NEW PRIMO AUTHENTICATION

TRANSITIONING FROM PDS TO SAML

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

ExLibris
a ProQuest Company

Introductions

Andrew Walsh

Paul McBride

2
ExLibris

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

ExLibris

Agenda

1 Primo Authentication Manager

2 How It Works

3 Configuration

4 Customization & Sandbox

5 Next Steps and Support Resources

ExLibris

Primo Authentication Manager

ExLibris

Primo Authentication Manager

Supports	Single Sign-On	SAML
		CAS
	Direct Login	Alma
		LDAP/ADFS
		Aleph
	OAuth2	Facebook
		Google
		Twitter
Features	Parallel Login	University users
		Community borrowers
	Cascading Login	Try LDAP first
		Try Alma second
	Attribute Mapping	Similar to PDS
		More limited

ExLibris

Nota Bene

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

How It Works

Authentication & Authorization Flow
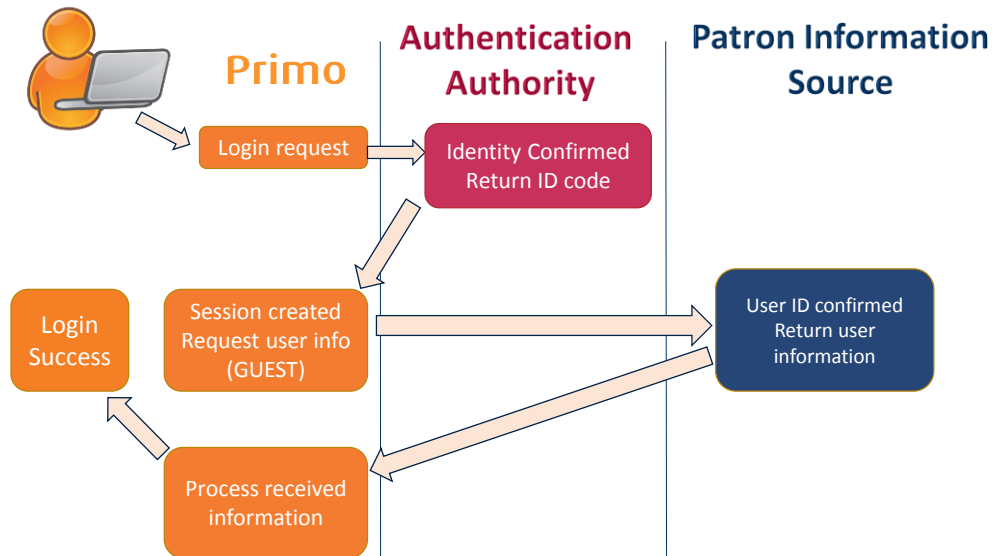
OAuth2 – Authentication Flow
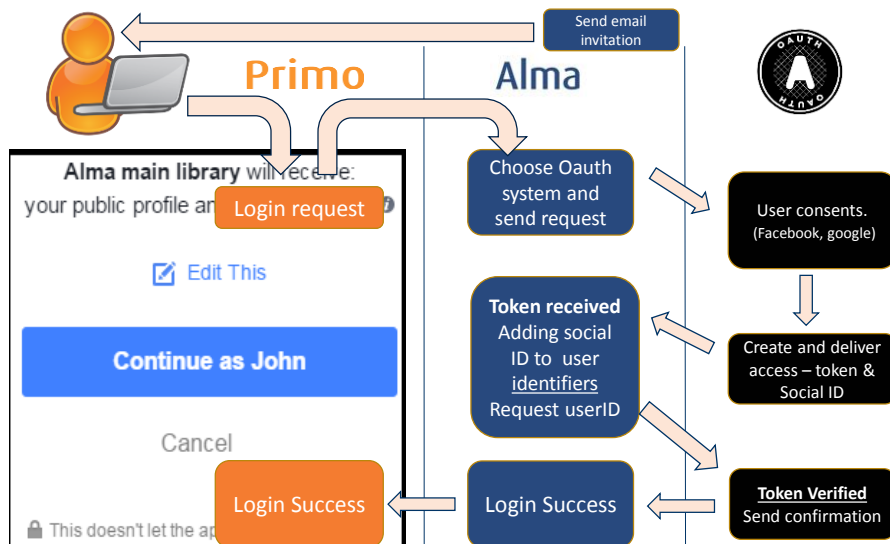
Request & Loans API
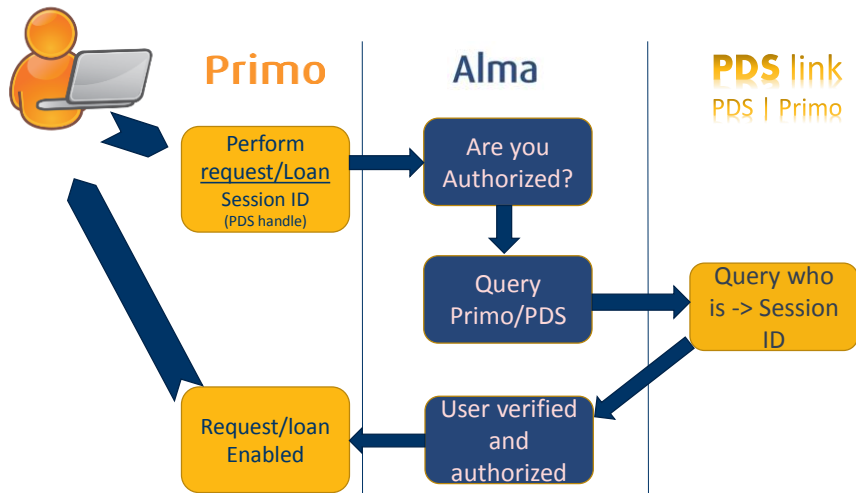
Patron ID pitfall

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

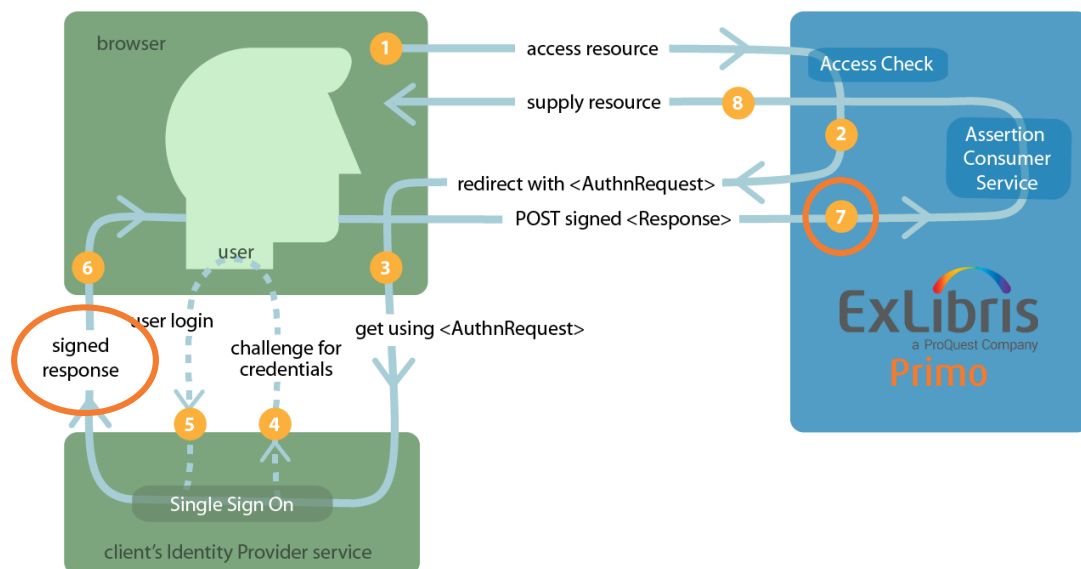| Cascading Login | Setup | Only with LDAP & Alma profiles |
		Determines the order profiles are checked
		Requires 2 other profiles be created first
	Use cases	Multiple LDAP servers
		Over 5 LDAP search bases
		Alma users not in LDAP
Parallel Login	Setup	Works with all profile types
		Select a Second 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

ExLibris

SAML Certificate Primer

browser
1 access resource → Access Check
8 supply resource
2 Assertion Consumer Service
redirect with <AuthnRequest>
POST signed <Response> 7
user
6 user login   3 get using <AuthnRequest>
signed response   challenge for credentials
5   4
Single Sign On
client's Identity Provider service

ExLibris
a ProQuest Company
Primo

ExLibris

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

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:

Login Profile	Authentication Method
ALMA	ALMA
ALMA-LDAP	Cascading
INCOMP ⚠	SAML
LDAP	LDAP
SAML	SAML

> IDP_LOGIN_URL parameter must be specified
> IDP_ISSUER parameter must be specified
> KeyStore file must be uploaded
> Information method is not selected

LIVE DEMO!

SEARCH_BASE_1

Configuring

Collect A
Data

Configu
Alma P

Select
Inforr
sourc

Attri
Mar

Select Us

Profile Name: ALMA

Select Authentication Method: ALMA ▼

ALMA_LOGIN_URL   http://sandbox.alma.exlibrisgroup.com/mng/login/r

ALMA_INSTITUTION   SUPHQ1_INST

Select User Information Method: ALMA ▼

USER_INFO_URL   http://sandbox.alma.exlibrisgroup.com

C=com

RESPON

Cascading Login Profile – Creating

Login Profiles

Owner: Volcano Island University ▼

Active Login Profiles:

Main Profile: Alma1 ▼
Secondary Profile: Select Profile ▼

Profiles:

Login Profile	Authentication Method	User Information Method	
Alma	ALMA	ALMA	Edit
Ldap	LDAP	LDAP	Edit

Create a New Login Profile

Profile Name [   ] Create

Create a New Cascading Profile

Profile Name [   ] Create

Cancel & Go Back   Clear   Save

Cascading Login Profile – Profile Selection

> **Create Cascading Profile**

Set Profiles:

Profile #1   ALMA ▼

Profile #2   LDAP ▼

Cascading Login Profile

> **Login Profiles**

Owner: Volcano Island University ▼

Active Login Profiles:

Main Profile:	Alma1 ▼
Secondary Profile:	Select Profile ▼

Profiles:

Login Profile	Authentication Method	User Information Method	
Alma	ALMA	ALMA	Edit
Casc Alma Ldap	Cascading		Edit Delete
Ldap	LDAP	LDAP	Edit

Create a New Login Profile

Profile Name [   ] (Create)

Create a New Cascading Profile

Profile Name [   ] (Create)

(Cancel & Go Back)   (Clear) (Save)

Parallel Login in the BE

Parallel Login

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

ExLibris

Attribute & Value Mapping Example

Primo Attribute	Source Attribute	
email_address	email	Set Value Mappings
group	group	Set Value Mappings
01	graduate	+ −
02	undergraduate	+ −
03	staff	+ −
Source Value	Target Value	+ −
id	sn	Set Value Mappings
ils_api_id		Set Value Mappings
institute		Set Value Mappings
name	cn	Set Value Mappings

ExLibris

Attributes List

Attribute	Description
email_address	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.
group	The user group. For Alma the default mapping is group.
id	The user ID. For Alma the default mapping is id.
ils_api_id	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.
institute	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.
name	The name that displays for the user in the Primo Front End. For Alma the default mapping is userName.

Alma Configuration – PDS IPs

- Update PDS IPs table
- Should already be setup for OvP
- Contact ExLibris to confirm set up

Table Information

Sub System	INFRA
Updated By	exl_impl
Table Description	Allowed PDS IP values for ExLibris internal APIs' authentication

	Table Name	PDS IPs
	Last Updated	01/28/2016

— Mapping Table Rows

Tools

	Enabled	IP value	IP description	Updated By	Last Updated	
1	✓	10.28.104.71	Primo IMPL FE1	exl_impl	11/24/2015	Delete
2	✓	66.151.7.163	Primo IMPL LB	exl_impl	11/24/2015	Delete
3	✓	10.28.120.123	Primo PMTNA03 FE1	exl_impl	11/24/2015	Delete
4	✓	10.28.120.124	Primo PMTNA03 FE2	exl_impl	11/24/2015	Delete
5	✓	10.28.120.125	Primo PMTNA03 FE3	exl_impl	11/24/2015	Delete
6	✓	66.151.7.11	Primo PMTNA03 LB	exl_impl	11/24/2015	Delete
7	✓	10.28.136.29	Primo MTD Sandbox FE1	exl_impl	11/24/2015	Delete
8	✓	64.74.237.218	Primo MTD Sandbox LB	exl_impl	11/24/2015	Delete
9	✓	10.28.120.110	Primo PMTNA02 FE1	exl_impl	12/23/2015	Delete
10	✓	10.28.120.111	Primo PMTNA02 FE2	exl_impl	12/23/2015	Delete
11	✓	10.28.120.112	Primo PMTNA02 FE3	exl_impl	12/23/2015	Delete
12	✓	66.151.7.8	Primo PMTNA02 LB	exl_impl	12/23/2015	Delete
13	✓	192.80.206.206	New Chicago Firewall IP	exl_impl	12/23/2015	Delete

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?

19	page_size	general	20	
20	primo_patron_info_updatable	general	Y	user is updatable
21	primo_pds_url	general	https://primo-pmtna02.hosted.ex	Primo pds url
22	primo_service_page_url	general	http://exl-impl-primo.hosted.exlil	

ExLibris

Alma Configuration – Patron Identifier

- Check patron record for identifier value and make sure they have the "Patron" permissions

External authentication application's attribute (LDAP, CAS, Shibb) must match a value in one of the Alma identifier fields in order for bor_info to be retrieved in Primo.

ExLibris

15
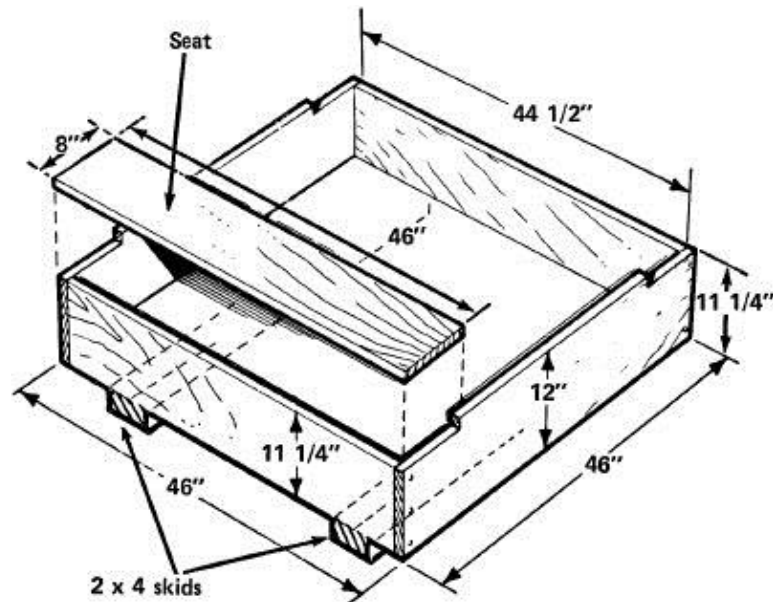
Customization & Sandbox

ExLibris

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

ExLibris

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
  - almasingle_services
  - Almaviewit_remote
  - Almagetit_remote
  - Almagetit
  - Almasingle_service_remote
  - almaviewit_services
  - almagetit_services
  - Almasingle_service
  - Almaviewit

42

ExLibris

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)

43

ExLibris

Q & A

Any Questions?

49
ExLibris

Session Survey Evaluation

Please use the following link
https://www.surveymonkey.com/r/techsem2017
to provide feedback on your sessions.

50
ExLibris

THANK YOU
Andrew.Walsh@exlibrisgroup.com

ExLibris
a ProQuest Company
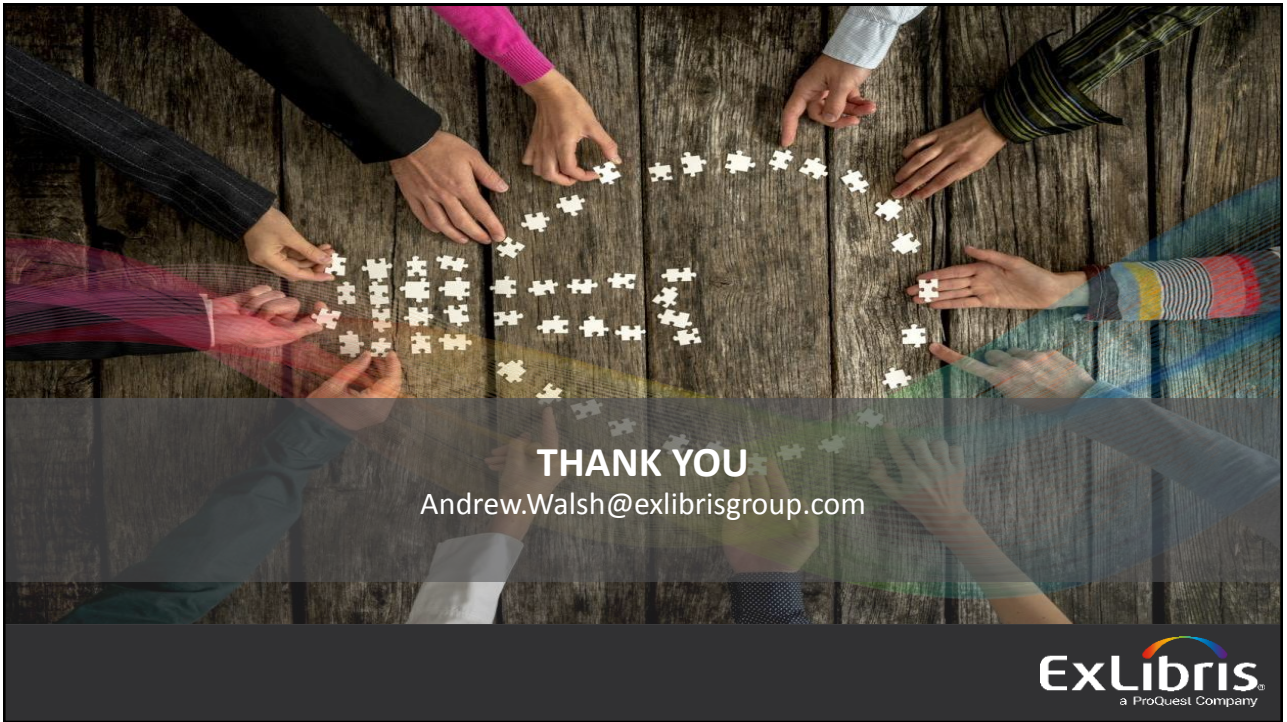
Image Credits

Lock & Key

Gears 1

Gears 2

SAML

Sandbox

ExLibris