

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

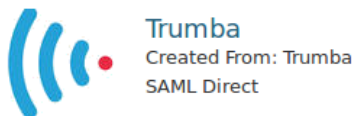
Procedure

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**.

The screenshot shows the 'Edit Connection' page for a Trumba connection. The page title is 'Trumba' with a gear icon. In the top right corner, there are 'Cancel' and 'Next Step →' buttons. A message at the top states 'All fields are required (except where noted)'. The 'Basic Information' section contains a 'Name' field with 'Trumba' entered, a 'Description (optional)' text area, and a 'Disabled' checkbox with a help icon. A sidebar on the left lists steps: '1. Basic Information >', '2. Connection Profile', '3. User Access', and '4. Portal Display'. At the bottom right, there are 'Cancel' and 'Next Step →' buttons.

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.

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): 57pznwfmawrj

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:
05/11/2021

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**.

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

Service Provider

Assertion Consumer Service (ACS) URL ?

https://www.trumba.com/sp/saml2/post

Audience (Service Provider Entity ID) ?

https://www.trumba.com/sp

- 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.

User Identity ?

NameID

Identifier Type

Email Address

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.



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*.

TRUMBA® 24 Days Left in Free Trial | Buy Now | Administer Accounts | Publisher Dashboard | Account Settings | Address Book | Help

Signed in as Monali Shinde | Sign Out

Administer Accounts

Return to emc Events

CUSTOMER INFORMATION FOR "EMC"	
Customer ID:	1048155
Organization name:	emc
Billing contact:	
Billing address:	
City:	State/Province: Postal code:
Country:	United States
Phone number:	8308450926 Person at phone number:
Primary account:	Monali Shinde <monali.shinde@emc.com>
Administrator:	Monali Shinde <monali.shinde@emc.com>
Accounts active:	1
Accounts licensed:	1
Accounts expire:	July 5, 2017, 12:30 PM EDT
Sales contact:	1-800-925-0388

Setup Single Sign-On

4. Following UI will be displayed.

TRUMBA® 24 Days Left in Free Trial | Buy Now | Administer Accounts |

Single Sign-On Setup

Return to emc Events | Administer Accounts

SINGLE SIGN-ON SETUP	
Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No Enable SAML Single Sign-On
Permit Direct Sign-In:	<input checked="" type="radio"/> Yes <input type="radio"/> No Support ongoing sign-in with Trumba user names/passwords
Identity Provider Entity ID:	57pznwfmawrj Unique Identity Provider ID as a URL
Sign-In Email Location:	<input checked="" type="radio"/> NameIdentifier Element of the Subject Statement Where the Identity Provider stores user email addresses <input type="radio"/> eduPersonPrincipalName Attribute <input type="radio"/> Custom Attribute
Unique User ID Location:	<input checked="" type="radio"/> None Where the Identity Provider stores the unique user ID. <input type="radio"/> NameIdentifier Element of the Subject Statement <input type="radio"/> eduPersonPrincipalName Attribute <input type="radio"/> eduPersonTargetedID Attribute <input type="radio"/> Custom Attribute
SAML SINGLE SIGN-ON INFORMATION	
Trumba Entity ID:	https://www.trumba.com/sp Unique Trumba SAML Service Provider ID
Your Sign-In URL:	https://www.trumba.com/sp/signin/1048155 Custom Trumba sign-in URL

Save Changes Cancel

- 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