# Single Sign On (Session 2)

***Initially created by Ashish Sharma***
(Please go thru the Single Sign On (Session 1) Doc and Recording for complete understanding)

**TOPICS COVERED:**

- Salesforce as Identity provider.
- How to enable IDP in Salesforce
- Create connected app
- Create Single Sign on Setting in other dev org
- Login using Single sign on using sp initiated and IDP initiated flows.
- Use of Federation Id
- How to check certificate from SAML response.
- Delegated SSO - Overview
- How to setup Delegated SSO - permissions required.
- Login using Axiom (Delegated) after setting up in Salesforce.
- Check delegated history for errors.
- Delegated Authentication Error History
- Common Scenarios

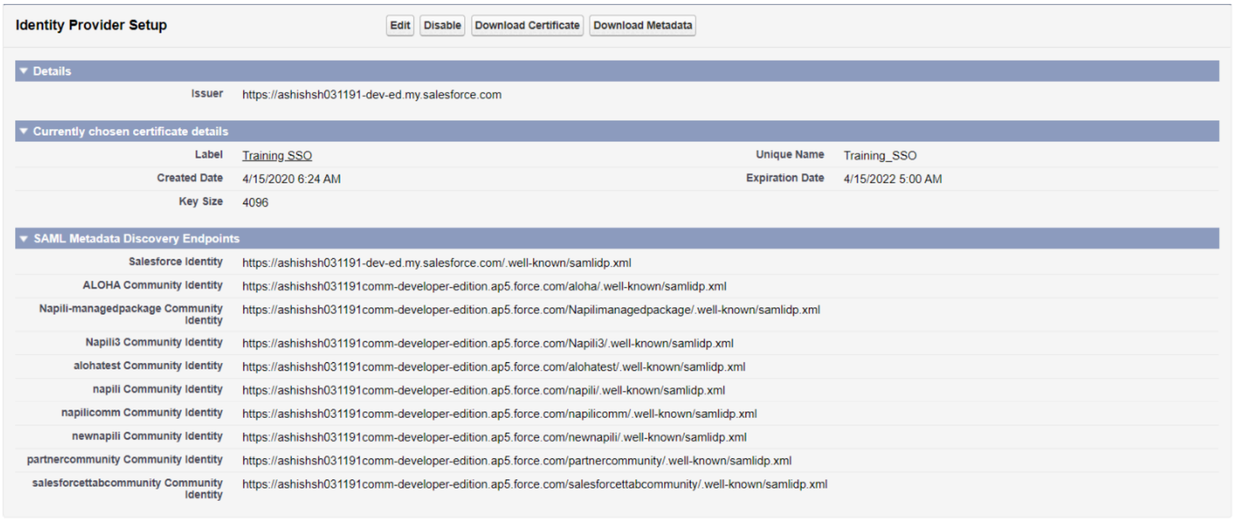
**SALESFORCE AS AN IDENTITY PROVIDER**

**Salesforce** can act as a single sign-on (SSO) **identity provider** to service **providers**, allowing end users to easily and securely access many web and mobile applications with one login. When using **SAML** for federated authentication, enable **Salesforce** as an **identity provider** and then set up connected apps.

**HOW TO ENABLE IDP IN SALESFORCE**

Configure a domain using My Domain and deploy it to all users. For instructions, see Set Up a My Domain Name.
From Setup, enter Identity Provider in the Quick Find box, select **Identity Provider**, and click **Enable Identity Provider**.
By default, a Salesforce identity provider uses a self-signed certificate generated with the SHA-256 signature algorithm. If you've already created self-signed certificates, select the certificate to use when securely communicating with other services.
If you want to use a CA-signed certificate instead of self-signed certificate, follow these steps.
After you enable Salesforce as an identity provider, you can create connected apps to provide access to service providers.
https://help.salesforce.com/articleView?id=identity_provider_enable.htm&type=5

***IMAGE of Salesforce IDP setting after following the above steps***



**Identity Provider Setup**

▼ Details

| | |
|---|---|
| Issuer | https://ashishsh031191-dev-ed.my.salesforce.com |

▼ Currently chosen certificate details

| | | | |
|---|---|---|---|
| Label | Training SSO | Unique Name | Training_SSO |
| Created Date | 4/15/2020 6:24 AM | Expiration Date | 4/15/2022 5:00 AM |
| Key Size | 4096 | | |

▼ SAML Metadata Discovery Endpoints

| | |
|---|---|
| Salesforce Identity | https://ashishsh031191-dev-ed.my.salesforce.com/.well-known/samlidp.xml |
| ALOHA Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/aloha/.well-known/samlidp.xml |
| Napili-managedpackage Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/Napilimanagedpackage/.well-known/samlidp.xml |
| Napili3 Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/Napili3/.well-known/samlidp.xml |
| alohatest Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/alohatest/.well-known/samlidp.xml |
| napili Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/napili/.well-known/samlidp.xml |
| napilicomm Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/napilicomm/.well-known/samlidp.xml |
| newnapili Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/newnapili/.well-known/samlidp.xml |
| partnercommunity Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/partnercommunity/.well-known/samlidp.xml |
| salesforcettabcommunity Community Identity | https://ashishsh031191comm-developer-edition.ap5.force.com/salesforcettabcommunity/.well-known/samlidp.xml |

After Enabling, you need to provide metadata file to the Service provider that you can download and give to your service provider. To obtain this metadata, from Setup, enter Identity Provider in the Quick Find box, select **Identity Provider**, then click **Download Metadata**. Then get the following information from your service provider:

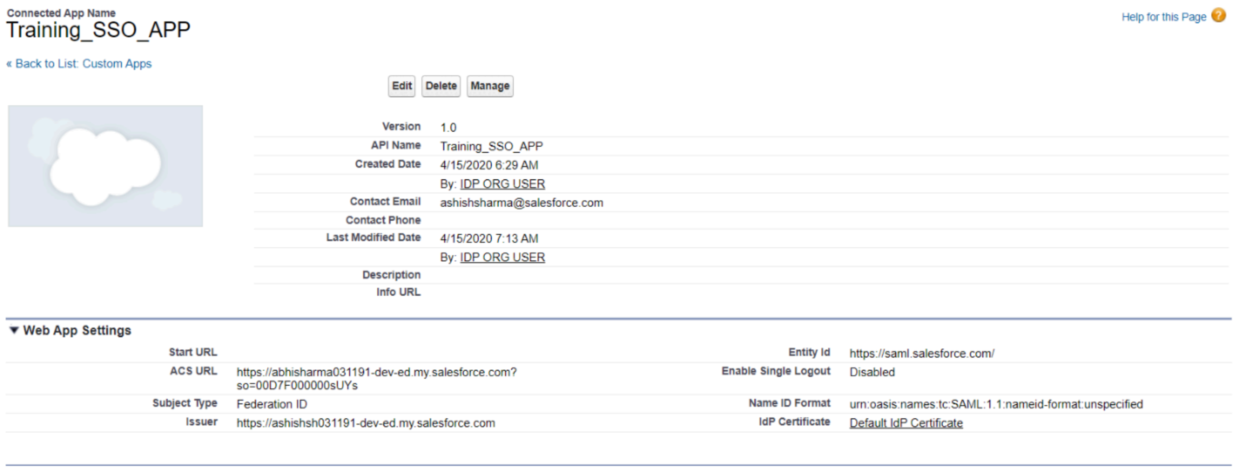
- Assertion consumer service (ACS) URL
- Entity ID
- Subject type—Specifies if the subject for the SAML response from Salesforce (as an identity provider) is a Salesforce user name or a federation ID

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

### CREATE CONNECTED APP

From Setup, enter Apps in the Quick Find box, then select **Apps**.
Under Connected Apps, click **New**.
Specify the required fields under Basic Information.
Follow below article:
https://help.salesforce.com/articleView?id=service_provider_define.htm&type=5

***Connected APP ScreenShot after following the above steps. Image 1***



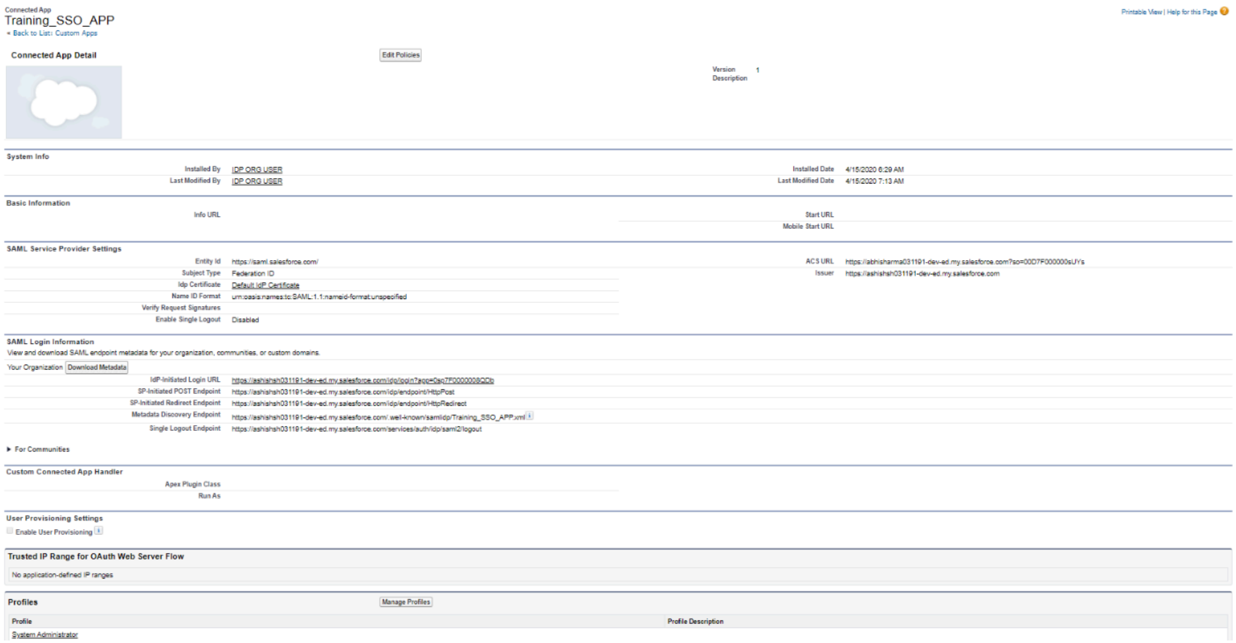
Connected App Name
Training_SSO_APP

| | |
|---|---|
| Version | 1.0 |
| API Name | Training_SSO_APP |
| Created Date | 4/15/2020 6:29 AM |
| | By: IDP ORG USER |
| Contact Email | ashishsharma@salesforce.com |
| Contact Phone | |
| Last Modified Date | 4/15/2020 7:13 AM |
| | By: IDP ORG USER |
| Description | |
| Info URL | |

▼ Web App Settings

| | | | |
|---|---|---|---|
| Start URL | | Entity Id | https://saml.salesforce.com/ |
| ACS URL | https://abhisharma031191-dev-ed.my.salesforce.com?so=00D7F000000sUYs | Enable Single Logout | Disabled |
| Subject Type | Federation ID | Name ID Format | urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified |
| Issuer | https://ashishsh031191-dev-ed.my.salesforce.com | IdP Certificate | Default IdP Certificate |

**Image 2 (after clicking on Manage *button)***



Connected App
Training_SSO_APP
« Back to List: Custom Apps

**Connected App Detail**

| | |
|---|---|
| Version | 1 |
| Description | |

**System Info**

| | | | |
|---|---|---|---|
| Installed By | IDP ORG USER | Installed Date | 4/15/2020 6:29 AM |
| Last Modified By | IDP ORG USER | Last Modified Date | 4/15/2020 7:13 AM |

**Basic Information**

| | | | |
|---|---|---|---|
| Info URL | | Start URL | |
| | | Mobile Start URL | |

**SAML Service Provider Settings**

| | | | |
|---|---|---|---|
| Entity Id | https://saml.salesforce.com/ | ACS URL | https://abhisharma031191-dev-ed.my.salesforce.com?so=00D7F000000sUYs |
| Subject Type | Federation ID | Issuer | https://ashishsh031191-dev-ed.my.salesforce.com |
| Idp Certificate | Default IdP Certificate | | |
| Name ID Format | urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified | | |
| Verify Request Signatures | | | |
| Enable Single Logout | Disabled | | |

**SAML Login Information**

View and download SAML endpoint metadata for your organization, communities, or custom domains.

Your Organization

| | |
|---|---|
| IdP-Initiated Login URL | https://ashishsh031191-dev-ed.my.salesforce.com/idp/login?app=0sp7F0000008QDb |
| SP-Initiated POST Endpoint | https://ashishsh031191-dev-ed.my.salesforce.com/idp/endpoint/HttpPost |
| SP-Initiated Redirect Endpoint | https://ashishsh031191-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect |
| Metadata Discovery Endpoint | https://ashishsh031191-dev-ed.my.salesforce.com/.well-known/samlidp/Training_SSO_APP.xml |
| Single Logout Endpoint | https://ashishsh031191-dev-ed.my.salesforce.com/services/auth/idp/saml2/logout |

▸ For Communities

**Custom Connected App Handler**

| | |
|---|---|
| Apex Plugin Class | |
| Run As | |

**User Provisioning Settings**

□ Enable User Provisioning

**Trusted IP Range for OAuth Web Server Flow**

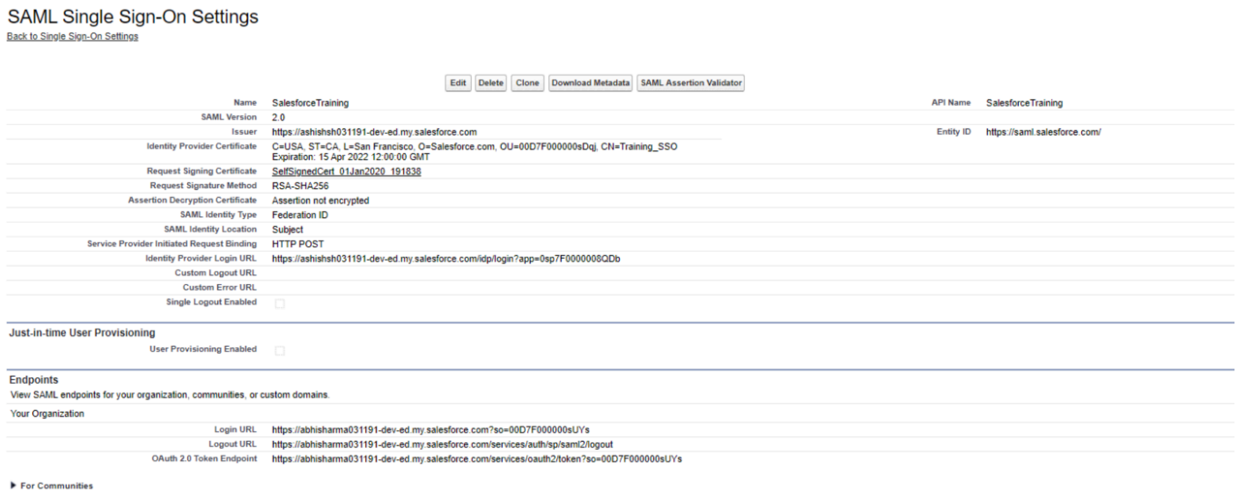
No application-defined IP ranges

**Profiles**

| Profile | Profile Description |
|---|---|
| System Administrator | |

## CREATE SINGLE SIGN ON SETTING IN OTHER DEV ORG

After Enabling The Identity provider in IDP org, you need to create Single Sign ON Setting in Other org:



SAML Single Sign-On Settings
Back to Single Sign-On Settings

| | | | |
|---|---|---|---|
| Name | SalesforceTraining | API Name | SalesforceTraining |
| SAML Version | 2.0 | | |
| Issuer | https://ashishsh031191-dev-ed.my.salesforce.com | Entity ID | https://saml.salesforce.com/ |
| Identity Provider Certificate | C=USA, ST=CA, L=San Francisco, O=Salesforce.com, OU=00D7F000000sDqj, CN=Training_SSO<br>Expiration: 15 Apr 2022 12:00:00 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://ashishsh031191-dev-ed.my.salesforce.com/idp/login?app=0sp7F0000008QDb | | |
| Custom Logout URL | | | |
| 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 |

▸ For Communities

## LOGIN USING SINGLE SIGN ON USING SP INITIATED AND IDP INITIATED FLOWS.

***>> USING IDP initiated flow:***

Click on the IDP initiated Provider Login URL:
https://ashishsh031191-dev-ed.my.salesforce.com/idp/login?app=0sp7F0000008QDb
SAML response will be sent to Service Provider if it is a valid one, we will be to login in SP org.

***>> USING SP initiated flow:***

Go to mydomain:
https://abhisharma031191-dev-ed.my.salesforce.com/
Click on SSO button, SAML request will be sent to IDP (information like issuer), we will login in IDP.
Then IDP org will send the SAML assertion, if it is valid, we will be able to login.

**USE OF FEDERATION ID:**

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

If the Subject Type for the service provider definition is Federation ID, you must map the Salesforce user to the username used to sign into the service provider.
To map a Salesforce user to the app user:

1. From Setup, enter Users in the Quick Find box, then select **Users**, then click **Edit** for every user who needs to be mapped.
2. In Federation ID, under Single Sign On Information, enter the username to be used to log into the service provider.
3. Click **Save**.

**HOW TO CHECK CERTIFICATE FROM SAML RESPONSE.**

Capture the SAML response and search for the Certificate tag. Copy its encoded value and save to different file with .crt extension. Once saved, you will be able to see the certificate. This certificate can be matched with the existing certificate in SSO settings and if it is incorrect, you need to make the change in salesforce or IDP end.

**DELEGATED SSO - OVERVIEW**

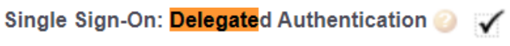
You can integrate Salesforce with the authentication method of your choice using delegated authentication single sign-on (SSO). You can integrate with your LDAP (Lightweight Directory Access Protocol) server or authenticate with a token instead of a password. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some users to use delegated authentication and others to use their Salesforce-managed password.

When a user tries to log in—either online or using the API—Salesforce validates the username and checks the user's permissions and access settings.
If the user has the Is Single Sign-On Enabled user permission, Salesforce doesn't validate the username and password. Instead, a web service call is made to the user's org to validate the username and password. When this user permission is enabled, Salesforce no longer manages the policies for user passwords, such as when passwords expire or the required minimum length. Instead, the delegated authentication endpoint's service enforces password policies.

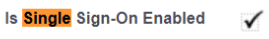
**HOW TO SETUP DELEGATED SSO**

**HTTPS://HELP.SALESFORCE.COM/ARTICLEVIEW?ID=SSO_DELAUTHENTICATION_CONFIGURING.HTM&TYPE=5**

***BT permissions required.***


Single Sign-On: Delegated Authentication ✓

***Profile level Permission***


Is Single Sign-On Enabled ✓

*We can provide a permission set having this system setting to a particular user as well.

**LOGIN USING AXIOM (DELEGATED) AFTER SETTING UP IN SALESFORCE.**

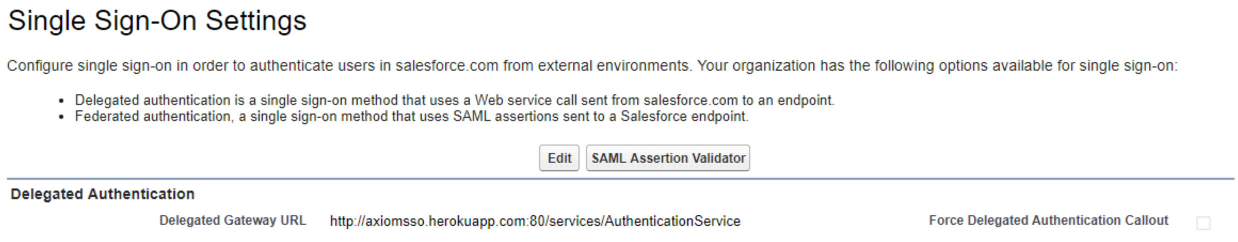
http://axiomsso.herokuapp.com/GenerateToken.action

***Configure***

Ensure Salesforce is configured for Delegated Authentication Single Sign-On with this service:

- Delegated Authentication Single Sign-On must be activated for the organization.
- Enable the *Is Single Sign-On Enabled* profile permission for the users who should be re-directed to this service.
- Go to *Setup | Security Controls | Single Sign-On Settings | Delegated authentication* and set the *Delegated Gateway URL* to the following

-
```
http://axiomsso.herokuapp.com:80/services/AuthenticationService
```



## Single Sign-On Settings

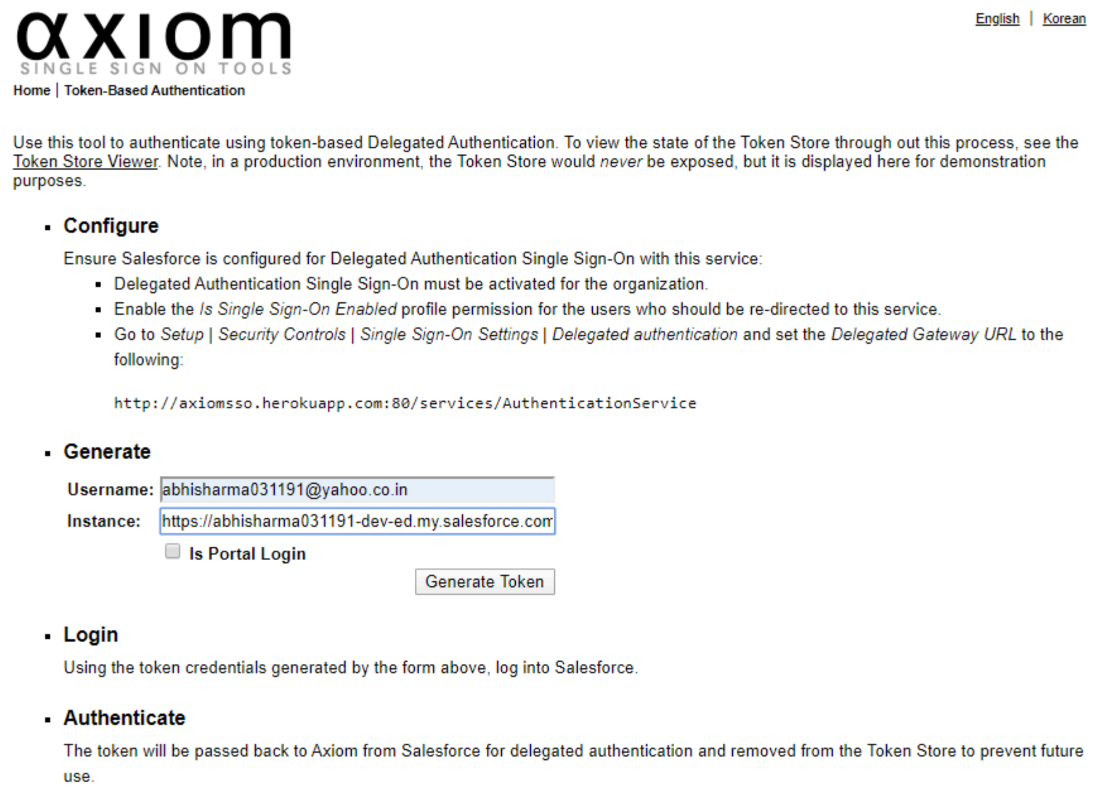
Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

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

**Delegated Authentication**

Delegated Gateway URL http://axiomsso.herokuapp.com:80/services/AuthenticationService

Force Delegated Authentication Callout □



**Home | Token-Based Authentication**

Use this tool to authenticate using token-based Delegated Authentication. To view the state of the Token Store through out this process, see the Token Store Viewer. Note, in a production environment, the Token Store would *never* be exposed, but it is displayed here for demonstration purposes.

- **Configure**

  Ensure Salesforce is configured for Delegated Authentication Single Sign-On with this service:
  - Delegated Authentication Single Sign-On must be activated for the organization.
  - Enable the *Is Single Sign-On Enabled* profile permission for the users who should be re-directed to this service.
  - Go to *Setup* | *Security Controls* | *Single Sign-On Settings* | *Delegated authentication* and set the *Delegated Gateway URL* to the following:

  ```
  http://axiomsso.herokuapp.com:80/services/AuthenticationService
  ```

- **Generate**

  **Username:** abhisharma031191@yahoo.co.in

  **Instance:** https://abhisharma031191-dev-ed.my.salesforce.com

  □ **Is Portal Login**

- **Login**

  Using the token credentials generated by the form above, log into Salesforce.

- **Authenticate**

  The token will be passed back to Axiom from Salesforce for delegated authentication and removed from the Token Store to prevent future use.

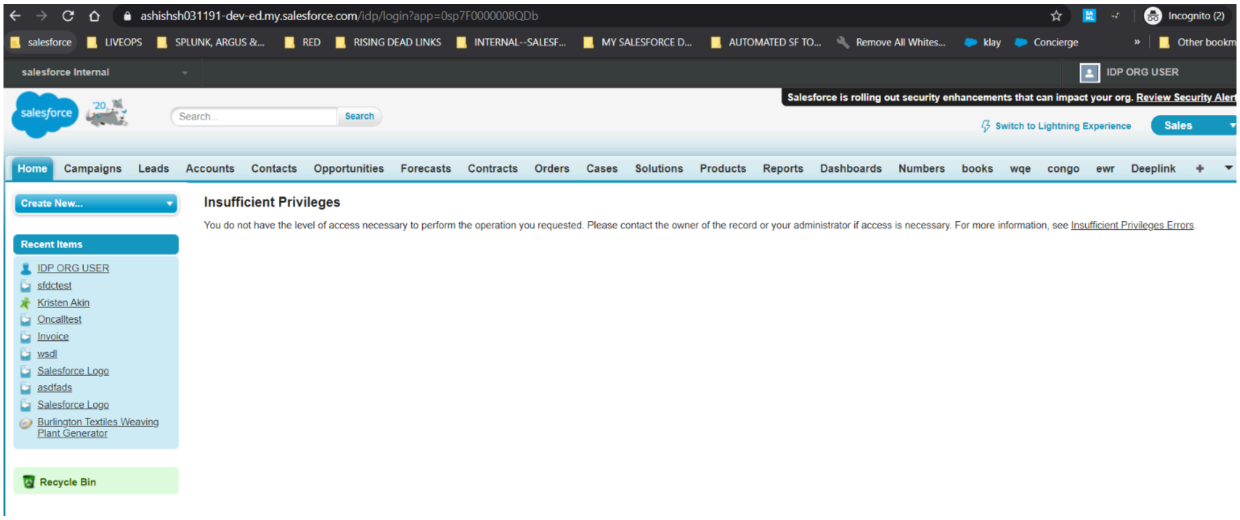
**DELEGATED AUTHENTICATION ERROR HISTORY**

From Setup, enter Delegated Authentication Error History in the Quick Find box, then select **Delegated Authentication Error**

**History**.
For the twenty-one most recent login errors, you can view the user's username, login time, and the error.

**COMMON SCENARIOS:**

***>> INSUFFICIENT PRIVILEGES ERROR AFTER LOGGING INTO IDP ORG.***



Insufficient Privileges

You do not have the level of access necessary to perform the operation you requested. Please contact the owner of the record or your administrator if access is necessary. For more information, see Insufficient Privileges Errors

***Resolution***:

Add Profile in the connected app created in IDP org(manage option).

***>> USE SAML AND DELEGATED AUTHENTICATION SIMULTANEOUSLY***

Yes, Delegated Authentication (DA) and Federated authentication can be enabled in an Org at the same time. You would have to make sure that the Salesforce 'Login Page' is also selected as a Login method under My Domain, in addition to SAML. If it is not selected, the request would be redirected to the IdP automatically. Since 'Is Single Sign-On Enabled' is a Profile Permission, Salesforce would validate their identity with the DA provider, where this is set on the Users Profile. Also, setting up DA with an invalid URL is the recommended way to prevent Password Resets even for SAML Based Auth, so they can certainly work together.

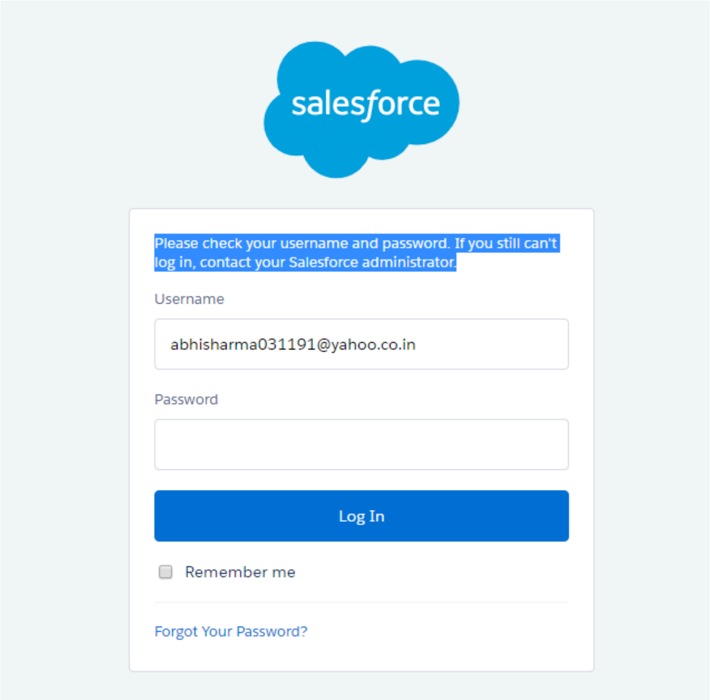
https://help.salesforce.com/articleView?id=000329322&language=en_US&type=1&mode=1

**User Specific Settings**
For Users needing to use DA: 'Is Single Sign-On Enabled' = true assigned via permission set or set on profile
For Users needing to use Federated: 'Is Single Sign-On Enabled' = false (i.e. DA not applied)
For Users needing to manually log-in via standard SF login page (i.e. Admins) : 'Is Single Sign-On Enabled' = false (i.e. DA not applied)

**General Settings**
Leave DA setup as-is in Org
Enable Federated SSO (perform the necessary sub-steps to enable SSO)
Enable MyDomain in SF
Ensure available authentication methods selected includes both the Federated SSO service AND Login Page (these are what are

available to select on the SF login page) Domain Management | MyDomain
Ensure 'Prevent login from https://login.salesforce.com' setting is not checked

***>> ERROR 1:***



Please check your username and password. If you still can't log in, contact your Salesforce administrator.

Username

abhisharma031191@yahoo.co.in

Password

*>> IS single Sign on permission is checked on user and they are trying to login using salesforce username password*

>> Customer needs to use network password since delegated permission is checked
and Delegated Gateway URL is not empty in SSO setting.

>> Else they need to use Federated SSO if the option is provided on login page.

***>> ERROR 2:***

*In this scenario, Delegated permission is checked for the user but delegated gateway url is not provided.*

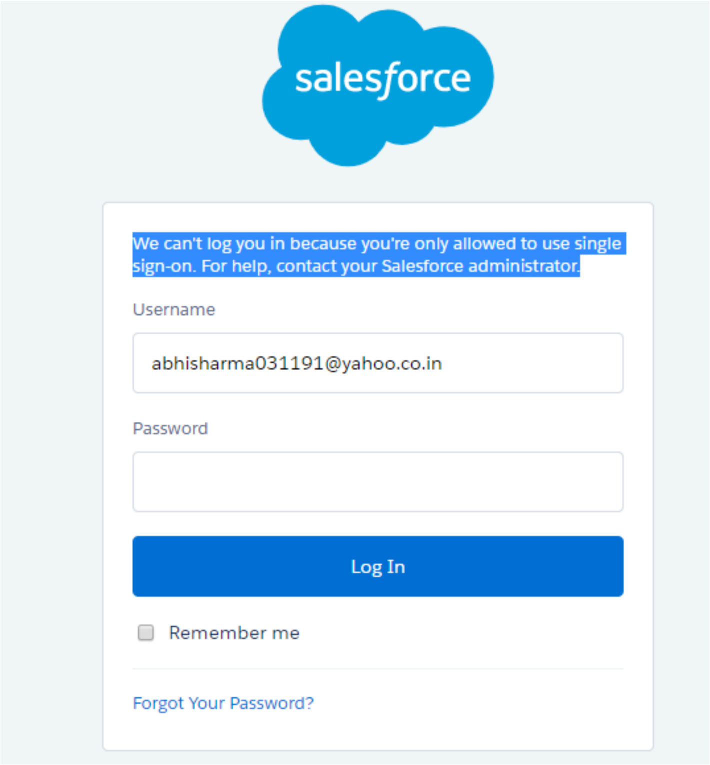
Customer can’t login using Salesforce Username and password.

If they claim, that they are using the network password, still not able to login.

Go to BT and check the Delegated Authentication Error History, you should see below type of logs:

**Username-------- Login Time------- ------------Error**

**abhisharma031191@yahoo.co.in**



We can't log you in because you're only allowed to use single sign-on. For help, contact your Salesforce administrator.

Username: abhisharma031191@yahoo.co.in

Password:

**-------4/15/2020 8:58:09 AM PDT------------**

**java.net.MalformedURLException**

This means, their delegated URL is not correctly setup, in SSO settings and they need to update it.

Based on the other options (federated SSO) is not present in org, we need to act i.e. disable Delegated authentication so that they can login.

Check the scenario in dev org with axiom before requesting org wide disablement.