

Last Modified: May 18, 2018

Evernote Business makes the ideas, research and expertise of your team easily discoverable, creating an open, productive and smart workplace.

Before You Begin

- Acquire an Evernote Business account.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the RSA SecurID Access manual.

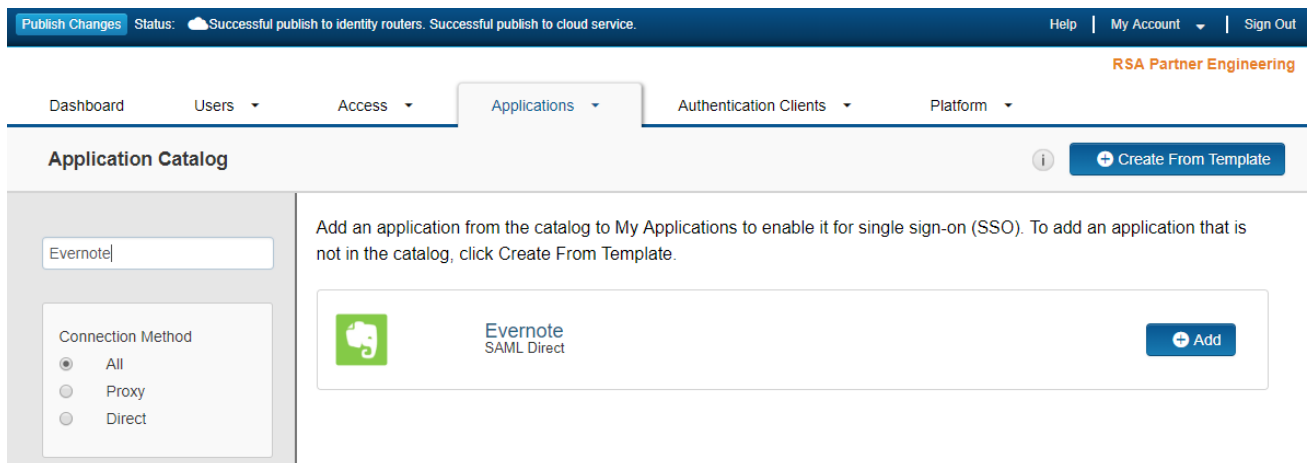
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Evernote 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.



3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, leave the URL blank and select **IDP -initiated**.

Connection Profile

Define the SAML connection for this application.

Connection URL


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

Choose File

Generate Certificate Bundle

5. Scroll down to **SAML Identity Provider (Issuer)** section.
6. Take note of the Identity Provider URL it will be needed to configure Evernote.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): evernote

Override

7. Click **Choose File** and upload the private key.

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

✓ Private Key Loaded

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion

⚠ No certificate loaded

Choose File

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://www.evernote.com/SamlConsumer.action>
 - b. In the **Audience (Service Provider Entity ID)** field, enter <https://www.evernote.com/saml2>
9. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

⌵ Show Advanced Configuration

- Click **Show Advanced Configuration** and scroll down to Uncommon Formatting SAML Response Options.
- Verify that **Send encoded URL in outgoing assertion** is unchecked.


Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

Entire SAML response
 Assertion within response

Signature Algorithm Digest Algorithm

Encrypt Assertion ?

 No certificate loaded

Encryption Algorithm Encryption Key Transport

Relay State URL Encoding

Send encoded URL in outgoing assertion ?

Include Issuer NameID Format

NameID Format

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

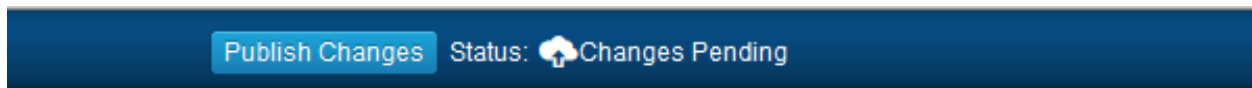
All fields are required (except where noted)

User Access

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

Allow All Authenticated Users
 Select Custom Policy

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



Next Steps

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

4. In the **SAML HTTP Request URL** field, enter the RSA SecurID Access Identity Provider URL.
5. In the x509 certification window paste the RSA SecurID Access public certification, including the Begin and End lines.
6. Click **Save & Enable**.
7. Navigate to **Admin Console > Add users**.
8. Enter manually invite users.