LDAP: What Is It, Do I Want It, and How Do I Make It Work for Me?

Rebecca Hyams
SUNY Maritime College
Overview

- LDAP: more than random letters?
- Determining if you have LDAP
- Advantages/disadvantages
- Making ILLiad play nice
- Working out the kinks
But First...

- Show of hands:
- How many of you already use LDAP?
- ILLiad Authentication?
- Something else?
- Not sure?
- Want to set up LDAP?
Disclaimer:

I am not a trained IT Person
(The upside is I can spare you the jargon)

My knowledge comes solely from the ILLiad side of the equation

As far as I’m concerned, the backend is wizard magic!
LDAP...?

- Stands for **Lightweight Directory Access Protocol**
- Standardized way of storing user permissions and directory information
- Installed on a centralized server
- Works in the background to authenticate sign-in for various services
Do we have that?

- Do you or your users use the same username/password for multiple services like:
  - EZ-Proxy (or other off-site database access)
  - Email
  - Library accounts
  - Course Management Platforms
According to the Atlas Documentation there are actually five methods of authentication:

- **Basic ILLiad**
  - Default setup
- **ILLiad Exclusive**
  - Users are pre-populated/approved, users can’t self-register and staff can’t add them
- **LDAP**
  - Has to exist at institution
- **User Gateway**
  - Really complicated
- **III Patron API**
  - Only if you use Innopac and have the module
Default Setting

- By default ILLiad uses “ILLiad Authentication”
  - Username/password stored in the ILLiad user database
- When a new user approaches the system they need to click a “new user” link and go to the New User Registration form
- After they fill the form they get placed in the Clear Users queue in ILLiad
With LDAP

- Everyone (new and existing users) use the same logon box
  - If the LDAP username has no match in the ILLiad database, the user is brought to NewAuthRegistration to fill out a registration form
  - If the LDAP username matches a name in the ILLiad database, they are taken to the Main Menu

- ILLiad database does not contain LDAP passwords.
  - Passwords are used only to match on the LDAP authentication
  - Password resets cannot be done by ILL Staff
Making the Decision

- If you have the buy-in from IT and have an LDAP Server at your institution, considerations include:
  - Time spent clearing users
  - Handling existing vs. new users
    - Is it feasible to make a correlation table?
    - Will the reference/instruction folks support the changes?
  - Are you hosted?
    - If you’re self-hosted you may have way more to grapple with
The Good

- One fewer username/password to remember for your users
  - At Maritime our users now have the same login for ILLiad that they have for campus wifi, desktop workstations, their email, off-campus database access, and Angel
- No more clearing users manually
  - LDAP authenticates only if they’re active
The Bad

- Need to get buy-in from the keeper of the LDAP (likely IT)
  - They may need to help with configuration and testing
  - There may be firewall or security issues
- If the LDAP Server is down, no one can sign into your ILLiad page
- If you already have users you *may* have a mess on your hands…
The (possibly very) Ugly

- If you already have users in your ILLiad system you have three options:
  1. Grandfather in existing users with their ILLiad usernames/passwords, make new users use LDAP.
  2. Start everyone over with LDAP, creating new accounts for existing users.
  3. Make a correlation table of existing usernames and their corresponding LDAP names. Have OCLC do some magic.
Option 1: Grandfathering

- Keeps the existing accounts in the system as-is
  - Existing users will continue to log in as they have in the past (ILLIad authentication)
  - Only users that create accounts after LDAP implementation will go through LDAP

- Can cause many headaches for Reference/Instruction folks
  - Users might not know which camp they’re in
Option 2: Burn and Rebuild

- All users to use LDAP log-in
- Everyone has the same log-in process
- Existing users also have to reregister
- Existing users lose account history
  - Which can be disastrous if they refer back to their old requests for citations
Option 3: Down and Dirty

- "You’re probably not going to want to do this but…"
- Create a table of existing usernames and their LDAP equivalents
  - Can be super involved if usernames are not predictable or obvious
- If you’re hosted, OCLC will merge the LDAP usernames and existing user data
- End result is that everyone uses LDAP and existing users remain in the system with their history

<table>
<thead>
<tr>
<th>ILLiad Username</th>
<th>LDAP Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>abdullahkoc.09</td>
<td>abdullahkoc.09</td>
</tr>
<tr>
<td>Acolleran</td>
<td>acolleran</td>
</tr>
<tr>
<td>AlexanderSha</td>
<td>AlexanderSha.12</td>
</tr>
<tr>
<td>Alexcarela</td>
<td>alexandreca.08</td>
</tr>
<tr>
<td>alexcar.11</td>
<td>Alexcar.11</td>
</tr>
<tr>
<td><a href="mailto:alexvug.11@sunymaritime.edu">alexvug.11@sunymaritime.edu</a></td>
<td>alexvug.11</td>
</tr>
</tbody>
</table>
Maritime chose option #3
Ran a report of all registered users (we only had about 240)
Added a column for LDAP name
In some cases a single user had more than one account so they had to be merged
Made sure everyone had the right delivery and notification preferences set
  - Users who created accounts before those were hidden default fields sometimes skipped them or put weird preferences
Correlating Names:

If their username already followed one of our LDAP patterns, I copied it to the LDAP name column.

If they used their campus email, I copied that, trimming off the @sunymaritime.edu suffix.

If they were faculty or staff I used the first initial + last name LDAP pattern.

If they were a student I looked them up in the campus directory (because our pattern includes their year of entry).

If they weren’t in the campus directory I flagged them (9 users) because they’re presumably no longer valid.
The Easy Part

- Once LDAP was enabled for ILLiad we made some tweaks to the log-in page
  - (for about 10 days we had a Grandfather solution)
    - 6 requests in that entire time
  - We did the whole process in early January when everything was quiet
- OCLC support ran a bunch of scripts and did testing to make sure things were right
IT and the Fun Stuff

- There are several keys in Customization Manager that deal with LDAP
- You will almost definitely need someone from IT to assist
- If you’re lucky they’ll just give you the information you need
  - (If you’re me you have two guys come and bumble for a bit before getting it right)
By the way...

- There are two styles of LDAP, one-step and two-step
  - Two-step is more secure (but whatever your institution uses is what you’ll use here)
- They require different keys in Customization Manager
- Set type in LDAPBindStyle
  - OneStep or TwoStep
About Setup

- Your local friendly IT person *should* be able to provide the information
  - The required information appears to be similar from platform to platform
- They may need to open the firewall to allow communication between ILLiad and the LDAP server
Your Keys

- All the keys you need are located under Web Interface → LDAP in Customization Manager
Info You’ll Need:

- LDAPPortNo
- LDAPSearchPrefix
- LDAPSearchSuffix
- LDAPServerName
- LDAPVersion
- LDAPInitialBindDN
- LDAPInitialBindPassword
- LDAPSearchFilter
- LDAPSearchScope
- LDAPSearchSuffix
- LDAPSecureSSL
- LDAPSecureSSLPort
- LDAPServerName
- LDAPVersion
What Do I Put For...?

- I can show you what we have, but...
- Every setup is going to be different
- Variables include how many directories you have, OneStep vs. TwoStep
- The keeper of your server should know what works with your LDAP
Super Important!

For ILLiad to know which type of authentication you’re using by default you need to set the key in Customization Manager.

- Web Interface → Authentication → WebAuthType
Also Good to Know

- Even if you have LDAP Authentication as default, you can still have users that use ILLiad Authentication
  - “ILLiad Authentication” box **MUST** be checked off for them to log in to their account
Coexistence

- It’s complicated, but LDAP and ILLiad authentication can co-exist, even for new users
  - Nassau Community College has students use LDAP and Faculty/Staff use ILLiad authentication
  - Page has to have both sets of instructions
    - (And sometimes students don’t follow them and try to create accounts manually)
On the Web Side...

- Biggest problem is that there is only one way to view NewAuthRegistration as your users will see it:
  - Log in with a valid LDAP username that does not exist in your ILLiad database
  - Essentially a one-shot page
Maritime’s Experience

- There had been a previous unsuccessful attempt to set up LDAP when we installed ILLiad in 2009
- Over 4 ½ years prior to LDAP implementation approx. 240 users registered for accounts
  - Some of those were duplicate accounts
    - (one faculty member had created three separate ones!)
- Added approx. 30 new accounts post-LDAP so far
  - Tied for best spring for registration with Spring 2011
Requests by User Status

- Fall 09:
  - Faculty/Staff/Admin: 7
  - Student: 24
  - Other: 1

- Spring 10:
  - Faculty/Staff/Admin: 49
  - Student: 3
  - Other: 22

- Fall 10:
  - Faculty/Staff/Admin: 46
  - Student: 1
  - Other: 50

- Spring 11:
  - Faculty/Staff/Admin: 64
  - Student: 8
  - Other: 17

- Fall 11:
  - Faculty/Staff/Admin: 59
  - Student: 3
  - Other: 74

- Spring 12:
  - Faculty/Staff/Admin: 41
  - Student: 4
  - Other: 39

- Fall 12:
  - Faculty/Staff/Admin: 38
  - Student: 0
  - Other: 60

- Spring 13:
  - Faculty/Staff/Admin: 117
  - Student: 2
  - Other: 20

- Fall 13:
  - Faculty/Staff/Admin: 68
  - Student: 3
  - Other: 46

- Spring 14:
  - Faculty/Staff/Admin: 1
  - Student: 1
  - Other: 32

With LDAP
A Few Factors

- Shortly before adding LDAP, we also added OpenURL links.
- Some librarians have been encouraging new students to make accounts at orientation to speed the request process when they actually need something.
- Fall is peak time for new accounts, so the payoff may be a few months away.
There’s Always Issues

- We stumped OCLC Support with a bug:
  - If a user skipped any of the required fields in NewAuthRegistration, hit submit, and then tried to correct their mistake, the form would clear and their registration could not be completed
    - After the initial attempt the username was added to the ILLiad database, but no other data was added to the record
    - Had to manually add user info in ILLiad so they could use their account
    - Problem may have stem from missing `<#STATUS>` line in code of page
In the End...

- Was it worth it?
  - Minus the one bug the registration process has been simplified
  - No more worry that users will forget their usernames/passwords
  - Can do preemptive registration
    - Dual benefit of early exposure for students plus avoiding the conflict between OpenURL and the need to register for ILLiad
Questions/Comments?

Contact info:
Rebecca Hyams
rhyams@sunymaritime.edu