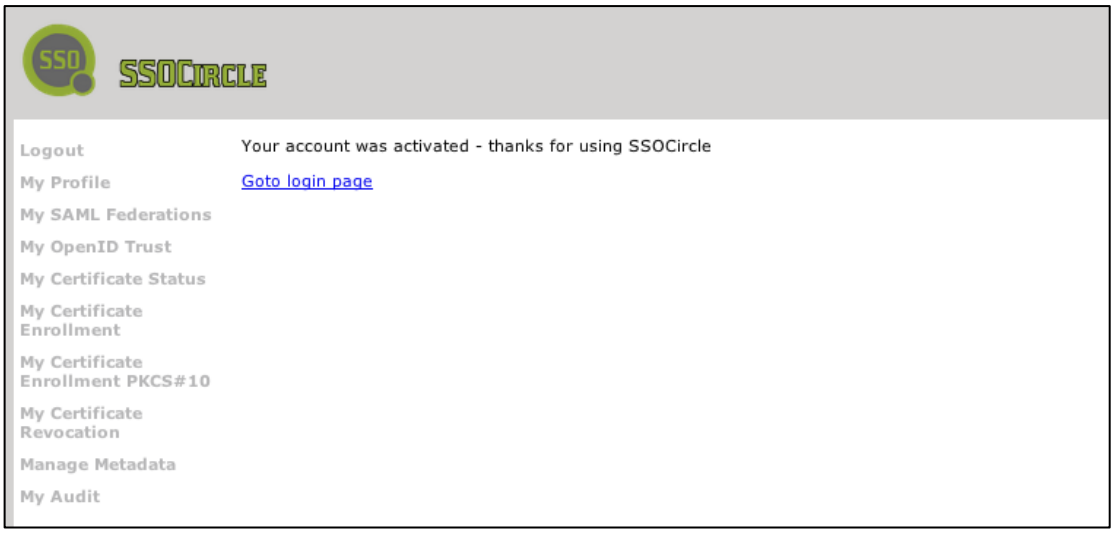
9. Copy and paste the full link provided in the email from **SSOCircle** into a browser to activate your account.



©2014 ServiceNow, Inc. All rights reserved.

Lab Success Verification

1. Verify you received a message that your account was activated as shown below.

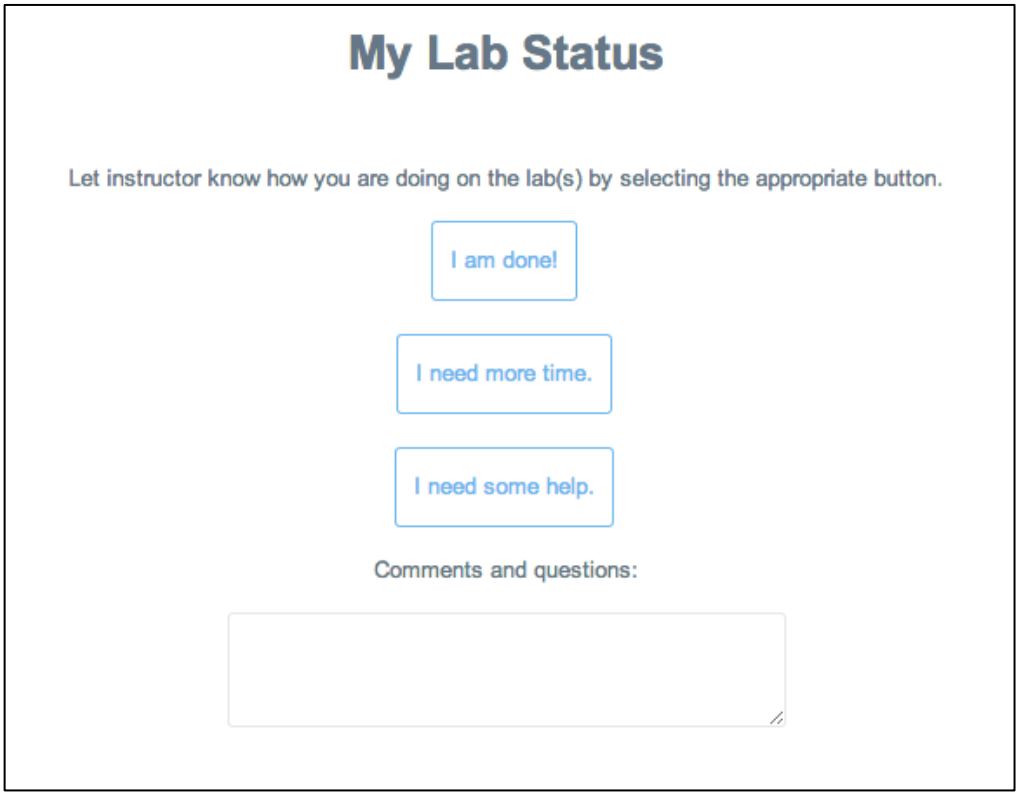


Mark Completion of this lab

1. Navigate to the **Lab Management > Report Lab Progress**.

©2014 ServiceNow, Inc. All rights reserved.

2. Click on **I'm Done** button to notify your instructor that you are done with the lab exercise.



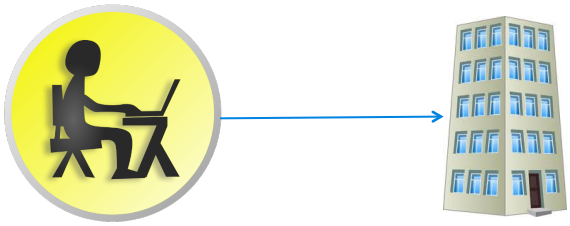
NOTE: Click the other buttons for future labs if you need more time or some help.

®2014 ServiceNow, Inc. All rights reserved.

Identity Provider Initiated Logon

The user logs into the company portal and then choses to go to ServiceNow from the Portal





© 2014 ServiceNow All Rights Reserved

Identity Provider Initiated Logon



The Corporate portal will then…

1. Build and encode an XML-based SAML Response Document
2. Tell the browser to redirect back to ServiceNow with the SAMLResponse as a POST parameter

© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Identity Provider Initiated Logon

The browser redirects to ServiceNow while POSTing the parameter from the IDP



© 2014 ServiceNow All Rights Reserved

Identity Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table
5. Authenticate as that user

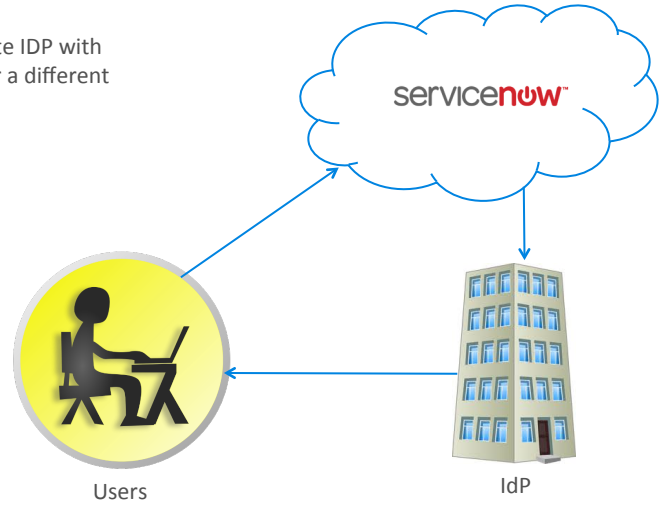


© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Identity Provider Initiated Logon

You have now successfully linked up the corporate IDP with ServiceNow and users will not have to remember a different login.



© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Lab Goal

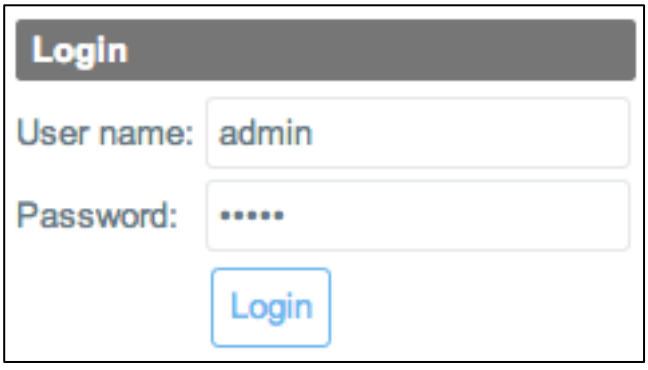
This lab will take you through enabling the SAML 2.0 Update 1 plugin and configuring the SAML 2.0 Authentication.

Lab 2
Setup SAML 2.0

Instance Login

1. Your instructor will provide you with your own instance URL.

2. Log into your instance using the username **admin** and the password **admin**.



©2014 ServiceNow, Inc. All rights reserved.

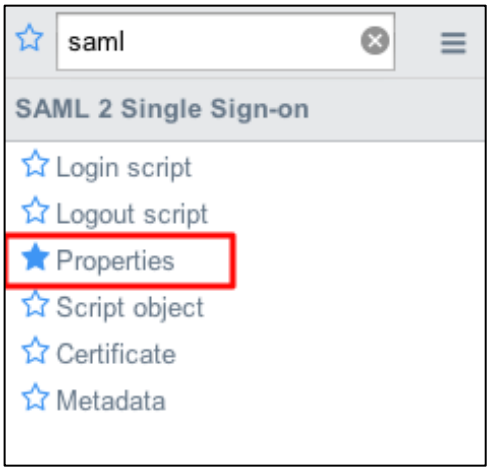
Enable SAML 2.0 Plugin

1. The **SAML 2.0 Single Sign-On Update 1: security enhancements** plugin has been enabled for you already in the lab instance.

NOTE: In a real instance you need to request this plugin to be enabled via HI. System administrators cannot activate this plugin by themselves.

Create an SSO Account

1. After the plugin is activated, navigate to **SAML 2 Single Sign-on > Properties.**



NOTE: There are several base URL properties that are preconfigured for SSOCircle out-of-the-box when the plugin is installed. We have removed the settings and are going to walk through those so you understand where they come from. These properties can be found in an XML document provided by SSOCircle at https://idp.ssocircle.com.

©2014 ServiceNow, Inc. All rights reserved.

2. Open your browser to https://idp.ssocircle.com. This XML metadata page is where you can obtain the property values to configure SAML 2.0 in your ServiceNow instance. The values you need to extract are highlighted below:

   - **EntityID**
   - **ds:X509Certificate**
   - **SingleLogoutService** (HTTP-Direct Binding)
   - **NameIDFormat** (emailAddress)
   - **SingleSignOnService** (HTTP-Direct Binding)



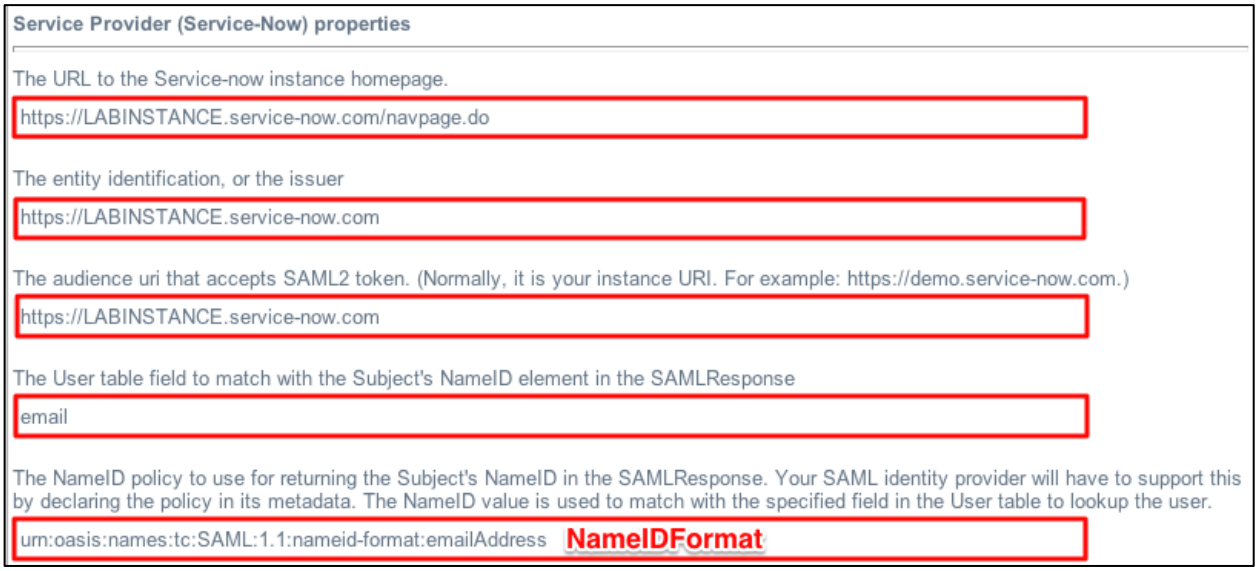
®2014 ServiceNow, Inc. All rights reserved.

```
<ArtifactResolutionService index="0" isDefault="true"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/ArtifactResolver/metaAlias/ssocircle"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idp.ssocircle.com:443/sso/IDPSloPost/metaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPSloPost/metaAlias/ssocircle"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/IDPSloSoap/metaAlias/ssocircle"/>
<ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ssocircle.com:443/sso/IDPMniRedirect/metaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPMniRedirect/metaAlias/ssocircle"/>
<ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idp.ssocircle.com:443/sso/IDPMniPOSTmetaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPMniPOST/metaAlias/ssocircle"/>
<ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/IDPMniSoap/metaAlias/ssocircle"/>
▼<NameIDFormat>
   urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
</NameIDFormat>
▼<NameIDFormat>
   urn:oasis:names:tc:SAML:2.0:nameid-format:transient
</NameIDFormat>
▼<NameIDFormat>
   urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
</NameIDFormat>
▼<NameIDFormat>
   urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
</NameIDFormat>
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idp.ssocircle.com:443/sso/SSOPOST/metaAlias/ssocircle"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/SSOSoap/metaAlias/ssocircle"/>
<NameIDMappingService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/NIMSoap/metaAlias/ssocircle"/>
</IDPSSODescriptor>
```

©2014 ServiceNow, Inc. All rights reserved.

3. Configure these settings in the **SAML 2.0 Single Sign-on properties** page as shown in the diagram below.





IMPORTANT: Remember to replace **LABINSTANCE** with the full name of your lab instance name.

©2014 ServiceNow, Inc. All rights reserved.

4. Click **Turn on debug logging for SAML 2.0 Authentication** to enable debugging.



5. Click **Save**.

6. Navigate to **SAML 2 Single Sign-on > Certificate**.

7. Open the **SAML 2.0** Certificate record.

8. Paste the **ds:X509Certificate** text you copied from the XML metadata in Step 2 under the **PEM Certificate** field.

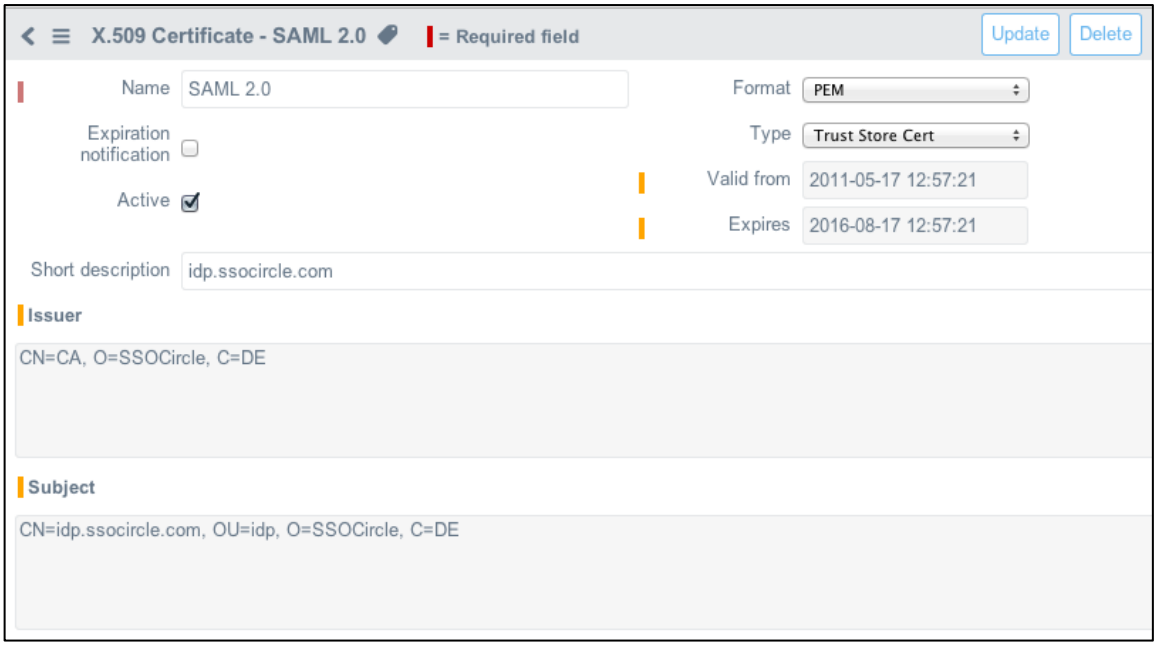


IMPORTANT: The certificate text must be copied in between the -----*BEGIN CERTIFICATE*----- and -----*END CERTIFICATE*----- text.

©2014 ServiceNow, Inc. All rights reserved.

9. Right click on the title bar and select **Save**.

10. Ensure the **Issuer**, **Subject**, **Valid from** and **Expires** fields are populated correctly as shown below.



Configure Metadata

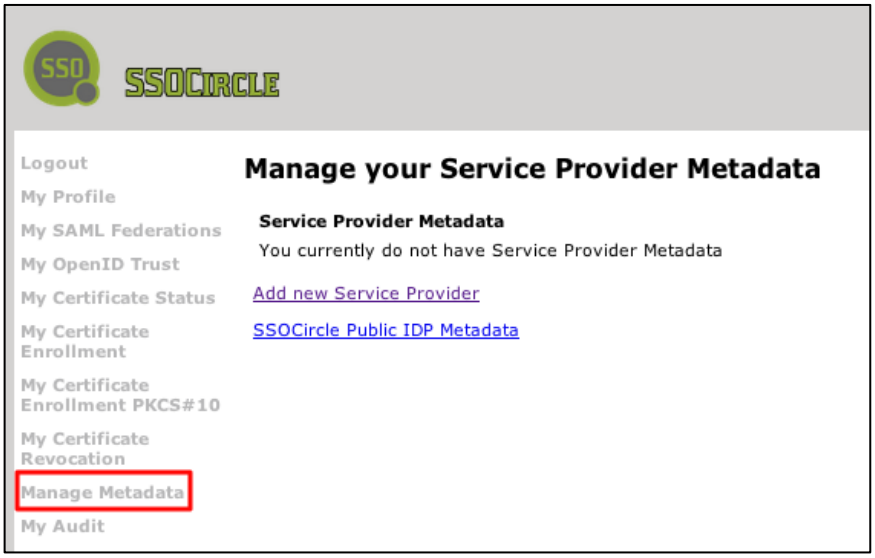
1. Navigate to **SAML 2 Single Sign-on > Metadata**.

2. Copy the metadata text displayed.

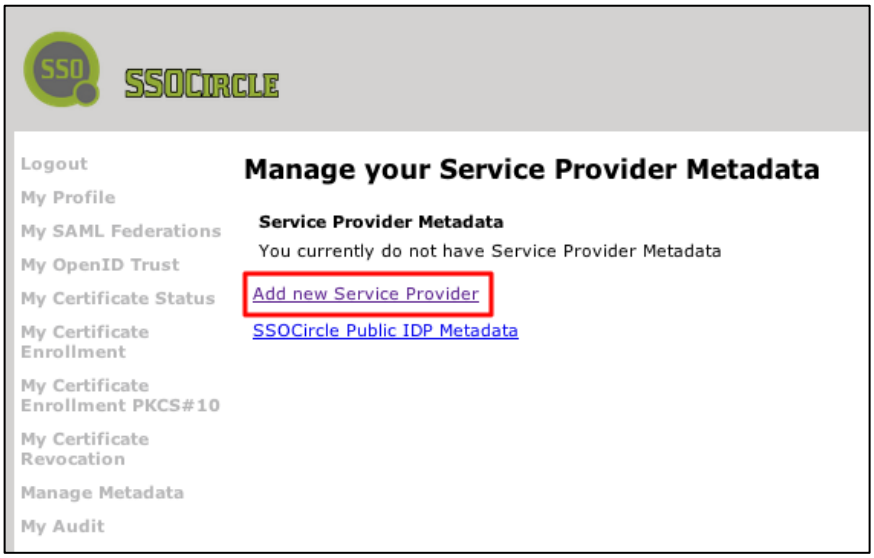
3. Go back to SSOCircle and log in using your username and password entered earlier during registration.

©2014 ServiceNow, Inc. All rights reserved.

4. From the left pane, click **Manage Metadata.**

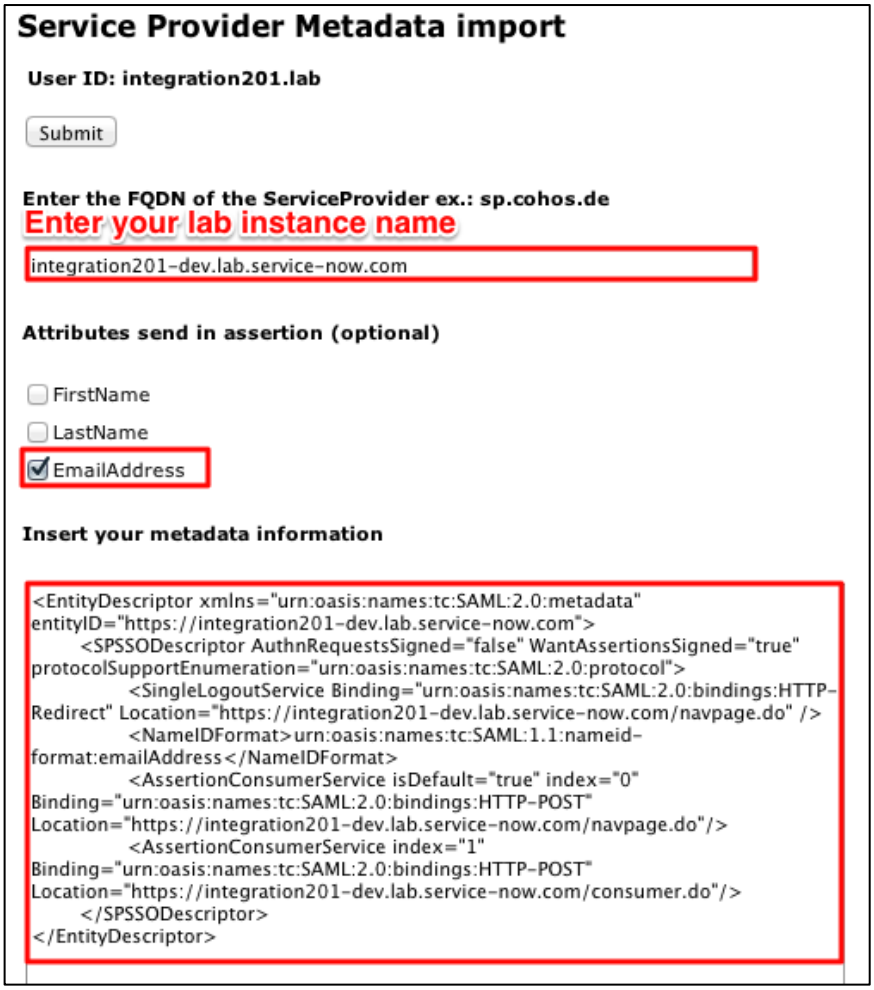


5. Click **Add new Service Provider link**.



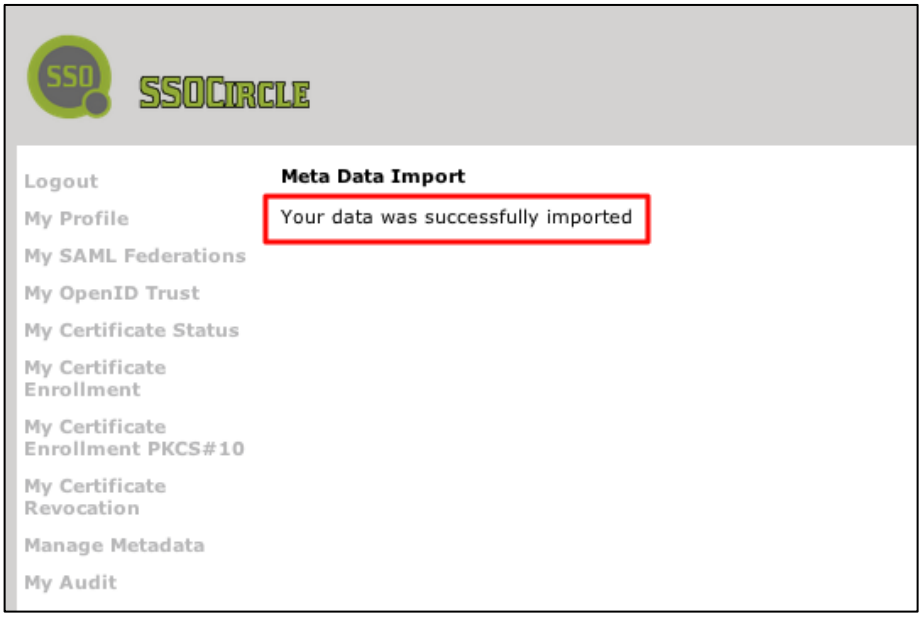
©2014 ServiceNow, Inc. All rights reserved.

6. Complete the form as shown below by entering the fully qualified domain name (FQDN) of your ServiceNow lab instance. Select **EmailAddress** checkbox to send in the assertion, and paste the metadata you just copied in Step 2.



©2014 ServiceNow, Inc. All rights reserved.

7. Click **Submit** and ensure you metadata is successfully imported.



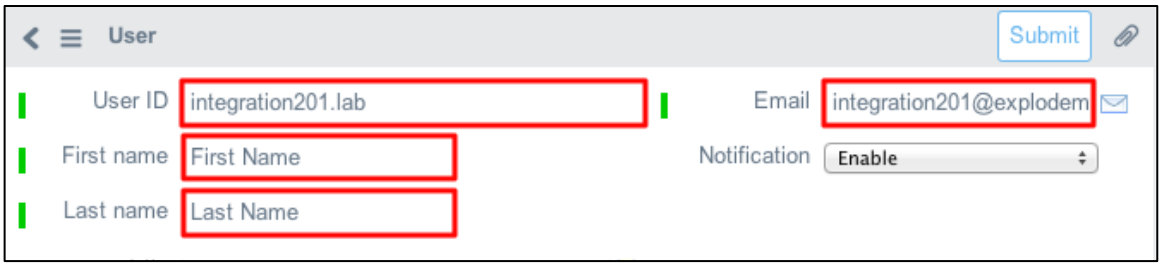
Configure SSO in ServiceNow

1. From your ServiceNow instance navigate to **User Administration > Users**.

2. Click **New.**

©2014 ServiceNow, Inc. All rights reserved.

3. Create a new account for yourself as shown. Remember to enter the same temporary email address used for your SSOCircle account.



NOTE: Your email address is used as the reconciliation key between your SSOCircle and ServiceNow accounts. Therefore, it must match exactly.

4. Right-click the form header and choose **Save.**

5. Under the **Roles** related list tab, click **Edit** and assign **admin** role to this user account.

6. Click **Save**.

Enable SAML 2.0 for Single Sign-On

1. Log out of your ServiceNow instance and SSOCircle account and close your browser.

2. Open your browser and navigate to your ServiceNow instance URL.

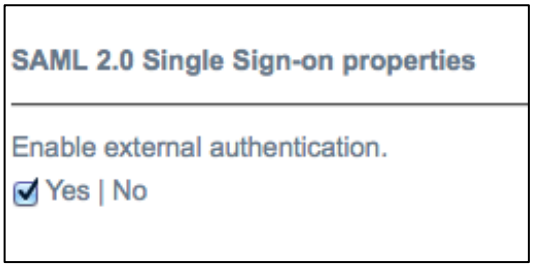
©2014 ServiceNow, Inc. All rights reserved.

NOTE: You are still presented with the ServiceNow login screen because SAML 2.0 is not currently enabled.

3. Login with **admin/Knowledge14.**

4. Navigate to **SAML 2 Single Sign-on > Properties.**

5. Select **Enable external authentication** to enable SAML 2.0 authentication.



6. Click **Save.**

®2014 ServiceNow, Inc. All rights reserved.

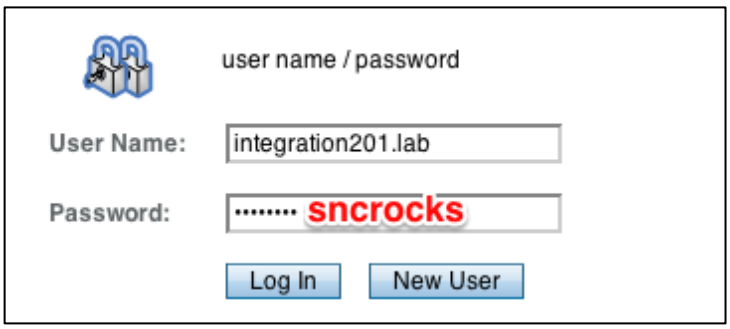
Lab Success Verification

1. Log out of ServiceNow and then close your browser.

2. Open a new browser session and navigate to your ServiceNow instance.

NOTE: You should be redirected to SSOCircle login page. If you run into any errors and need to log back into your personal instance you can enter https://<LABINSTANCE>.lab.service-now.com/login.do to bypass the SSO login screen.

3. Enter your **User Name** and **Password** as configured on SSOCircle earlier.



4. Click **Log In** to successfully login to your instance using Single Sign-On.

NOTE: It is important to note in an enterprise implementation of SSO, the third party SAML identity provider will query an LDAP store in the customer's network during login. An LDAP integration is needed to import those users into ServiceNow in order to match them up on our side during login and assign the appropriate roles.

Mark Completion of this lab

1. Navigate to the **Lab Management > Report Lab Progress**.

2. Click on **I'm Done** button to notify your instructor that you are done with the lab exercise.

©2014 ServiceNow, Inc. All rights reserved.

Tools for SAML

- Logs in ServiceNow Instance (Can be turned on and off)
- SAML 2.0 Encoder/Decoder
  - https://rnd.feide.no/simplesaml/module.php/saml2debug/debug.php
- Trace with Chrome
  - View > Developer > Developer Tools
- Trace with Firefox
  - Tools > Web Developer > Web Console
- Tracing with Fiddler
  - http://www.fiddler2.com/fiddler2/

© 2014 ServiceNow All Rights Reserved

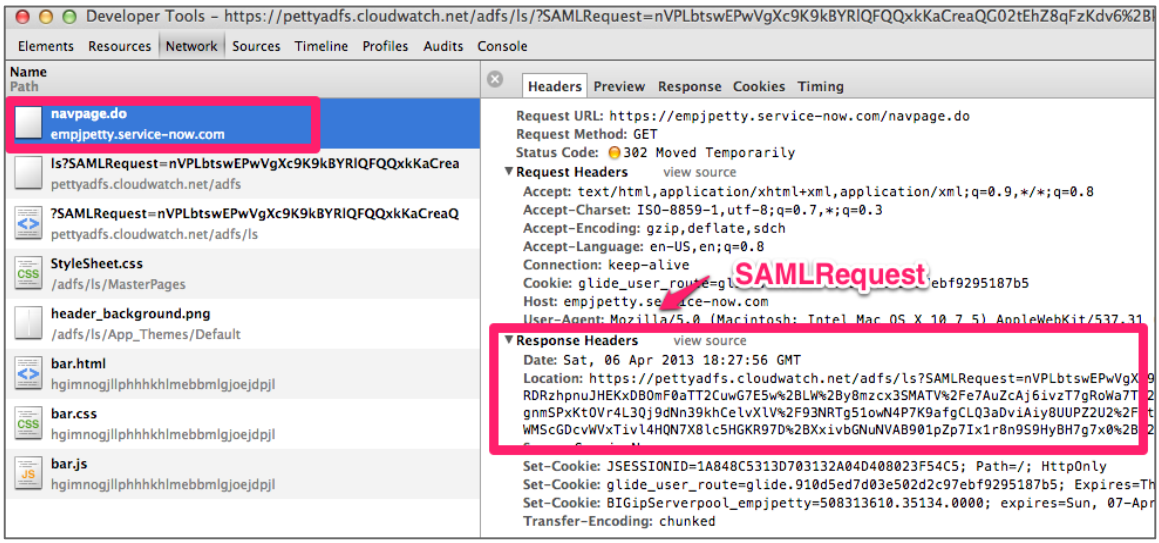
Logs in ServiceNow Instance

2013-04-06 12:35:42	Information	Got signature
2013-04-06 12:35:42	Information	Issue Instant: 2013-04-06T19:35:41.939Z
2013-04-06 12:35:42	Information	Conditions validated.
2013-04-06 12:35:42	Information	Public key created
2013-04-06 12:35:42	Information	SAML Response xml: <samlp:Response ID="_40482050-da77-49a9-89db-7f0c1545d458" Version="2.0" Is Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></samlp:Status><Assertion ID="_f06e9d98-e7b0-4 /><ds:Reference URI="#_f06e9d98-e7b0-43ec-a7e3-45cedde4f021"><ds:Transforms><ds:Transform Algo /cFgaBeolUO1ucnHddgz+inJXIIPHzHRxfkltaOpW5cmQ7Kd4Y/GayqCtjGHSyXAYVFrStEclqslnwK/tHqJeG <ds:X509Certificate>MIIC7DCCAdSgAwIBAgIQERQqiQ0aVq5K+5l9udsU3DANBgkqhkiG9w0BAQsFADAy /Svhtj4avCN5eXTuCrliUWGxlZ4ORU/7ZTUL+qR13asTbyPtlIL1RVDYQMndmvfU8zCFPArcNkm+XnO7fuc: /hDZUrvP2LbBqQuTtBcGu10M6Dsd++eIW95YH5D5gFkboGks8AbwZr8PPeu1JmTRq9JJTslYkkqvNUNE2 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData InResponseTo="SNC2ad8c Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"><AttributeValue>jason.petty
2013-04-06 12:35:37	Information	requestURI: /navpage.do
2013-04-06 12:35:37	Information	SAML Request xml: <saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Assert now.com</saml2:Issuer><saml2p:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:1.
2013-04-06 12:35:37	Information	Generating a Relay State of: https://empjpetty.service-now.com/navpage.do
2013-04-06 12:35:37	Information	Stripping down the serviceURL: https://empjpetty.service-now.com/navpage.do to a base URL of: https://en
2013-04-06 12:35:37	Information	Redirecting to: https://pettyadfs.cloudwatch.net/adfs/ls?SAMLRequest=nVPLbtswEPwVgXc93cgJYRlQFR(/7fjiSkH7uujZuv266qcFOCnD3gf2vlr%2BDw5Bd0JdkZLmYoqeTcne%2Bjcui2MsKyPKv0xfp%2BYzTxJ6O2
2013-04-06 12:35:37	Information	Query String (qs): null
2013-04-06 12:35:34	Information	Redirecting to: https://pettyadfs.cloudwatch.net/adfs/ls?SAMLRequest=nVPLbtswEPwVgXe9LNtJCcuAqqC %2Bx6fUlGlosxejoq95fbuC6KvayALP86fZFezjhPdHTQvrprrJL8OaqUsofaAwu9n%2BA7GFejWXhfRp7kYC
2013-04-06 12:35:34	Information	Query String (qs): null
2013-04-06 12:35:34	Information	Stripping down the serviceURL: https://empjpetty.service-now.com/navpage.do to a base URL of: https://en

© 2014 ServiceNow All Rights Reserved

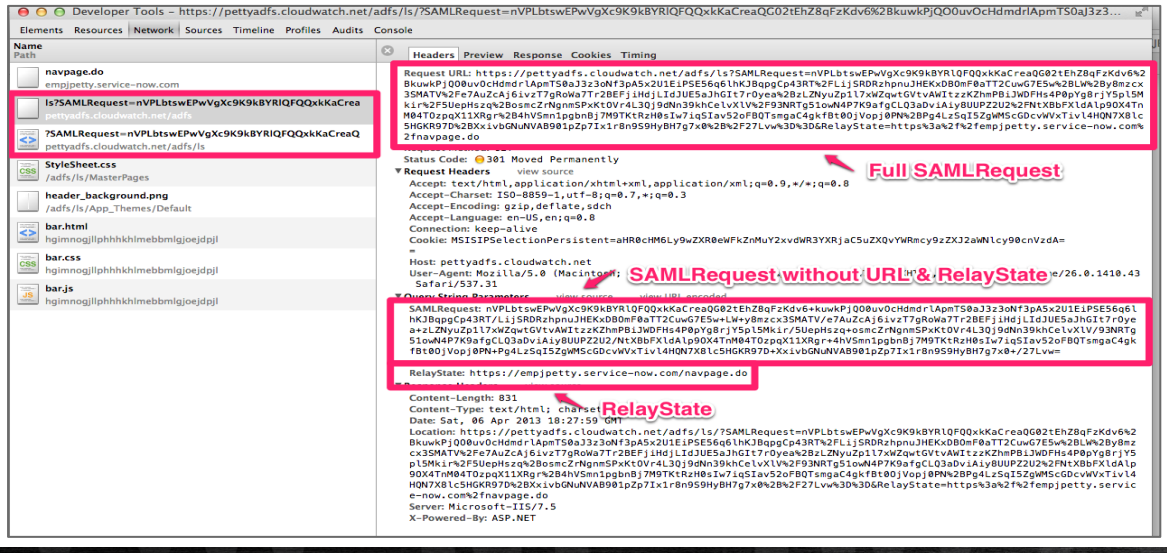
®2014 ServiceNow, Inc. All rights reserved.

Tracing In Chrome



© 2014 ServiceNow All Rights Reserved

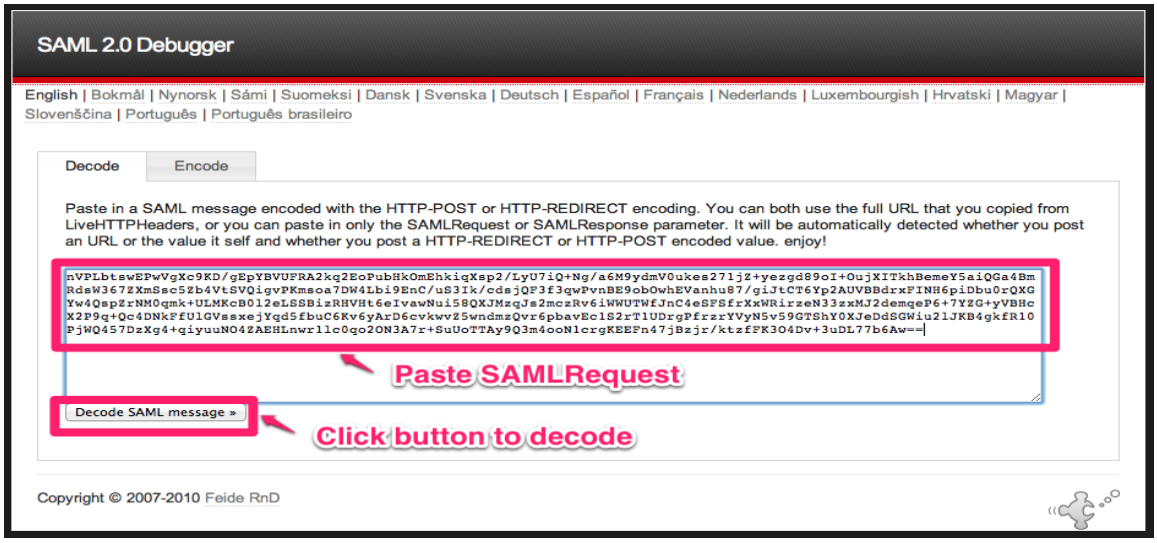
Tracing In Chrome



© 2014 ServiceNow All Rights Reserved

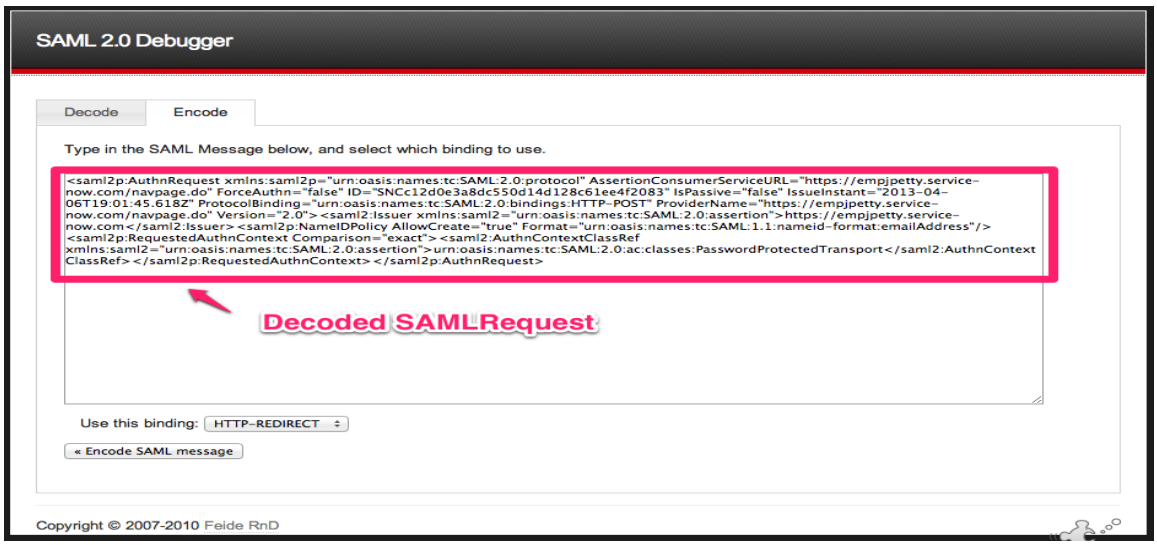
®2014 ServiceNow, Inc. All rights reserved.

Tracing In Chrome



© 2014 ServiceNow All Rights Reserved

Tracing In Chrome



© 2014 ServiceNow All Rights Reserved

®2014 ServiceNow, Inc. All rights reserved.

Lab Goal

This lab will take you through using Chrome to trace your SAML 2.0 authentication.

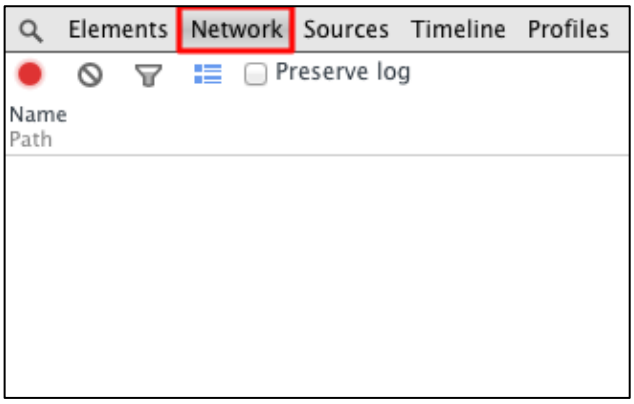
Lab 3
Trace Your Own SAML Login

Trace Your Login With Chrome

1. Launch Chrome and ensure you're logged out of ServiceNow and SSOCircle.

2. Click on **View > Developer > Developer Tools.**

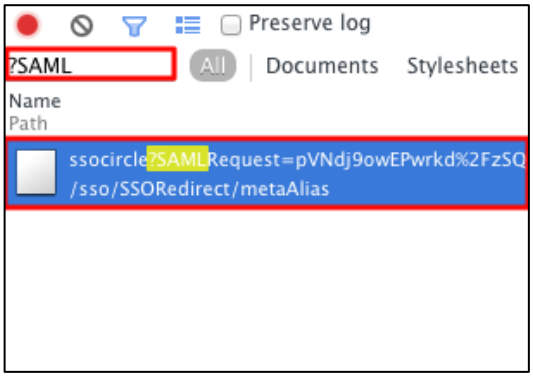
3. Click on **Network** tab.



4. Go to your ServiceNow instance URL.

©2014 ServiceNow, Inc. All rights reserved.

5. Find in the first column entry a transaction containing the text **?SAML**. (Hint: you can use the filter button to easily locate the transaction)

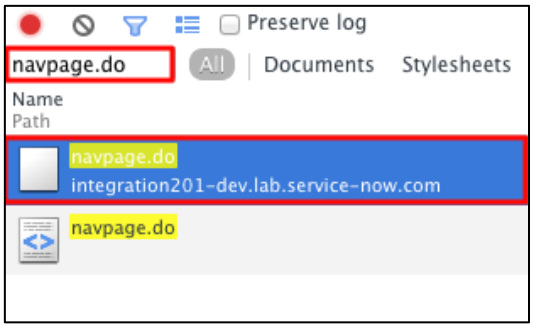


6. Take a look at the **Request URL**, under the Headers section on the right page.



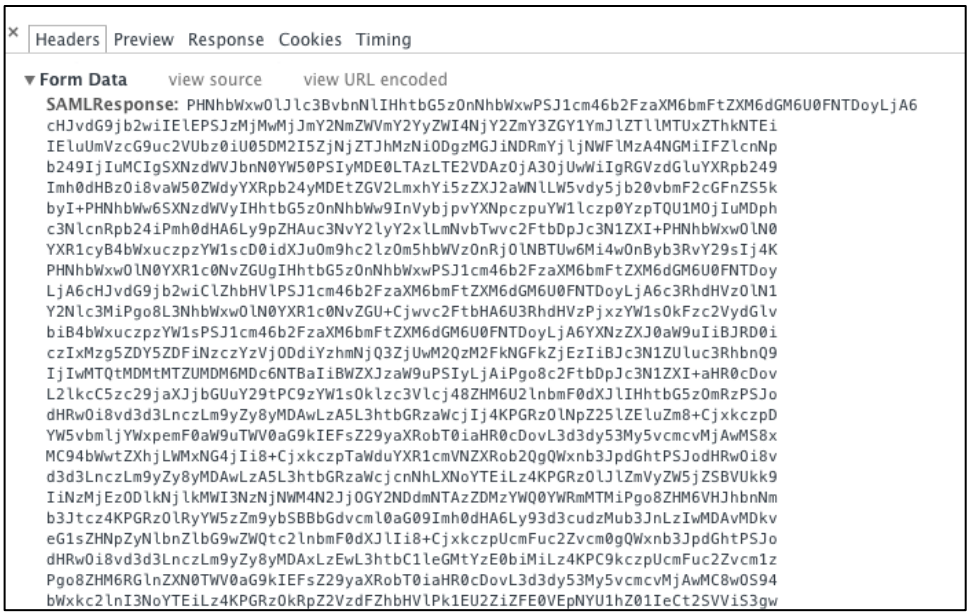
7. Log in to your instance at the SSOCircle login prompt.

8. Scroll all the way to the top of your trace and find the first column entry with **navpage.do**.

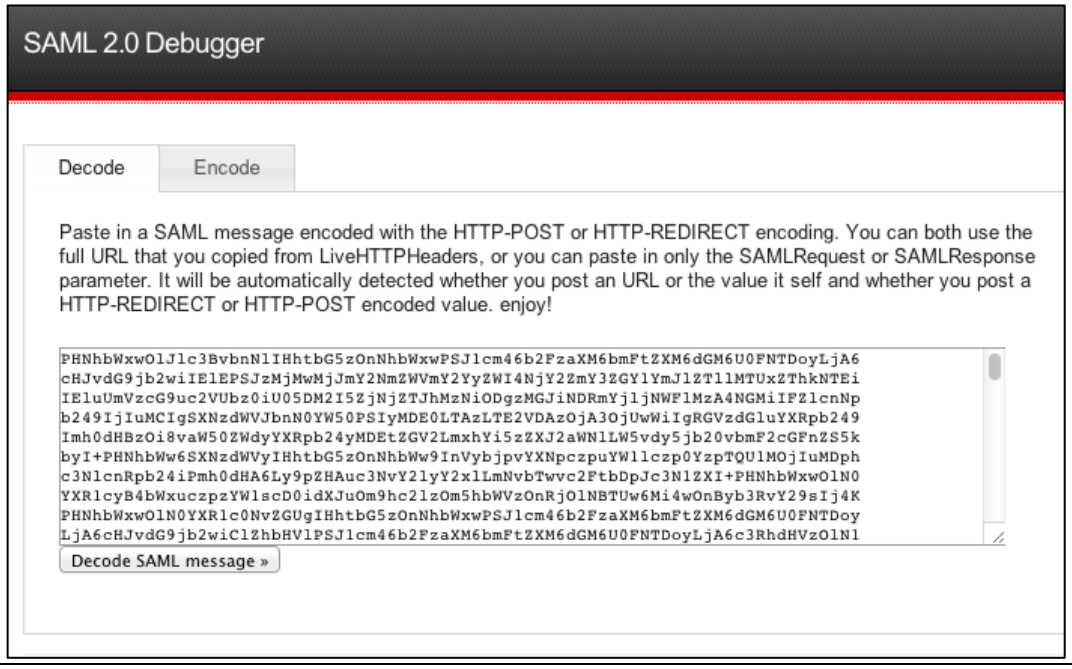


©2014 ServiceNow, Inc. All rights reserved.

9. Take a look at the Headers section and find the **SAMLResponse.** Select and copy the encoded text.



10. Use the SAML 2.0 Debugger to decode the SAMLResponse and look at it.



©2014 ServiceNow, Inc. All rights reserved.

Deactivate Single Sign-On

1. Navigate to **SAML 2 Single Sign-on > Properties**.
2. Unselect **Enable external authentication** to disable SAML 2.0 authentication.
3. Click **Save**.

Mark Completion of this lab

1. Navigate to the **Lab Management > Report Lab Progress**.
2. Click on **I'm Done** button to notify your instructor that you are done with the lab exercise.

©2014 ServiceNow, Inc. All rights reserved.

Additional Resources

SAML 2.0 Decoder/Encoder
https://rnd.feide.no/simplesaml/module.php/saml2debug/debug.php

Tracing with Fiddler
http://www.fiddler2.com/fiddler2/

Setting up OpenAM as your IDP for ServiceNow
https://community.servicenow.com/people/jason.petty/blog/2013/04/05/2638

Configuring ADFS for SAML 2.0
http://wiki.servicenow.com/index.php?title=Configuring_ADFS_2.0_to_Communicate_with_SAML_2.0

SAML 2.0 Browser Profile
http://wiki.servicenow.com/index.php?title=SAML_2.0_Web_Browser_SSO_Profile

SAML 2.0 Troubleshooting
http://wiki.servicenow.com/index.php?title=SAML_2.0_Troubleshooting

SAML 2.0 On-Demand Login/User Provisioning
https://community.servicenow.com/message/683704

©2014 ServiceNow, Inc. All rights reserved.