



# **NetScaler with Unified Gateway**

**Configuring  
BambooHR**

# Contents

- CONTENTS ..... 1
- DISCLAIMER (DOCUMENTATION) ..... 2
- PREFACE ..... 3
- OVERVIEW ..... 4
- CONFIGURING BAMBOOHR 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.

BambooHR can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to BambooHR 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 BambooHR for Single Sign-On

BambooHR supports SP/IDP initiated flow, which is supported in Netscaler (12.1).

Before you start, you need the following:

- Admin account for BambooHR.
- Customer instance.  
For example, if your deployment URL is [https://<customer\\_domain>.bamboohr.com/](https://<customer_domain>.bamboohr.com/) your customer Instance is <customer\_domain>.
- This is required for App Catalog creation in NetScaler.
- Admin account for NetScaler.

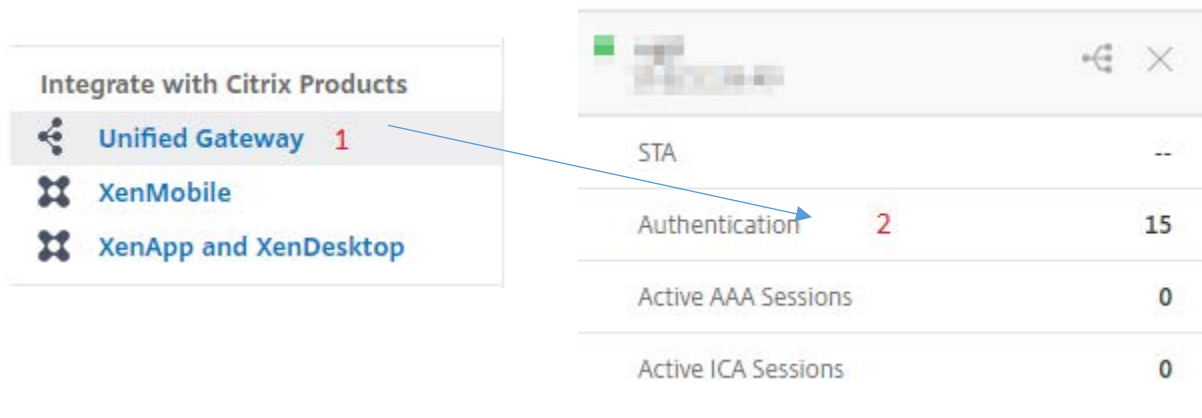
## BambooHR Configuration

The BambooHR configuration steps are as follows:

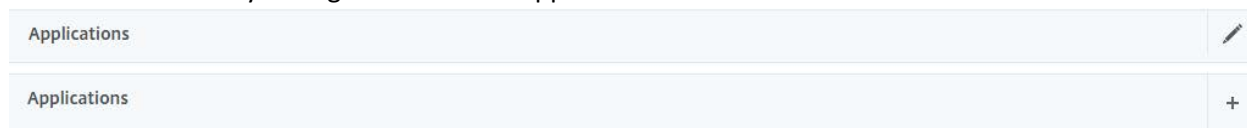
1. Configure BambooHR with the App Catalog.
2. Configure SAML Setting into BambooHR.



### Step 1: Configure BambooHR with App catalog

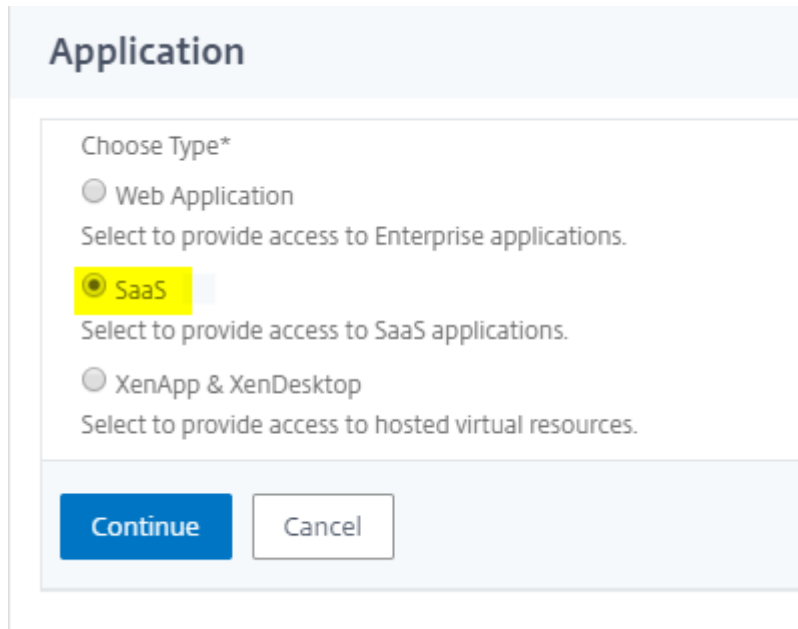
1. Click on Unified Gateway > Authentication



The Unified Gateway Configuration screen appears.



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



**Application**

Choose Type\*

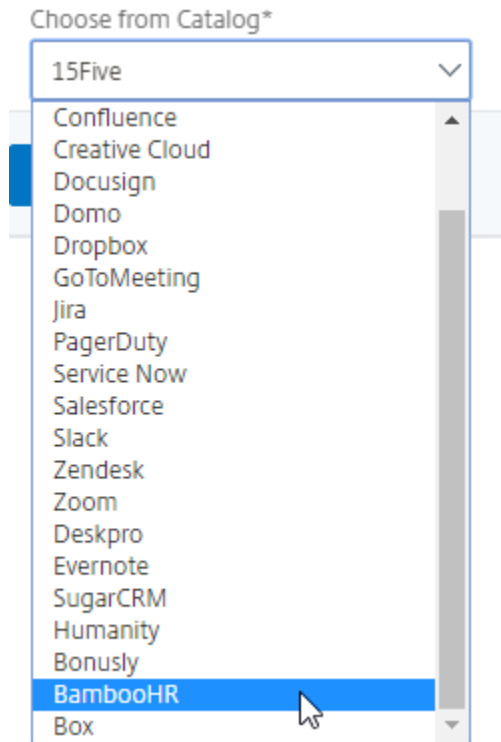
Web Application  
Select to provide access to Enterprise applications.

SaaS  
Select to provide access to SaaS applications.

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

**Continue** Cancel

3. Select **SaaS** from the Application type.
4. Select BambooHR from the dropdown list.




5. Fill the Application template with appropriate values.



Name  
BambooHR

Comments  
BambooHR

Icon URL\*  
Choose File  /var/netcaler/logon/BambooHRicoi



Service Provider Login URL\* 1  
https://[redacted].bamboohr.com/hom

Service Provider ID\* 2  
BambooHR-SAML

Assertion Consumer Service Uri\* 3  
https://[redacted].bamboohr.com/sam

Audience 4  
https://[redacted].bamboohr.com/sam

IDP Certificate Name\* 5  
[redacted] + ✎

Issuer Name 6  
UG\_VPN\_BambooHR

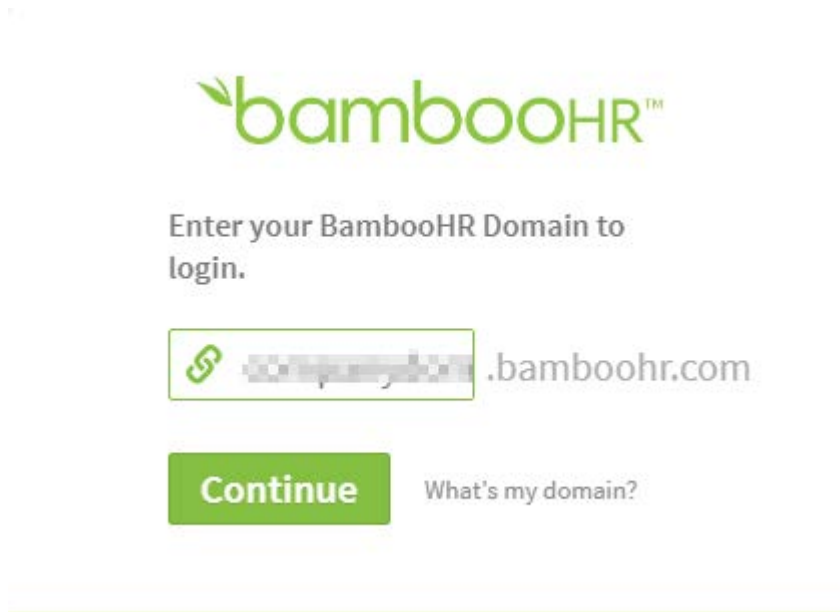
6. You must update the fields in Netscaler with the following values:

Field Name	Values
URL	<a href="https://&lt;custom_domain&gt;.bamboohr.com/home">https://&lt;custom_domain&gt;.bamboohr.com/home</a>
Service Provider ID	BambooHR-SAML
ACS URL	<a href="https://&lt;custom_domain&gt;.bamboohr.com/saml/consume.php">https://&lt;custom_domain&gt;.bamboohr.com/saml/consume.php</a>
Audience	<a href="https://&lt;custom_domain&gt;.bamboohr.com/saml/consume.php">https://&lt;custom_domain&gt;.bamboohr.com/saml/consume.php</a>
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

7. In place of <customer\_domain>, enter your company domain name (See **Introduction** to know more about the <customer\_domain> values).
8. After providing the required values, click **continue**. Click **done**.

## Step 2: Configure SAML Setting into BambooHR

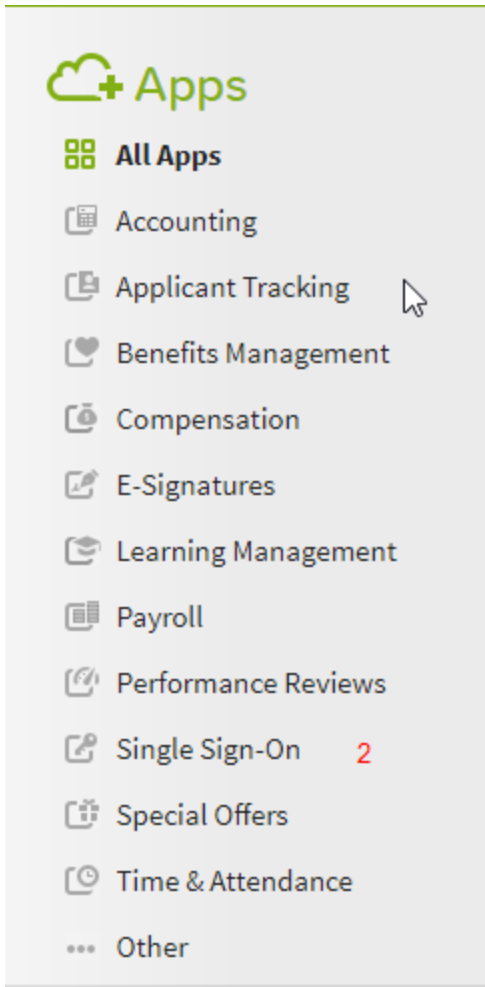
1. Login to **BambooHR** as an Admin user.



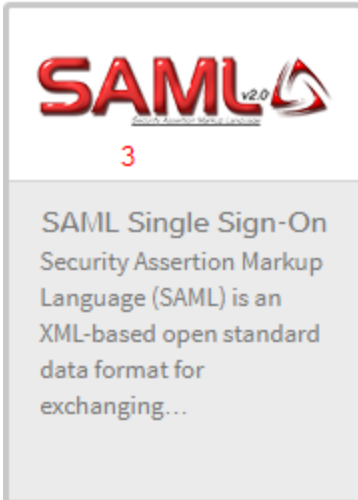
2. Click on App icon on right top corner.



3. All Apps services window will appears, Click on Single Sign-On listed on left side.



4. Single Sign-On window will appear, click on SAML tab.



5. SAML Single sign-on window will appear, Scroll down and click on install.



6. Setting window will appear.

## Settings

SSO Login URL \*

`https://ug1.<customer_domain>.com/saml/login`

x.509 Certificate \*

```
-----BEGIN CERTIFICATE-----
MIIEBTCCAeGgAwIBAgIBATANBgkqhkiG9w0BAQsFAD...
-----END CERTIFICATE-----
```

Install

Cancel

7. Fill the required field.

Field Name	Values
SSO Login URL	https://ug1.<customer_domain>.com/saml/login
x.509 certificate	Paste IdP certificate

8. Click on **install** button.