CITRIX®

NetScaler with Unified Gateway

Configuring Podio

Abstract

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

Contents

Disclaimer (Documentation)

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.

Citrix Podio provides cloud based social collaboration tool to build apps and set up workspaces to support users' preferred workflows and help users to effectively manage projects.

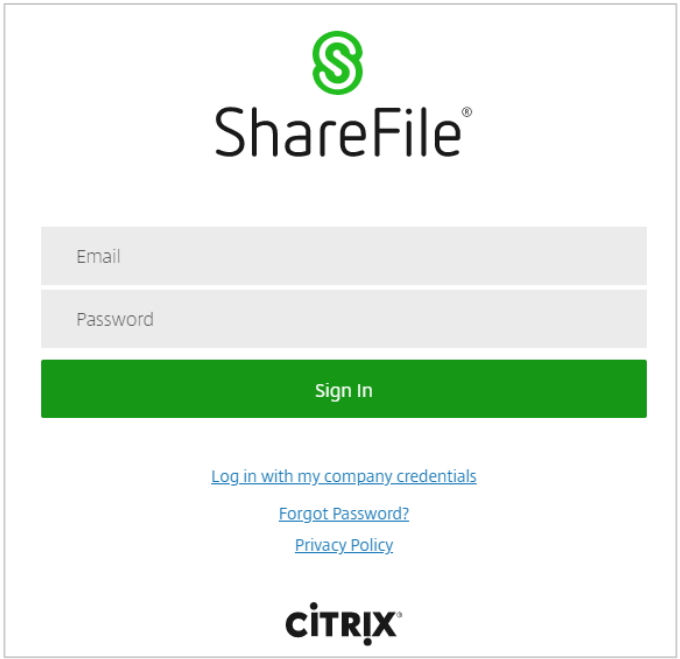
You can connect Podio with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring Podio for Single Sign-On

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

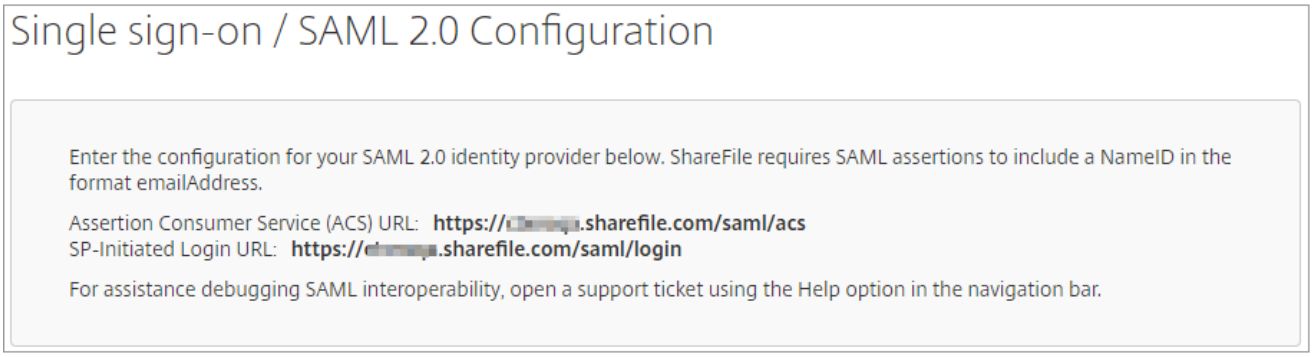
To configure Podio for single sign on through SAML, follow the steps below:

1. In a browser, type https://secure.sharefile.com/Authentication/Login and press Enter.
2. Log on to your Podio account.

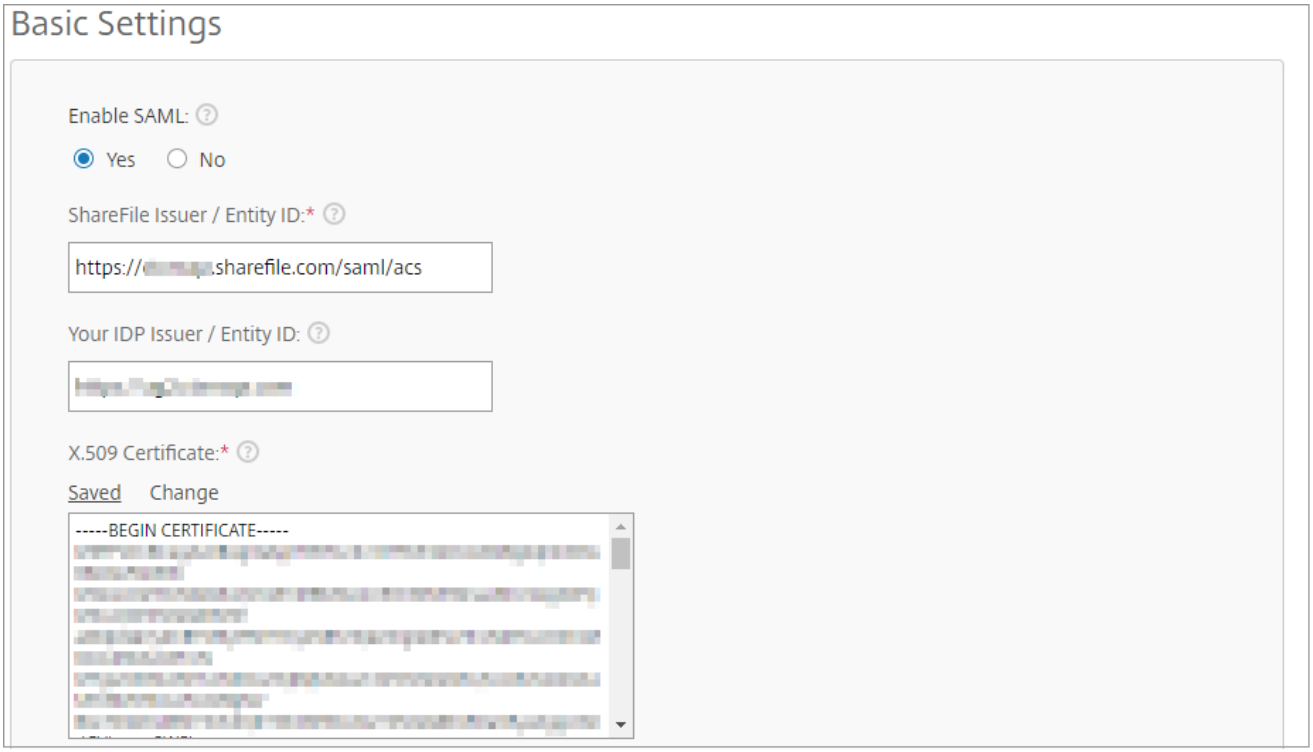


3. Click the company sub domain.
4. Click **Login & Security Policy**.
5. The **Single sign-on/SAML 2.0 Configuration** section displays values for Assertion Consumer Service URL and SP-Initiated Login URL.

   Copy these values to use them while configuring NetScaler for SSO.



6. In the **Basic Settings** section, specify the following information:



   i. **Enable SAML** – click **Yes**.

   ii. **Entity ID** – type the URL in the https://<subdomain>.sharefile.com/saml/acs format.

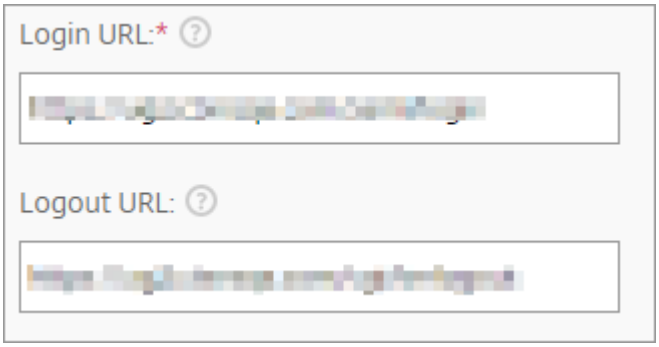
   iii. **X.509 Certificate** – paste the Identity provider certificate.

   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

iv. Type the Login URL and Logout URL.



7. Click on **Save**.

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

Configuring NetScaler for Single Sign-On

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

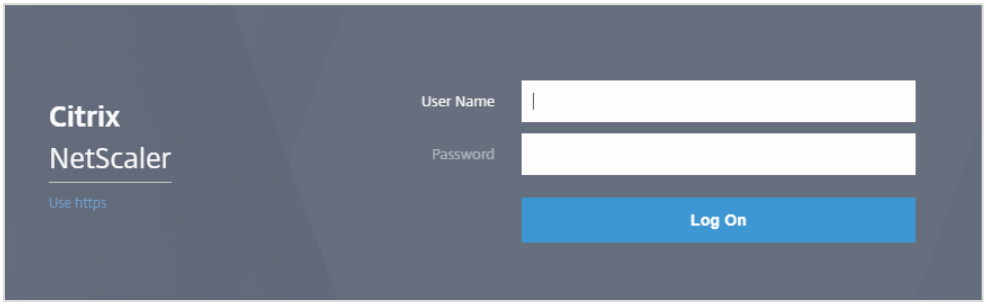
Prerequisites

Ensure that you obtain the SP certificate before you start with the configuration.
To obtain the SP certificate from support team follow the steps below:

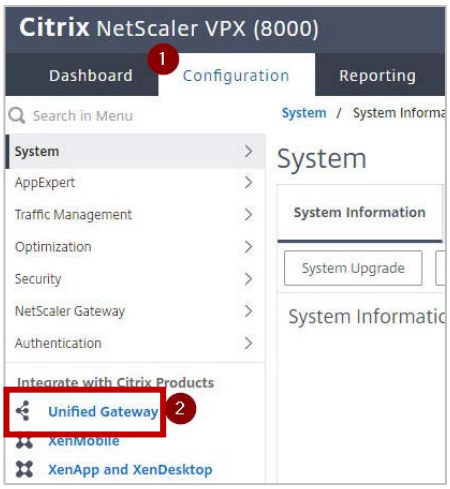
a. Copy certificate to your netscaler using WinScp into /nsconfig/ssl folder.
b. Remotely access your NetScaler instance using PuTTY.
c. Run the following command:
   add ssl certkey slack-sp -cert slack-sp.pem

To configure NetScaler for single sign on through SAML, follow the steps below:

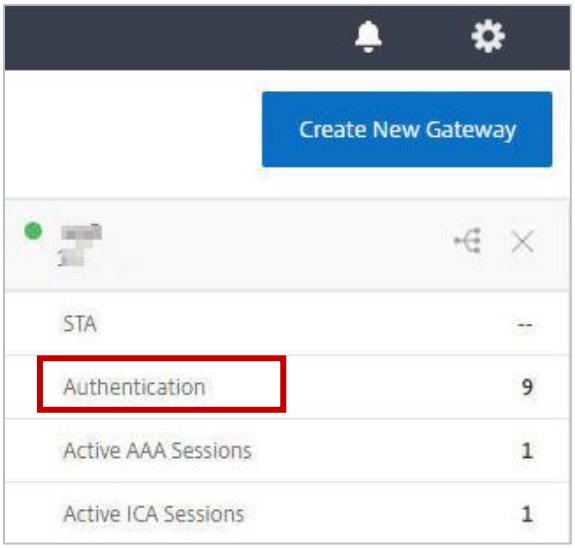
1. Connect to VPN using NetScaler with Unified Gateway.
   Note: Ensure that you obtain SP certificate before you start with the configuration.
2. Log on to NetScaler using your user name and password.



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

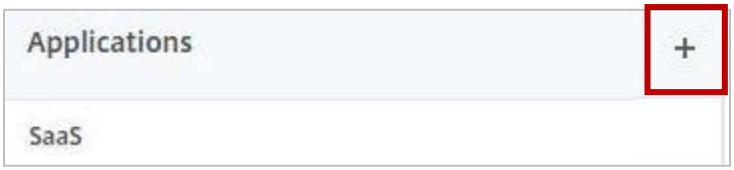


4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.

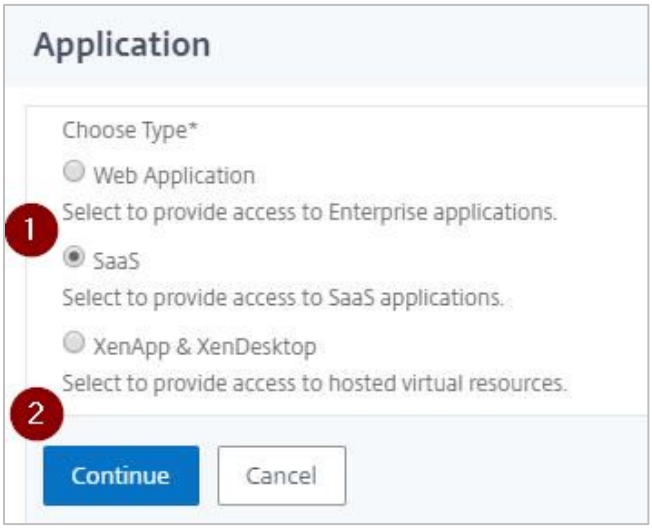


5. Click the edit icon for **Applications** section.

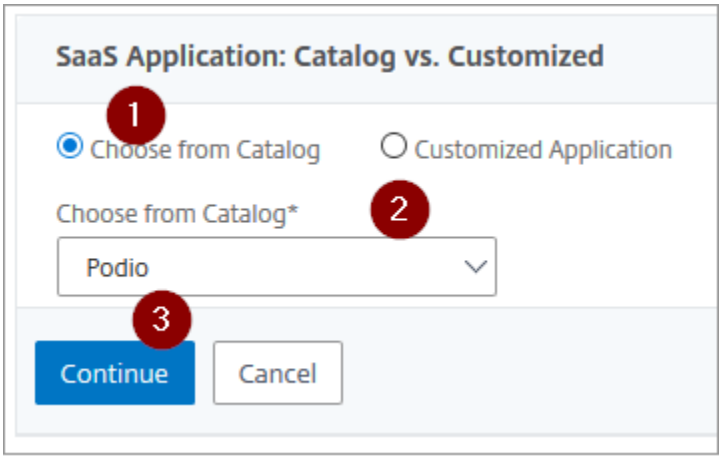
6. For adding a SaaS application, click the plus icon ⊞ that appears in the edit mode.



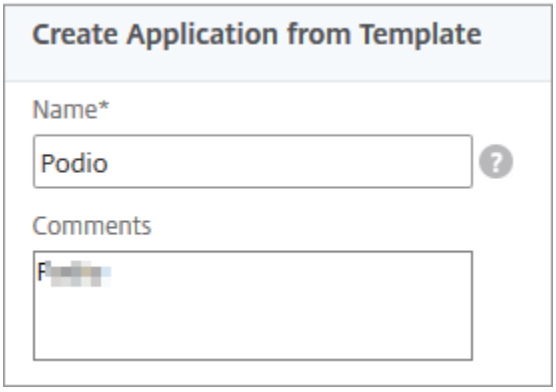
7. Click **SaaS** > **Continue**.



8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **Podio**.



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



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) Podio	Identity Provider (IdP) NetScaler
IDP Issuer / Entity ID	Issuer Name
SP-Initiated Login URL	Service Provider Login URL
ShareFile Issuer / Entity ID	Service Provider ID

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

i. **Service Provider Login URL** - enter the URL that you use to access Podio as https://podio.com/login?provider=sharefile_limited.

ii. **Service Provider Log Out URL** – enter the URL that you use to access Podio in https://<customer>.sharefile.com/saml/acs format.

iii. **Service Provider ID** – type the entity ID.

iv. **SP Certificate Name** – click the appropriate certificate name.
To obtain the SP certificate follow the steps below:

   a. Copy the file that you saved in pem format while configuring Podio for SSO and paste it to NetScaler I.P. at /nsconfig/ssl using WinSCP or similar tool.
   b. Remotely access your NetScaler instance using PuTTY.
   c. Run the following command:
   add ssl certkey Podio-sp -cert Podio-sp.pem

v. **IDP Certificate Name** – click the appropriate certificate name.
Refer to the appropriate public key certificate provided by NetScaler which you referred while configuring Podio.

vi. **Issuer Name** – type the issuer ID that you entered for Identity Provider Issuer while configuring Podio.

13. Click **Continue.**

14. Click **Done**.
    The Podio logo appears.

15. Click **Done**.

You have completed the NetScaler configuration for Podio.

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 **Podio**.
   Your Sharefile profile is displayed.
   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 vanity URL/signin.
2. You are redirected to NetScaler appliance's log in page.
3. Log on to NetScaler appliance using your enterprise credentials.

   Your Podio profile is displayed which indicates that you have successfully logged on to Podio.

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