

**Last Modified:** December 11, 2014

Zscaler ensures advanced security and policy compliance for all users, all devices and locations while simultaneously providing IT administrators in-depth visibility and control over all their user traffic.

## Before You Begin

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

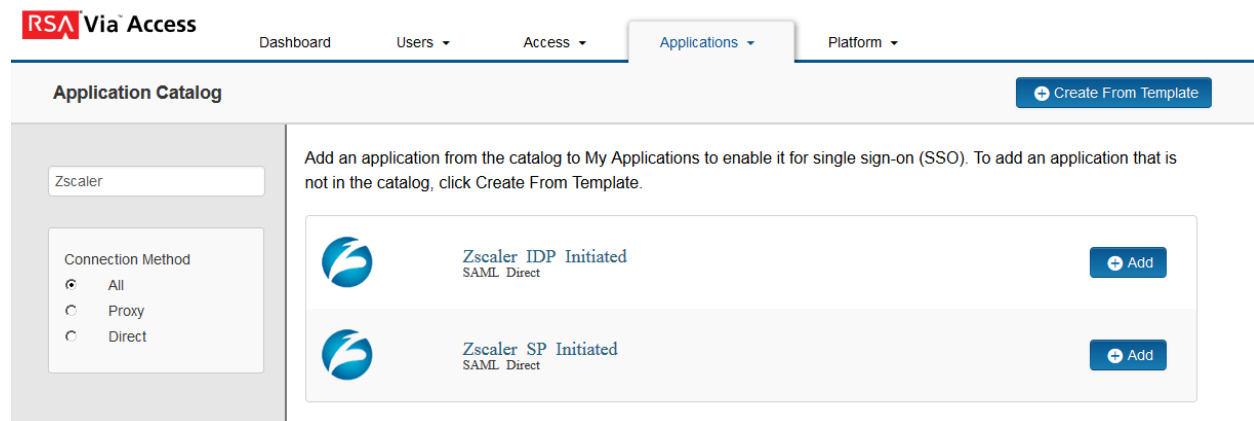
## Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Zscaler 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, search for Zendesk 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** and leave the URL blank.

## 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 the **SAML Identity Provider (Issuer)** section.

## SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp\_id): 1t8izzm20lth

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

https://login.zscalerbeta.net:443/sso\_upd/3797101

Audience (Service Provider Entity ID)

https://login.zscalerbeta.net

- a. In the **Assertion Consumer Service (ACS) URL** field, modify the URL with your Zscaler cloud name and your organization id. The **orgid** can be found in the organization's information page in the Zscaler Admin console.  
[https://login.<cloud-name>:443/sso\\_upd/<orgid>](https://login.<cloud-name>:443/sso_upd/<orgid>)
  - b. In the **Audience (Service Provider Entity ID)** field, enter the **Entity ID** to match the configured value from the Service Provider.
7. 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

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 Zscaler to Use RSA SecurID Access as an Identity Provider](#)

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

## Procedure

1. Login into the Zscaler administration console. <https://admin.zscalerbeta.net/policy/>
2. Navigate to **Manage Users & Authentication**.

The screenshot shows the Zscaler Administration console interface. At the top, there are navigation tabs: SECURE, MANAGE, COMPLY, MOBILE, ADMINISTRATION (highlighted), and ANALYTICS new. On the left is a sidebar menu with options like Organization Info, General Information, Subscription, Backup & Restore Policies, Print All Policies, Traffic forwarding, Internet Gateways & SSL, PAC File Hosting, Blacklisted IPs, Manage Administrators & Roles, Manage Users & Authentication, and Administrator Audit Trail. The main content area is titled 'Organization Information' and contains a table for 'Your Organization's General Information'.

Your Organization's General Information	
Organization ID	zscalerbeta.net-3797101
Organization Name	EMC
Domain Name	emc.com
Address #1	Your company HQ location address
Address #2	
City	City
State	State
ZIP Code	100100
Country	United States

3. Select the **View SAML Single Sign-on Parameters** link.

## Configure User Authentication

The screenshot shows the 'Configure User Authentication' settings page. It is divided into several sections:

- Choose Authentication Options for your Organization:**
  - Require Users to Authenticate (Users will be prompted for password): Every Session
  - Show Acceptable Usage Policy: Never
  - Authenticate using SAML Single Sign-On:  [View SAML Single Sign-On Parameters](#)
  - Authentication Option:  Hosted User Database,  Microsoft Active Directory,  OpenLDAP
- Hosted DB Password Options:**
  - Password Strength: None
  - There will be no restriction of the strength or complexity of passwords. But, only ASCII characters are all
  - Password Expiry: Never
- Manage End Users in Hosted user Database:**

	User ID	User Name	Group	Department	Comments
1	admin@emc.com	DEFAULT ADMIN	Service Admin	Service Admin	
2	zoey@emc.com	zoey@emc.com	IT	IT	

- In the Identity Provider section enter the Identity Provider URL you copied from the RSA SecurID Access Application page.

### Configure Single sign-on using SAML

Identity Provider (IDP) Options	
URL of the SAML Portal to which users are sent for authentication	<input type="text" value="https://pe110.pe-lab.com/IdPServlet?idp_id= zscaler"/>
Attribute containing Login Name	<input type="text" value="NameID"/>
Upload SSL Public Certificate	Currently Loaded Certificate : <input type="button" value="Browse"/>
Service Provider(SP) Options	
Sign SAML Request	<input type="checkbox"/>
Auto-Provisioning Options	
Enable SAML Auto-Provisioning	<input type="checkbox"/>
Attribute containing User Display Name	<input type="text"/>
Attribute containing Group Name	<input type="text"/>
Attribute containing Department Name	<input type="text"/>
<i>Note: Attribute for login name, User Display Name, Group and Department are case-sensitive</i>	

- Enter **NameID** in the **Attribute containing Login Name** field.
- Select **Browse** and upload your SSL public certificate.

---

 **Note: Refer to Zscaler documentation for Auto-Provisioning information.**

---


- Click **Close**.

8. Navigate to **Manage Users & Authentication** and click **+Add New End User**.
9. Fill in all required fields. The User ID must match the Active Directory email credentials used to login to the RSA SecurID Access portal.
10. Click **Done**.

## End User Management

Add New End User	
User ID	<input type="text"/> @ emc.com
User Name	<input type="text"/>
New Password	<input type="password"/> ?
Re-type New Password	<input type="password"/>
Group	<input type="text"/> <a href="#">Select</a>
Department	<input type="text"/> <a href="#">Select</a>
Comments	<input type="text"/>

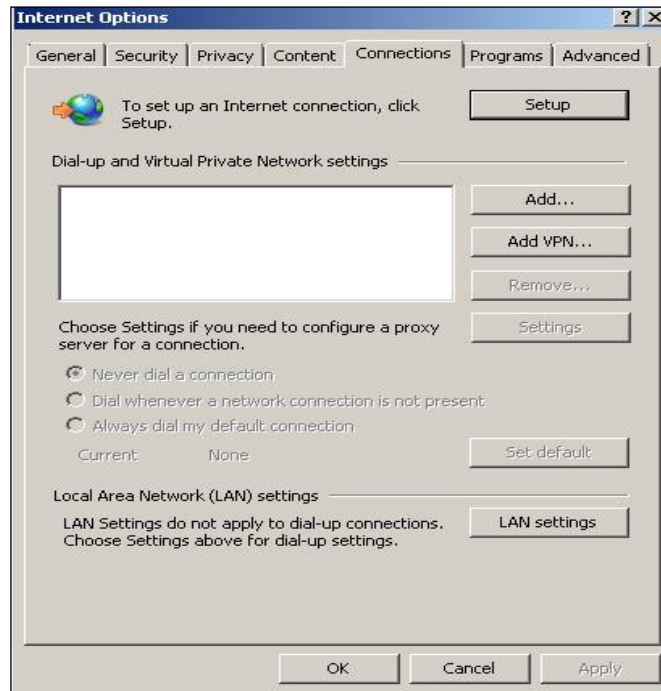
---

 **Note:** Please ensure the domain name in the email address is the same as the Zscaler admin logon-name. If your admin login is [admin@example.com](#), ensure that the username you send in the SAML response is of the format `user@example.com`.

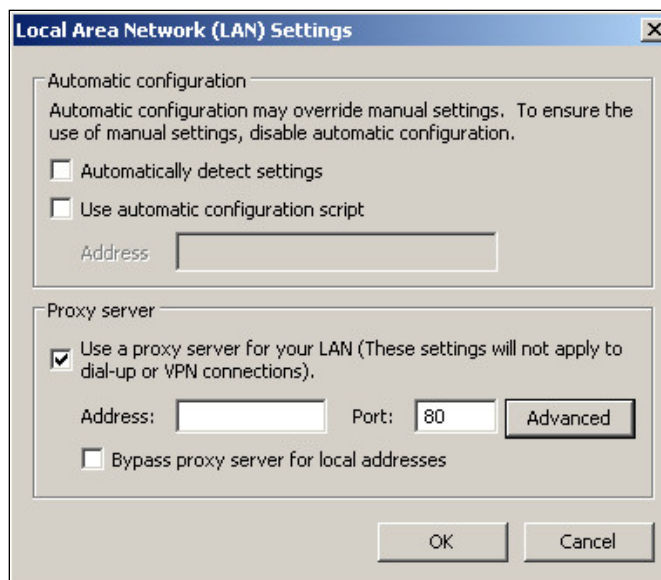
---

## Configure Proxy Settings on Browser

1. Open your browser and perform the following:
  - a. For Chrome, go to **Settings** tab and select **Change proxy settings**
  - b. For Internet Explorer, go to **Tools > Internet Options**.
2. Select **Connection** tab and click **LAN settings**.

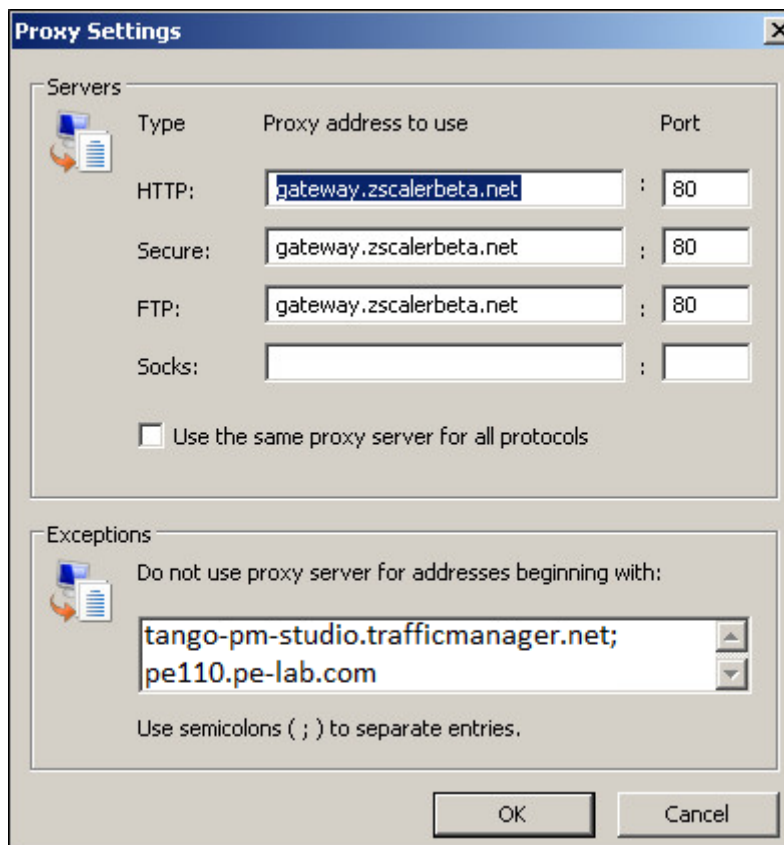


3. Disable **Automatically detect settings** and enable **Use a proxy server for your LAN**.






4. Select **Advanced** and enter the following:
  - a. Set **the Proxy address to use** fields to the correct gateway address that is relevant to your Zscaler cloud instance. In this example use **gateway.zscalerbeta.net**.
  - b. Set **Port** to the appropriate port that is relevant to your Zscaler cloud instance.
  - c. Enter the RSA SecurID Access instance and RSA SecurID Access portal in the Exception field.



5. Click **OK**.

---

 **Note:** The Exceptions URLs do not go through the Zscaler proxy server.

---