

East Tennessee State University

## Digital Commons @ East Tennessee State University

---

ETSU Faculty Works

Faculty Works

---

5-1-2018

### Authentication via OpenAthens: Implementing a Single Sign-on Solution for Primo, Alma, and EZproxy

Travis Clamon

East Tennessee State University, [clamon@etsu.edu](mailto:clamon@etsu.edu)

Follow this and additional works at: <https://dc.etsu.edu/etsu-works>



Part of the [Computer Engineering Commons](#)

---

#### Citation Information

Clamon, Travis. 2018. Authentication via OpenAthens: Implementing a Single Sign-on Solution for Primo, Alma, and EZproxy. *ELUNA 2018 Annual Meeting*, Spokane, Washington. <http://documents.el-una.org/1641/>

This Presentation is brought to you for free and open access by the Faculty Works at Digital Commons @ East Tennessee State University. It has been accepted for inclusion in ETSU Faculty Works by an authorized administrator of Digital Commons @ East Tennessee State University. For more information, please contact [digilib@etsu.edu](mailto:digilib@etsu.edu).

---

## Authentication via OpenAthens: Implementing a Single Sign-on Solution for Primo, Alma, and EZproxy



# Authentication via OpenAthens

Implementing a Single Sign-on Solution for Primo, Alma, and EZproxy

Travis Clamon

Christian Trombetta

*ELUNA May 2nd, 2018*

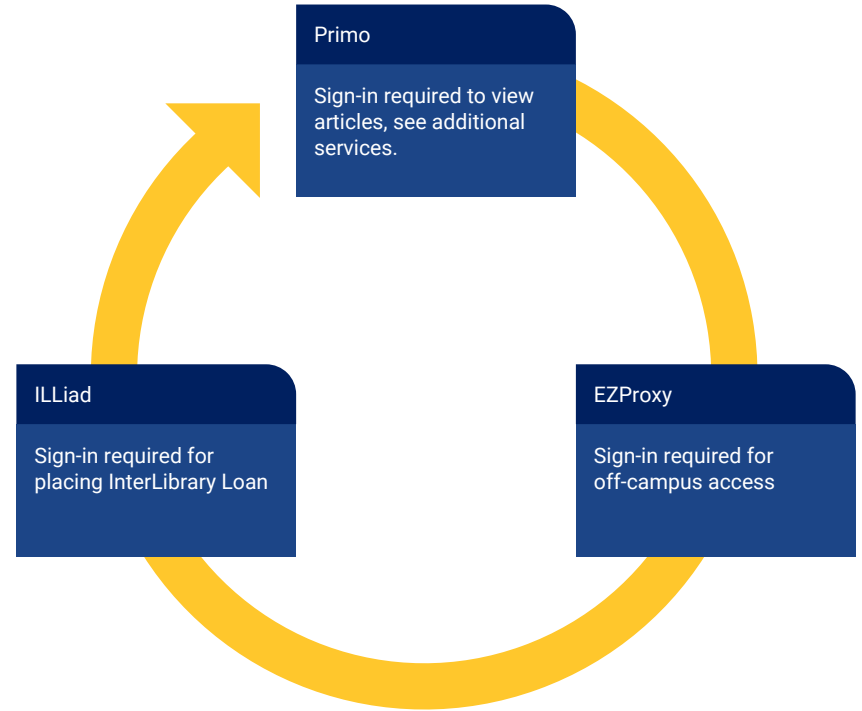


East Tennessee State University  
University Libraries



# The problem

Students and Faculty overwhelmingly expressed their desire for a SSO experience when navigating library resources.





## Needed solution

- Single Sign-On (SSO) SAML 2 compliant
- Hosted solution
- Compatible with LDAPS
- Compatible with Ex Libris (Alma/Primo), EzProxy, ILLiad, and Springshare Platforms
- SSO deployment needed to coincide with the launch of the Library's new website
- Federated Resource Access
- Potential EzProxy alternative

# Options for SSO



## CAS via IT

- Existing Auth System
- No Control of Config and Data Structure
- Missed Timeline
- Support



Commons Photo Credit: Source

## CAS Hosted

- Cost
- Lacks Proxy Functionality



## OpenAthens

- Cost
- Reputation
- Industry Leader
- Federated resource access



## Inaction

- Problem remains
- User experience
- Bad PR

# Choice: OpenAthens

The screenshot shows the homepage of the Charles C. Sherrod Library at East Tennessee State University. The browser address bar displays 'https://libraries.etsu.edu/home'. The page features a search bar with the placeholder text 'Find books, articles, media and more!' and a 'Search' button. Below the search bar, there are navigation links for 'Research', 'Use the Library', 'About', 'My Accounts', and 'Ask'. The main content area is divided into four columns: 'Top Databases', 'Quick Links', 'Computers', and 'Study Spaces'. The 'Top Databases' section lists CINAHL, ERIC, JSTOR, PsychInfo, and Pubmed. The 'Quick Links' section includes 'Access off-campus', 'Borrow, Renew, Request', 'Research Help Appointments', 'Library Floor Maps', 'People and Offices', 'Testing Services', and 'Tutoring Services'. The 'Computers' section shows 'Available Now' with 'Lab Desktops' at 60 and 'Laptops' at 39. The 'Study Spaces' section lists '24-Hour Study', 'Group Study', and 'Individual Study'. At the bottom, there is a 'News, Events & Exhibits' section and a 'Graduate Students' section with links for 'Citation Management' and 'Instruction and Workshops'.

East Tennessee State University

CHARLES C. SHERROD LIBRARY  
EAST TENNESSEE STATE UNIVERSITY

Research - Use the Library - About - My Accounts - Ask

Find books, articles, media and more! Search Advanced Search

What am I searching?

Hours: Friday Mar 30, 2018: Open 24 hours OPEN

**Top Databases**

- CINAHL
- ERIC
- JSTOR
- PsychInfo
- Pubmed

[View All Databases](#)

**Quick Links**

- Access off-campus
- Borrow, Renew, Request
- Research Help Appointments
- Library Floor Maps
- People and Offices
- Testing Services
- Tutoring Services

**Computers**

Available Now

Lab Desktops:	60
Laptops:	39

**Study Spaces**

- 24-Hour Study
- Group Study
- Individual Study

**News, Events & Exhibits**

**Graduate Students**

- Citation Management
- Instruction and Workshops



# Implementation

**April 2017**

Acquired OpenAthens through EBSCO

**June 2017**

Alma & Primo Sandbox configuration/testing

Jan Feb Mar Apr May Jun Jul Aug Sept Oct Nov Dec

**May 2017**

Started the process of configuring resources for federated access

**Aug 2017**

Primo NUI, Alma, and EZproxy fully integrated





# How OpenAthens works

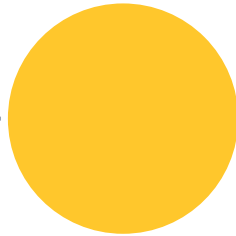
## Authentication

Validate user credentials and establish the identity of the user



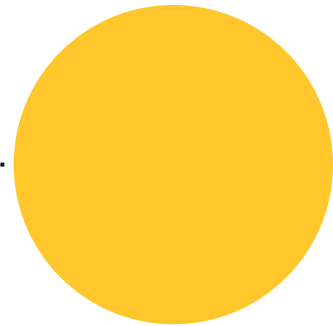
## Permission Allocation

Assign permission sets (groupings) to users based upon user attributes or rules



## Resource Authorization

Authorize user access to resources by allocating permission on a resource by resource basis



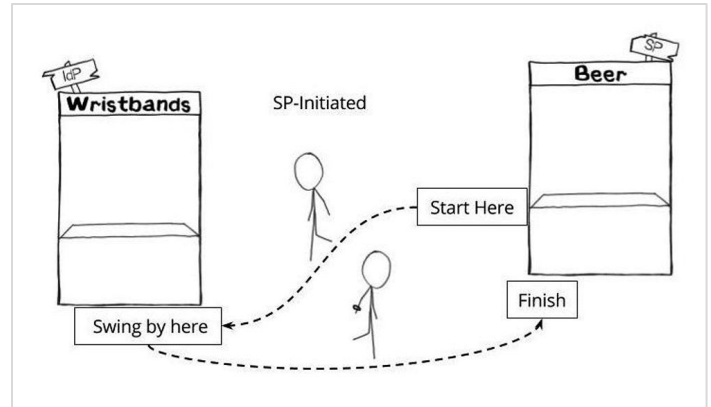
# OA Single Sign-On

Getting Started - Basic Building Blocks

Accounts  
Resources  
Permissions  
Authentication Point



SAML based Single Sign-On (SSO) in Action



Source: The Beer Drinker's Guide to SAML by Greg Seador.  
(<https://duo.com/blog/the-beer-drinkers-guide-to-saml>)



# OA Accounts

## Internal OA accounts

## Local Authentication

**Brokered:** Authentication is entered at the OpenAthens authentication point (AP), and credentials are checked against the institution's authentications system. (LDAP, SirsiDynix)







**Delegated:** Users are directly passed to the institution's authentication point and redirected back to OpenAthens following authentication. (SAML, CAS, API, ADFS)



**Internal:** User credentials stored in OpenAthens

## Local authentication connector accounts

Select local authentication system type. ✕

 <b>LDAP</b> Connect to an LDAP directory, including Microsoft ActiveDirectory.	 <b>ADFS</b> Connect using Microsoft ActiveDirectory Federation Services.
 <b>API</b> Connect via the OpenAthens Local Authentication REST API.	 <b>SirsiDynix</b> Connect to a SirsiDynix library system for authentication.
 <b>CAS</b> Connect to a Client Access Server (version 5.x) using SAML.	 <b>SAML 1.1/2.0</b> Connect to a local identity provider using SAML.

Cancel Configure



# OA Resources

## Resource Types

- Federated
- OpenAthens (legacy)
- Proxied
- **SAML (Custom)** - Alma, Primo, EZproxy

### OA Enabled Resource Listings:

<https://www.openathens.net/resources.php>

### OA Documentation:

<https://docs.openathens.net/display/public/MD/Add+and+manage+custom+SAML+resources>

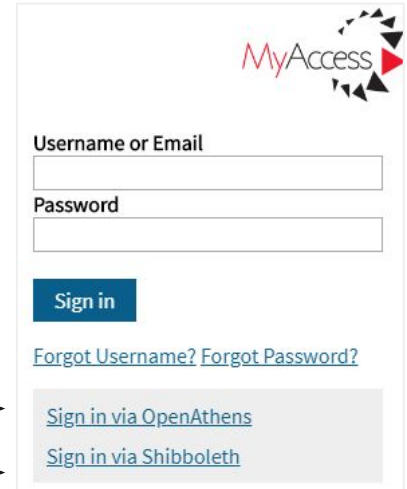
A service provider's content may be accessible via multiple Openathens enabled resource types.

### Example:

AccessMedicine allows for Federated authentication in addition to the legacy OpenAthens.

OpenAthens Login →

Federated Login →



MyAccess

Username or Email

Password

Sign in

[Forgot Username?](#) [Forgot Password?](#)

[Sign in via OpenAthens](#)

[Sign in via Shibboleth](#)

# OA Permissions

## Permission Set Allocation

- Attributes
- Rules

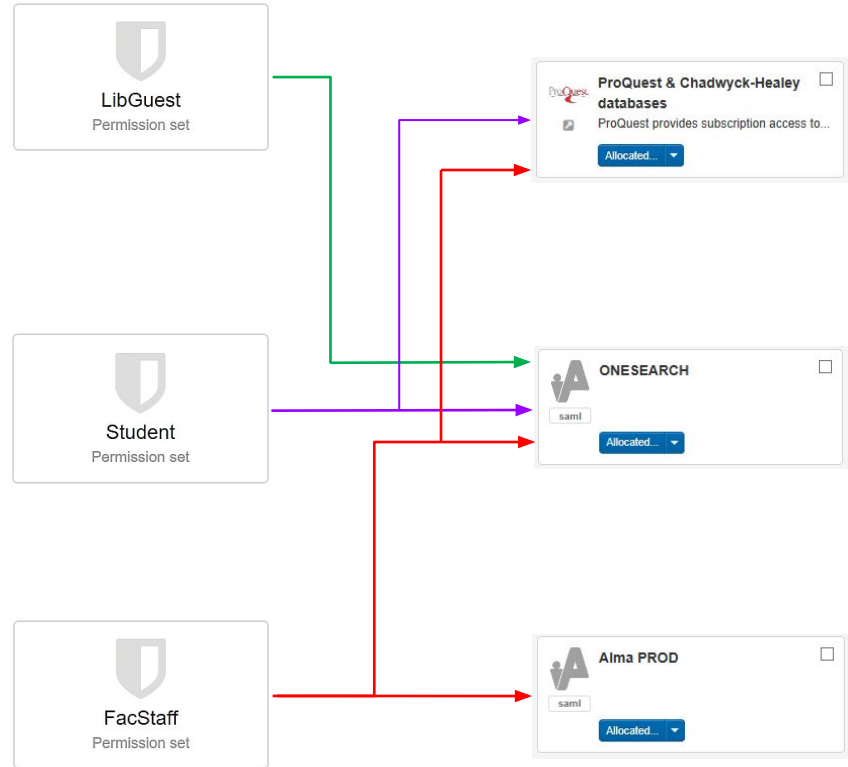
Rule-based allocation example:

Rule name\*

When  of these conditions are met:

Apply permission sets

## Permission Sets



# OA Authentication

## Authentication Point (AP) :

User login portal for accessing OA-enabled resources.

**Session Length:** 8 hours or exiting browser

### Note:

If OA is used for Primo authentication, setting a Primo session length shorter than the OA-defined length (8 hours) will cause other OA-enabled resource sessions to end prematurely.

Default OpenAthens Login Portal

The screenshot shows the default OpenAthens login portal. It features the OpenAthens logo at the top left. The main content is divided into two columns. The left column is titled "Sign in with an OpenAthens account." and contains a "Username" section with a text input field labeled "Email address or username" and a "Password" section with a text input field labeled "Password". Below these fields is a purple "Sign in" button and a link "Problems signing in?". The right column is titled "Find your organisation." and contains a search input field labeled "Search" with the placeholder text "Type the name of your organisation" and a magnifying glass icon.

Default OpenAthens Login Portal with Organization Identified

The screenshot shows the default OpenAthens login portal with the organization identified. The OpenAthens logo is at the top left, and the "UNIVERSITY LIBRARIES EAST TENNESSEE STATE UNIVERSITY" logo is at the top right. The main content is divided into two columns. The left column is titled "Sign in via your organisation." and contains a "Username" section with a text input field labeled "ETSU Username (Do not include @etsu.edu)" and a "Password" section with a text input field labeled "Password". Below these fields is a purple "Sign in" button and a link "Problems signing in?". The right column is titled "Find your organisation." and contains a search input field labeled "Search" with the placeholder text "Type the name of your organisation" and a magnifying glass icon.

Pre-branded OpenAthens Login Portal with search section omitted

The screenshot shows a pre-branded OpenAthens login portal for McGraw-Hill Medical. The McGraw-Hill Medical logo is at the top left. The main content is titled "Sign In via Shibboleth". Below the title are two dropdown menus: "Location:" with "OpenAthens Federation" selected and "Institution:" with "East Tennessee State..." selected. Below these is a black "Select" button.

The screenshot shows the pre-branded OpenAthens login portal with the search section omitted. The "UNIVERSITY LIBRARIES EAST TENNESSEE STATE UNIVERSITY" logo is at the top left. The main content is titled "Sign in to continue." and contains a "Username" section with a text input field labeled "ETSU Username (Do not include @etsu.edu)" and a "Password" section with a text input field labeled "Password". Below these fields is a blue "Sign in" button and a link "Problems signing in?". A red arrow points from the McGraw-Hill Medical portal to this one.



# Year 1

## Our Experience:

### OA Administration Experience

- Learning curve of how to setup resources
- Time consuming setup process with vendors
- Limited customization of login page
- Lack of OA Listserv in North America
- Limited search capabilities for local authentication connections (LDAP).
- New analytics/reporting interface
- Must use reseller support portal - mixed emotions

### OA End User Experience

- Signing in : username vs email
- Medical Students / VA users already accustomed to OpenAthens
- Confusion about multiple login options on vendor sites (Shibboleth vs OpenAthens)
- 10k+ unique logins out of 15k users.
- Minimal help tickets



# Year 1 Lack of Redundancy:

## OpenAthens Outages

- Scheduled outages are posted on the OA status page (<http://status.openathens.net/>)
- Multiple unscheduled outages occurred during our first year. (March 2018 - most recent)
- Outage time length have ranged from minutes to hours.
- Failed to meet our expectations as a world-wide provider of authentication services in its inability to provide redundancy on a hosted platform

## OpenAthens Conference Call - April 2018

- Outages were “migration pains”
- OA is migrating to US in the Google Cloud
- 90% complete as of April
- Redundancy is part of the goal
- Reseller relations and support requirements will continue





# Year 1

## Lessons Learned:

### In event of downtime:

- Reverting EZProxy back to LDAP authentication
- Keep both OA and existing authentication in user.txt (comment out when needed)

### In event of extended downtime:

- Primo - support for multiple authentication methods
- Alma - shortcut link / adjust URL

### Other Lessons Learned

- Keep session length in sync with Primo & OpenAthens (8 Hours)
- OA does not allow you to specify session length
- OAProxy - we decided to keep our own EZProxy Installation

# Setup Examples



OCLC™

  
ExLibris®  
a ProQuest Company



# Adding Federated Resources

## Steps:

Add Resource from OpenAthens Resource Catalogue

Allocate permission sets (Students/Staff/etc)

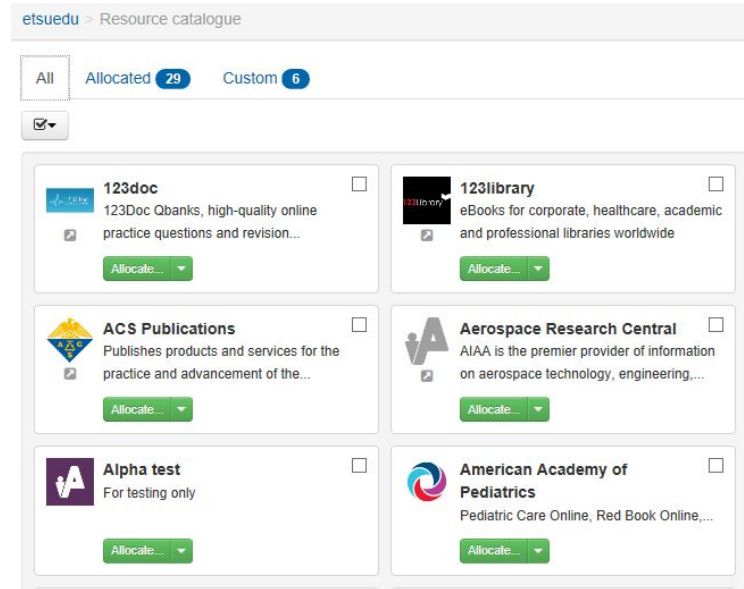
OpenAthens Attribute Release (Global Policy - OK)

Contact Vendor - What do they need?

**Organization ID:** (8 digit number)

**Scope:** etsu.edu (domain-wide)

**Entity ID:** <https://idp.etsu.edu/openathens>



The screenshot shows the 'etsuedu > Resource catalogue' page. It features a navigation bar with 'All', 'Allocated 29', and 'Custom 6' tabs. Below the navigation is a list of six resource cards, each with a logo, title, description, and an 'Allocate...' button. The resources listed are:

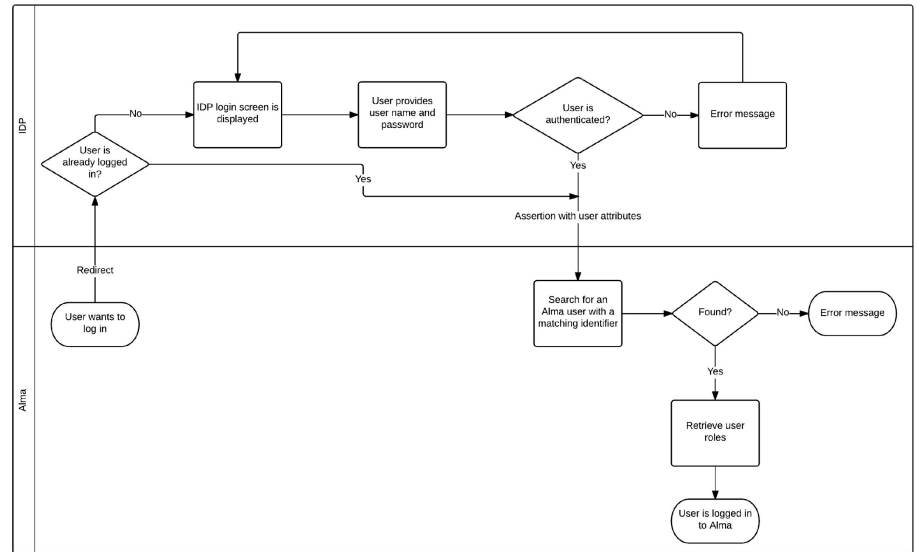
- 123doc**: 123Doc Qbanks, high-quality online practice questions and revision...
- 123library**: eBooks for corporate, healthcare, academic and professional libraries worldwide
- ACS Publications**: Publishes products and services for the practice and advancement of the...
- Aerospace Research Central**: AIAA is the premier provider of information on aerospace technology, engineering,...
- Alpha test**: For testing only
- American Academy of Pediatrics**: Pediatric Care Online, Red Book Online,...

**OA Enabled Resource Listings:**

<https://www.openathens.net/resources.php>

# Alma Authentication using OpenAthens

When the user attempts to log in to Alma, Alma redirects to OpenAthens (IDP) and sends an authentication request. OA performs a single-sign-on check, and if the user is not logged in, then an OpenAthens branded login page is displayed. After the user logs in, OA redirects back to Alma with a SAML response and assertion. Alma retrieves the user profile based on the attribute released in the SAML response and logs the user in.



Source: Ex Libris Developer Network. Authentication of Primo Users to Retrieve Alma Information. ([https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst\\_idp/saml](https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst_idp/saml))



# Alma Authentication using OpenAthens

## Steps:

- Alma - SAML Integration Profile
- OpenAthens Resource Configuration
- OpenAthens Attribute Release Configuration

# Alma – SAML Integration Profile (Step 1)

Required OpenAthens information:

Metadata file URL

(<https://login.openathens.net/saml/2/metadata-idp/DOMAIN>)

User ID attribute name

(cn)

IDP logout URL

(<https://login.openathens.net/signout?>)

The screenshot shows the 'Integration Profile' configuration page in Alma. The title is 'SAML OpenAthens'. At the top right are 'Cancel' and 'Save' buttons. Below the title is a table with the following data:

Code	SAML OA
Integration Type	SAML

Below the table are three tabs: 'General Information', 'Actions', and 'Contact Info'. The 'General Information' tab is active and contains the following fields:

- Code \* (SAML OA)
- Name \* (SAML OpenAthens)
- System \* (Other)
- System Description (empty)
- Description (OpenAthens SAML SSO)



## Alma – SAML Integration Profile cont.

Metadata upload method: Metadata link

Enter Metadata file URL & Alma will auto populate the following:

- IDP Issuer, IDP login URL ,User Id location, Certificate Upload Method

Enter User Id attribute name (Alma – OpenAthens match point)

Enter IDP logout URL

Save & Generate Metadata File

# Alma – Integration Profile cont.

Upon opening the saved integration profile, the certificate text box will be empty and the following message displayed “Certificate file already exists”.

Generate Metadata File (save local - will be uploaded into the OA SAML resource in created in step 2.)

## SAML DEFINITIONS

Metadata upload method  Metadata link  Metadata upload

Metadata file link

Default SAML profile

IdP issuer \*

IdP login URL \*

User ID location \*

User ID attribute name \*

IdP logout URL

IdP single logout service

Sign single logout requests

Alma metadata file version \*

Certificate upload method  Free-text certificate  JKS file  Certificate file

Enter certificate text





# Alma – OA Resource Configuration (Step 2)

## Add SAML Resource

Upload Metadata file downloaded from the Alma Integration Profile

Add a SAML resource. ✕



Upload SAML 2 metadata via a URL or file.

Metadata URL

Upload file

Cancel

Create resource

# Alma – OA Resource Configuration cont.

## Edit Resource

Add Access URL – Alma login URL for authentication using OpenAthens as the authentication point.

### Access URL Example:

`https://sandbox01-na.alma.exlibrisgroup.com/mng/login?institute=01ABCD_INST&auth=SAML`



Allocated...

Type SAML

Entity ID `https://sandbox01-na.alma.exlibrisgroup.com/mng/login`

Resource details | Visibility | Certificates | SAML

Title\*

Description

Information URL

Access URL  Test ?

Categories   
Categories should be separated with spaces.

Hidden from users



# Alma – OA Resource Configuration cont.

Test logins yield the following error until the appropriate attributes are released and the permission sets are allocated



## Forbidden

You are not entitled to access this resource  
For assistance please [contact your organisation administrator](#).

---

# Alma – OA Resource Configuration cont.

Allocate appropriate user access

Permission set allocation for 'AlmaSB'.

None  Default  All

- Default permission set
- FacStaff
- LibGuest



Allocated...

- Select permission sets...
- Cascade...
- Revoke...

Resource details

Visibility

Certificates

SAML

Title\* AlmaSB

Description

Information URL

Access URL

https://sandbox01-na.alma.exlibrisgr

# Alma – OA Attribute Release (Step 3)

Configure OA to release the **User Id Attribute** specified in the Alma-SAML integration profile. Upon successful authentication, OA will release the attribute to Alma for matching against the unique identifier fields.

Released attributes:  Username  Title  First name(s)  Last name  Department  Position  Email address  Phone number  Fax number  Staff/student number

Postal address  userPrincipalName  CN  Organisation ID  Persistent user identifier  Role  Entitlement

SAML NameID format:

SAML NameID attribute:

Selecting an attribute will cause the value to be released to the service provider for this resource.

Attribute aliases:   mapped to

# Alma – OA Attribute Release cont.

Test the SAML authentication point

**&auth=local** (used for Internal and LDAP)

**&auth=SAML** (Case sensitive – Used for OpenAthens or other SAML service)

UNIVERSITY LIBRARIES  
EAST TENNESSEE STATE UNIVERSITY

Sign in to continue.

Username  
ETSU Username (Do not include @etsu.edu)

Password  
Password

Sign In

Problems signing in?

By using this site you agree to us setting cookies. Please see our [privacy and cookie information](#).  
Enter username without the @etsu.edu

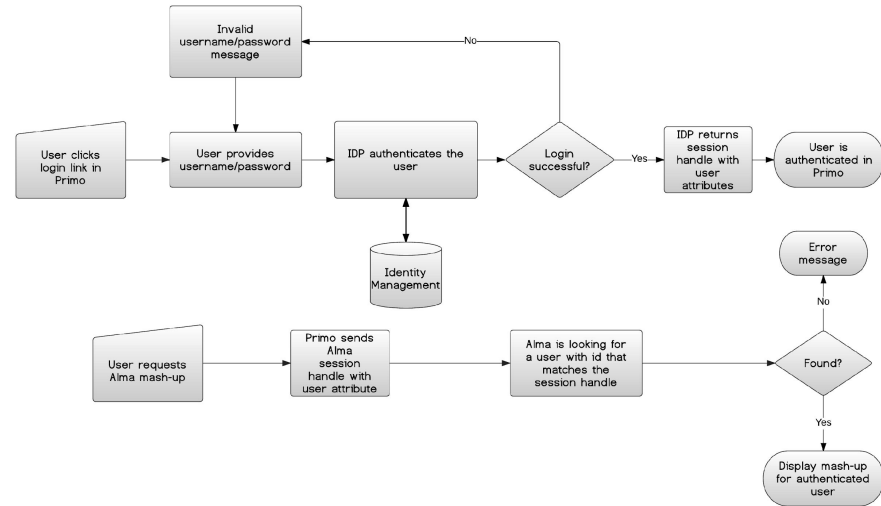
[https://sandbox01-na.alma.exlibrisgroup.com/mng/login?institute=01ETSU\\_INST&auth=local](https://sandbox01-na.alma.exlibrisgroup.com/mng/login?institute=01ETSU_INST&auth=local)

[https://sandbox01-na.alma.exlibrisgroup.com/mng/login?institute=01ETSU\\_INST&auth=SAML](https://sandbox01-na.alma.exlibrisgroup.com/mng/login?institute=01ETSU_INST&auth=SAML)

# Primo Authentication Workflow via OpenAthens

## Primo - Alma - OpenAthens (IDP)

Primo redirects logins to OpenAthens (IDP) and sends an authentication request. OA performs a single-sign-on check, and if the user is not logged in, then an OpenAthens branded login page is displayed. After the user logs in, OA redirects back to Primo with a SAML response and assertion. Primo then passes this response to Alma for user account retrieval.



Source: Ex Libris Developer Network. Authentication of Primo Users to Retrieve Alma Information. (<https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/primo>)



# Primo Authentication using OpenAthens

## Steps:

- Primo - SAML Authentication Profile
- Primo Active Metadata
- OpenAthens Resource Configuration
- Primo Metadata Activation
- OpenAthens Attribute Release Configuration



# Primo – SAML Authentication Profile (Step 1)

Required OpenAthens information:

IDP Login URL

(<https://login.openathens.net/saml/2/sso/DOMAIN>)

IDP Issuer

(<https://idp.DOMAIN/openathens>)

User ID attribute name

(cn)

IDP logout URL (<https://login.openathens.net/signout?>)

The screenshot shows a configuration form for a SAML authentication profile. The form is organized into several sections:

- Profile Name:** OpenAthensETSU
- Select Authentication Method:** SAML (dropdown menu)
- IDP Configuration:**
  - IDP\_LOGIN\_URL:**
  - IDP\_ISSUER:**
  - USER\_ID\_ATTR\_NAME:**
  - IDP\_LOGOUT\_URL:**
  - IDP\_LOGOUT\_URL\_REDIRECT\_ONLY:** True (dropdown menu)
  - SILENT\_LOGIN\_ENABLE:** True (dropdown menu)
  - EMAIL\_OVERRIDE:** False (dropdown menu)
  - AUTH\_BASE\_URL:**
  - ADFS:** False (dropdown menu)
  - Certificate File:**
- Select User Information Method:** ALMA (dropdown menu)
- USER\_INFO\_URL:**

At the bottom of the form, there are three buttons: "Cancel & Go Back" (light blue), "Attributes Mapping" (orange), and "Save" (orange).



# Primo – SAML Authentication Profile cont.

## Multi-Institution authentication and AUTH\_BASE\_URL

For Multi-Institution Primo configurations, the AUTH\_BASE\_URL must match the base URL of the Primo institution being configured in the Primo Authentication Manager.

<https://etsu-edu-primo.hosted.exlibrisgroup.com/primo-explore/search?vid=01ETSU> (CNAME record)

<https://primo-pmtna02.hosted.exlibrisgroup.com/primo-explore/search?vid=01NESCC>

**AUTH\_BASE\_URL**

`https://etsu-edu-primo.hosted.exlibrisgroup.com`

# Primo – SAML Authentication Profile cont.

## Install OpenAthens certificate into Primo

Certificate file provided by OpenAthens via the OA Metadata URL

<https://login.openathens.net/saml/2/metadata-idp/DOMAIN>

Copy the X509 certificate field value into a file, topping and tailing as follows and upload into Primo as a .cer file:

-----BEGIN CERTIFICATE-----


```
ThisIsAnExampleANBgkqhkiG9w0BAQsFADCB0DEoMCMYGCsGSIb3DQEJARYZYXR0ZW5zaGVscEIBIZHVzZXJ2Lm9yZy51azELMWkGA1UEBhMCR0lxETAPBgNVBAgMCFNvbWVyc2V0MQ0wCwYDVQQHEDARCXYRoCYGCSqGSI=
```

-----END CERTIFICATE-----

```
<ds:X509Data>
  <ds:X509Certificate>
    MIIDvjCCAqagAwIBAgIEV0xCIjANBgkqhkiG9w0BAQ
    CwYDVQQHDARCXYRoMRAwDgYDVQQKDAZFHVzZXJ2MF
    WjCB0DEoMCMYGCsGSIb3DQEJARYZYXR0ZW5zaGVscE
    EQYDVQQLDAPcGVuQXR0ZW5zHR4wHAYDVQQDBVnYX
    mokXXu+m5Gm+1f+3lyN5IA2YMn9Z8Yo37JQjIHs+xV
    WUVUqgGbMH5BGr7ZEhPrz+Vwcf9lhPW+tKpKpZEzJf
    AAEwDQYJKoZIhvcNAQELBQADggEBAFhmhuJLZueiJ6
    TnB6Z/XcdMMIiCeok4kqe5KMd5oRAyNskHYZ+8kzhs
    4gl2noVbCvYNjd6GYze/w4lgwiemkby7wu5sN1lEuc
  </ds:X509Certificate>
</ds:X509Data>
```

## Primo – Active Metadata (Step 2).

- Select a certificate from the drop down list.
- **Download** the certificate metadata. Metadata will be uploaded into the OA SAML resource created in step 3.
- **Edit** metadata AUTH\_BASE\_URL fields if needed
- **Do Not Activate** metadata until the corresponding Primo Resource has been created in OpenAthens and the Primo metadata has been uploaded.

OpenAthensETSU   SAML   ALMA    [Certificate](#) [Edit](#)

> **Certificate Management**

**Profile Name:** OpenAthensETSU

<b>Certificate*</b>	<input type="text" value="Select Certificate"/>	<input type="button" value="Save"/>
<b>Active Certificate</b>	<input type="text" value="Self-Signed (sha256) 2021-Nov-12"/>	<input type="button" value="Download Active Metadata"/>



# Primo – OA Resource Configuration (Step 3)

## Add SAML Resource

Upload the Primo Certificate  
Metadata in xml format.

Add a SAML resource. ✕



Upload SAML 2 metadata via a URL or file.

Metadata URL

Upload file

Cancel

Create resource

# Primo – OA Resource Configuration cont.

## Edit Resource

- Add Access URL – Primo institutional URL rather than a direct link to the Primo authentication point.
- Access URL provides a link to Primo via the MyAthens interface.
- Allocate Permissions



Allocated...

Type SAML

Entity ID [https://primosb-pmtna.hosted.exlibrisgroup.com/primo\\_library/libweb/01ETSU](https://primosb-pmtna.hosted.exlibrisgroup.com/primo_library/libweb/01ETSU)

Resource details | Visibility | Certificates | SAML

Title\*

Description

Information URL

Access URL

Categories   
Categories should be separated with spaces.

Hidden from users



## Primo – Metadata Activation (Step 4)

After creating the OpenAthens Primo Resource and uploading the Primo certificate metadata, users will not be able to log into Primo until the certificate has been activated and OpenAthens has been configured to release the necessary attribute(s).

OpenAthensETSU

SAML

ALMA



[Certificate](#)

[Edit](#)

**Certificate\***

Select Certificate

Save

**Active Certificate**

Self-Signed (sha256) 2021-Nov-12

Download Active Metadata

Activate New Certificate

# Primo – OA Attribute Release (step 5)

Configure OA to release the **USER\_ID\_ATTR\_NAME** specified in the Primo-SAML integration profile. Upon successful authentication, OA will release the attribute to Primo, which in turn, will send the attribute to Alma as the user match point.

Released attributes:  Username  Title  First name(s)  Last name  Department  Position  Email address  Phone number  Fax number  Staff/student number  
 Postal address  userPrincipalName  CN  Organisation ID  Persistent user identifier  Role  Entitlement

SAML NameID format:

SAML NameID attribute:   
Selecting an attribute will cause the value to be released to the service provider for this resource.

Attribute aliases:  mapped to





# EZProxy Authentication using OpenAthens

## Steps:

- Generate certificate
- Config.txt
- user.txt
- OpenAthens Resource Configuration
- OpenAthens Attribute Release Configuration
- shibuser.txt



# EZProxy - Generate cert

Generate a self-signed certificate in EZProxy for Shibboleth Communication.

This file will be uploaded into OpenAthens as a new SAML Resource (future step)

[Administration](#) | [Manage SSL \(https\) certificates](#)

## Create New SSL Certificate for Shibboleth Communication


Server name:	iris.etsu.edu (can only be changed in config.txt)
Digest:	<input type="text" value="SHA-256"/>
Key size:	<input type="text" value="2048"/>
Country:	<input type="text"/>
State or Province (optional):	<input type="text"/>
City or Locality (optional):	<input type="text"/>
Organization:	<input type="text"/>
Organization Unit (optional):	<input type="text"/>
Administrator email:	<input type="text"/>
Certificate name:	login.iris.etsu.edu
Expiration (for self-signed only)	<input type="text" value="1 year"/>
Create:	<input type="button" value="Self-Signed Certificate"/> or <input type="button" value="Certificate Signing Request"/>

You can generate self-signed certificates for no additional cost. These certificates will generate warnings in remote web browsers when used, but they are an excellent choice when you are first testing SSL features. If you find the browser warnings acceptable, you can use them for production use.

Certificate Signing Requests are used when you purchase a certificate from a certificate authority. By purchasing a certificate, you avoid warnings in remote web browsers. If you are using or plan to use proxy by hostname, you should consider purchasing a wildcard certificate. These certificates are more expensive to purchase, but suppress all warnings in remote web browsers. If you use a regular certificate with proxy by hostname, users will receive a browser warning whenever they access a proxied https web site.

If you are unclear on the advantages and disadvantages of any of these certificate options, contact [support@oclc.org](mailto:support@oclc.org) for more information.

Copyright (c) 1993-2017 OCLC (ALL RIGHTS RESERVED).



# EZProxy - config.txt

SP Entity Name

OA Metadata File

Cert List #

OA Metadata URL for ETSU

```
#-----  
config.txt - OpenAthens Configuration  
#-----  
  
ShibbolethDisable 1.3  
ShibbolethMetadata \  
  -EntityID=https://iris.etsu.edu/sp/shibboleth \  
  -File=OA-metadata.xml \  
  -Cert=5  
  
-URL=https://login.openathens.net/saml/2/metadata-idp/  
etsu.edu \  

```



# EZProxy - user.txt

ETSU Identity Provider (OA)

WAYF - Automatically directs to OA for  
login

```
#-----  
user.txt - OpenAthens Configuration  
#-----
```

```
::Shibboleth  
IDP20 https://idp.etsu.edu/openathens  
/Shibboleth
```

```
##If you want to redirect all authentication handling to  
Shibboleth, editing user.txt and add the line:  
::WAYF
```



# EZProxy - OA Setup

## Add SAML Resource

Upload EZProxy Certificate from  
Step 1

Add a SAML resource. ✕



Upload SAML 2 metadata via a URL or file.

Metadata URL

Upload file

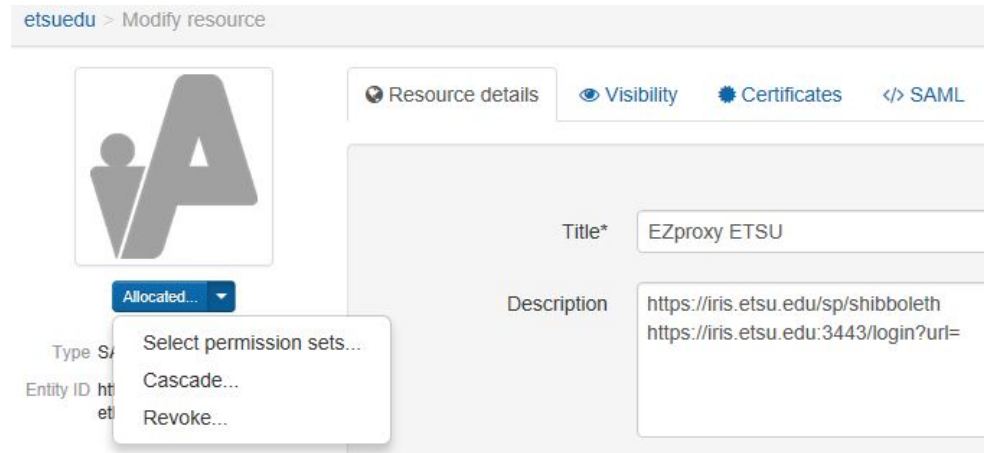
Cancel

Create resource



# EZProxy - OA Setup

Allocate appropriate user access



etsuedu > Modify resource

Resource details Visibility Certificates SAML

Title\* EZproxy ETSU

Description https://iris.etsu.edu/sp/shibboleth https://iris.etsu.edu:3443/login?url=

Allocated...  
Select permission sets...  
Cascade...  
Revoke...

Type S  
Entity ID ht  
et

# EZProxy -OA Release Attributes

## EZproxy ETSU

Released attributes:

Username  Title  First name(s)  Last name  Department  Position  Email address  Phone number  Fax number  Staff/student number

Postal address  userPrincipalName  CN  Organisation ID  Persistent user identifier  Role  Entitlement

SAML NameID format:

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

SAML NameID attribute:

CN

Selecting an attribute will cause the value to be released to the service provider for this resource.

Attribute aliases:

mapped to

Done

Cancel

Advanced...



# EZProxy - shibuser.txt

Shibuser.txt allows you to use OA attributes for EZProxy group or user configuration:

Deny affiliate@etsu.edu access to EZProxy

Add student@etsu.edu to the EZProxy Students group

Give a particular username administrator access

Sets EZProxy Username as OA Username  
\*\*Useful for EZProxy Logs\*\*

```
#-----  
# shibuser.txt  
#-----
```

```
If auth:urn:oid:1.7.6.1.4.1.1234.1.4.1.9 eq  
"affiliate@etsu.edu";  
Deny deny.htm
```

```
If auth:urn:oid:1.7.6.1.4.1.1234.1.4.1.9 eq  
"student@etsu.edu";  
Group +Students
```

```
If auth:cn eq "SMITH";  
Admin
```

```
Set login:loguser = auth:cn
```





# EZProxy - shibuser.txt

Where do you find a list of OA Attributes?

- 1) Go to EZProxy Administration
- 2) Click **Manage Shibboleth**
- 3) **Show Shibboleth 2.0 Attributes**

```
#-----  
# shibuser.txt  
#-----
```

```
If auth:urn:oid:1.7.6.1.4.1.1234.1.4.1.9 eq  
"affiliate@etsu.edu";  
Deny deny.htm
```

```
If auth:urn:oid:1.7.6.1.4.1.1234.1.4.1.9 eq  
"student@etsu.edu";  
Group +Students
```

```
If auth:cn eq "SMITH";  
Admin
```

```
Set login:loguser = auth:cn
```



# Resource Lists

OpenAthens MD Documentation <https://docs.openathens.net/display/public/MD/OpenAthens+MD>

OpenAthens Debug Mode <https://docs.openathens.net/display/public/MD/How+to+use+debug+mode>

Ex Libris Developer Network User Authentication (SAML)

[https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst\\_idp/saml](https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst_idp/saml)

SAML Tracer (Firefox) & SAML Chrome Panel (Chrome) <https://www.samltool.com>

EZProxy Shibboleth 1.3/2.x/3.x Authentication

<https://www.oclc.org/support/services/ezproxy/documentation/usr/shibboleth.en.html>



# Questions?

**Travis Clamon**  
Electronic Resources Librarian  
*clamon@etsu.edu*

**Christian Trombetta**  
Library Technology Manager  
*trombettac@etsu.edu*



East Tennessee State University  
University Libraries