Contents

Overview

Definitions

Concept
  Single Sign-on Process Flow
  Single Sign-on Authentication Process

Single Sign-on into Desire2Learn

Authentication Request Generation Component
  Generating the GUID using the Security Check Component
  Posting the guid and user identifier

Security Check Component

Authentication Processing Component
Overview

This document contains the information required to use the D2L Single Sign-On Authentication Interface. It’s intended for development and design teams implementing integrations using the Single Sign-On component. This document is intended for use with the Security Check API documentation, which describes how the Generation and Validation of GUIDs is accomplished.

Definitions

**Destination System**  The system that processes the Single Sign-On Request for authentication.

**GUID**  Globally Unique Identifier. The GUID contains information about the system it was generated for, the transaction it was approved for, and its operating lifespan.

**GUID Version 1**  GUID version available in the LMS prior to and including version 9.0

**GUID Version 2**  GUID version available in the LMS starting from version 9.0

**Integrated System**  The systems that is being integrated with the LMS.

**LMS**  The D2L Application

**Source System**  The system that generates Single Sign-On request. This system may generate the GUID, or acquire it from an external system.

Concept

The Single Sign-On Authentication Interface provides a mechanism for authenticating with the Desire2Learn LMS without requiring the end user to enter a username and password if they are coming from a system they already authenticated with. The Source System submits to the LMS a user identifier for the SSO request, as well as a GUID which guarantees the integrity of the request.

The Security Check component can also be utilized for implementing a Single Sign-On implementation where the Desire2Learn system is the source system, and another system is the Destination.

Single Sign-on Process Flow

The general process flow for the Single Sign-on process is as follows:
1. A trusted Source System generates a GUID.

2. The Source System passes the GUID along with a user identifier to the Destination System.

3. The Destination System verifies that the GUID and user identifier are valid for the Authentication request, at the time of receipt.

4. The Destination System Responds with the appropriate action:
   a. If the GUID and user identifier is valid, the user is authenticated to the system.
   b. If the GUID is user identifier is invalid, the user is given an opportunity to authenticate with the system using their username and password.

---

**Single Sign-on Authentication Process**

The Single Sign-On process flow can be summarized with the following flow chart.
Single Sign-on into Desire2Learn

Single Sign-on into Desire2Learn consists of three main components, two of which have already been developed by Desire2Learn and a third, which must be developed by those with access to the source system. Samples are provided for the component that requires development.

Authentication Request Generation Component

The authentication request generation component is activated via a link or button in the source system. The component has two main phases: one to generate the GUID using the Security Check Component, one to post the transaction to the Authentication Processing Component within the Desire2Learn LMS.

Generating the GUID using the Security Check Component

Starting from version 9.0, two versions of the GUID are supported:

- Version 1 – backwards compatible with LMS versions prior to 9.0
• Version 2 – new as of LMS version 9.0

Version 2 of the GUID is more secure and is recommended over version 1.

In order to generate the GUID, the GenerateExpiringGuid method of the Security Check Component is used. The Security Check Component provides details on how to utilize the GenerateExpiringGuid method from a dll or Web Service.

Version 2 of the GUID can only be obtained from the Web Service. Version 1 can be obtained from the dll or Web Service.

Version 1

The GenerateExpiringGuid method of the Version 1 dll has 5 parameters that are required for SSO to function. They are as follows:

1. guidType – SSO
2. orgID – The OrgID of the destination Desire2Learn Organization
3. installCode – The Unique Installation Code for the destination Desire2Learn Installation
4. TTL – The length of time that the GUID will be considered Valid. The default is 30 seconds, and 30 seconds is the maximum.
5. Key – The key for single sign-on is actually made up of the following two strings concatenated together
   a. The Destination Organizations LocalPrivateKey, which is configured in the DOME at Tools/Login/LocalPrivateKey
   b. The unique identifier being used for the user (username, orgdefinedid, or userid), where the unique identifier matches the corresponding identifier in the LMS.

C# GUID Generation Sample

```csharp
D2LGuids.D2LGuid d2lguid = new D2LGuids.D2LGuid();
String guid = d2lguid.GenerateExpiringGuid(
    D2LGuids.D2LGuid.GuidType.SSO,  // GuidTypeEnumeration
    "6605",  // OrgId
    "D2L_Test",  // Installation Code
    5,  // TTL
    "fakesharedsecretjsmith" );  // Key
```

Version 2

The GenerateExpiringGuid method of the Version 2 Web Service has 6 parameters that are required for SSO to function. They are as follows:

1. guidType – SSO
2. orgID – The OrgID of the destination Desire2Learn Organization
3. **installCode** – The Unique Installation Code for the destination Desire2Learn Installation

4. **TTL** – The length of time that the GUID will be considered Valid. The default is 30 seconds, and 30 seconds is the maximum.

5. **data** - The unique identifier being used for the user (username, orgdefinedid, or userid), where the unique identifier matches the corresponding identifier in the LMS.

6. **key** - The Destination Organizations LocalPrivateKey, which is configured in the DOME at Tools.Login.LocalPrivateKey

**Version 2 GUID Generation Sample Request**

```
POST /d2l/guids/d2l.guid.2.asmx?op=GenerateExpiringGuid
HTTP/1.1
Host: d2lurl
Content-Type: application/x-www-form-urlencoded
Content-Length: length

guidType=SSO&orgId=6605&installCode=D2L_Test&TTL=5&data=jsmith&key=fakesharedsecret
```

**Posting the guid and user identifier**

The guid that was generated in the previous step must be posted or passed on the query string along with the unique identifier for the user to the destination Desire2Learn organization. The unique identifier must be the same unique identifier that was used to generate the guid, and can consist of one of: username, orgdefinedid, userid.


**Required Parameters:**
Guid (generated in previous step)

**Required Parameters:**
One of:
- userid
- username
- orgdefinedid

**Sample Full Authentication Requests:**
**Note** It is also possible to submit a destination org unit along with the guid and user identifier using the orgid parameter and a valid org unit the user is enrolled in. This will direct the user to that homepage when they are authenticated.

---

**Security Check Component**

The Security Check component (D2LGuids) is described in detail in the document: API Document – Security Check.

---

**Authentication Processing Component**

The Authentication Processing Component is provided by Desire2Learn, and consists of the necessary processing logic to ensure that the SSO Authentication request is legitimate and allowed for the organization.

In order for the Authentication Processing Component to function, the LocalPrivateKey must be configured in the DOME for the organization being configured. The variable is found under Tools.Login.LocalPrivateKey. The value set in this location must match that used by the Source application generating the SSO request.

The authentication processing component has the following behavior:

1. Obtain the variables from the query string
   a. Guid
   b. Username, userid, or orgdefinedid
2. Obtain the LocalPrivateKey from the database
3. Obtain the installCode from the database
4. Check the Validity of the guid
   a. If the guid is valid, the user is authenticated to the LMS and sent to their homepage
   b. If the guid is invalid, the user is presented the standard login page for the destination environment.

**Note** The authentication processing component can optionally receive an orgid which directs the user to a particular homepage once they have been authenticated. The user must be enrolled in this org unit id in order for this to work.