RSA SecurID Access SAML Configuration for OneDesk

Last Modified: March 8th, 2017

OneDesk is a platform for product management, project management, and customer service. It provides streamlined product management: Capture and manage ideas, stories & requirements. Manage build releases, create product hierarchies and share plans in progress.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and OneDesk.
- Obtain SP metadata details from service provider.
- Obtain IdP metadata from IDR portal.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	*https://app.onedesk.com/*
ACS URL	*https://app.onedesk.com/sso/saml/SSO/alias/onedesk.com_gslab*
Service Provider Issuer ID	*onedesk.com_gslab*

Procedure

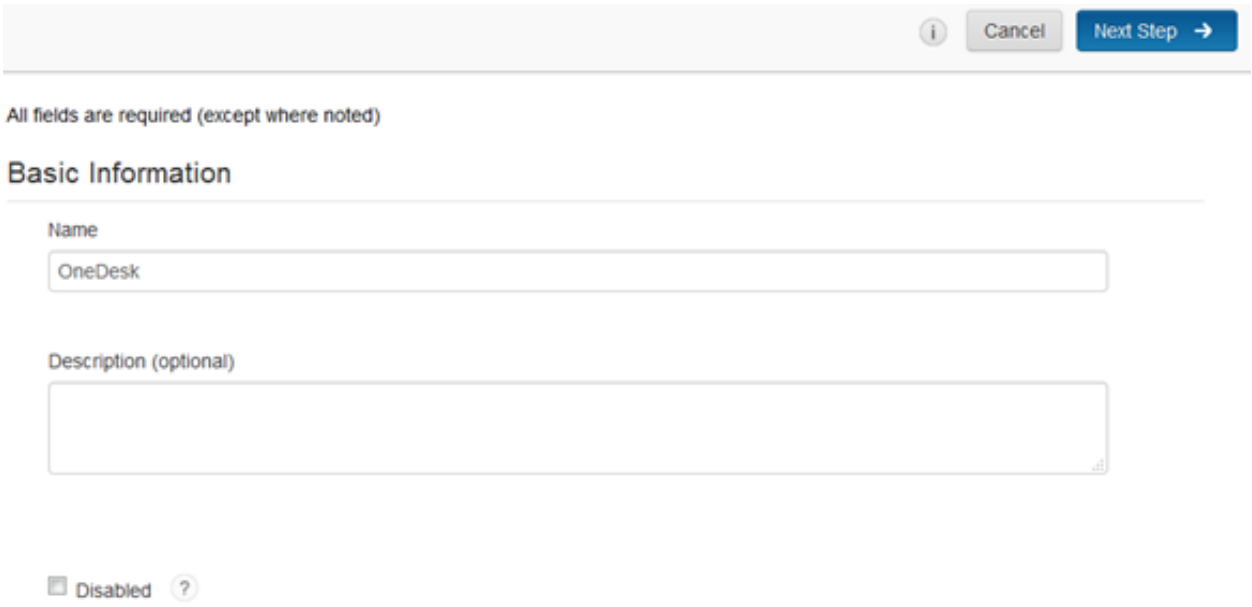
1. Add the Application in RSA SecurID Access
2. Configure OneDesk to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

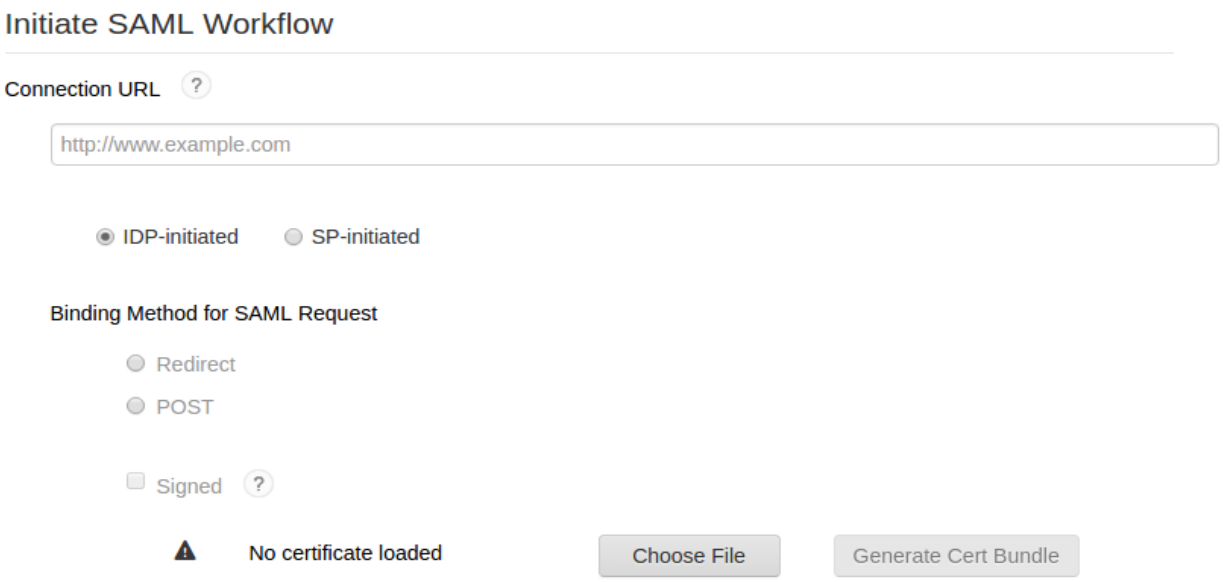
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for OneDesk.

3. On the Basic Information page, specify the application name and click **Next Step**.

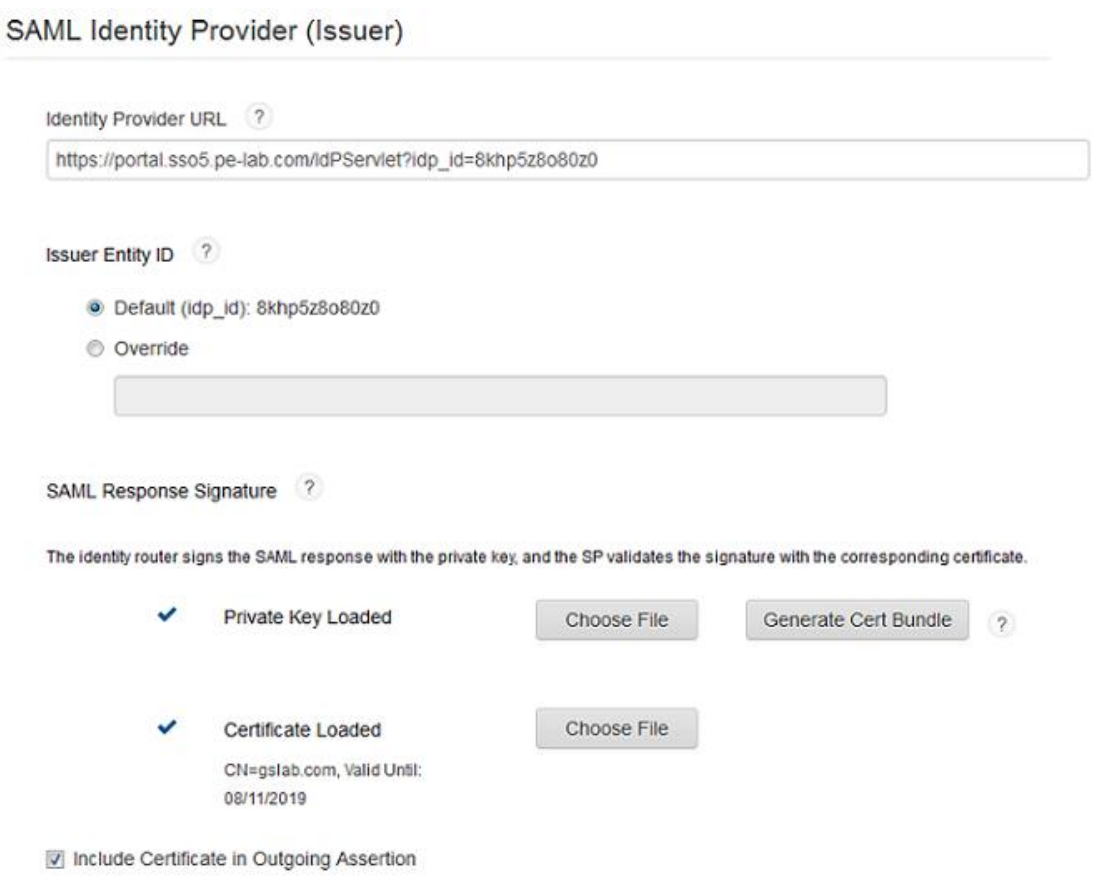


4. Navigate to **Initiate SAML Workflow** section.
   a) In the **Connection URL** field, keep the field blank as the value is not required.
   b) Choose **IDP–initiated**.

Note: The following IdP-initiated configuration works for SP-initiated OneDesk connections as well.



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

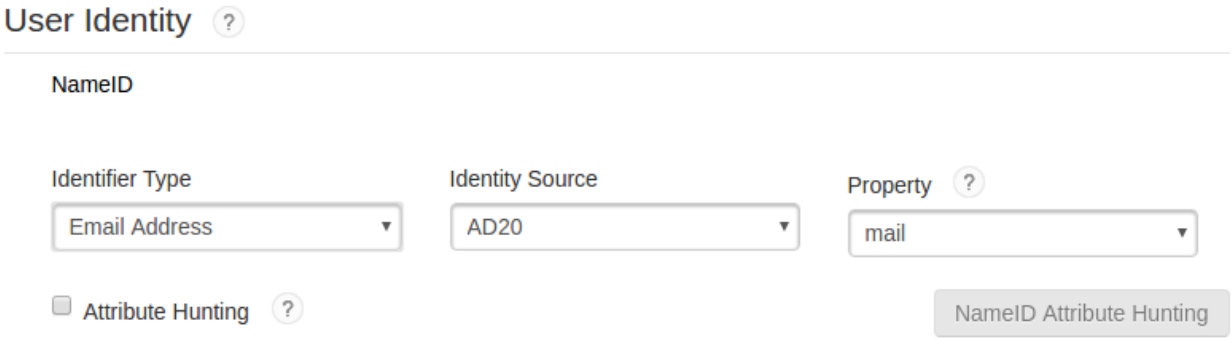


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

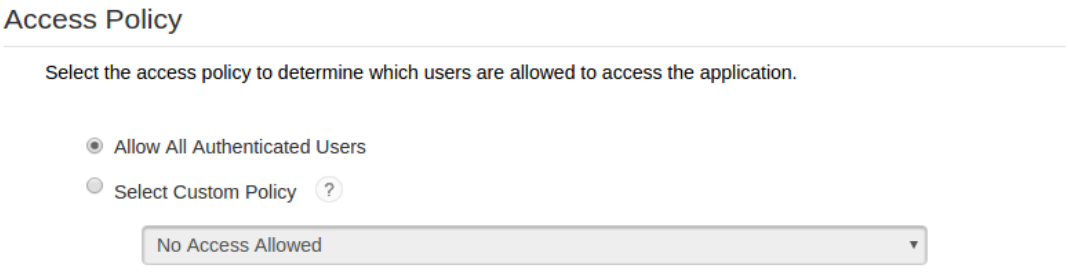
6. Scroll down to the **Service Provider** section.

   a. In the **Assertion Consumer Service (ACS) URL** field, insert value as provided by Service Provider.
   b. In the **Audience (Service Provider Entity ID)** field, insert value as provided by Service Provider.

7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

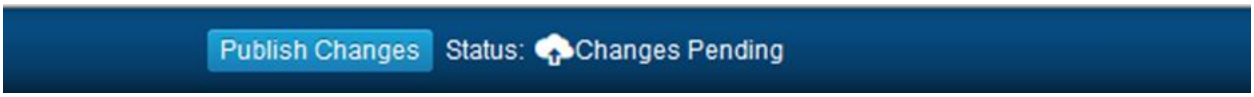


8. Click **Next Step**.
9. On the **User Access page,** select **Allow All Authenticated Users** option from drop down list.



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.

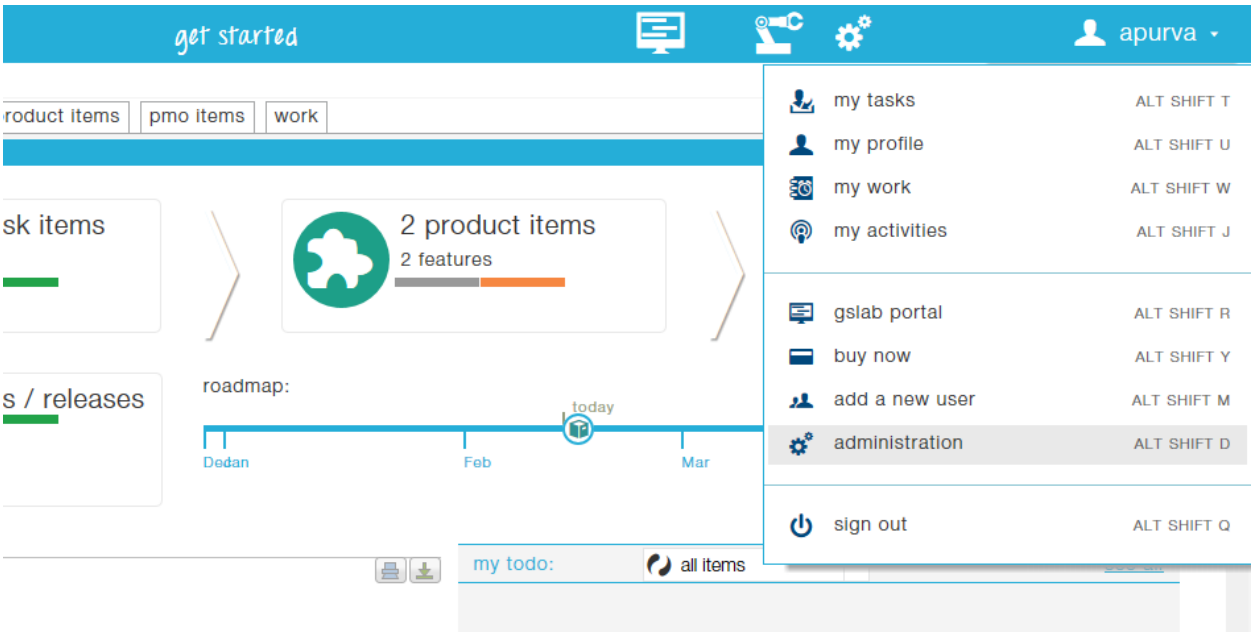


14. Navigate to **Applications > My Applications**.
15. Locate OneDesk in the list and from the **Edit** pulldown select **Export Metadata**. This is your IDP metadata file.

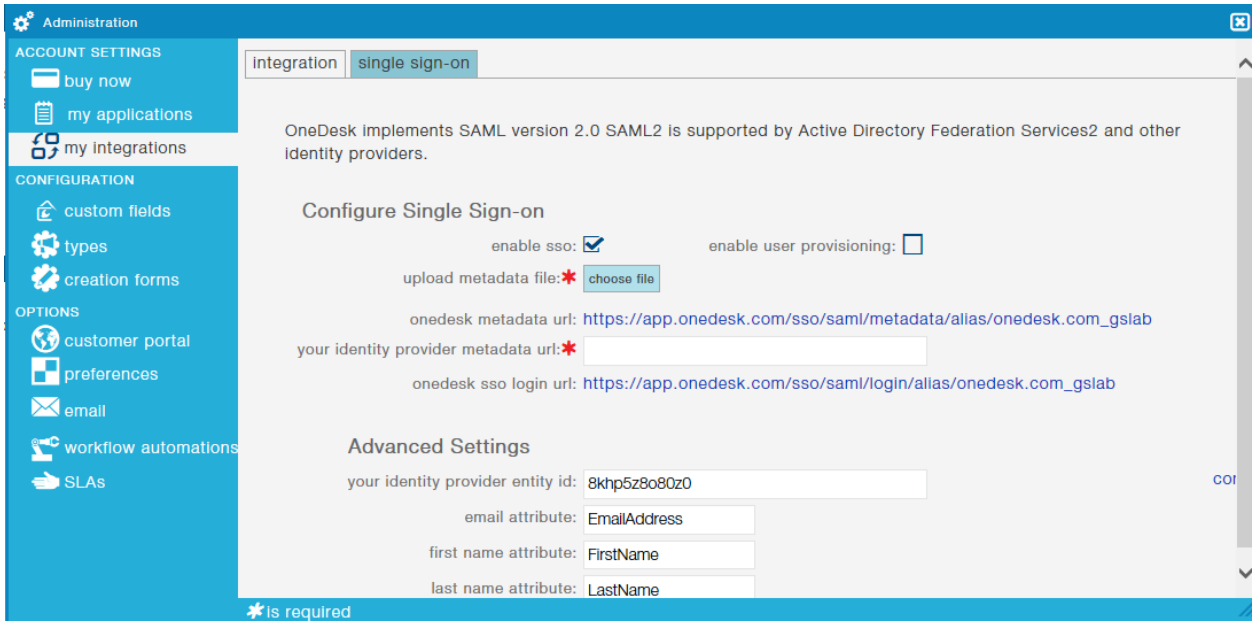
Configure OneDesk to Use RSA SecurID Access as an Identity Provider

1. Login to your OneDesk account. (https://app.onedesk.com/)

2. Click on **Arrow** in top-right corner of the page followed by **administration** option.



3. Following pop-up will be displayed. In left panel, go to **my integration.** Click on **Single sign-on** option tab.



a. Select checkbox **enable sso**.
b. In **upload metadata file** section, upload IDP metadata file.
c. Leave identity provider metadata URL option blank.
d. In **Advanced Settings**, enter IDP entity ID.
e. Close the pop-up window.
f. You can use **onedesk sso login url** for SP initiated SSO.

That's it! Your OneDesk account is enabled for SSO.

AB