RSA SecurID Access SAML Configuration for Trumba

Last Modified: June 12, 2017

Trumba is a web-based events calendar used on the MassArt website. Currently, it is used to host MassArt's Events Calendar and Academic Calendar. Any member of the public can view the calendar information on the website. The calendars are administered by MassArt staff. The Events Calendar and Academic Calendar are publicly available for viewing.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Trumba.
- Obtain the IDR Portal metadata file.

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

SP Login URL	*https://www.trumba.com/sp/signin/1048155*
ACS URL	*https://www.trumba.com/sp/saml2/post*
Service Provider Issuer	*https://www.trumba.com/sp*

Procedure

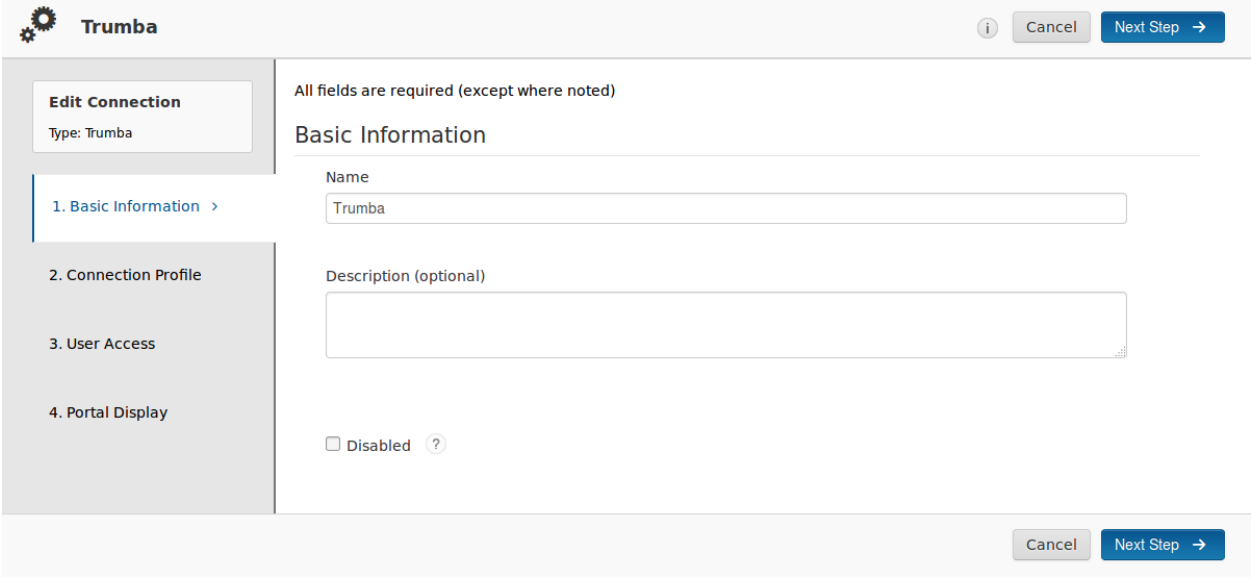
1. Add the Application in RSA SecurID Access
2. Configure Trumba to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

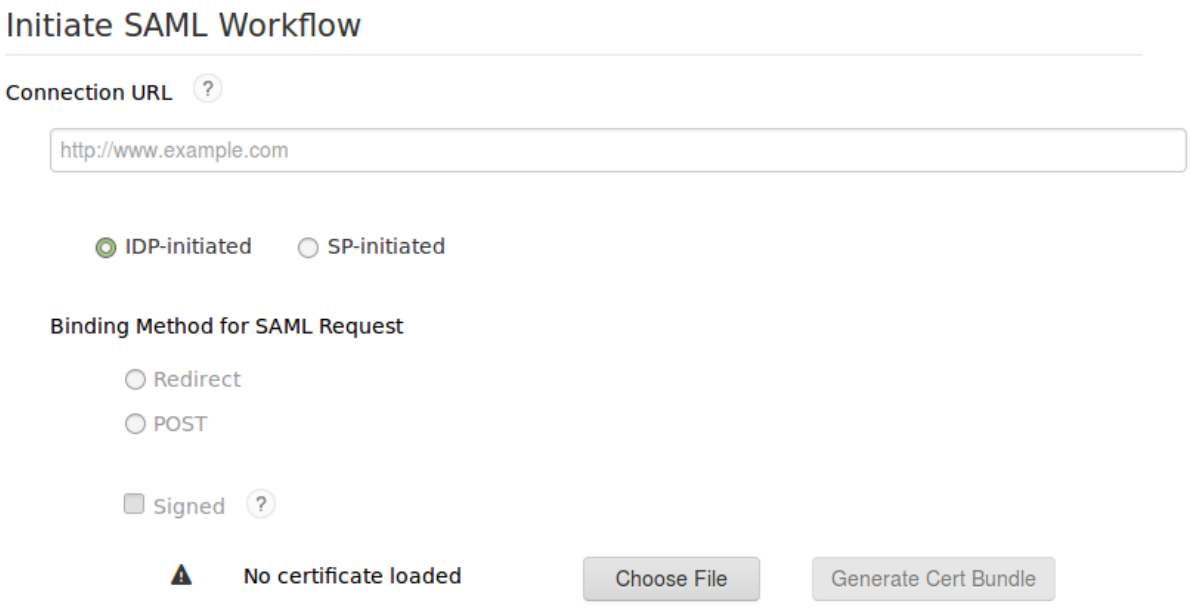
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Trumba.

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

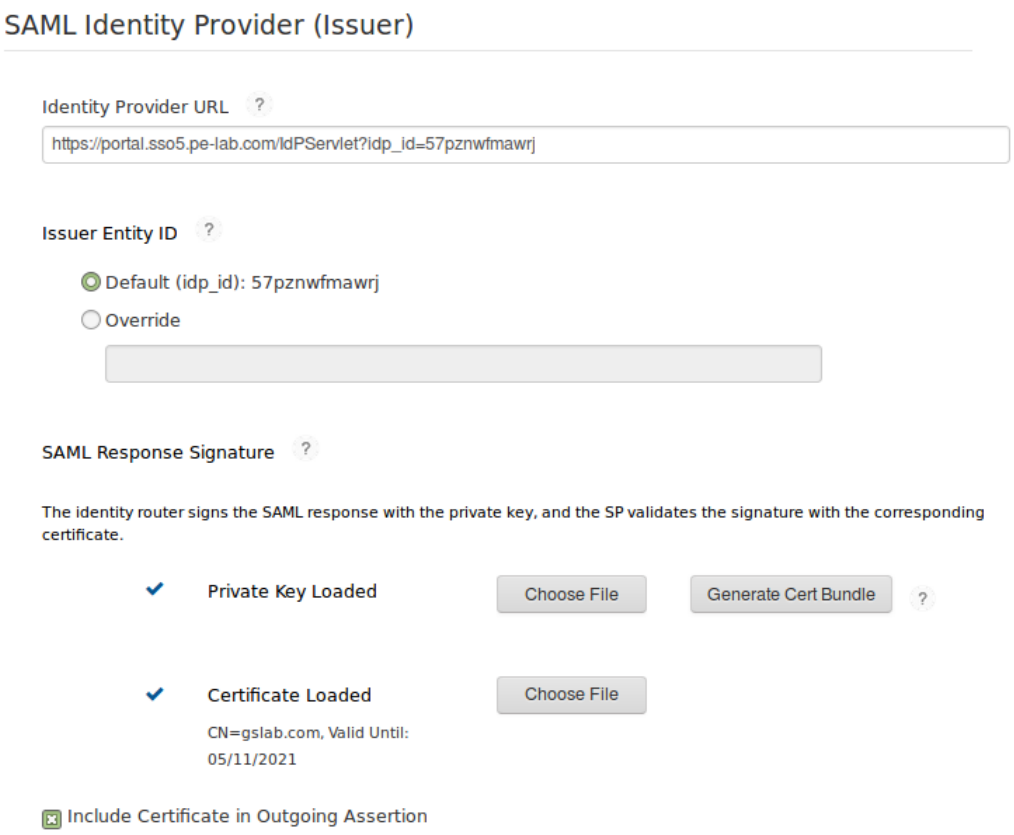


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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



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

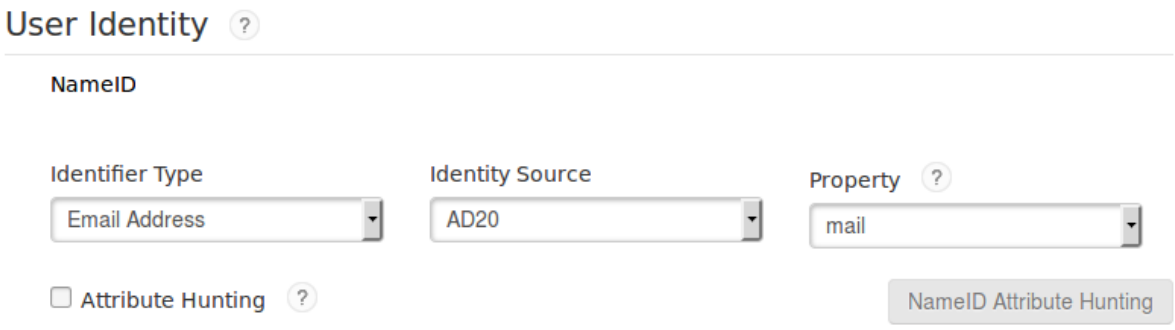


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File**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

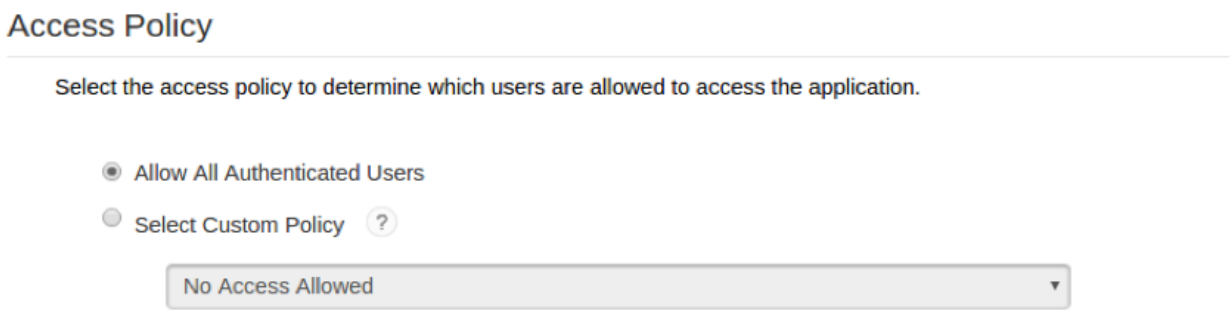
6. Scroll down to the **Service Provider** section.

   a. In the **Assertion Consumer Service (ACS) URL** field, provide value as per received from service provider.
   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.

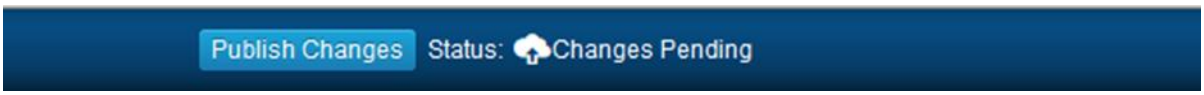


8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users** user policy from the available options.



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.

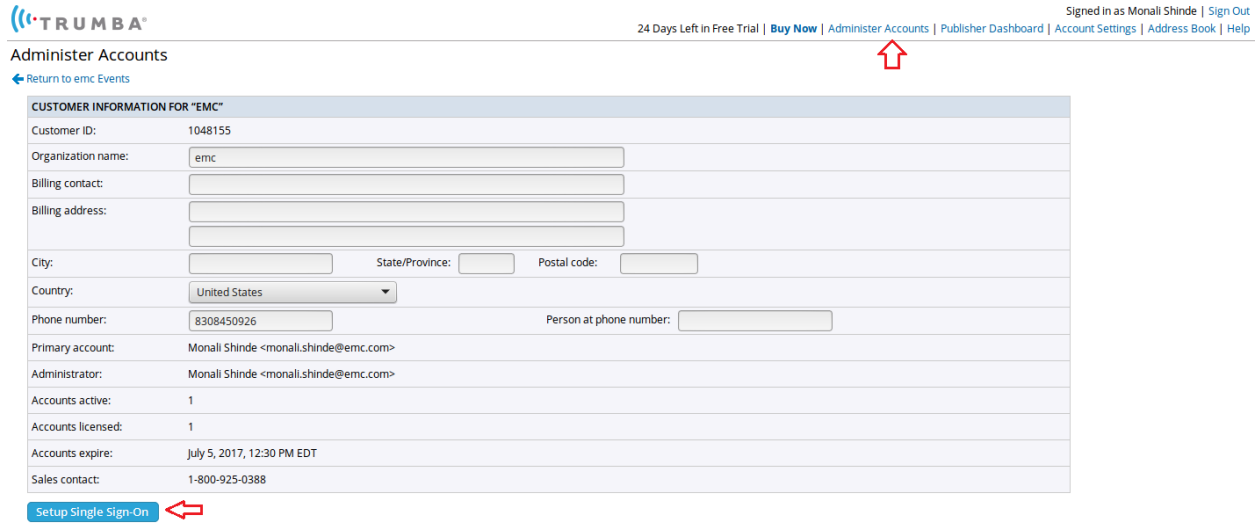


14. Navigate to **Applications > My Applications**.
15. Locate Trumba in the list and from the **Edit** pulldown select **Export Metadata**.

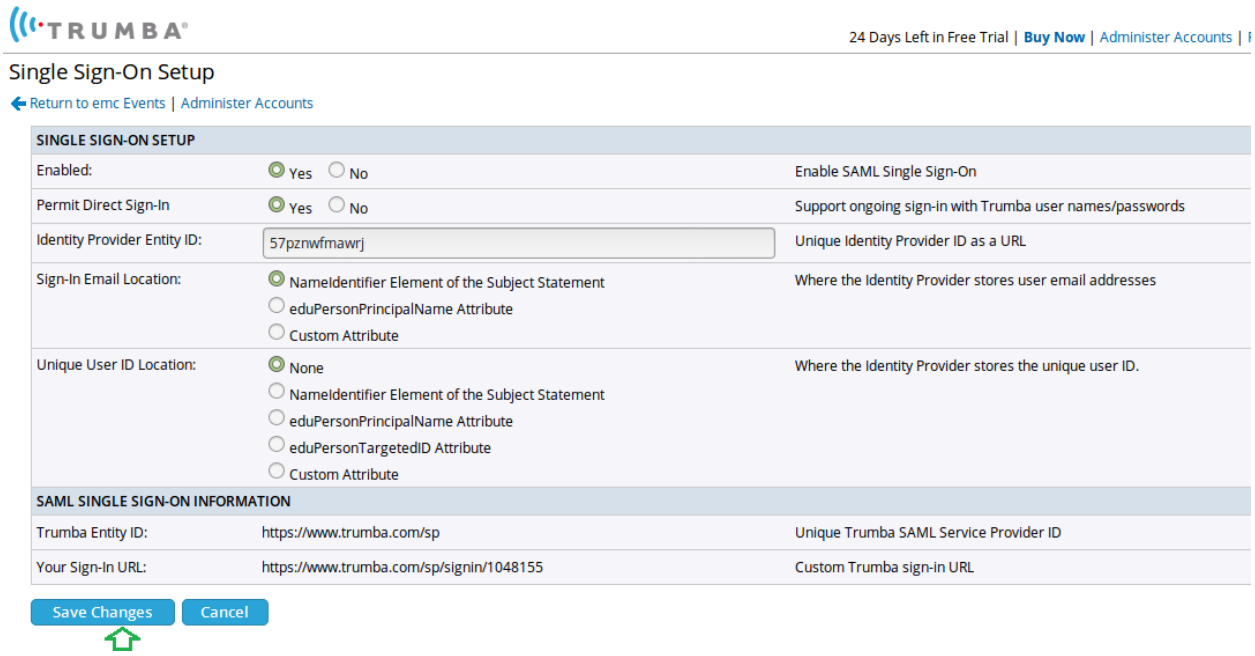
Configure Trumba to Use RSA SecurID Access as an Identity Provider

Procedure

1. Contact Trumba support and ask that your RSA metadata file get uploaded to your account.
2. Login to your Trumba application web account. (https://www.trumba.com/t.aspx?z=SignIn)
3. Following UI will be displayed. Click on *Administer Accounts -> Setup Single Sign-on.*



4. Following UI will be displayed.



   a) Complete all required fields.
   b) Enter the Identity Provider Entity ID from page 3 step 5.
   c) Click on *Save Changes* to save the configuration.

5. Your Trumba account is now enabled for SAML authentication.

MS