NetScaler with Unified Gateway

Configuring Salesforce

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.

Overview

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

Salesforce can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to Salesforce using the same Single Sign On (SSO

Terminology

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 various terms that are used alternatively for completing configurations for service providers and identity providers.

Table 2: Terminology used for SP and IdP configurations

Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

Configuring Salesforce for Single Sign-On

Salesforce has SP/IdP initiated flow, which is supported in Netscaler (12.1).

Before you start, you need the following:

- Admin account for Salesforce.
- Customer instance.
  For example, if your deployment URL is https://<customer_domain>.my.salesforce.com, your customer Instance is <*customer_domain*>.

  This is required for App Catalog creation in NetScaler.
- Admin account for NetScaler.

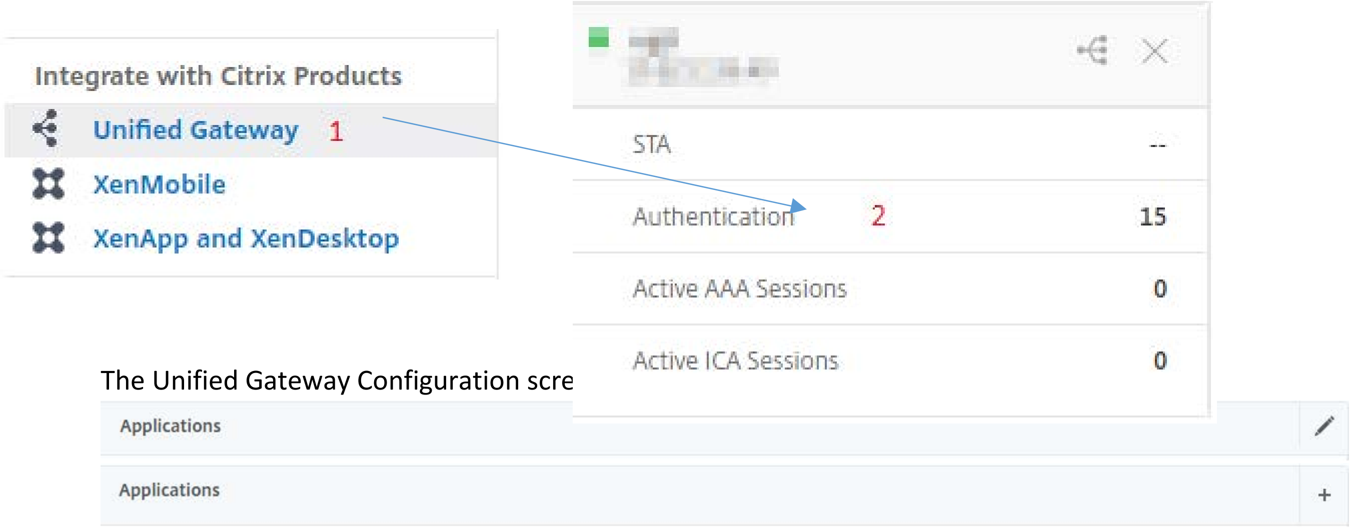
Salesforce Configuration

The Salesforce configuration steps are as follows:

1. Configure Salesforce with the App Catalog.
2. Export Salesforce IdP metadata from Netscaler.
3. Import IdP metadata into Salesforce.

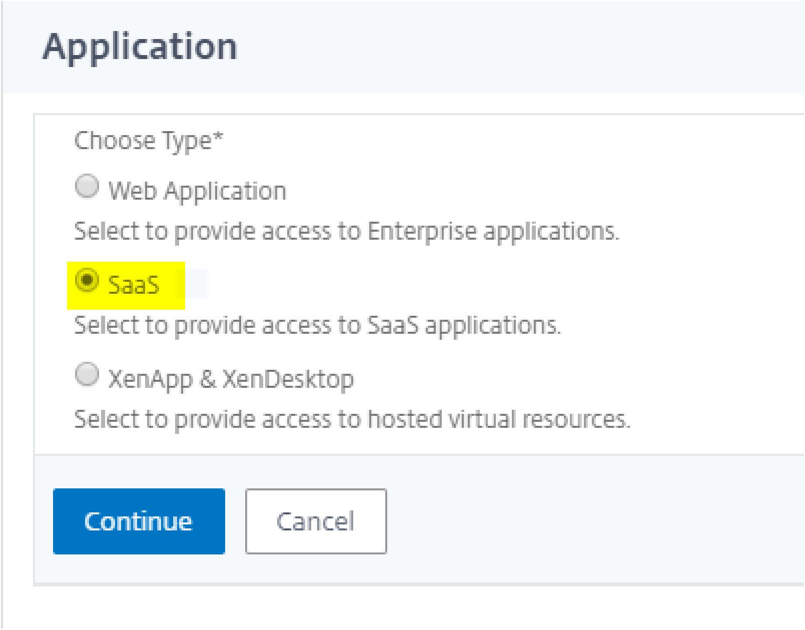
Step 1: Configure Salesforce with App catalog

1. Click on Unified Gateway > Authentication



The Unified Gateway Configuration scre

2. Go to **Application** section. click on ✎ icon. Now you can see + **icon.** Click on it. The **Application** window appears.



Application

Choose Type*

○ Web Application

Select to provide access to Enterprise applications.

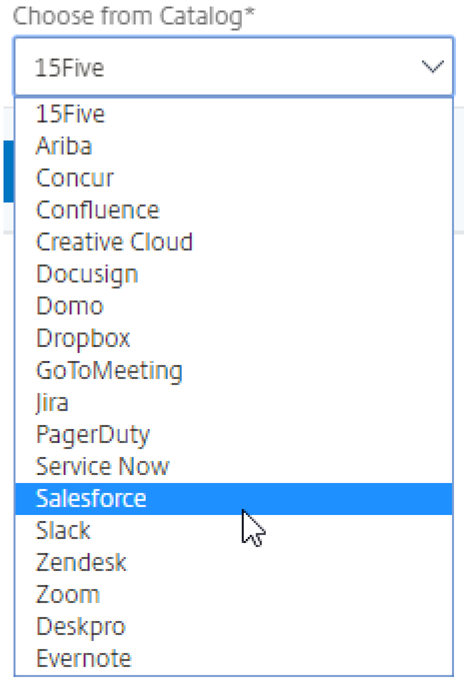
● SaaS

Select to provide access to SaaS applications.

○ XenApp & XenDesktop

Select to provide access to hosted virtual resources.

3. Select **SaaS** from the Application type.
4. Select salesforce from the dropdown list.

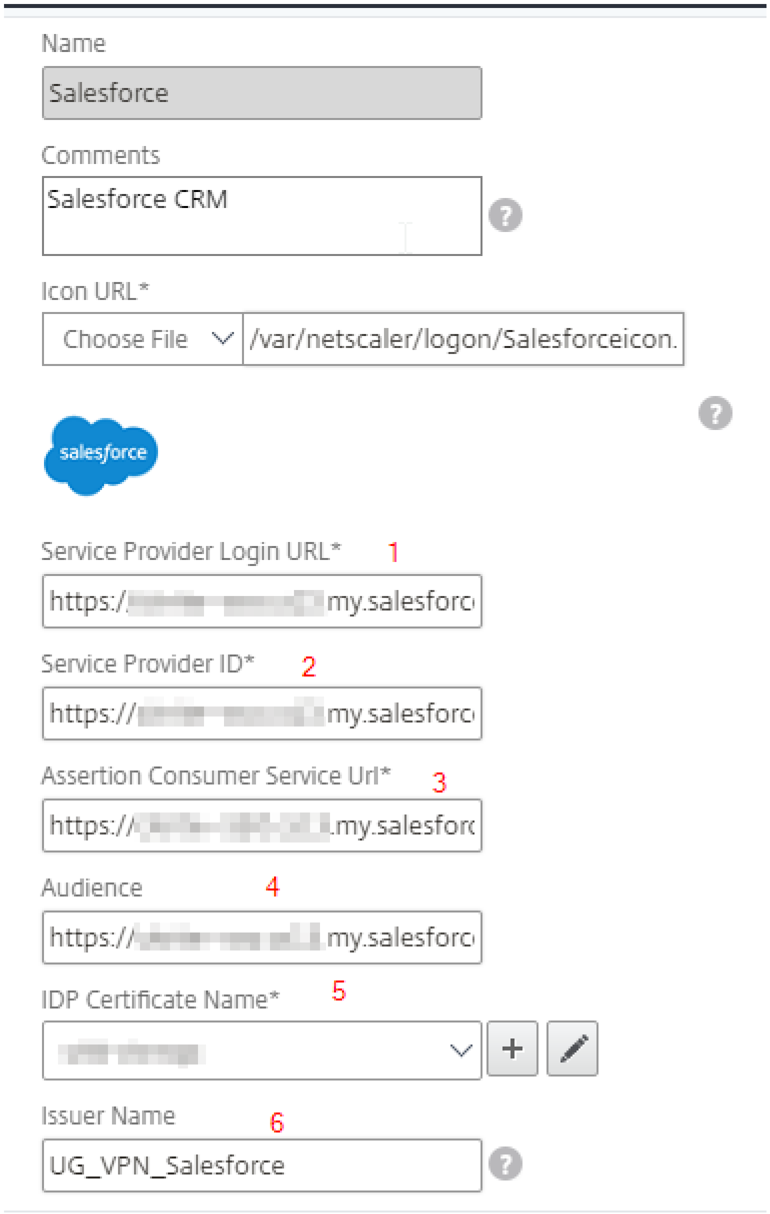


Choose from Catalog*

15Five

- 15Five
- Ariba
- Concur
- Confluence
- Creative Cloud
- Docusign
- Domo
- Dropbox
- GoToMeeting
- Jira
- PagerDuty
- Service Now
- Salesforce
- Slack
- Zendesk
- Zoom
- Deskpro
- Evernote

5. Fill the Application template with appropriate values.



Name

Salesforce

Comments

Salesforce CRM

Icon URL*

Choose File /var/netscaler/logon/Salesforceicon.

Service Provider Login URL* 1

https:/[redacted]my.salesforc

Service Provider ID* 2

https://[redacted]my.salesforc

Assertion Consumer Service Url* 3

https://[redacted].my.salesforc

Audience 4

https://[redacted]my.salesforc

IDP Certificate Name* 5

[redacted]

Issuer Name 6

UG_VPN_Salesforce

6. You must update the fields in Netscaler with the following values:

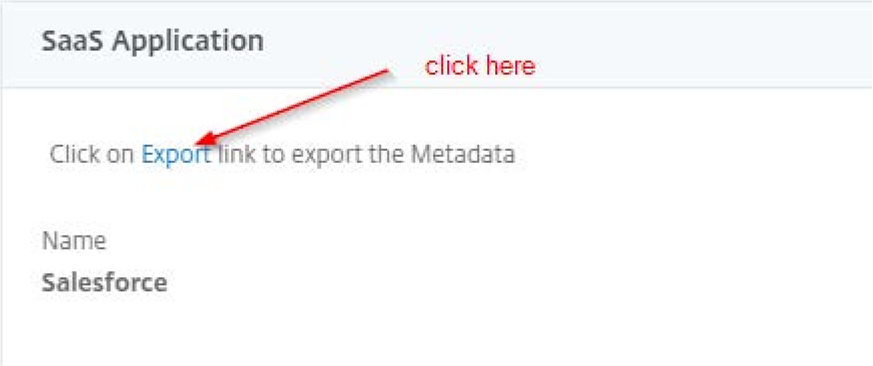
Field Name	Values
URL	https://<customer_domain>.my.salesforce.com/?so=<customer_id >
Service Provider ID	https://<customer_domain>.my.salesforce.com
ACS URL	https://<customer_domain>.my.salesforce.com?so=<customer_id>
Audience	https://<customer_domain>..my.salesforce.com
IdP Certificate Name	IDP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

7. In place of <customer_domain>, enter your company domain name (See **Introduction** to know more about the <customer_domain> values).
8. In place of <customer_id>, enter your customer id (Follow **step 3** to get the customer id)

9. After providing the required values, click **continue.** Click **done**.

Step 2: Export Salesforce IDP metadata from Netscaler

1. Click on **Unified Gateway > Authentication.**
2. Scroll down and click on **Salesforce** template. The **SaaS Application** window **appears.** Click on **Export** link.



SaaS Application

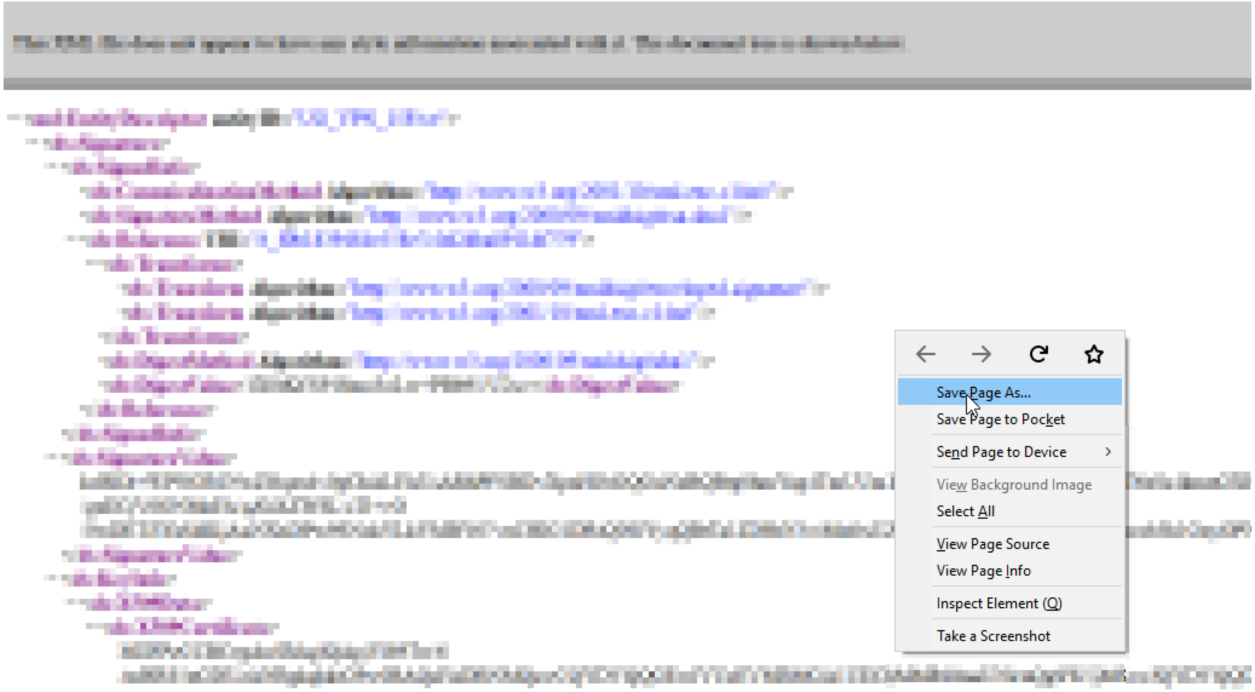
click here

Click on Export link to export the Metadata

Name

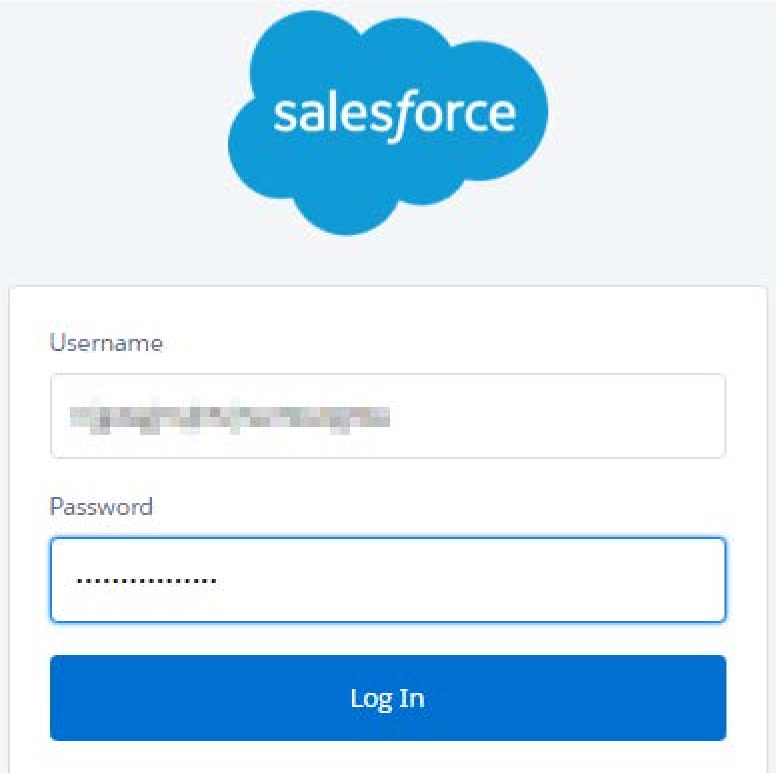
Salesforce

3. **Metadata** will open in a different window. Save the **IDP Metadata** file.



Step 3: Import IDP certificate into salesforce

1. Login to Salesforce as an Admin user.



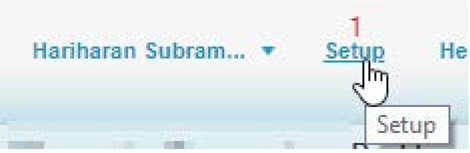
Username

[redacted]

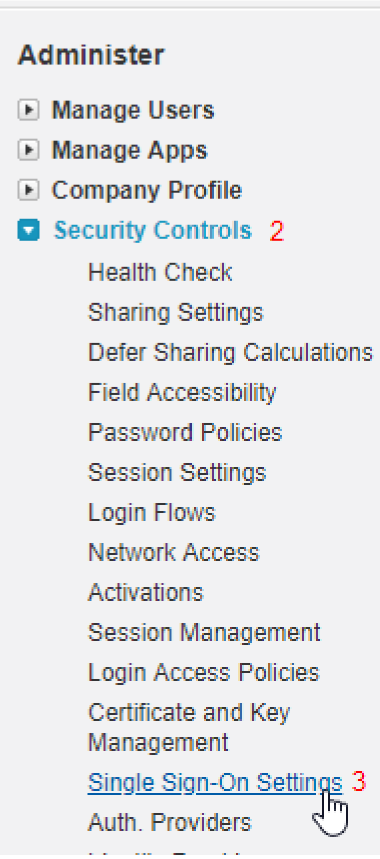
Password

....

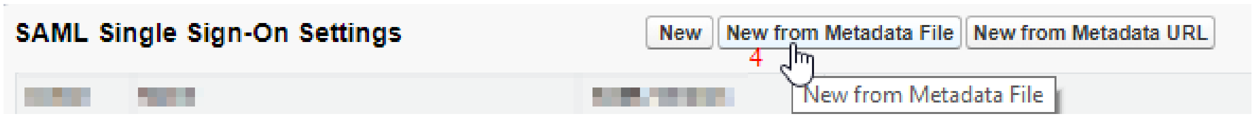
2. Click on **Setup,** on right top corner section.



3. In left side panel, under **Administer** section click on **Security Controls > Single Sign**-O**n Settings**.

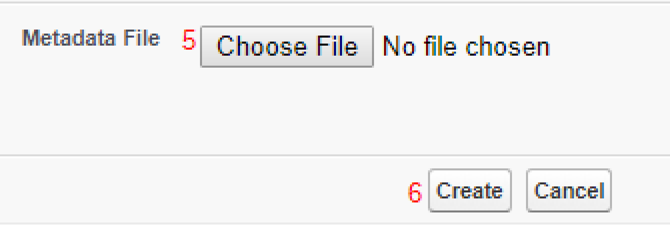


4. Single Sign-On Settings window will appears, under SAML Single Sign On Settings section, click on **New from Metadata File.**

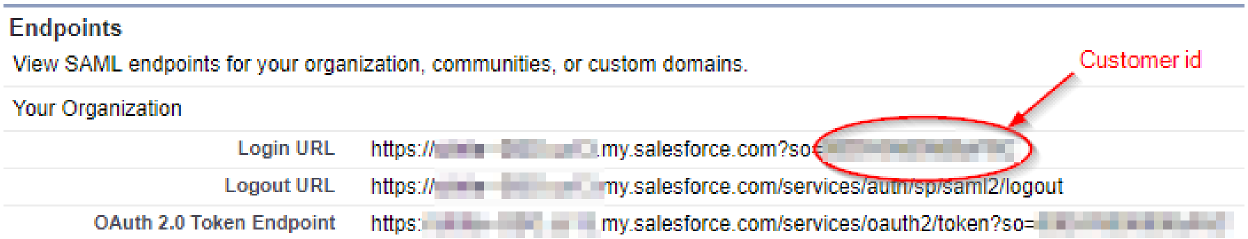


[redacted]

5. SAML Single Sign On Settings window will appears, Upload your metadata file which is exported in step 2 and click on **create**.



6. All URLs will populate in new windows, From **Endpoints** section copy your customer id.



Endpoints

View SAML endpoints for your organization, communities, or custom domains.

Your Organization

Login URL	https://[redacted].my.salesforce.com?so=[redacted]
Logout URL	https://[redacted]my.salesforce.com/services/auth/sp/saml2/logout
OAuth 2.0 Token Endpoint	https:[redacted]my.salesforce.com/services/oauth2/token?so=[redacted]

Customer id