



NetScaler with Unified Gateway

Configuring New Relic

Abstract

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

Contents

ABSTRACT	0
CONTENTS	1
DISCLAIMER (TECHNOLOGY PREVIEW)	ERROR! BOOKMARK NOT DEFINED.
DISCLAIMER (DOCUMENTATION)	2
PREFACE	3
OVERVIEW	4
CONFIGURING NEW RELIC FOR SINGLE SIGN-ON	4
CONFIGURING NETSCALER FOR SINGLE SIGN-ON	8
TESTING THE CONFIGURATION	13

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.

New Relic provides digital intelligence platform that enables development teams to measure and monitor the performance of their applications and infrastructure.

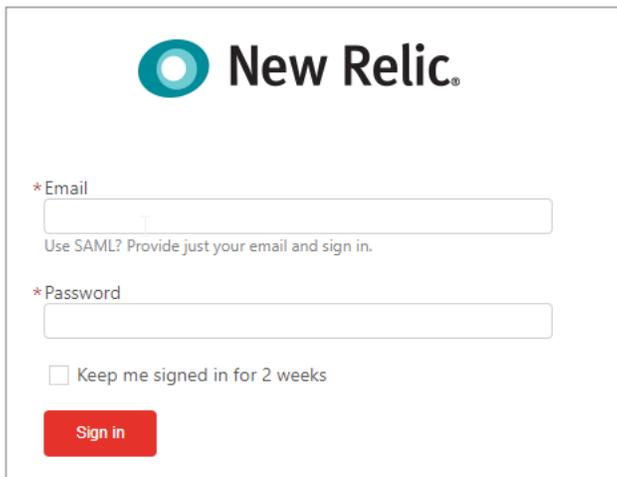
You can connect New Relic with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring New Relic for Single Sign-On

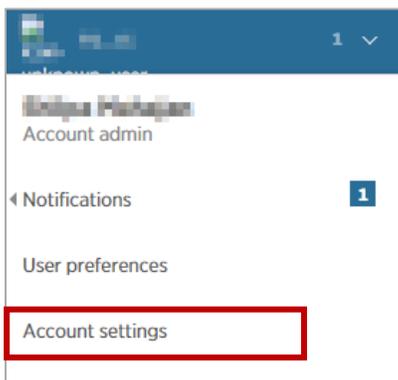
Configuring New Relic for SSO enables administrators to manage their users using NetScaler. Users can securely log on to New Relic using their enterprise credentials.

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

1. In a browser, type `https://rpm.newrelic.com` and press Enter.
2. Log on to your New Relic account.



3. On the home page, in the upper right corner, click the arrow and then click **Account Settings**.

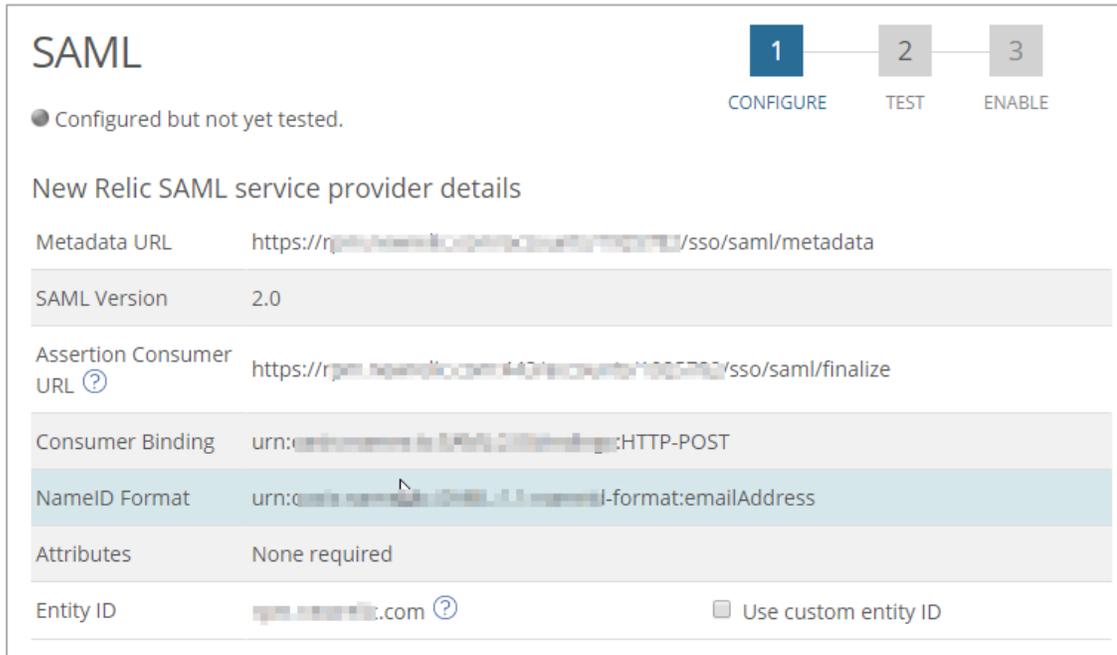


4. On the **Account Settings** page, in the **AUTHENTICATION** section, click **Single sign-on**.



5. On the **SAML** page, in the upper right corner click 1. .
6. In the **Configure** section, New Relic displays values for Metadata URL, Assertion Consumer URL, Consumer Binding, NameID Format, Attributes, and Entity ID fields. Review the details.

Note: The values are added based on the service provider metadata file. For more information refer: <https://rpm.newrelic.com/accounts/< your-org-id >E/sso/saml/metadata>



SAML

● Configured but not yet tested.

1 CONFIGURE 2 TEST 3 ENABLE

New Relic SAML service provider details

Metadata URL	https://rpm.newrelic.com/accounts/1005792/sso/saml/metadata
SAML Version	2.0
Assertion Consumer URL ?	https://rpm.newrelic.com/accounts/1005792/sso/saml/finalize
Consumer Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Attributes	None required
Entity ID	rpm.newrelic.com ? <input type="checkbox"/> Use custom entity ID

7. In the **Your SAML Identity Provider certificate** section, **Issuer** and **Subject** displays the values after you upload the IdP certificate.

Your SAML Identity Provider certificate

Issuer
/C=US/O=DigiCert, Inc./CN=DigiCert SHA2 Secure Server CA

Subject
/C=US/O=DigiCert, Inc./CN=DigiCert SHA2 Secure Server CA

Valid until
2018-08-30 12:00:00 UTC

*Upload a new certificate **1**

Browse files...

Your SAML identity provider details

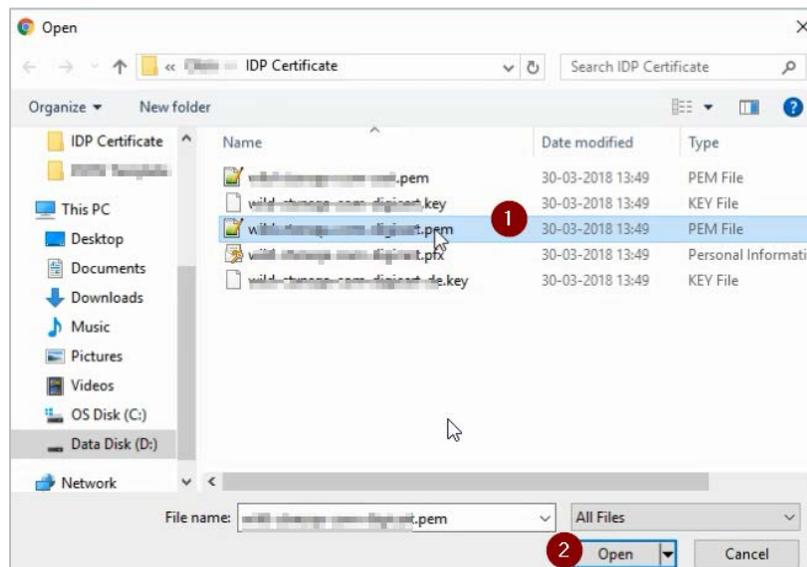
*Remote login URL **2**
https://us2.atlassian.com

Logout landing URL (optional) **3**

Save my changes **4**

For the subsequent fields, specify the following details:

- i. Upload a new certificate – click **Browse files...** to browse to the folder where you saved the IdP provided certificate and upload it.

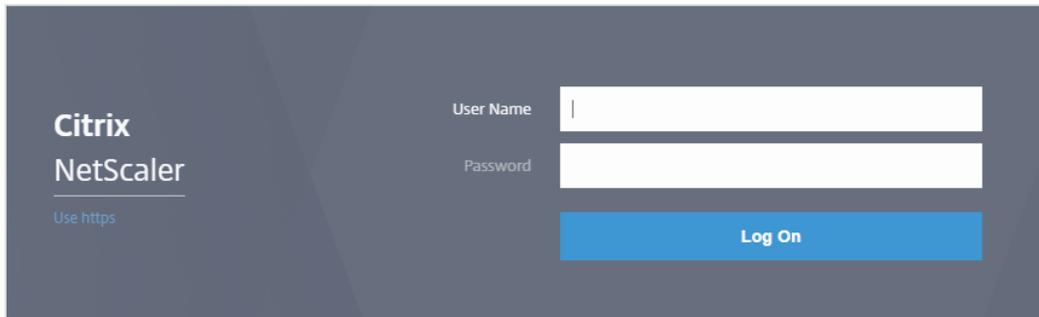


Configuring NetScaler for Single Sign-On

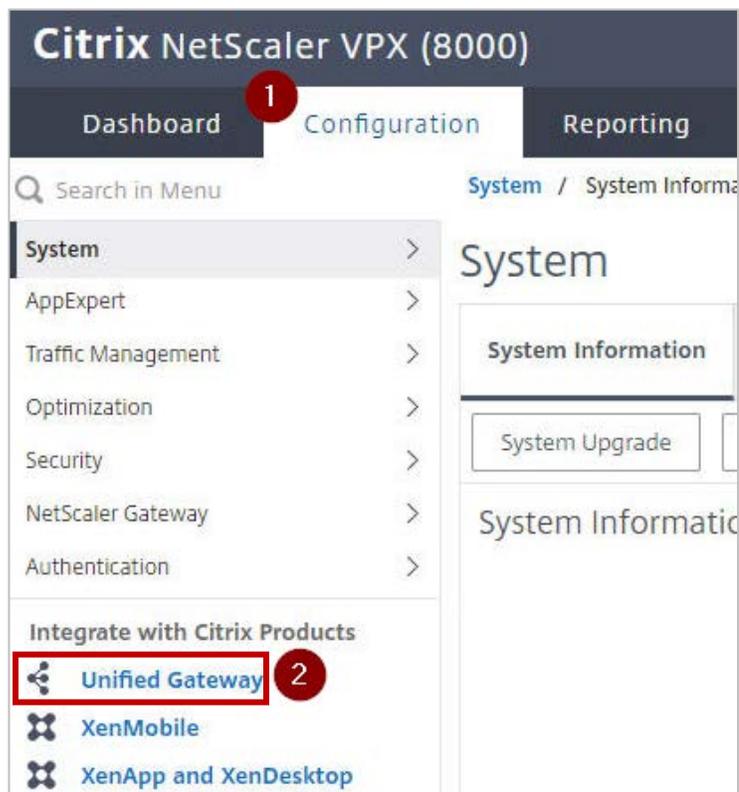
For configuring NetScaler for New Relic, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

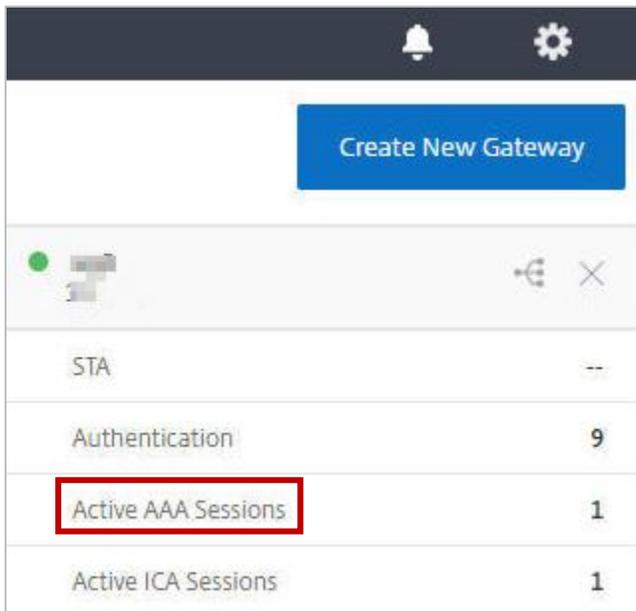
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



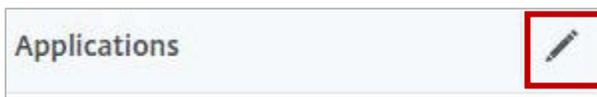
3. Click the **Configuration > Unified Gateway**.



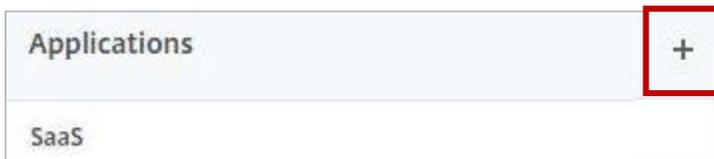
4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



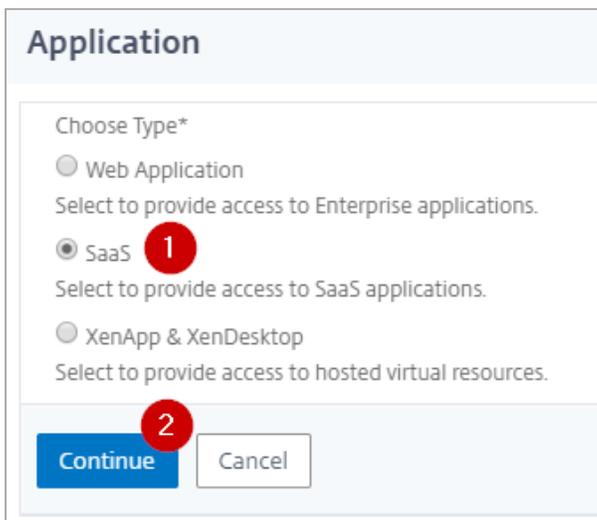
5. Click the edit icon for **Applications** section.



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 **New Relic**.

SaaS Application: Catalog vs. Customized

Choose from Catalog Customized Application

Choose from Catalog*

NewRelic

Continue Cancel

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

Create Application from Template

Name*

New Relic

Comments

Digital Performance Monitoring and Management

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) New Relic	Identity Provider (IdP) NetScaler
Entity ID	Service Provider ID

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

The screenshot shows the New Relic configuration interface. At the top left is the New Relic logo. Below it are several input fields and dropdown menus, each with a red circle containing a number from 1 to 7. Field 1 is 'Service Provider Login URL*' with the value 'https://rpm.newrelic.com:443/accou'. Field 2 is 'Service Provider ID*' which is empty. Field 3 is 'Assertion Consumer Service Url*' with the value 'https://rpm.newrelic.com:443/accou'. Field 4 is 'SP Certificate Name' with a dropdown menu. Field 5 is 'IDP Certificate Name*' with a dropdown menu. Field 6 is 'Issuer Name' with the value 'URL_4438_1042'. At the bottom are 'Continue' and 'Cancel' buttons.

- i. **Service Provider Login URL** - enter the URL that you use to access New Relic: <https://rpm.newrelic.com:443/accounts/<your-org-id>/sso/saml/finalize>.
- ii. **Service Provider ID** - type the URL that you entered for Entity ID while configuring New Relic.
- iii. **Assertion Consumer Service Url*** - enter the URL that you use to access New Relic: <https://rpm.newrelic.com:443/accounts/<your-org-id>/sso/saml/finalize>.

- iv. **SP Certificate Name** – click the appropriate certificate name.
To obtain this value, access the metadata file:
<https://rpm.newrelic.com:443/accounts//<your-org-id>/sso/saml/metadata>
- v. **IDP Certificate Name** – click the appropriate certificate name.
Refer to the appropriate public key certificate provided by NetScaler which you referred while configuring New Relic.
- vi. **Issuer Name** – type a unique name.
- vii. Click **Continue**.

13. Click **Done**.

The New Relic logo appears.

14. Click **Done**.

You have completed the NetScaler configuration for New Relic.

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 **New Relic**.
Your New Relic 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 the login URL.
2. You are redirected to NetScaler appliance's log in page.
3. Log on to NetScaler appliance using your enterprise credentials.

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



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

© 2018 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).