CITRIX

NetScaler with Unified Gateway

Configuring Wepow

Abstract

Configuring Wepow 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.

Overview

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

Wepow provides video and communications platform to improve recruiter productivity. Wepow helps to connect recruiters, job candidates, and employers through the mobile and video interviewing solutions.

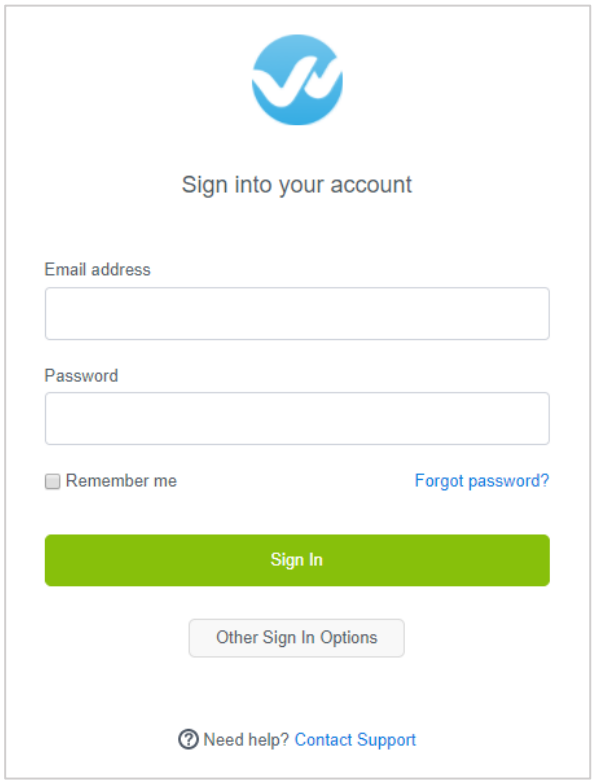
You can connect Wepow with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring Wepow for Single Sign-On

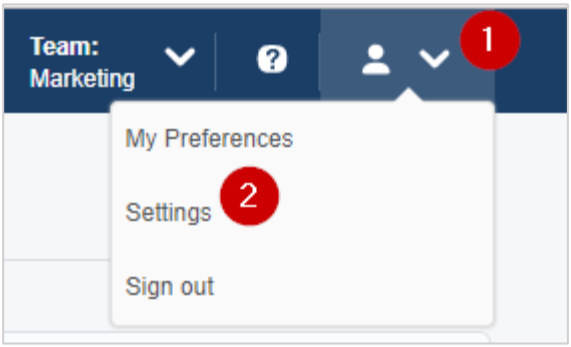
Configuring Wepow for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Wepow using their enterprise credentials.

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

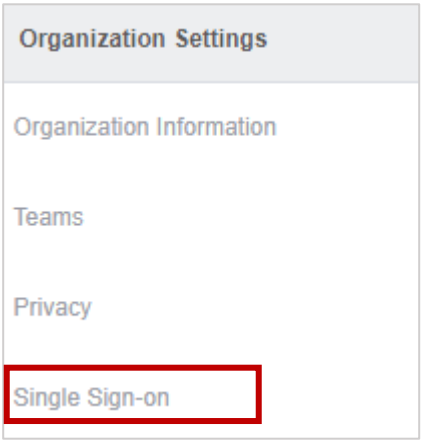
1. In a browser, type https://<your-organization>.wepowapp.com/ and press enter.
   Note: For example, if the URL you use to access pager duty is https://myserver.wepowapp.com, then you must replace <your-organization> with myserver.
2. Log on to your Wepow account as an administrator.



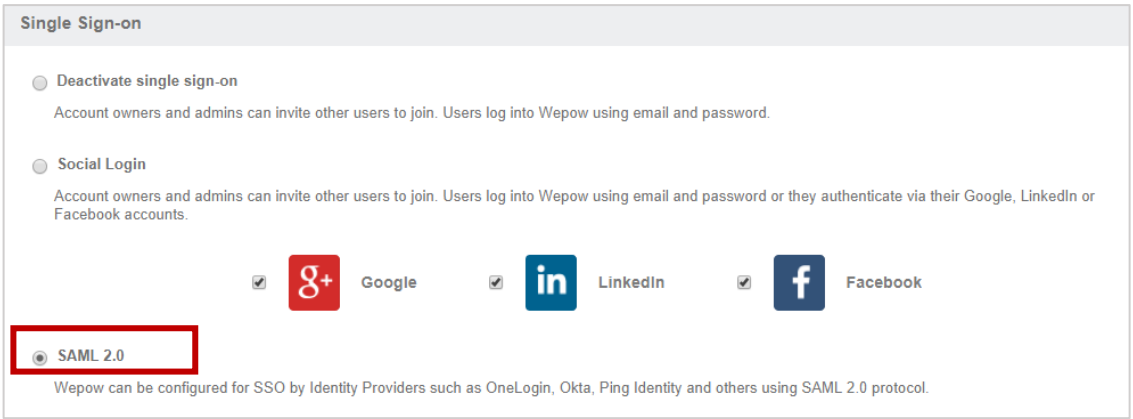
3. On the home page, in the upper right corner, click the profile icon  and click **Settings**.



4. On the settings page, scroll down to the Organization Settings section in the lower left corner click **Single Sign-on**.



5. On the Single-Sign-on page, click **SAML 2.0**.



6. In the **X.509 Certificate** box, paste the Identity provider certificate.

To obtain your IdP certificate, follow the steps below:

i. Remotely access your NetScaler instance using PuTTY.

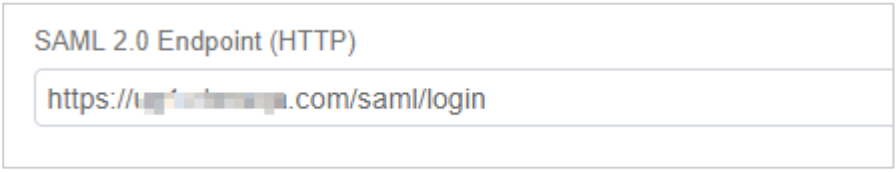
ii. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.

iii. Type cat <certificate-name> and press Enter.

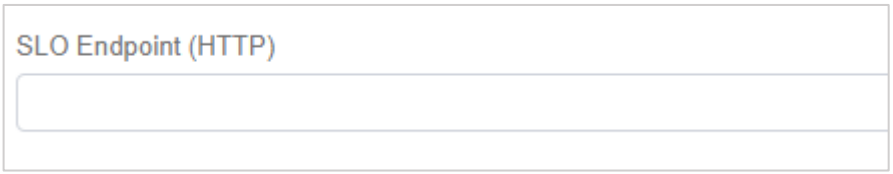
iv. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----

v. Paste the text in a text editor and save the file in an appropriate format such as <your organization name>.pem

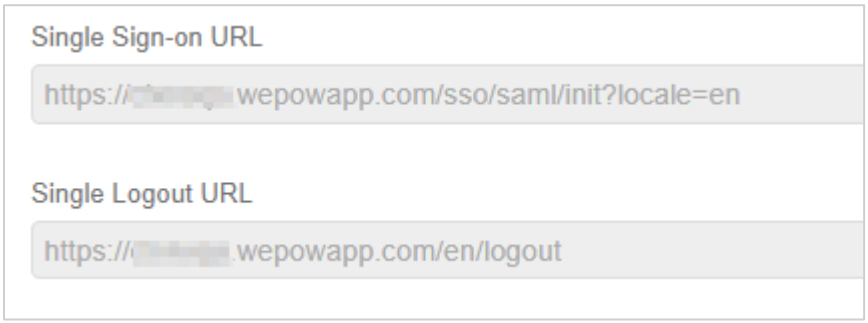
7. In the **SAML 2.0 Endpoint (HTTP)** box, type the endpoint URL in https://<customerFQDN>/saml/login format.



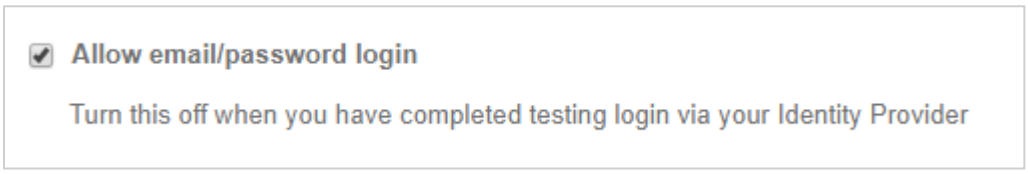
8. In the **SLO Endpoint (HTTP)** box, type the URL in https://<customerFQDN>/cgi/tmlogout format.



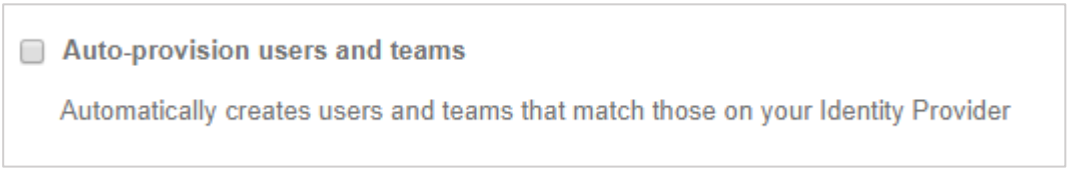
9. The Single Sign-on URL box displays the SSO URL and the Single Logout URL displays the URL to which the user will be redirected after logging out.



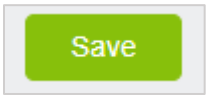
10. Select the **Allow email/password login** check box. Clear the check box after completing testing of logging on via Identity Provider if you do not want users to log on using user name and password.



11. Select the **Auto-provision users and teams** check box to auto-provision users. After you enable auto-provisioning, if a user for whom a user account is not created uses SSO to log on to Wepow, the associated user account is created automatically.



12. Click **Save**.



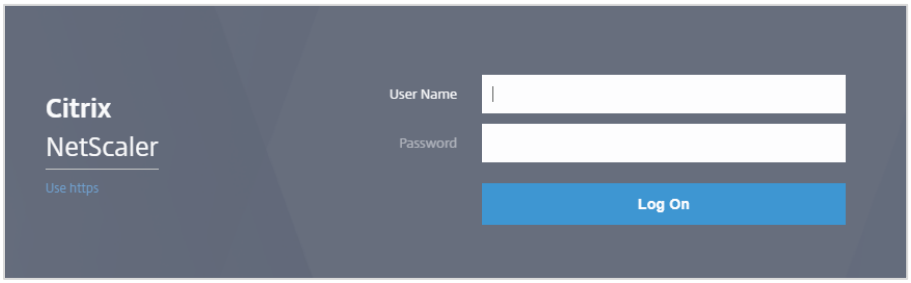
You have completed the required configuration for the service provider which is in this case –Wepow.

Configuring NetScaler for Single Sign-On

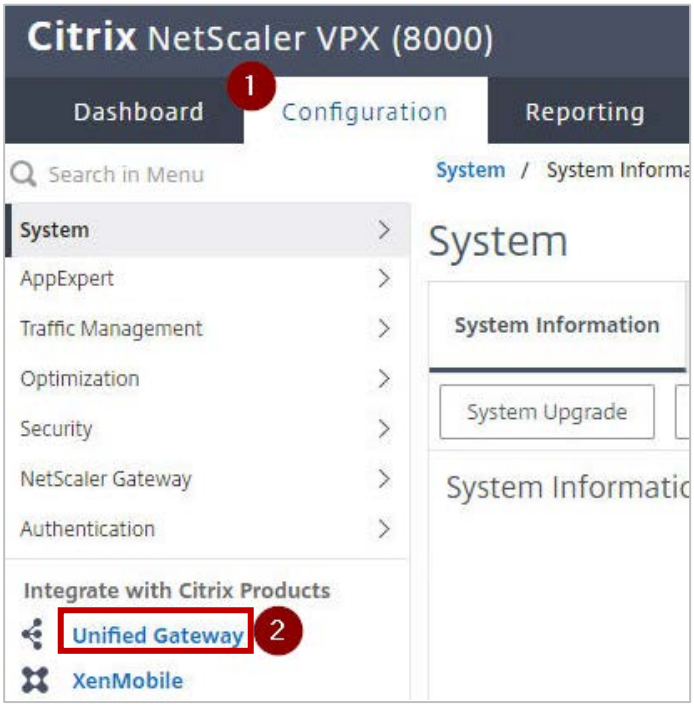
For configuring NetScaler for Wepow, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

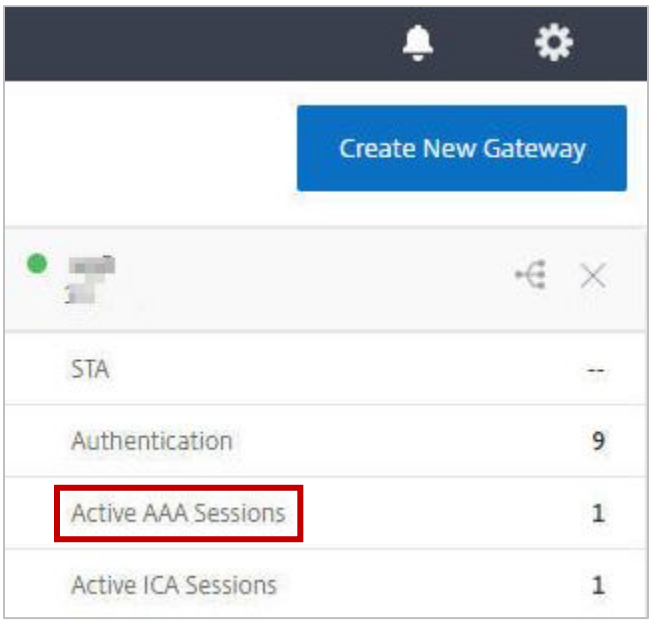
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



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

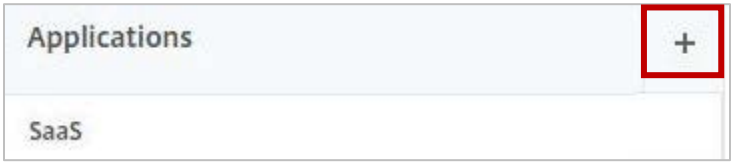


4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.

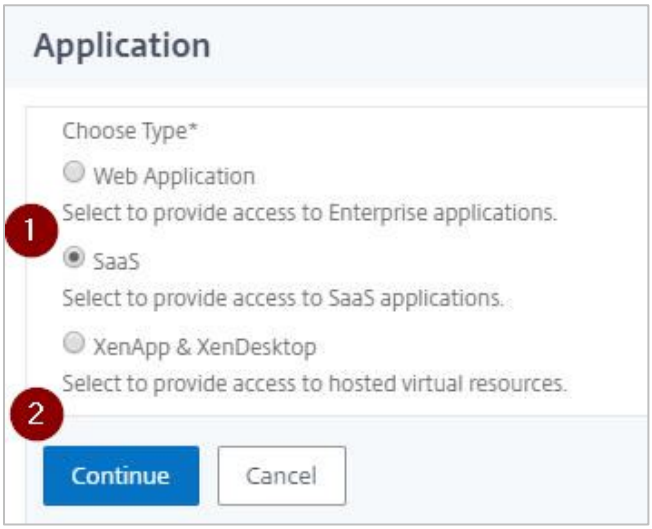


5. Click the edit icon for **Applications** section.

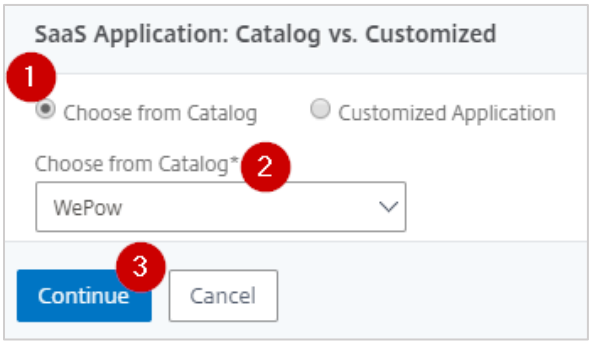
6. For adding a SaaS application, click the plus icon ⊞ that appears in the edit mode.



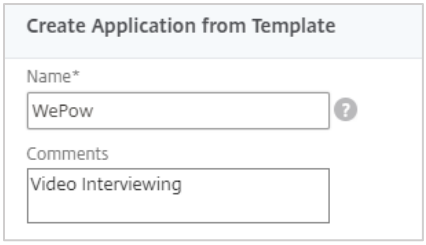
7. Click **SaaS** > **Continue**.



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



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



Note:

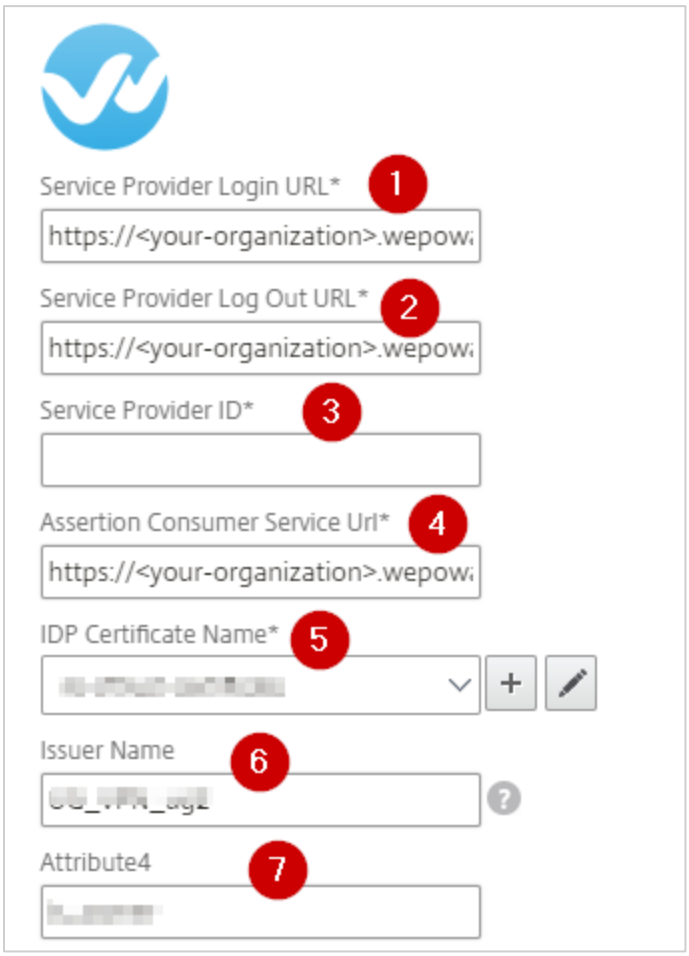
An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

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) Wepow	Identity Provider (IdP) NetScaler
Single Logout URL	Service Provider Log Out URL*

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



i. **Service Provider Login URL** - type the URL in https://<your-organization>.wepowapp.com format.
Note: For example, if the organization's URL is https://myserver.wepowapp.com, you must replace <your-organization> with myserver.

ii. **Service Provider Logout URL** - type the URL in https://<your-organization>.wepowapp.com/en/logoutformat.
Note: For example, if the organization's URL is https://myserver.wepowapp.com, you must replace <your-organization> with myserver.

iii. **Service Provider ID** – type https://wepowapp.com.

iv. **Assertion Consumer Service Url*** - type the URL in https://<your-organization>.wepowapp.com/sso/saml/consume format.
Note: For example, if the organization's URL is https://myserver.wepowapp.com, you must replace <your-organization> with myserver.

v. **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.

vi. **Issuer Name** – type a unique issuer ID. For example: MyServer_NS_Wepow

13. Click **Continue.**

14. Click **Done**.

    The Wepow logo appears.

15. Click **Done**.

    You have completed the NetScaler configuration for Wepow.

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 **Wepow**.
   Your Wepow 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 Wepow.
2. Click **Other Sign In Options**.
3. In the Single Sign-on area, click **Sign in with your identity provider**.
4. Type your organizational user name.
   You are redirected to NetScaler appliance's log in page.
5. Log on to NetScaler appliance using your enterprise credentials.

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

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