

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://gslabssso.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.



OnlyOffice
SAML Direct



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

OnlyOffice

Cancel Next Step →

Edit Connection
Type: OnlyOffice

All fields are required (except where noted)

Basic Information

1. Basic Information >

2. Connection Profile

3. User Access

4. Portal Display


Name
OnlyOffice

Description (optional)

Disabled ?

Cancel Next Step →

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

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

Initiate SAML Workflow

Connection URL ?

http://www.example.com


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): otest
 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: 08/05/2017

Include Certificate in Outgoing Assertion

- Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
- 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.
- Select **Choose File** and upload the private key.
- Select **Choose File** to import the public signing certificate.
- 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://<DOMAIN>/samlogin.ashx

Audience (Service Provider Entity ID) ?

https://<DOMAIN>/samlogin.ashx

- 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.

User Identity ?

NameID

Identifier Type

unspecified

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** user policy from the available options.

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.

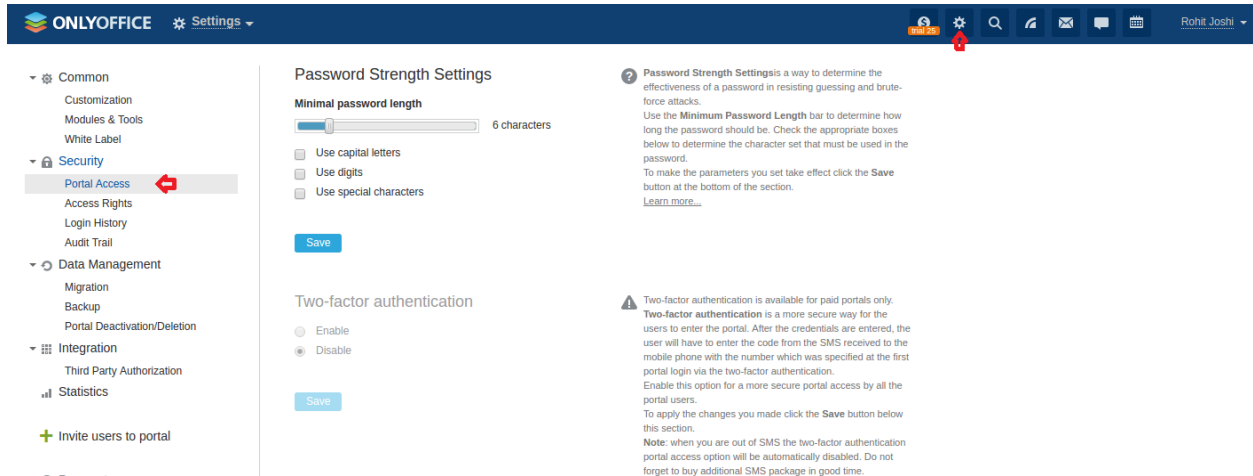
[Publish Changes](#)

Status:  Changes Pending

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 (gearing icon) → Security → Portal Access*.




The screenshot displays the OnlyOffice Settings page. The left sidebar shows a navigation menu with categories: Common, Security, Data Management, Integration, and Statistics. The 'Security' category is expanded, and 'Portal Access' is selected. The main content area is divided into two sections:

- Password Strength Settings:** This section includes a slider for 'Minimal password length' set to 6 characters. Below the slider are three checkboxes: 'Use capital letters', 'Use digits', and 'Use special characters'. A 'Save' button is located at the bottom of this section. A help icon (?) is present to the right of the section title.
- Two-factor authentication:** This section features a warning icon (!) and a note stating that two-factor authentication is available for paid portals only. It includes two radio buttons: 'Enable' and 'Disable', with 'Disable' selected. A 'Save' button is at the bottom. A detailed note explains that users will need to enter a code from an SMS received on their mobile phone after entering credentials.

The top of the interface shows the 'ONLYOFFICE' logo, a 'Settings' dropdown menu, and a user profile for 'Rohit Joshi'.

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

Single Sign-on

- Enable 
 Disable

SSO Type

SAML 

Issuer URL




SSO Endpoint URL



SLO Endpoint URL

Signature Validation Type

X.509 


Key


```
-----BEGIN CERTIFICATE-----  
MICrTCCA ZUCBgFAT+Rz7TANBgkqhkiG9w0BAQsFADAaMRgwFgYDVQQDDA9zYWxl  
c2ZvcnNIX3NhbWwwHhcNMTMwODA1MTkxMTQ2WWhcNMTcw  
ODA1MTkxMTQ2WjAaMRgwFgYDVQQDDA9zYWxl c2ZvcnNIX3NhbWwwggEIMA0GC8qGSI  
b3DQEBAQUAA4IBDwAwggEKAoIBAQC3wyfUcG'YmppZCip8K75T+m3DxNMce9fGCck  
pZwQS7P3mPIrOfyot
```



Client certificate public key

[Download client certificate public key !\[\]\(683dba75afe26e28cd4de5730b776760_img.jpg\)](#)



 **Single Sign-on** allows to enable or disable third party authentication using the installed SSO services (OneLogin) without providing additional credentials. Select the most convenient SSO type for you (SAML/JWT) and enter the required fields using the information from the SSO service account. The hints for fields entries can be found next to them. After enabling single sign-on select the **SSO Type** from the drop-down list, **Issuer URL**, **SSO Endpoint URL**, **SLO Endpoint URL** and **Signature Validation Type** (for JWT only). To disable this option select the appropriate radio button. All the data will be saved and you will be able to enable them later. We recommend that you use SAML protocol as more secure. [Learn more...](#)

- Click on **Enable** radio button to make this account available for SAML SSO authentication.
- Choose **SAML** from available drop down options for **SSO Type** field.
- Issuer URL** : Enter [IDP Issuer Entity ID](#) value received from idp settings.
- 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>&
- Keep the **SLO Endpoint URL** and **Signature Validation Type** field to their default values.
- Key** : Paste the RSA SecurID Access IdP public certificate here.
- 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