NetScaler with Unified Gateway

Configuring Kintone

Abstract

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

Contents

ABSTRACT..0

CONTENTS 1

DISCLAIMER (DOCUMENTATION) 2

PREFACE..3

OVERVIEW..4

CONFIGURING KINTONE FOR SINGLE SIGN-ON..4

CONFIGURING NETSCALER FOR SINGLE SIGN-ON 8

TESTING THE CONFIGURATION..12

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.

Kintone provides social collaboration cloud service that enables users to build apps and dynamic databases and offers a portal for communication, data and business process management.

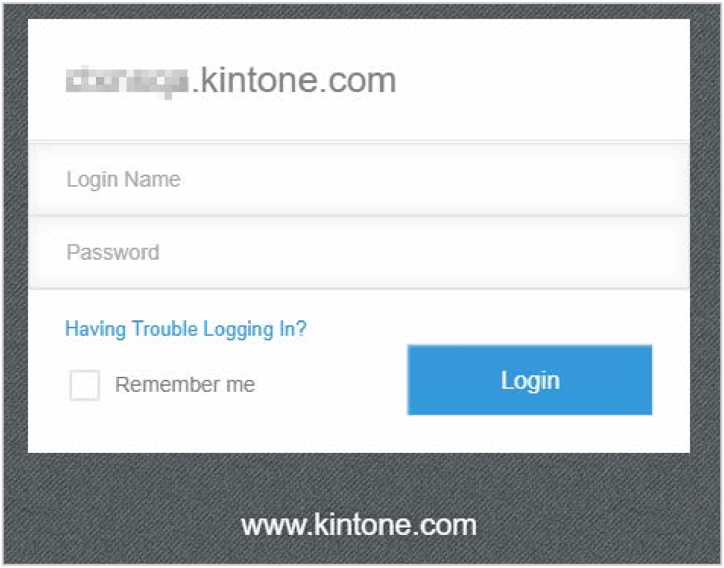
You can connect Kintone with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring Kintone for Single Sign-On

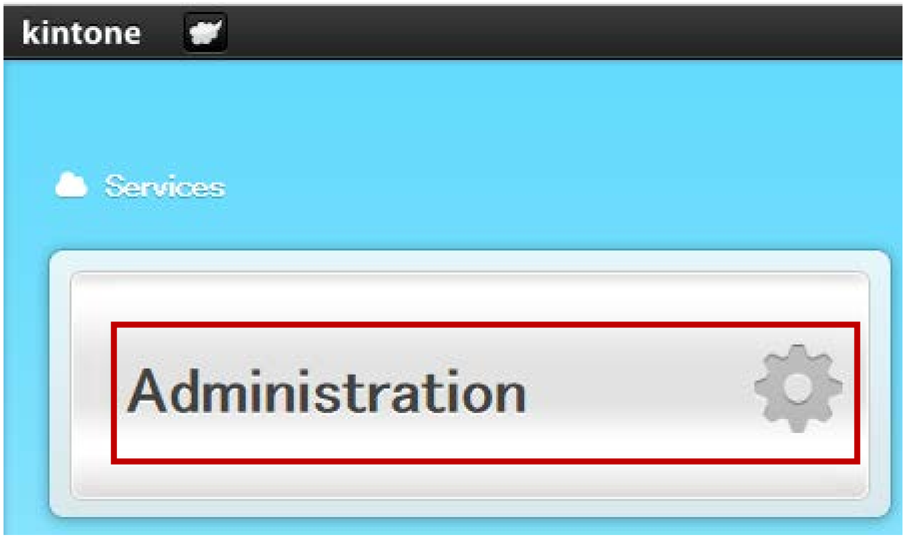
Configuring Kintone for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Kintone using their enterprise credentials.

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

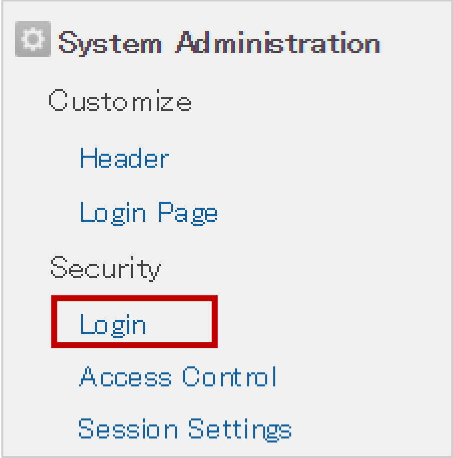
1. In a browser, type https://<your-organization>.kintone.com/ and press enter.
   Note: For example, if the URL you use to access pager duty is https://myserver.Kintone.com, then you must replace <your-organization> with myserver.
2. Log on to your Kintone account as an administrator.



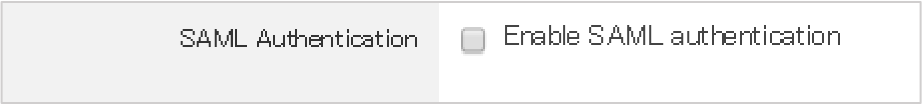
3. On the home page, click **Administration**.



4. On the **Service Usage** page, in the left pane, scroll down to the **System Administration** section and under **Security**, click **Login**.



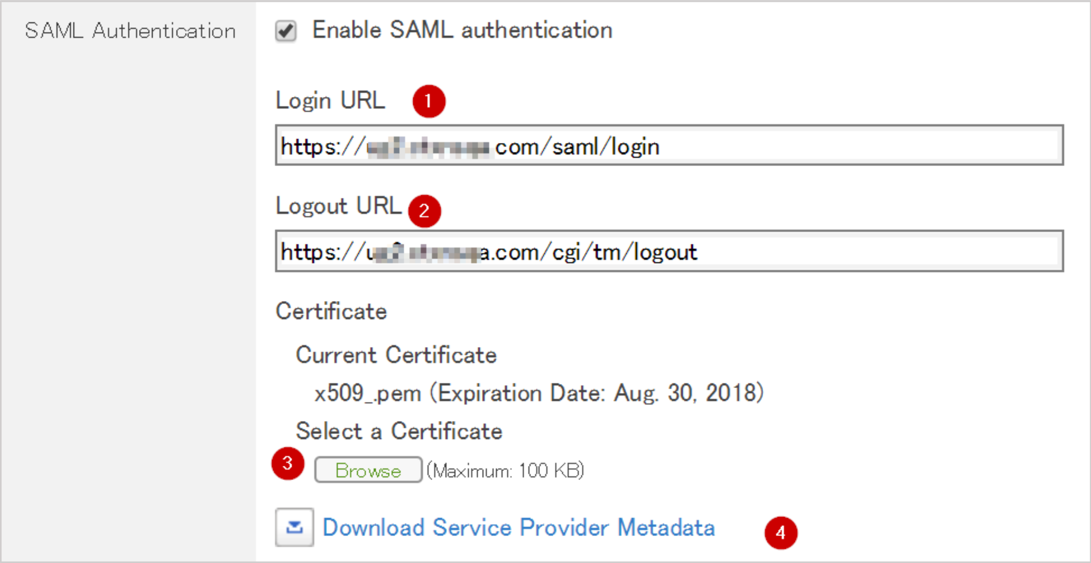
5. On the **Login Security** page, scroll down to the **SAML Authentication** section and select the **Enable SAML authentication** check box.



SAML Authentication □ Enable SAML authentication

The section expands and displays additional fields.

6. In the expanded SAML Authentication section, specify the following information:



SAML Authentication

☑ Enable SAML authentication

Login URL

https://[redacted] com/saml/login

Logout URL

https://u[redacted]a.com/cgi/tm/logout

Certificate

Current Certificate

x509_.pem (Expiration Date: Aug. 30, 2018)

Select a Certificate

i. **Login URL** – type the login URL in https://<your organizationFQDN>/saml/login format.

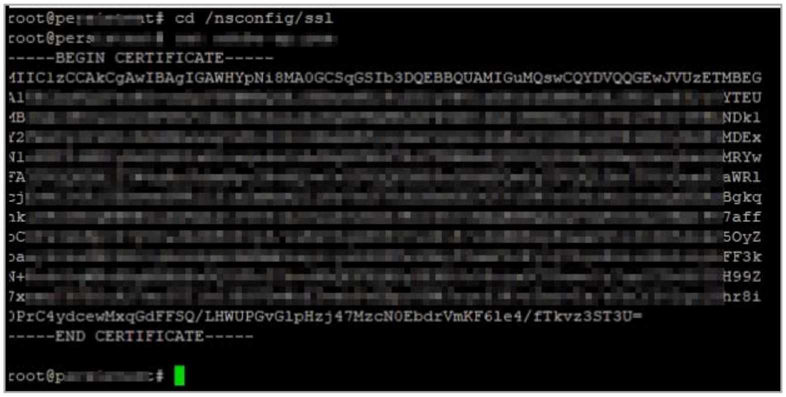
~~ii.~~ **Logout URL** – type a redirect URL to which you want users to be redirected after they log out from Kintone.

iii. **Certificate** – Upload the IdP Signing Certificate.
Click **Browse** to browse to the folder where you saved the IdP provided certificate and upload it.
To obtain your IdP X.509 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.



```
coot@per[redacted]t# cd /nsconfig/ssl
coot@pers[redacted]
-----BEGIN CERTIFICATE-----
4IIC1zCCAkCgAwIBAgIGAWHYpNi8MA0GCSqGSIb3DQEBBQUAMIGuMQswCQYDVQQGEwJVUzETMBEG
[redacted]
)PrC4ydcewMxqGdFFSQ/LHWUPGvGlpHzj47MzcN0EbdrVmKF6le4/fTkvz3ST3U=
-----END CERTIFICATE-----

coot@p[redacted]#
```

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 organization name>.pem

iv. To download the metadata in XML format, Click **Download Service Provider Metadata**.

7. Click **Save**.

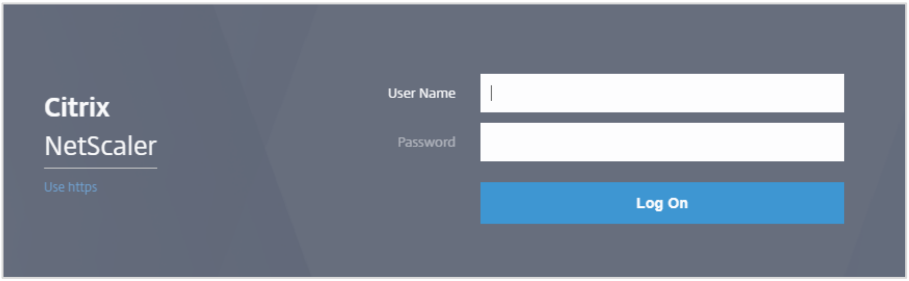
You have completed the required configuration for the service provider which is in this case –Kintone.

Configuring NetScaler for Single Sign-On

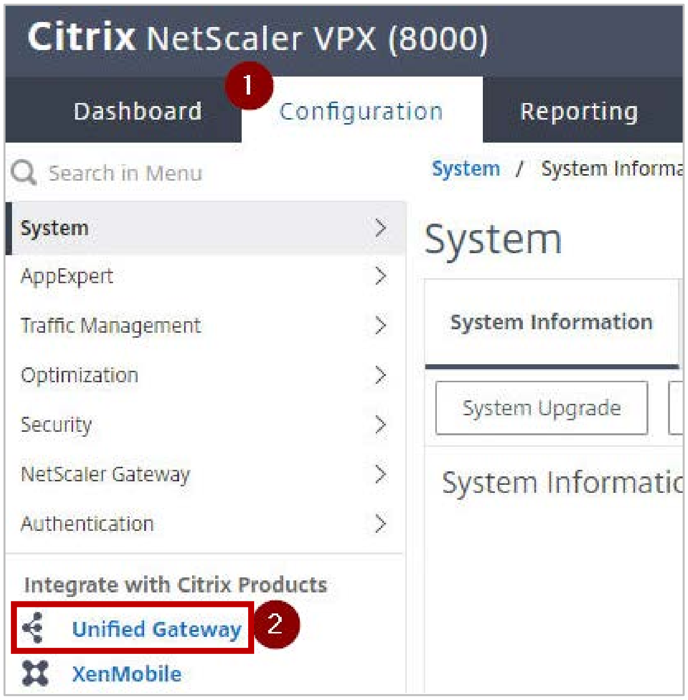
For configuring NetScaler for Kintone, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

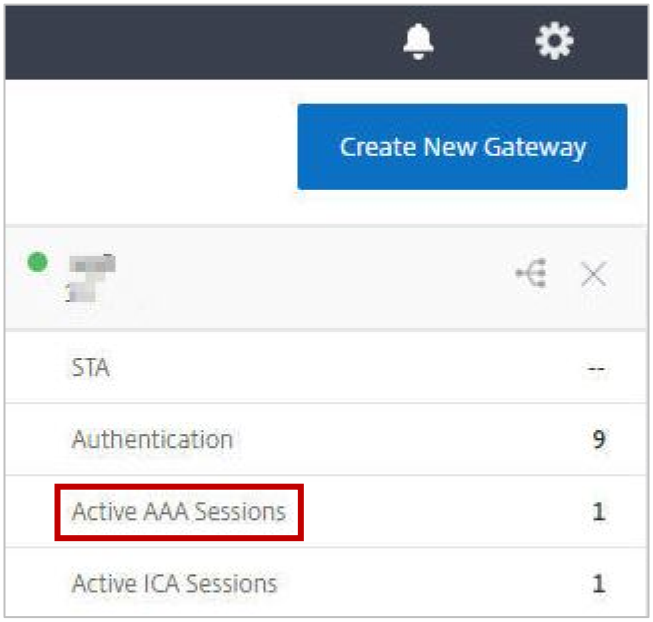
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



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



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



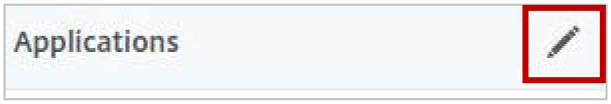
STA --

Authentication 9

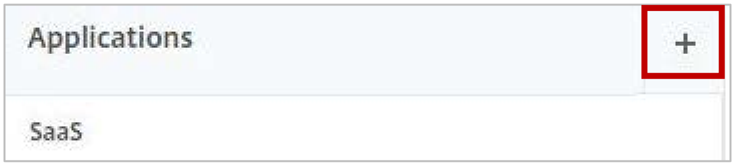
Active AAA Sessions 1

Active ICA Sessions 1

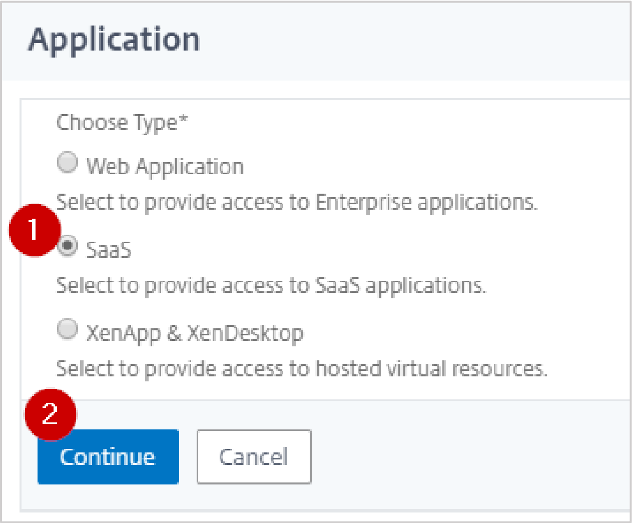
5. Click the edit icon for **Applications** section.



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



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



Choose Type*

○ Web Application

Select to provide access to Enterprise applications.

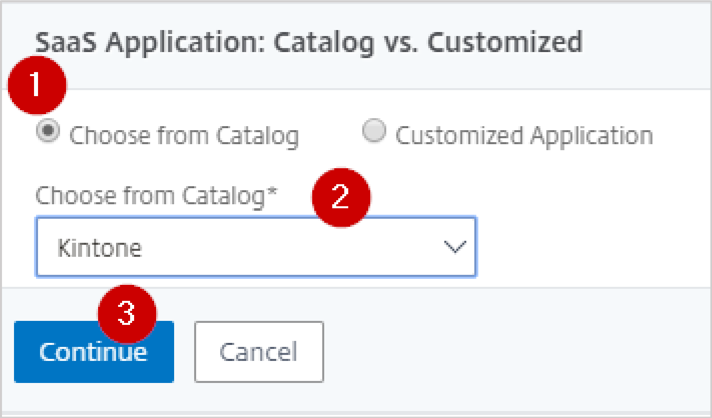
● SaaS

Select to provide access to SaaS applications.

○ XenApp & XenDesktop

Select to provide access to hosted virtual resources.

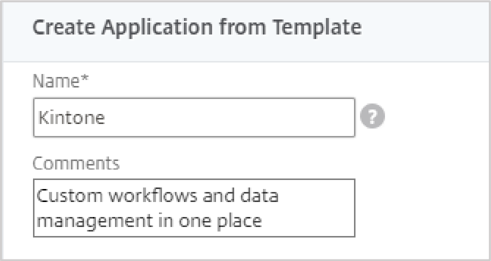
8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **Kintone**.


SaaS Application: Catalog vs. Customized

● Choose from Catalog ○ Customized Application

Choose from Catalog*: Kintone

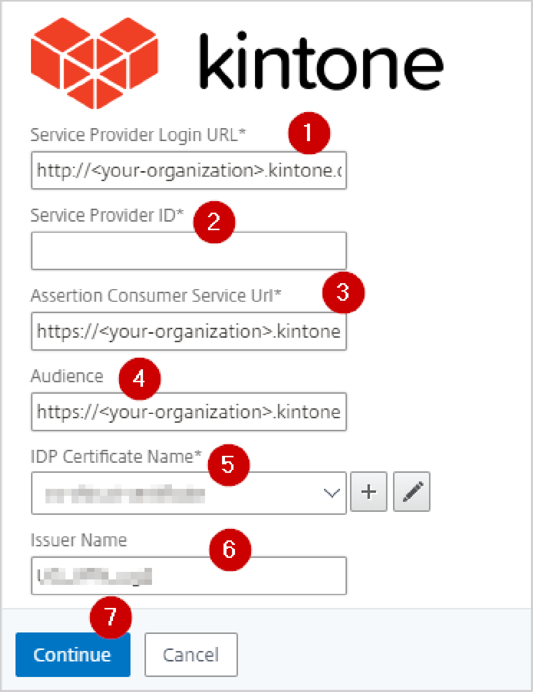
10. Click **Continue**.
11. In the **Create Application from Template** section, type the name of your SaaS application, in this case Kintone, and relevant comments.


Create Application from Template

Name*: Kintone

Comments: Custom workflows and data management in one place

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



Service Provider Login URL*: http://<your-organization>.kintone.c

Service Provider ID*:

Assertion Consumer Service Url*: https://<your-organization>.kintone

Audience: https://<your-organization>.kintone

IDP Certificate Name*: [redacted]

Issuer Name: [redacted]

i. **Service Provider Login URL** - type the URL in https://<your-organization>.kintone.com format. **Note**: For example, if the organization's URL is https://myserver.Kintone.com, you must replace <your-organization> with myserver.
ii. **Service Provider ID** - copy the value for entityID attribute of the EntityDescriptor tag mentioned in the metadata xml file that you downloaded while configuring Kintone for SAML and paste it to this box.
iii. **Assertion Consumer Service Url*** - copy the value for Location attribute of the AssertionConsumerService tag mentioned in the metadata xml file that you downloaded while configuring Kintone for SAML and paste it to this box. For example: https://<your-organization>.kintone.com/saml/acs
iv. **Audience** – type the URL that represents service provider in https://<your-organization>.kintone.com format.
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 a unique name to identify NetScaler. For example: MyServer_NS_Kintone

13. Click **Continue.**

14. Click **Done**.

    The Kintone logo appears.

15. Click **Done**.

You have completed the NetScaler configuration for Kintone.

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

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**