



# **NetScaler with Unified Gateway**

## **Configuring Bluejeans**

# Contents

- CONTENTS ..... 1
- DISCLAIMER (DOCUMENTATION) ..... 2
- PREFACE ..... 3
- OVERVIEW ..... 4
- CONFIGURING BLUEJEANS FOR SINGLE SIGN-ON..... 5

# 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
<b>Bold</b>	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.
<b>Note</b>	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.

Bluejeans can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to Bluejeans using the same Single Sign On (SSO).

## Terminology

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 various terms that are used alternatively for completing configurations for service providers and identity providers.

**Table 2: Terminology used for SP and IdP configurations**

<b>Service Provider (SP)</b>	<b>Identity Provider (IdP)</b>
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

# Configuring Bluejeans for Single Sign-On

Bluejeans has SP/IdP initiated flow, which is supported in NetScaler (12.1.).

Before you start, you need the following:

- Admin account for Bluejeans
- Customer instance

For example, if your deployment url `https://<company_domain>.bluejeans.com/`, your customer instance is `<customer domain>`.

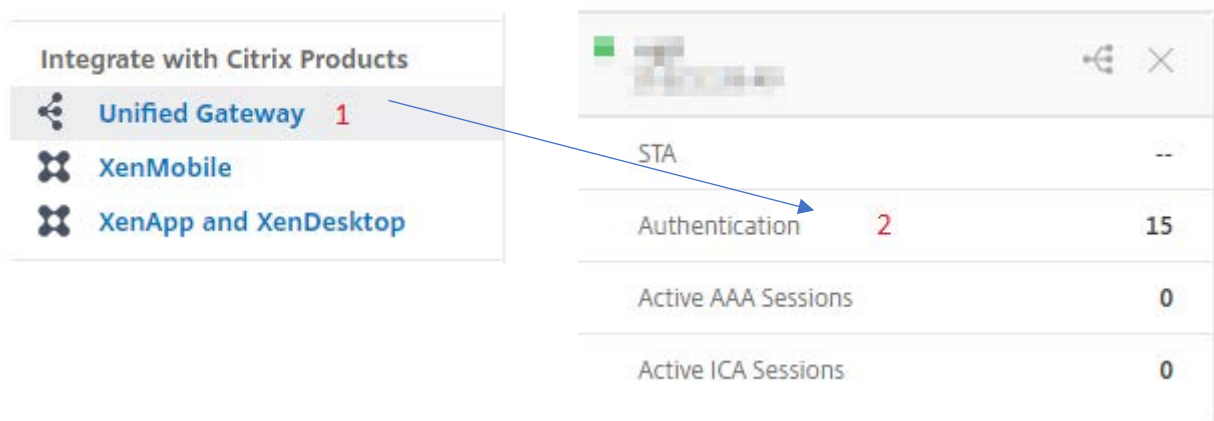
Admin account for NetScaler is required for App Catalog creation in NetScaler.

The Bluejeans configuration steps are as follows:

1. Configure Bluejeans with the App Catalog.
2. Configure IdP into Bluejeans.
3. Relay State in Bookmarks.



## Step 1: Configure Bluejeans with App Catalog

1. Click on **Unified Gateway > Authentication**.



The **Unified Gateway Configuration** screen appears.



2. Go to **Applications** section. Click on  icon. Now, you can see  icon. Click on it. The **Application** window appears.

## Application

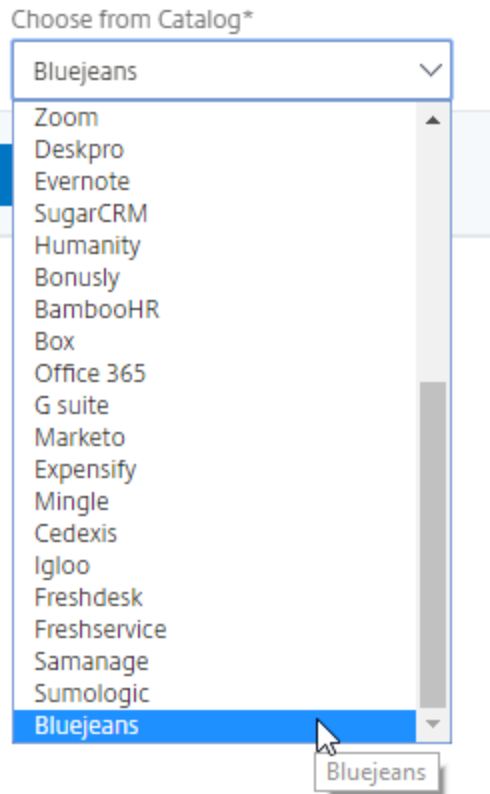
Choose Type\*

Web Application  
Select to provide access to Enterprise applications.

SaaS  
Select to provide access to SaaS applications.

XenApp & XenDesktop  
Select to provide access to hosted virtual resources.

3. Select **SaaS** from the Application type.
4. Select **Bluejeans** from the drop-down list.




5. Fill the application template with the appropriate values.



Name  
Bluejeans

Comments  
Bluejeans

Icon URL\*  
Choose File ▾ /var/netscaler/logon/Bluejeansicon.1



Service Provider Login URL\* **1**  
https://<company domain>.bluejeans.com/enter

Service Provider ID\* **2**  
http://samlsp.bluejeans.com

Assertion Consumer Service Url\*  
https://bluejeans.com/sso/saml2/

IDP Certificate Name\* **3**  
[dropdown menu] + [edit icon]

Issuer Name **4**  
UG\_VPN\_Bluejeans

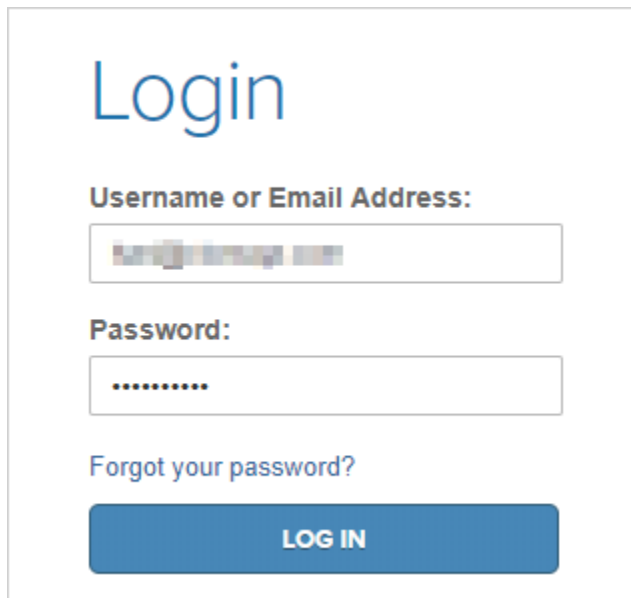
**Continue** **Cancel**

6. You must update the fields in NetScaler with the following values:

Field Name	Values
URL	<a href="https://&lt;company domain&gt;.bluejeans.com/enterprise-admin/#onboarding">https://&lt;company domain&gt;.bluejeans.com/enterprise-admin/#onboarding</a>
Service Provider ID	<a href="http://samlsp.bluejeans.com">http://samlsp.bluejeans.com</a>
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

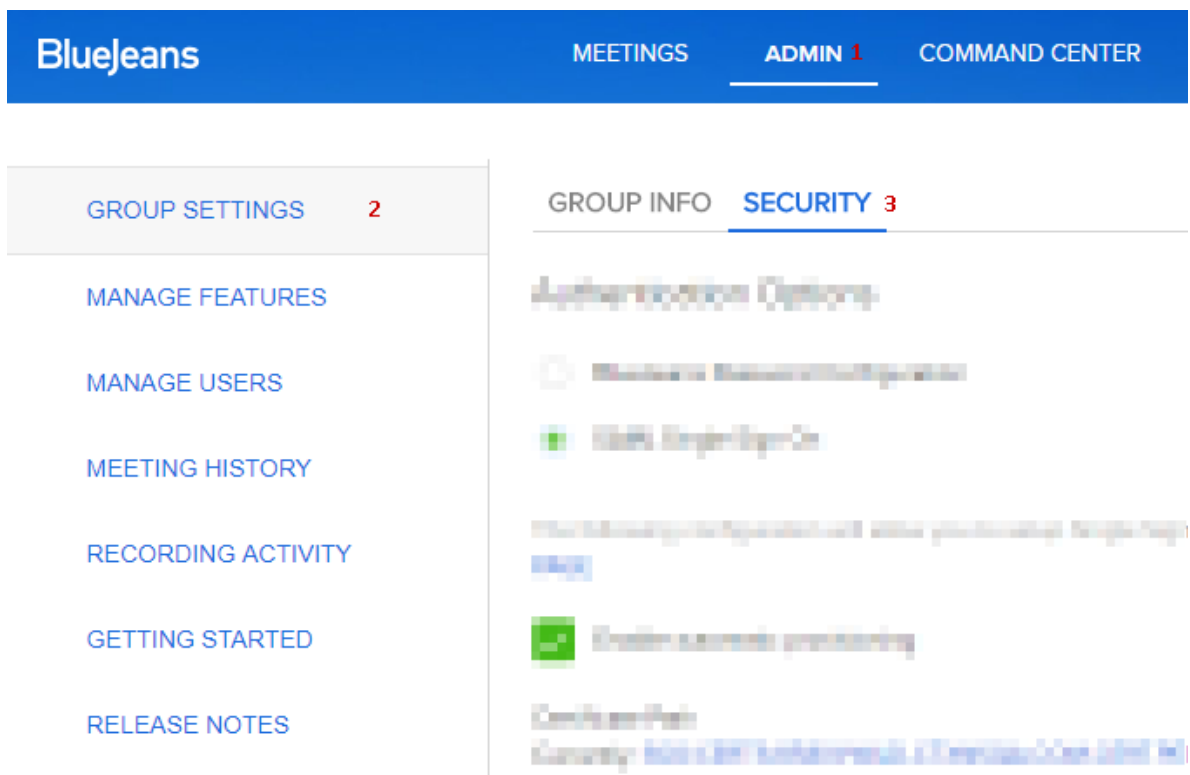
- In place of <customer domain>, enter your company name (See **Introduction** to know more about the <customer domain> value.)
- After providing the required values, click **Continue**. Click **Done**.

## Step 2: Configure IdP into Bluejeans



The image shows a login form for BlueJeans. It features a large blue 'Login' heading. Below it, there are two input fields: 'Username or Email Address:' and 'Password:'. The password field is masked with dots. A link for 'Forgot your password?' is located below the password field. At the bottom, there is a blue button labeled 'LOG IN'.

1. Login to Bluejeans as an Admin user.



The image is a screenshot of the BlueJeans administrative interface. At the top, there is a blue navigation bar with the 'BlueJeans' logo on the left and three menu items: 'MEETINGS', 'ADMIN 1', and 'COMMAND CENTER'. The 'ADMIN 1' item is highlighted with a white underline. Below the navigation bar, the main content area is divided into two columns. The left column contains a sidebar menu with the following items: 'GROUP SETTINGS 2', 'MANAGE FEATURES', 'MANAGE USERS', 'MEETING HISTORY', 'RECORDING ACTIVITY', 'GETTING STARTED', and 'RELEASE NOTES'. The 'GROUP SETTINGS 2' item is highlighted with a light gray background. The right column displays the 'GROUP INFO SECURITY 3' settings page. It has a sub-heading 'Authentication Options:' and lists several options with status indicators (circles). The 'SAML Single Sign-On' option is highlighted with a green circle and is currently enabled. Below this, there is a link for 'Manage SAML Single Sign-On' and another option 'Enable SAML provisioning' which is also enabled with a green circle. At the bottom of the right column, there is a section for 'Certificate Path' with a link to 'Certificate Path'.

2. Go to **ADMIN** at the top panel > Select **GROUP SETTINGS** > Click on **SECURITY**.

## Authentication Options

- BlueJeans Password Configuration
- 1**  SAML Single Sign On

The following configuration will allow you to setup Single Sign On for your group. For more information, see the [SAML Single Sign On Configuration](#) **PAGE**

- 2**  Enable automatic provisioning

Certificate Path **3**

Currently: `C:\Program Files\NetScal\Gateway\certificates\certificates`

Change:

Login URL

URL for signing into the remote authentication system

`https://ug1.ug1.com/saml/login` **4**

Logout URL

URL to which a user is redirected to on logout

`https://ug1.ug1.com/cgi/logout` **5**

Custom Error Page URL

URL to which a user is redirected to on an error

Default URL: `/sso/saml2/error/` **6**

SAML Meta Data


SAML Meta Data url for IdP initiated SSO

`https://ug1.com/saml2/metadata/ug1.com` **7**

RelayState

For IdP initiated SSO, configure your IdP with the following RelayState

`https://ug1.com/saml2/metadata/ug1.com` **8**

9  Pick User Id from <saml2:NameID> element

Email \*

 10

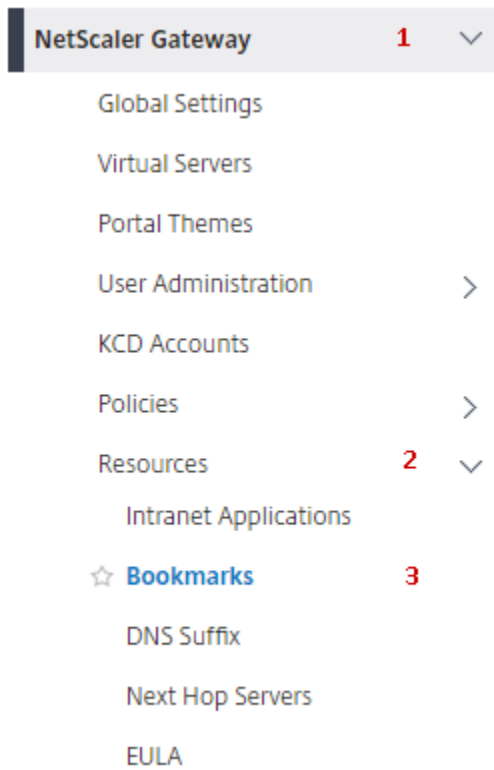
3. **SECURITY** window will open > Fill the template with appropriate values.

Field Name	Values
SAML Single Sign On	Should be Checked.
Enable automatic provisioning	Should be Checked.
Certificate Path	Upload IdP certificate
Login URL	<a href="https://ug1.&lt;customer_domain&gt;.com/saml/login">https://ug1.&lt;customer_domain&gt;.com/saml/login</a>
Password Change URL	<a href="https://ug1.&lt;customer_domain&gt;.com/cgi/logout">https://ug1.&lt;customer_domain&gt;.com/cgi/logout</a>
Logout URL	<a href="https://ug1.&lt;customer_domain&gt;.com/cgi/logout">https://ug1.&lt;customer_domain&gt;.com/cgi/logout</a>
Custom Error Page URL	Default <a href="URL:/sso/saml2/error/">URL:/sso/saml2/error/</a> (It will auto generate)
SAML Meta Data	Default value will generate automatically
RelayState	Unique RelayState will generate automatically
Pick User Id from <saml2:NameID> element	Should be Checked.
Email	Email

**Note:** Copy the RelayState for further use as it need to be used in IdP.

4. Click on **SAVE CHANGES**.

### Step 3: Relay State in Bookmarks.



1. Click on **NetScaler Gateway > Resources > Bookmarks.**

	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication
	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication
	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication
	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication
	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication
	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication
	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication
	is-bulk	is-bulk	https://cbxnsqa.bluejeans.com/enterprise-admin/#onboarding	/logon/Bluejeansicon.png	SAML Based Authentication

2. **Bookmarks** window will open > Click on **Bluejeans.**

Application Type  
SaaS

SSO Type  
SAML Based Authentication

SAML SSO Profile\*  
\_SAML\_Bluejeans > + ?

Use NetScaler Gateway As a Reverse Proxy

Comments  
Bluejeans

3. **Configure Bookmark** window will open > Click on **OK** of the field **SAML SSO Profile**.

Name

Assertion Consumer Service Url\*  
 ?

Relay State Expression Expression Editor

Select ▼    Select ▼    Select ▼    ✕

`https://bluejeans.com/sso/saml2/`

[Evaluate](#)

4. Pop-up window will open > Paste the Relay State (As shown in Step 2).
5. Click on **OK**.