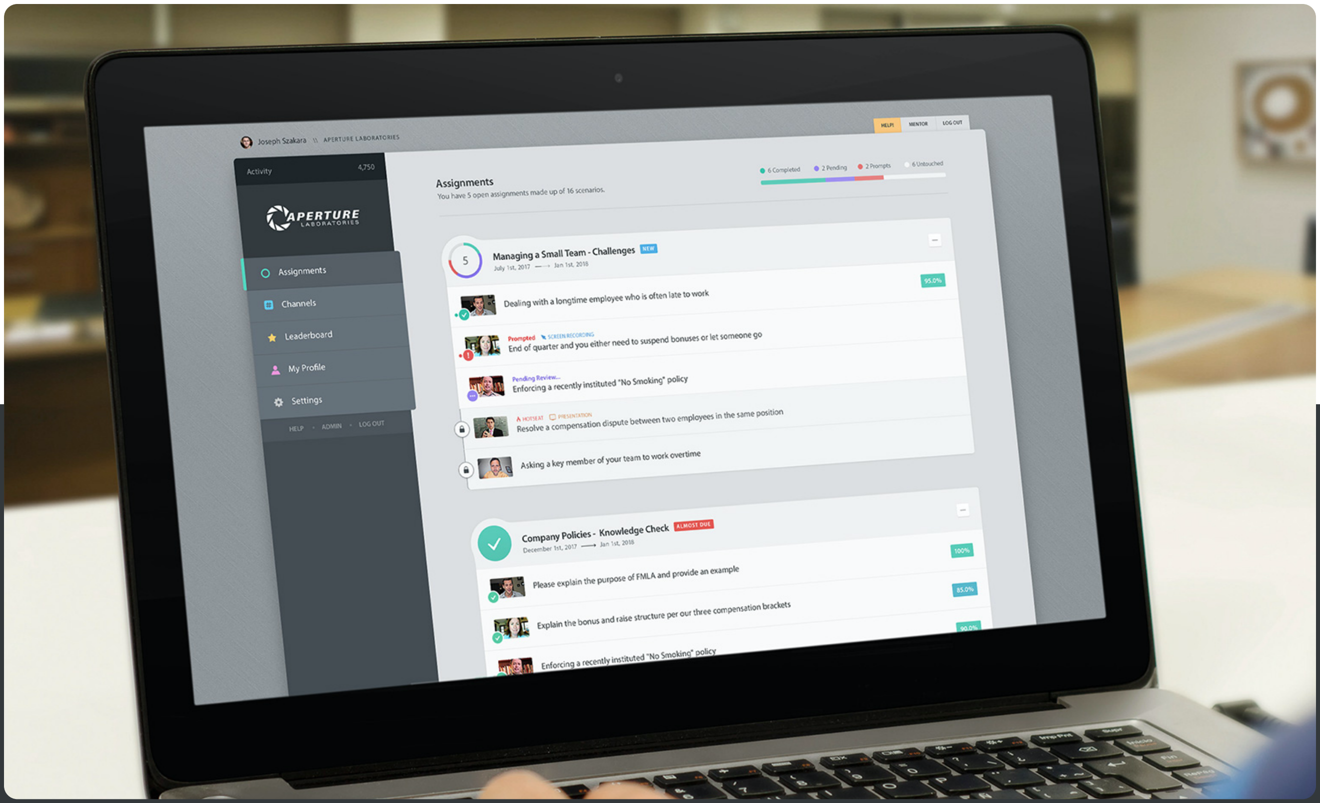
Joseph Szakara
APERTURE LABORATORIES
HELP!
MENTOR
LOG OUT
Activity
4,750
APERTURE LABORATORIES
Assignments
Channels
Leaderboard
My Profile
Settings
HELP
ADMIN
LOG OUT
Assignments
You have 5 open assignments made up of 16 scenarios.
6 Completed
2 Pending
2 Prompts
6 Untouched
Managing a Small Team - Challenges
NEW
July 1st, 2017 → Jan 1st, 2018
95.0%
Dealing with a longtime employee who is often late to work
Prompted
SCREENRECORDING
End of quarter and you either need to suspend bonuses or let someone go
Pending Review...
Enforcing a recently instituted "No Smoking" policy
HOTSEAT
PRESENTATION
Resolve a compensation dispute between two employees in the same position
Asking a key member of your team to work overtime
Company Policies - Knowledge Check
ALMOST DUE
December 1st, 2017 → Jan 1st, 2018
100%
Please explain the purpose of FMLA and provide an example
85.0%
Explain the bonus and raise structure per our three compensation brackets
90.0%
Enforcing a recently instituted "No Smoking" policy

Rehearsal SSO-SAML 2.0 Integration Guide v3.1

Key information regarding the integration points between the Rehearsal platform and a customer's SSO security domain using SAML 2.0

rehearsal

Contents

1. Introduction

This document's purpose is to provide key information regarding the integration points between the Rehearsal platform and a customer's SSO security domain using SAML 2.0.

2. SSO Integration Options and User Information

When integrating SSO with Rehearsal there are a couple of initial decisions that need to be made regarding information that will be passed between the systems. Our SSO integration allows you to provide basic user information for authentication and optionally the ability to pass additional information that can be used to configure the system automatically.

2.1 Basic User Information (Required)

The basic user information required by the Rehearsal system is as follows:

- Email address
- First name
- Last name

2.2 Additional User Information

Additional user information can be passed to enhance reporting, searching and overall user management. The additional information is as follows:

- **Title** – Title of the user.
- **Country** – Country the user is associated with. (Examples: US, Germany, Spain, or EMEA, APAC, LATAM, NA).
- **Region** – Region the user is associated with. (Examples: North East, Central, West)
- **Territory** – Territory the user is associated with. (Examples: Ohio Valley, New York, Northern Nevada).
- **Department** – Department the user is associated with. (Examples: Marketing, Sales, Services).
  Location – Location the user is associated with. (Examples: Corporate HQ, Bldg 2, Floor 3).

2.3 User Relationships

The Rehearsal system allows you to pass additional information regarding group membership and mentoring relationships. This is NOT Required and can also be set up at a later date.

- **Hierarchy –** The Rehearsal system allows you to pass an Employee ID (also known as Enterprise ID or World Wide ID) of the manager and user to form a direct relationship that should be set up as user specific mentors of the user.

  Note: Users must have an account within the system to log in.

- **User Specific Mentors** – The Rehearsal system also allows you to pass email addresses of users that should be set up as user specific mentors of the user.
  - **Mentee Of Users** – These are users who will be setup as a mentor for the user.
  - **Mentor Of Users** – These are users who will be setup as a mentee for the user.

  Note: Users must have an account within the system to log in.

- **Group Membership** – The Rehearsal system allows you to pass group names where the user should be added. You have two options for group membership.
  - **Member Of Groups** – These are groups where you want the user added as a learner.
  - **Mentor Of Groups** – These are groups where you want the user added as a mentor.

  Note: Groups are automatically created if they don't exist within the system.

2.3.1 Additive or Deductive?

When setting up SSO for Rehearsal and passing user relationship details you will need to determine if you want the system to be additive or deductive when setting up the information.

- **Additive** (default): When we set your SSO integration to additive this means that the system will just add the details under specific claims and won't remove the user from other areas. This is the best option if you are not trying to have strict control over user relationships. Below is a list of the specific claims affected and how they will work with this method.
  - ***Member Of***: The system will add the user as a learner to the listed groups, however it will not remove the user from any other groups.
  - ***Mentor Of***: The system will add the user as a mentor to the listed groups, however it will not remove the user as a mentor from any other groups.
  - ***User Specific Mentors***: The system will add the additional user specific mentors to the user's profile, however it will not remove existing user specific mentor.
- **Deductive**: When we set your SSO integration to deductive this means that the system will add the details under specific claims and will remove the user from other areas not listed in the claim. This is the best option if you are trying to have strict control over user relationships. Below is a list of the specific claims affected and how they will work with this method.
  - ***Member Of***: The system will add the user as a learner to the listed groups and will remove the user from any other groups not listed.

- ***Mentor Of***: The system will add the user as a mentor to the listed groups and will remove the user as a mentor from any other groups not listed.
- ***User Specific Mentors***: The system will add the additional user specific mentors to the user's profile and will remove existing user specific mentors who are not in the details provided.

Note that the ***default setting is additive*** and is flagged in the system on the Rehearsal side.

2.4 User Tags

The Rehearsal system allows you to pass any additional information regarding the user and will add the information as tags for the user. Passing additional information is NOT Required and can also be set up at a later date.

As an example, you can pass Country, Department, Title, and the system will create a tag for each (Country:US, Departments:Sales, Title:Account Manager).

3. SSO Configuration and Testing Process

This section outlines the general SSO process we will follow to get your Rehearsal site configured for SSO and tested.

SSO Steps	**Summary**
1. Initial Meeting	• Discuss the Rehearsal SSO configuration and overall process. • Technical teams to discuss needs and ask questions.
2. Staging Configuration	• Rehearsal creates Staging Site. • Rehearsal provides Staging Site SAML Metadata to Customer. • Customer adds Rehearsal as Service Provider in SSO system. • Customer provides SSO staging configuration data to Rehearsal.
3. Staging Test	• Customer tests the Staging Site with 3-5 users. • Rehearsal verifies configuration with customer.
4. Production Configuration	• Rehearsal provides Production Site SAML Metadata to Customer. • Customer adds Rehearsal as Service Provider in SSO system. • Customer provides SSO production configuration data to Rehearsal.
5. Go-Live	• Customer establishes a Go-Live Date/Time. • Customer conducts an Immediate Test upon Go-Live.

4. SAML Assertion

4.1 Subject Element

SAML assertions with Rehearsal are made about a subject, represented by the `<saml:Subject>` element in the assertion which identifies the authenticated principal. This element contains the `<saml:NameID>` element, which should be a unique property of the user that will never change. An employee ID is a good candidate for this property. Try not to use an employee's email address, as these may change over time.

Example SAML assertion showing the `<saml:NameID>` element:

```
<saml:Assertion
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75"
   Version="2.0"
   IssueInstant="2004-12-05T09:22:05Z">
   <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
   <ds:Signature
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
   <saml:Subject>
     <saml:NameID
       Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
       3f7b3dcf-1674-4ecd-92c8-1544f346baf8
     </saml:NameID>
     ...
```

Note: the SAML assertion above is truncated and for illustrative purposes only. Yours may differ.

4.2 Supported Attribute Assertions

A SAML attribute assertion contains information about a user in the form of a series of attributes. The following is a list of attribute assertions accepted by Rehearsal.

Note that the `emailaddress` attribute assertion is **required** by Rehearsal.

Note the attribute assertions must be **lowercase**.

Attribute Assertion (must be lowercase)	Usage	Example
`emailaddress` (Required)	- email address of the user - Accepts a single valid email string	sam.jones@rehearsal.com
`firstname`	- First Name of the user - Accepts a single string	Sam
`lastname`	- Last Name of the user	Jones

	• Accepts a single string	
`title`	• Title of the user • Accepts a single string	Client Services
`country`	• Country of the user • Accepts a single string	US
`region`	• Region of the user • Accepts a single string	West
`territory`	• Territory of the user • Accepts a single string	Northwest
`department`	• Department of the user • Accepts a single string	CS
`location`	• Location of the user • Accepts a single string	Reno
`hierarchy`	• User to Manager relationship via enterprise IDs • Accepts a string formatted with “managerid,userid” • Rule: If a Manager ID is not present the user is created in the system	
`menteeofusers`	• Email Addresses of users that are specific mentors of the user • Accepts a string of comma separated email addresses • Rule: If a user specific mentor is not present the user is created in the system • Rule: Additive/Deductive – See Section 2.3.1 for details	mentee1@rehearsal.com
`mentorofusers`	• Email Addresses of users that are specific mentees of the user • Accepts a string of comma separated email addresses • Rule: If a user specific mentor is not present the user is created in the system • Rule: Additive/Deductive – See Section 2.3.1 for details	mentee2@rehearsal.com
`memberofgroups`	• Groups where the user is to be added as a learner of the group • Accepts a string of comma separated group names • Rule: If a group doesn’t exist the group will be created in the system • Rule: Additive/Deductive – See Section 2.3.1 for details	GroupNameB, GroupNameC
`mentorofgroups`	• Groups where the user is to be added as a mentor of the group • Accepts a string of comma separated group names • Rule: If a group doesn’t exist the group will be created in the system • Rule: Additive/Deductive – See Section 2.3.1 for details	GroupNameA
`tag`	• Accepts a string of comma separated values • Each value will be treated as a separate tag. • Example: “customtagattribute1,customtagattribute2" will be added to the user as two separate tags “customtagattribute1” and “customtagattribute2”.	Country:US, Departments:Sales, Title:Account Manager

	• Rule: If a tag doesn't already exist it will be added to the user	