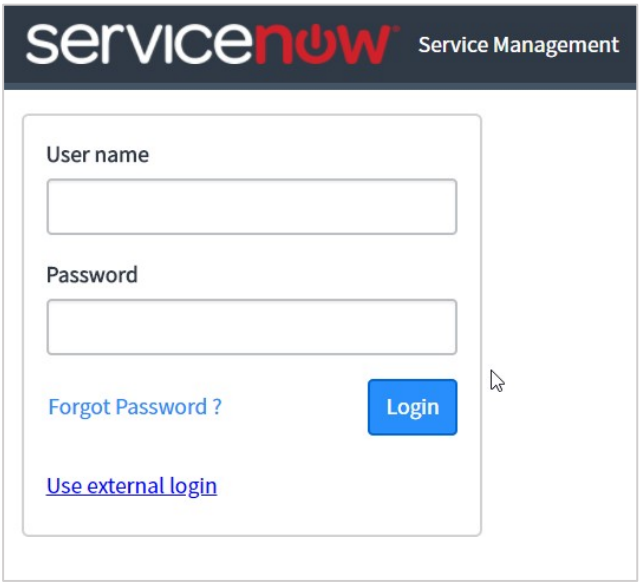
Configuring ServiceNow

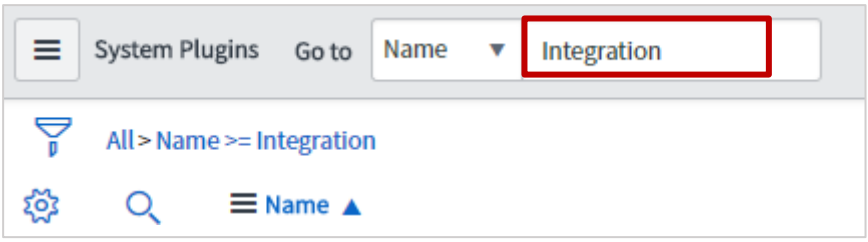
Users can securely log on to ServiceNow using their enterprise credentials. To configure ServiceNow for SSO through SAML, follow the steps below:

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.

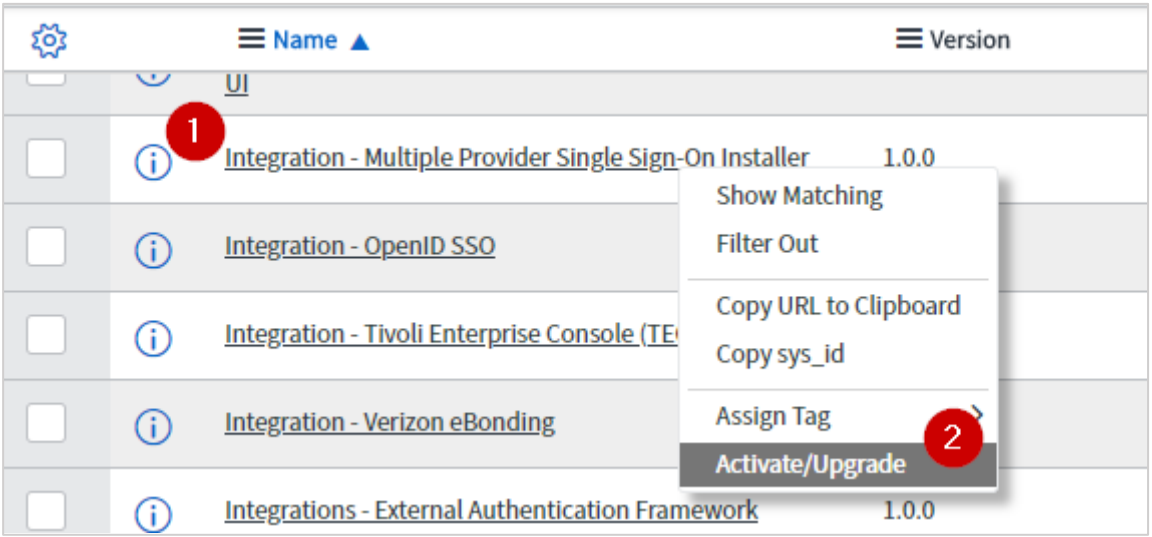


3. In the upper-left corner, using the **Filter Navigator**, search for plugins, and click **Plugins** in the search results.

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

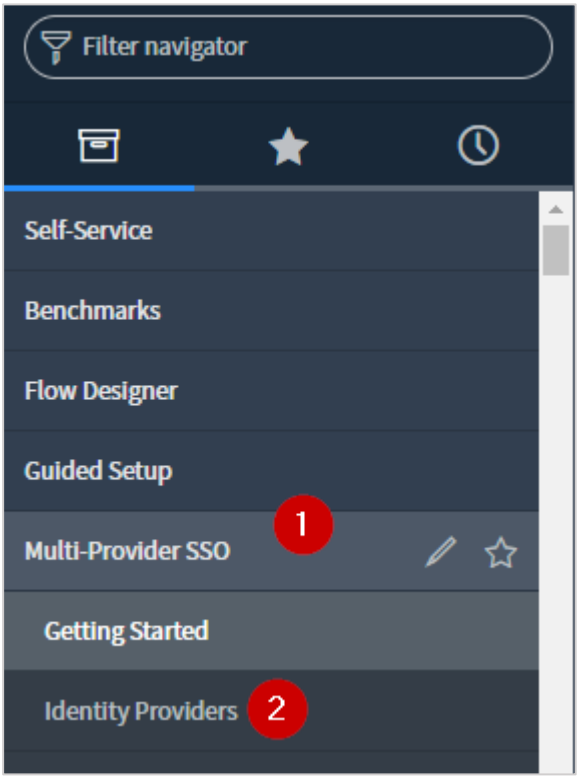


5. In the search results, right-click **Integration - Multiple Provider Single Sign-On Installer** and click **Activate/Upgrade**.

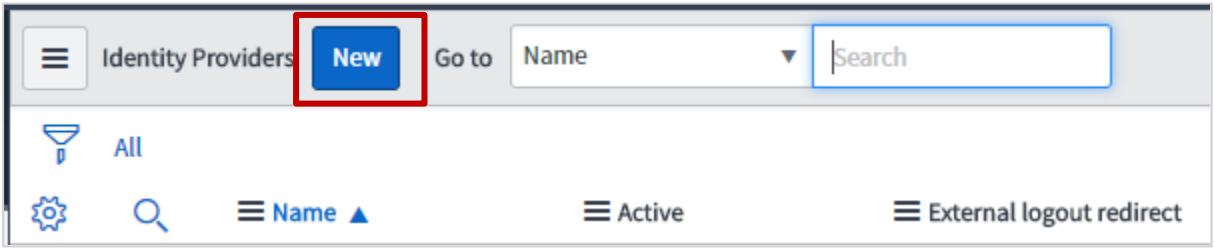


6. Click **Activate**.
A progress bar indictaes the completion of activation process.

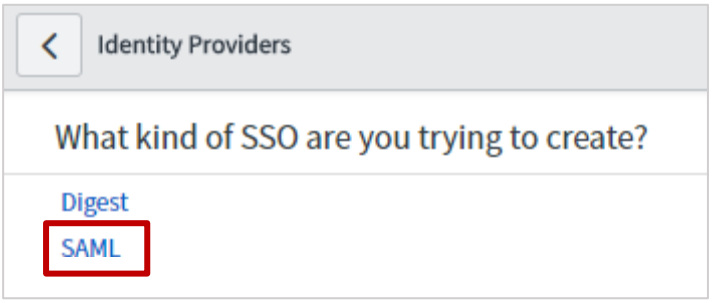
7. In the left pane, scroll down to the **Multi-Provider SSO** section and click **Multi-Provider SSO > Identity Providers**.



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

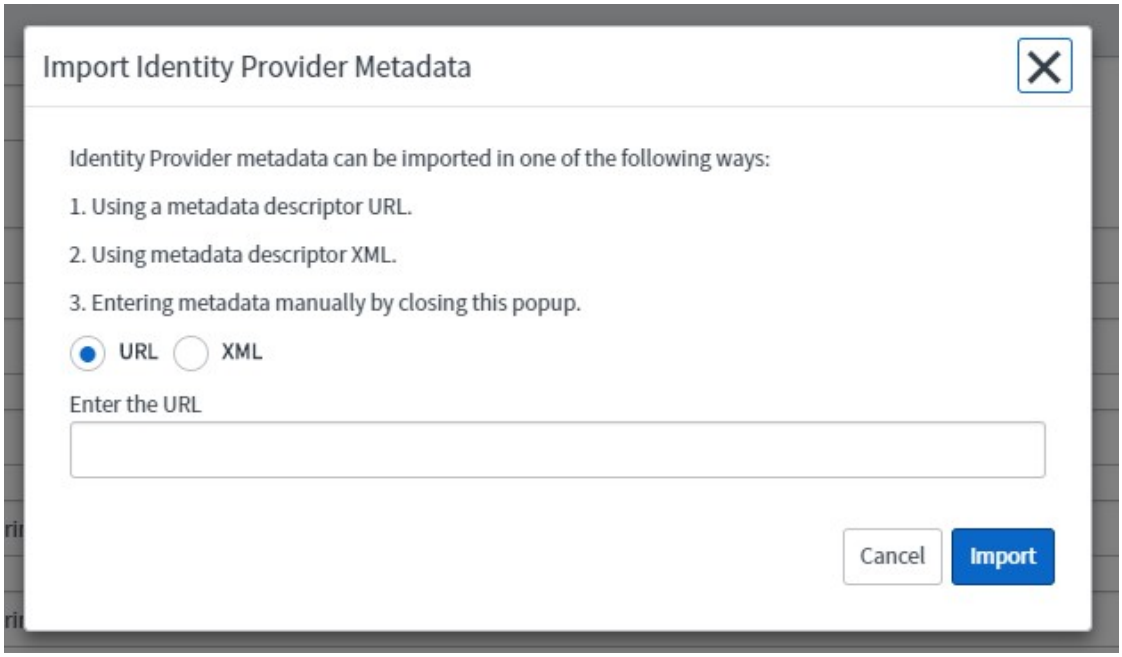


9. Click **SAML**.

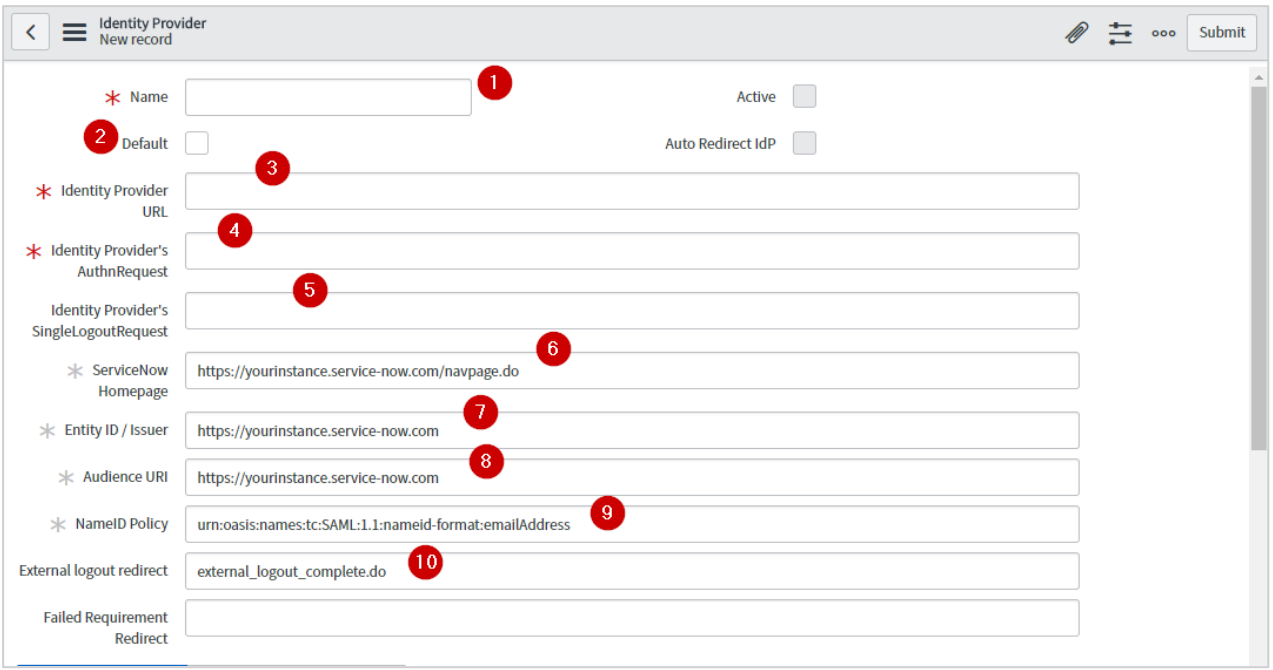


10. If you have the metadata URL, in the **Identity Provider New Record** section, in the **Import Identity Provider Metadata** pop-up window, click **URL** and enter the metadata URL and click **Import**.
    The values for the Identity Provider record fields are automatically populated.

    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.



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:



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>

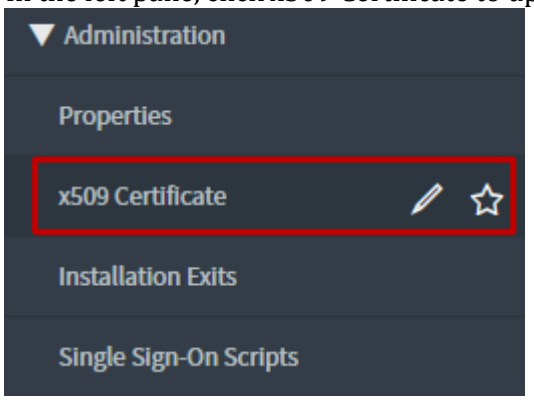
viii. **Audience URI** – type the URL in https://<yourorg.service-now.com> format.

ix. **NameID Policy** – type urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

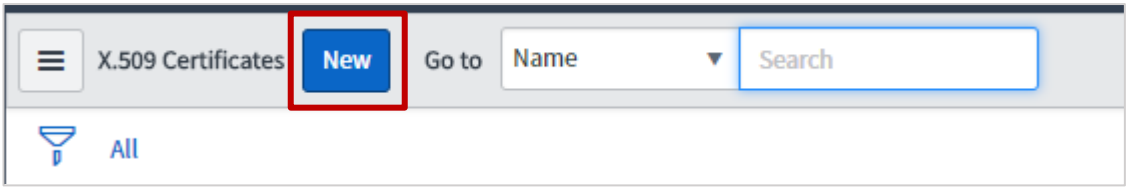
x. **External logout redirect** – retain the default values.

12. Click **Submit**.

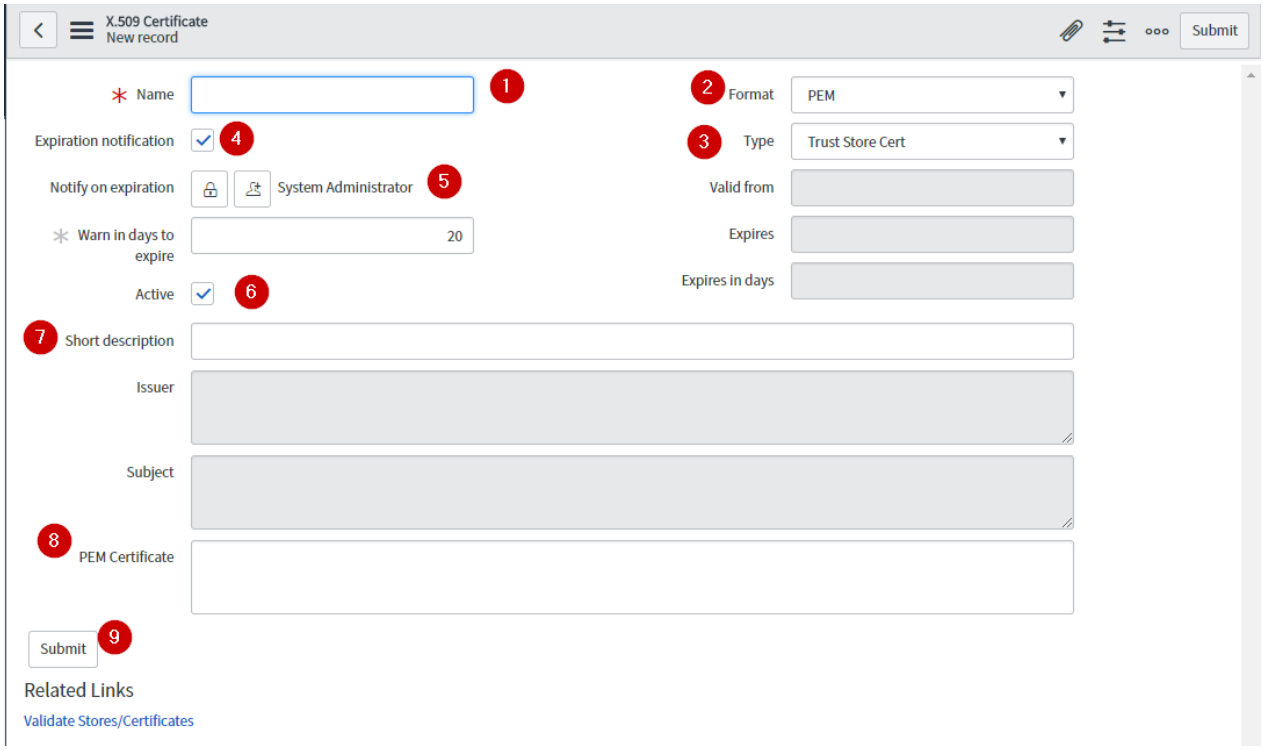
13. In the left pane, click x509 Certificate to upload x509 certificate.



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



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



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.

v. **Notify on expiration** – click the **Add me** icon  to get notified. Click the **Unlock Notify on expiration**  to add more users.

vi. **Active** – select the check box.

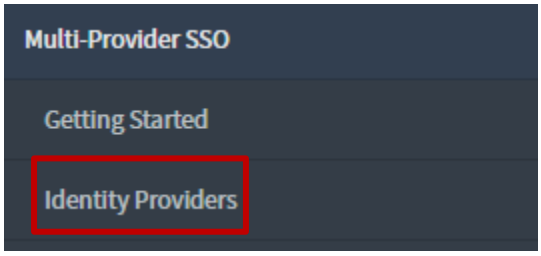
vii. **Short Description** – type description for the certificate.

viii. **PEM Certificate** – paste the PEM certificate.
To obtain your IdP certificate, follow the steps below:

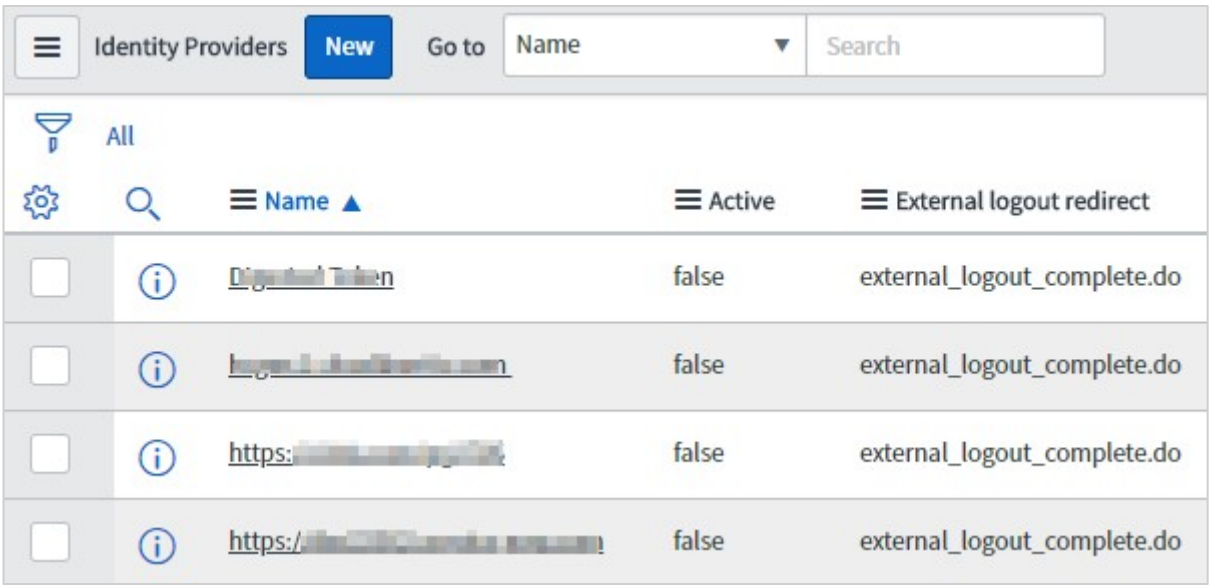
i. Remotely access your NetScaler instance using PuTTY.
ii. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.
iii. Type cat <certificate-name> and press Enter.
iv. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----
v. Paste the text in a text editor and save the file in an appropriate format such as <your organization name>.pem

ix. Click **Submit**.

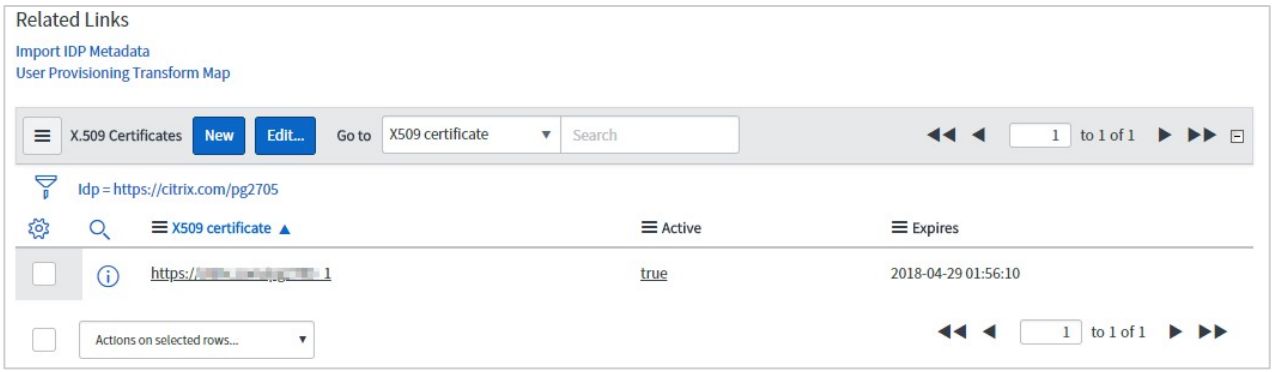
16. In the left pane, click **Identify Providers**.



17. Click the Identity Provider that you have added.

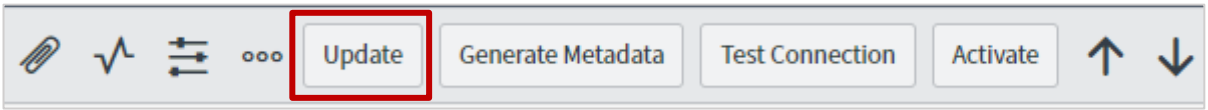


18. On the identity Provider details page, scroll down to the Related Links section. In the X.509 Certificate row, search for the X.509 certificate, and add the appropriate certificate for the identity provider by clicking **Edit**.

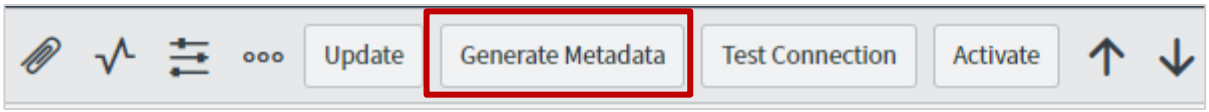


Note: To add a new x.509 certificate, click **New** and to add or remove the certificates, click **Edit**.

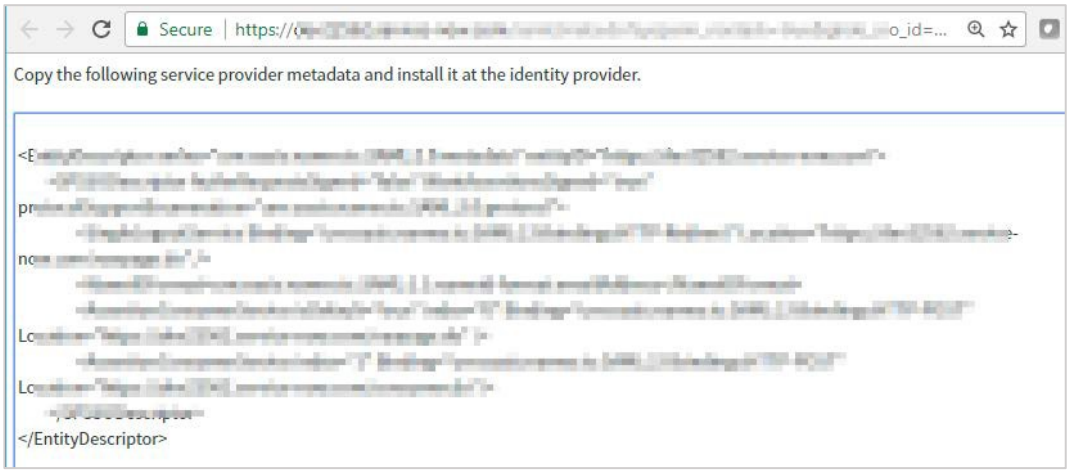
19. To save the changes, in the upper right corner on the identity provider details page, click **Update**.



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.