

**Last Modified:** December 16, 2014

Egnyte allows companies to securely access, share, and store files with business partners and employees in multiple offices as if they were in a single location, without using complex VPN services or dedicated FTP sites and FTP servers.

## Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Egnyte.
- Obtain the ACS URL information from Egnyte.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

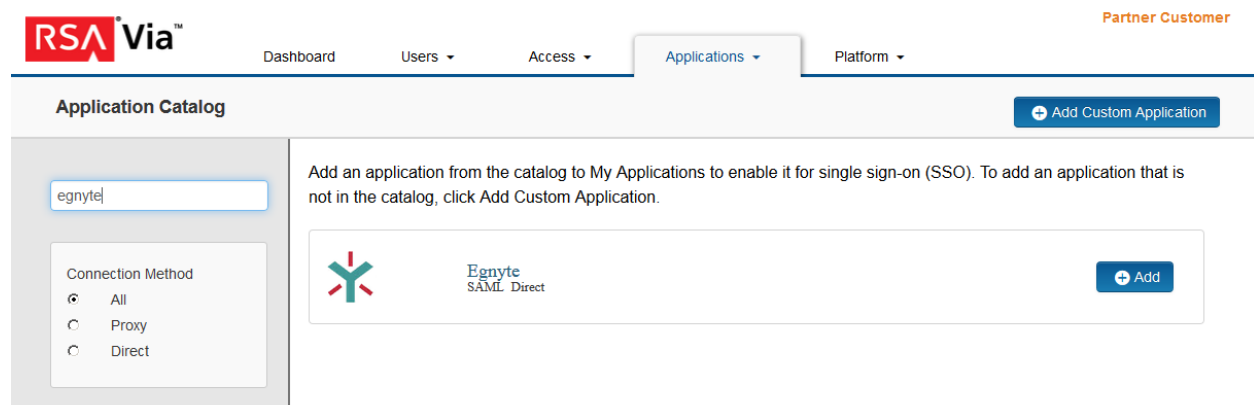
## Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Egnyte 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, select **Egnyte SAML Direct** and click **+Add**.



3. On the **Basic Information** page, specify the application name and click **Next Step**.
4. On the Connection Profile page, choose **IDP -initiated** if the user will be connecting to the RSA SecurID Access portal to access the application or **SP -initiated** if the user will be connecting from the Service Provides site.

---

 **Note:** When configuring for IDP -initiated leave the Connection URL blank. When configuring for SP -initiated enter <https://saml-auth.egnyte.com> in the Connection URL field.

---

#### Connection URL

IDP-initiated    SP-initiated

Binding Method for SAML Request

Redirect

POST

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

#### SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp\_id): egnyte

Override

Certificate Bundle


The certificate bundle is required to ensure a secure transaction.

private.key

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion

 No certificate loaded

Choose File

- 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.

6. 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, replace %DOMAIN% with your Egnyte subdomain. <https://%DOMAIN%.egnyte.com/samlconsumer/RSA>
  - b. In the **Audience (Service Provider Entity ID)** field, replace %DOMAIN% with your Egnyte subdomain. <https://%DOMAIN%.egnyte.com/samlconsumer/RSA>
7. Scroll down to the **User Identity** section. Set the Identifier Type to **Email** and Property to **mail**.

## User Identity

---

Name ID

Identifier Type

User Store

Property

8. Click **Next Step**.

9. 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 →

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

Publish Changes


Status:  Changes Pending

## Next Steps

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

## Configure Egnyte to Use RSA SecurID Access as an Identity Provider

### Procedure

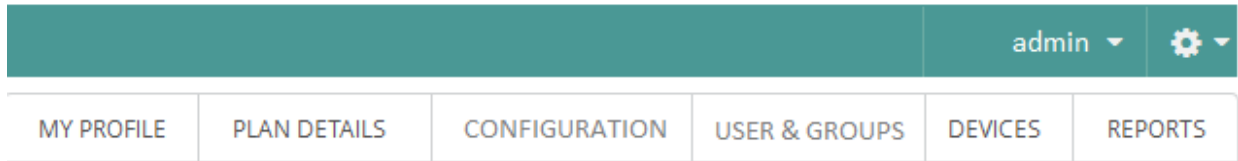
1. Login into the Egnyte administration console. <https://<CompanyAccount>.Egnyte.com/>
2. Select the gauge icon pull down  and choice **Settings**.
3. Navigate to **Security** from the left side menu.
4. On the Security page scroll down to the Single Sign-On Authentication section.

### Single Sign-on Authentication

Single sign-on authentication	<input type="text" value="SAML 2.0"/>
Identity provider	<input type="text" value="RSA"/>
Identity provider login URL	<input type="text" value="https://pe110.pe-lab.com/IdPServlet?idp_id=egnyte"/>
Identity provider entity ID	<input type="text" value="egnyte"/>
Identity provider certificate	<pre>MIICrTCCAZUCBgFAT+Rz7TA NBgkqhkiG9w0BAQsFADAa MRgwFgYDVQQDDA9zYWxl c2ZvcnNIX3NhbWwwHhcNM TMwODA1MTkxMTQ2WhcN</pre>
Default user mapping	<input type="text" value="Email address"/>
Use domain-specific Issuer value	<input type="text" value="disabled"/>

- a. From the Single sign-on authentication pull down select **SAML 2.0**.
- b. From the Identity provider pull down select **RSA**.
- c. In the **Identity provider login URL** field enter the Identity Provider URL from the RSA SecurID Access Application page.
- d. In the **Identity provider entity ID** field enter the Identity Provider Entity ID from the RSA SecurID Access Application page.
- e. In the **Identity provider certificate** field paste the public key without the ---BEGIN and ---END.
- f. From the Default user mapping pull down select **Email address**.
- g. Click **Save**.

5. Select the **USERS & GROUPS** tab.



6. Add a user by select the **Add** button.
7. Enter the First Name, Last Name, Email, Username for the user.
8. Select the User role from the pull down.
9. In the Authentication Type field select **Single Sign-On** from the pull down.
10. Enter the Idp Username for user. This will be just the username without the domain.
11. Click **Save**.

### New Power User

First Name	<input type="text" value="tim"/>
Last Name	<input type="text" value="salvalzo"/>
Email*	<input type="text" value="tim@pe-lab.com"/>
Username*	<input type="text" value="tim"/>
User role	<input type="text" value="Default"/>
Authentication Type	<input type="text" value="Single Sign-On"/>
IdP Username	<input type="text" value="tim"/>
	<input type="checkbox"/> Add custom message to email

[Cancel](#)