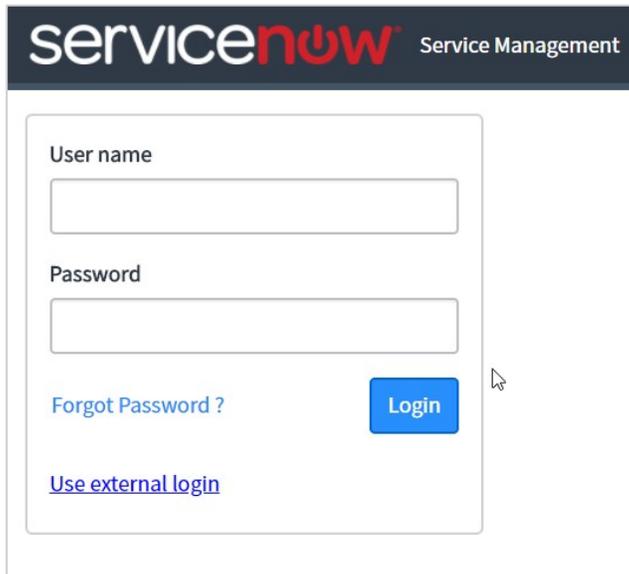


# Configuring ServiceNow

Users can securely log on to ServiceNow using their enterprise credentials. To configure ServiceNow for SSO through SAML, follow the steps below:

1. In a browser, type `https://<your-organization>.service-now.com/` and press Enter.  
**Note:** For example, if the URL you use to access pager duty is `https://myserver.service-now.com`, then you must replace `<your-organization>` with `myserver`.
2. Log on to your ServiceNow account as an administrator.

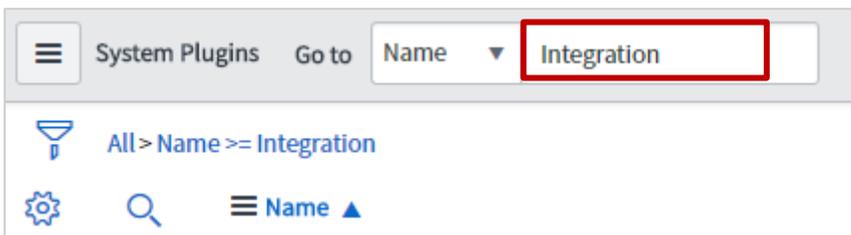


The image shows a screenshot of the ServiceNow login page. At the top, there is a dark blue header with the "serviceNOW" logo in white and red, and the text "Service Management" in white. Below the header is a white login form with a thin grey border. Inside the form, there are two input fields: "User name" and "Password". Below the "Password" field, there is a blue button labeled "Login". To the left of the "Login" button, there is a blue link that says "Forgot Password?". Below the "Forgot Password?" link, there is another blue link that says "Use external login". A mouse cursor is visible over the "Login" button.

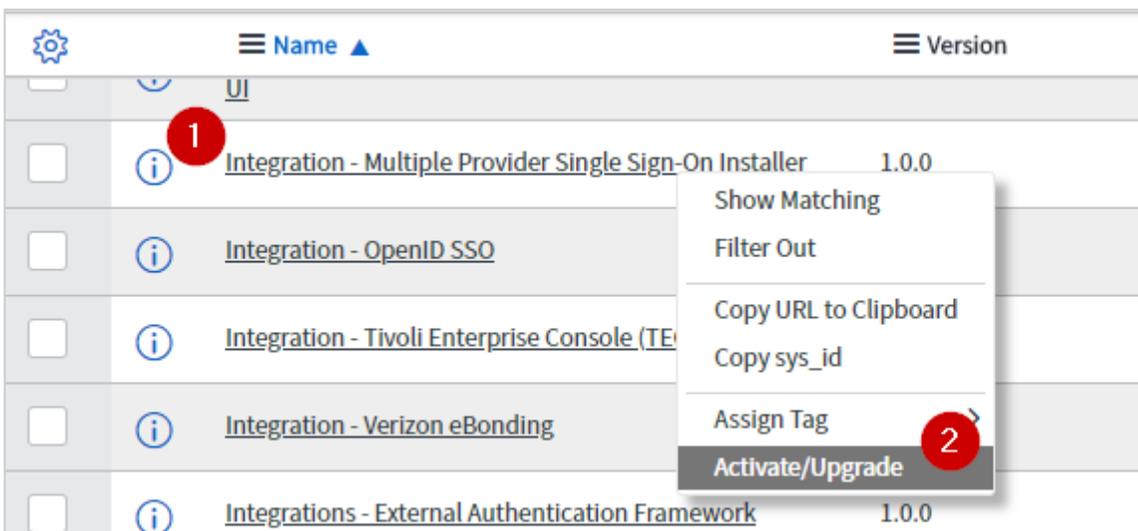
3. In the upper-left corner, using the **Filter Navigator**, search for plugins, and click **Plugins** in the search results.



4. In the right pane, in **System Plugins** section, search for integration.

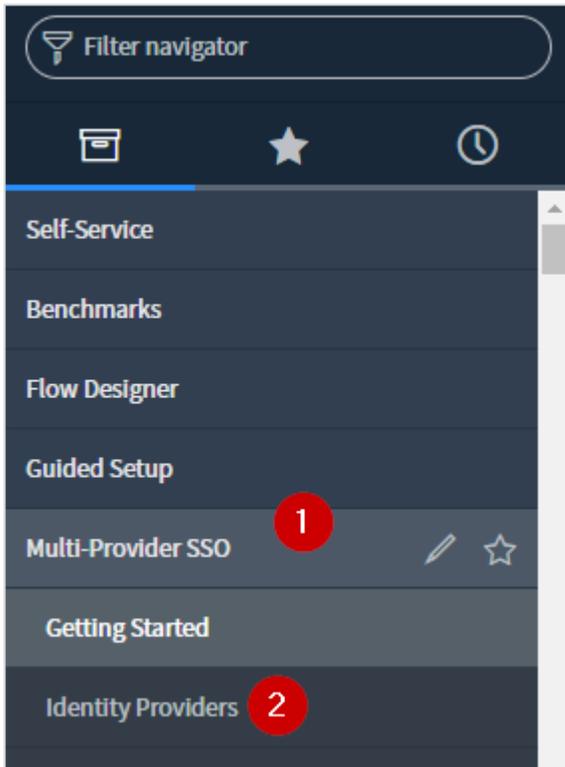


5. In the search results, right-click **Integration - Multiple Provider Single Sign-On Installer** and click **Activate/Upgrade**.

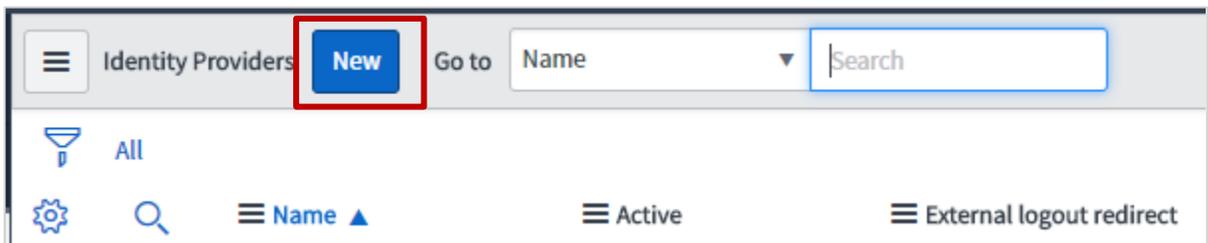


6. Click **Activate**.  
A progress bar indicates the completion of activation process.

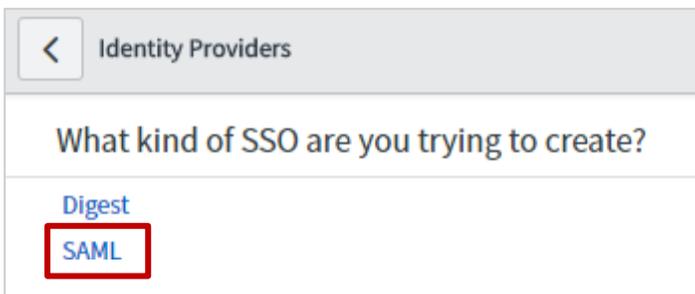
7. In the left pane, scroll down to the **Multi-Provider SSO** section and click **Multi-Provider SSO > Identity Providers**.



8. In the right pane, click **New**.



9. Click **SAML**.



10. If you have the metadata URL, in the **Identity Provider New Record** section, in the **Import Identity Provider Metadata** pop-up window, click **URL** and enter the metadata URL and click **Import**.

The values for the Identity Provider record fields are automatically populated.

If you have the metadata XML file, click **XML**. Copy the Identity Provider Metadata XML data and paste in the box. Click **Import**.

The values for the Identity Provider record fields are automatically populated. You can update the values if required.

Import Identity Provider Metadata

Identity Provider metadata can be imported in one of the following ways:

1. Using a metadata descriptor URL.
2. Using metadata descriptor XML.
3. Entering metadata manually by closing this popup.

URL  XML

Enter the URL

Cancel Import

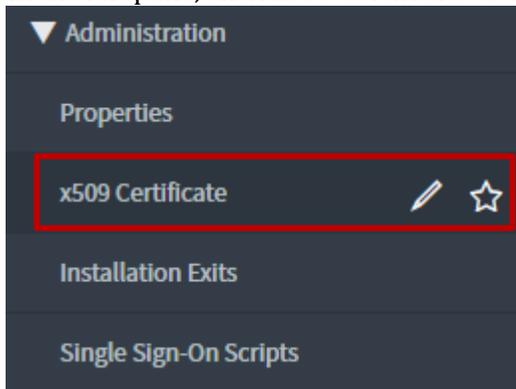
11. If you want to enter the values manually without uploading a metadata file, close the **Import Identity Provider Metadata** pop-up window. In the **Identity Provider New record** section, specify the following information:

The screenshot shows a web form titled "Identity Provider New record". The form contains several input fields and checkboxes, each with a red circle and a number indicating a specific field to be filled. The fields are: 1. Name (text input), 2. Default (checkbox), 3. Identity Provider URL (text input), 4. Identity Provider's AuthnRequest (text input), 5. Identity Provider's SingleLogoutRequest (text input), 6. ServiceNow Homepage (text input, containing "https://yourinstance.service-now.com/navpage.do"), 7. Entity ID / Issuer (text input, containing "https://yourinstance.service-now.com"), 8. Audience URI (text input, containing "https://yourinstance.service-now.com"), 9. NameID Policy (text input, containing "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"), and 10. External logout redirect (text input, containing "external\_logout\_complete.do"). There are also checkboxes for "Active" and "Auto Redirect IdP". A "Submit" button is located in the top right corner.

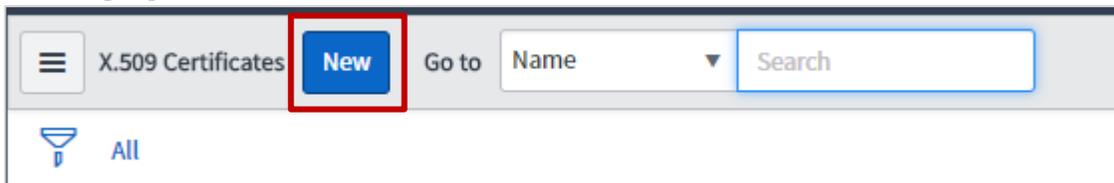
- i. **Name** – type the name that you want to use for the identity provider.
- ii. **Default** – select the check box if you want to set this configuration as default.
- iii. **Identity Provider URL** – type the issuer name that can be used while configuring IdP NetScaler for SSO.
- iv. **Identity Provider's AuthnRequest** – type the NetScaler URL followed by /saml/login. For example: https://<customerFQDN>/saml/login
- v. **Identity Provider's SingleLogoutRequest** – If you users to log out from NetScaler after they log out from ServiceNow, enter the logout URL of NetScaler: https://<customerFQDN>/cgi/logout.
- vi. **ServiceNow Homepage** – type the URL to access the home page: https://yourinstance.service-now.com/navpage.do
- vii. **Entity ID / Issuer** – Type a unique Issuer ID. For E.g. https://<yourorg.service-now.com>
- viii. **Audience URI** – type the URL in https://<yourorg.service-now.com> format.
- ix. **NameID Policy** – type urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- x. **External logout redirect** – retain the default values.

12. Click **Submit**.

13. In the left pane, click x509 Certificate to upload x509 certificate.



14. In the right pane, click **New**.



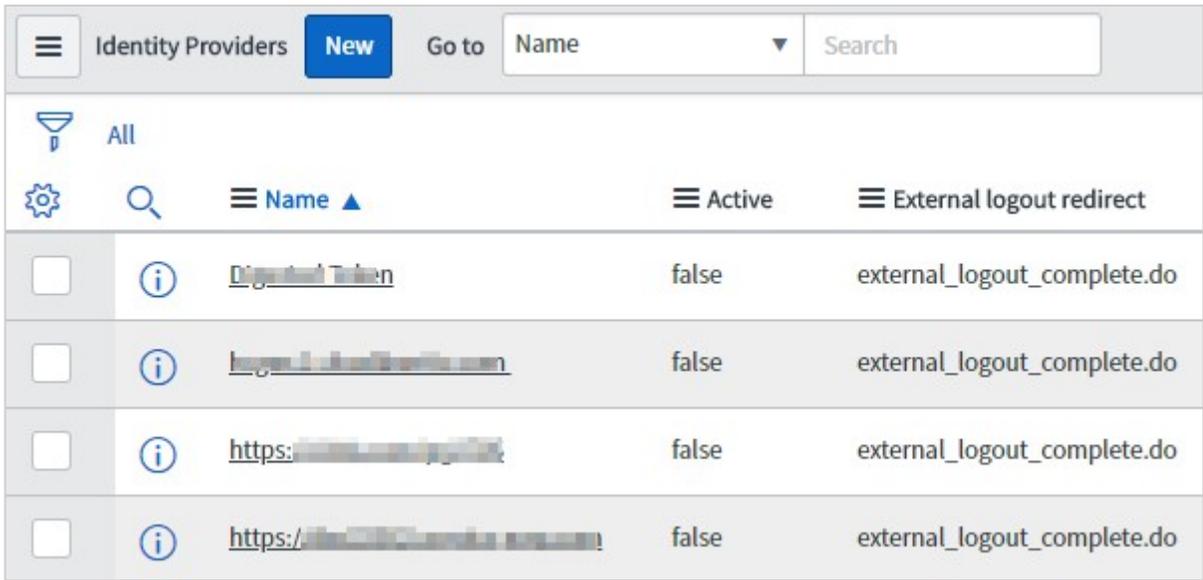
15. In the X.509 Certificate **New record** section, specify the following information:

A screenshot of the 'X.509 Certificate New record' form. The form is titled 'X.509 Certificate New record' and has a 'Submit' button in the top right. The form fields are: 1. Name (text input), 2. Format (dropdown menu, currently 'PEM'), 3. Type (dropdown menu, currently 'Trust Store Cert'), 4. Expiration notification (checkbox, checked), 5. Notify on expiration (checkbox, checked) with a user selection dropdown (currently 'System Administrator'), 6. Active (checkbox, checked), 7. Short description (text input), 8. PEM Certificate (text input), 9. Submit button. There are also fields for 'Valid from', 'Expires', and 'Expires in days' which are currently empty. A 'Related Links' section at the bottom contains a link 'Validate Stores/Certificates'.

- i. **Name** – type a certificate name.
- ii. **Format** – click the appropriate format: for e.g. PEM.
- iii. **Expiration notification** – select the check box.
- iv. **Type** – click the appropriate type.

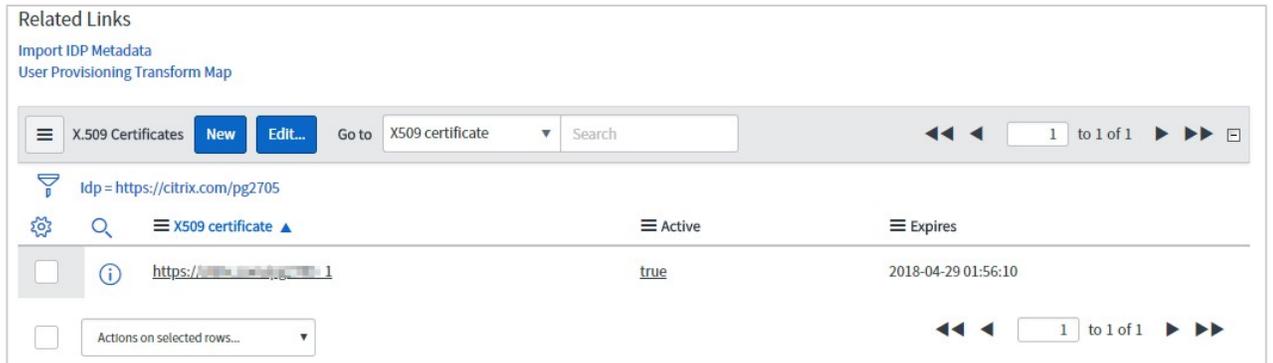


17. Click the Identity Provider that you have added.



		Name ▲	Active	External logout redirect
<input type="checkbox"/>	<a href="#">i</a>	<a href="#">DigiNotch Token</a>	false	external_logout_complete.do
<input type="checkbox"/>	<a href="#">i</a>	<a href="#">https://citrix.com/pg2705</a>	false	external_logout_complete.do
<input type="checkbox"/>	<a href="#">i</a>	<a href="#">https://citrix.com/pg2705</a>	false	external_logout_complete.do
<input type="checkbox"/>	<a href="#">i</a>	<a href="#">https://citrix.com/pg2705</a>	false	external_logout_complete.do

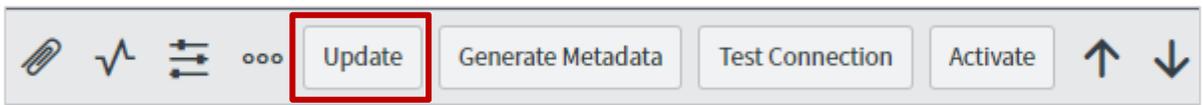
18. On the identity Provider details page, scroll down to the Related Links section. In the X.509 Certificate row, search for the X.509 certificate, and add the appropriate certificate for the identity provider by clicking **Edit**.



		X.509 certificate ▲	Active	Expires
<input type="checkbox"/>	<a href="#">i</a>	<a href="#">https://citrix.com/pg2705</a>	true	2018-04-29 01:56:10

**Note:** To add a new x.509 certificate, click **New** and to add or remove the certificates, click **Edit**.

19. To save the changes, in the upper right corner on the identity provider details page, click **Update**.

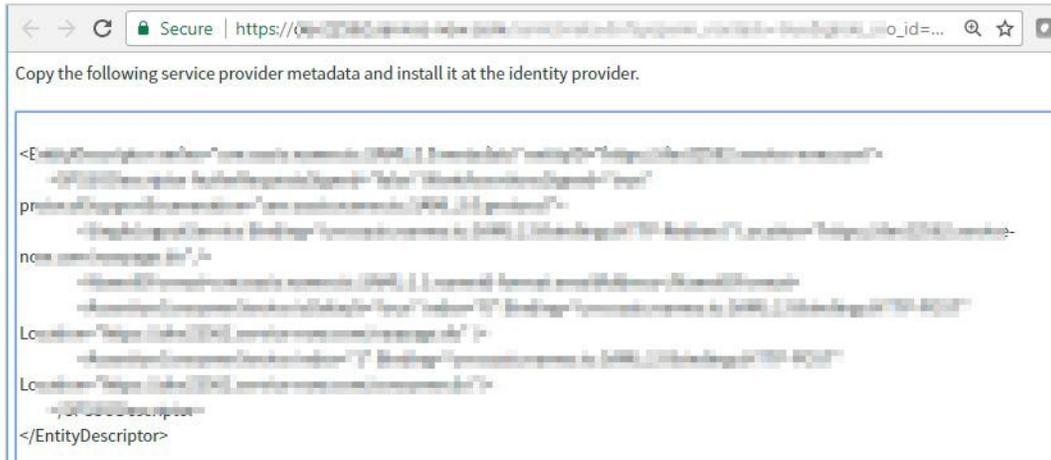


20. To obtain metadata to be used for IdP configuration, click **Generate Metadata**.

**Note:** You must click **Generate Metadata** to complete the updates.



The service provider metadata appears in a new window. Save the metadata in xml format to use it while configuring IdP for SSO.



You have completed the required configuration on the service provider which is in this case – ServiceNow.