

**Last Modified:** March 8<sup>th</sup>, 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:

<b>SP Login URL</b>	<a href="https://app.onedesk.com/">https://app.onedesk.com/</a>
<b>ACS URL</b>	<a href="https://app.onedesk.com/sso/saml/SSO/alias/onedesk.com_gslab">https://app.onedesk.com/sso/saml/SSO/alias/onedesk.com_gslab</a>
<b>Service Provider Issuer ID</b>	<a href="https://app.onedesk.com/sso/saml/SSO/alias/onedesk.com_gslab">onedesk.com_gslab</a>

## 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.



OneDesk  
SAML Direct



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

? Cancel Next Step →

---

All fields are required (except where noted)

### Basic Information

---

Name


Description (optional)

Disabled ?

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.

---

### Initiate SAML Workflow

---

Connection URL ?


IDP-initiated     SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?

 No certificate loaded    Choose File    Generate Cert Bundle

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

## SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): 8khp5z8o80z0

Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded

?

Certificate Loaded

CN=gslab.com, Valid Until:  
08/11/2019

Include Certificate in Outgoing Assertion

- 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.

### Service Provider

Assertion Consumer Service (ACS) URL ?

https://app.onedesk.com/sso/saml/SSO/alias/onedesk.com\_gslab

Audience (Service Provider Entity ID) ?

onedesk.com\_gslab

- 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.

### User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

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

### Access Policy

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy ?

No Access Allowed

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.



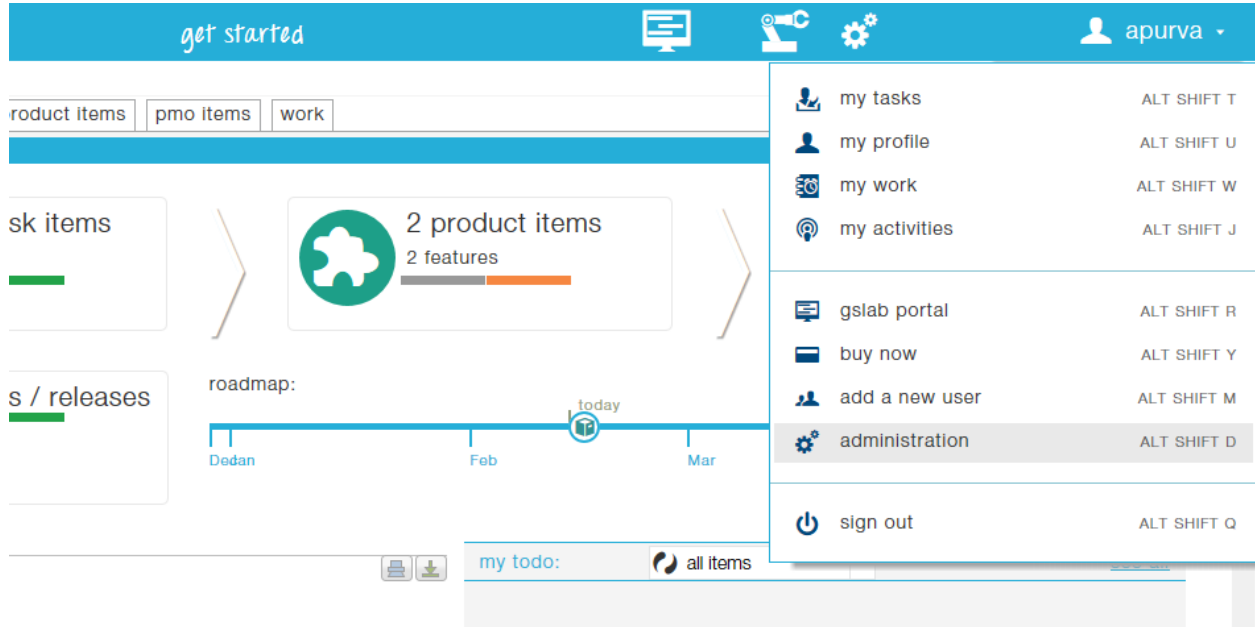
14. Navigate to **Applications > My Applications**.

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.



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

Administration

ACCOUNT SETTINGS

- buy now
- my applications
- my integrations

CONFIGURATION

- custom fields
- types
- creation forms

OPTIONS

- customer portal
- preferences
- email
- workflow automations
- SLAs

Integration single sign-on

OneDesk implements SAML version 2.0 SAML2 is supported by Active Directory Federation Services2 and other identity providers.

### Configure Single Sign-on

enable sso:  enable user provisioning:

upload metadata file: \*

onedesk metadata url: [https://app.onedesk.com/sso/saml/metadata/alias/onedesk.com\\_gslab](https://app.onedesk.com/sso/saml/metadata/alias/onedesk.com_gslab)

your identity provider metadata url: \*

onedesk sso login url: [https://app.onedesk.com/sso/saml/login/alias/onedesk.com\\_gslab](https://app.onedesk.com/sso/saml/login/alias/onedesk.com_gslab)

### Advanced Settings

your identity provider entity id:

email attribute:

first name attribute:

last name attribute:

\* is required

- Select checkbox **enable sso**.
- In **upload metadata file** section, upload [IDP metadata file](#).
- Leave identity provider metadata URL option blank.
- In **Advanced Settings**, enter [IDP entity ID](#).
- Close the pop-up window.
- You can use **onedesk sso login url** for SP initiated SSO.

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