

Single Sign-On Technical Specification

Overview

LearningZen supports Single Sign-On (SSO). To integrate with SSO, you will need to place a user-specific link to LearningZen.com on your site (or intranet, etc.).  You will also need to create a simple web service with which the LearningZen server can communicate. The web service will tell us if the user is currently logged in and will provide some basic information about that user.  If the user already has an account inside LearningZen, their basic information will be updated.  If it is a new user, a LearningZen account will automatically be created. Your web service must implement two methods: /loginCheck and /getUserInfo and your LearningZen portal will need to be configured properly.

Configuration

To properly configure SSO, the Third Party (TP) must provide LearningZen with the following information:

* **Base Web Service URL**: the base URL of your web service. The API method name will be appended to the end of this URL when making an API call. e.g. https://third-party.com/api
* **Authentication Failure URL**: where we should send your users when authentication fails, presumably your log in page. e.g. https://third-party.com/login

Step-by-Step

The steps below walk you through the SSO mechanism:

* A user logs into the TP site, intranet, etc.
* TP presents the user with a link that sends them to LearningZen via any valid LearningZen URL passing the authentication token for the given user
  + <http://thirdparty.learningzen.com/Study/priv/MyStudy.aspx?token=abc123>
* To authenticate the user, the LearningZen server will send an HTTP POST to the TP API by appending “/loginCheck” to the “Base Web Service URL”:
  + <https://third-party.com/api/loginCheck>
  + Request:

<?xml version=”1.0” encoding=”UTF-8” ?>

<request>

<token>abc123</token>

<sourceIP>127.0.0.1</sourceIP>

<portalHost>thirdparty</portalHost>

</request>

* If the response is a failure (<success>0</success>), redirect user to the “Authentication Failure URL”
* If the response is a success (<success>1</success>), record <accountID/>
  + Response:

<?xml version=”1.0” encoding=”UTF-8” ?>

<response>

<success>1</success>

<accountID>54321</accountID>

</response>

* To get/update the user’s information, the LearningZen server will send an HTTP POST to the TP API by appending “/getUserInfo” to the “Base Web Service URL”:
  + <https://third-party.com/api/getUserInfo>
  + Request:

<?xml version=”1.0” encoding=”UTF-8” ?> 

<request>

<token>abc123</token>

<sourceIP>127.0.0.1</sourceIP>

<portalHost>thirdparty</portalHost>

</request>

* If the response is a failure (<success>0</success>), redirect user to the “Authentication Failure URL”
* If the response is a success (<success>1</success>), either create the user (if they don't exist in LearningZen), or update the existing user's information. Associate the <accountID/> with the user.
  + Response:

<?xml version=”1.0” encoding=”UTF-8” ?>

<response>

<success>1</success>

<userGroups>Group One,Group Two</userGroups>

<managerGroups>Group Three</managerGroups>

<isPortalAdmin>0</isPortalAdmin>

<isAuthor>1</isAuthor>

<isManager>0</isManager>

<firstName>John</firstName>

<lastName>Doe</lastName>

<emailAddress>john@doe.com</emailAddress>

<timeZoneName>Eastern Standard Time</timeZoneName>

</response>

* The data that the TP API returns to a getUserInfo request may contain invalid combinations (e.g. managerGroups contains group names, but isManager is 0). In most cases, LearningZen can ignore invalid combinations and update the user appropriately (we call these warnings). However, in some cases, if the data is incorrect (errors), authentication fails and the user is redirected to the Authentication Failure URL. If the getUserInfo call results in any warnings or errors, an email will be sent to all the portal administrators summarizing the problems.
* At this point, if the user has not been redirected to the Authentication Failure URL, they will be logged into LearningZen and will be redirected to the page they were originally trying to access. The user will remain logged into LearningZen until their LearningZen session is ended.

Data Format

Data Requirements

Each request initiated by LearningZen will contain common elements.

|  |  |  |
| --- | --- | --- |
| **Name** | **Type** | **Notes** |
| token | string | The security/session token passed for each request, this can be time-based and is separate from the accountID |
| sourceIP | IP address | The IP address of the originating user |
| portalHost | string | The LearningZen portal hostname |

Responses from the destination API will also contain common elements.

|  |  |  |
| --- | --- | --- |
| **Name** | **Type** | **Notes** |
| success | bit | “1” if the request was successful; “0” if it failed. |

Data Format

Data requests and responses are encapsulated in an XML format. The following is an example of the common elements sent when LearningZen initiates a request.

<?xml version=”1.0” encoding=”UTF-8” ?>

<request>

<token>U38Neqk0lqz4Cx</token>

<sourceIP>127.0.0.1</sourceIP>

<portalHost>sandbox</portalHost>

</request>

The response from the destination API with only the common elements would be formatted as follows:

<?xml version=”1.0” encoding=”UTF-8” ?>

<response>

<success>1</success>

</response>

Calls to Third-Party API

loginCheck

Called by LearningZen to authenticate a user

**URL example:** <https://third-party-api.com/api/loginCheck>

**Request example:**

<?xml version=”1.0” encoding=”UTF-8” ?> 

<request>

<token>abcdef123456</token>

<sourceIP>127.0.0.1</sourceIP>

<portalHost>thirdpartysandbox</portalHost>

</request>

**Response example:**

<?xml version=”1.0” encoding=”UTF-8” ?>

<response>

<success>1</success>

<accountID>54321</accountID>

</response>

|  |  |  |
| --- | --- | --- |
| **Name** | **Type** | **Notes** |
| accountID | string | The user’s unique account ID. This element is required if success is “1”. |

getUserInfo

Called by LearningZen to authenticate a user

**URL example:** <https://third-party-api.com/api/getUserInfo>

**Request example:**

<?xml version=”1.0” encoding=”UTF-8” ?>

<request>

<token>abcdef123456</token>

<sourceIP>127.0.0.1</sourceIP>

<portalHost>thirdpartysandbox</portalHost>

</request>

**Response example:**

<?xml version=”1.0” encoding=”UTF-8” ?>

<response>

<success>1</success>

<userGroups>Group One,Group Two</userGroups>

<managerGroups>Group Three</managerGroups>

<isPortalAdmin>0</isPortalAdmin>

<isAuthor>1</isAuthor>

<isManager>0</isManager>

<firstName>John</firstName>

<lastName>Doe</lastName>

<emailAddress>john@doe.com</emailAddress>

<timeZoneName>Eastern Standard Time</timeZoneName>

</response>

|  |  |  |
| --- | --- | --- |
| **Name** | **Type** | **Notes** |
| userGroups | string list | Comma separated list of groups to which the user belongs. LearningZen will automatically update the user’s membership in the portal groups specified, removing the user from all groups not included in the list. Groups that do not exist will be ignored. |
| managerGroups | string list | Comma separated list of groups for which the user is a manager. Functionality is otherwise the same as for the userGroups element. Only applicable if isManager below is “1”. |
| isPortalAdmin | bit | If “1”, LearningZen will update the user’s access rights to be a portal administrator. If “0”, LearningZen will remove any administrative rights for the user. |
| isAuthor | bit | If “1”, LearningZen will add the user to the list of portal authors. If the portal is already at the maximum number of portal authors, this request will be ignored. If “0”, LearningZen will remove the user from the list of portal authors. |
| isManager | bit | If “1”, LearningZen will add the user to the list of portal managers. If “0”, LearningZen will remove the user from the list of portal managers. |
| firstName | string | User’s first name. |
| lastName | string | User’s last name. |
| emailAddress | string | User’s email address. Used in LearningZen as the account login. |
| timeZoneName | string | Possible values found here:  http://www.learningzen.com/developers |