RSA SecurID Access SAML Configuration for Netskope

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.

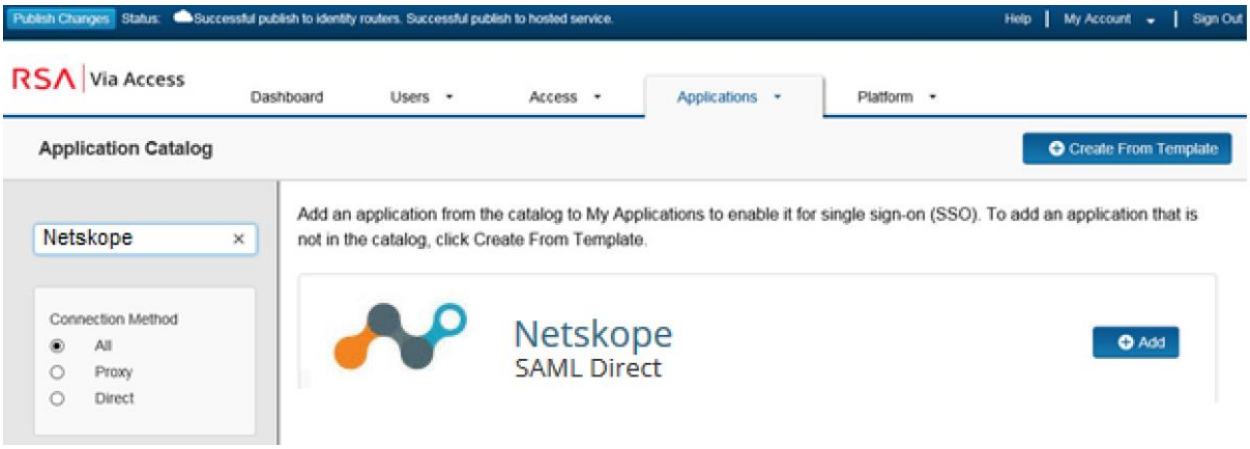
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Netskope to Use RSA SecurID Access as an Identity Provider

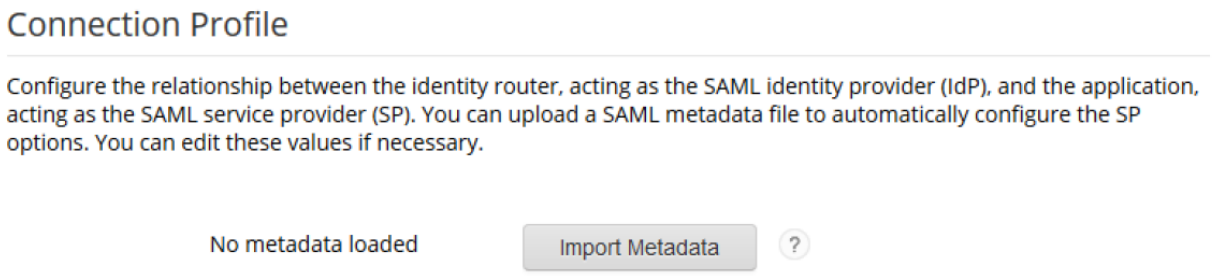
Add the Application in RSA SecurID Access

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**.



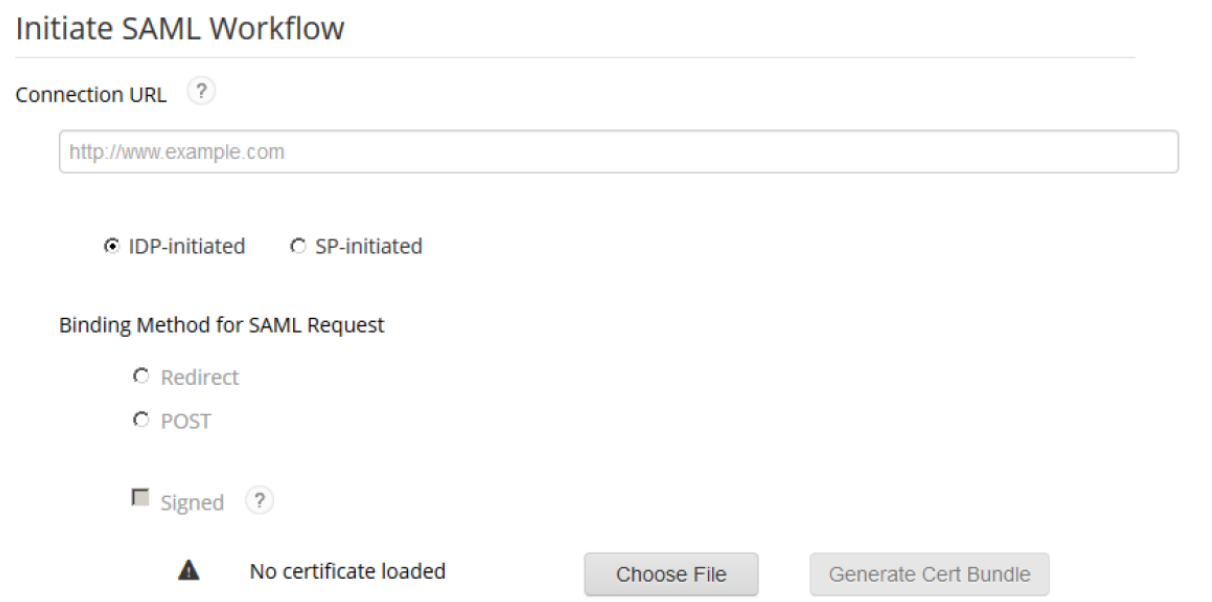
3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, select Import Metadata.
   Select the file you downloaded from Netskope on page 6 step 4.



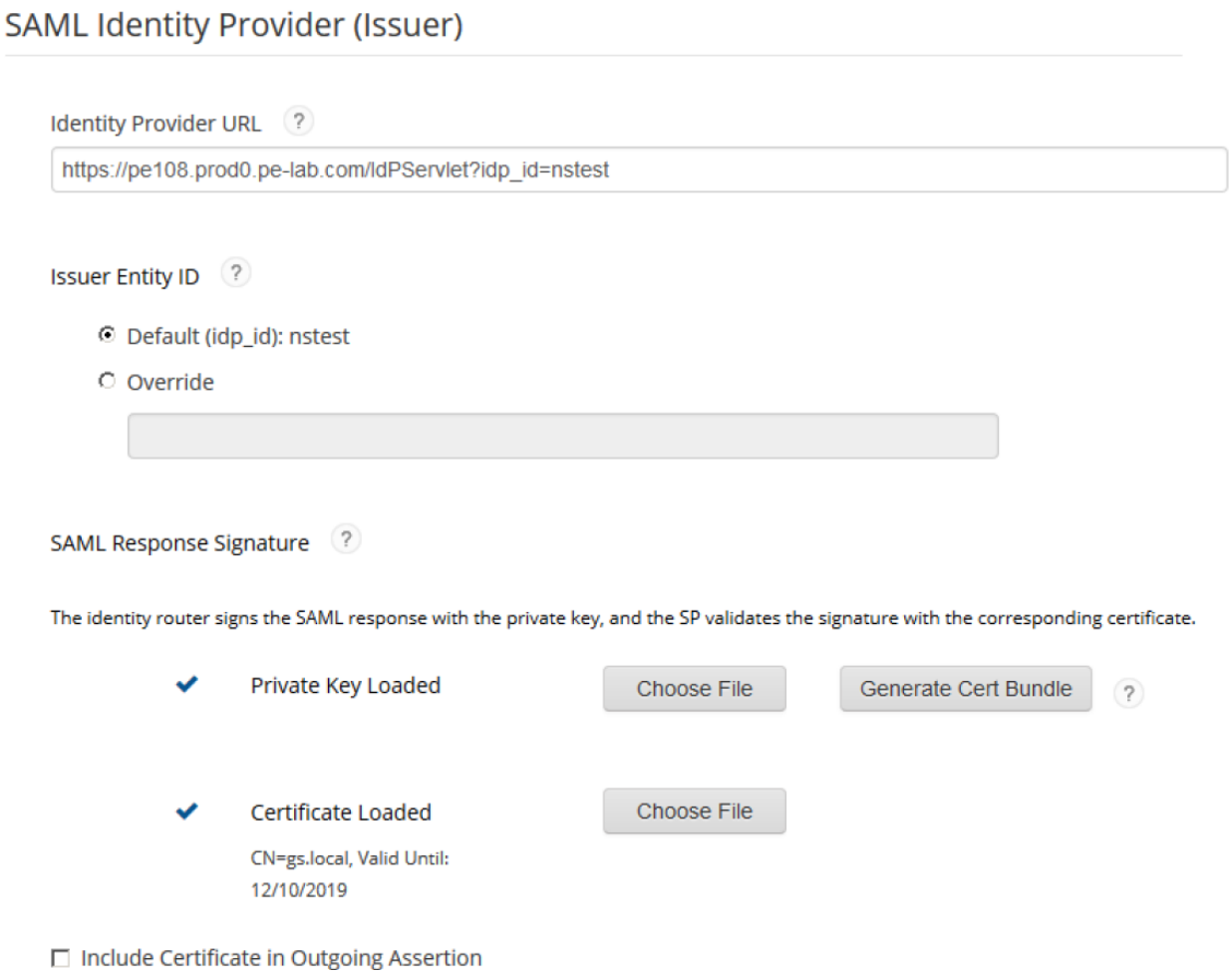
Note: If the metadata file fails to import remove the -----BEGIN CERTIFCATE---- and ---END CERTIFICATE----- from the x.509 certificated section of the metadata file.

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.



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

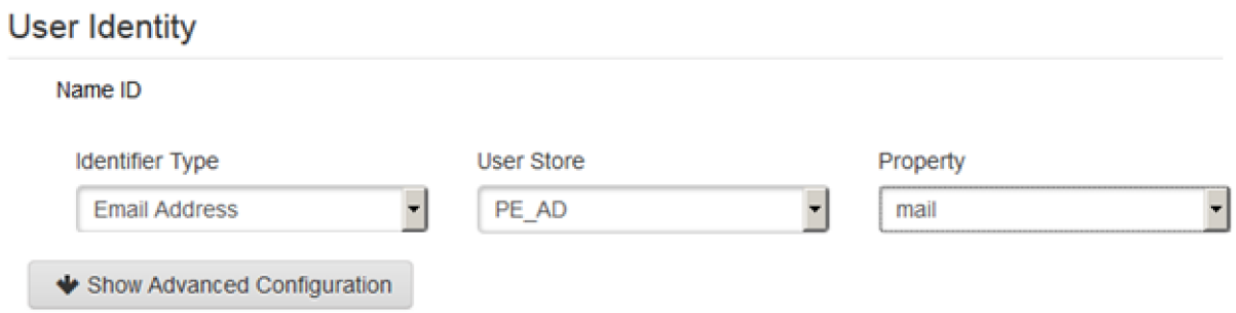


   a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Service Provider configuration.
   b. Take note of the **Issuer Entity ID**.
   c. Select **Choose File** and upload the private key.
   d. Select **Choose File** and upload the public certificate.

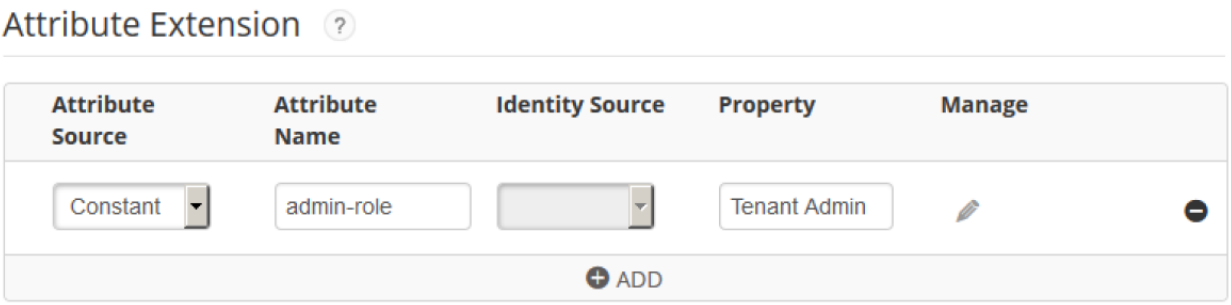
8. Scroll down to the **Service Provider** section.

   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.

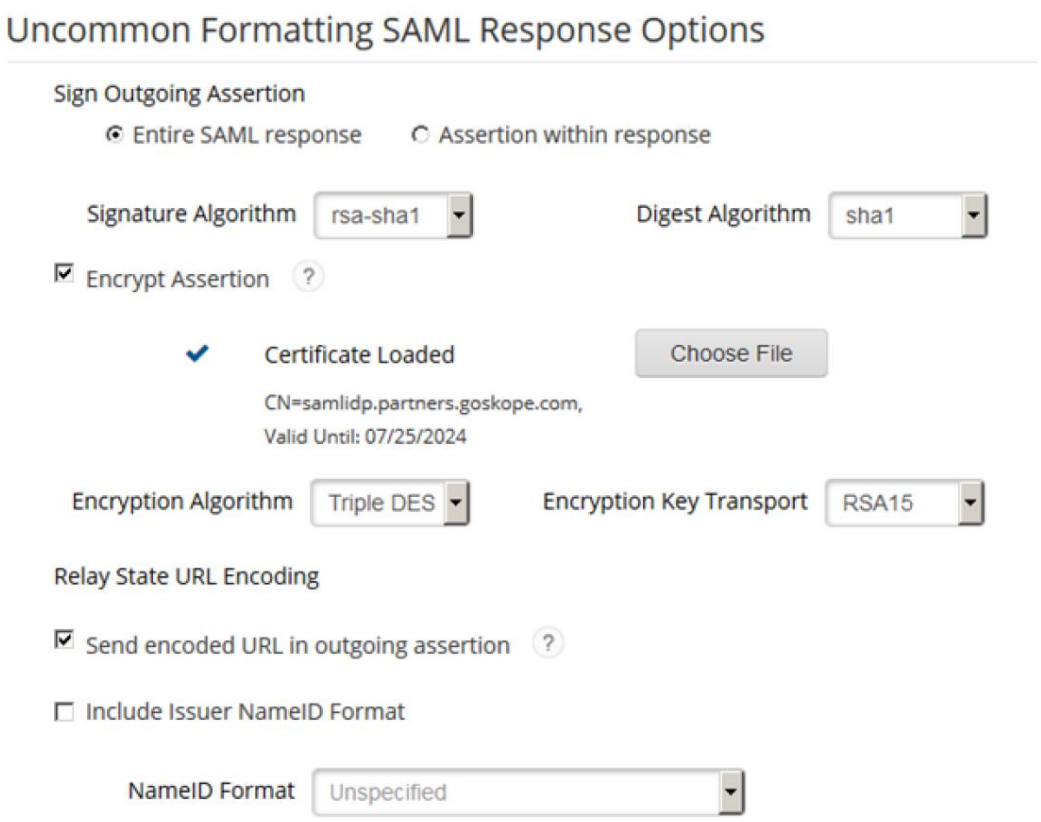
9. Scroll down to the User Identity section. Set **Identifier Type** to **Email** and **Property** to **mail**.



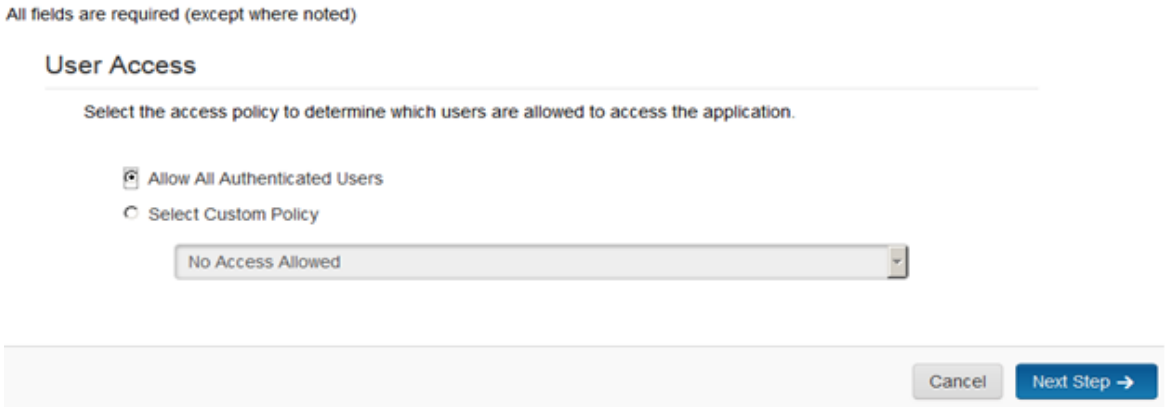
10. Click **Show Advanced Configuration** and scroll down to **Attribute Extension**.
11. Add attributes **admin-role** and set the **Property** field.



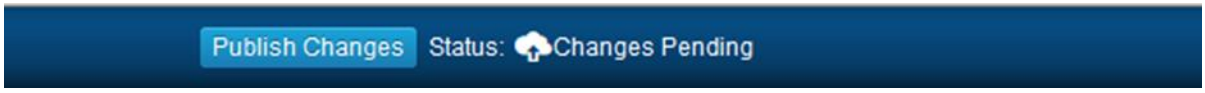
12. If your account requires that your assertion be encrypted, Netskope will inform you an dprovide you with their certificate file; else leave the **Encrypt Assertion** box unchecked.



13. Click **Next Step**.
14. On the **User Access** page, select the desired user policy from the drop down list.



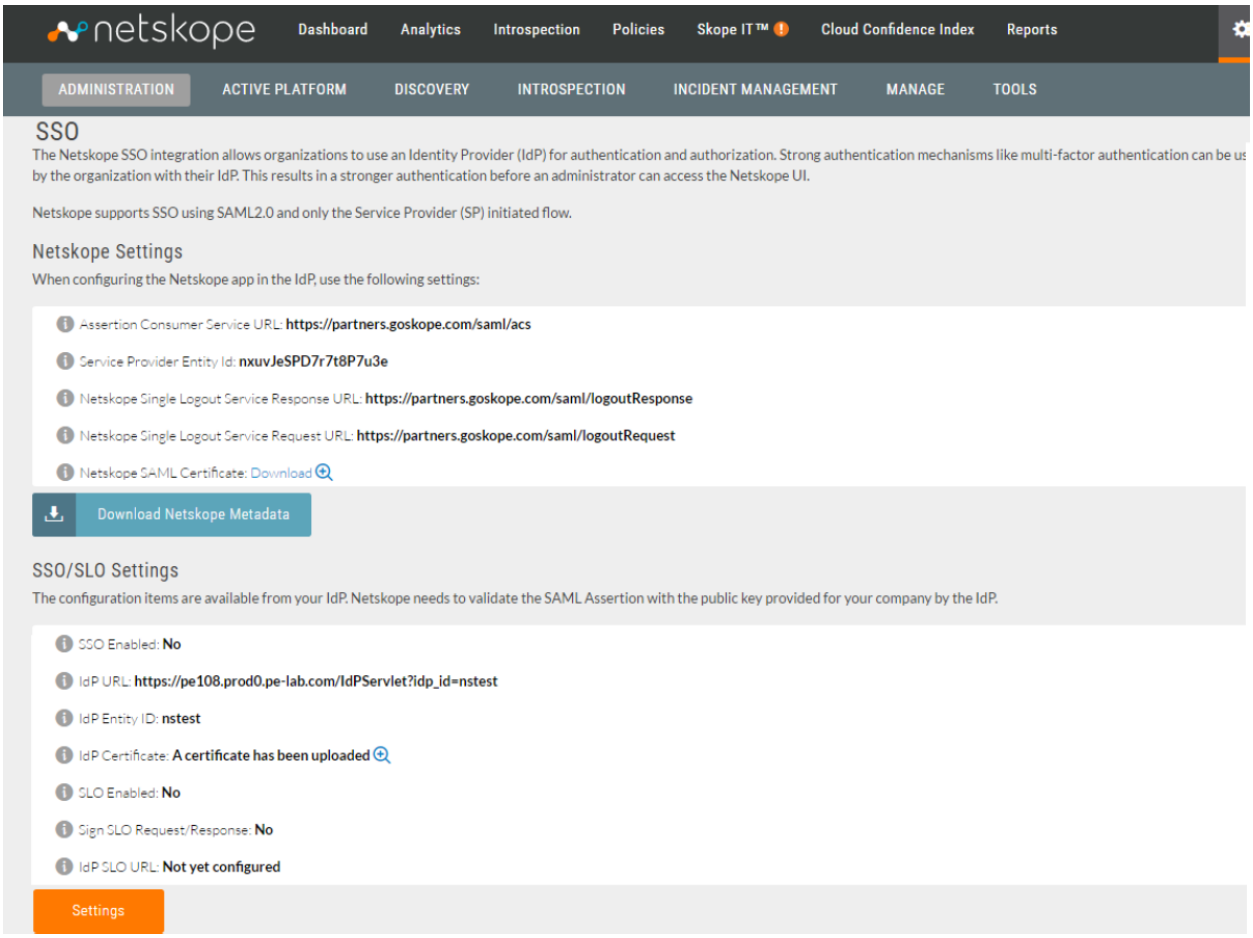
15. Click **Next Step**.
16. On the **Portal Display** page, select **Display in Portal**.
17. Click **Save and Finish**.
18. Click **Publish Changes**. Your application is now enabled for SSO.



Configure Netskope to Use RSA SecurID Access as an Identity Provider

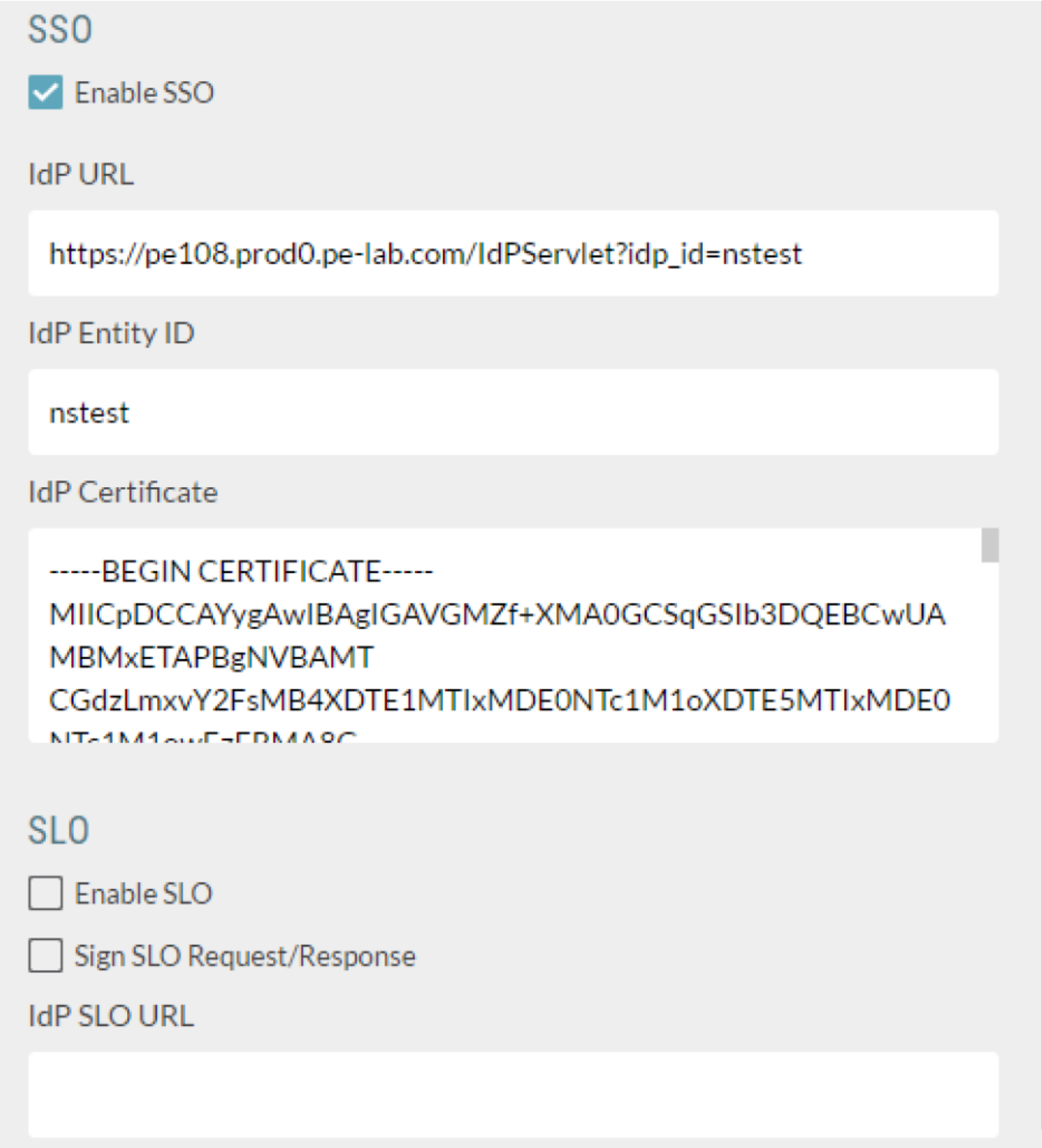
Procedure

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.



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

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



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**.

GLS