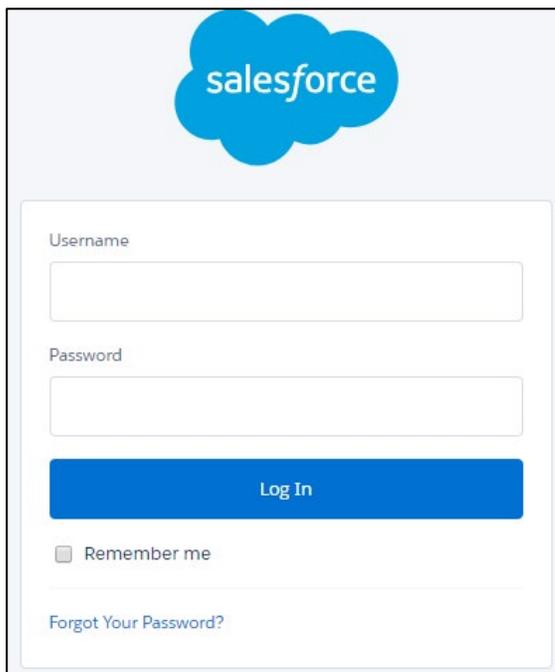


Configuring Remedyforce

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**.

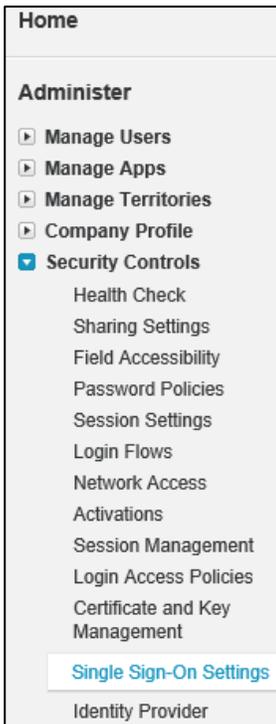
A screenshot of the Salesforce login page. At the top is the Salesforce logo, a blue cloud with the word "salesforce" in white. Below the logo is a white login form with a light blue border. The form contains a "Username" label above a text input field, a "Password" label above another text input field, a blue "Log In" button, a "Remember me" checkbox, and a "Forgot Your Password?" link.

The Getting Started page appears.

A screenshot of the BMC Remedyforce "Getting Started" page. The page has a light blue header with the BMC Remedyforce logo, a search bar, and navigation links for "Hari S", "Setup", "Help & Training", and "BMC Remedyforce". Below the header is a navigation menu with "Home", "Getting Started" (highlighted), "Chatter", "Dashboards", "Remedyforce Console", "Knowledge Articles", "Reports", "Remedyforce Administration", "Remedyforce Marketplace", and "Remedyforce CMDB". The main content area features a "Remedyforce Search" box, a "Welcome to BMC Remedyforce" heading, a paragraph of introductory text, and a "BMC Remedyforce" section with a recommendation to compile Apex classes. At the bottom, there is a progress bar with "STEP 1", "STEP 2", and "NEXT STEPS".

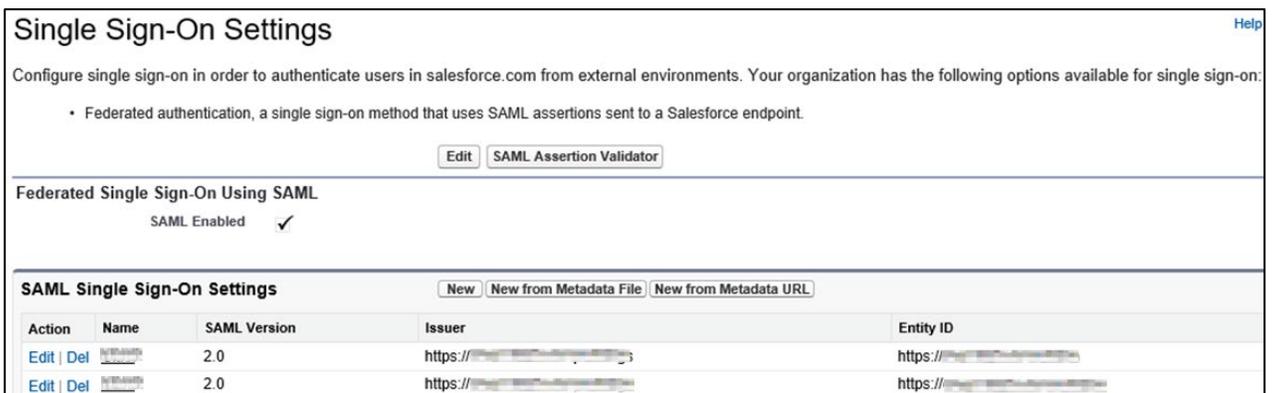
3. On the Getting Started page, click **Setup**.

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.
- New** - Specify all settings manually.
 - 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:

The screenshot shows the 'SAML Single Sign-On Settings' page. It includes a header with 'Save', 'Save & New', and 'Cancel' buttons. The main form area contains several sections: 'Name' (1), 'SAML Version' (2.0), 'Issuer' (2), 'Identity Provider Certificate' (3), 'Request Signing Certificate' (CPQIntegrationUserCert), 'Request Signature Method' (RSA-SHA256), 'Assertion Decryption Certificate' (Assertion not encrypted), 'SAML Identity Type' (radio buttons for Salesforce username, Federation ID, or User ID), 'SAML Identity Location' (radio buttons for NameIdentifier or Attribute), 'Service Provider Initiated Request Binding' (radio buttons for HTTP POST or HTTP Redirect), 'Identity Provider Login URL' (6), 'Custom Logout URL' (7), 'Custom Error URL', 'Single Logout Enabled' (checkbox), 'Identity Provider Single Logout URL', and 'Single Logout Request Binding' (radio buttons for HTTP POST or HTTP Redirect). On the right side, there are fields for 'API Name' (4), 'Entity ID' (5), and 'Current Certificate' (CN=*, ctmnsqa.com, O=Citrix Systems, Inc., L=Fl. Lauderdale, ST=FL, C=US, Expiration: 30 Aug 2018 12:00:00 GMT). At the bottom, there is a 'Just-in-time User Provisioning' section with a 'User Provisioning Enabled' checkbox. A legend at the bottom right indicates that a red 'i' icon means 'Required 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**.

```
1 -----BEGIN CERTIFICATE-----
2 MIIFPzCCBCegAwIBAgIQApjY189Tw/6/mHRS5nGDuzAMBgqhkiG9w0BAQsFADBN
3 NQs=
4 allc
5 HTe
6 BAe
7 LJE
8 ADC
9 yVj
10 Kjf
11 vde
12 RK2
13 RYC
14 MBa
15 +Cc
16 Y2V
17 BBy
18 LyS
19 Ois
20 MDC
21 dCE
22 GGF
23 Y2V
24 dDA
25 PA6
26 +Xz
27 gSf
28 c+r
29 UOZLmnmupre1cnaJjor3tiwLCzckp0u9TqenlWqLAdQ0aLz/m7az0qBzy4ND
30 6ED5
31 -----END CERTIFICATE-----
32
```

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

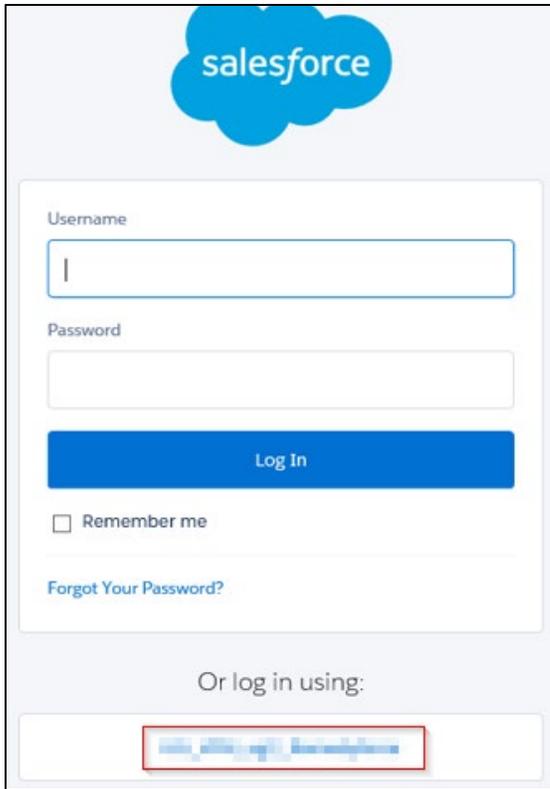
- iv. **API Name:** Type unique API name.
- v. **Entity ID:** Type the domain name.
- vi. **Identity Provider Login URL:** Enter the IdP URL, SAML 2.0 endpoint, for example, <https://example.com/saml/login>
- vii. **Custom Logout URL:** Enter the IdP Log off URL, for example, <https://example.com/cgi/tmlogout>

8. Click **Save**.

The configuration is saved and the details are displayed.

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 image shows the Salesforce login interface. At the top is the Salesforce logo. Below it is a form with the following elements:

- A "Username" label above a text input field containing a vertical cursor.
- A "Password" label above a text input field.
- A blue "Log In" button.
- A checkbox labeled "Remember me".
- A link labeled "Forgot Your Password?".
- A section titled "Or log in using:" with a red-bordered button below it.

The SP initiated configuration is completed.