

RSA SecurID Access SAML Configuration for EZOfficeInventory



Last Modified: June 19, 2017

EZOfficeInventory is a cloud-based asset tracking software used in tracking physical and technological assets. EZOfficeInventory provides businesses with a complete asset management solution. The Web-based app features equipment QR tagging, asset check-in and checkout, maintenance and service records, and usage auditing. The app runs on any device with a Web browser. EZOfficeInventory also supports auto provisioning for users.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and EZOfficeInventory.

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

SP Login URL	https://emc2.EZOfficeInventory.com/users/sign_in
ACS URL	https://emc2.EZOfficeInventory.com/users/auth/saml/callback
Service Provider Issuer ID	https://www.EZOfficeInventory.com

Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure EZOfficeInventory 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** EZOfficeInventory.



EZOfficeinventory
SAML Direct



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


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 EZOfficeInventory connections as well.

Initiate SAML Workflow

Connection URL ?


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?

 No certificate loaded

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): kmtlc9v53ih5

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

- Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
- Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
- 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://<COMPANY_NAME>.ezofficeinventory.com/users/auth/saml/callback

Audience (Service Provider Entity ID) ?

https://www.ezofficeinventory.com

- a. In the **Assertion Consumer Service (ACS) URL** field, replace <COMPANY_NAME> value with your organization name value.
 - b. In the **Audience (Service Provider Issuer ID)** field, provide value as per received from 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

▼ Show Advanced Configuration

8. Click on **Show Advanced Configuration** button.

9. In the **Attribute Extension** section,

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity So ▾	email	AD20 ▾	mail ▾	 
Identity So ▾	first_name	AD20 ▾	givenName ▾	 
Identity So ▾	last_name	AD20 ▾	sn ▾	 
 ADD				


- a. Select Attribute source as **Identity Source**.
- b. In Attribute name column, add three attribute names first_name, last_name, email respectively.
- c. Select Identity source against which values of first_name, last_name and email will be validated, enter respective property names.

10. Click **Next Step**.

11. 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 ▾


12. Click **Next Step**.

13. On the **Portal Display** page, select **Display in Portal**.

14. Click **Save and Finish**.

15. Click **Publish Changes**. Your application is now enabled for SSO.

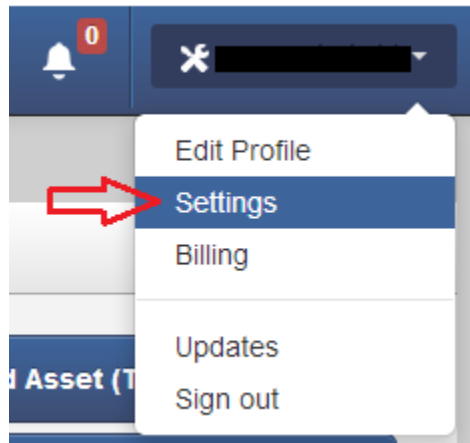
Publish Changes

Status:  Changes Pending

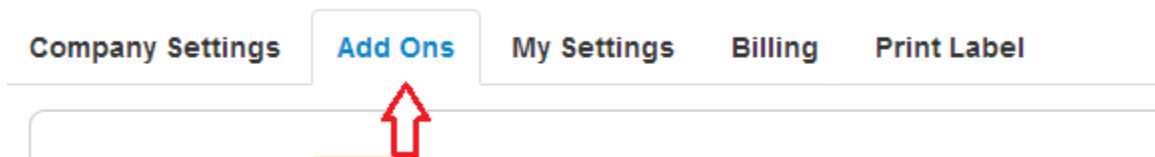
Configure EZOfficeInventory to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to your EZOfficeInventory application web account.
(https://emc2.EZOfficeInventory.com/users/sign_in)
2. In the top right corner of the homepage, go to **Username** and click on **Settings** option.



3. On the displayed page, click on **Add Ons**.



4. Scroll down to **SAML Integration** section. Select **Enabled** to enable SAML.

SAML Integration PLATINUM

Enabling Security Assertion Markup Language(SAML) enables your organization to sign in via a unified URL. Learn more about our [SAML integration](#). Please note that it is necessary for a SAML(2.0) identity provider to be present. A list of identity providers can be found [here](#).

To whitelist our IPs on your Directory server, use the following two IPs:

1. 54.221.243.145
2. 50.16.201.234

The EZOfficeInventory consumer service url is:

<https://emc2.ezofficeinventory.com/users/auth/saml/callback>

Your EZOfficeInventory metadata can be viewed here:

<https://emc2.ezofficeinventory.com/users/auth/saml/metadata>

Enabled

Disabled

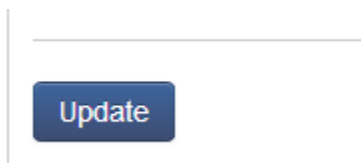


5. SAML settings will get open.

Identity Provider URL:	<input type="text" value="https://portal.sso5.pe-lab.com/Idf"/>
Identity Provider Certificate:	<pre>-----BEGIN CERTIFICATE----- MIICpjCCAY6gAwIBAgIGAU8c N6NcMA0GCSqGSIb3DQEBC wUAMBQxEjAQBgNVBAMT CWdzbGFILmNvbTAeFw0xNT</pre>
Login Button Text: (?)	<input type="text" value="Access through SAML SSO"/>
Clock Drift(seconds): (?)	<input type="text" value="0"/>
EZOfficeInventory requires Last Name and Email attributes from SAML configuration.	
First Name:	<input type="text" value="first_name"/>
Last Name:	<input type="text" value="last_name"/>
Email:	<input type="text" value="email"/> Use Another Identifier?
EZOfficeInventory Role By default: (?)	<input type="text" value="Staff User"/>

- a. In **Identity Provider URL** section, enter [IDP URL](#) from identity provider.
- b. In **Identity Provider Certificate** section, Copy the [public certificate](#) file contents which we used in Identity provider settings.
- c. In the **EZOfficeInventory Role By default** section, select the role to be given to the users when their account will be auto created. The auto creation happens when this user logs in successfully for the first time using SAML.

6. Scroll down and click on **Update** to save the SAML settings.



7. Your EZOfficeInventory account now is enabled for SAML SSO.

AB