**Authentication**

Ex Libris campusM Configuration Form

**Overview**

**campusM Authentication (CMAuth)** is a standardized token-based authentication mechanism and framework that seamlessly supports the handshake, validation, and mapping attributes for authenticated users using standard **SAML 2.0** and **OAuth 2.0** based systems.

|  |  |
| --- | --- |
| **Complexity Level** | High |
| **Customer Owner** | IT (typically) |
| **Required for activation** | Yes |
| **More information** | **System (Supplier and Product)** - [Managing Token Based Authentication](https://knowledge.exlibrisgroup.com/campusM/Product_Documentation/Managing_Token_Based_Authentication)  **Product Version** - [Authentication Integration Profiles](https://knowledge.exlibrisgroup.com/campusM/Product_Documentation/Managing_Token_Based_Authentication/Configuring_Integration_Profiles) |

**Authentication Type**

Select the relevant section below according to your chosen **Authentication Type.**

# SAML

## required information

Download the campusM SAML metadata file from the following URL: <org\_web\_hostname>/cmauth/saml/metadata?cert=SAML\_081222

\*\* Do this for each campusM environment that you work with: Production, Sandbox, and Preview.

Add each of the metadata files to the IdP’s configuration.

|  |  |
| --- | --- |
| **Branding Option** | **Value** |
| System (Supplier and Product) |  |
| Product Version |  |
| Entity ID |  |
| Single Sign On URL |  |
| IDP Logout URL (optional) |  |
| Certificate |  |
| Username Mapping |  |
| Mail Mapping |  |
| First Name Mapping |  |
| Last Name Mapping |  |
| Additional Mapping 1 (optional) |  |
| Additional Mapping 2 (optional) |  |
| Token Lifetime |  |
| Test User 1 - Username |  |
| Test User 1 - Password |  |
| Test User 2 - Username |  |
| Test User 2 - Password |  |
| Comments |  |

## Notes

**Entity ID** - This is an attribute on the root EntityDescriptor element in the IdP’s metadata.

**Single Sign On URL** - Towards the end of the IDPSSODescriptor element (normally there is only one element – if not, select the first element), there are one or more SingleSignOnService elements. Select the element that has its Binding element set to: urn:oasis:names:tc: SAML :2.0:bindings:HTTPRedirect and fill the Location attribute here.

**IDP Logout URL (optional)** - This is a general logout URL which allows the IdP to terminate the user’s session. For Shibboleth, the syntax is usually: https://<hostname>/idp/profile/Logout

**Certificate** - Within the IDPSSODescriptor element in the metadata are, one or more KeyDescriptor elements. Those may have an optional use attribute. If so, select the one with that attribute set to signing, and copy the content inside the X509Certificate element.

**Username Mapping** - The name of the attribute in the SAML response that is used as the campusM app username.

**Mail Mapping** - The name of the attribute in the SAML response that contains the user’s email.

**First Name Mapping** - The name of the attribute in the SAML response that contains the user’s first name.

**Last Name Mapping** - The name of the attribute in the SAML response that contains the user’s last name.

**Additional Mappings (optional)** - This field takes multiple comma delimited names and value pairs that will be added in a designated part of the token, where additional information can be kept and then used in the different parts of the application. A single value can be supplied if the same attribute name in the response should be used (so instead of department=department, typing just department is sufficient) Example: job=title,tel=mobile,office,department.

**Token Lifetime** - This sets the expiration date for the generated token used by campusM. If left empty, it defaults to 30 days for both Web and Native mobile. Examples: 30d, 120m, 72h.

Note: it is recommended to have the token lifetime (expiration) set the 30d level to avoid the need for the user to frequently need to re-login/authenticate to campusM.

**Test Users** - At least one test IdP user credential is mandatory. To test other functionality and integrations, it is recommended to provide more than one test user with different representative types of data and/or a single user with all representative types of data.

# OAuth

## required information

Register the app as a client on the customer’s side from which a client ID and optionally a client secret (recommended) is produced.

Use the following redirect URI: <org\_web\_hostname>/cmauth/oauth/callback

\*\*Do this for each campusM environment that you work with: Production, Sandbox, and Preview.

Add each of the metadata files to the IdP’s configuration.

|  |  |
| --- | --- |
| **Branding Option** | **Value** |
| System (Supplier and Product) |  |
| OAuth Client ID |  |
| OAuth Client Secret |  |
| Authorization Endpoint |  |
| Access Token Endpoint |  |
| Token Endpoint Auth |  |
| User Info Endpoint |  |
| OAuth Scope |  |
| Logout URL |  |
| Token Verification Certificate |  |
| Username Mapping |  |
| Mail Mapping |  |
| First Name Mapping |  |
| Last Name Mapping |  |
| Additional Mapping 1 (optional) |  |
| Additional Mapping 2 (optional) |  |
| Token Lifetime |  |
| Test User 1 - Username |  |
| Test User 1 - Password |  |
| Test User 2 - Username |  |
| Test User 2 - Password |  |
| Comments |  |

## Notes

**Username Mapping** - The name of the attribute in the OAuth response that is used as the campusM app username.

**Mail Mapping** - The name of the attribute in the OAuth response that contains the user’s email.

**First Name Mapping** - The name of the attribute in the OAuth response that contains the user’s first name.

**Last Name Mapping** - The name of the attribute in the OAuth response that contains the user’s last name.

**Additional Mappings (optional)** - This field takes multiple comma delimited names and value pairs that will be added in a designated part of the token, where additional information can be kept and then used in the different parts of the application. A single value can be supplied if the same attribute name in the response should be used (so instead of department=department, typing just department is sufficient enough) Example: job=title,tel=mobile,office,department.

**Token Lifetime** - This sets the expiration date for the generated token used by campusM. If left empty, it defaults to 30 days for both Web and Native mobile. Examples: 30d, 120m, 72h.

Note: We recommend setting the token lifetime (expiration) to the 30d level to avoid the user needing to frequently re-login/authenticate to campusM.

**Test Users** - At least one test IdP user credential is mandatory. To test other functionality and integrations, we recommended providing more than one test user with different representative types of data and/or a single user with all representative types of data.