

**Last Modified:** March 9, 2016

New Relic offers a suite of software analytics tools used by developers, and operation teams to understand how applications are performing.

## Before You Begin

- Acquire an administrator account to both RSA SecurID Access and New Relic Pro edition.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the RSA SecurID Access Manual.

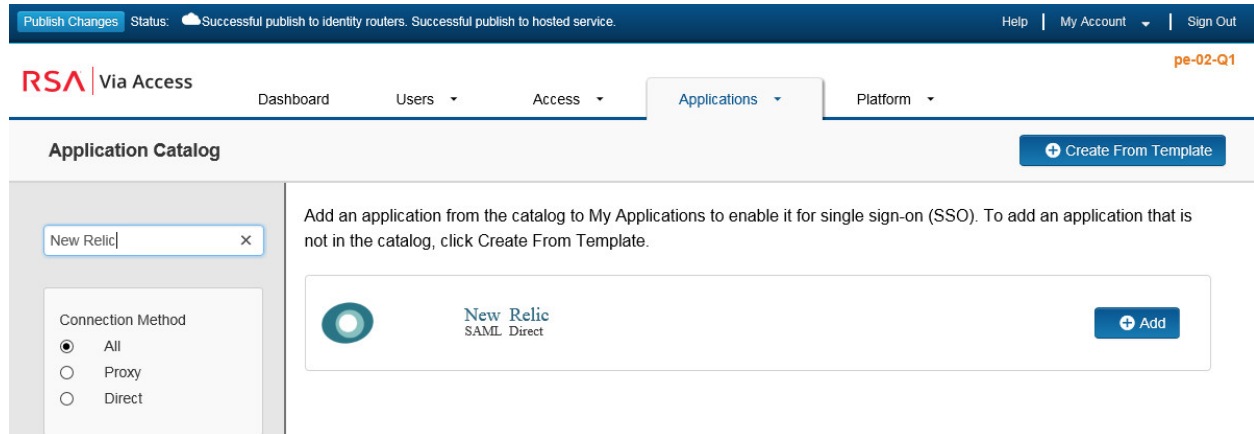
## Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure New Relic to Use RSA SecurID Access as an Identity Provider](#)

## Add the Application in RSA SecurID Access

### Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.



3. On the Basic Information page, specify the application name and click **Next Step**.

---

 **Note:** The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.

---

4. On the Connection Profile page, choose **IDP –initiated** and leave the URL blank.

### Connection URL


IDP-initiated  SP-initiated

Binding Method for SAML Request

Redirect


POST


Signed

 No certificate loaded

5. Scroll down to the **SAML Identity Provider (Issuer)** section.


### SAML Identity Provider (Issuer)

Identity Provider URL 


Issuer Entity ID 

Default (idp\_id): newrelictest

Override

SAML Response Signature 

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded   

Certificate Loaded

CN=gs.local, Valid Until:  
12/10/2019

Include Certificate in Outgoing Assertion

- a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the New Relic.
- b. Select **Choose File** and upload the RSA SecurID Access private key.
- c. Select **Choose File** and upload the RSA SecurID Access public certificate.
- d. Select the check box **Include Certificate in Outgoing Assertion**.

6. Scroll down to the **Service Provider** section.

## Service Provider

Assertion Consumer Service (ACS) URL ?

`https://rpm.newrelic.com:443/accounts/<your_accountnumber>/sso/saml/finalize`

Audience (Service Provider Entity ID) ?

`rpm.newrelic.com`

- a. In the **Assertion Consumer Service (ACS) URL** field, replace **<your\_accountnumber>**. Example:  
<https://rpm.newrelic.com:443/accounts/1265280/ssp/saml/finalize>
  - b. In the **Audience (Service Provider Entity ID)** field, enter **rpm.newrelic.com**.
7. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

## User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

8. Click **Show Advanced Configuration** and scroll down to **Uncommon Formatting SAML Response Options**.
9. Under Sign Outgoing assertion, select **Assertion within response**.

## Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

Entire SAML response  Assertion within response

Signature Algorithm `rsa-sha1`

Digest Algorithm `sha1`

Encrypt Assertion ?

**▲** No certificate loaded

Choose File

Encryption Algorithm `Triple DES`

Encryption Key Transport `RSA15`

Relay State URL Encoding

Send encoded URL in outgoing assertion ?

Include Issuer NameID Format

NameID Format `Unspecified`

10. Click **Next Step**.

11. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

## User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


12. Click **Next Step**.

13. On the **Portal Display** page, select **Display in Portal**.

14. Click **Save and Finish**.

15. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

## Next Steps

[Configure New Relic to Use RSA SecurID Access as an Identity Provider](#)

# Configure New Relic to Use RSA SecurID Access as an Identity Provider

## Procedure

1. Login to New Relic with an admin account. <https://login.newrelic.com/login>
2. Under your company name in the upper right corner, select **Account setting**.
3. Select **ACCOUNT > Summary** and select **Add user**.
4. Enter the user's email address and role type then click **Add this user**.
5. The user will be sent an email. The user must click the link in the email to activate their account.

Name	Email	Job title	Role
Gina Salvazo	gsalvalzo@pe-lab.com	Web Developer/Engineer	Owner
Gina Salvazo_2	gina.salvalzo@rsa.com	Web Developer/Engineer	Admin
tim bergeron	tim@pe-lab.com	Web Developer/Engineer	User

6. From the left side menu, select **AUTHENTICATION > Single sign-on**.

**SAML** 1 — 2 — 3  
CONFIGURE TEST ENABLE

● Configured but not yet tested.

**New Relic SAML service provider details**

Metadata URL	https://rpm.newrelic.com/accounts/1265280/sso/saml/metadata
SAML Version	2.0
Assertion Consumer URL	https://rpm.newrelic.com:443/accounts/1265280/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

• Upload a new certificate  
Browse files...

**Your SAML identity provider details**

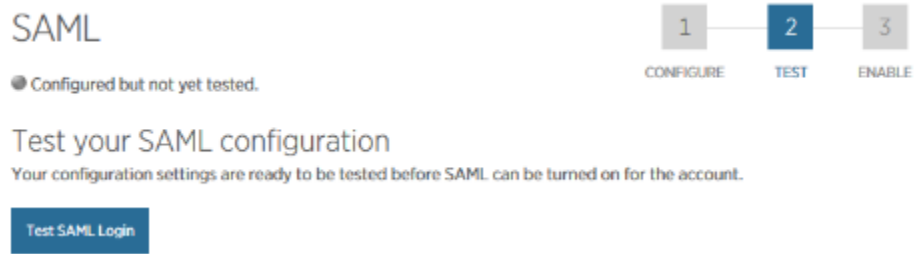
• Remote login URL

Logout landing URL (optional)

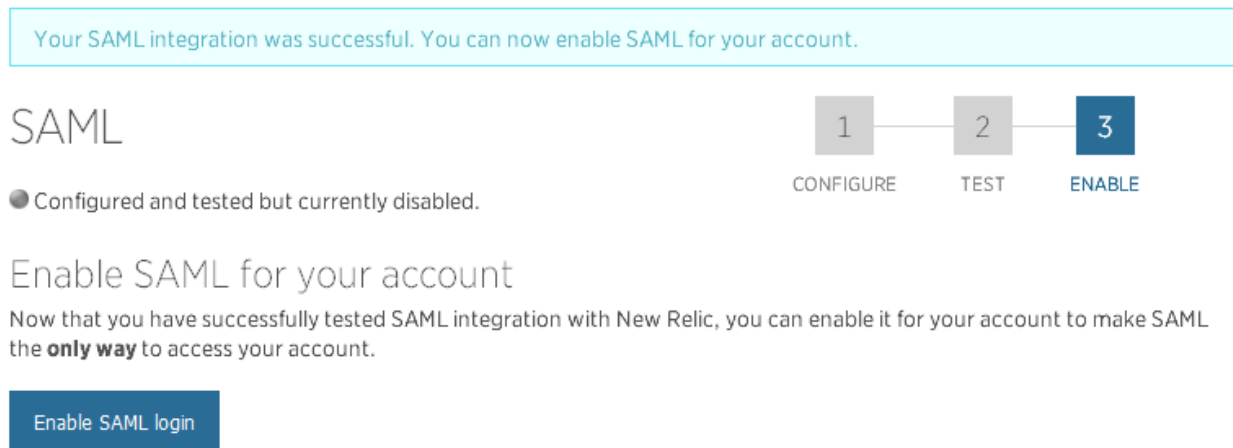
7. On the SAML page, select the **Browse files** and upload the RSA public certificate.
8. In the **Remote login URL** field, enter the Identity Provider URL from page 2 step 5.
9. Click **Save my changes**.

10. The SAML test page will appear.

11. Click **Test SAML Login**.



12. Once the test is successful, **click Enable SAML Login**.



13. Select **Add User**.

14. Select **Enable SAML login**.