Implementing and Demystifying ILLiad’s Integrated SAML Module

Heidi Webb
Discovery and Systems Librarian
Upstate Medical University
IDS Project Summer Conference 2022
Overview

• ILLiad Authentication Options
• Why SAML Integrated Module
• What is SAML
• User Login Experience
• Attribute/Metadata Exchange in the Background
• Getting Started
• Items to Ask Your SAML Administrator
• Items Your SAML Administrator Will Ask You
• Wrap Up
ILLiad Authentication Options

• ILLiad Authentication (ILLiadAuth)
• LDAP Authentication
• RemoteAuth
  • Usually requires an intermediary system
    • Ex: OCLC’s EZ Proxy
  • ILLiad SAML authentication (NEW)
Why is Upstate Medical University interested in the SAML module?

• SAML is more secure than LDAP
• Improve user experience with single sign on
• OpenAthens implemented in 2019
  • Currently uses campus Azure system and local OpenAthens accounts
• ILLiad is the only library funded product still running through EZ Proxy
What is SAML?

• SAML = Security Assertion Markup Language

• Open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP)
  • Identity Provider (IdP) = SAML authentication system
  • Service Provider (SP) = ILLiad

• Login information is not managed or stored in the tool users are accessing

• Enables Single-Sign On (SSO) – where users can log in once and those same credentials can be reused in the background to log into other services

• An example of interoperability
Two Primary Purposes

• SAML authentication is the process of verifying the user’s identity and credentials

• SAML authorization tells the service provider what access to grant the authenticated user
Examples of SAML Systems

• ADFS
• Azure Active Directory
• Central Authentication Server (CAS)
• OpenAthens
• Oracle Identity Federation
• Sailpoint Identity Now
• SecureAuth
• Shibboleth
Click ILLiad Link

Is the user logged in to the SAML system already?

Yes: Does an ILLiad account already exist?

Yes: View ILLiad homepage or request page

No: Login

No: New User Registration Page
Link Format

- https://{ILLiadbaseURL}/illiad/
  - Example: https://upstate.illiad.oclc.org/illiad/


- Note: No login parameter. No proxy prefix.
Pause for Reality
Access Link In Live Action

• Albany Medical College’s Schaffer Library of Health Sciences
  • https://amc.illiad.oclc.org/illiad/
What is Happening in the Background?

• If the user is valid, metadata in XML format is getting passed between systems
  • Metadata from your SAML authentication system to ILLiad
    • Specifically, attributes available from the SAML xml file get passed to ILLiad and ILLiad, using the RemoteAuthValidation table in the Customization Manager, translates those attributes to fields in ILLiad

• Metadata = Attributes
Snippet from XML file coming from Azure

```
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
  <AttributeValue>Webb</AttributeValue>
</Attribute>

<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
  <AttributeValue>WebbH@upstate.edu</AttributeValue>
</Attribute>

<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
  <AttributeValue>WebbH@upstate.edu</AttributeValue>
</Attribute>

<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/forenames">
  <AttributeValue>Heidi</AttributeValue>
</Attribute>

<Attribute Name="hrtitle">
  <AttributeValue>Senior Assistant Librarian</AttributeValue>
</Attribute>

<Attribute Name="employeetype">
  <AttributeValue>STEMP</AttributeValue>
</Attribute>

<Attribute Name="dept">
  <AttributeValue>Library</AttributeValue>
</Attribute>
```
RemoteAuthValidation Table

Using the snippet from Azure and depending on what fields you want to ingest into ILLiad, the table would look like:

<table>
<thead>
<tr>
<th>ID</th>
<th>NVTC</th>
<th>ILLIdFieldName</th>
<th>RemoteFieldName</th>
<th>Validation</th>
<th>ValidAction</th>
<th>InvalidAction</th>
<th>ValidDefault</th>
<th>Invalid...</th>
<th>Overwrite</th>
<th>LogIfChang...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ILL</td>
<td>Username</td>
<td>CN</td>
<td>.+</td>
<td>accept</td>
<td>reject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ILL</td>
<td>#EMailAddress</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>.+</td>
<td>accept</td>
<td>reject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ILL</td>
<td>FirstName</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/firstname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/firstname</a></td>
<td>.+</td>
<td>accept</td>
<td>ignore</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ILL</td>
<td>LastName</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a></td>
<td>.+</td>
<td>accept</td>
<td>ignore</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>ILL</td>
<td>Department</td>
<td>dept</td>
<td>.+</td>
<td>accept</td>
<td>ignore</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RemoteAuthValidation in the Wild

• Albany Medical College

<table>
<thead>
<tr>
<th>ID</th>
<th>NVTC</th>
<th>LIllIdFieldName</th>
<th>RemoteFieldName</th>
<th>Validation</th>
<th>ValidAction</th>
<th>InvalidAction</th>
<th>ValidateDefault</th>
<th>InvalidDefault</th>
<th>Overwrite</th>
<th>LogIfChanged</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ILL</td>
<td>Username</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/dms/name">http://schemas.xmlsoap.org/ws/2005/05/identity/dms/name</a></td>
<td>.+</td>
<td>accept</td>
<td>reject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>ILL</td>
<td>EmailAddress</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/dms/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/dms/emailaddress</a></td>
<td>.+</td>
<td>accept</td>
<td>ignore</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>ILL</td>
<td>LastName</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/dms/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/dms/surname</a></td>
<td>.+</td>
<td>accept</td>
<td>ignore</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>ILL</td>
<td>FirstName</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/dms/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/dms/givenname</a></td>
<td>.+</td>
<td>accept</td>
<td>ignore</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Using Azure
• Lessons learned: fields are case sensitive
New User Registration

- NewAuthRegistration.html
- Choose to show but not allow the user to edit fields coming from Azure: First Name, Last Name, and Email
Ready for Implementation? Now What?

• Must be on version 9.2

• Check out the documentation
  • It includes step by step setup and indicates who needs to do what (library staff vs. staff that host/manage the ILLiad server)

• Contact your SAML Administrator

• Contact your ILLiad server host
  • OCLC ➔ contact OCLC, express interest, and ask to get on the list
  • Self hosted or other hosting providers ➔ start the conversation. Send the documentation.
What You Need to Ask From the SAML Admin

• Metadata URL
  • ILLiad hosting provider will need this information to get started
  • Examples:
    • https://login.openathens.net/saml/2/metadata-idp/upstate.edu
    • https://login.microsoftonline.com/{localcodefromazure}/federationmetadata/2007-06/federationmetadata.xml?appid=5df6c7c4-642c-42fa-8782-9ad912d17f56
    • https://idp.upstate.edu/metadata/samlidp/OpenAthens_SAML_IDP_Profile

• What attributes to release (ex: username, email, first name, etc.)

• Format of attributes – What the attribute “Name” is that will pass through the XML file
  • SAML Administrator should be able to see these values

• Security Certificate
  • If required, after some of the configuration is setup, the SAML admin can generate a security certificate
Questions the SAML Administrator Will Ask

• ILLiad Metadata URL
  • Once files are configured, it will be https://{ILLiadserverURL}/illiad/metadata/
  • ILLiad hosting provider will download this and give you the file after you have given the ILLiad host your SAML’s metadata URL and configured some files using that information

• Attributes
  • Which ones and why?

• Security Certificates
  • These come as files from the ILLiad hosting provider once some initial configuration files are set up
Where is Upstate in Implementation?

- Documentation read
- Metadata URL for OpenAthens sent to OCLC
- Waiting for OCLC to start the configuration process
- Remote Authentication Table is minimally configured except for the username field which is currently setup for EZ Proxy
- Note: because Upstate is using OpenAthens as the SAML product, the SAML administrator is within the library
Expected Next Steps

• OCLC will populate saml.config file and then run a powershell script on the server

• OCLC will send ILLiad metadata file from the url https://upstate.illiad.oclc.org/ILLiad/metadata

• Upstate will use the metadata file to create “ILLiad” as a resource in SAML system

• Upstate will set attributes to release - Since we are using OpenAthens, we will release only the minimum needed for ILLiad specifically. Not a global release of all attributes in the system.

• Exchange security certificates
Expected Steps at Go Live

• OCLC updates IdpMapping.config
• Upstate edits files in the Customization Manager
  • RemoteAuthWebLogoutURL – We will send users to an intermediary page for now because some users will need to logout of two systems to fully logout: OpenAthens AND Azure.
  • RemoteAuthValidation - confirm values and switch username from EZ Proxy Version to field needed from OpenAthens
  • UseLegacyRemoteAuthHandling - set to no
• Upstate changes access URLs
Additional Resources

• Documentation from Atlas Systems
  • RemoteAuth Configuring the Integrated SAML Module
  • Automatic User Creation
  • ILLiad Database Tables
  • Configuring RemoteAuth Validation Table

• Presentations by Atlas Systems
  • IDS Spring 2022 Virtual User Group
    • Introducing Integrated SAML Setup with Single Sign-on Support (Video)
  • Atlas Training
    • ILLiad Integrated SAML Module
Special Thanks to Debra Wellspeak at Albany Medical College
Questions and Next Steps

• Will email the IDS listserv with a synopsis of implementation as an OCLC hosted site

• Contact
  • Heidi Webb
  • webbh@upstate.edu