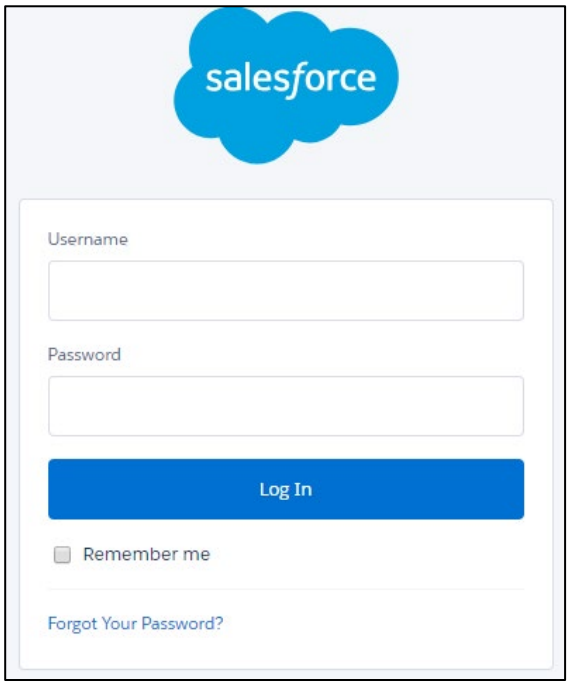
Configuring Remedyforce

Configuring Remedyforce for SSO enables administrators to manage their users using Citrix Gateway. Users can securely log on to Remedyforce using their enterprise credentials.

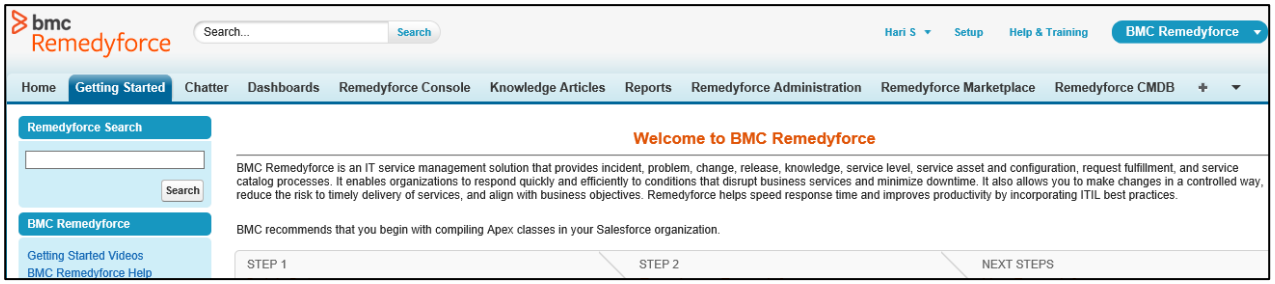
To configure Remedyforce for SSO through SAML, follow the steps below:

1. In a browser, type the URL, https://login.salesforce.com/ and press **Enter.**

2. Type the credentials, and click **Log In**.

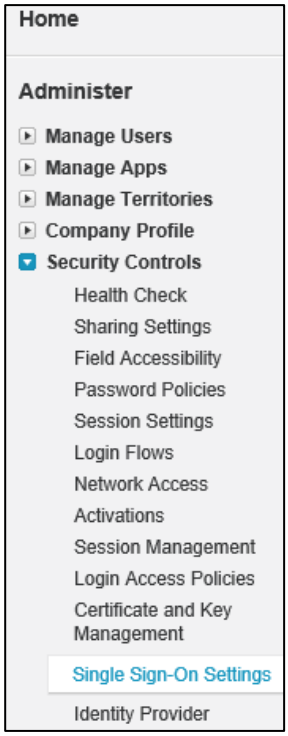


The Getting Started page appears.



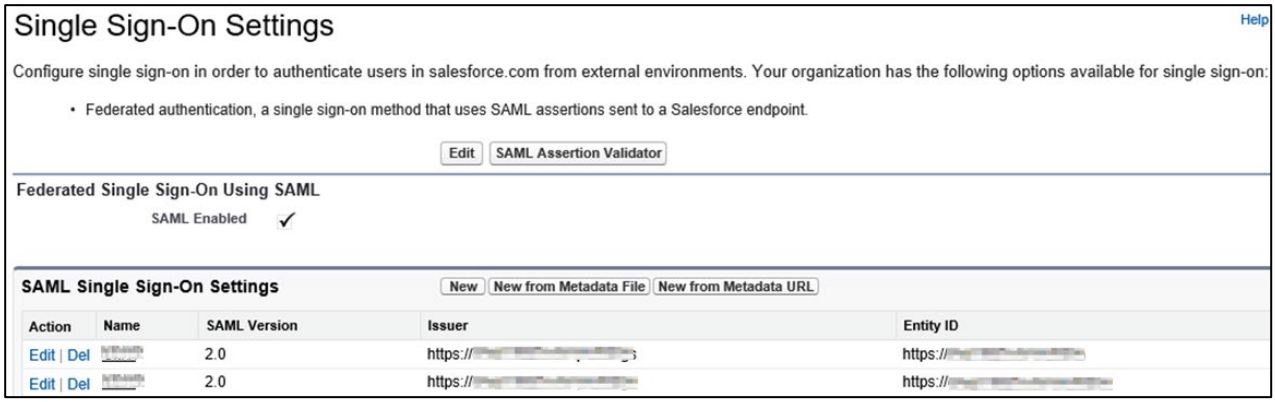
3. On the Getting Started page, click **Setup**.

4. In the left pane, click **Administer > Security Controls > Single Sign-On Settings**.



The Single Sign-On page appears.

5. On the Single Sign-On page, select **SAML Enabled** checkbox to view the SAML single sign-on settings.



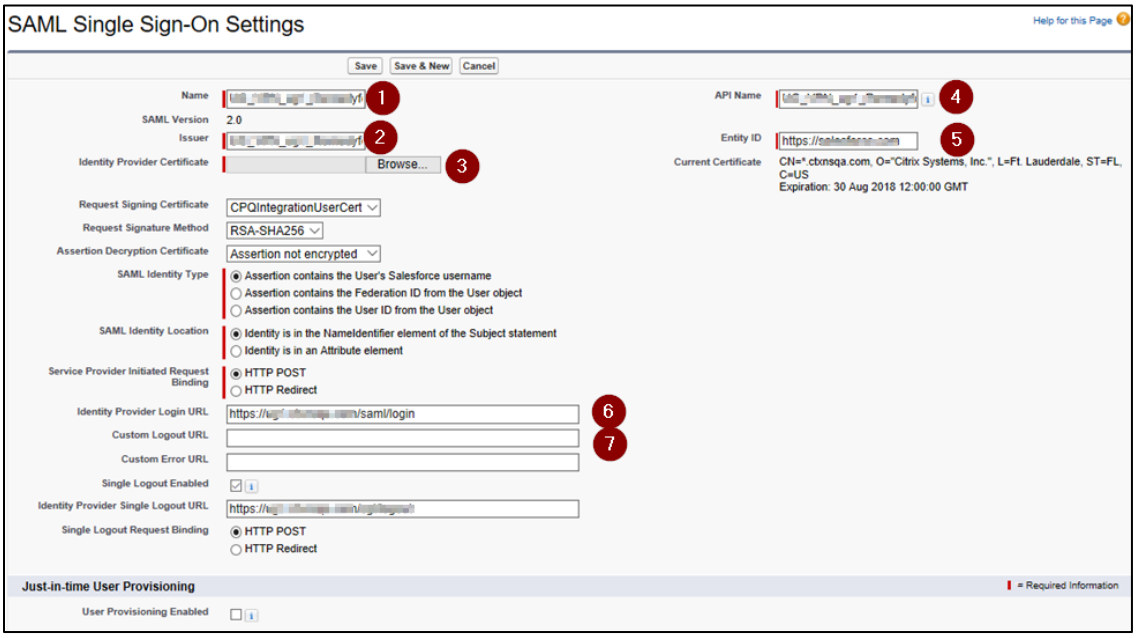
6. In SAML Single Sign-On Settings, click the appropriate button to create a configuration, as follows.
   i. **New** - Specify all settings manually.
   ii. **New from Metadata File** - Import SAML 2.0 settings from an XML file from your identity provider. This option reads the XML file and uses it to complete as many of the settings as possible.

Note: If your XML file contains information for more than one configuration, the first configuration that occurs in the XML file is used.

iii. **New from Metadata URL** - Import SAML 2.0 settings from a public URL. This option reads the XML file at a public URL and uses it to complete as many of the settings as possible. The URL must be added to Remote Site Settings to access it from your Salesforce org.

The SAML Single Sign-On page appears.

7. On the SAML Single Sign-On page, type the following information:



i. **Name:** Type a name for the SSO settings.

ii. **Issuer:** type a unique issuer ID. For example: https://example.com/saml/metadata/546600

iii. **Identity Provider Certificate:** click **Browse**, and navigate to the folder where you saved the Identity provider certificate in.pem format. Add the IdP certificate.

Note: To upload your IdP certificate, follow the steps below:

a. Remotely access your NetScaler instance using PuTTY.
b. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press **Enter**.
c. Type cat <certificate-name> and press **Enter**.

d. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

iv. **API Name**: Type unique API name.

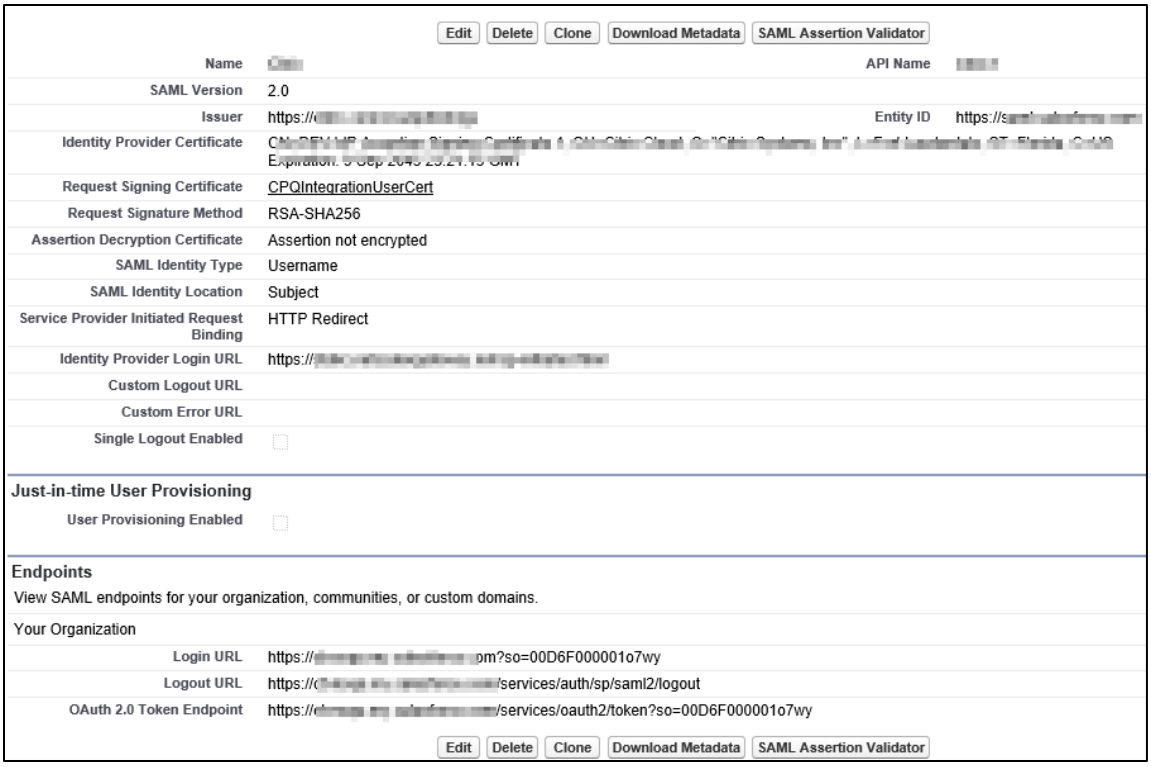
v. **Entity ID**: Type the domain name.

vi. **Identity Provider Login URL**: Enter the IdP URL, SAML 2.0 endpoint, for example, https://example.com/saml/login

vii. **Custom Logout URL**: Enter the IdP Log off URL, for example, https://example.com/cgi/tmlogout

8. Click **Save**.

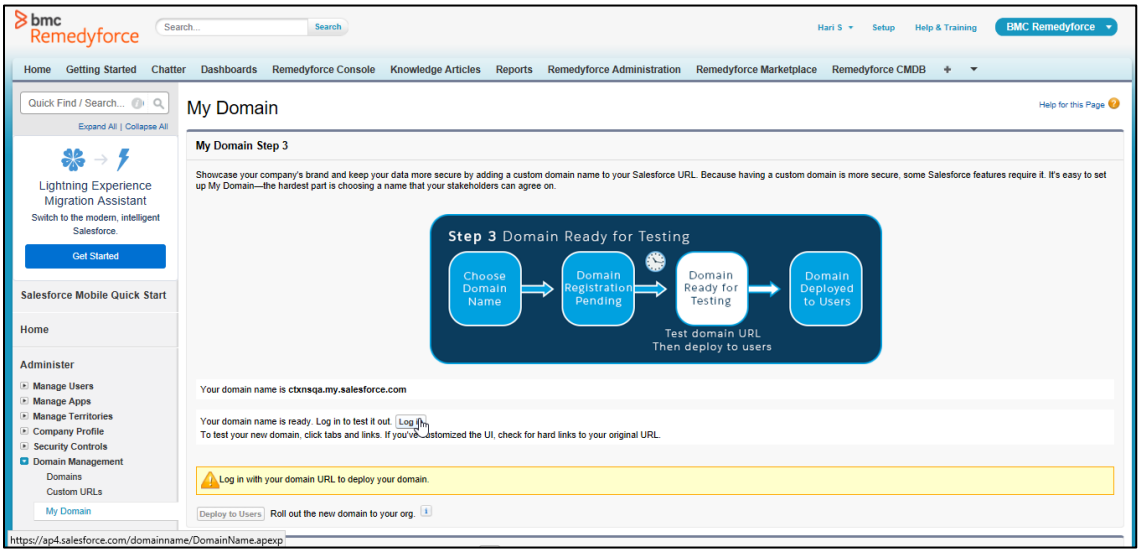
   The configuration is saved and the details are displayed.



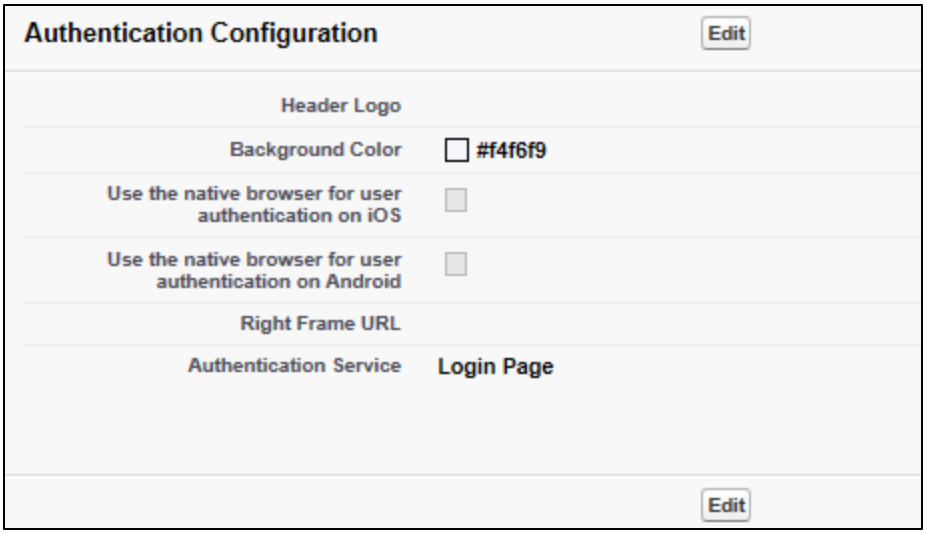
SP Initiated Flow Configuration

For SP initiated flow, perform the following steps to complete the configuration:

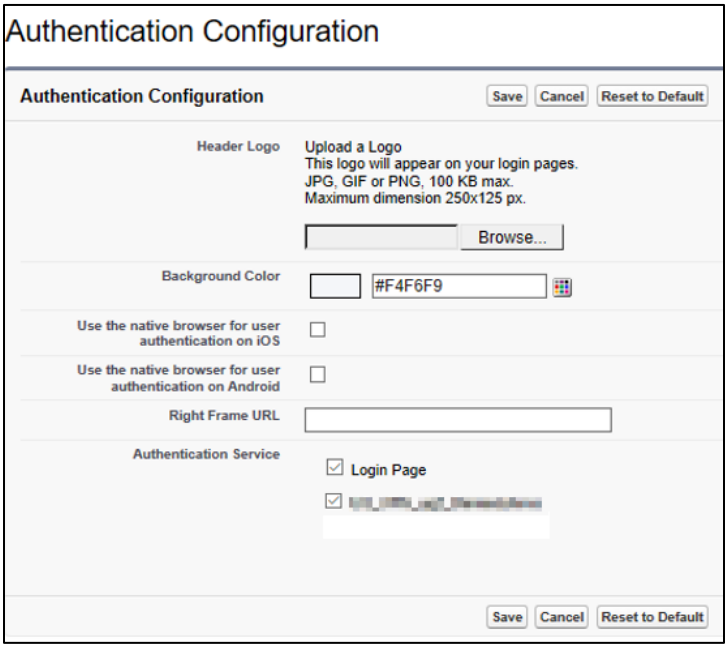
1. In the left pane, click **Administer > Domain Management > My Domain.**



2. On the My Domain page, under the Authentication Configuration section, click **Edit**.

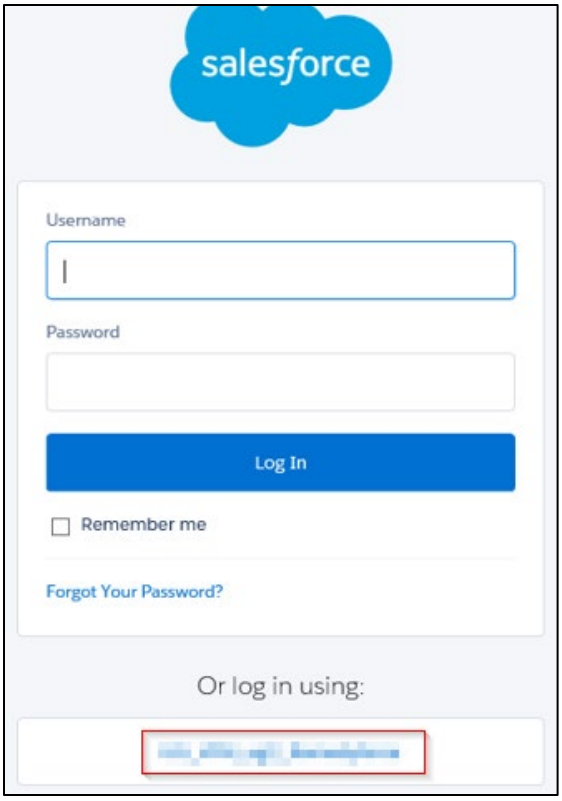


3. In the Authentication Service field, select the check box against your **Name** which you have specified in the SSO settings page.



4. Click **Save**. You are redirected to the Login page OR you can click **Log In**, on the My Domain page.

5. Type your credentials, and click on your **IDP name** to log in.



The SP initiated configuration is completed.