CITRIX

NetScaler with Unified Gateway

Configuring Aha

Abstract

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

Contents

ABSTRACT....0
CONTENTS....1
DISCLAIMER (DOCUMENTATION)....2
PREFACE....3
OVERVIEW....4
CONFIGURING AHA FOR SINGLE SIGN-ON....4
CONFIGURING NETSCALER FOR SINGLE SIGN-ON....8
TESTING THE CONFIGURATION....13

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.

Aha provides web-based product management tools and expert services.

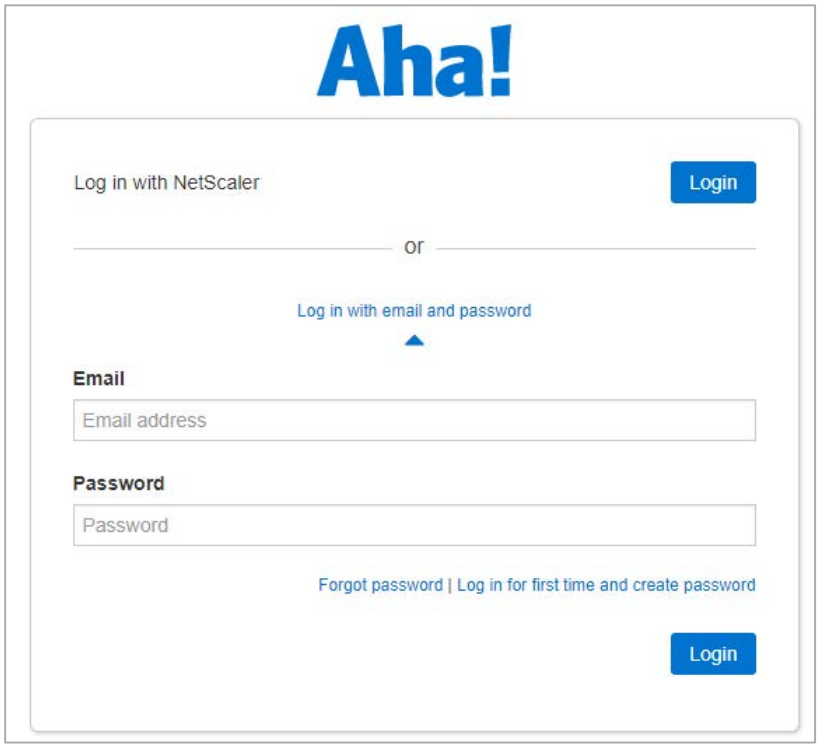
You can connect Aha with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring Aha for Single Sign-On

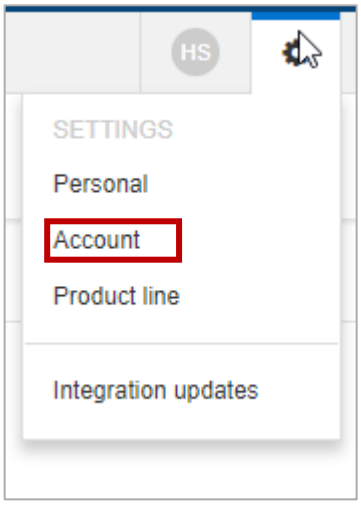
Configuring Aha for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Aha using their enterprise credentials.

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

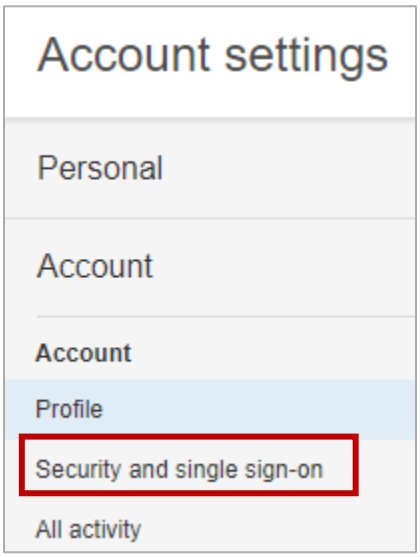
1. In a browser, type https://ctxnsqa.aha.io and press Enter.
2. Click **Log in with email and password**.
3. Log on to your Aha account.



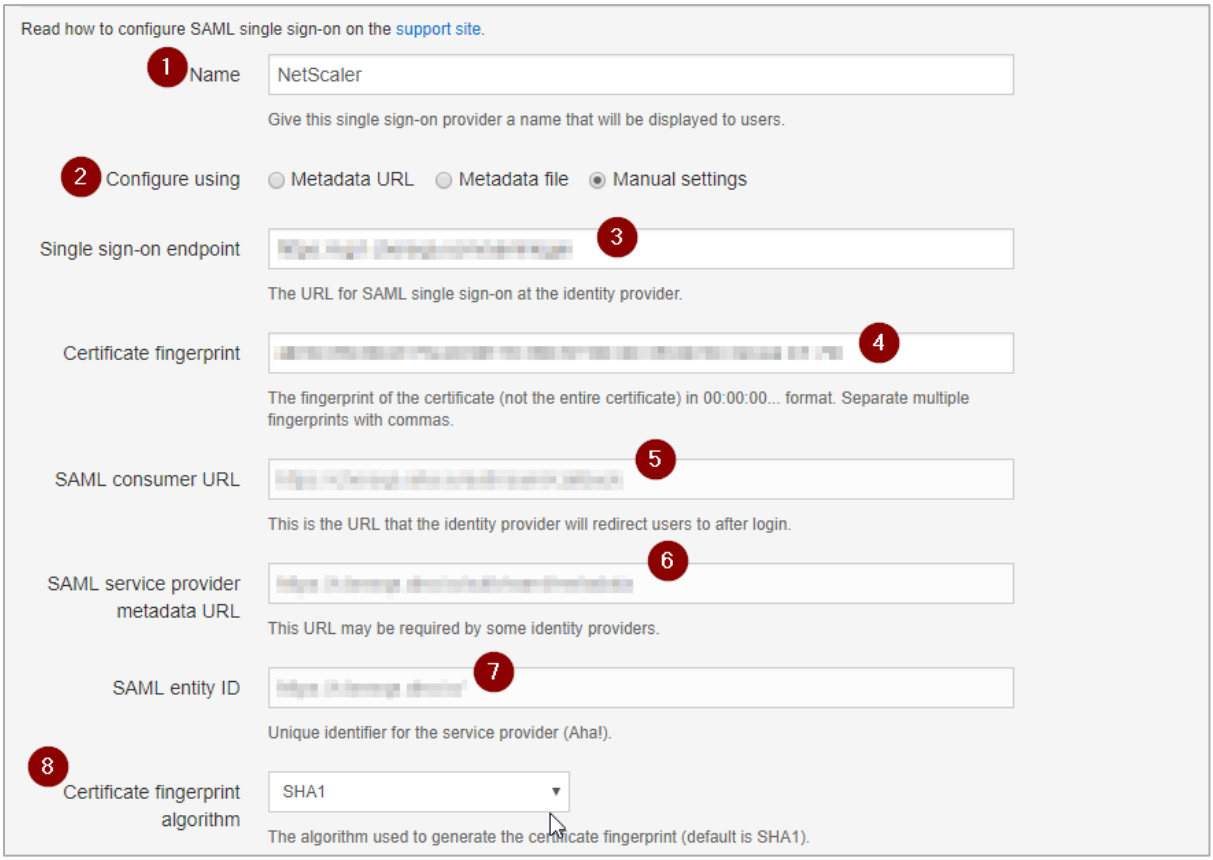
4. On the **Home** page, at the upper-right corner, click the SETTINGS icon  and click **Account**.



5. In the left pane, under Account, click **Security and single sign-on**.



6. In the right pane, in the Single sign-on section, specify the following information:



i. **Name** – enter the IdP name.
ii. **Configure using** – click **Manual settings**.
iii. **Single sign-on endpoint** - enter the NetScaler URL followed by /saml/ login. For example: https://<customerFQDN>.com/saml/ login
iv. **Certificate fingerprint** – paste the certificate fingerprint.
To add fingerprint of the NetScaler IDP SAML Signing certificate, follow the steps below:
    a. Remotely access your NetScaler instance using PuTTY.
    b. Log on to Shell by typing Shell.
    c. Navigate to /nsconfig/ssl folder (cd /nsconfig/ssl) and press Enter.
    d. Type openssl x509 -in certificatename shell.pem -fingerprint –noout and press Enter.
    e. Copy the fingerprint that has been generated and paste that in the Certificate fingerprint box.
v. **SAML consumer URL** – displays the Assertion Consumer Service URL.
Note: Copy this value to use it while configuring NetScaler for SSO for the Assertion Consumer Service URL field.
vi. **SAML service provider metadata URL –** displays metadata URL. Access this URL to download an XML file that contains data such as endpoints, supported bindings,

identifier, and public keys required for interaction with SAML-enabled identity or service provider.

i. **SAML entity ID** – displays the unique identifier that you can use for the SP Entity ID field while configuring NetScaler for SSO.

ii. **Certificate fingerprint algorithm** - click the fingerprint algorithm from which you generated the IdP signing certificate fingerprint, in this case SHA1.

7. Click **Save Configuration**.

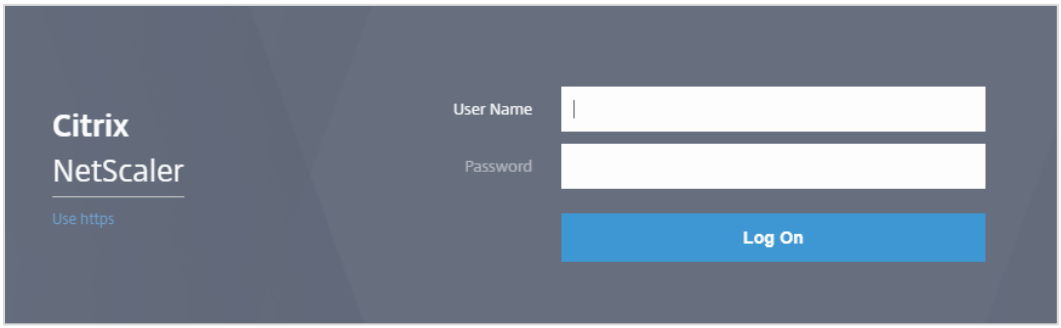
.

Configuring NetScaler for Single Sign-On

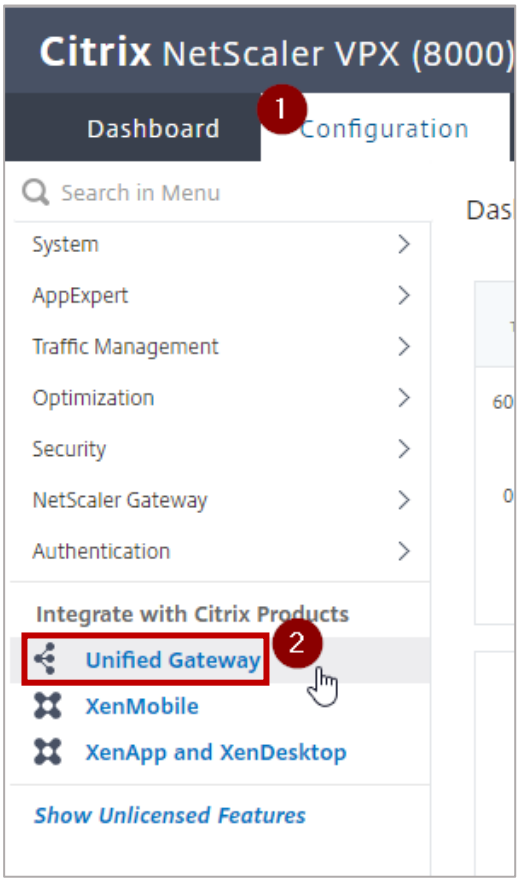
For configuring NetScaler for Aha, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

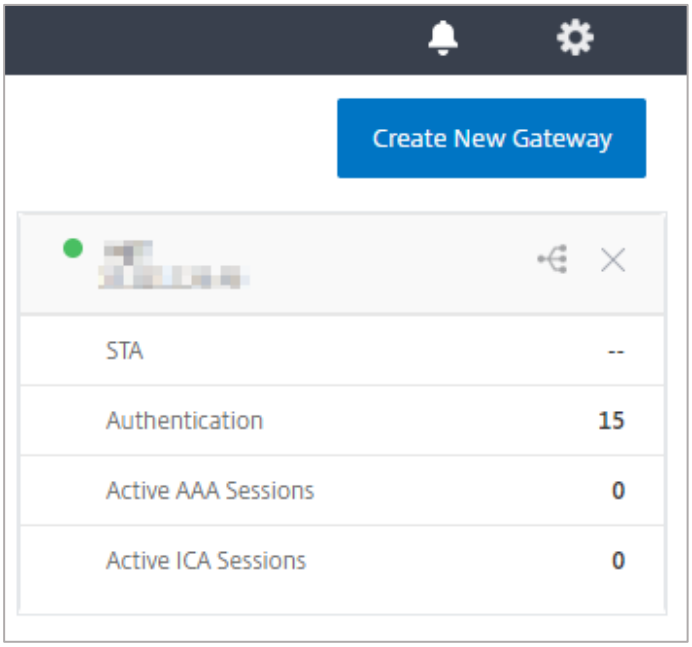
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



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



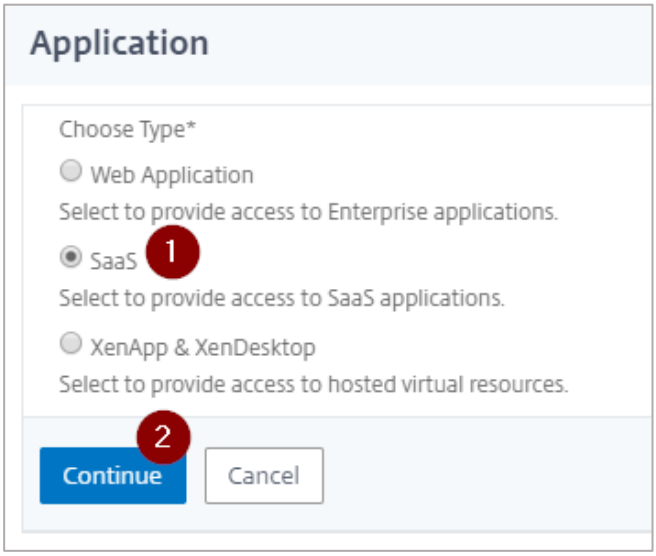
4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



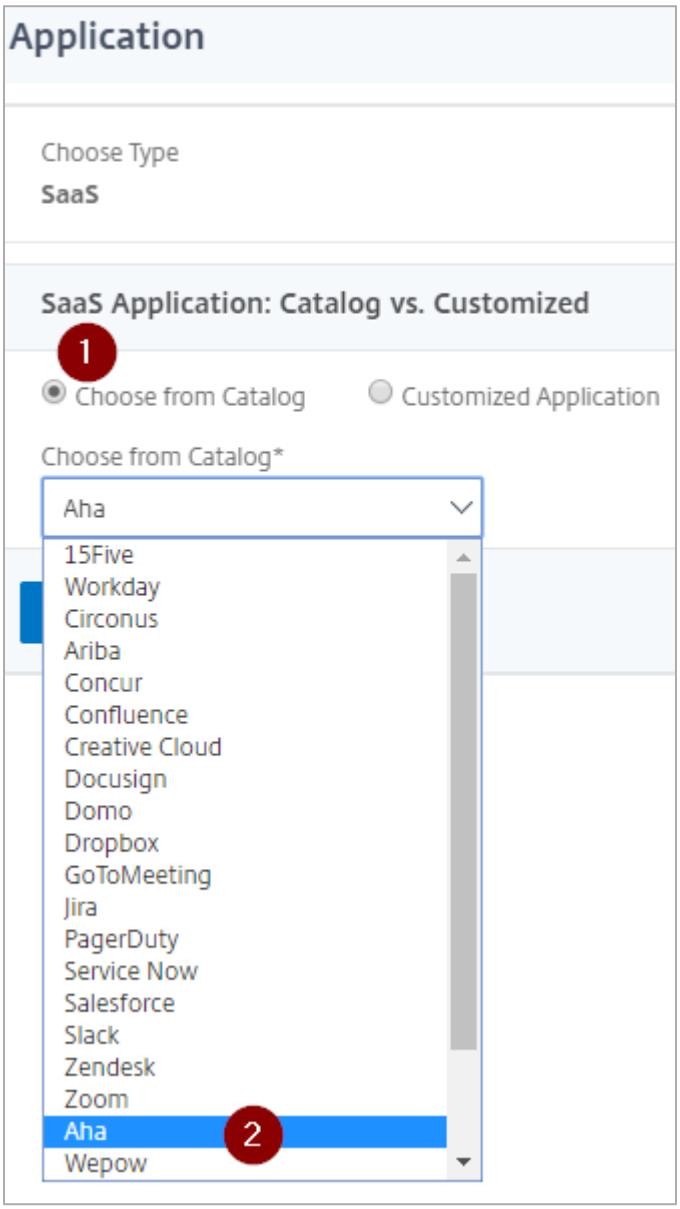
5. Click the edit icon for **Applications** section.

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

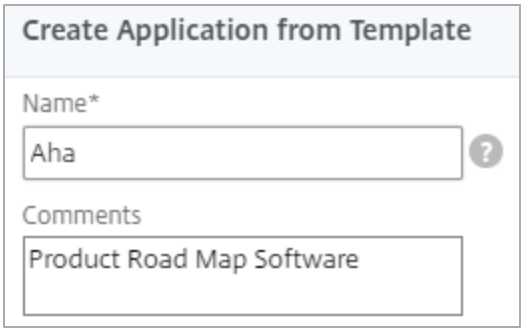
7. Click **SaaS** > **Continue**.



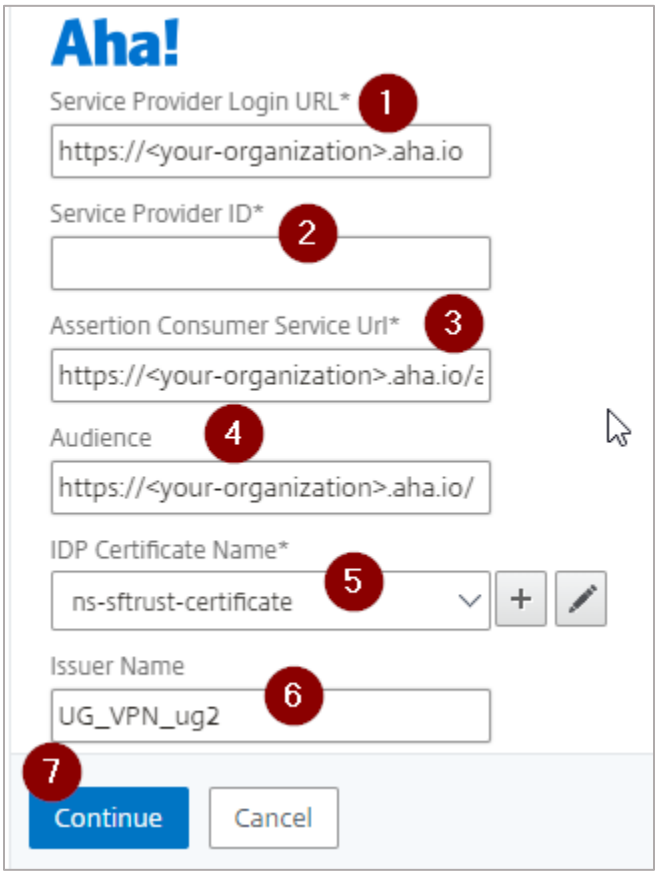
8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **Aha**.



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



12. In the subsequent section, specify the following information:



i. **Service Provider Login URL** - type the Aha URL in https://<your-organization>.aha.io format.
ii. **Service Provider ID** - paste the SP Entity ID that you copied from the **SAML entity ID** field on the **SAML Single sign-on** page while configuring SAML for Aha.
iii. **Assertion Consumer Service Url*** - paste the URL displayed by the **SAML consumer URL** field while configuring Aha.
iv. **Audience** - paste the URL displayed by the SAML entity ID field while configuring Aha.
v. **IDP Certificate Name** - select an appropriate certificate that will be used for signing SAML requests and responses.
vi. **Issuer Name** - type a unique issuer name.

13. Click **Continue.**
14. Click **Done**.
    The Aha logo appears.

    You have completed the NetScaler configuration for Aha.

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

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