Single Sign On (Session 1)

Initially created by Ashish Sharma

Topics covered:

- SSO Overview and benefits
- Types of SSO: FEDERATED SSO (SAML based)   Delegated SSO
- ++Federated SSO++
- Execution Flow
- Difference between Service provider and Identity provider
- Salesforce as Service Provider
- Login in Salesforce Org Using Axiom using IDP initiated and SP initiated flows.
- Login in Salesforce Community Using Axiom using IDP initiated and SP initiated flows.
- Capture SAML response, Validation and some generic errors.

Overview

Single sign-on (SSO) lets users access authorized network resources with one login. You validate usernames and passwords against your corporate user database or other client app rather than Salesforce managing separate passwords for each resource.

Benefits of SSO

Implementing SSO brings several advantages to your org.

- **Reduced administrative costs**—With SSO, users memorize a single password to access network resources and external apps and Salesforce.
- **Leverage existing investment**—Many companies use a central LDAP(Lightweight Directory Access Protocol) database to manage user identities. You can delegate Salesforce authentication to this system.
- **Time savings**—On average, users take 5–20 seconds to log in to an online app. It can take longer if they mistype their username or password and are prompted to reenter them.
- **Increased user adoption**—Due to the convenience of not having to log in, users are more likely to use Salesforce regularly. For example, users can send email messages that contain links to information in Salesforce, such as records and reports. When the recipient of the email message clicks the links, the corresponding Salesforce page opens.
- **Increased security**—All password policies that you've established for your corporate network are in effect for Salesforce. Sending an authentication credential that's only valid for a single time also increases security for users who have access to sensitive data.

Salesforce offers the following ways to use SSO.

- Federated authentication using Security Assertion Markup Language (SAML) lets you send authentication and authorization data between affiliated but unrelated web services. You can log in to Salesforce from a client app. Salesforce enables federated authentication for your org automatically.

- Delegated authentication SSO integrates Salesforce with an authentication method that you choose. You can integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or use a token instead of a password for authentication. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

FEDERATED SSO (SAML based)

>> Execution Flow

SAML

Salesforce Identity uses the XML-based Security Assertion Markup Language (SAML) protocol for single sign-on into Salesforce from a corporate portal or identity provider. With SAML, you can transfer user information between services, such as from Salesforce to Microsoft 365.

Your identity provider sends SAML assertions to Salesforce using the SAML web Single Sign-on Browser POST profile. Salesforce sends SAML responses to the identity provider login URL specified under Setup by entering Single Sign-On in the Quick Find box, then selecting **Single Sign-On Settings**. Salesforce receives the assertion, verifies it against your Salesforce configuration, and, if the assertion is true, allows SSO.

There are a few basic terms to remember for Single Sign-On:

1. **Security Assertion Markup Language (SAML):** A language specification for federated authentication.
2. Identity Provider (IdP): The authentication server.
3. Service Provider (SP): An accessible business application.

There will be one Identity Provider and many Service Providers. Identity Providers will authenticate all Service Providers.
Salesforce Single Sign-On Support:
• Salesforce can be the **Identity Provider**, accessing other applications**.**
• Salesforce can also be **Service Provider**, accessed from another authentication server.
SAML Assertion
SAML Assertion is in XML format, and it's sent by Identity Providers. SP validates the IdP using this assertion.
SAML assertion requests mainly have the following components:
• The Identity Provider's digital signature.
• Issuer: The name of the Identity Provider.
• Entity Id: The name of the Service Provider. Generally a URL format. (Example – https://saml.salesforce.com)
• The Subject: The user ID or the Federation ID.

Identity Providers and Service Providers

An identity provider is a trusted provider that lets you use single sign-on (SSO) to access other websites. A service provider is a website that hosts apps. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other apps directly from Salesforce using SSO. SSO is a great help to your users—instead of having to remember many passwords, they only have to remember one.

https://help.salesforce.com/articleView?id=identity_provider_about.htm&type=5

>> Difference between SP and IDP initiated flows

IdP Initiated Single Sign-On:
IdP provides a digital certificate which is then uploaded to a Service Provider.
The user then tries to login to IdP. IdP will send SAML Assertion in request to the proper Salesforce instance (SP). SAML assertion is validated in SP, and If it’s valid, the user gets logged into SP.

Service Provider Initiated Single Sign-On:
In this case, the user has SP URL link, and tries to log into SP. SP redirects to IdP for proper authentication. If authenticated, the user is redirected to the link which was requested.

>> Salesforce as Service Provider

CONFIGURE SAML SETTINGS FOR SINGLE SIGN-ON

Step by step instructions to create Single Sign On settings in Salesforce:
https://developer.salesforce.com/docs/atlas.en-us.sso.meta/sso/sso_saml.htm

ALL IDP ATTRIBUTES:

https://developer.salesforce.com/docs/atlas.en-us.sso.meta/sso/sso_saml_idp_values.htm

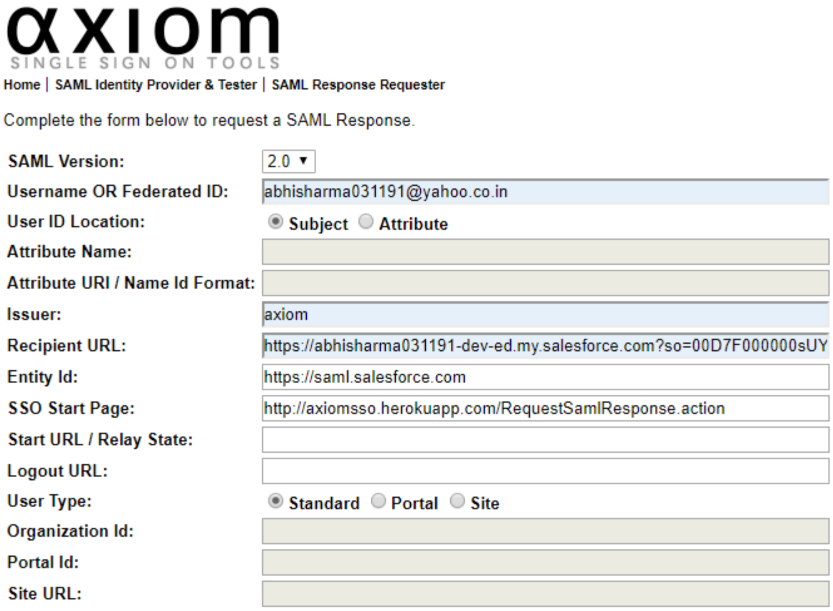
LOGIN INTO SALESFORCE USING AXIOM

Home page URL:
https://axiomsso.herokuapp.com/Home.action

To create the single sign on setting;
https://axiomsso.herokuapp.com/SamlIdpHome.action

- Install this IdP's certificate in the Salesforce org for login to via SAML:
    - Download the Identity Provider Certificate
    - In Salesforce, go to *Setup | Security Controls | Single Sign-On Settings | Federated single sign-on using SAML*
    - Install the dowloaded certificate in the Identity Provider Certificate field
    - Configure the Issuer, User Id Type, and User Id Location settings. These values are arbitrary, but must be matched when generating the SAML Response in the next step.

IMAGE OF AXIOM SETTING FOR MY DEV ORG

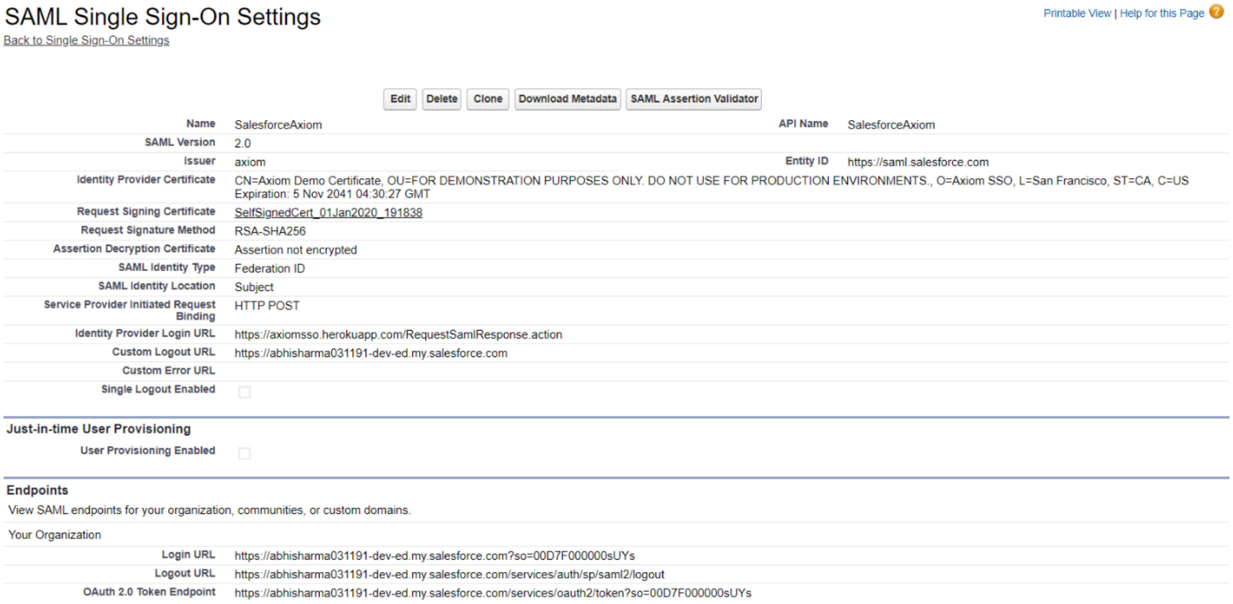


αxιom
SINGLE SIGN ON TOOLS
Home | SAML Identity Provider & Tester | SAML Response Requester

Complete the form below to request a SAML Response.

SAML Version:	2.0 ▾
Username OR Federated ID:	abhisharma031191@yahoo.co.in
User ID Location:	● Subject ○ Attribute
Attribute Name:	
Attribute URI / Name Id Format:	
Issuer:	axiom
Recipient URL:	https://abhisharma031191-dev-ed.my.salesforce.com?so=00D7F000000sUY
Entity Id:	https://saml.salesforce.com
SSO Start Page:	http://axiomsso.herokuapp.com/RequestSamlResponse.action
Start URL / Relay State:	
Logout URL:	
User Type:	● Standard ○ Portal ○ Site
Organization Id:	
Portal Id:	
Site URL:	

IMAGE OF SSO SETTING IN MY DEV ORG(DOUBLE CLICK ON IMAGE TO VIEW PROPERLY)



Printable View | Help for this Page
Back to Single Sign-On Settings
Edit
Delete
Clone
Download Metadata
SAML Assertion Validator

SAML Single Sign-On Settings

Name	SalesforceAxiom	API Name	SalesforceAxiom
SAML Version	2.0		
Issuer	axiom	Entity ID	https://saml.salesforce.com
Identity Provider Certificate	CN=Axiom Demo Certificate, OU=FOR DEMONSTRATION PURPOSES ONLY. DO NOT USE FOR PRODUCTION ENVIRONMENTS., O=Axiom SSO, L=San Francisco, ST=CA, C=US Expiration: 5 Nov 2041 04:30:27 GMT		
Request Signing Certificate	SelfSignedCert_01Jan2020_191838		
Request Signature Method	RSA-SHA256		
Assertion Decryption Certificate	Assertion not encrypted		
SAML Identity Type	Federation ID		
SAML Identity Location	Subject		
Service Provider Initiated Request Binding	HTTP POST		
Identity Provider Login URL	https://axiomsso.herokuapp.com/RequestSamlResponse.action		
Custom Logout URL	https://abhisharma031191-dev-ed.my.salesforce.com		
Custom Error URL			
Single Logout Enabled	□		

Just-in-time User Provisioning

User Provisioning Enabled	□

Endpoints

View SAML endpoints for your organization, communities, or custom domains.

Your Organization

Login URL	https://abhisharma031191-dev-ed.my.salesforce.com?so=00D7F000000sUYs
Logout URL	https://abhisharma031191-dev-ed.my.salesforce.com/services/auth/sp/saml2/logout
OAuth 2.0 Token Endpoint	https://abhisharma031191-dev-ed.my.salesforce.com/services/oauth2/token?so=00D7F000000sUYs

IDP INITIATED FLOW:

After you create Single Sign-on Setting in your org, hit the below link and pass the required parameters, this will send SAML assertion to Salesforce ACS(Assertion Consumer URL)/login URL and if it is valid:

HTTPS://AXIOMSSO.HEROKUAPP.COM/REQUESTSAMLRESPONSE.ACTION

SP INITIATED FLOW:

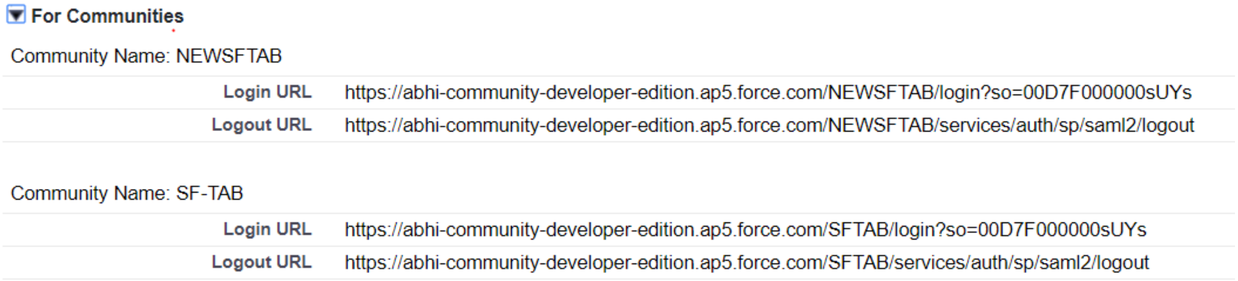
For this flow, we need to configure My domain Settings in Salesforce and check the SSO setting in Authentication Configuration under my domain.

To initiate the flow, hit my domain URL of your local org and click on the SSO button:
https://abhisharma031191-dev-ed.my.salesforce.com/

This will send SAML Request to IDP destination URL and you need to pass the required parameters. After which you will be redirected to Salesforce ACS(Assertion Consumer URL)/login URL with SAML response.
If a valid response is passed, you will be able to log in.

LOGIN INTO THE COMMUNITY USING AXIOM:

The same process, we just need to keep the below parameters in mind:
>> Issuer — Issuer value from IDP.
>> Entity ID — Should be different from org SSO setting (recommended community URL)
>> Recipient URL/Login URL — Login URL for the community in SSO.



For Communities

Community Name: NEWSFTAB

Login URL	https://abhi-community-developer-edition.ap5.force.com/NEWSFTAB/login?so=00D7F000000sUYs
Logout URL	https://abhi-community-developer-edition.ap5.force.com/NEWSFTAB/services/auth/sp/saml2/logout

Community Name: SF-TAB

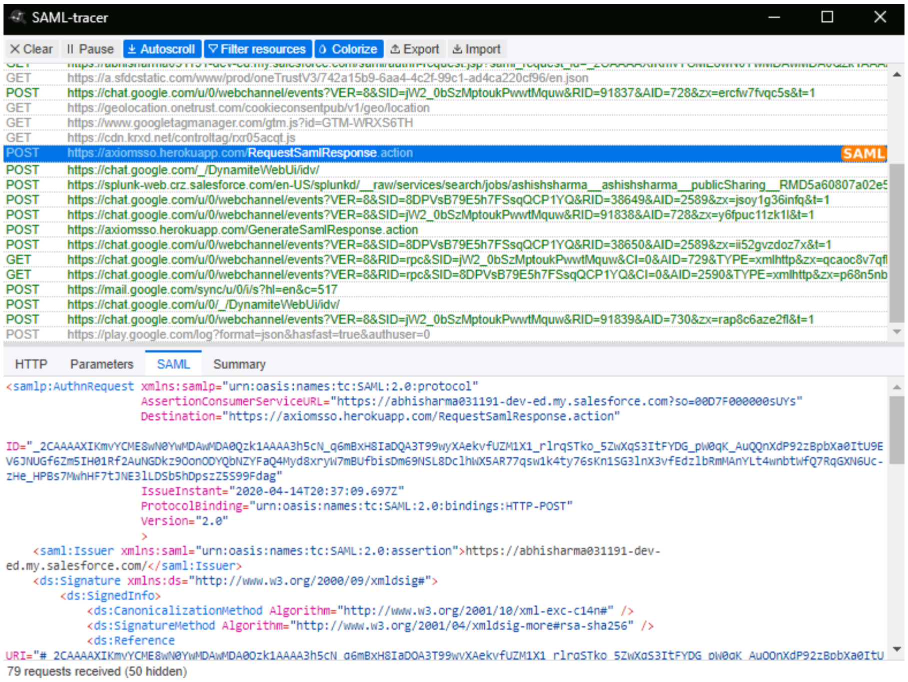
Login URL	https://abhi-community-developer-edition.ap5.force.com/SFTAB/login?so=00D7F000000sUYs
Logout URL	https://abhi-community-developer-edition.ap5.force.com/SFTAB/services/auth/sp/saml2/logout

CAPTURE SAML RESPONSE

TOOLS:

Google extensions:

- SAML Tracer
- SAML Message Decoder.



```
GET     https://a.sfdcstatic.com/www/prod/oneTrustV3/742a15b9-6aa4-4c2f-99c1-ad4ca220cf96/en.json
POST    https://chat.google.com/u/0/webchannel/events?VER=8&SID=jW2_0bSzMptoukPwwtMquw&RID=91837&AID=728&zx=ercfw7fvqc5s&t=1
GET     https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location
GET     https://www.googletagmanager.com/gtm.js?id=GTM-WRXS6TH
GET     https://cdn.krxd.net/controltag/rxr05acqt.js
POST    https://axiomsso.herokuapp.com/RequestSamlResponse.action                                                          SAML
POST    https://chat.google.com/_/DynamiteWebUi/idv/
POST    https://splunk-web.crz.salesforce.com/en-US/splunkd/__raw/services/search/jobs/ashishsharma__ashishsharma__publicSharing__RMD5a60807a02e5
POST    https://chat.google.com/u/0/webchannel/events?VER=8&SID=8DPVsB79E5h7FSsqQCP1YQ&RID=38649&AID=2589&zx=jsoy1g36infq&t=1
POST    https://chat.google.com/u/0/webchannel/events?VER=8&SID=jW2_0bSzMptoukPwwtMquw&RID=91838&AID=728&zx=y6fpuc11zk1l&t=1
POST    https://axiomsso.herokuapp.com/GenerateSamlResponse.action
POST    https://chat.google.com/u/0/webchannel/events?VER=8&SID=8DPVsB79E5h7FSsqQCP1YQ&RID=38650&AID=2589&zx=ii52gvzdoz7x&t=1
GET     https://chat.google.com/u/0/webchannel/events?VER=8&RID=rpc&SID=jW2_0bSzMptoukPwwtMquw&CI=0&AID=729&TYPE=xmlhttp&zx=qcaoc8v7qfl
GET     https://chat.google.com/u/0/webchannel/events?VER=8&RID=rpc&SID=8DPVsB79E5h7FSsqQCP1YQ&CI=0&AID=2590&TYPE=xmlhttp&zx=p68n5nb
POST    https://mail.google.com/sync/u/0/i/s?hl=en&c=517
POST    https://chat.google.com/u/0/_/DynamiteWebUi/idv/
POST    https://chat.google.com/u/0/webchannel/events?VER=8&SID=jW2_0bSzMptoukPwwtMquw&RID=91839&AID=730&zx=rap8c6aze2fl&t=1
POST    https://play.google.com/log?format=json&hasfast=true&authuser=0
```

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://abhisharma031191-dev-ed.my.salesforce.com?so=00D7F000000sUYs"
                    Destination="https://axiomsso.herokuapp.com/RequestSamlResponse.action"

ID="_2CAAAAXIKmvYCME8wN0YwMDAwMDA0Qzk1AAAA3h5cN_q6mBxH8IaDQA3T99wyXAekvfUZM1X1_rlrqSTko_5ZwXqS3ItFYDG_pW0qK_AuQQnXdP92zBpbXa0ItU9E
V6JNUGf6Zm5IH01Rf2AuNGDkz9OonODYQbNZYFaQ4Myd8xryW7mBUfbisDm69NSL8DclhWX5AR77qsw1k4ty76sKn1SG3lnX3vfEdzlbRmMAnYLt4wnbtWfQ7RqGXN6Uc-
zHe_HPBs7MwhHF7tJNE3lLDSb5hDpszZ5S99Fdag"
                    IssueInstant="2020-04-14T20:37:09.697Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://abhisharma031191-dev-
ed.my.salesforce.com/</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference
URI="#_2CAAAAXIKmvYCME8wN0YwMDAwMDA0Qzk1AAAA3h5cN_q6mBxH8IaDQA3T99wyXAekvfUZM1X1_rlrqSTko_5ZwXqS3ItFYDG_pW0qK_AuQQnXdP92zBpbXa0ItU
```

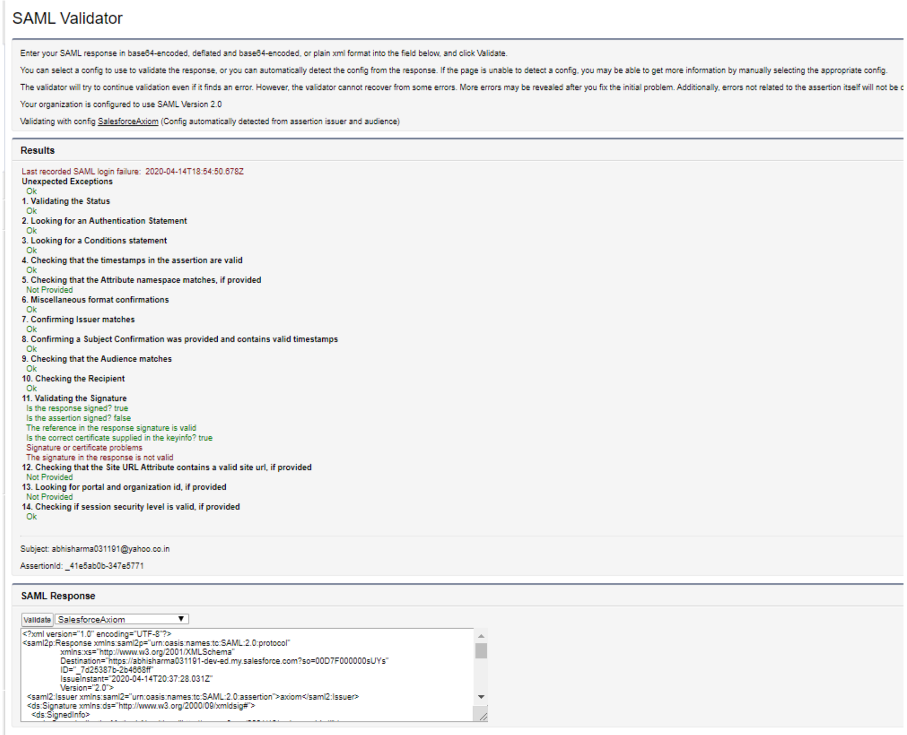
79 requests received (50 hidden)

VALIDATING SAML SETTINGS FOR SINGLE SIGN-ON:

If users have difficulty logging into Salesforce after you configure Salesforce for single sign-on, use the SAML Assertion Validator and the login history to validate the SAML assertions sent by your identity provider.

1. Obtain a SAML assertion from your identity provider. The assertion can be either in plain XML format or base64 encoded. If a user tries to log in to Salesforce and fails, the invalid SAML assertion is used to automatically populate the SAML Assertion Validator if possible.
2. From Setup, enter Single Sign-On Settings in the `Quick Find` box, then select **Single Sign-On Settings**, then click **SAML Assertion Validator**.
3. Enter the SAML assertion into the text box, and click **Validate**.
4. Share the results of the validation errors with your identity provider.

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_loginhistory.htm



SAML Validator

Enter your SAML response in base64-encoded, deflated and base64-encoded, or plain xml format into the field below, and click Validate.

You can select a config to use to validate the response, or you can automatically detect the config from the response. If the page is unable to detect a config, you may be able to get more information by manually selecting the appropriate config.

The validator will try to continue validation even if it finds an error. However, the validator cannot recover from some errors. More errors may be revealed after you fix the initial problem. Additionally, errors not related to the assertion itself will not be c

Your organization is configured to use SAML Version 2.0

Validating with config SalesforceAxiom (Config automatically detected from assertion issuer and audience)

Results

```
Last recorded SAML login failure:  2020-04-14T18:54:50.678Z
Unexpected Exceptions
  Ok
1. Validating the Status
  Ok
2. Looking for an Authentication Statement
  Ok
3. Looking for a Conditions statement
  Ok
4. Checking that the timestamps in the assertion are valid
  Ok
5. Checking that the Attribute namespace matches, if provided
  Not Provided
6. Miscellaneous format confirmations
  Ok
7. Confirming Issuer matches
  Ok
8. Confirming a Subject Confirmation was provided and contains valid timestamps
  Ok
9. Checking that the Audience matches
  Ok
10. Checking the Recipient
  Ok
11. Validating the Signature
  Is the response signed? true
  Is the assertion signed? false
  The reference in the response signature is valid
  Is the correct certificate supplied in the keyinfo? true
  Signature or certificate problems
  The signature in the response is not valid
12. Checking that the Site URL Attribute contains a valid site url, if provided
  Not Provided
13. Looking for portal and organization id, if provided
  Not Provided
14. Checking if session security level is valid, if provided
  Ok
```

Subject: abhisharma031191@yahoo.co.in

AssertionId: _41e5ab0b-347e5771

SAML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
          Destination="https://abhisharma031191-dev-ed.my.salesforce.com?so=00D7F000000sUYs"
          ID="_7d25387b-2b4668ff"
          IssueInstant="2020-04-14T20:37:28.031Z"
          Version="2.0">
 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">axiom</saml2:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
```

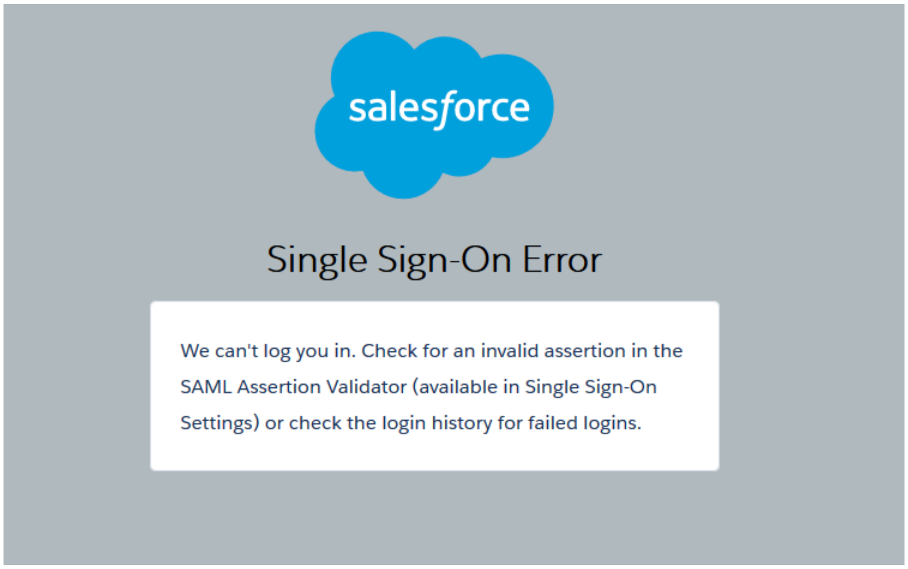
SAML ASSERTION VALIDATION ERRORS

https://developer.salesforce.com/docs/atlas.en-us.sso.meta/sso/sso_saml_validation_errors.htm

MOST COMMON ERRORS:

1. **Generic Single Single Sign on Error:**

This error comes up whenever the parameter values passed in SAML response doesn’t match with the values present Salesforce Single Sign On settings.



Single Sign-On Error

We can't log you in. Check for an invalid assertion in the SAML Assertion Validator (available in Single Sign-On Settings) or check the login history for failed logins.

How to Troubleshoot:

1. Capture SAML response (either directly going to SAML Validator from BT or System Admin access and find the Invalid response). If it is not captured, you need to replicate the issue with user and capture the SAML response using above mentioned tools.
2. Then SAML response needs to be validated in SAML validator and you should be able to find the root cause.

2. **GACK ERROR IN SP INITIATED FLOW AFTER HITTING MY DOMAIN**

Sandboxes created as a mirror of their production environment will have their SAML settings disabled after a sandbox refresh, due to the recipient URL being updated.

Recipient URL is updated to match your sandbox URL that Salesforce gives when the sandbox is refreshed, for example http://cs1.salesforce.com. Other than Recipient URL, all SSO config options, including certificates, will be mirrored in the sandbox SSO configs.

We need to keep in mind

- If you have SSO enabled in the Production environment with a custom profile with the SSO permission enabled, when the Sandbox refresh occurs, login will be blocked. You'll need to check the permissions. This won't apply to a user with a standard profile. (This is due to a sandbox refresh limitation)
- The org ID of the sandbox environment is changed every time you refresh the sandbox and will negate SSO settings, requiring that they be reconfigured.
- Once the Recipient URL is updated , download the metadata and provide it to the IDP (Identity Provider) and have it updated at IDP end.
- After Sandbox refresh, one of the system admin user of the Org may need to reach out to Salesforce support for a password reset email to bypass the security question prompt so that they can set up their password to access the Sandbox.

https://help.salesforce.com/articleView?id=000329819&language=en_US&type=1&mode=1

Referenced case

https://org62.lightning.force.com/lightning/r/Case/5000M00000h6LwdQAE/view

Other Referenced articles:
https://help.salesforce.com/articleView?id=sso_saml_setting_up.htm&type=5

Confluence:
https://confluence.internal.salesforce.com/pages/viewpage.action?pageId=49527871#tab-Beginner