DIGI[cation]™

Digication Single Sign-On Process

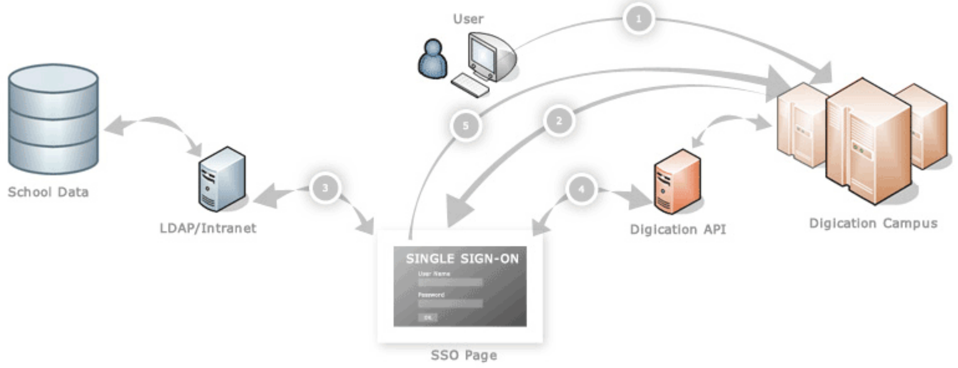
Overview

The purpose of this document is to outline the process of implementing single password or single sign-on between Digication and an external institution.

Digication does not talk directly to an LDAP server or other source of authentication information, both for performance reasons and due to firewalls and transport-level security issues. In addition, true single-sign on (where a user enters a username and password once and can access all systems) cannot be implemented using this method.

Please note that this document covers the minimum information necessary to get an SSO installation running. Please contact support@digication.com for assistance and reference implementation code.

Process Overview



The **SSO page** consists of one or more web-based programs hosted at the school or university. It is capable of requesting that the user login through a form, verifying the user's login information is correct, and passing information to the Digication API.

A typical SSO implementation occurs through the following steps:

1) The user visits Digication and clicks a 'Login' button or attempts to access a protected resource.
2) The user is redirected to an SSO page.
3) The user successfully logs in (or is determined to already be logged in) within the school or institution.
4) The SSO page sends a request via the Digication API to sign in a user. The API will respond with a single-use, time-restricted token that allows the user to login.
5) The SSO page redirects the user back to Digication with the login token.

The user is now logged in and automatically directed back to the resource they originally requested.

API Access

All requests to the Digication API use the same format – they include an API Access Key, a method, and one or more parameters. Requests are valid over both HTTP and HTTPS, however secure transport is strongly encouraged.

The API access key is a shared secret that enables you to access and modify school or institution data. It should be protected the same way an administrator password would be. The API access key can be obtained and changed by anyone with an Administrator account.

A example request is as follows:

```
    http://campus.digication.com/api/?method=user.login&otherid=H482372837&key=4892348923
```

The 'method' parameter indicates which API function to call. The 'key' parameter is the Digication API Key described above. The 'otherid' parameter refers to the shared unique identifier used when creating your user accounts. It is also referred to as the SyncID.

The results from an API request will be returned in the same format they were sent in. In the example above, the parameters are sent via a URL encoded string, so the results will be returned the same way.

The response will be a url encoded set of key/value pairs representing the data returned from the method called. A result will always have an index called 'success' which is a boolean value that will be true if the request was successful and false if it failed. A successful login, using URL encoding, would return a response:

```
result%5Bloginkey%5D=aceff76fe536ea8023afdf1842d55a941937e7ac8&success=1
```

If decoded, this would look like:

```
    result[loginkey] = aceff76fe536ea8023afdf1842d55a941937e7ac8
    success = 1
```

A failed request will return success=0 as well as a short error string and a human-readable error message, such as

```
errorcode=usernotfound&error=No+user+with+that+id&success=0
```

Using a Login Token

The login key returned by the user.login method can be used by a user once to access their account. They should be directed to http://[domain].digication.com/login_redirect.digi?loginkey=[loginkey], where [domain] is the web address used by your school or institution and [loginkey] is the key returned above.

API Methods for SSO

Single Sign-On typically requires only two methods: user.login and user.create. The school or institution must decide whether users will be pre-created via an import or created at first sign-in attempt.

user.login

Parameters: otherid [string] (required) – the unique identifier (also called SyncID) entered when the user was created

Responses: loginkey [string] – a temporary token that enables the user to login to their account

user.create

Parameters:

firstname [string] (required)
lastname [string] (required)
username [string] (required)
otherid [string] (required) – the unique identifier (also called SyncID)
password [string] (optional)
email [string] (required)
facultyf [boolean] (optional, default=0)
timezonekey [string] (optional)
alumnif [boolean] (optional, default=0)
deactivatef [boolean] (optional, default=0)

Responses: userid (integer) – the Digication internal ID used to reference the user