LIGHTBOX

RIMS® Single Sign On (SSO) / SAML Fact Sheet

Introduction

RIMS supports Security Assertion Markup Language v2 (SAMLv2), an open standard protocol for Single Sign On.

This allows lending institutions on the RIMS platform to manage their users and those users' identities within the institution's system.

With SAML, selected data can be sent to automatically log users into RIMS.

Functionality

SAML exchanges digitally signed XML documents (SAML assertions) between system entities referred to as an Identity Provider and a Service Provider to authenticate a User.

Identity Provider (IdP)

An IdP is the source application or database where lenders manage their users' accounts and roles. This is also where the user will manually log in. The IdP makes SAML assertions about the identity of the user.

Service Provider (SP)

RIMS is the SP and uses the SAML assertions it receives from the IdP to verify and translate the data to a RIMS session by either looking up the user or creating a new account. Once found, it automatically logs the user into the application.

RIMS SSO is an IdP initiated authentication. The RIMS URL will redirect to the lender's SSO page provided.

Auto-provisioning options

1. **Auto-create Users:** If a user logs in via SAML and RIMS cannot find an existing user within the system, it will automatically create the user with the information from the required SAML Assertions. This setting is optional.
2. **Auto-update Users:** If a user logs in via SAML and RIMS finds the user, it compares the information from the SAML Assertions to the identified RIMS account. If the RIMS information does not match, the system will overwrite RIMS data with the SAML Assertions. This setting is optional.

Assumptions and expectations

1. Development and testing within a system outside of RIMS is the responsibility of the Client or other outside contracted partner.
2. RIMS is not responsible for the performance of any other third-party web service and sign on requirements they might have.
3. All RIMS code is proprietary to LightBox.

What RIMS requires for the process

1. **SAML Certificate fingerprint:** The lender must provide the certificate to be used as a fingerprint for each SAML request. IdP will use this certificate to digitally sign the SAML document before sending it to the SP. LightBox will then use this same certificate to validate the authenticity of each SAML request received. Generally, a member of the lender's Domain Trust Management team will have this information and can work with a member of LightBox's team to get the SAML configuration requirements identified and set up.
2. **SAML Entity ID:** Typically included within lender's metadata. If unable to provide metadata, SAML Entity ID will need to be provided separately.
3. **SAML Assertions (Fields):** The lender must select a field (or combination of fields) from a provided list to match a unique identity for each user. IdP will include these data points in their SAML assertions and SP will look up those values within the RIMS database to create a user session based on the RIMS account found. Additional details on fields may be found on the following page.

   a. **Field or field combination to authenticate against:** After determining the SAML Assertions to be brought over, this is identification of the specific fields used for authentication of users.

   It is recommended for this to be ImportUserID, although Email has been used in some instances, or a combination such as ImportUserID (or) Email (or) Name in combination with Role.
   ImportUserID is based on an internal lender identification, such as employee ID.
4. **Remote login URL:** This is the RIMS SSO application link (OKTA terminology: App Embed Link; Azure terminology: User Access URL). RIMS will use this link to redirect users if they try to log in directly within RIMS.
5. **Remote logout URL:** Users will be redirected to the logout URL when clicking the Logout button within RIMS. It is recommended to be an internal lender intranet site.
6. **Auto-provisioning:** Decision whether the options to auto-create users and/or auto-update users will be activated.

SAML Assertions (Fields)

At least 1 of the fields below must be required for authenticating.

<table>
<tr><th>Field Name</th><th>Required for Auto-Provisioning</th><th>Notes</th></tr>
<tr><td><b>Email</b></td><td>Yes</td><td></td></tr>
<tr><td><b>Import User ID/External User ID (SAML “NameID”)</b></td><td>Yes, if authenticating on ImportUserID</td><td>This is a text field within RIMS the lender can use to store another unique identifier for the user.
Typically, this is the user code within the lender’s internal system.</td></tr>
<tr><td><b>Role</b></td><td>Yes</td><td>Values are either User Type IDs or User Type name.
<i>Acceptable Role Value Examples:</i>
<table>
<tr><th>RIMS User Type</th><th>UserTypeID</th><th>User Type</th></tr>
<tr><td>Content Administrators</td><td>200</td><td>RIMS_ContentAdmins</td></tr>
<tr><td>Job Manager</td><td>500</td><td>RIMS_JobMgrs</td></tr>
<tr><td>Vendor Job Manager</td><td>600</td><td>RIMS_VendorJobMgrs</td></tr>
<tr><td>Account Officer</td><td>800</td><td>RIMS_AcctOfficers</td></tr>
</table></td></tr>
<tr><td><b>First Name</b></td><td>Yes</td><td></td></tr>
<tr><td><b>Last Name</b></td><td>Yes</td><td></td></tr>
<tr><td><b>Address</b></td><td>No</td><td></td></tr>
<tr><td><b>City</b></td><td>Optional</td><td>Based upon request to be required field</td></tr>
<tr><td><b>State</b></td><td>Optional</td><td>Based upon request to be required field</td></tr>
<tr><td><b>Zip</b></td><td>Optional</td><td>Based upon request to be required field</td></tr>
<tr><td><b>Phone Number</b></td><td>No</td><td></td></tr>
<tr><td><b>Cost Center</b></td><td>No</td><td></td></tr>
<tr><td><b>Lending Group</b></td><td>No</td><td></td></tr>
<tr><td><b>Job Type Restriction</b></td><td>No</td><td>Comma-separated list of job types to be available for a Job Manager when user is auto-created.
Acceptable job types:
Appraisal, Construction, Environmental
Values are case-insensitive and can be listed in any order.</td></tr>
<tr><td><b>Job Type Restriction Access</b></td><td>No</td><td>Comma-separated value indication as to the level of access for the job types listed in JobTypeRestriction; it must follow order set by JobTypeRestriction.
Acceptable values: Full, Restricted, None
Values are case-insensitive.
Order requirement example, for a Job Manager able to create and update Construction jobs but not Appraisal or Environmental the following fields and values would be included:
JobTypeRestriction: Appraisal, Construction, Environmental
JobTypeRestrictionAccess: None, Full, None</td></tr>
</table>

LightBox RIMS SSO Checklist

Use the below checklist to ensure information needed for SSO setup has been reviewed and is ready for RIMS.

RIMS SSO customer setup checklist

Lender Institution Name		Done
SAML Certificate Fingerprint	Sent to LightBox on ____________	□
SAML Entity ID	Sent to LightBox on ____________	□
SAML Assertations (Fields) determined	Sent to LightBox on ____________	□
Authentication Field Identification		□
Remote Login URL		□
Remote Logout URL		□
Auto-create?	Yes or No	□
Auto-update?	Yes or No	□

lightboxre.com

LIGHTBOX

LOCATE. ANALYZE. ACT.