RSA SecurID Access SAML Configuration for Zendesk

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.

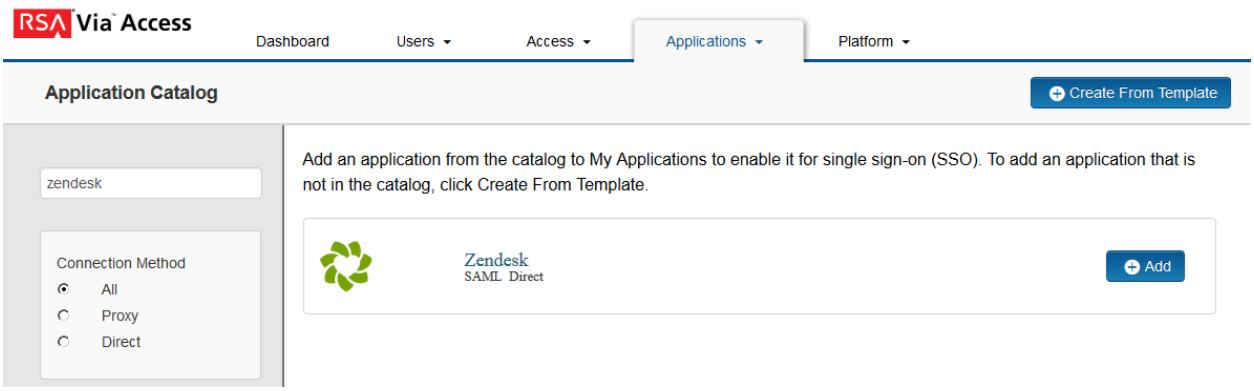
Procedure

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

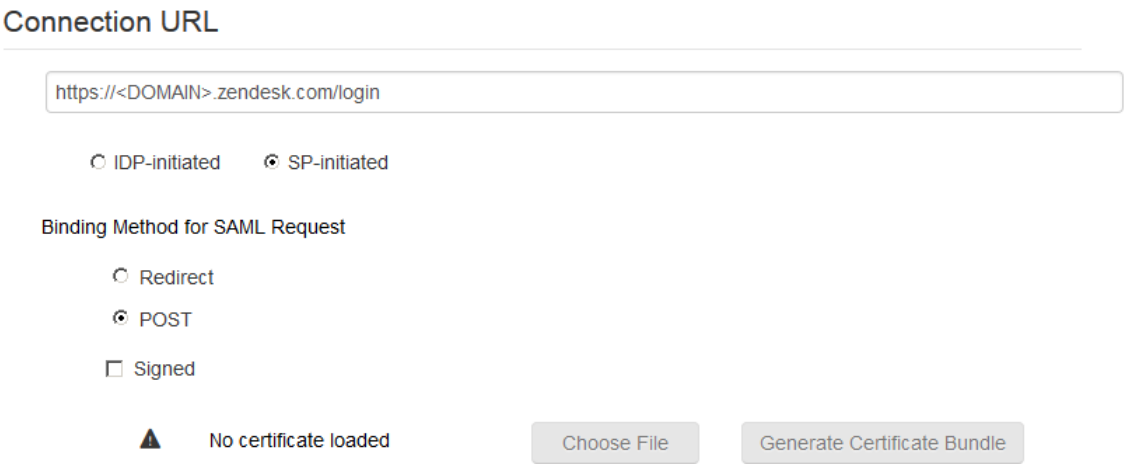
Procedure

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**.

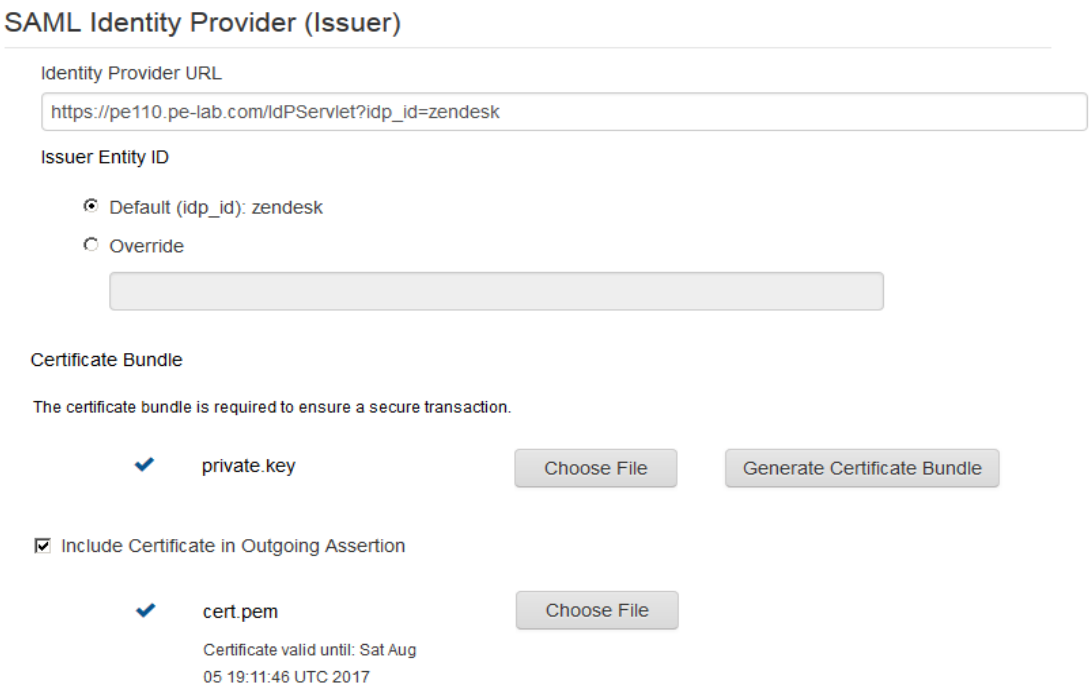


3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, modify the URL for your site.
   https://<domain>.zendesk.com/login
5. Choose **SP -initiated** and binding method **POST**.

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



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

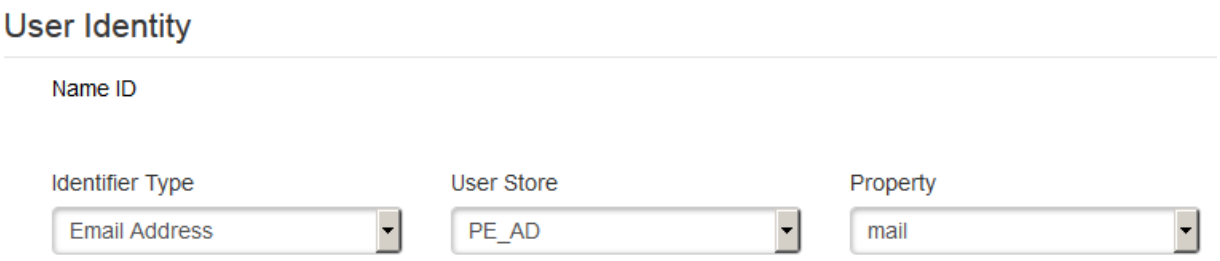


   a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Service Provider configuration.
   b. Select **Choose File** and upload the private key.
   c. Check **Include Certificate in Outgoing Assertion**, select **Choose File,** and upload the public certificate.

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

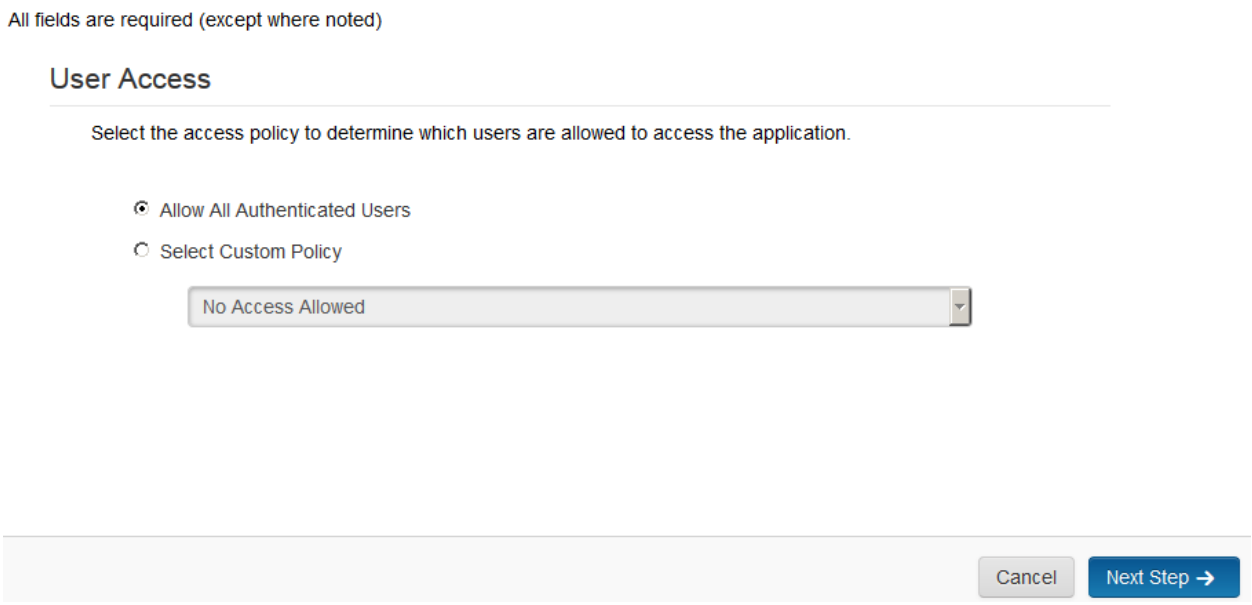
   a. In the **Assertion Consumer Service (ACS) URL** field, modify the URL with your company's Zendesk site domain. https://<domain>.zendesk.com/access/saml
   b. In the **Audience (Service Provider Entity ID)** field, enter **zendesk.com**.

8. Scroll down to the **User Identity** section. Set the Identifier Type to **Email Address** and Property to **mail**.

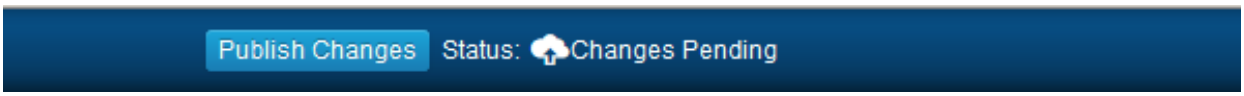


9. Click **Next Step**.

10. On the **User Access** page, select the desired user policy from the drop down list.



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.



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

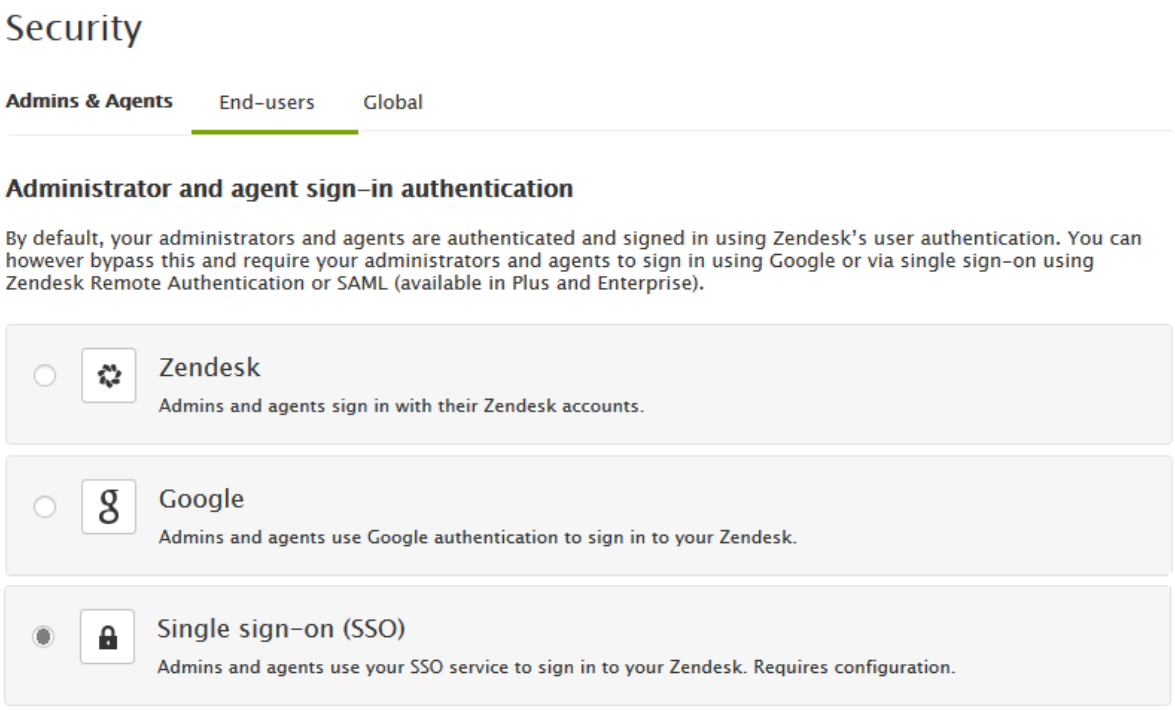
Configure Zendesk to Use RSA SecurID Access as an Identity Provider

Procedure

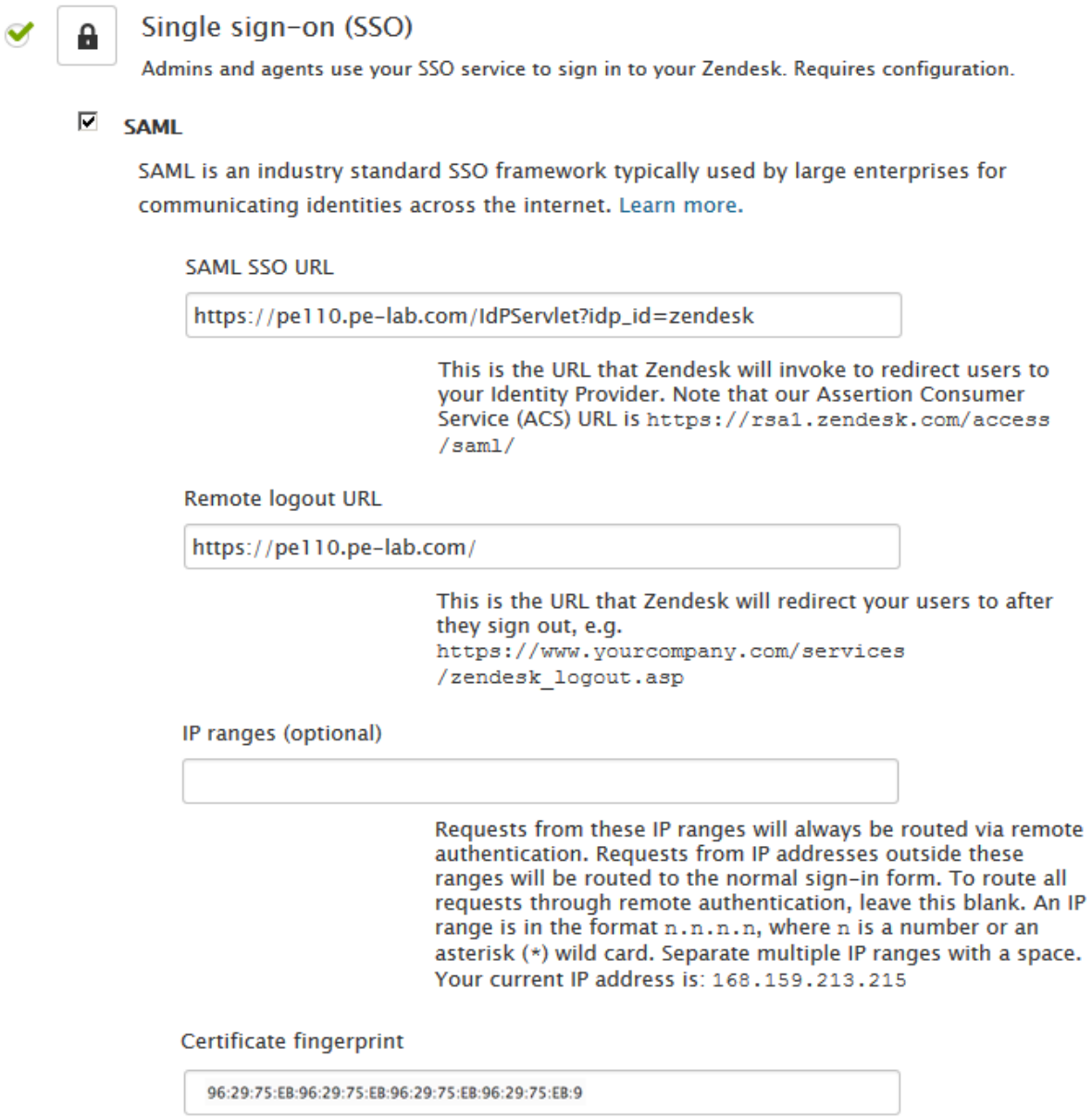
1. Login into the Zendesk administration console.
2. Click the Admin icon at the bottom of the sidebar.
3. Under the SETTINGS section, select **Security**.
4. Select the **Admins & Agents** or **End-users** tab.

> **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.



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



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

GLS