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

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

Part of the Computer Engineering Commons

Citation Information

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

This presentation is available at Digital Commons @ East Tennessee State University: https://dc.etsu.edu/etsu-works/3960
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
- Lack of Support

CAS Hosted
- Cost
- Lacks Proxy Functionality

OpenAthens
- Cost
- Reputation
- Industry Leader
- Federated resource access

Inaction
- Problem remains
- User experience
- Bad PR
Choice: OpenAthens
Implementation

April 2017
Acquired OpenAthens through EBSCO

May 2017
Started the process of configuring resources for federated access

June 2017
Alma & Primo Sandbox configuration/testing

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

(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)
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
OA Permissions

Permission Set Allocation
- Attributes
- Rules

Rule-based allocation example:

<table>
<thead>
<tr>
<th>Rule name</th>
<th>When</th>
<th>Apply permission sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibGuest</td>
<td></td>
<td>LibGuest</td>
</tr>
</tbody>
</table>
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.
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
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

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.

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?)
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.)
Alma – OA Resource Configuration (Step 2)

Add SAML Resource

Upload Metadata file downloaded from the Alma Integration Profile
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
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.
Allocate appropriate user access

Permission set allocation for 'AlmaSB'.

- None
- Default
- All

- Default permission set
- FacStaff
- LibGuest
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
- CN
- UserPrincipalName
- Organization 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 alias name...
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)

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
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.

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?)
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
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-----
ThisIsAnExampleANBgkqhkiG9w0BAQsFADCBoDEoMCYGCSqGS
Ib3DQJEARYZYXRoZW5zaGVscEBIZHVzZXJ2Lm9yZy51azELMWkGA1
UEBhMCR0lxETAPBgNVBAgMCFNvbWVyc2V0MQ0wCwYDVQQH
DARCYXRoCYGCSqGSI=
-----END CERTIFICATE-----
```
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.
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 Browse...
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
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).

<table>
<thead>
<tr>
<th>OpenAthensETSU</th>
<th>SAML</th>
<th>ALMA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Image](https://via.placeholder.com/150)

- **Certificate**: Select Certificate
- **Active Certificate**: Self-Signed (sha256) 2021-Nov-12
- **Save**
- **Download Active Metadata**
- ![Activate New Certificate](https://via.placeholder.com/150)
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.
EZProxy Authentication using OpenAthens

Steps:

- Generate certificate
- Config.txt
- user.txt
- OpenAthens Resource Configuration
- OpenAthens Attribute Release Configuration
- shibuser.txt
Generate a self-signed certificate in EZProxy for Shibboleth Communication.

This file will be uploaded into OpenAthens as a new SAML Resource (future step)
# 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
Allocate appropriate user access
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 alias name...
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**
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


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