

**Last Modified:** March 24, 2015

Zoho is a cloud based team collaboration site offering a suite of business apps. Zoho provides services for Email hosting, Collaboration Apps, Business Apps and Productivity Apps.

## Before You Begin

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

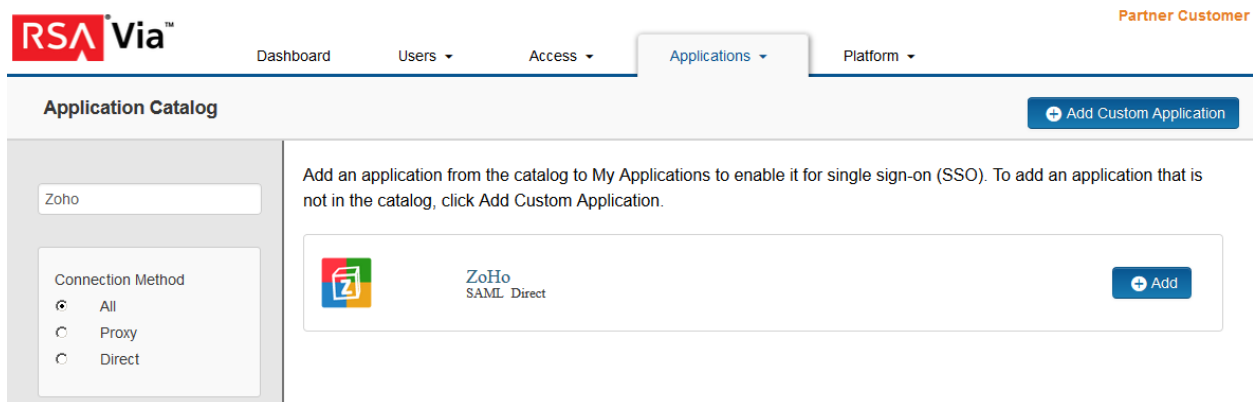
## Procedure

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

---

 **Note:** The following **SP -initiated** configuration will work for both **SP-initiated** and **IDP-initiated** connections.

---

4. In the **Connection URL** field enter the Zoho portal url from page 6, step 12.
5. Choose **SP -initiated** and binding method **POST**.

### Connection URL

---


IDP-initiated     SP-initiated

#### Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

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

### SAML Identity Provider (Issuer)

---

Identity Provider URL

Issuer Entity ID

Default (idp\_id): zohotest

Override

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

#### 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

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

#### Service Provider

Assertion Consumer Service (ACS) URL

https://accounts.zoho.com/samlresponse/<mydomain>.com

Audience (Service Provider Entity ID)

zoho.com

- a. In the **Assertion Consumer Service (ACS) URL** field, enter your ACS URL by replacing the <mydomain>.com with your site domain.  
<https://accounts.zoho.com/samlresponse/pe-lab.com>
- b. In the **Audience (Service Provider Entity ID)** field, enter **zoho.com**.

10. 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

11. Click **Next Step**.

12. 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 →


13. Click **Next Step**.

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

15. Click **Save and Finish**.

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

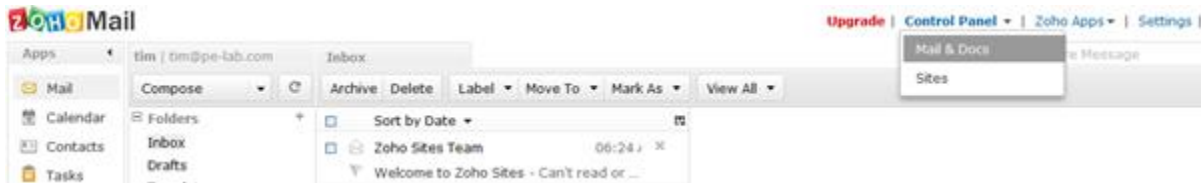
Publish Changes

Status:  Changes Pending

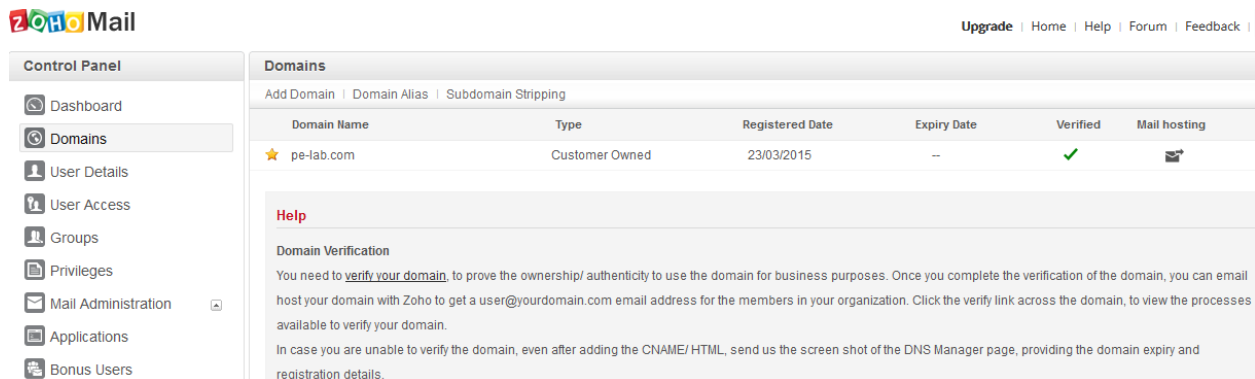
# Configure Zoho to Use RSA SecurID Access as an Identity Provider

## Procedure

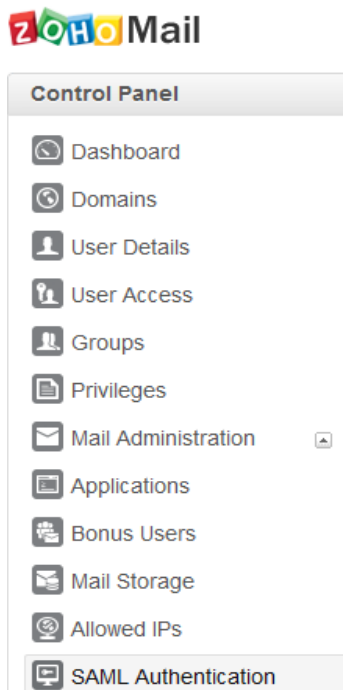
1. Login into the Zoho Apps administration console.  
<https://www.zoho.com/mail/login>
2. Go to **Control Panel > Mail & Docs**.



3. Select **Domains**.
4. Add and verify your domain.



5. Select **SAML Authentication**.



6. Under SAML Authentication Details, enter the **Login URL**.  
This is the Identity Provider URL from RSA SecurID Access on page 2, step 7.
7. Enter the **Logout URL**.
8. Enter the **Change Password URL**.
9. Select **Get key From File** and upload the public certificate.
10. Click **OK**.

**SAML Authentication Details**

Login URL :

Logout URL :

Change Password URL :

PublicKey :  [Get key From File](#)

Algorithm :

**Help**

**Login process**

1. Go to your portal URL ( say for example: mydomain.business.zoho.com )
2. Will be redirected to the SAML authentication page
3. The Authentication will be done on the IDP
4. Then the data will be encrypted and posted back to us
5. We will decrypt and find the authenticated user.
6. If the user is found in the same organization we will approve and set a ticket for that User.
7. If the user is present in a different organization, an error will be shown for the user.

11. Select **User Details** to add a user.

Add User | Import User | Export User(s) | Role | Location | Delete

User Details	Location	Phone No
<b>tim</b> tim@pe-lab.com	--	--

12. Select **Dashboard** to view your Portal URL.

**Control Panel**

- Dashboard
- Domains
- User Details
- User Access
- Groups
- Privileges
- Mail Administration

**Dashboard**

General | Locations | Two Factor Authentication | Delete Organization

**pe-lab.com**

pe-lab.com Portal URL : <https://mail.zoho.com/portal/pelab>

[2 User\(s\) Signed Up](#) Super Administrator : tim

[0 Organization Group\(s\) Created](#) Contact Email id : tim@pe-lab.com