Authentication Methods

Overview

In addition to the OU Campus-managed authentication system, OU Campus supports LDAP, CAS, and Shibboleth authentication methods.

LDAP users can be configured through the standard process to create an administrator or user in OU Campus. The administrator can create matching users in OU Campus for every LDAP user. There are three supported LDAP security options and two types of supported distinguished names (DNs). When logging in, users will still log in through the normal OU Campus login interface.

The Central Authentication Service (CAS) is a single sign-on protocol for the web. Its purpose is to permit a user to access multiple applications while providing their credentials (such as user identification and password) only once. It also allows web applications to authenticate users without gaining access to a user's security credentials, such as a password. When logging in, users are redirected to the CAS authentication page from where they can enter their credentials.

Standard Shibboleth Native Service Provider (SP) software integrates with OU Campus. User accounts are created and managed in OU Campus to establish workflow and permission levels; Shibboleth is used to authenticate only. When logging in, users are redirected to the Identity Provider (IdP) page to authenticate. OU Campus verifies that the user identification attribute defined returned by the IdP matches the username of an OU Campus user.

LDAP

When a user logs in to OU Campus, they visit a login page housed on the application server that holds their account. The server may be located in the OmniUpdate server farm (for OU SaaS hosting solutions) or in the server located at the institution (for self-hosted customers). The user enters their login credentials, which are then passed back to the OmniUpdate server using SSL encryption.

OU Campus first looks up the username in its local database. If a matching user is not found, access is denied. If the user is found, the system attempts to authenticate the user. If LDAP information is specified for the account, the OU Campus server attempts to bind to the sever specified with the given DN, and the password submitted by the user at log in time. The OU Campus user is granted access only if the bind is successful.

Creating LDAP Users in OU Campus

To create an LDAP user in OU Campus, follow the same process for creating any user or administrator.

1. From the OU Campus interface, when logged in as a Level 10 administrator, navigate to **Setup > Users**.
2. Click the **New** button.
3. Complete the new user form, leaving the **Password** field in the User Information panel blank.
4. Fill in the LDAP Configuration fields, which are as follows:
   - **Authentication Type**: LDAP security level or authorization type
   - **Hostname**: LDAP server hostname or IP
• **DN**: The user’s unique distinguished name (DN)

There are three supported security options for Authentication Type when using LDAP with OU Campus. Each supported option uses the simple method of binding. The options for Authentication Type are:

- **Simple**: When using the Simple method, the LDAP session is conducted in plain text, without encryption.
- **Simple (SSL)**: When using SSL encryption, OmniUpdate needs to install a copy of the customer’s X.509 public certificate on the OmniUpdate server. The SSL method is commonly used in many LDAP installs, including installs utilizing Microsoft’s Active Directory.
- **Simple (StartTLS)**: The StartTLS security method is also supported by OmniUpdate.

There are generally two types of DNs that can be used with OU Campus. The first is the standard LDAP DN, comprising of relative distinguished names (RDN), which looks similar to this:

```
CN=FirstName LastName,OU=Staff,DC=domain,DC=edu
```

The second type of DN looks like an email address. Usually this format is seen in a Microsoft Active Directory environment. A DN for Active Directory might look similar to this: `user@domain.edu`.

**CAS**

The Central Authentication Service (CAS) protocol involves at least three parties: a client web browser, the web application requesting authentication, and the CAS server. It may also involve a back-end service, such as a database server, that does not have its own HTTP interface but communicates with a web application.

When the client visits an application desiring to authenticate to it, the application redirects it to the CAS server. CAS validates the client’s authenticity, usually by checking a username and password against a database (such as SQL or Active Directory).

If the authentication succeeds, CAS returns the client to the application by passing along a security ticket. The application then validates the ticket by contacting CAS over a secure connection and providing its own service identifier and the ticket. CAS then gives the application trusted information about whether a particular user has successfully authenticated.

**Configuring OU Campus for CAS**

When a user logs in to OU Campus directly, they visit a login page housed on the application server that holds their account. The server may be located in the OmniUpdate server farm (for OU SaaS hosting solutions) or in the server located at the institution (for self-hosted customers). The user enters their login credentials, which are then passed back to the OmniUpdate server using SSL encryption.

If an institution desires to use CAS authentication in place of the built-in authentication method, the institution must provide their CAS server’s SSL certificate, as well as their CAS login and logout page URLs. The CAS server’s SSL certificate must be installed on the OmniUpdate server before OU Campus will be able to authenticate via CAS.
When CAS is configured, users will then be redirected to the CAS login and logout pages when logging in and logging out, respectively, as opposed to the standard OU Campus login page. CAS then authenticates, compares the username with the usernames configured in OU Campus and, if everything validates, the user is granted access to OU Campus.

If OU Campus is configured with a CAS URL, any password and LDAP information that has been configured for OU Campus users is ignored. OU Campus usernames must match usernames on the CAS server in order to be authenticated and logged in via CAS. All user levels, including level 10 admins, are authenticated through CAS. However, users in the SuperAdmin interface are separate entities; they do not use CAS server to authenticate and must either use the standard authentication method or LDAP.

Creating CAS Users in OU Campus

OmniUpdate’s CAS authentication module is very easy to use. A level 10 administrator creates a matching user in OU Campus for every CAS user that will log in to the system.

Since users are administrated at the Account level in OU Campus, CAS is also enabled at the Account level. When CAS is enabled, all users within an OU Campus account — no matter what site within it they are attempting to access — will be redirected to the CAS login page.

To create a CAS user in OU Campus, follow the same process as for creating any other user, with the exception of leaving the password and LDAP fields blank.

1. First, as a level 10 administrator, ensure that CAS is configured correctly by navigating to Setup > Account.
2. In the Login Page panel, configure the CAS or Shibboleth URL and Logout URL fields.
3. Once CAS has been configured, navigate to Setup > Users to create new users who will authenticate over CAS.
4. Click the New button.
5. Complete the new user form, leaving the Password field in the User Information field blank. The OU Campus username must match the user's CAS ID.

Shibboleth

Shibboleth operates in a similar manner to CAS, in that users will be redirected to an external server to authenticate before accessing OU Campus.

Since users are administrated at the Account level in OU Campus, Shibboleth is also enabled at the Account level. When Shibboleth is enabled, all users within an OU Campus account — no matter what site within it they are attempting to access — will be redirected to the IdP. Each account can have a separate IdP specified.

Requirements for Shibboleth Authentication Integration

The requirements for Shibboleth authentication integration are:

- Be a member of the InCommon Federation (http://incommon.org). OmniUpdate is a member and InCommon acts as a broker between the OmniUpdate service provider (SP) and the identity provider.
- Release user ID attribute to the OmniUpdate service provider.
OU Campus integrates with standard Shibboleth service provider software, which is not specific to OmniUpdate and uses the mod_shib extension for Apache (or its IIS equivalent). The service provider metadata will be included in that installation.

**Configure the Service Provider and OU Campus**

Once installed, the following steps must be taken to configure the Shibboleth service provider software:

Included in the OU Campus WAR is a JSP for Shibboleth support, located under `/secure`. The file can be adjusted for specific configuration parameters.

Assuming that the Shibboleth service provider is set up and working properly, the next steps must be taken to set up OU Campus:

1. Place the JSP into the `/secure` directory of the installation.
2. Open two different web browsers (e.g., Firefox and Chrome). To easily test Shibboleth integration, have one session to the system that stays open, and another that does not and therefore must authenticate.
3. Update the OU Campus account to use Shibboleth authentication. As a level 10 user (or from the SuperAdmin interface), navigate to Setup > Account (or click on the desired account in SuperAdmin).
4. In the Login Page panel, configure the CAS or Shibboleth URL field. Point to the file `shib:/secure/shibboleth.jsp` (file name for the JSP file may vary).
5. Configure the Logout URL field as well.
6. Save the changes.

This setting takes effect immediately and takes over authentication for that OU Campus account and all sites inside the account. It is not possible to have one user authenticate using Shibboleth and another authenticating using CAS, LDAP, or the standard authentication.

Multiple accounts may all use the same JSP file, if linking to the same IdP, or each have their own JSP file for different IdPs.

**Testing Authentication**

To test Shibboleth authentication, attempt a log in to edit a page from that account in a separate browser. For example (substituting the appropriate values for the domain, skin, and account):

```
http://oucampus.school.edu/skin/login.jsp?user=account
```

This redirects to the Where are You From (WAYF) service, at which point one can choose the IdP, authenticate there, and be redirected back to OU Campus. If a link is made between the provided user name and an OU Campus user name, then access is granted.

**Creating Shibboleth Users in OU Campus**

To create a Shibboleth user in OU Campus, follow the same process as for creating any other user, with the exception of leaving the password and LDAP fields blank.

1. As a level 10 administrator in OU Campus, navigate to Setup > Users.
2. Click the New button.
3. Complete the new user form, leaving the **Password** field in the User Information panel blank. The OU Campus username must match the user's Shibboleth ID.