CITRIX

NetScaler with Unified Gateway

Configuring GitHub Enterprise

Abstract

Configuring GitHub Enterprise 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.

GitHub Enterprise provides version control and source code management functionalities with access control and collaboration features. Using GitHub Enterprise, you can use collaboration features locally, on your server. Additionally, it supports LDAP and CAS that enables you to use your existing corporate authentication systems.

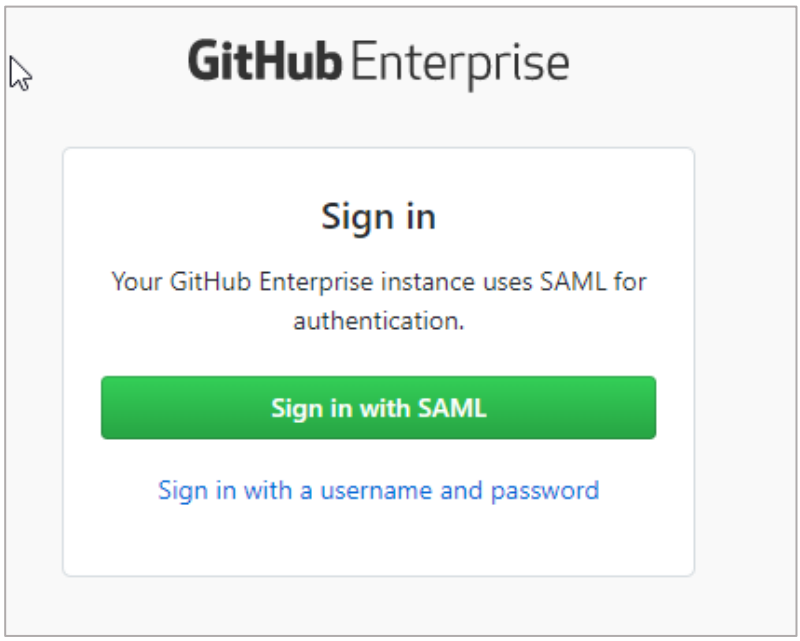
You can connect GitHub Enterprise with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring GitHub Enterprise for Single Sign-On

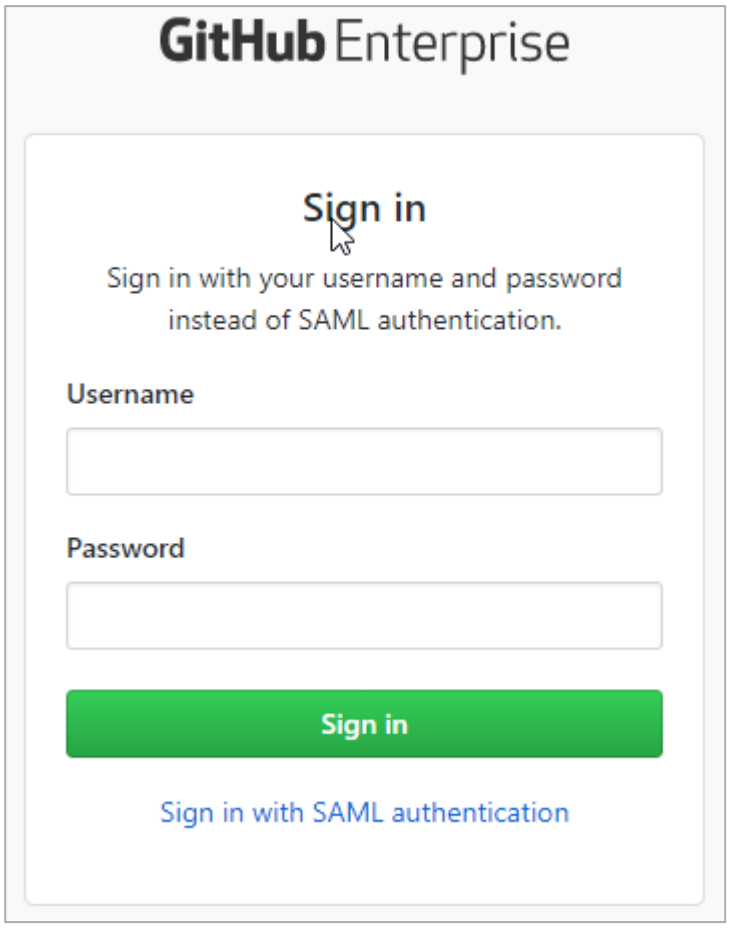
Configuring GitHub Enterprise for SSO enables administrators to manage their users using NetScaler. Users can securely log on to GitHub using their enterprise credentials.

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

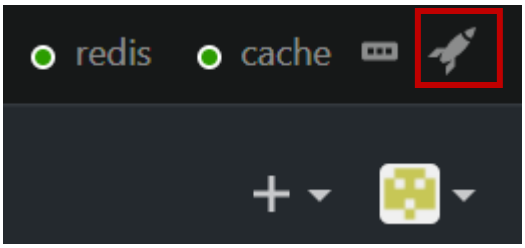
1. Access your GitHub Enterprise site for example: https://mygithubenterprise.com.
2. To log on to your GitHub Enterprise account as an administrator, click **Sign in with a username and password** link.



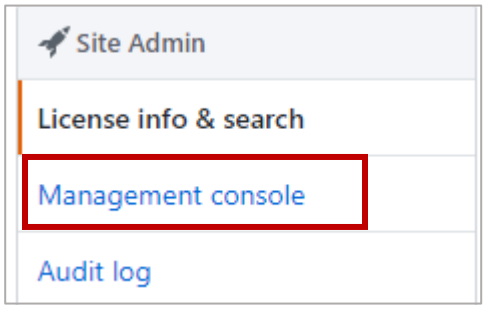
3. Type user name and password and click **Sign in**.



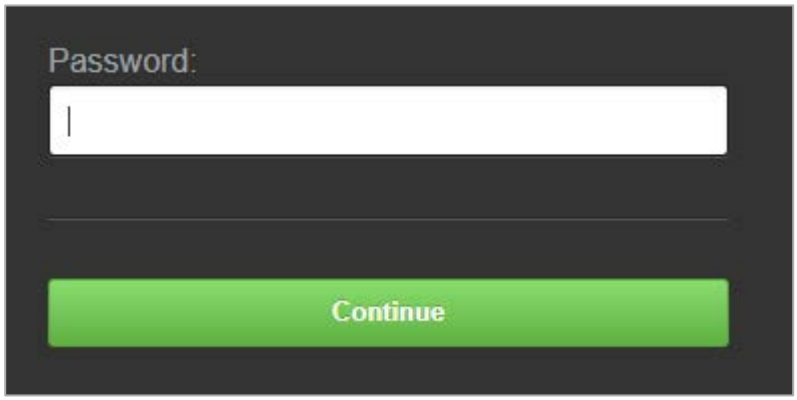
4. On the home page, in the upper right corner, click the **Site Admin** icon  .



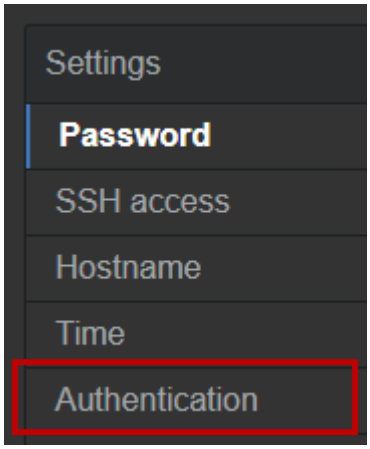
5. Click **Management console**.



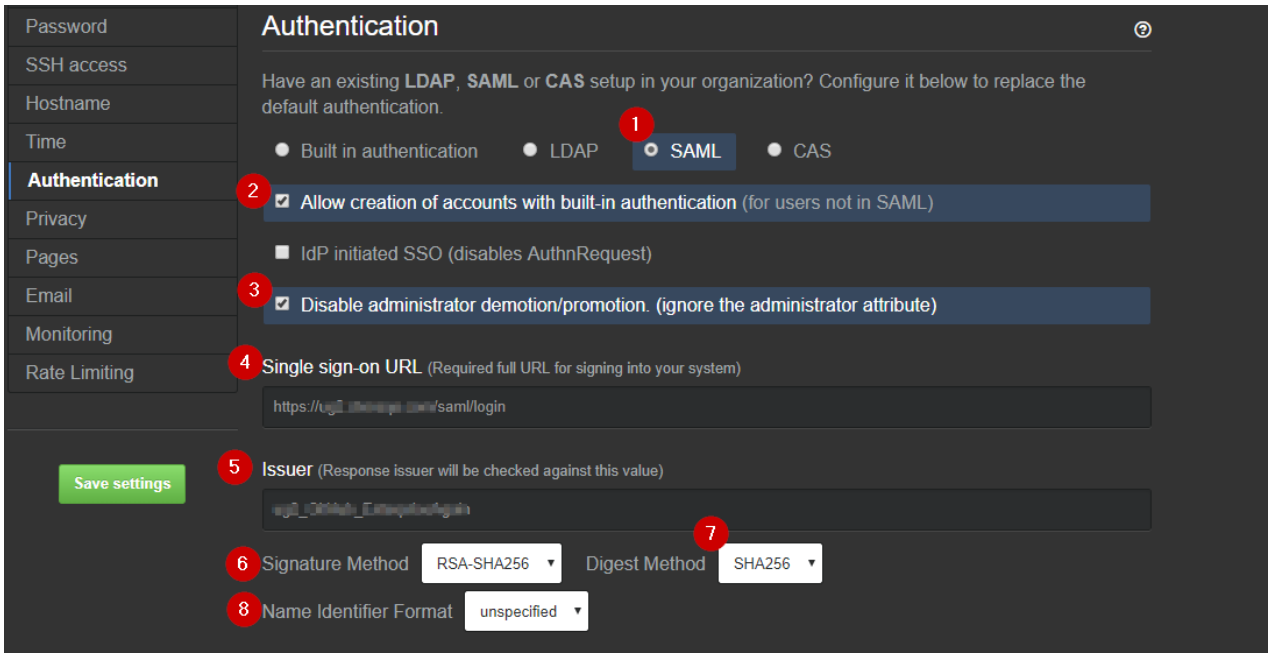
6. Type the password to access Management console.



7. On the **Settings** page, click **Authentication**.



8. In the **Authentication** section, specify the following information:



i. Click the autentication type **SAML**.

ii. To allow authentication of users who do not have access to your identity provider that uses SAML, select the **Allow creation of accounts with built-in authentication (for users not in SAML)** check box.

iii. If you do not want to demote or promote users based on attributes sent in SAML, select the **Disable administrator demotion/promotion. (ignore the administrator attribute)** check box.

iv. **Single sign-on URL** - type the IdP URL followed by /saml/login. For example: https://<NetSaclerFQDN>/saml/login

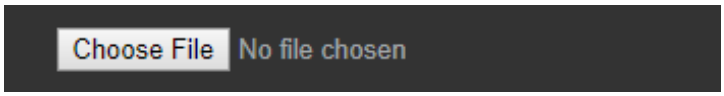
v. **Issuer** - type a unique issuer name.

vi. **Signature Method** - click **RSA-SHA256**.

vii. **Digest Method** - click **SHA256**.

viii. **Name Identifier Format** - click **unspecified**.

ix. In the **Verification certificate** area, to upload the IDP signing certificate, click **Choose File**.



Browse to the folder where you saved the IdP provided certificate and upload it. Based on the certificate that you upload, the values for the fields Domain, Alternate names, Issuer, Valid From, and Expires After are automatically populated.

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.

Note: Replace <certificate name> with your IdP signing certificate name.

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 IDP signing Certificate>.pem.

9. Click **Save Settings**.

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

Configuring NetScaler for Single Sign-On

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

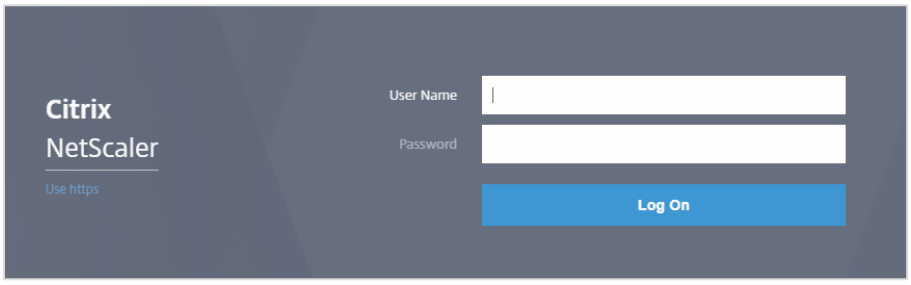
Prerequisites

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

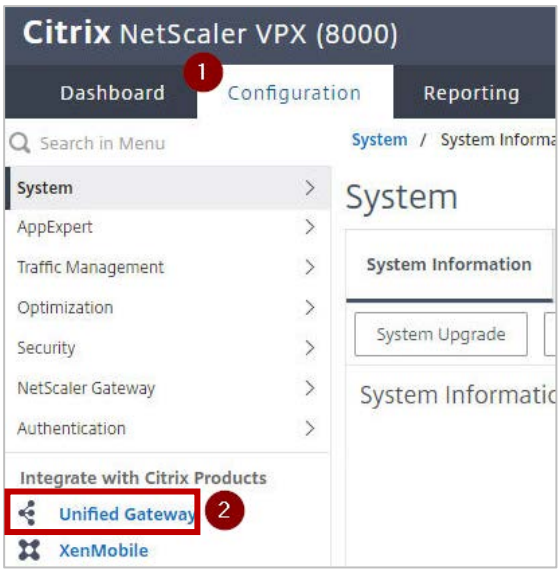
a. Connect to VPN using NetScaler with Unified Gateway.
b. Download the XML file using the URL displayed by the SAML Metadata URL field while configuring GitHub Enterprise.
c. Access the metadata URL <Your-github-EnterpriseFQDN>/saml/metadata
d. Open the file in notepad and copy the text inside the X509Certificate tag.
e. Open a base64 decoder for e.g. https://base64decode.org, paste the copied content in the decoder and click Decode.
f. Copy the decoded text.
g. Create a new notepad file, add the text that you have copied between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.
h. Save the file using an appropriate name in PEM format for example: GitHubenterprise_sp.pem.
i. Copy the file to the NetScaler I.P. at /nsconfig/ssl using WinSCP or other similar tool.
j. Remotely access your NetScaler instance using PuTTY.
k. Run the following command: add ssl certkey GitHub-enterprise-sp -cert GitHubEnterprise_sp.pem

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

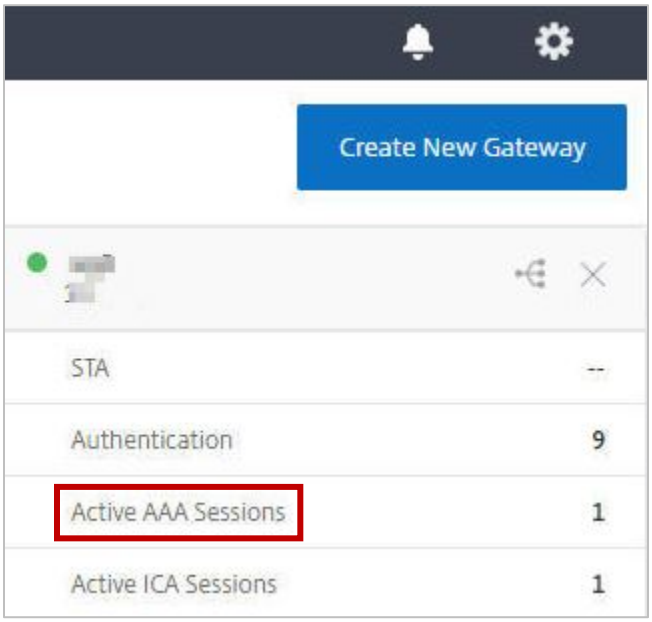
1. Connect to VPN using NetScaler with Unified Gateway.
   Note: Ensure that you obtain SP certificate before you start with the configuration. For more information refer Prerequisites.
2. Log on to NetScaler using your user name and password.



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



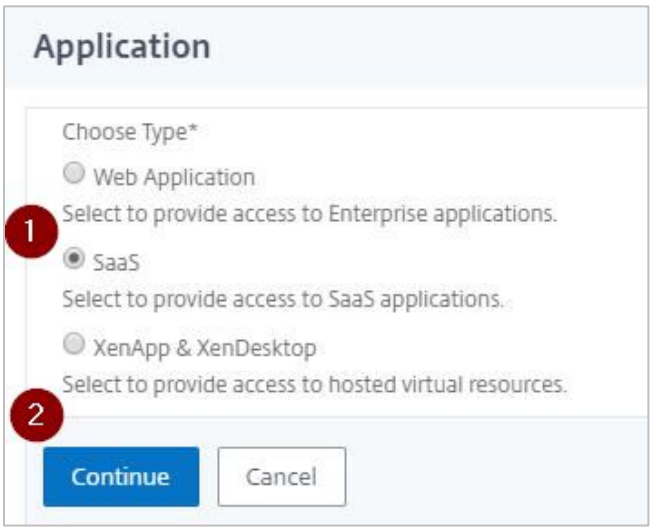
4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



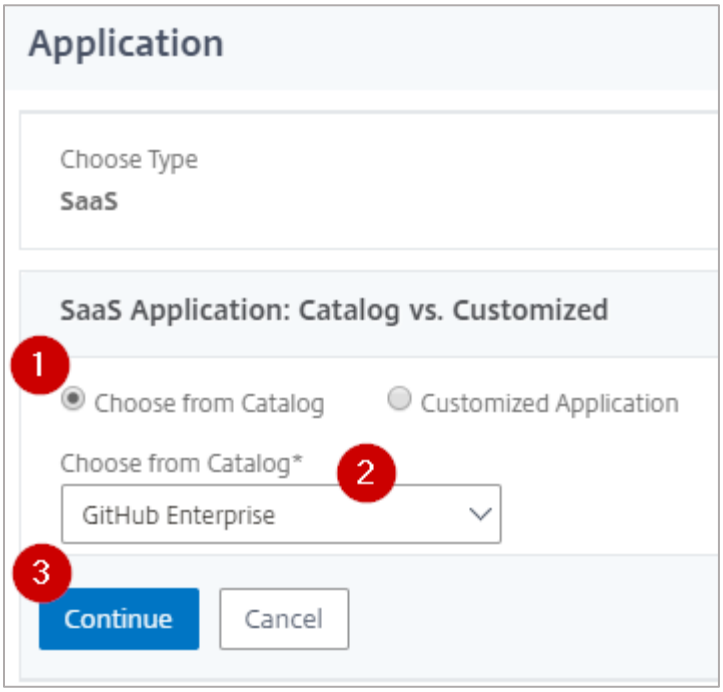
5. Click the edit icon for **Applications** section.

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

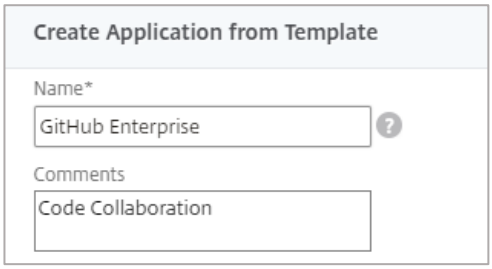
7. Click **SaaS** > **Continue**.



8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **GitHub Enterprise**. > **Continue**.



10. In the **Create Application from Template** section, type the name of your SaaS application, in this case GitHub Enterprise, 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) GitHub Enterprise	Identity Provider (IdP) NetScaler
Service Provider Issuer	Service Provider ID
Identity Provider Issuer	Issuer Name
SAML Endpoint URL	Assertion Consumer Service Url

11. In the subsequent area, specify the following information:

i. **Service Provider Login URL** – type your GitHubEnterpriseFQDN.
ii. **Service Provider ID** - enter the URL that you use for accessing GitHub Enterprise.

iii. **Assertion Consumer Service Url*** - type GitHubEnterpriseFQDN/saml/consume
iv. **SP Certificate Name** – click the appropriate certificate name. To obtain this value, refer to the metadata xml file that you downloaded while configuring GitHub Enterprise for SAML. For more information about how to obtain SP certificate, refer Prerequisites.
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 the unique name that you entered in the **Issuer** field while configuring GitHub Enterprise. For example: MyServer_GitHub_Enterprise

12. Click **Continue.**
13. Click **Done**.

    The GitHub logo appears.

14. Click **Done**.

    You have completed the NetScaler configuration for GitHub Enterprise.

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 **GitHub Enterprise**.
   You must be logged on to the GitHub Enterprise.
   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 your GithubEnterpriseFQDN.
2. Click **Sign in with SAML**.

   You are redirected to NetScaler appliance's log in page.
3. Log on to NetScaler appliance using your enterprise credentials.

   You are successfully logged on to GitHub Enterprise.

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