

RSA SECURID[®] ACCESS

Implementation Guide

MyWebTimesheets

Gina Salvazo, RSA Partner Engineering
Last Modified: October 31, 2017

Solution Summary

MyWebTimesheets is Web Timesheet software to track employee hours by Customers, Projects, tasks and activities with powerful reporting features. This integration supports only SP-initiated authentication flow as of now. MyWebTimesheets application does not support auto-provisioning of the user.

RSA SecurID Access Features	
MyWebTimesheets	
On Premise Methods	
RSA SecurID	<input checked="" type="checkbox"/>
On Demand Authentication	<input checked="" type="checkbox"/>
Risk-Based Authentication (AM)	<input type="checkbox"/>
Cloud Authentication Service Methods	
Authenticate App	<input checked="" type="checkbox"/>
FIDO Token	<input checked="" type="checkbox"/>
SSO	
SAML SSO	<input checked="" type="checkbox"/>
HFED SSO	<input type="checkbox"/>

Identity Assurance	
Collect Device Assurance and User Behavior	<input checked="" type="checkbox"/>

Configuration Summary

All of the supported use cases of RSA SecurID Access with MyWebTimesheets require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – MyWebTimesheets can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

[Cloud Authentication Service – Identity Router IdP Configuration](#)
[MyWebTimesheets SAML Configuration](#)

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for MyWebTimesheets in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

Configure RSA Identity Router SAML IdP

Procedure

1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for MyWebTimesheets and click **+Add** to add the connector.



MyWebTimesheets
SAML Direct

+ Add

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
 - a. In the **Connection URL** field, provide appropriate value for the user to be able to get redirected properly.
 - b. Choose **SP-initiated**.
 - c. Choose **Redirect** binding method.

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

4. Scroll down to SAML Identity Provider (Issuer) section.

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): b1mtwlnyotwf

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**.

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

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.MyWebTimesheets.com/samllogin.aspx

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.MyWebTimesheets.com

- a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your organization unique domain value received after creating account.
 - b. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your organization unique domain value received after creating account.
6. 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


7. Click **Next Step**.


- 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 

- Click **Next Step**.
- On the **Portal Display** page, select **Display in Portal**.
- Click **Save and Finish**.
- Click **Publish Changes**. Your application is now enabled for SSO.

[Publish Changes](#)

Status:  Changes Pending

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Interact with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All MyWebTimesheets components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

MyWebTimesheets SAML Configuration

Procedure

1. Login to your MyWebTimesheets application web account.
<https://live1.MyWebTimesheets.com/Login.aspx>
2. Following UI will be displayed. Click on *System Setup* option.

The screenshot displays the MyWebTimesheets application interface. The top navigation bar includes 'MOBILE VERSION', 'MY CALENDARS', and the user name 'Rohit Joshi'. Below the navigation bar, there are tabs for 'Projects & Tasks', 'Timesheets', 'LMS Dashboard', 'Reports', 'Users', 'Social Intranet', and 'System Setup'. A red arrow points to the 'System Setup' tab. The main content area shows 'My recent timesheets' with a 'Log time' button and a link to 'Timesheets In The Last 5 Timesheets'. Below this, there are sections for 'Timesheet Queries' and 'No Discussions found!'. At the bottom, there are two panels: 'By Customer' and 'By Project', both showing 'No timesheet logged'.

3. Following UI will be displayed. Go to *Security Management -> Company SAML Settings*.

The screenshot shows a navigation menu with the following sections and items:

- TOIL and Overtime**
 - Overtime Types
 - TOIL & Overtime Settings
- Shifts**
 - Set Shifts
 - Schedule Template
 - User Schedules
 - User Schedule Exceptions
- Timesheets**
 - Company Timesheet settings
 - Timesheet Models
 - Timesheet Approval Paths
 - Timesheet Validation Rules
 - Timesheet Unlock Reasons
 - Timesheet Approval Triggers
 - Insufficient Time entry Reminders
 - Timesheet Header/Footers
 - Overtime Alerts
- Project Management**
 - Project/Task Settings
 - Project Approval Path
 - Milestone Types
 - Activity Types
 - Positions
 - Project Groups
 - Permission Setup
 - List Items
- Security Management**
 - Filters
 - Application Users
 - Give permissions for users to apply leave/apply overtime for other users
 - Company SAML Settings (highlighted with a red house icon)
 - Roles
 - Network Security
 - SCIM User Provisioning

4. Following UI will be displayed. Click on *Edit (Pencil icon)* option to add SAML settings.

The screenshot shows the SAML Settings page in the MyWebTimesheets application. The page includes a navigation bar with the following items:

- MOBILE VERSION
- MY CALENDARS
- R J Rohit Joshi

The main navigation bar contains the following items:

- Users (selected)
- Enter search keywords
- Quick Add
- Quick Action
- Home
- Calendar
- Help
- Tools
- Notifications

The SAML Settings page displays the following information:

- SAML Settings** (with Edit and Back icons)
- Login URL : https://portal.sso5.pe-lab.com/IdPServlet?idp_id=120fpzr45jqv
- Logout URL :
- Is Enable : Yes
- SAML Configuration**
- Consumer Service URL (ACS) : <https://rohitwce91.MyWebTimesheets.com/samllogin.aspx>
- EntityID : <https://rohitwce91.MyWebTimesheets.com>
- Metadata**
- [Click here](#) to download the XML file.

5. Following UI will be displayed. Click on *Identity Providers* button.

The screenshot shows the 'Update SAML Settings' form in the MyWebTimesheets application. The form has the following fields and values:

- Login URL ***: (with a red arrow pointing to the right)
- Logout URL**:
- Certificate ***:

```
-----BEGIN CERTIFICATE-----
MIICpjCCAY6gAwIBAgI GAVgp4T9kMA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNVBAMT
CWdzbGFILmNvbTAeFw0xNjExMDMxMTA5MzdaFw0yMDExMDMxMTA5MzdaMBQxEjAQ
BgnVBAMTCWdzbGFILmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJoUHRNu+TFz94saWXzK/jWbSzhkYw8dGAOAPI6C/m7dO1D/AIRUJPzcza+7dkU
nBizdStBm5OGO66AbQfsbBPezHHie2EZSRri5HTJhn831VO/33Hwz94U/kpLbBgg
TF2G60jL9z66lrW0fbjhQAFg7eU/9h2CD4eEafGMkq1YerweQGwYMs8z7ZoDRmR
EGkT+GW8Qo0PsRsiHL8yzQYODqk4XypwXn9Rz2+b6wdJ9MyD/Jj912rqzpZrXeB
HeOF1IbZ1wml/N5VshaWBr5yFTGK5Q6Zilsxsei+opLPXOSZc4z2iNmKFxzxbiKs
ACp2zdoVFpyKssLYxnqjMBMCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEASVerg9WL
fk5eUDzuiDEu7O3yBSyym0RqfZMOal0kN86emlzCBEle4GGtZh93od6NJF31Hna
```

 (with a red arrow pointing to the right)
- Is Enable**: Yes No (with a red arrow pointing to the right)

At the bottom of the form, there is a green arrow pointing right, followed by 'Save' and 'Cancel' buttons.

- Login URL** : Enter the Identity Provider URL which can be found in step : 4a. on page 5. It is of following format : **https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>**.
- You can keep **Logout URL** field blank as it is optional. If provided, users will be redirected to this URL after logging out from the account.
- Certificate** : Paste the public certificate used in step 4d. on page 5.
- Is Enable** : Select **Yes** radio button to enable SAML SSO authentication.
- Once sure of all settings, click on **Save** button to complete SAML configuration.

6. Your MyWebTimesheets account is now enabled for SAML SSO authentication.