NEW PRIMO AUTHENTICATION

TRANSITIONING FROM PDS TO SAML

ANDREW WALSH | PRIMO SUBJECT MATTER EXPERT
PAUL McBRIDE | SENIOR PRIMO SUPPORT ANALYST

Introductions

Andrew Walsh

Paul McBride
Objectives and Target Audience

Brief Session Description:
• This session will examine the new Primo Authentication mechanism, including Cascading and Parallel Login configurations.

Session Objective(s)
• By the end of this sessions you will know, understand and/or be able to:
  • Plan for moving to the Primo Authentication Manager
  • Understand the advantages and limits of this new option
  • Configure and enable a Profile

Session Target Audience:
• New or Experienced Customers
• Systems or Technical Librarians
• Developers
• Familiarity with current authentication setup

Agenda

1. Primo Authentication Manager
2. How It Works
3. Configuration
4. Customization & Sandbox
5. Next Steps and Support Resources
<table>
<thead>
<tr>
<th>Primo Authentication Manager</th>
</tr>
</thead>
</table>

### Supports

<table>
<thead>
<tr>
<th>Single Sign-On</th>
<th>SAML</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CAS</td>
</tr>
<tr>
<td>Direct Login</td>
<td>Alma</td>
</tr>
<tr>
<td></td>
<td>LDAP/ADFS</td>
</tr>
<tr>
<td></td>
<td>Aleph</td>
</tr>
<tr>
<td>OAuth2</td>
<td>Facebook</td>
</tr>
<tr>
<td></td>
<td>Google</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
</tr>
</tbody>
</table>

### Features

<table>
<thead>
<tr>
<th>Parallel Login</th>
<th>University users</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Community borrowers</td>
</tr>
<tr>
<td>Cascading Login</td>
<td>Try LDAP first</td>
</tr>
<tr>
<td></td>
<td>Try Alma second</td>
</tr>
<tr>
<td>Attribute Mapping</td>
<td>Similar to PDS</td>
</tr>
<tr>
<td></td>
<td>More limited</td>
</tr>
</tbody>
</table>
# Nota Bene

<table>
<thead>
<tr>
<th>Authentication vs. Patron Information</th>
<th>Authorization and Patron Information are separated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Similar to PDS</td>
</tr>
<tr>
<td>Interim Login Page</td>
<td>a.k.a. Parallel Login</td>
</tr>
<tr>
<td></td>
<td>Displayed whenever there are two profiles</td>
</tr>
<tr>
<td>Users</td>
<td>Patrons only</td>
</tr>
<tr>
<td></td>
<td>Cannot be used for Primo staff users</td>
</tr>
<tr>
<td>LDAP</td>
<td>Connection must be secure (SSL or TLS)</td>
</tr>
<tr>
<td></td>
<td>Certificate must be signed by a recognized certificate authority</td>
</tr>
<tr>
<td></td>
<td>SAML cannot use LDAP for patron information</td>
</tr>
<tr>
<td>Customization</td>
<td>Limited (compared to PDS)</td>
</tr>
<tr>
<td></td>
<td>Shares header &amp; footer of the View</td>
</tr>
<tr>
<td>SSO</td>
<td>SAML only</td>
</tr>
<tr>
<td></td>
<td>SAML must be the first profile</td>
</tr>
</tbody>
</table>

# How It Works

![Diagram of gears]
Authentication & Authorization Flow

Primo

- Login request
- Session created: Request user info (GUEST)
- Login Success
- Process received information
- Identity Confirmed: Return ID code
- User ID confirmed: Return user information

Patron Information Source

OAuth2 – Authentication Flow

Primo

- Login request
- Send email invitation
- Continue as John
- Login Success

Alma

- Choose OAuth system and send request
- User consents: (Facebook, Google)
- Token received: Adding social ID to user identifiers
- Request user ID
- Login Success
- Create and deliver access – token & Social ID
- Token Verified: Send confirmation
Request & Loans API

Primo

- Perform request/Loan
  - Session ID (PDS handle)

- Request/loan Enabled

Alma

- Are you Authorized?
  - Query Primo/PDS
    - User verified and authorized

PDS link

- PDS | Primo

Patron ID pitfall

Primo stores everything based on the ID returned from PDS

- E-Shelf
- Saved Search
- Saved Search Alerts
- Tags & Reviews
- Search Preferences (e.g. results per page)
- Personalized Results

Switching may result in the ID changing

- This will make all previous information inaccessible
- Migrating user content to new IDs is **not** covered by Support
Cascading & Parallel Login

Cascading Login

Setup
- Only with LDAP & Alma profiles
- Determines the order profiles are checked
- Requires 2 other profiles be created first

Use cases
- Multiple LDAP servers
- Over 5 LDAP search bases
- Alma users not in LDAP

Parallel Login

Setup
- Works with all profile types
- Select a Second Profile

Use cases
- SAML for University Patrons
- Alma for Community Borrowers
- SAML for University Patrons
- Different SAML for Alumni Patrons

Interim login page
- User selects a login profile
- Link order matches profile order

SAML Certificate Primer

1. User supplies credentials
2. Access Check
3. POST signed <Response>
4. Redirect with <AuthnRequest>
5. User login
6. Supply resource
7. signed response
8. access resource

Interim login page
- User selects a login profile
- Link order matches profile order
SAML Certificate Primer

Key Pairs

- Use **Public Key** to ensure only those holding the **Private Key** can use the data
- Use **Private Key** to prove data came from you

IdP produces the Signed Response (step 5 to 6)

- Signs the data with the **IdP Private Key** (i.e. proves the response came from the IdP)
- Encrypts the data with the **Primo SP Public Key** (i.e. only the Primo SP can access the data)

Primo SP receives the Signed Response (step 7)

- Decrypts the data with the **Primo SP Private Key** (i.e. source has the **Primo SP Public Key**)
- Checks the signature with the **IdP Public Key** (i.e. verify the data is from the IdP)

**Keys must be exchanged outside of the SAML process**
Configuration

1. Configuring a Profile
2. Cascading Login
3. Parallel Login
4. Attribute & Value Mapping
5. Alma Configuration

Configuration Tooltip

Active Login Profiles:

Main Profile: ALMA
Secondary Profile: SAML

Profiles:

<table>
<thead>
<tr>
<th>Login Profile</th>
<th>Authentication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALMA</td>
<td>ALMA</td>
</tr>
<tr>
<td>ALMA-LDAP</td>
<td>Cascading</td>
</tr>
<tr>
<td>INCOMP</td>
<td>SAML</td>
</tr>
<tr>
<td>LDAP</td>
<td>LDAP</td>
</tr>
<tr>
<td>SAML</td>
<td>SAML</td>
</tr>
</tbody>
</table>

1. INCOMP: IDP_LOGIN_URL parameter must be specified
2. INCOMP: IDP_ISSUER parameter must be specified
3. INCOMP: KeyStore file must be uploaded
4. INCOMP: Information method is not selected
Cascading Login Profile – Creating

Login Profiles

Owner: Yarnaro Island University

Active Login Profiles:

Main Profile: Alma1
Secondary Profile: Select Profile

Profiles:

<table>
<thead>
<tr>
<th>Login Profile</th>
<th>Authentication Method</th>
<th>User Information Method</th>
<th>Edit</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alma</td>
<td>ALMA</td>
<td>ALMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>LDAP</td>
<td>LDAP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Create a New Login Profile

Profile Name

Create a New Cascading Profile

Profile Name
Parallel Login in the BE

**Login Profiles**

- **Owner:** Installation

**Active Login Profiles:**

- **Main Profile:** Ldap
- **Secondary Profile:** SAML

**Profiles:**

<table>
<thead>
<tr>
<th>Login Profile</th>
<th>Authentication Method</th>
<th>User Information Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ldap</td>
<td>LDAP</td>
<td>LDAP</td>
</tr>
<tr>
<td>SAML</td>
<td>SAML</td>
<td>SAML</td>
</tr>
</tbody>
</table>

Parallel Login

**Login using:**

**Shibboleth Login**

The link above is where you log into Primo using your Shibboleth credentials (for Students, Staff, Faculty)

**Alma Login**

The link above is where you log into Primo using your Alma internal user credentials (for Community Borrowers)

Cancel
Attribute & Value Mapping

Available after you save a profile

Defaults are filled in for you
  • Appropriate for Alma

Value Mapping instructions are backward
  • Follow the hints
  • First column is the value in the source system
  • Second column is the desired value

Attribute & Value Mapping Example

<table>
<thead>
<tr>
<th>Primo Attribute</th>
<th>Source Attribute</th>
<th>Set Value Mappings</th>
</tr>
</thead>
<tbody>
<tr>
<td>email_address</td>
<td>email</td>
<td></td>
</tr>
<tr>
<td>group</td>
<td>group</td>
<td></td>
</tr>
<tr>
<td>01</td>
<td>graduate</td>
<td>+</td>
</tr>
<tr>
<td>02</td>
<td>undergraduate</td>
<td>+</td>
</tr>
<tr>
<td>03</td>
<td>staff</td>
<td>+</td>
</tr>
<tr>
<td>Source Value</td>
<td>Target Value</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>sn</td>
<td></td>
</tr>
<tr>
<td>ils_api_id</td>
<td></td>
<td></td>
</tr>
<tr>
<td>institute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>cn</td>
<td></td>
</tr>
</tbody>
</table>
Attributes List

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>email_address</td>
<td>The user’s email address. Primo will use this email address if the user does not have an email address defined in Primo. If the EMAIL_OVERRIDE authentication parameter has been enabled, the value of this attribute will override the email address defined for the user in Primo. For Alma the default mapping is email_address.</td>
</tr>
<tr>
<td>group</td>
<td>The user group. For Alma the default mapping is group.</td>
</tr>
<tr>
<td>id</td>
<td>The user ID. For Alma the default mapping is id.</td>
</tr>
<tr>
<td>ils_api_id</td>
<td>The ID used for OPAC via Primo in case it is not the same as the regular ID. For Alma there is no default mapping because this attribute is not required for Alma.</td>
</tr>
<tr>
<td>institute</td>
<td>The Primo institution. This attribute can be used if there is a need to override the institution that the user signed in with (that is the institution of the view). For Alma there is no default mapping because the Primo institution defaults to the institution of the active view. If you want to override the institution of the view, you can specify an Alma attribute.</td>
</tr>
<tr>
<td>name</td>
<td>The name that displays for the user in the Primo Front End. For Alma the default mapping is userName.</td>
</tr>
</tbody>
</table>

Alma Configuration – PDS IPs

- Update PDS IPs table
- Should already be setup for OvP
- Contact ExLibris to confirm set up
**Alma Configuration – Primo PDS URL**

- Update the `primo_pds_url`
  - Found under Alma > General Configuration > Configuration Menu > General Configuration > Other Settings
  - Set it to a URL formatted like:

  ```
  http://<host>:<port>/primo_library/libweb/webservices/rest/PDSUserInfo?
  ```

**Alma Configuration – Patron Identifier**

- Check patron record for identifier value and make sure they have the “Patron” permissions
Login Page Customization

User Login Code Table
- Customize labels
- Localize labels
- Add descriptions for Parallel Login page

Static HTMLs
- Includes the header and footer of the View
- New Login Tips – Bottom element
  - Display login tips
  - Not on Parallel Login page

CSS
- Add elements to the customized View CSS
- Controls if Tips are displayed inline or as a column
- Selectors for the links, input fields, and buttons
**Sandbox Testing**

**In Alma**
- Update `primo_test_pds_url` to your Primo Sandbox
- Add the Primo Sandbox FE IP addresses to PDS IPs table

**In Primo**
- Append `&env_type=test` to the Template Code field of
  - `almasonic_services`
  - `Almaviewit_remote`
  - `Almagetit_remote`
  - `Almagetit`
  - `Almasingle_service_remote`
  - `almaviewit_services`
  - `almaggetit_services`
  - `Almasingle_service`
  - `Almaviewit`

**Next Steps and Support Resources**
- Customer Knowledge Center
  - [Primo User Authentication](#)
  - [Attribute Mapping](#)
  - [Primo Authentication configured and working but Alma GetIt still wants me to sign in](#)

- Additional support resources within the ExLibris Ecosystem:
  - [Idea Exchange](#)
  - System Status Pages: [Single Tenant ENV](#) / [Multi-Tenant ENV](#)
  - [Developer Network](#)

- [Technical Seminar Presentations](#)
  (located in the Cross-Product section of the CKC)
Q & A

Any Questions?

Session Survey Evaluation

Please use the following link https://www.surveymonkey.com/r/techsem2017 to provide feedback on your sessions.
THANK YOU
Andrew.Walsh@exlibrisgroup.com

Image Credits

- Lock & Key
- Gears 1
- Gears 2
- SAML
- Sandbox