RSA SecurID Access SAML Configuration for OnlyOffice

Last Modified: July 04, 2017

OnlyOffice (formerly Teamlab Office) is a multi functional online office suite integrated with CRM system, document and project management toolset, Gantt chart and email aggregator. It also includes an online office application suite working within a browser. It combines text, spreadsheet and presentation editors that include features similar to Microsoft desktop editors (Word, Excel and PowerPoint), also allow to co-edit, comment and chat in real time. OnlyOffice does support auto-provisioning of the user feature.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and OnlyOffice.
- Obtain SP metadata details from the Service Provider.

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

SP Login URL	*https://www.onlyoffice.com/signin.aspx*
ACS URL	*https://gslabsso.onlyoffice.sg/samllogin.ashx*
Service Provider Issuer ID	*https://gslabssso.onlyoffice.sg/samllogin.ashx*

Procedure

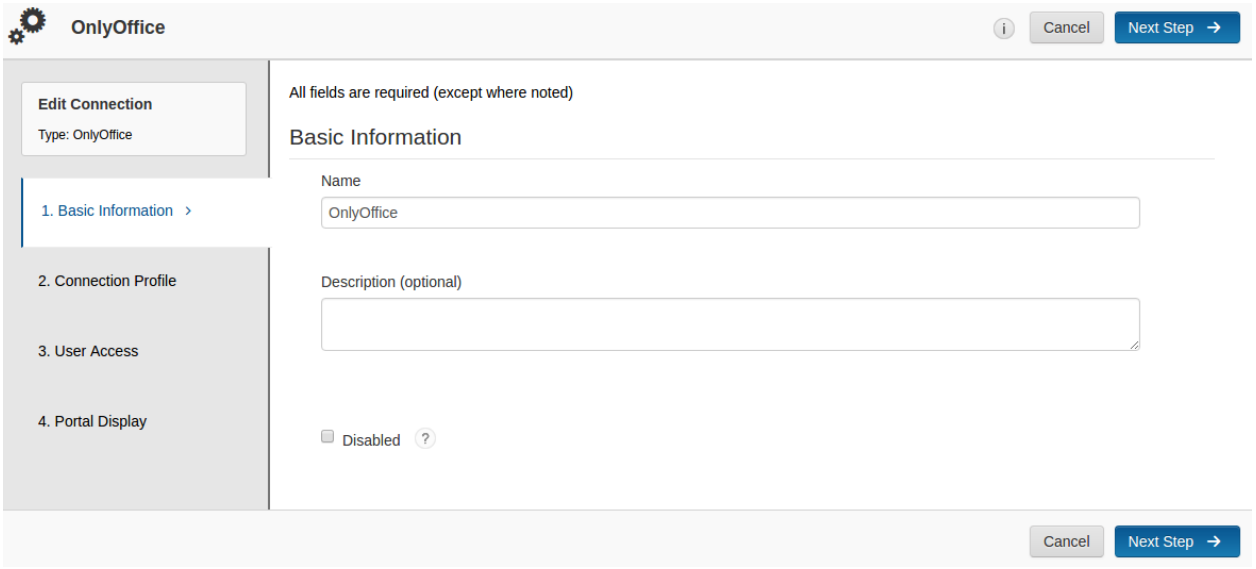
1. Add the Application in RSA SecurID Access
2. Configure OnlyOffice to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

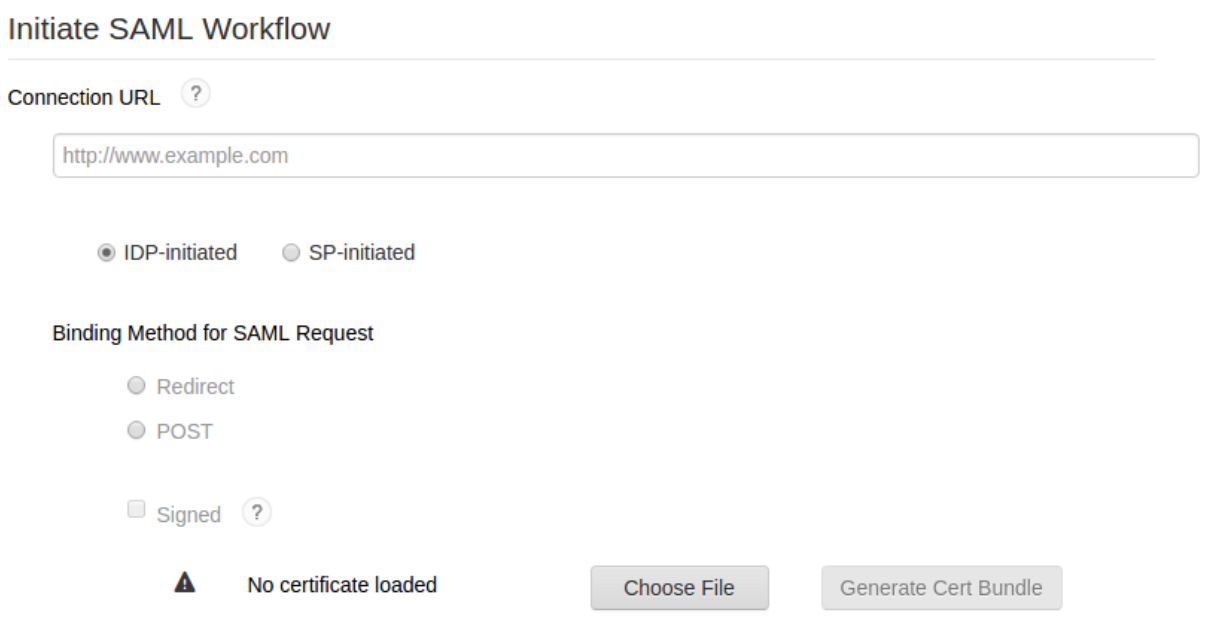
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** OnlyOffice.

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

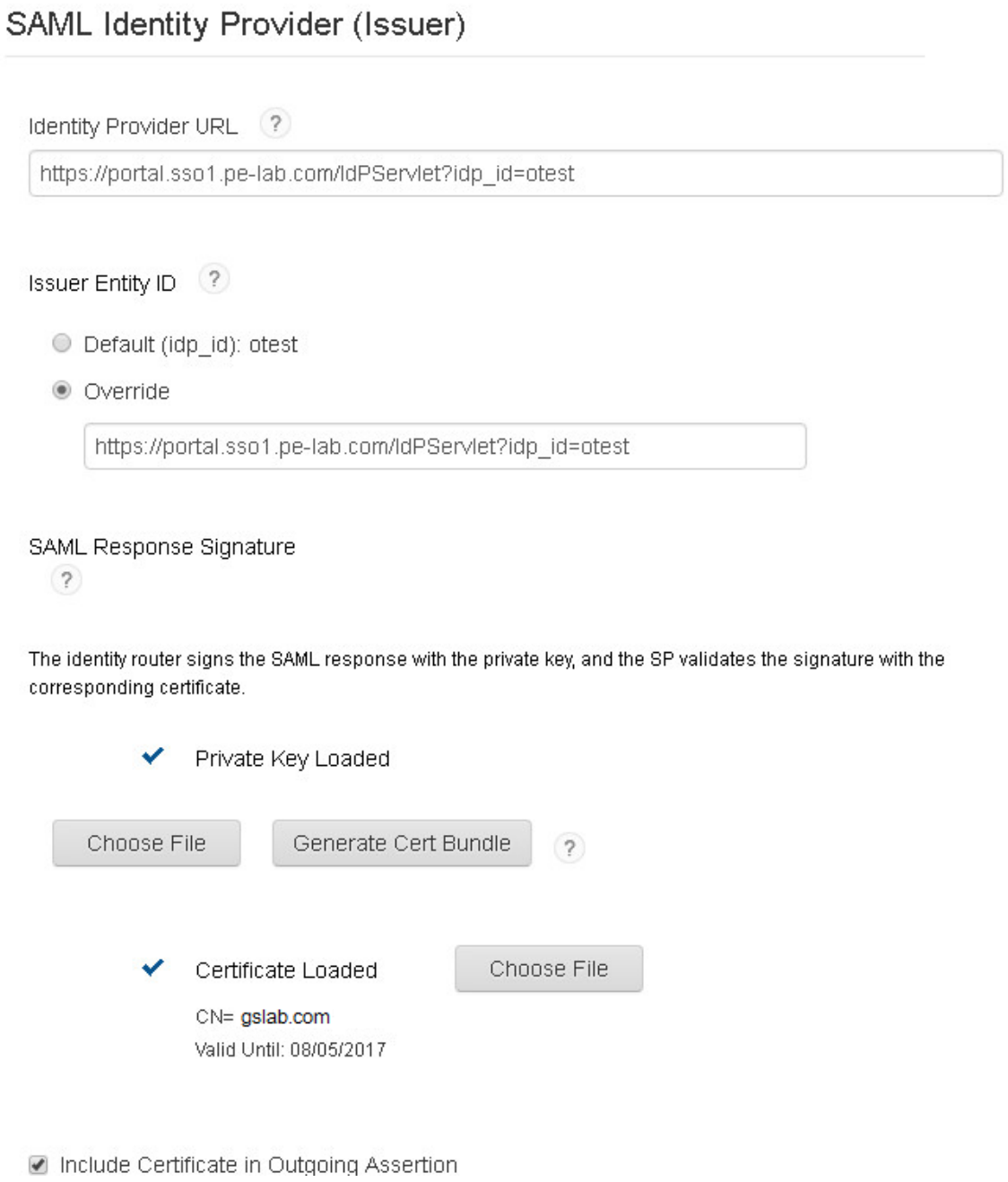


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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

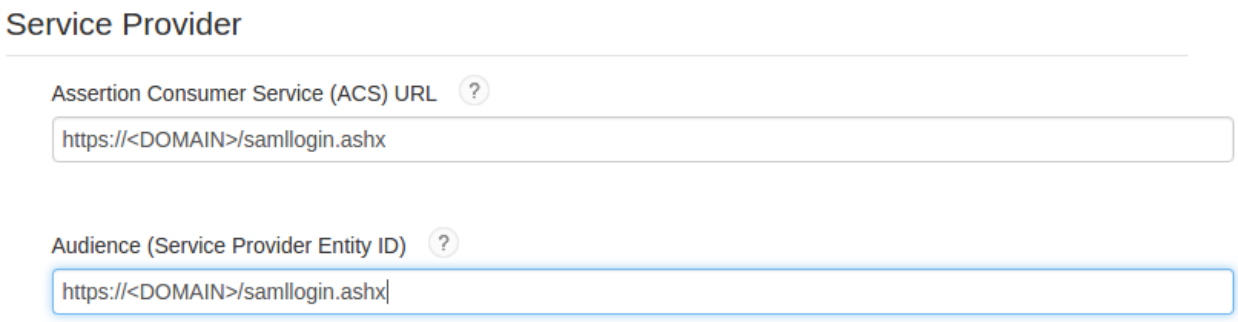


5. Scroll down to **SAML Identity Provider (Issuer)** section.



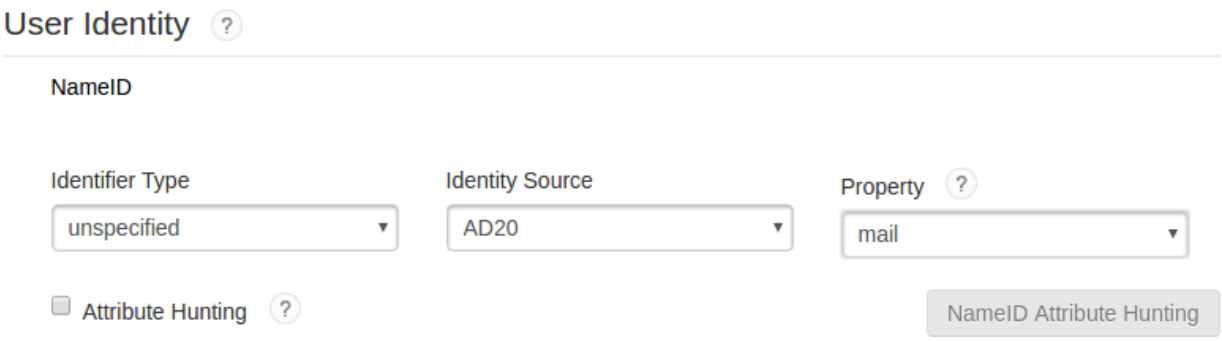
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Override** for value for the **Issuer Entity ID**. Make sure this is a URL format and use this as the **Issuer URL** at the SP-side configuration on page 7 step 3c.
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.

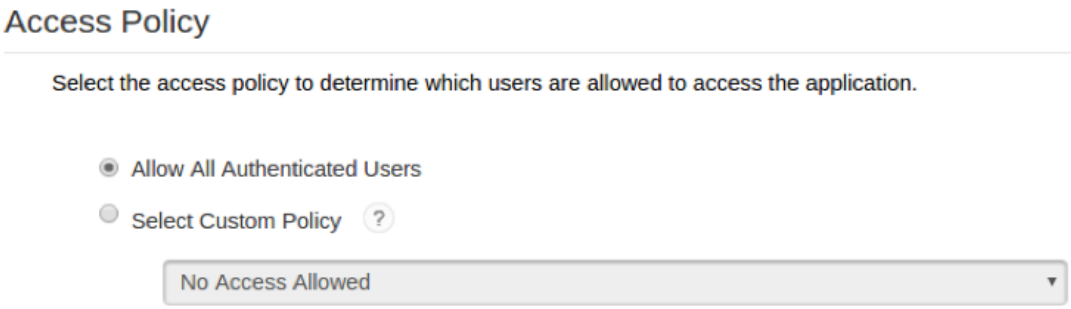


   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your unique organization domain value.
   b. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your unique organization domain value.

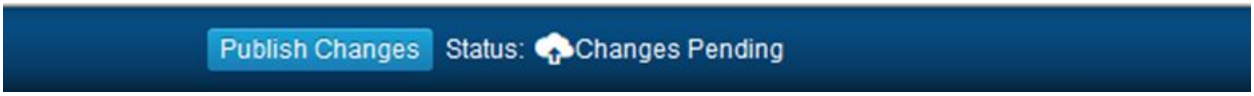
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users** user policy from the available options.



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.

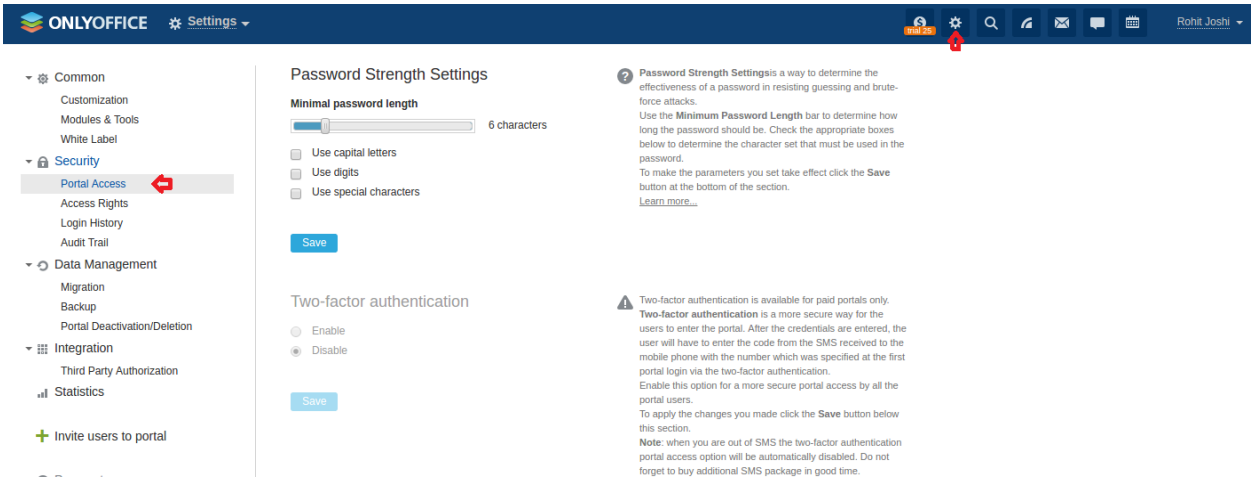


Configure OnlyOffice to Use RSA SecurID Access as an Identity Provider

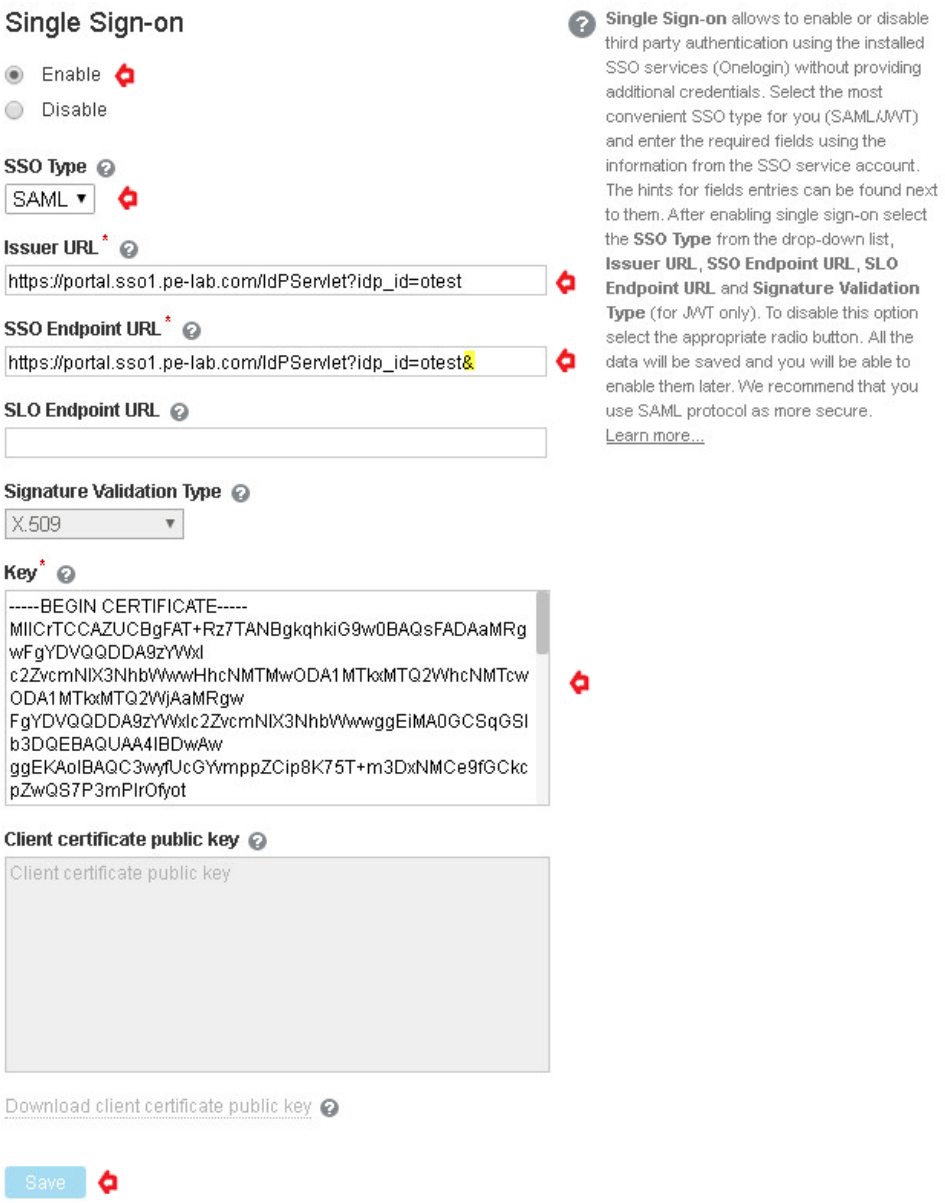
Procedure

1. Login to your OnlyOffice application web account. (https://www.onlyoffice.com/signin.aspx)

2. Following UI will be displayed. Go to *Settings (geared icon)* → *Security* → *Portal Access*.



3. Scroll down to *Single Sign-on* settings configuration option. Following UI will be displayed.



   a. Click on **Enable** radio button to make this account available for SAML SSO authentication.
   b. Choose **SAML** from available drop down options for **SSO Type** field.
   c. **Issuer URL** : Enter **IDP Issuer Entity ID** value received from idp settings.
   d. **SSO Endpoint URL** : Enter the Identity Provider URL which can be found in *step 5* on *page 3* and append &.
      https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>&
   e. Keep the **SLO Endpoint URL** and **Signature Validation Type** field to their default values.
   f. **Key** : Paste the RSA SecurID Access IdP public certificate here.
   g. Once sure of all the settings, click on **Save** button to complete the configurations.

4. Your OnlyOffice account is now enabled for SAML SSO authentication.

RJ