CITRIX

NetScaler with Unified Gateway

Configuring New Relic

Abstract

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

Contents

Disclaimer (Documentation)

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.

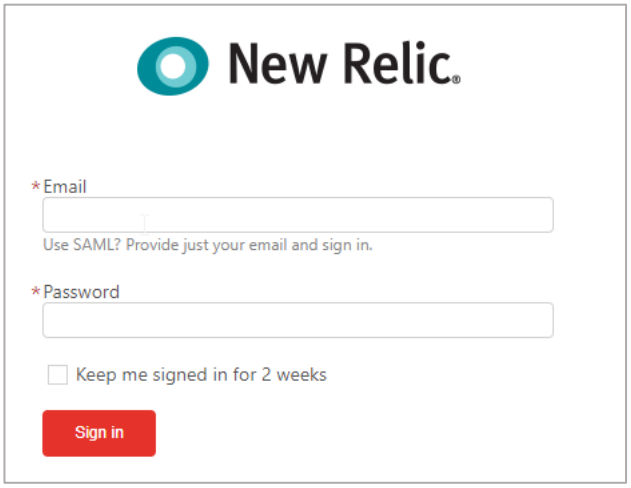
You can connect New Relic with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring New Relic for Single Sign-On

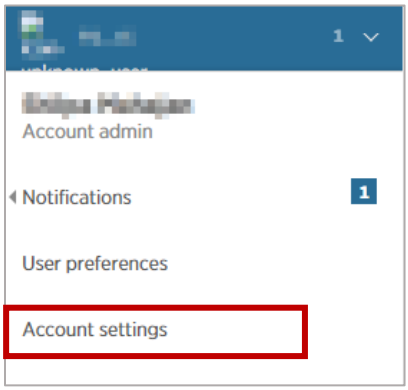
Configuring New Relic for SSO enables administrators to manage their users using NetScaler. Users can securely log on to New Relic using their enterprise credentials.

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

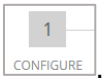
1. In a browser, type https://rpm.newrelic.com and press Enter.
2. Log on to your New Relic account.



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

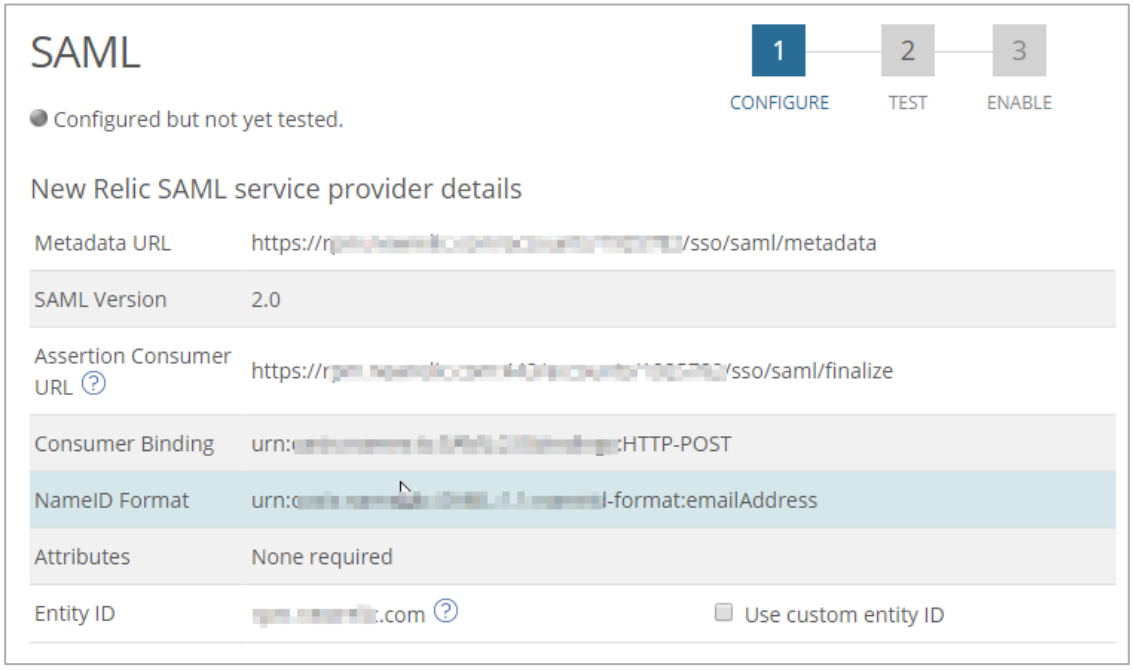


4. On the **Account Settings** page, in the **AUTHENTICATION** section, click **Single sign-on**.

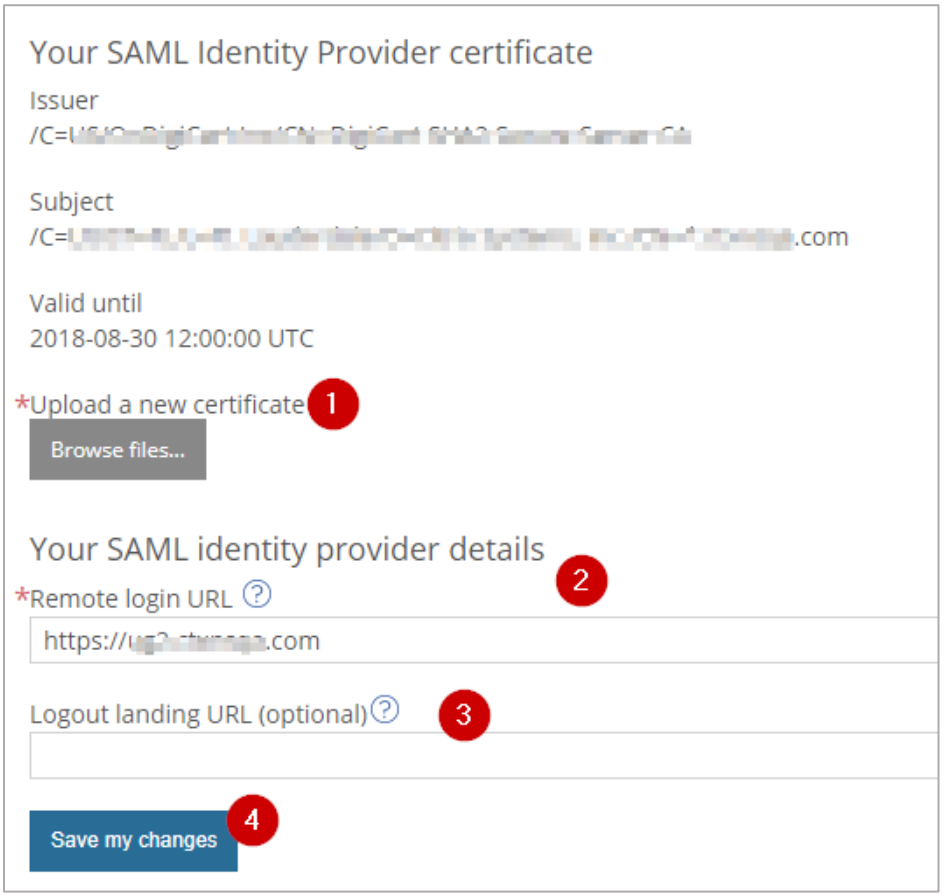
5. On the **SAML** page, in the upper right corner click 1. 

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

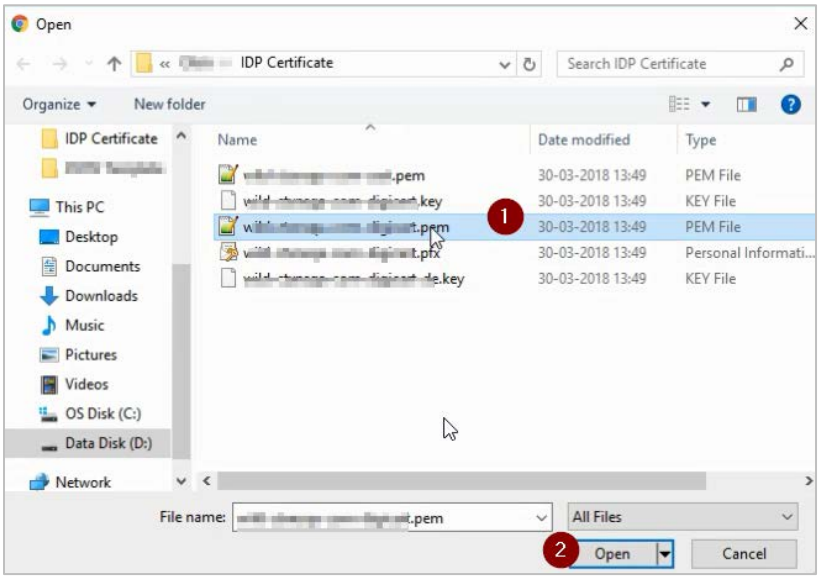


7. In the **Your SAML Identity Provider certificate** section, **Issuer** and **Subject** displays the values after you upload the IdP certificate.



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.



To obtain your IdP certificate, follow the steps below:

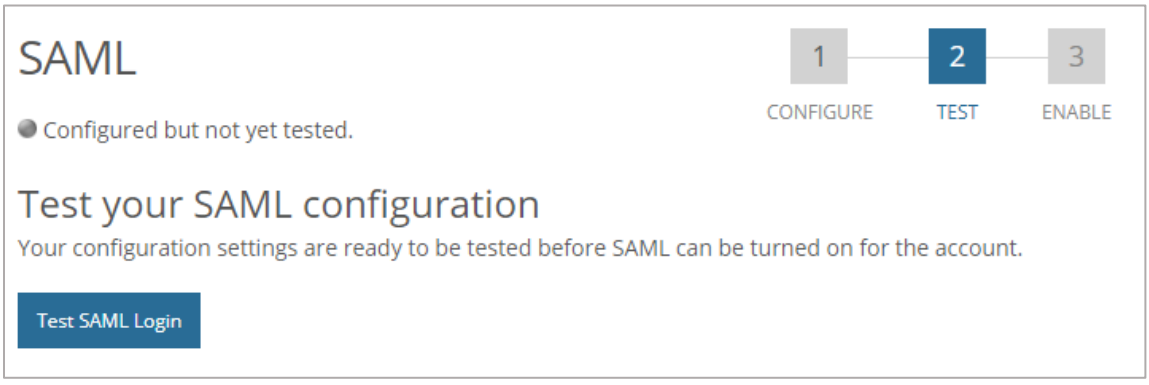
a. Remotely access your NetScaler instance using PuTTY.
b. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.
c. Type cat <certificate-name> and press Enter.
d. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----
e. Paste the text in a text editor and save the file in an appropriate format such as <your organization name>.pem

ii. **Remote login URL** – type a URL for single sign-on. The URL must be one of these URLs: authentication URL, Identity Provider (IdP) HTTP POST URL, SAML HTTP Endpoint, SAMLRequest Endpoint, SP-initiated Endpoint, POST Request Endpoint.

iii. **Logout landing URL (optional)** – type a redirect URL for logout to enable SAML authenticated users to be logged out securely. This is an optional field.

iv. Click **Save my changes**.

Note: Step 2 involves testing SAML configuration. After you complete configuring IdP profile and after it is validated, SSO for New Relic is enabled.



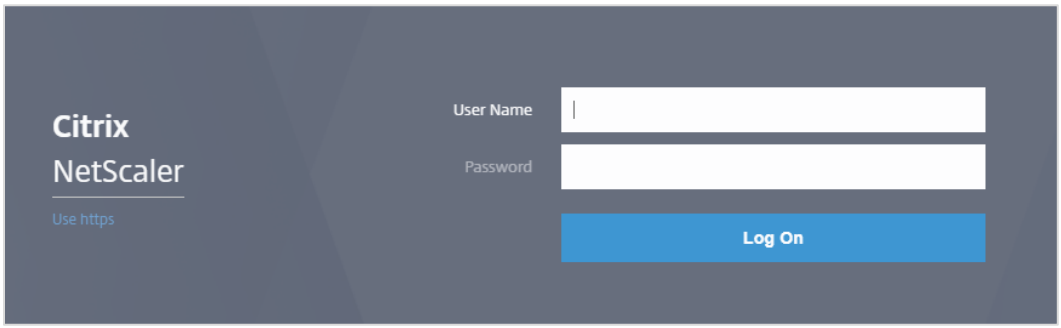
You have completed the required configuration on the service provider which is in this case – New Relic.

Configuring NetScaler for Single Sign-On

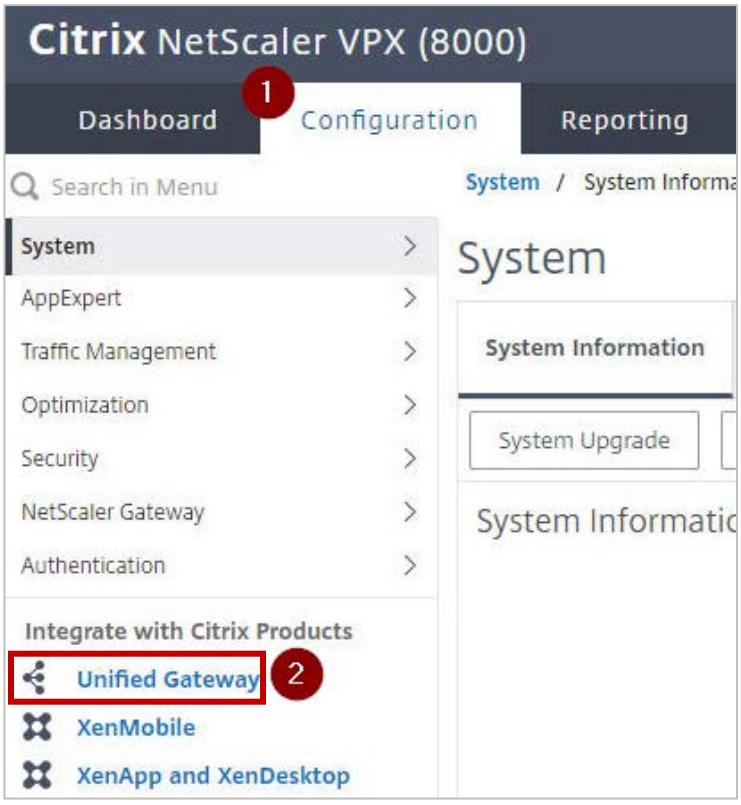
For configuring NetScaler for New Relic, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

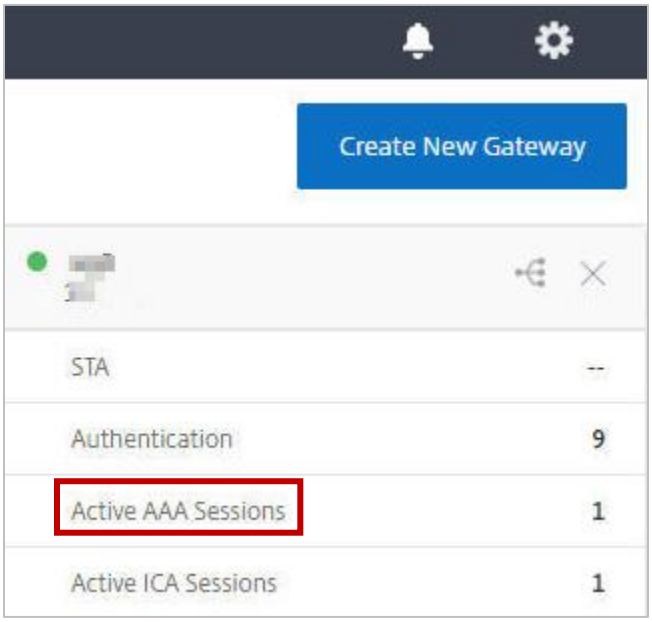
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



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

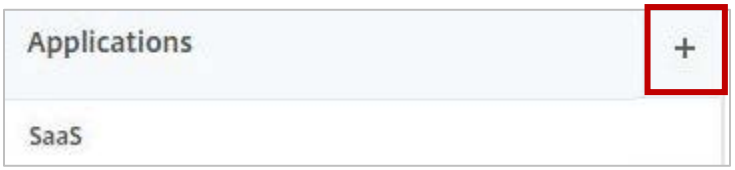


4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.

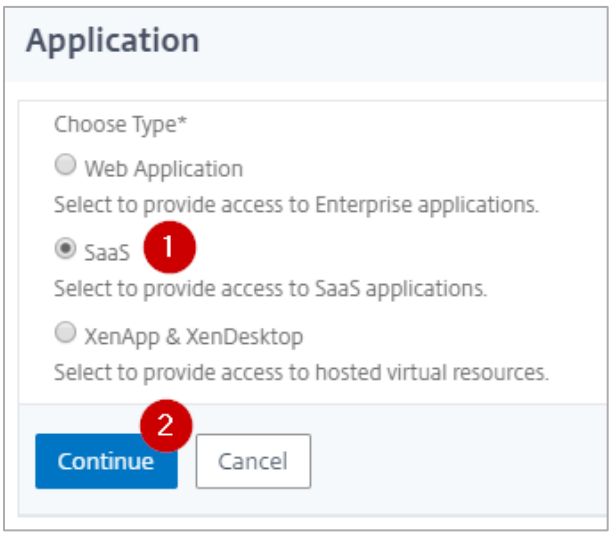


5. Click the edit icon for **Applications** section.

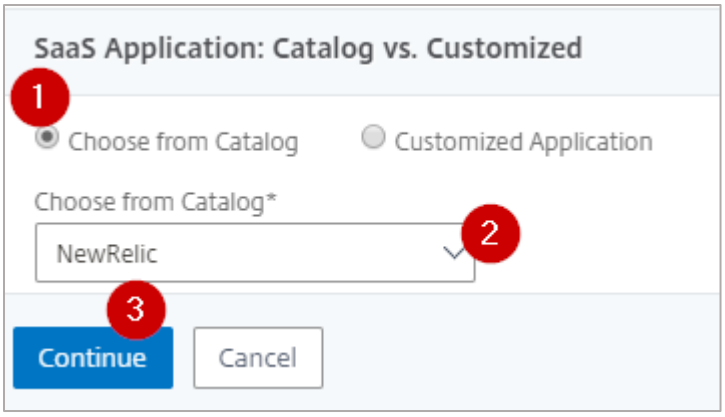
6. For adding a SaaS application, click the plus icon ⊞ that appears in the edit mode.



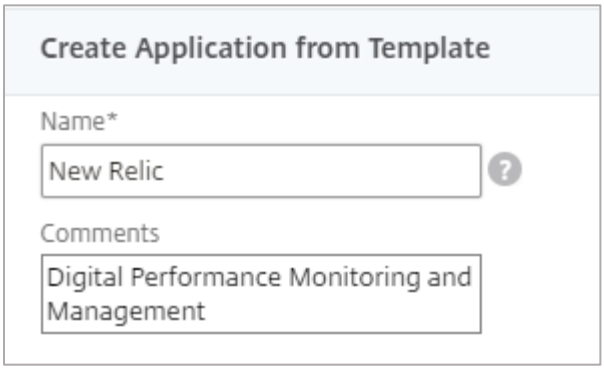
7. Click **SaaS** > **Continue**.



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



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.



Note:

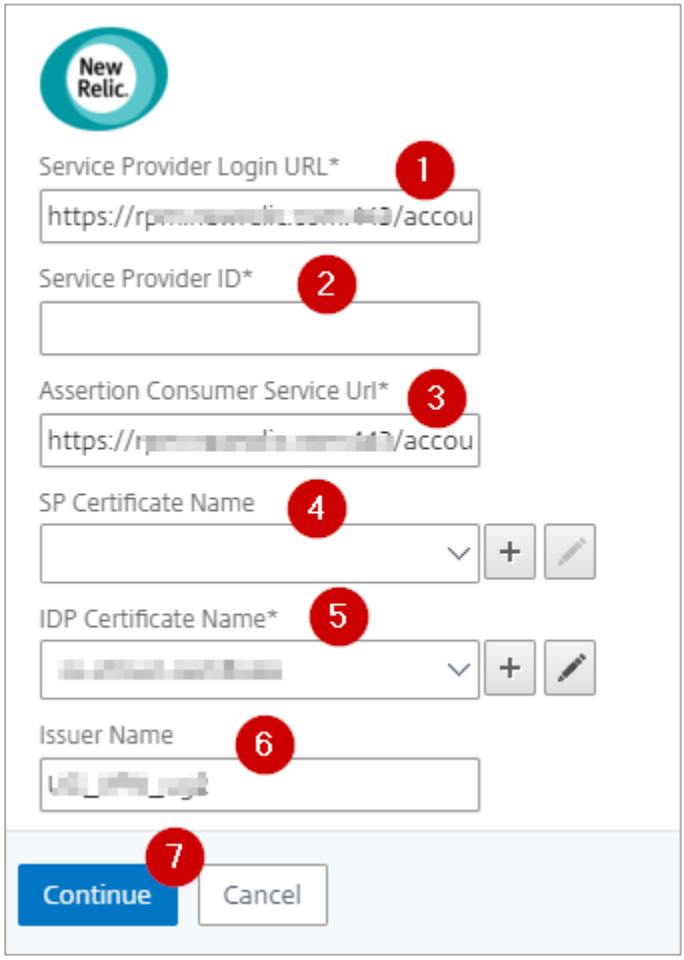
An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

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:



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.

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