CITRIX®

NetScaler with Unified Gateway

Configuring GoToMeeting

Abstract

Configuring GoToMeeting 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.

GoToMeeting is a web conferencing software that provides online meeting, desktop sharing, and video conferencing facilities to help users to collaborate online with other computer users like colleagues and customers in real time.

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

Configuring GoToMeeting for Single Sign-On

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

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

1. In a browser, type https://organization.logmeininc.com and press Enter.

2. Log on to your GoToMeeting account.
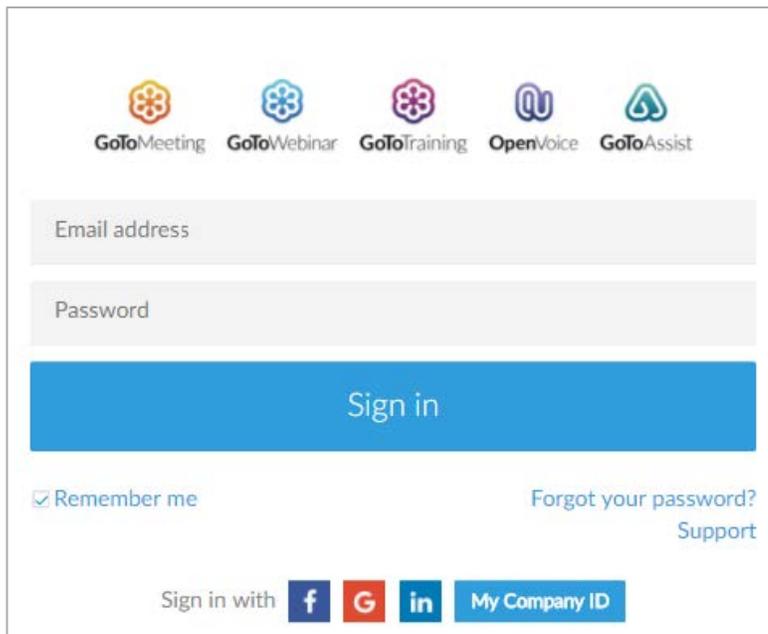
3. On the home page, in the **Email** tab you can add a domain.

4. In the **Identity provider** tab, specify the following details:

i. **How would you like to configure your SAML IDP?** – click **Manual**.

Note: You can click the appropriate option to configure automatically using a metadata URL, by uploading a SAML metadata file, or manually with sign-in and sign-out URLs, an identity provider ID and by uploading verification certificate.

ii. **Sign-in page url** - type the IdP URL followed by /saml/login. For example: https://<customerFQDN>/saml/login

iii. **Sign-in binding** – click the appropriate sign-in binding option. By default, GoToMeeting uses **REDIRECT**.

iv. **Sign-out page url (optional)** -type the log-out URL.

v. **Sign-out binding** – click the appropriate sign-in binding option. By default, GoToMeeting uses **REDIRECT**.

vi. **Identity Provider Entity ID** – type a unique IdP entity ID.

vii. **Verification certificate** – paste the IDP 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 company name>.pem

5. Select the **My identity provider has been updated with the new domain** check box.
6. Click **Save Configuration**.

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

Configuring NetScaler for Single Sign-On

For configuring NetScaler for GoToMeeting, 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 from the meatdata file: https://authentication.logmeininc.com/saml/sp.
   c.   Copy the file that you saved in pem format while configuring Slack for SSO and paste it to NetScaler I.P. at /nsconfig/ssl using WinSCP or similar tool.
   d.   Copy this to your netscaler using WinScp into /nsconfig/ssl folder.
   e.   Remotely access your NetScaler instance using PuTTY.
   f.   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:
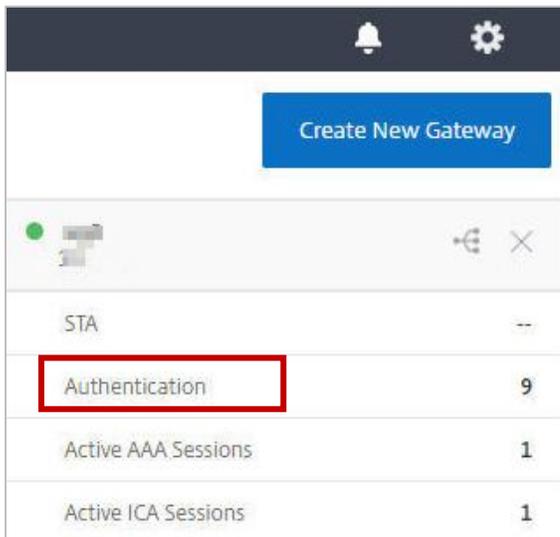
1. Connect to VPN using NetScaler with Unified Gateway.
   Note: Ensure that you obtain SP certificate before you start with the configuration.

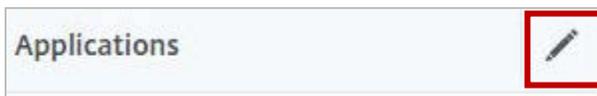2. Log on to NetScaler using your user name and password.
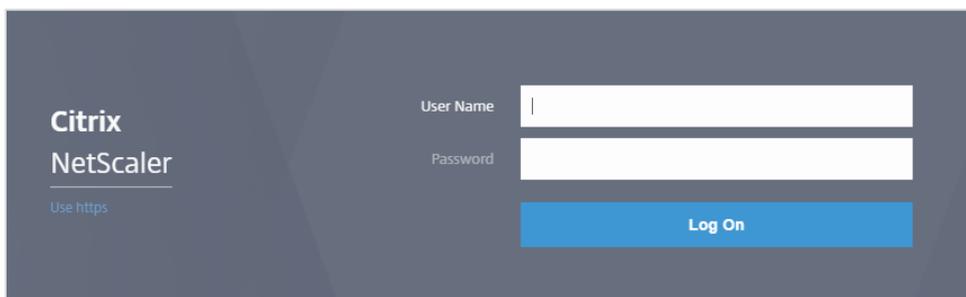
3. Click the **Configuration > Unified Gateway**.
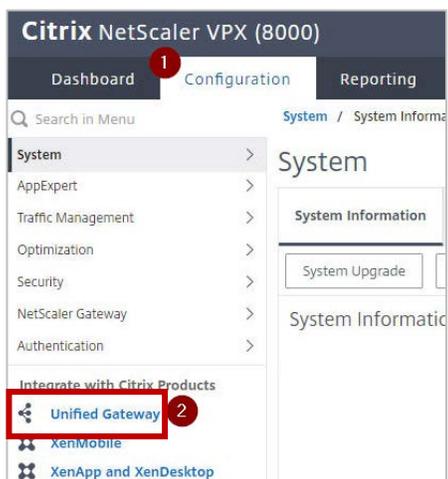
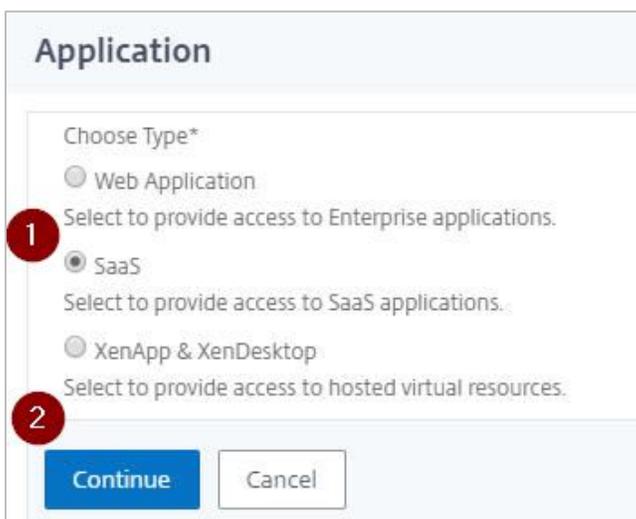4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.

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 **GoToMeeting**.

10. Click **Continue**.

11. In the **Create Application from Template** section, type the name of your SaaS application, in this case GoToMeeting, 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) GoToMeeting	Identity Provider (IdP) NetScaler
Identity Provider Entity ID	Issuer Name

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

i. **Service Provider Login URL** - enter the URL that you use to access GoToMeeting in https://<your-organization>.GoToMeeting.com format.
Note: For example, if the URL is https://myserver.GoToMeeting.com, you must replace <your-organization> with myserver.

ii. **Service Provider Log Out URL** – enter the URL that you use to access GoToMeeting.

To obtain this value, access https://authentication.logmeininc.com/saml/sp. An XML file is downloaded. Copy https://authentication.logmeininc.com/saml/SingleLogout and paste it in this field.

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

To obtain this value, access https://authentication.logmeininc.com/saml/sp. An XML file is downloaded. Copy the value for entityID and paste it in this field.

iv. **Audience** – type the URL that represents service provider.

     v.   **SP Certificate Name** – click the appropriate certificate name.
To obtain this value, access https://authentication.logmeininc.com/saml/sp. An XML file is downloaded.

To obtain the SP certificate follow the steps below:
    a.   Copy the file that you saved in pem format while configuring GoToMeeting 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 GoToMeeting-sp -cert GoToMeeting-sp.pem

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

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

13. Click **Continue.**

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

15. Click **Done**.

You have completed the NetScaler configuration for GoToMeeting.

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 **GoToMeeting**.
   Your GoToMeeting 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 https://global.gotomeeting.com.

2. You are redirected to NetScaler appliance's log in page.

3. Log on to NetScaler appliance using your enterprise credentials.

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

CITRIX®

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