

Last Modified: January 26, 2015

Zendesk supports Secure Assertion Markup Language (SAML), which allows you to provide single sign-on (SSO) for your Zendesk users. Single sign-on is available to Zendesk Plus and Enterprise accounts.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Zendesk.
- Obtain the ACS URL information from Zendesk.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.
- Create the SHA1 fingerprint from the x.509 SAML certificate in PEM format.

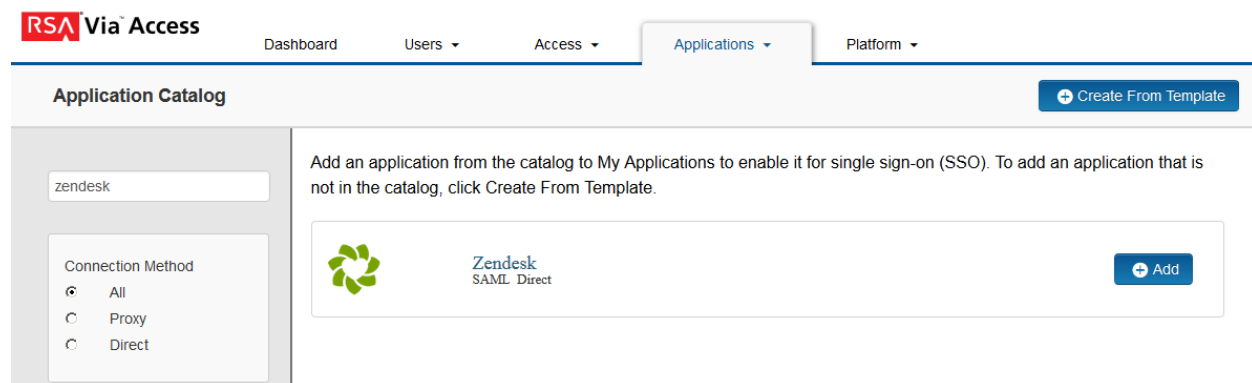
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Zendesk 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 **Zendesk 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, modify the URL for your site.
<https://<domain>.zendesk.com/login>
5. Choose **SP -initiated** and binding method **POST**.

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


Connection URL

https://<DOMAIN>.zendesk.com/login

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.

SAML Identity Provider (Issuer)

Identity Provider URL

https://pe110.pe-lab.com/IdPServlet?idp_id=zendesk

Issuer Entity ID

Default (idp_id): zendesk
 Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

private.key

Include Certificate in Outgoing Assertion

cert.pem

Certificate valid until: Sat Aug 05 19:11:46 UTC 2017

- a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Service Provider configuration.
- b. Select **Choose File** and upload the private key.
- c. Check **Include Certificate in Outgoing Assertion**, select **Choose File**, and upload the public certificate.

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

Service Provider

Assertion Consumer Service (ACS) URL

https://<DOMAIN>.zendesk.com/access/saml

Audience (Service Provider Entity ID)

zendesk.com

- a. In the **Assertion Consumer Service (ACS) URL** field, modify the URL with your company's Zendesk site domain. <https://<domain>.zendesk.com/access/saml>
 - b. In the **Audience (Service Provider Entity ID)** field, enter **zendesk.com**.
8. 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

9. Click **Next Step**.

10. 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 →


11. Click **Next Step**.

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

13. Click **Save and Finish**.

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

Publish Changes

Status:  Changes Pending

Create SHA1 fingerprint


1. To generate a SHA1 fingerprint of your SAML certificate you must use **openssl**.
2. Open your terminal or command prompt and navigate to the file location in which your cert.pem file resides.
3. Enter the following command in a terminal or command prompt (Windows users must install openssl) to obtain your SHA1 fingerprint:
`openssl x509 -sha1 -noout -fingerprint -in cert.pem`.
4. After entering the above command, your terminal or command window will display,
`SHA1 Fingerprint= yourSHA1_Fingerprint`.
5. Copy the value of your SHA1 fingerprint and paste it into a text editor for use later.

Next Steps

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

Configure Zendesk to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login into the Zendesk administration console.
2. Click the Admin icon  at the bottom of the sidebar.
3. Under the SETTINGS section, select **Security**.
4. Select the **Admins & Agents** or **End-users** tab.

 **Note:** In order for the SP-initiated workflow to work properly, Single Sign-On must be enabled for End Users.




5. Select the **Single sign-on (SSO)** option.

Security

Admins & Agents End-users Global

Administrator and agent sign-in authentication

By default, your administrators and agents are authenticated and signed in using Zendesk's user authentication. You can however bypass this and require your administrators and agents to sign in using Google or via single sign-on using Zendesk Remote Authentication or SAML (available in Plus and Enterprise).

<input type="radio"/>		Zendesk Admins and agents sign in with their Zendesk accounts.
<input type="radio"/>		Google Admins and agents use Google authentication to sign in to your Zendesk.
<input checked="" type="radio"/>		Single sign-on (SSO) Admins and agents use your SSO service to sign in to your Zendesk. Requires configuration.

6. Complete the **SAML SSO URL** and **Certificate Fingerprint** fields. All other fields are optional.



Single sign-on (SSO)

Admins and agents use your SSO service to sign in to your Zendesk. Requires configuration.

SAML

SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet. [Learn more.](#)

SAML SSO URL

This is the URL that Zendesk will invoke to redirect users to your Identity Provider. Note that our Assertion Consumer Service (ACS) URL is `https://rsa1.zendesk.com/access/saml/`

Remote logout URL

This is the URL that Zendesk will redirect your users to after they sign out, e.g. `https://www.yourcompany.com/services/zendesk_logout.asp`

IP ranges (optional)

Requests from these IP ranges will always be routed via remote authentication. Requests from IP addresses outside these ranges will be routed to the normal sign-in form. To route all requests through remote authentication, leave this blank. An IP range is in the format `n.n.n.n`, where `n` is a number or an asterisk (*) wild card. Separate multiple IP ranges with a space. Your current IP address is: `168.159.213.215`

Certificate fingerprint

- In the **SAML SSO URL** field enter the Identity Provider Entity ID URL you copied from the RSA SecurID Access Application page.
- Enter the **Certificate fingerprint** you created from the SAML certificate.