Configuring New Relic

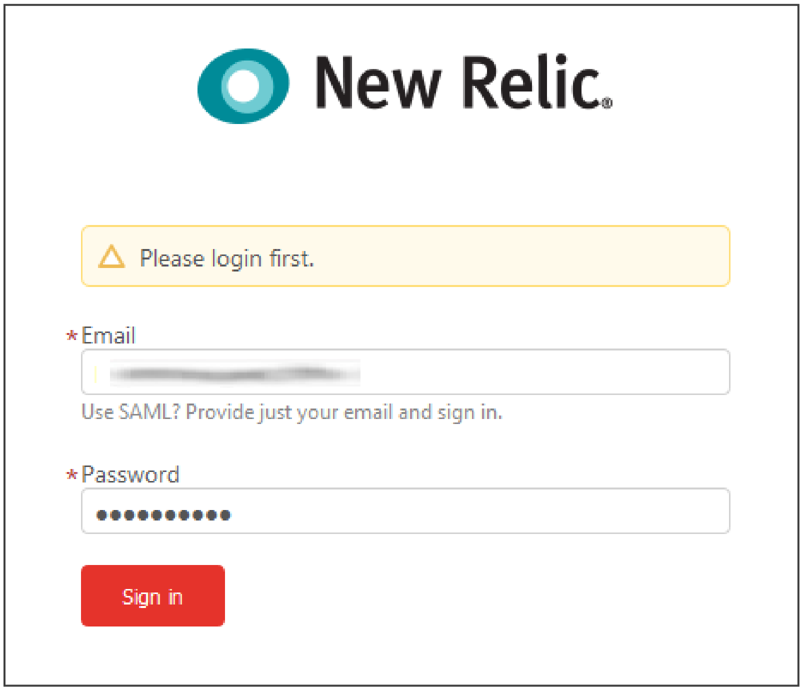
Configuring New Relic for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to New Relic by using the enterprise credentials.

Prerequisite
Browser Requirements: Internet Explorer 11 and above

To configure New Relic for SSO by using SAML:

1. In a browser, type https://newrelic.com/ and press **Enter**.

2. Type your New Relic admin account credentials (**Email** and **Password**) and click **Sign in**.



△ Please login first.

*Email

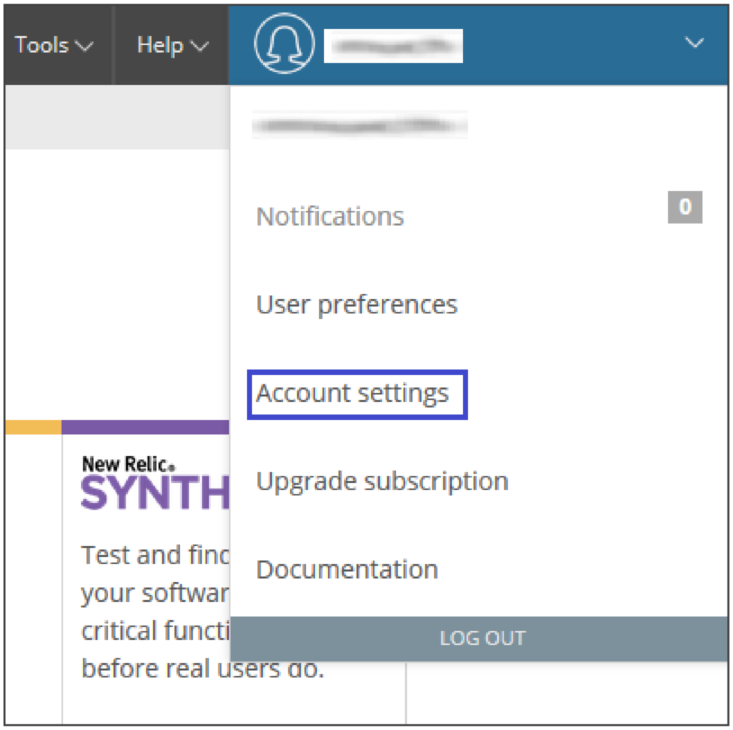
[redacted]

Use SAML? Provide just your email and sign in.

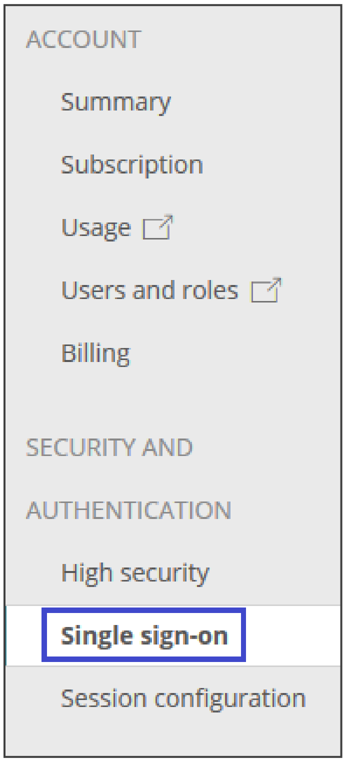
*Password

●●●●●●●●●●●

3. Click the user profile icon present at the top-right corner of the dashboard and select **Account Settings** from the drop-down menu.

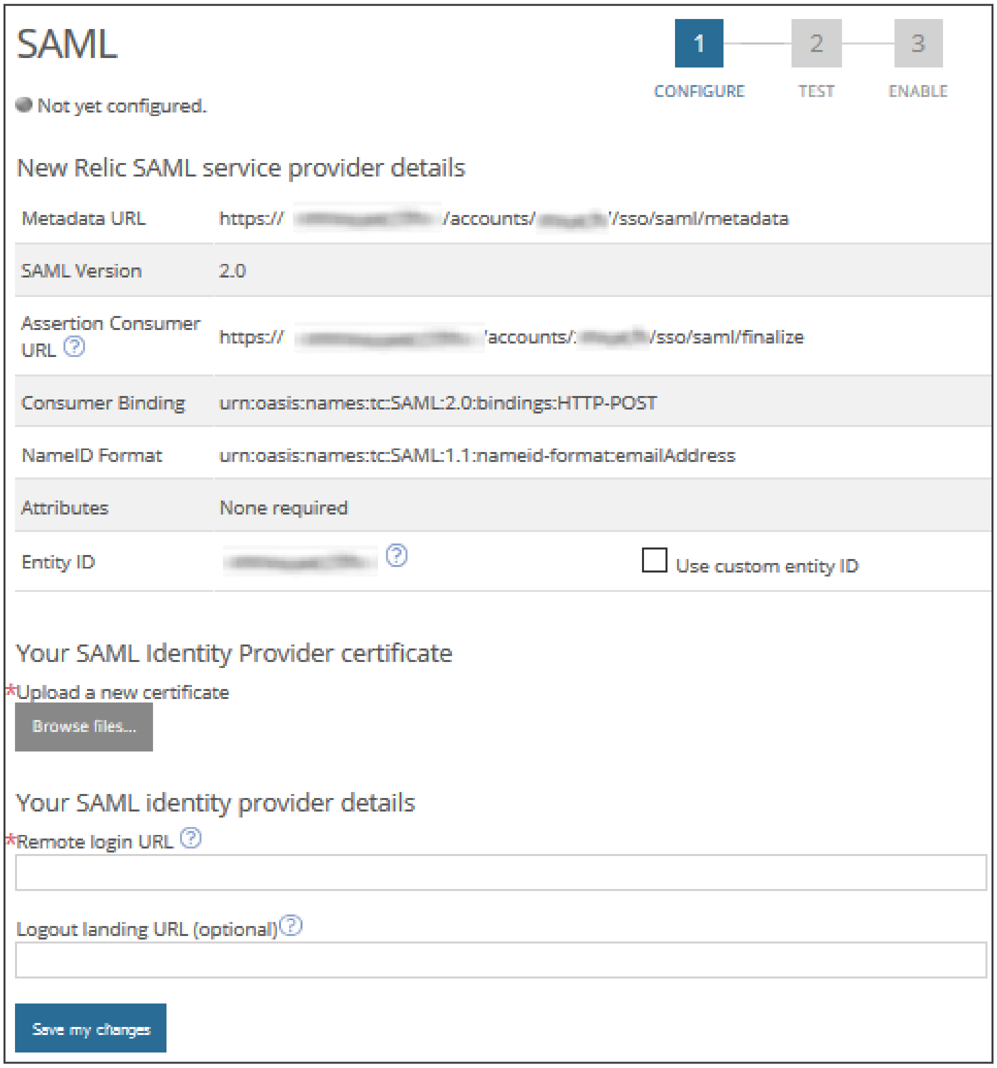


4. In the left panel, select **Single sign-on** under **SECURITY AND AUTHENTICATION**.



5. In the **SAML** section, enter the values for the following fields.

Field Name	Description
Upload a new certificate	Select **Browse files** and upload the IdP certificate. The IdP certificate must begin and end with - - - - -Begin Certificate- - - - - and - - - - -End Certificate- - - - - **Note**: The IdP Certificate is provided by Citrix and can be accessed from the following link: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml
Remote login URL	IdP logon URL
Logout landing URL	IdP logout URL



SAML

● Not yet configured.

New Relic SAML service provider details

Metadata URL	https:// [redacted] /accounts/ [redacted] /sso/saml/metadata
SAML Version	2.0
Assertion Consumer URL ⓘ	https:// [redacted] 'accounts/ [redacted] /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	[redacted] ⓘ □ Use custom entity ID

Your SAML Identity Provider certificate

*Upload a new certificate

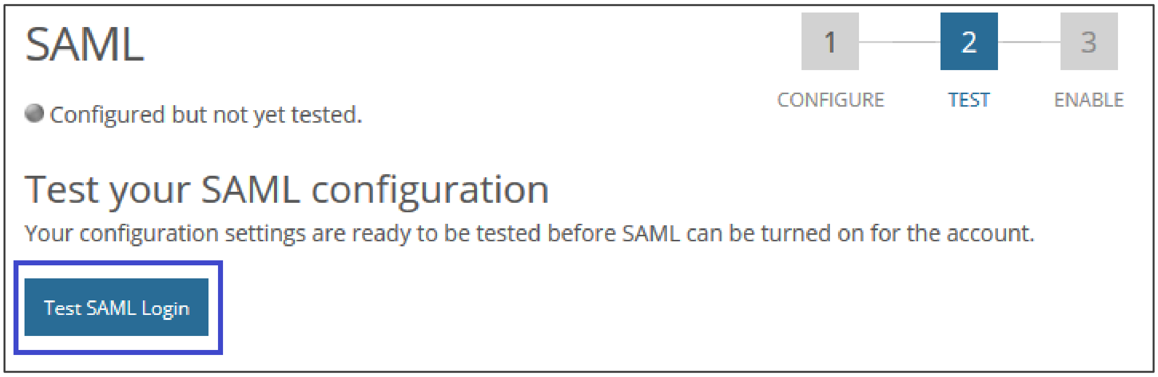
Your SAML identity provider details

*Remote login URL ⓘ

Logout landing URL (optional) ⓘ

6. Click **Save my changes**.

7. Click **Test SAML Login** to test the configuration of SAML.



SAML

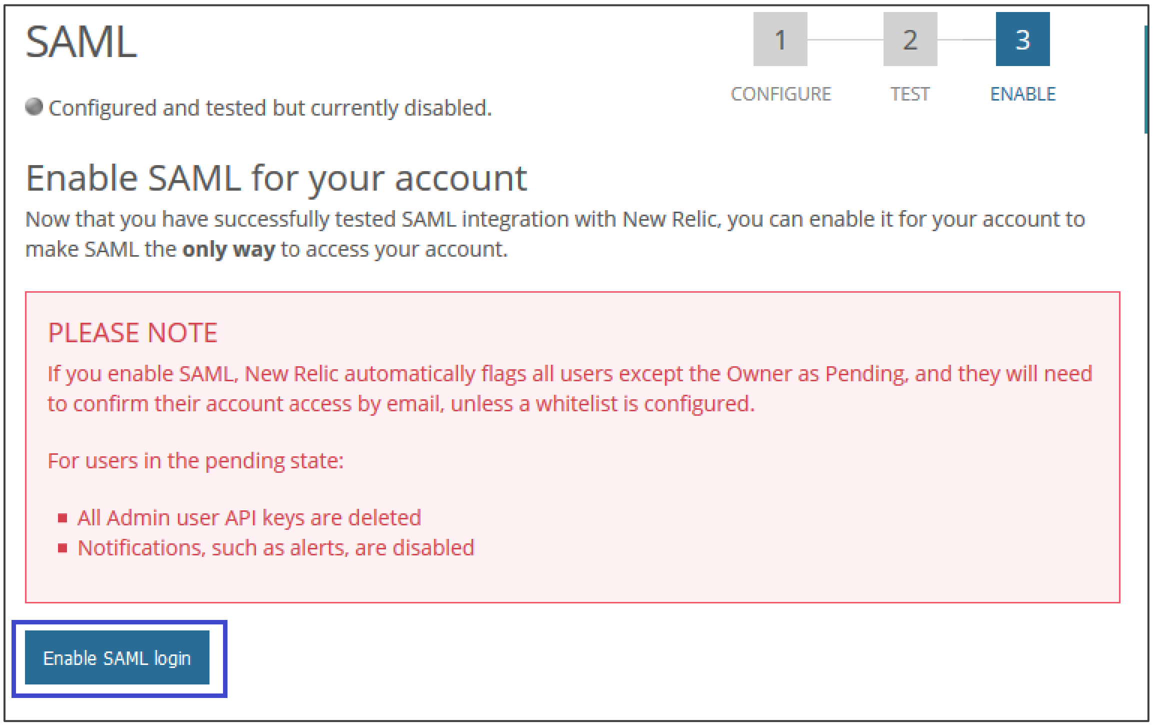
● Configured but not yet tested.

Test your SAML configuration

Your configuration settings are ready to be tested before SAML can be turned on for the account.

Note: After clicking the **TEST** tab, the testing of SAML configuration will be redirected to IdP. Once you provide the account credentials in Idp, it will be then redirected it to the New Relic website.

8. Click **Enable SAML login** to enable SAML configuration for the account.



SAML

● Configured and tested but currently disabled.

Enable SAML for your account

Now that you have successfully tested SAML integration with New Relic, you can enable it for your account to make SAML the **only way** to access your account.

PLEASE NOTE

If you enable SAML, New Relic automatically flags all users except the Owner as Pending, and they will need to confirm their account access by email, unless a whitelist is configured.

For users in the pending state:

- All Admin user API keys are deleted
- Notifications, such as alerts, are disabled