NetScaler with Unified Gateway

Configuring ServiceNow

Abstract

Configuring ServiceNow for SSO enables administrators to manage their users using NetScaler.

Contents

Disclaimer (Documentation)

This document is furnished "AS IS." Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix System, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

Citrix Systems, Inc., the Citrix logo, and Citrix Provisioning Services are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Preface

This section provides an overview about the information included in this guide.

Intended Audience

The information in this guide is intended for the System Administrators.

Document Conventions

The following table lists various conventions used in this guide.

Table 1: Document conventions used in this guide

Convention	Description
Bold	Used for names of interface elements (such as names of fields, panes, windows, menus, buttons, dialog boxes) and what the user specifically selects, clicks, presses, or types.
Note	Used to highlight information that is important.

Technical Support

The following table provides the technical support information for the application.

Overview

The Citrix NetScaler application delivery controller (ADC) helps to load balance, accelerate, optimize, and secure enterprise applications.

ServiceNow provides cloud-based solutions for IT service management in IT operations, business and software development, and security operations, and performance analytics.

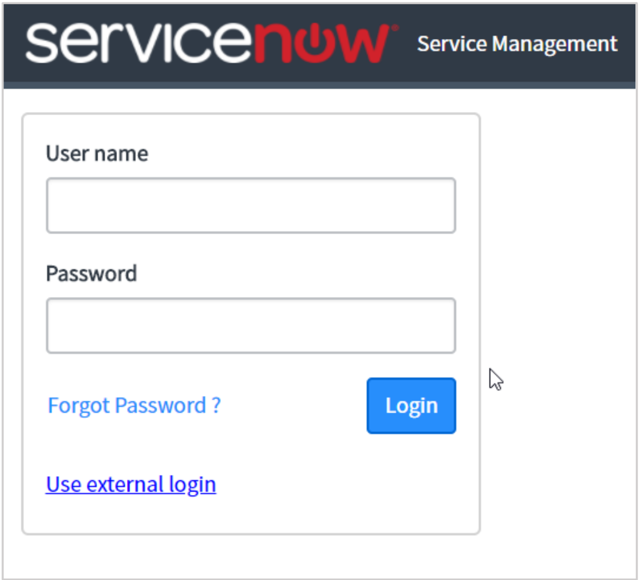
You can connect ServiceNow with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring ServiceNow for Single Sign-On

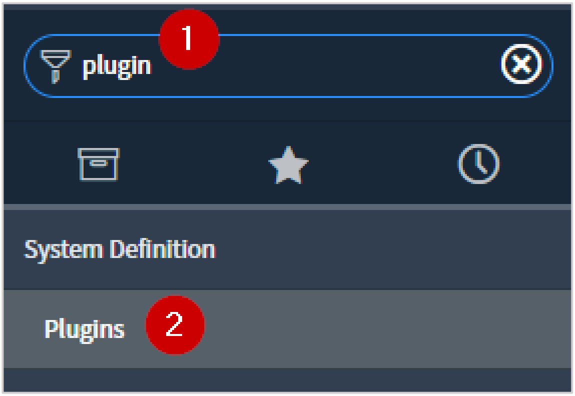
Configuring ServiceNow for SSO enables administrators to manage their users using NetScaler. Users can securely log on to ServiceNow using their enterprise credentials.

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

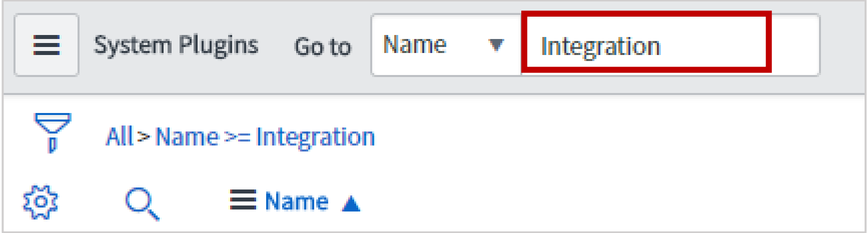
1. In a browser, type https://<your-organization>.service-now.com/ and press Enter.
   Note: For example, if the URL you use to access pager duty is https://myserver.service-now.com, then you must replace <your-organization> with myserver.
2. Log on to your ServiceNow account as an administrator.



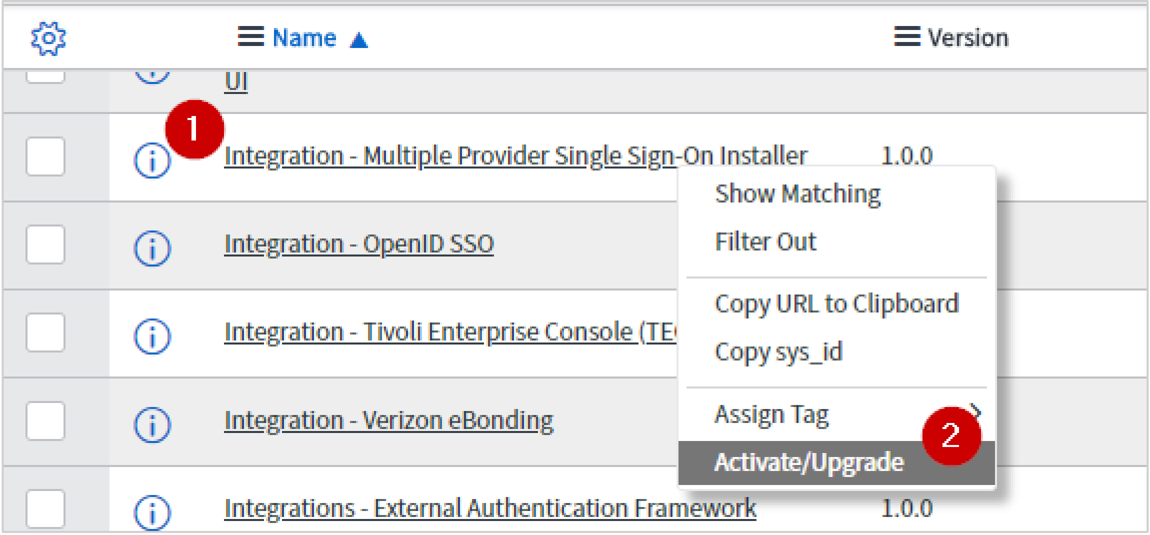
3. In the upper-left corner, using the **Filter Navigator**, search for plugins, and click **Plugins** in the search results.



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

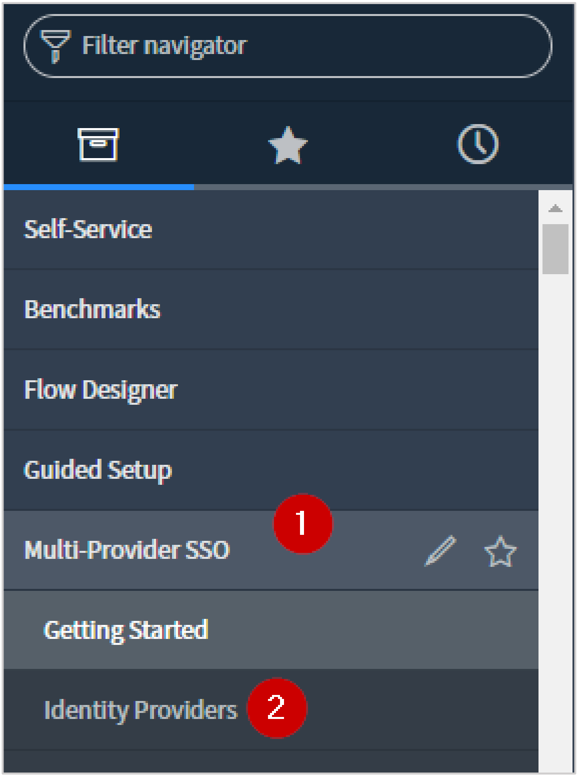


5. In the search results, right-click **Integration - Multiple Provider Single Sign-On Installer** and click **Activate/Upgrade**.

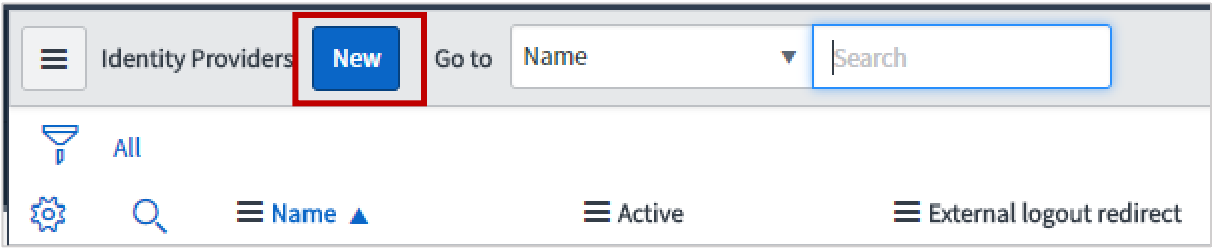

Name ▲
Version
UI
1
Integration - Multiple Provider Single Sign-On Installer
1.0.0
Integration - OpenID SSO
Integration - Tivoli Enterprise Console (TE
Integration - Verizon eBonding
Integrations - External Authentication Framework
1.0.0
Show Matching
Filter Out
Copy URL to Clipboard
Copy sys_id
Assign Tag
Activate/Upgrade
2

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

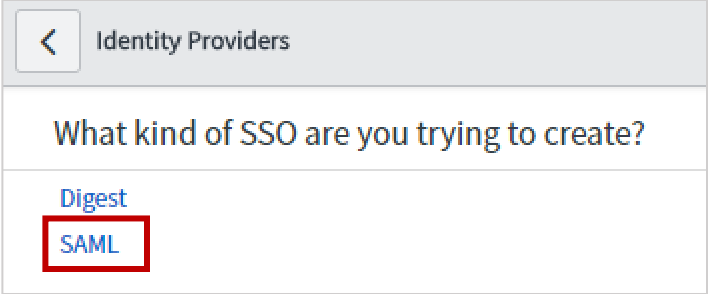
7. In the left pane, scroll down to the **Multi-Provider SSO** section and click **Multi-Provider SSO > Identity Providers**.



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

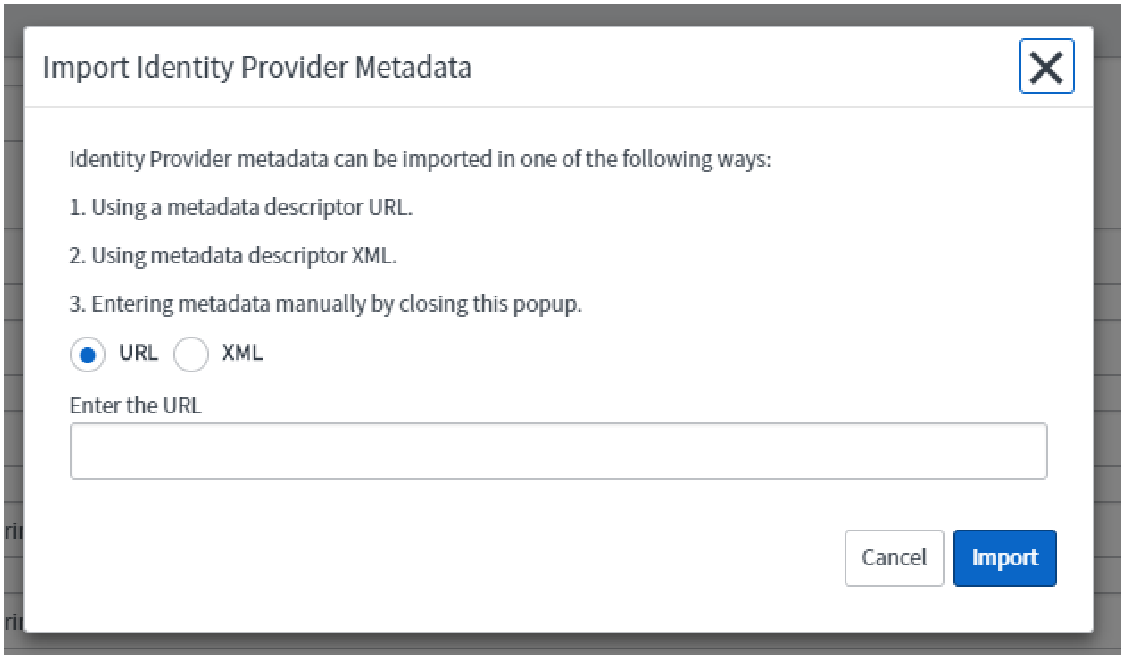


9. Click **SAML**.



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.



Import Identity Provider Metadata

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

1. Using a metadata descriptor URL.

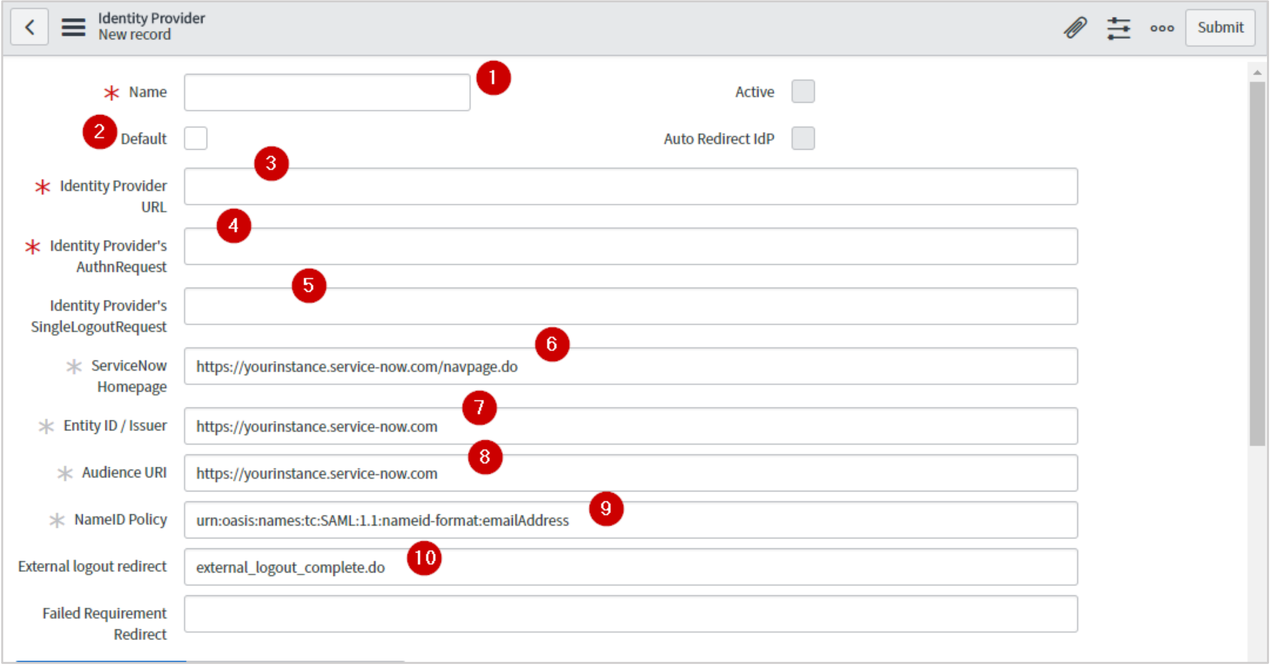
2. Using metadata descriptor XML.

3. Entering metadata manually by closing this popup.

● URL ○ XML

Enter the URL

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:



Identity Provider
New record

* Name	
Active	□
Default	□
Auto Redirect IdP	□
* Identity Provider URL	
* Identity Provider's AuthnRequest	
Identity Provider's SingleLogoutRequest	
* ServiceNow Homepage	https://yourinstance.service-now.com/navpage.do
* Entity ID / Issuer	https://yourinstance.service-now.com
* Audience URI	https://yourinstance.service-now.com
* NameID Policy	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
External logout redirect	external_logout_complete.do
Failed Requirement Redirect	

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>

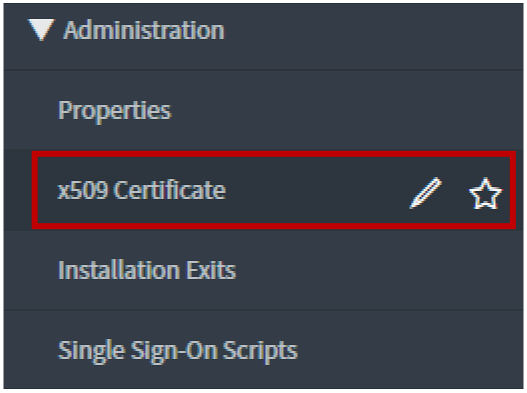
viii. **Audience URI** – type the URL in https://<yourorg.service-now.com> format.

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

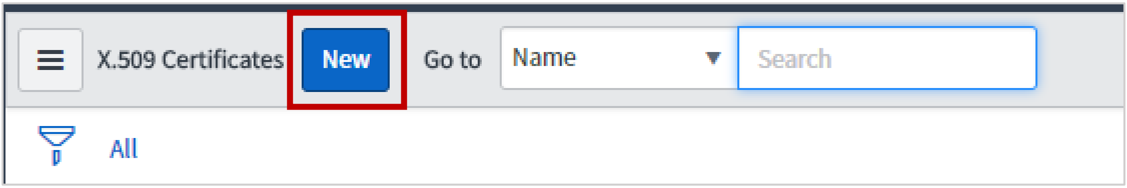
x. **External logout redirect** – retain the default values.

12. Click **Submit**.

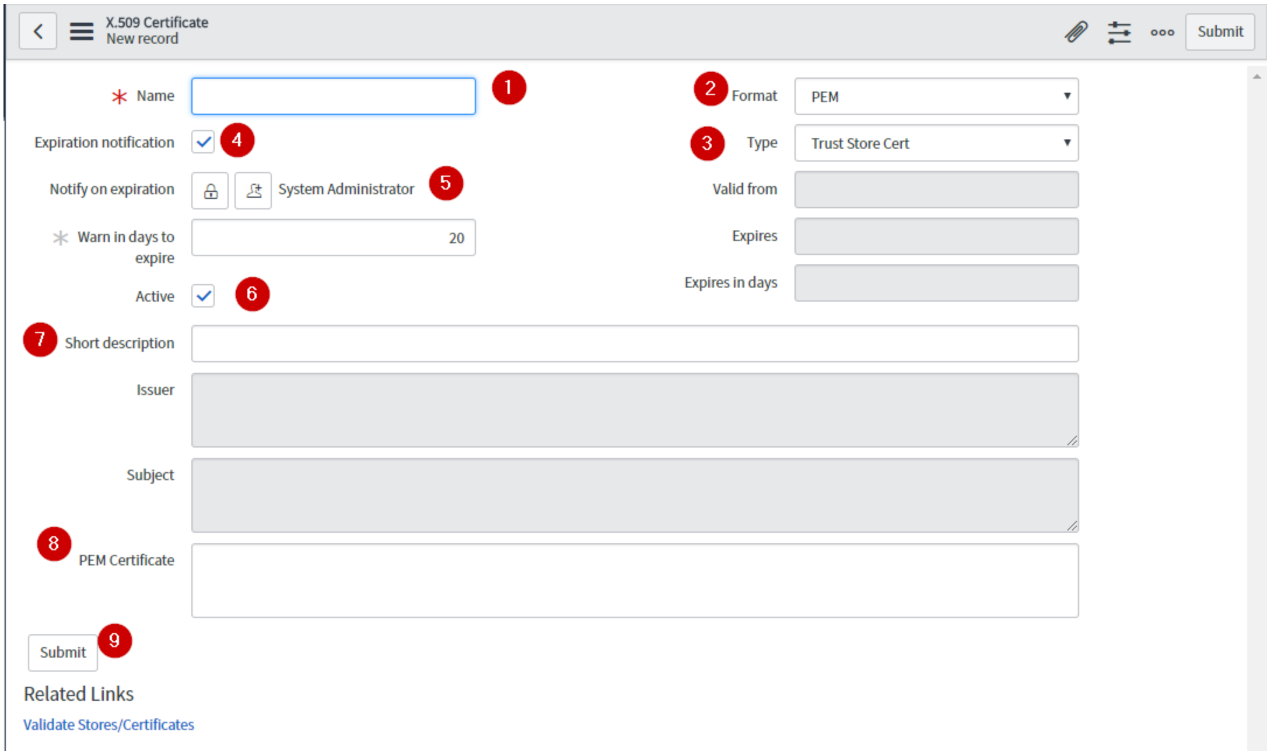
13. In the left pane, click x509 Certificate to upload x509 certificate.



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



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



X.509 Certificate
New record

1 * Name		2 Format	PEM
Expiration notification	☑ 4	3 Type	Trust Store Cert
Notify on expiration	System Administrator 5	Valid from	
* Warn in days to expire	20	Expires	
Active	☑ 6	Expires in days	
7 Short description			
Issuer			
Subject			
8 PEM Certificate			

i. **Name** – type a certificate name.

ii. **Format** – click the appropriate format: for e.g. PEM.

iii. **Expiration notification** – select the check box.

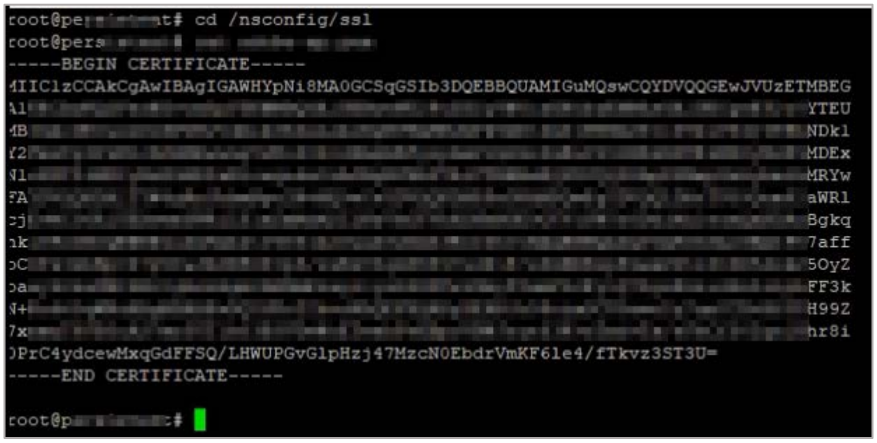
iv. **Type** – click the appropriate type.

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.

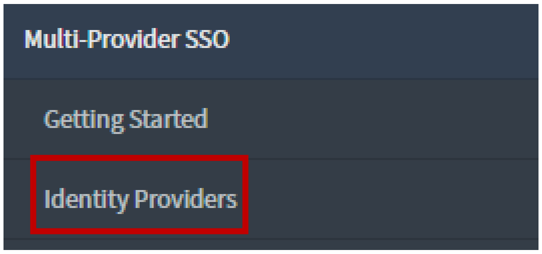
viii. **PEM Certificate** – paste the PEM certificate.
To obtain your IdP certificate, follow the steps below:
  i. Remotely access your NetScaler instance using PuTTY.
  ii. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.
  iii. Type cat <certificate-name> and 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



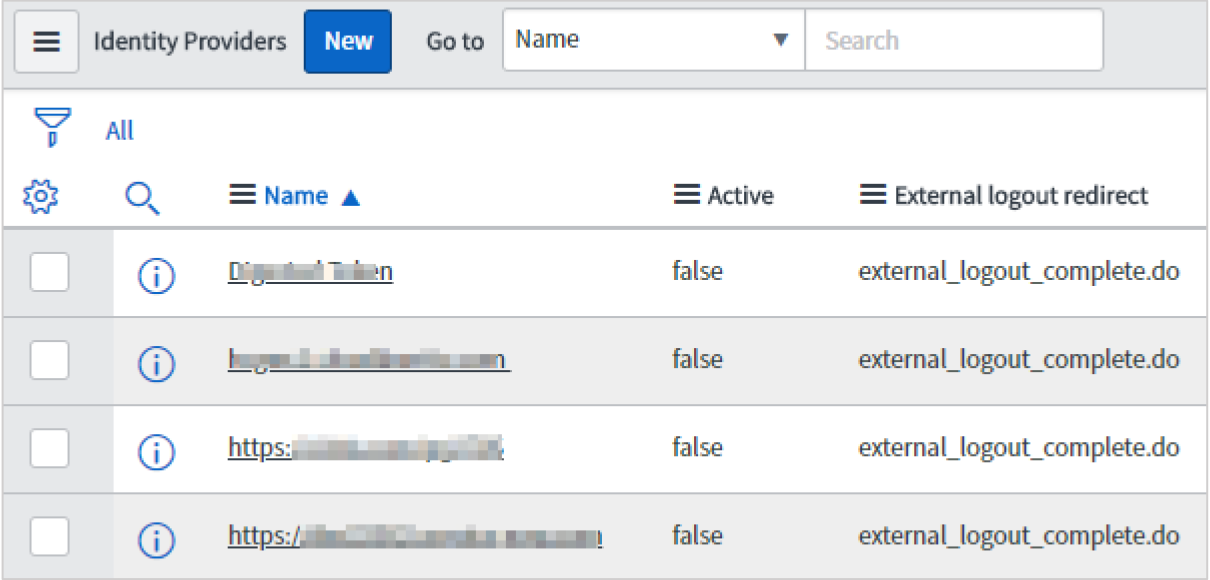
```
root@pe[redacted]t# cd /nsconfig/ssl
root@pers[redacted]
-----BEGIN CERTIFICATE-----
MIIC1zCCAkCgAwIBAgIGAWHYpNi8MA0GCSqGSIb3DQEBBQUAMIGuMQswCQYDVQQGEwJVUzETMBEG
A1[redacted]YTEU
MB[redacted]NDk1
Y2[redacted]MDEx
N1[redacted]MRYw
FA[redacted]aWR1
cj[redacted]Bgkq
nk[redacted]7aff
bC[redacted]5OyZ
ba[redacted]FF3k
N+[redacted]H99Z
7x[redacted]hr8i
DPrC4ydcewMxqGdFFSQ/LHWUPGvGlpHzj47MzcN0EbdrVmKF6le4/fTkvz3ST3U=
-----END CERTIFICATE-----

root@p[redacted]:#
```

ix. Click **Submit**.

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

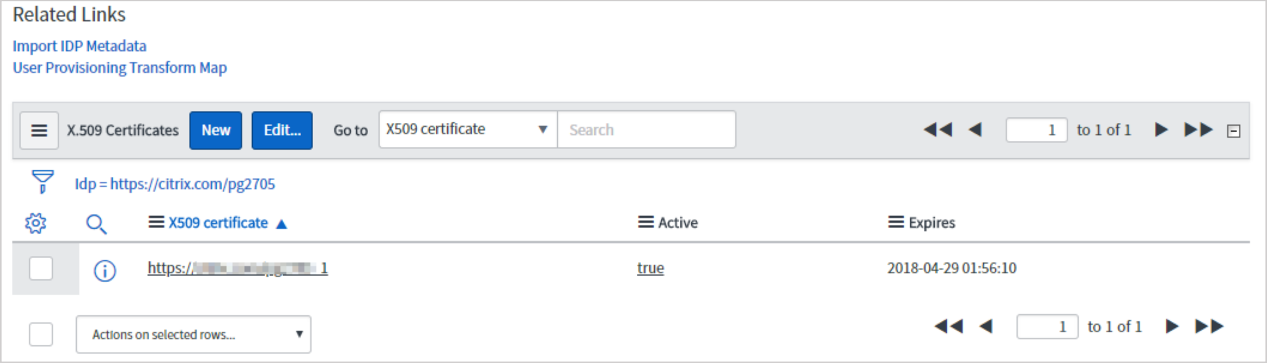


17. Click the Identity Provider that you have added.



Name ▲	Active	External logout redirect
[redacted]	false	external_logout_complete.do
[redacted]	false	external_logout_complete.do
https:[redacted]	false	external_logout_complete.do
https:/[redacted]	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**.



Related Links

Import IDP Metadata

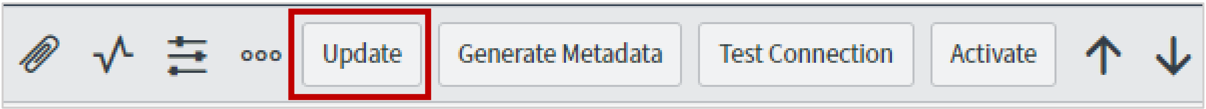
User Provisioning Transform Map

Idp = https://citrix.com/pg2705

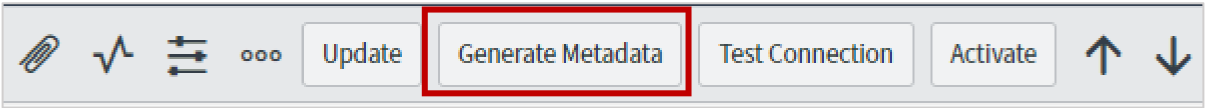
X509 certificate ▲	Active	Expires
https://[redacted] 1	true	2018-04-29 01:56:10

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

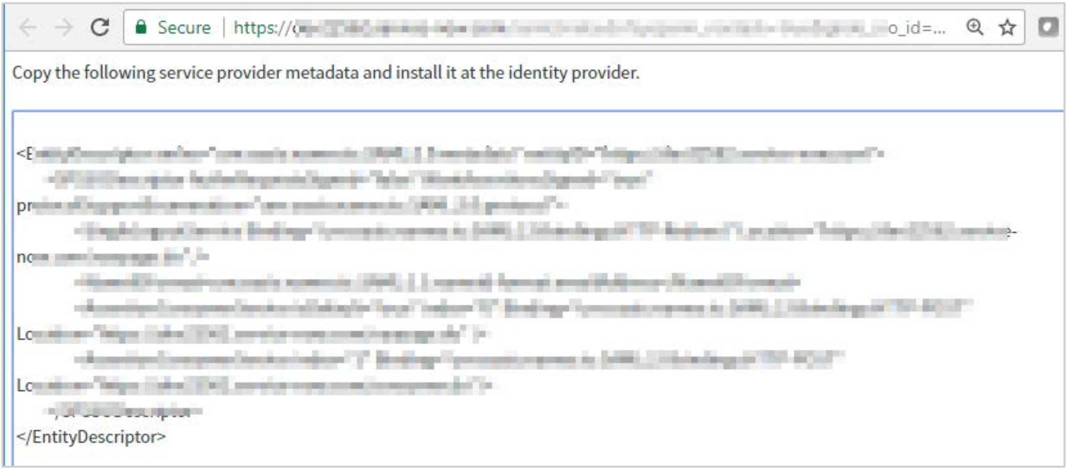
19. To save the changes, in the upper right corner on the identity provider details page, click **Update**.



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.



Copy the following service provider metadata and install it at the identity provider.

```
<E[redacted]
</EntityDescriptor>
```

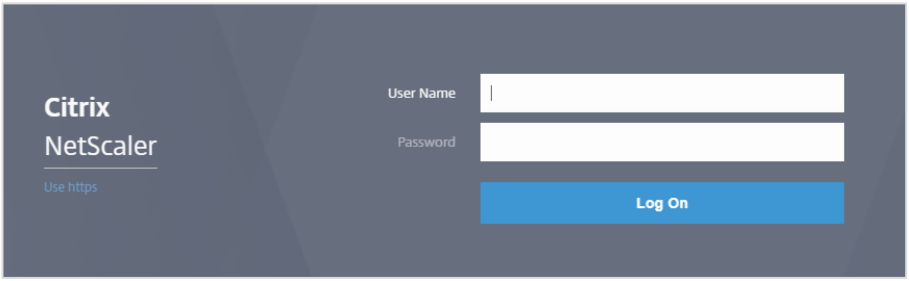
You have completed the required configuration on the service provider which is in this case – ServiceNow.

Configuring NetScaler for Single Sign-On

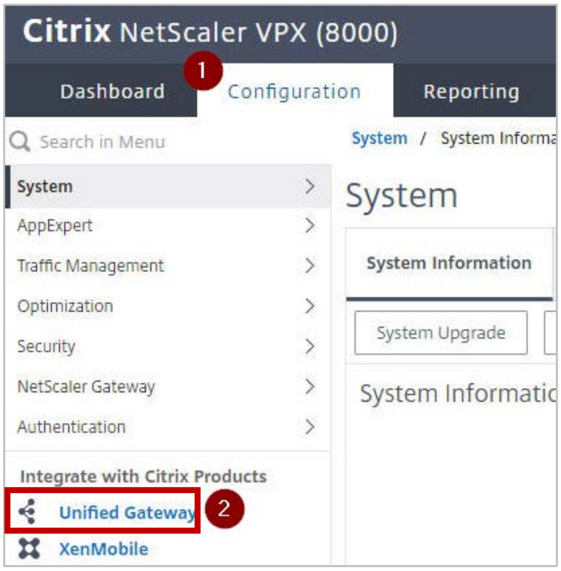
For configuring NetScaler for ServiceNow, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

To configure NetScaler for single sign on through SAML, complete the following steps:

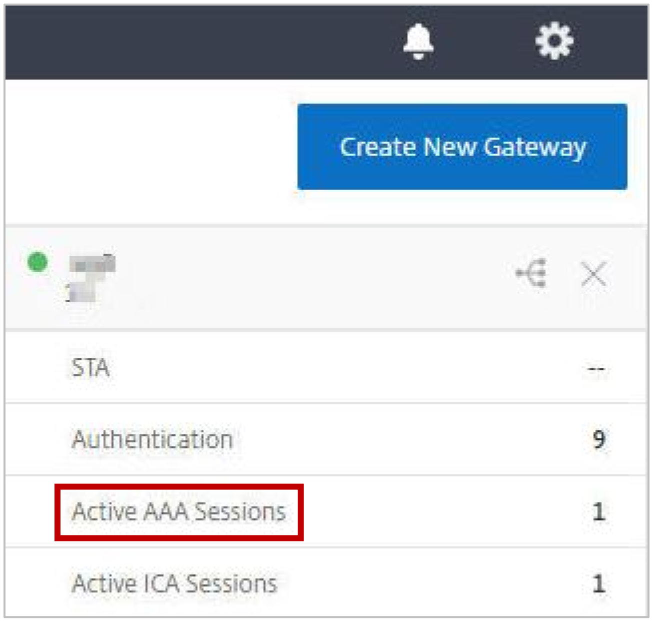
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



3. Click **Configuration** > **Unified Gateway**.

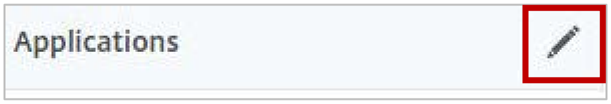


4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.

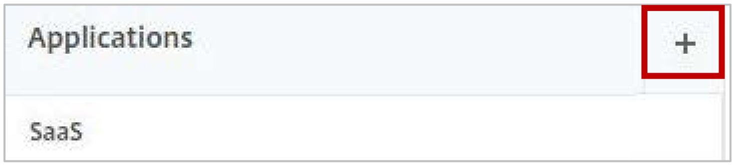


STA	--
Authentication	9
Active AAA Sessions	1
Active ICA Sessions	1

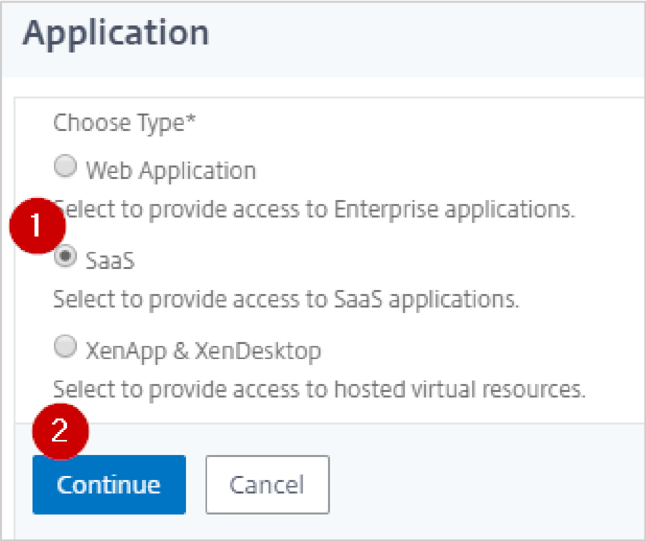
5. Click the edit icon for **Applications** section.



6. For adding a SaaS application, click the plus icon ⊞ that appears in the edit mode.



7. Click **SaaS** > **Continue**.


Application

Choose Type*

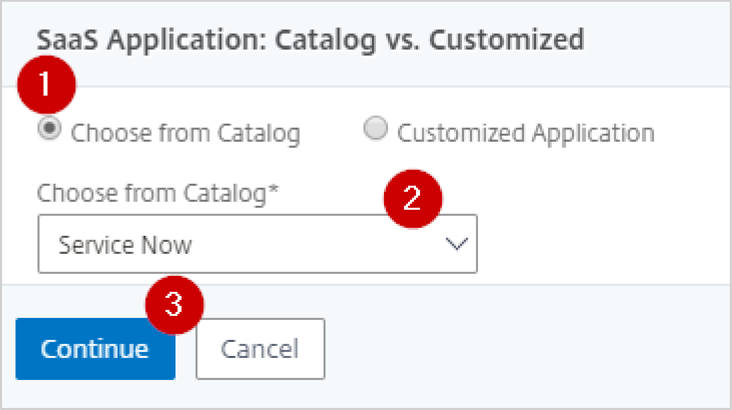
○ Web Application
Select to provide access to Enterprise applications.

● SaaS
Select to provide access to SaaS applications.

○ XenApp & XenDesktop
Select to provide access to hosted virtual resources.

8. Click **Choose from Catalog**.

9. In the **Choose from Catalog** list, click **ServiceNow**.



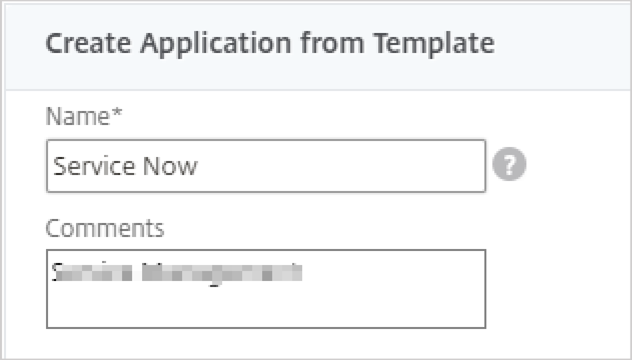
SaaS Application: Catalog vs. Customized

● Choose from Catalog ○ Customized Application

Choose from Catalog*: Service Now

10. Click **Continue**.

11. In the **Create Application from Template** section, type the name of your SaaS application, in this case ServiceNow, and relevant comments.



Create Application from Template

Name*: Service Now

Comments: [redacted]

Note:

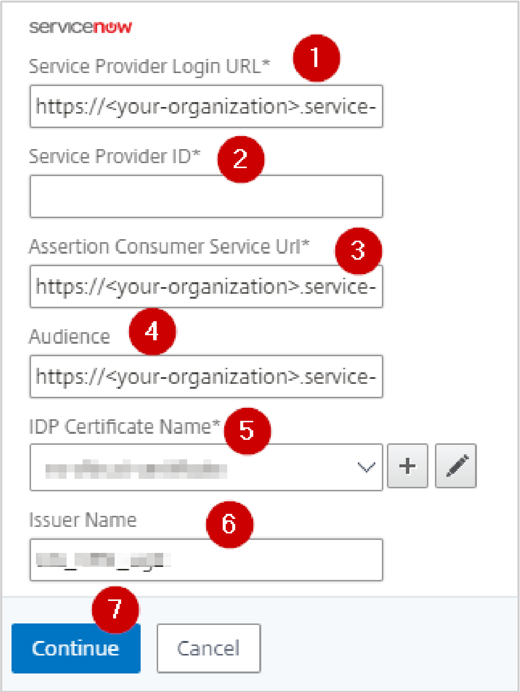
An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

The following table lists the SAML values that you need to copy while configuring SSO for SP and paste the values to appropriate fields while configuring SSO for IdP NetScaler.

Table 2: SSO field values used for SP and IdP configurations

Service Provider (SP) ServiceNow	Identity Provider (IdP) NetScaler
Entity Id/ Issuer	Service Provider ID
Identity Provider URL	Issuer Name

12. In the area below the logo, specify the following information:



servicenow

Service Provider Login URL*
https://<your-organization>.service-

Service Provider ID*

Assertion Consumer Service Url*
https://<your-organization>.service-

Audience
https://<your-organization>.service-

IDP Certificate Name*
[redacted]

Issuer Name
[redacted]

   i. **Service Provider Login URL -** type the ServiceNow URL in https://<your-organization>.service-now.com format.
      Note: For example, if the organization's URL is https://myserver.service-now.com, you must replace <your-organization> with myserver.
   ii. **Service Provider ID -** enter the URL that you entered in the Entity ID/ Issuer field while configuring ServiceNow.
   iii. **Assertion Consumer Service Url* -** type the URL that you entered in the ServiceNow Homepage field while configuring ServiceNow.
   iv. **IdP Certificate Name -** click the appropriate certificate name.
      The IdP certificate appears last in the hierarchy in the **Server Certificate** section on **Unified Gateway Configuration** page.
   v. **Issuer Name** –type the issuer ID that you entered in the Identity Provider URL field while configuring ServiceNow. For example: MyServer_NS_ServiceNow

13. Click **Continue.**

14. Click **Done**.

    The ServiceNow logo appears.

15. Click **Done**.

    You have completed the NetScaler configuration for ServiceNow.

Testing the Configuration

Testing the IdP Initiated Flow

To test the IdP initiated configuration, follow the steps below:

1. Access the IdP URL.

2. Log on to NetScaler appliance using your enterprise credentials.

3. Click **Clientless Access**.

4. On the home page, click **Apps** tab.

5. Click **ServiceNow**.
   Your ServiceNow profile appears.
   You have completed testing the IdP initiated flow.

Testing the SP Initiated Flow

To test the SP initiated configuration, follow the steps below:

1. Access the organization's URL for ServiceNow.

2. Type your organizational user name.
   You are redirected to NetScaler appliance's log in page.

3. Log on to NetScaler appliance using your enterprise credentials.

   Your ServiceNow profile appears which indicates that you have successfully logged on to ServiceNow.

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United
States Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States