

Last Modified: April 4, 2016

Netskope provides enterprise cloud security software and cloud security products that enforce policies for maximum security and efficiency.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Netskope.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

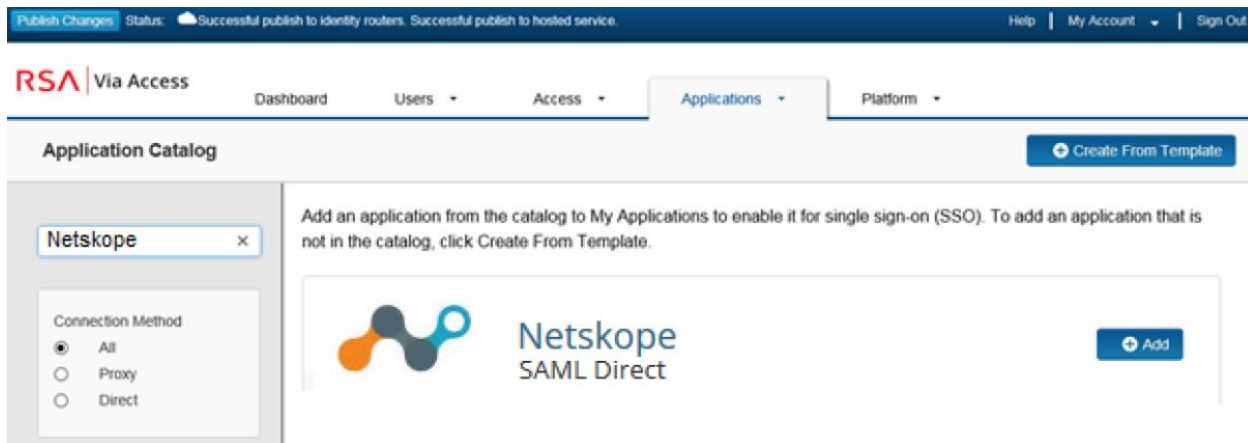
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Netskope 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 application that you wish to add. To add an application that is not in the list, click **+Create From Template**.



3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, select Import Metadata.
Select the file you downloaded from Netskope on page 6 step 4.


Connection Profile

Configure the relationship between the identity router, acting as the SAML identity provider (IdP), and the application, acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP options. You can edit these values if necessary.

No metadata loaded

Import Metadata




 **Note:** If the metadata file fails to import remove the -----BEGIN CERTIFICATE----- and ---END CERTIFICATE----- from the x.509 certificated section of the metadata file.

5. Click **Save** to import the metadata values.
6. In the SAML Workflow section, select **IDP-initiated**.

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

Initiate SAML Workflow

Connection URL 

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

Choose File

Generate Cert Bundle

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): nstest

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 Service Provider configuration.
- b. Take note of the **Issuer Entity ID**.
- c. Select **Choose File** and upload the private key.
- d. Select **Choose File** and upload the public certificate.

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

Service Provider

Assertion Consumer Service (ACS) URL 

Audience (Service Provider Entity ID) 

- a. In the **Assertion Consumer Service (ACS) URL** field, enter;
<https://partners.goskope.com/saml/acs>
 - b. In the **Audience (Service Provider Entity ID)** field, enter the Entity ID found on page 6 step 4.
9. Scroll down to the User Identity section. Set **Identifier Type** to **Email** and **Property** to **mail**.


User Identity

Name ID

Identifier Type




User Store

Property

 Show Advanced Configuration

10. Click **Show Advanced Configuration** and scroll down to **Attribute Extension**.
11. Add attributes **admin-role** and set the **Property** field.

Attribute Extension

Attribute Source	Attribute Name	Identity Source	Property	Manage
<input type="text" value="Constant"/>	<input type="text" value="admin-role"/>	<input type="text"/>	<input type="text" value="Tenant Admin"/>	 
 ADD				

12. If your account requires that your assertion be encrypted, Netskope will inform you and provide you with their certificate file; else leave the **Encrypt Assertion** box unchecked.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response Assertion within response

Signature Algorithm

Digest Algorithm

- Encrypt Assertion ?

Certificate Loaded

CN=samlidp.partners.goskope.com,
Valid Until: 07/25/2024

Encryption Algorithm

Encryption Key Transport

Relay State URL Encoding

- Send encoded URL in outgoing assertion ?

- Include Issuer NameID Format

NameID Format

13. Click **Next Step**.

14. 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

15. Click **Next Step**.

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

17. Click **Save and Finish**.

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

Status:  Changes Pending

Configure Netskope to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login into the Netskope administration console; <https://partners.goskope.com>
2. Click the gear icon in the upper right and select **Settings**.
3. Select **ADMINISTRATION > SSO**.
4. Click **Download Netskope Metadata**. This will be imported in the RSA Via Access.

The screenshot displays the Netskope administration console interface. At the top, there is a navigation bar with the Netskope logo and several menu items: Dashboard, Analytics, Introspection, Policies, Skope IT™ (with a warning icon), Cloud Confidence Index, and Reports. Below this is a secondary navigation bar with tabs for ADMINISTRATION (selected), ACTIVE PLATFORM, DISCOVERY, INTROSPECTION, INCIDENT MANAGEMENT, MANAGE, and TOOLS. The main content area is titled "SSO" and contains the following information:

- SSO**
The Netskope SSO integration allows organizations to use an Identity Provider (IdP) for authentication and authorization. Strong authentication mechanisms like multi-factor authentication can be used by the organization with their IdP. This results in a stronger authentication before an administrator can access the Netskope UI.
- Netskope supports SSO using SAML2.0 and only the Service Provider (SP) initiated flow.
- Netskope Settings**
When configuring the Netskope app in the IdP, use the following settings:

A list of settings is provided, each with an information icon (i) and a value:

- Assertion Consumer Service URL: <https://partners.goskope.com/saml/acs>
- Service Provider Entity Id: `nxuvJeSPD7r7t8P7u3e`
- Netskope Single Logout Service Response URL: <https://partners.goskope.com/saml/logoutResponse>
- Netskope Single Logout Service Request URL: <https://partners.goskope.com/saml/logoutRequest>
- Netskope SAML Certificate: [Download](#)

Below this list is a blue button with a download icon and the text "Download Netskope Metadata".

The next section is titled "SSO/SLO Settings" and includes the following text: "The configuration items are available from your IdP. Netskope needs to validate the SAML Assertion with the public key provided for your company by the IdP."

A list of SSO/SLO settings is provided, each with an information icon (i) and a value:

- SSO Enabled: **No**
- IdP URL: https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=nstest
- IdP Entity ID: `nstest`
- IdP Certificate: **A certificate has been uploaded**
- SLO Enabled: **No**
- Sign SLO Request/Response: **No**
- IdP SLO URL: **Not yet configured**

At the bottom of this section is an orange button with the text "Settings".

5. Select **Settings** on the bottom of the page.

6. Check the **Enable SSO** box.

SSO

Enable SSO

IdP URL

IdP Entity ID

IdP Certificate

SLO

Enable SLO

Sign SLO Request/Response

IdP SLO URL

7. Enter the **IDP URL** from page 3 step 7.
8. Enter the **IdP Entity ID** from page 3 step 7.
9. Paste the RSA SecurID Access public certificate in the **IdP Certificate** window.
10. Click **Submit**.