RSA SECURID® ACCESS
Implementation Guide

MyWebTimesheets

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

RSA READY

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	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

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)

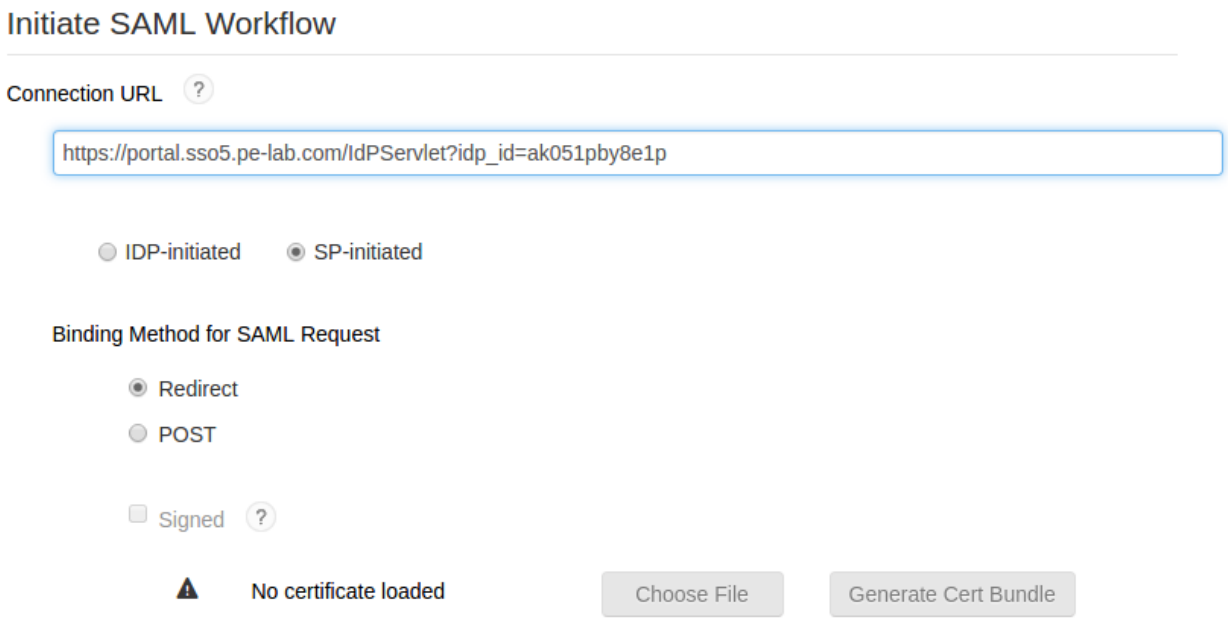
To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for MyWebTimesheets in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL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

Configure RSA Identity Router SAML IdP

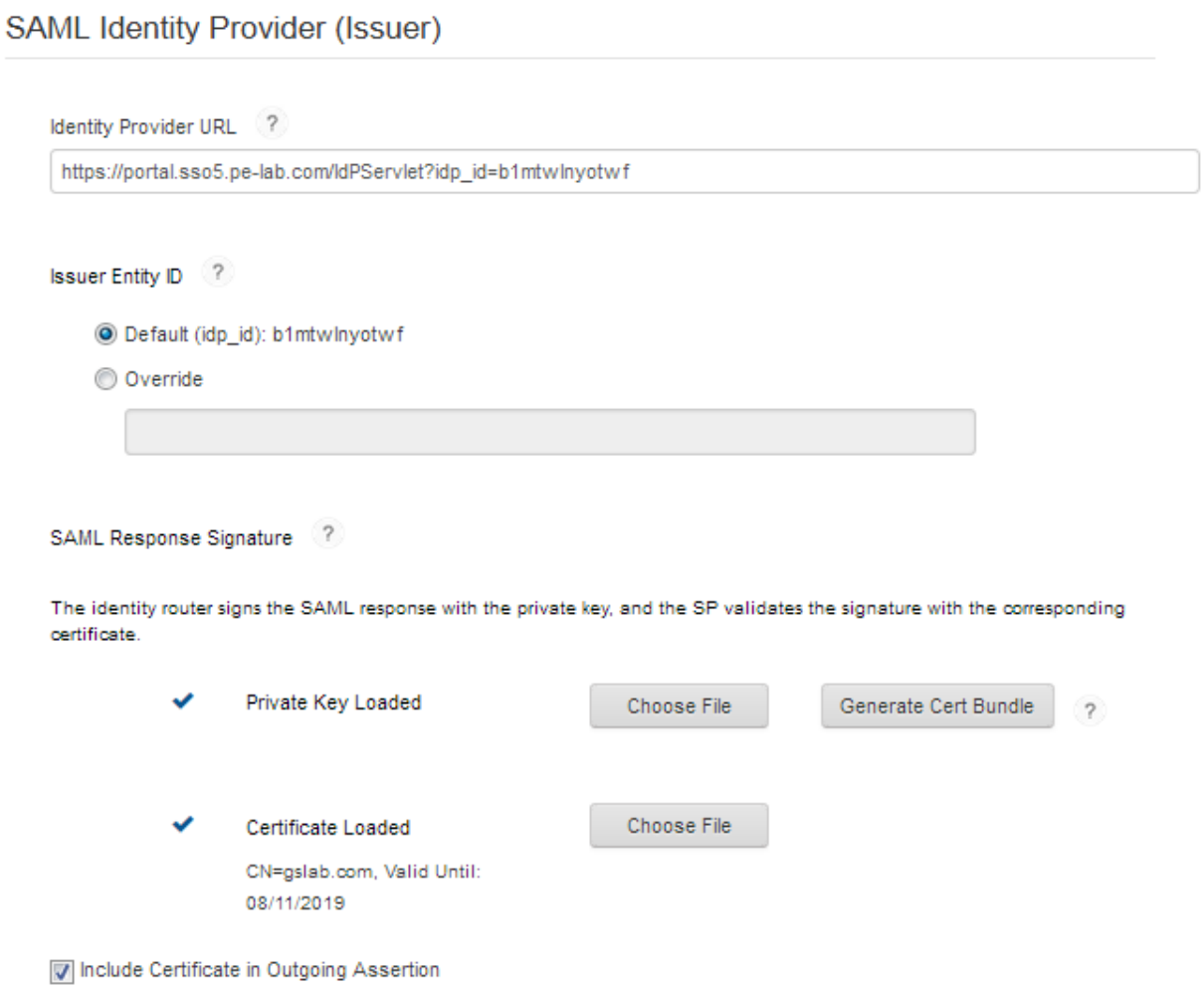
Procedure

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

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.

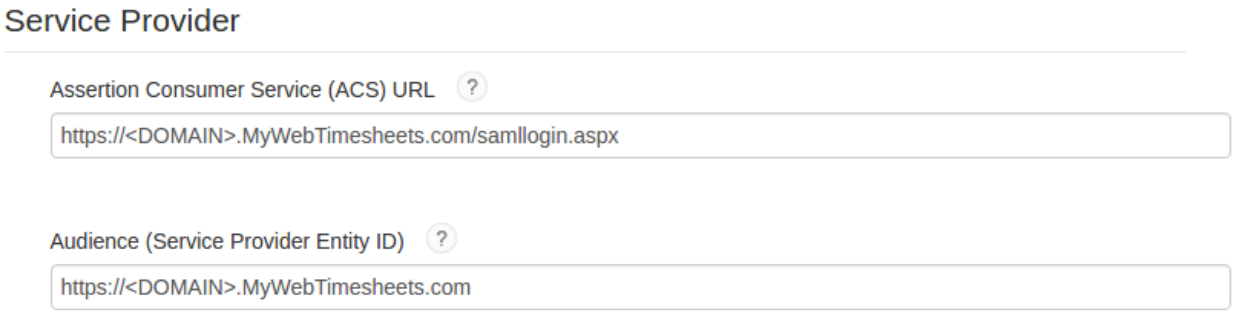


4. Scroll down to SAML Identity Provider (Issuer) section.



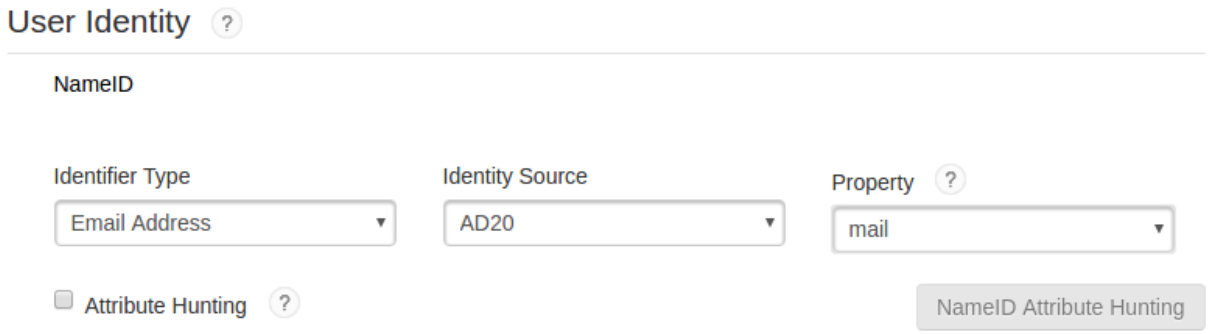
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** 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.



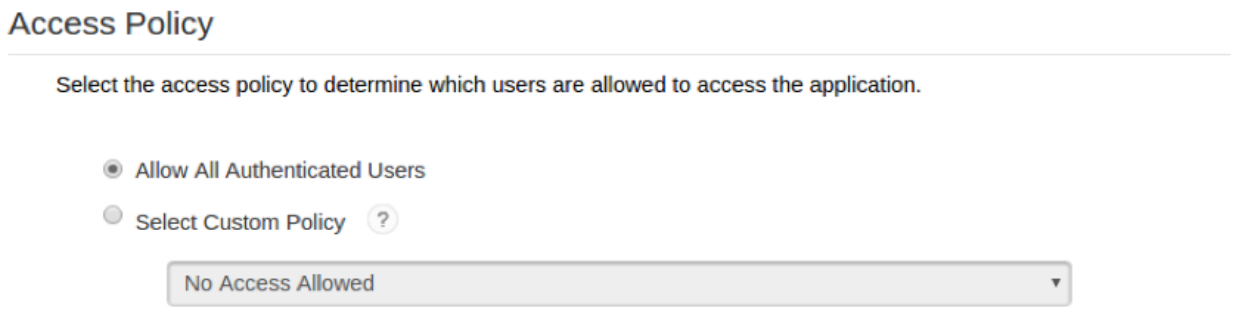
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your organization unique domain value received after creating account.
   b. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your organization unique domain value received after creating account.

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.

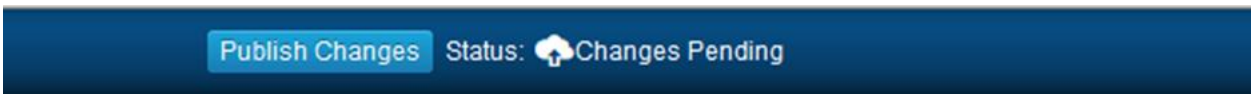


7. Click **Next Step**.

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



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



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.

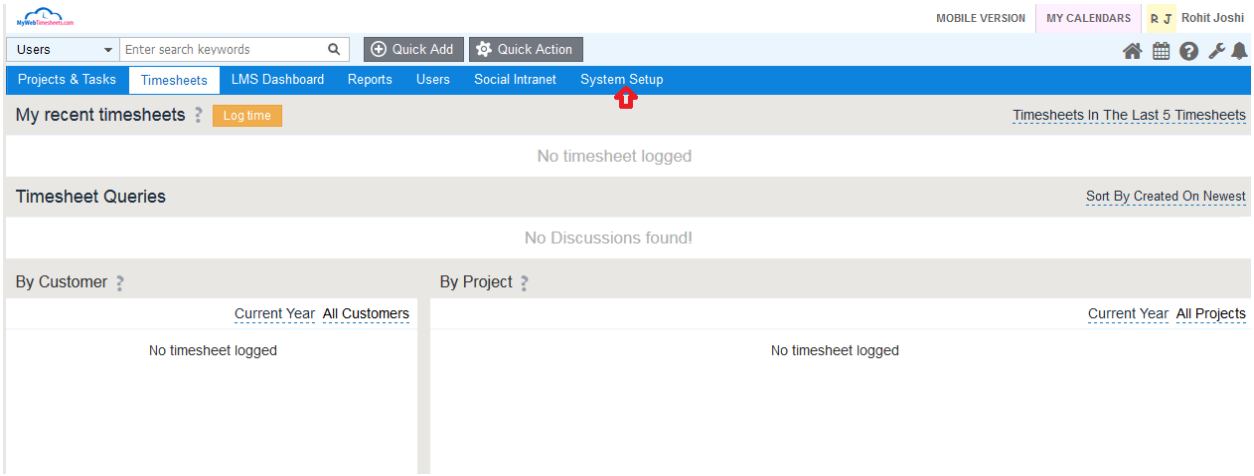
All MyWebTimesheets components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

MyWebTimesheets SAML Configuration

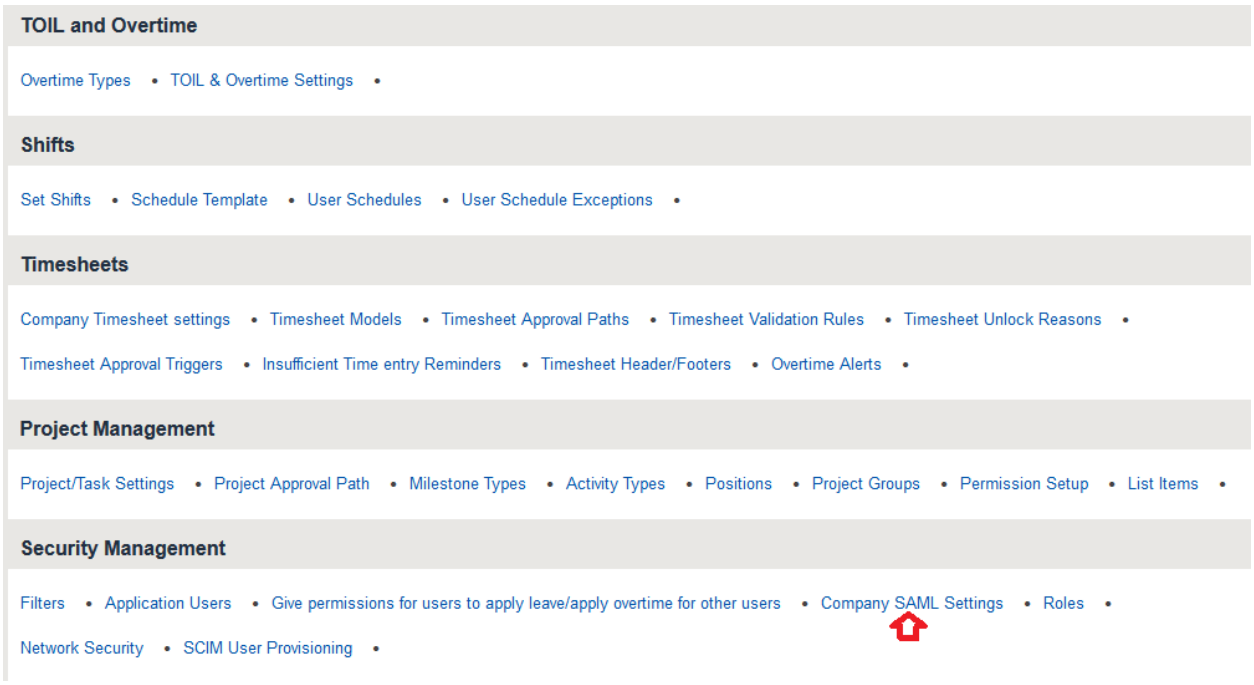
Procedure

1. Login to your MyWebTimesheets application web account.
   https://live1.MyWebTimesheets.com/Login.aspx

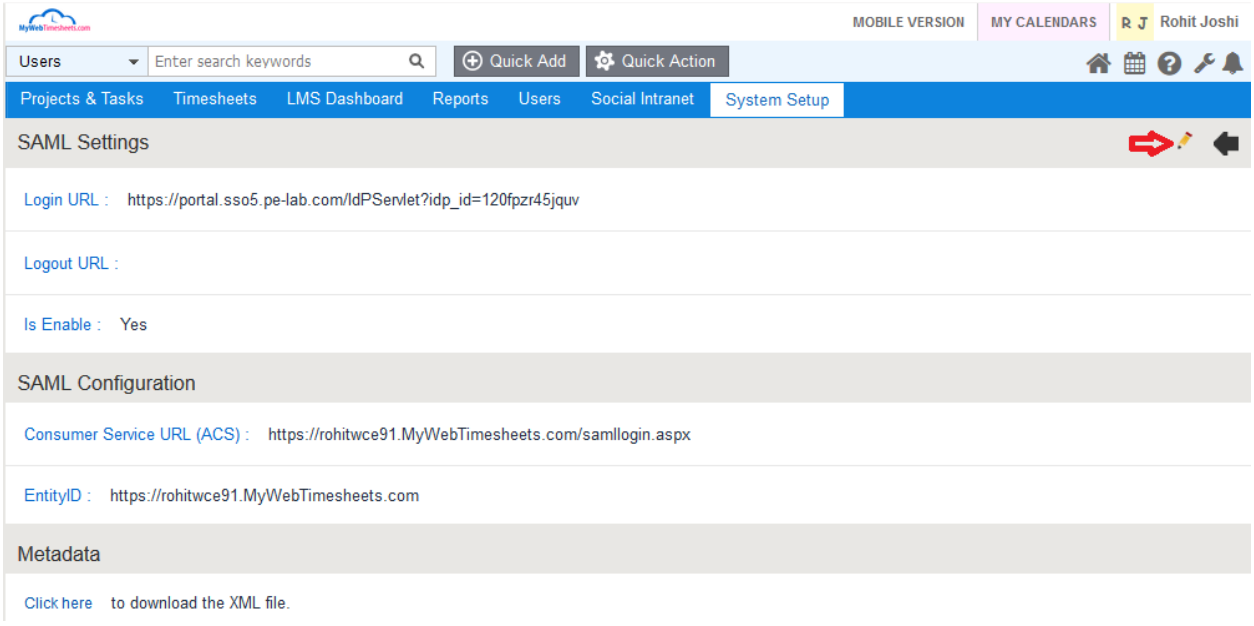
2. Following UI will be displayed. Click on *System Setup* option.



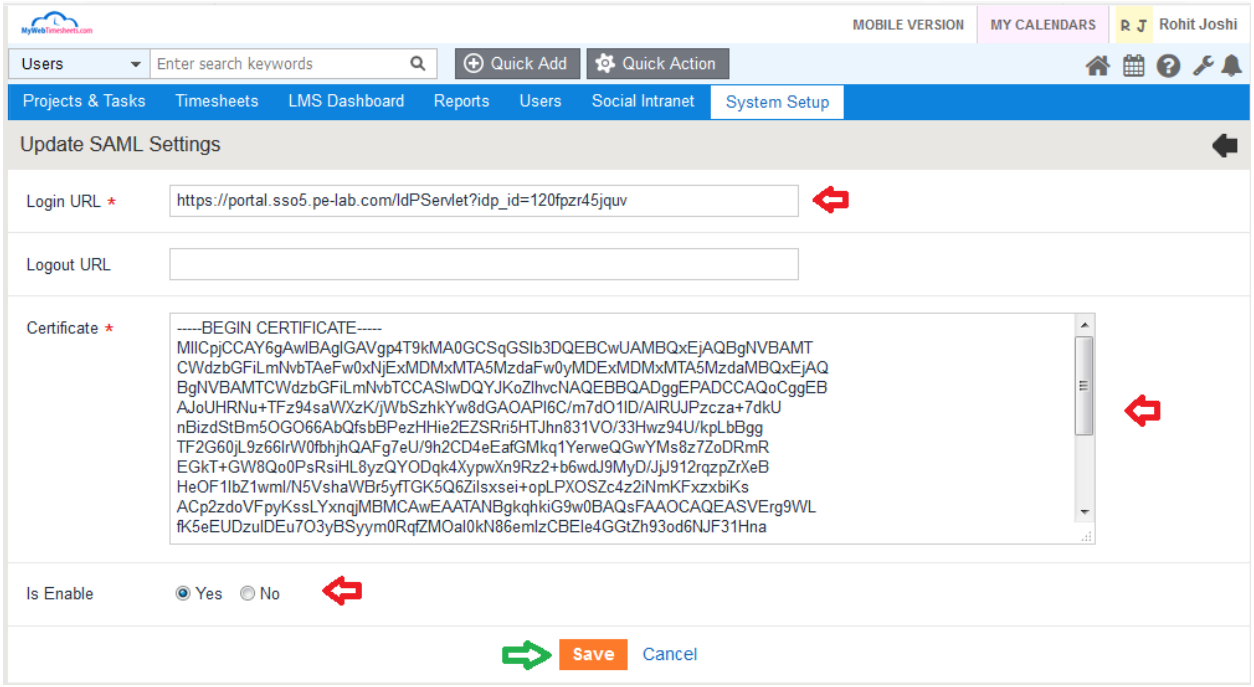
3. Following UI will be displayed. Go to *Security Management -> Company SAML Settings*.



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



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



a. **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>**.
b. 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.
c. **Certificate** : Paste the public certificate used in step 4d. on page 5.
d. **Is Enable** : Select **Yes** radio button to enable SAML SSO authentication.
e. Once sure of all settings, click on **Save** button to complete SAML configuration.

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