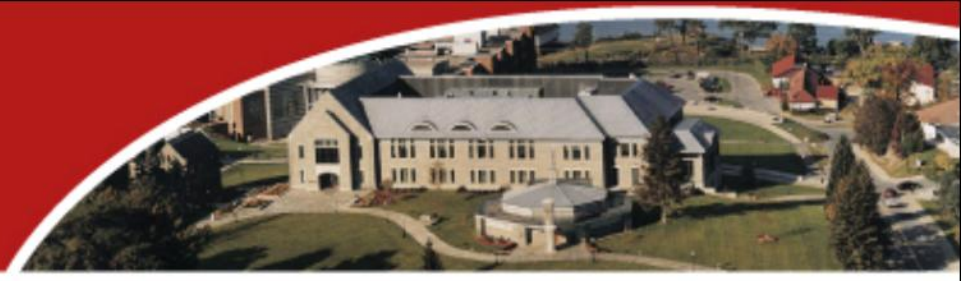
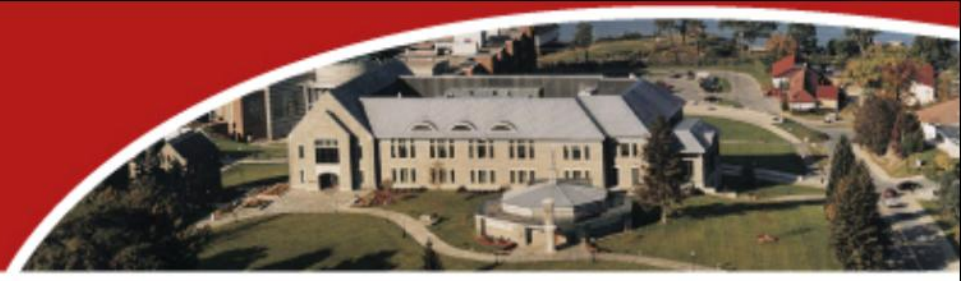
MARIST

INFORMATION TECHNOLOGY



Integrating Sakai and CAS

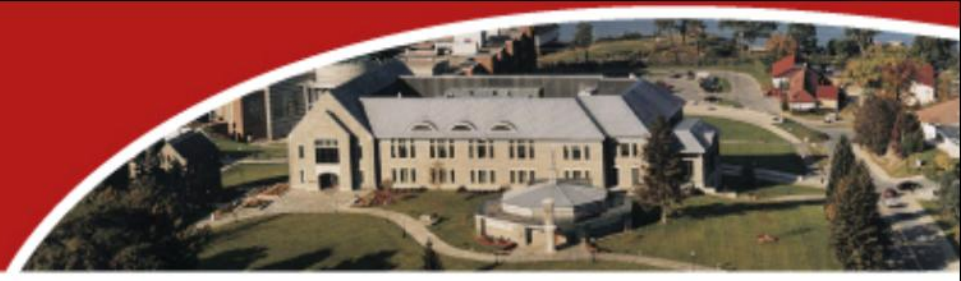
Ben Stoutenburgh
Earle Nietzel



Agenda

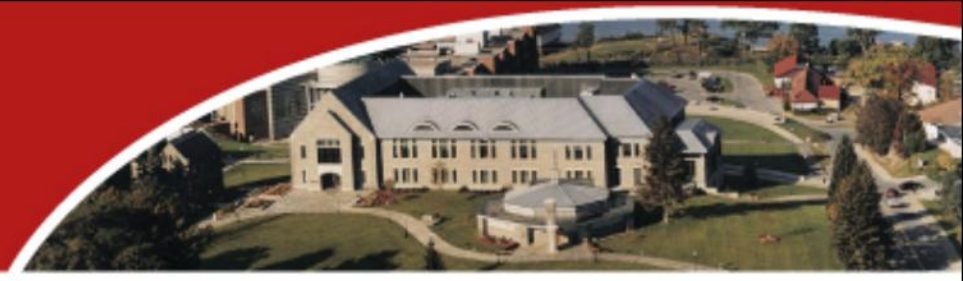
- Single Sign On, CAS w/LDAP
- Integrating SAKAI with CAS

MARIST
INFORMATION TECHNOLOGY



Single Sign On, CAS w/LDAP

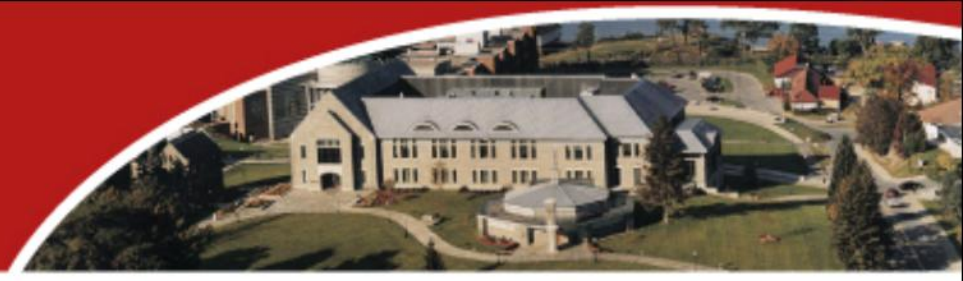
- Multiple userids and the Marist Account
- Password policies
- Potential CAS updates
- Sakai and LDAP before CAS
- Sakai and LDAP after CAS



Multiple userids and the Marist Account

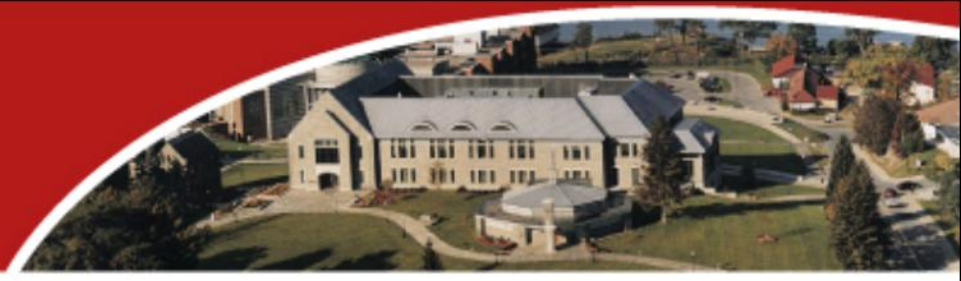
- LDAP has grown into a mess with multiple uids per person

```
uid: KBLCF
uid: STBE
uid: URBS
mail: Ben.Stoutenburgh@marist.edu
mail: benjamin.stoutenburgh@marist.edu
```



Multiple userids and the Marist Account

- Marist applications need to work with any uid or any email address
- CAS LDAP adaptor searches against uid, requires 2 changes to authenticate against anything a user might enter



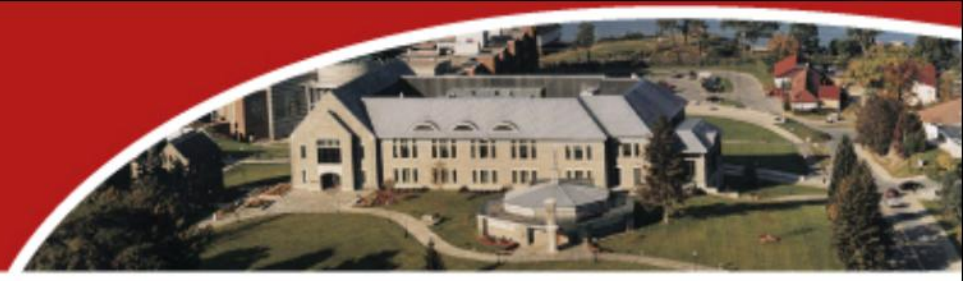
Multiple userids and the Marist Account

- webapp/WEB-INF/deployerConfigContext.xml

```
<bean
  class="edu.marist.cas.adaptors.ldap.BindLdapAuthentic
  ationHandler" >
  <property name="filter" value="(|(uid=%u)(mail=
  %u@marist.edu)(mail=%u))" />
  <property name="searchBase" value="o=marist" />
  <property name="contextSource" ref="contextSource" />
</bean>
```

- .../adaptors/ldap/util/LdapUtil.java

```
newFilter = newFilter.replaceAll(key, value);
```

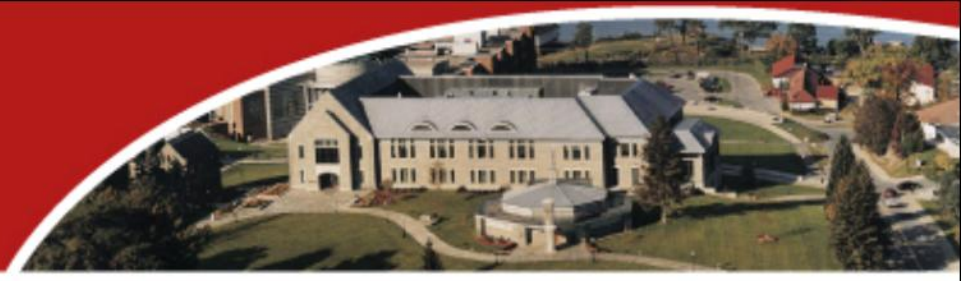


Multiple userids and the Marist Account

- Now CAS will authenticate against any possible user account, but returns what the user entered as the netid

- Marist chose to use eduPerson object class from EDUCAUSE in combination with new identification

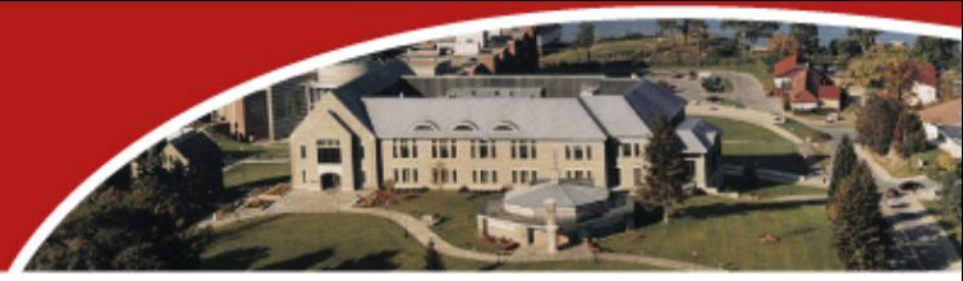
```
eduPersonPrincipalName: 10061803@marist.edu
maristCWID: 10061803
```



Multiple userids and the Marist Account

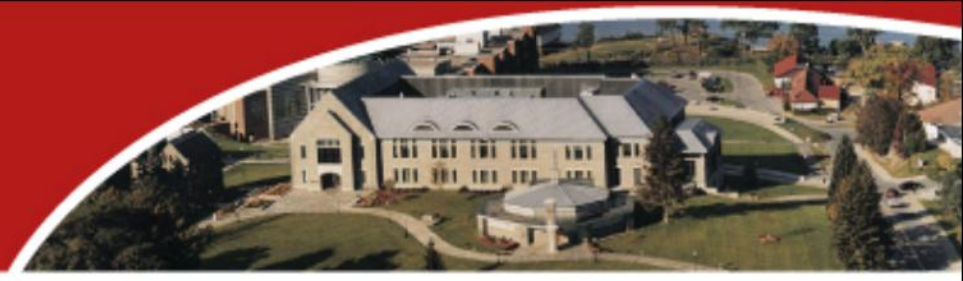
- Modified LDAP AuthenticationHandler to lookup `eduPersonPrincipalName` after authentication

- Call `credentials.setUsername` so the netid returned to applications is the `eduPersonPrincipalName`



Password policies

- Implemented a 180-day password reset policy
- If the password has expired, failed login would look just as if the user entered their password wrong
- Since users refuse to read email warnings, need to bounce them to a password reset page

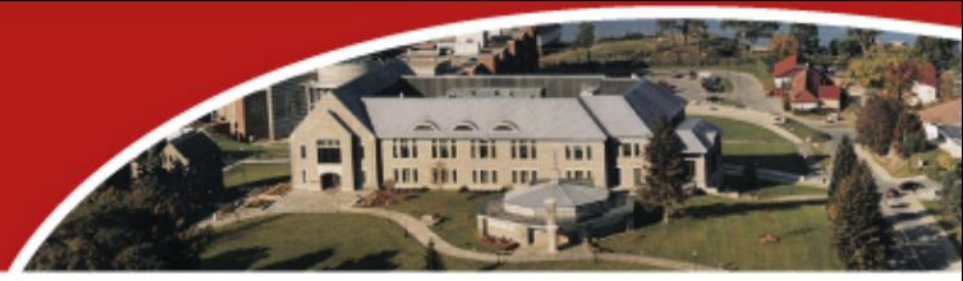


Password policies

- LDAP makes status and date of expiration available

```
maristpwwarning: -1
passwordexpiretime: 20080728010101
```

- Check `maristPWWarning` and have the Authentication Manager throw an exception
- Look forward to Expired Password Integration in CAS 4

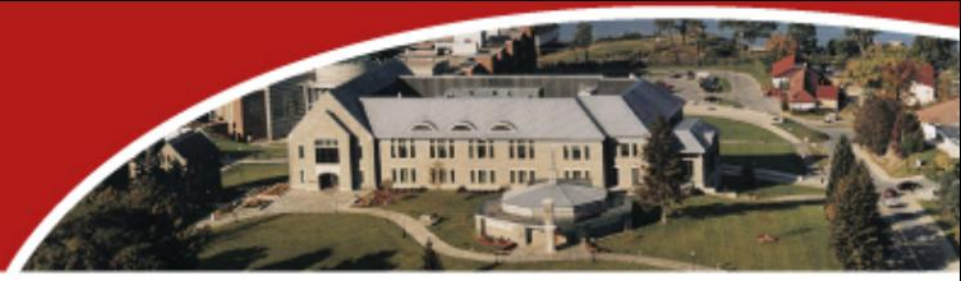


Potential CAS updates

- Upgrade 3.2.x
- Better reporting of problems
  - Missing attributes
  - Locked accounts
- Supply data in service ticket
- Cluster
- CAS-NG

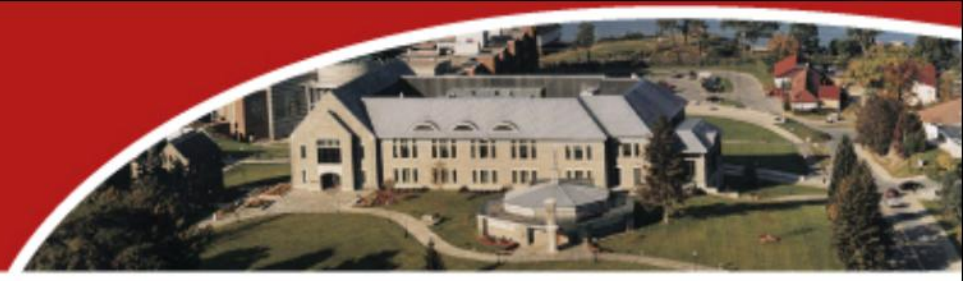
MARIST

INFORMATION TECHNOLOGY



Integrating SAKAI with CAS

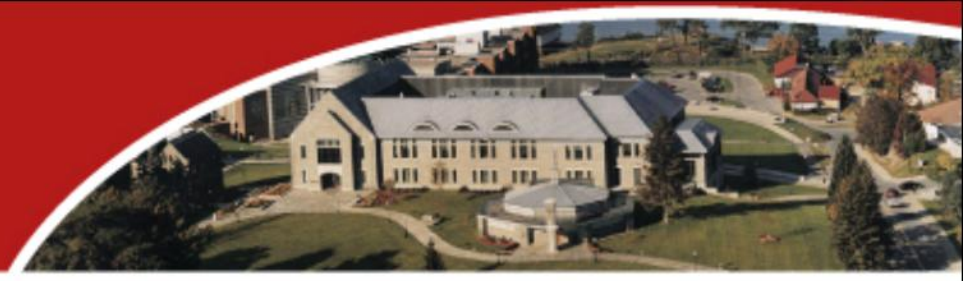
- How to get CAS to authenticate SAKAI users
- Do you need other authentication methods?
- Logging In
- LDAP Synchronizer
- Future Thoughts



How to get CAS to authenticate SAKAI users

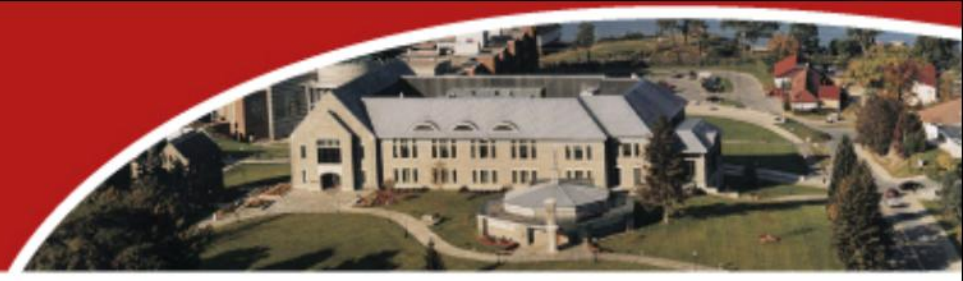
- Create a filter in the login tool
  - File `login/login-tool/tool/src/webapp/WEB-INF/web.xml`

```
<filter>
   <filter-name>CAS Filter</filter-name>
   <filter-class>edu.yale.its.tp.cas.client.filter.CASFilter</filter-class>
   <init-param>
        <param-name>edu.yale.its.tp.cas.client.filter.loginUrl</param-name>
        <param-value>https://login.marist.edu/cas/login</param-value>
   </init-param>
```



continued…

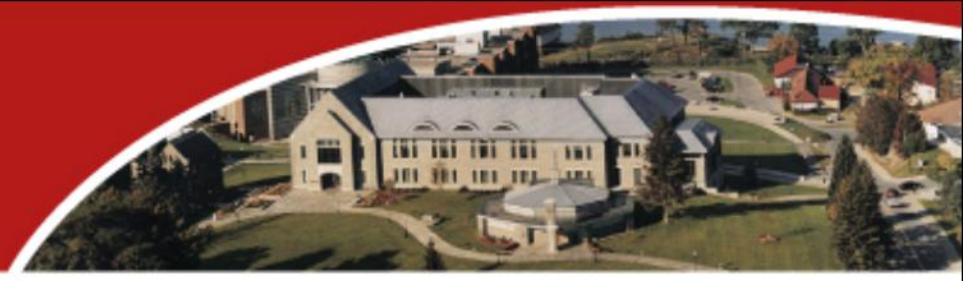
```
    <init-param>
          <param-name>edu.yale.its.tp.cas.client.filter.validateUrl</param-name>
          <param-value>https://login.marist.edu/cas/serviceValidate</param-value>
    </init-param>
    <init-param>
          <param-name>edu.yale.its.tp.cas.client.filter.serverName</param-name>
          <param-value>ilearn.marist.edu</param-value>
     </init-param>
     <init-param>
          <param-name>edu.yale.its.tp.cas.client.filter.wrapRequest</param-name>
          <param-value>true</param-value>
     </init-param>
</filter>
```



continued…

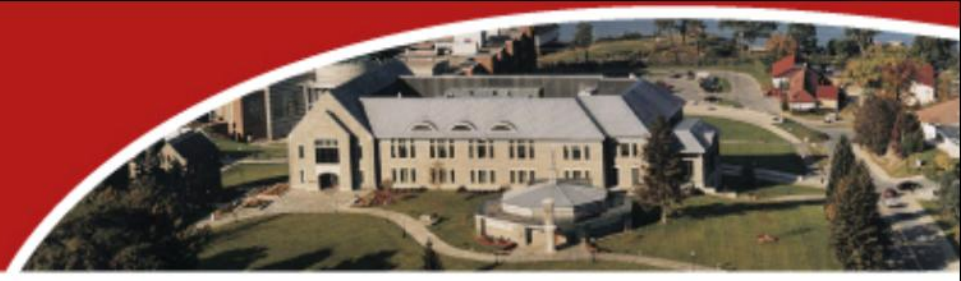
- Use a Filter on the container for all context urls
  - File `login/login-tool/tool/src/webapp/WEB-INF/web.xml`

```
<filter-mapping>
    <filter-name>CAS Filter</filter-name>
    <url-pattern>/container</url-pattern>
</filter-mapping>
```



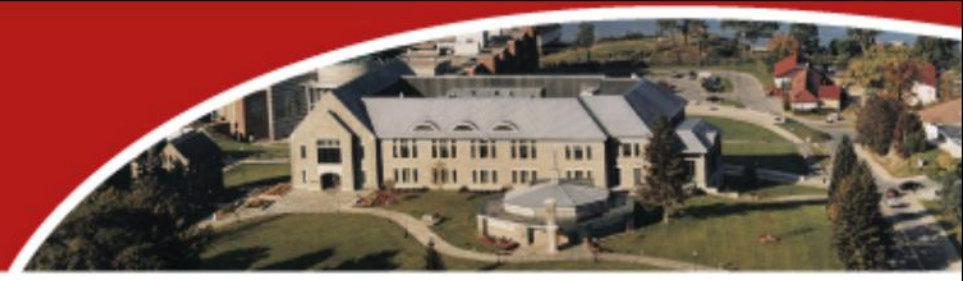
Do you need other authentication methods?

- Disable/Enable other authentication methods
  - File `providers/component/src/webapp/WEB-INF/components.xml`
    - Default local (org.sakaiproject.provider.user.SampleUserDirectoryProvider)
    - LDAP (edu.amc.sakai.user.JLDAPDirectoryProvider)
    - Kerberos (org.sakaiproject.component.kerberos.user.KerberosUserDirectoryProvider)



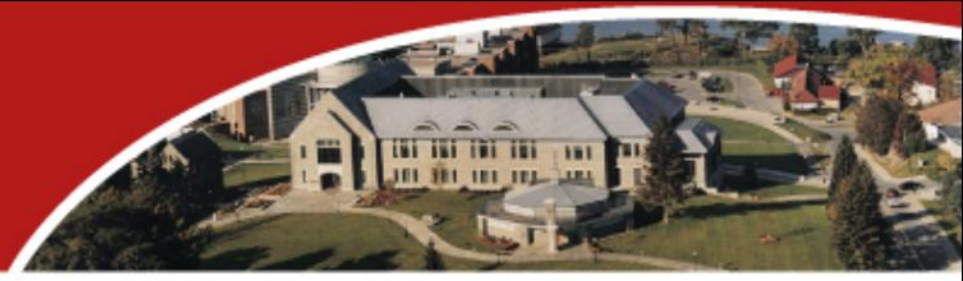
Logging In

- Use the standard sakai login url
  - https://ilearn.marist.edu/osp-portal/login
- Extreme login
  - https://ilearn.marist.edu/osp-portal/xlogin



Getting data from LDAP

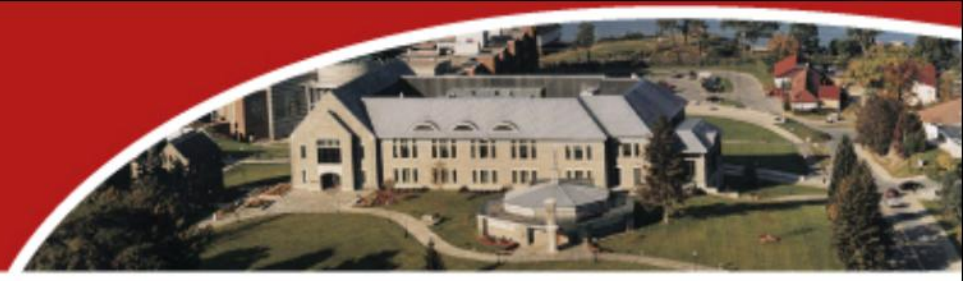
- Real time updates, needed?
- Yes, Implemented an LDAP data Synchronizer
  - This is required since we lost our ability to receive updates via LDAP when we switched to using CAS from JLDAP user provider.
- No, Can use nightly feeds.



LDAPSynchronizer

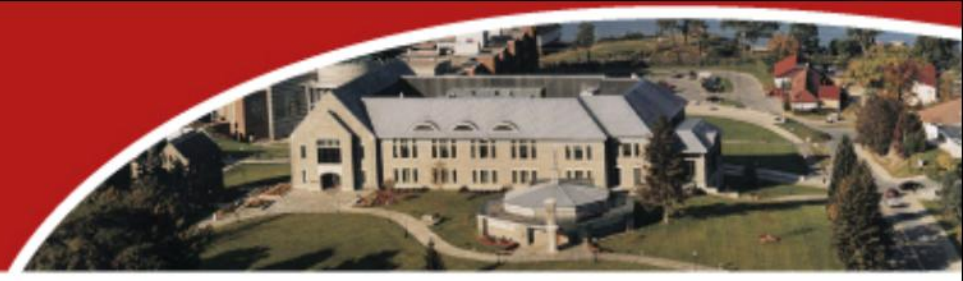
- Added class LDAPSynchronizer
  - Public method public void updateUserData(final String user)
  - Updates are performed using the sakai UserEdit api
    - `ue = UserDirectoryService.editUser(UserDirectoryService.getUserId(user));`
    - Users must have sakai realm permission to update their data (user.upd.own)
- Add LDAPSynchronizer to ContainerLogin
  - File login/login-tool/tool/src/java/org/sakaiproject/login/tool/ContainerLogin.java

```
// login the user
if (UsageSessionService.login(a, req))
{
    // update user data from ldap
    LDAPSynchronizer synchronizer = new LDAPSynchronizer();
    synchronizer.updateUserData(remoteUser.trim());
 .... }
```



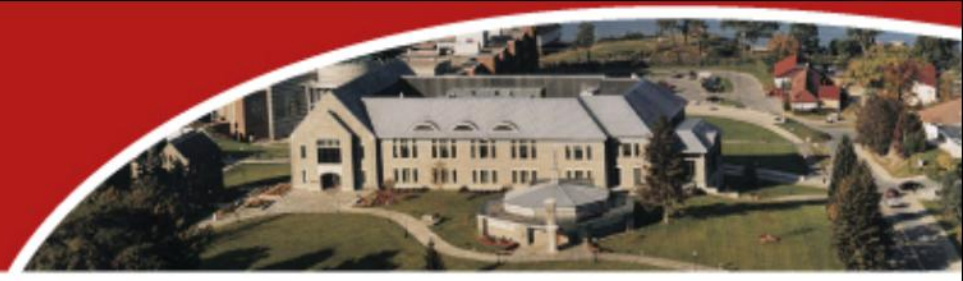
Example Log

```
INFO: edu.marist.login.LDAPSynchronizer@736f220.updateUserData(): UserEdit [Suresh|Chacko|suresh.chacko1@marist.edu] (2008-04-
INFO: edu.marist.login.LDAPSynchronizer@1df62975.updateUserData(): UserEdit [Jacklyn|LeBlanc|jacklyn.leblanc@marist.edu] (2008
INFO: edu.marist.login.LDAPSynchronizer@4b740bac.updateUserData(): UserEdit [Mary|Marist|mary.marist@marist.edu] (2008-04-29 1
INFO: edu.marist.login.LDAPSynchronizer@42ddf0d3.updateUserData(): UserEdit [Maureen|Boucher|maureen.boucher@marist.edu] (2008
INFO: edu.marist.login.LDAPSynchronizer@d842c3f.updateUserData(): UserEdit [Hannah|Haslam|hannah.haslam1@marist.edu] (2008-04-
INFO: edu.marist.login.LDAPSynchronizer@4c81dd58.updateUserData(): UserEdit [Carmelo|Ortiz|carmelo.ortiz@marist.edu] (2008-04-
INFO: edu.marist.login.LDAPSynchronizer@3f398ed2.updateUserData(): UserEdit [Jay|Brennerman|brennrj@gmail.com] (2008-04-29 16:
INFO: edu.marist.login.LDAPSynchronizer@66572588.updateUserData(): UserEdit [Brittany|Bobb|brittany.bobb1@marist.edu] (2008-04
INFO: edu.marist.login.LDAPSynchronizer@5c8f1186.updateUserData(): UserEdit [Sandeep|Pothuganti|sandeep.pothuganti1@marist.edu
nizer)
INFO: edu.marist.login.LDAPSynchronizer@44d4455a.updateUserData(): UserEdit [Joshua|Rickards|joshua.rickards1@marist.edu] (200
INFO: edu.marist.login.LDAPSynchronizer@6aca0083.updateUserData(): UserEdit [Kyle|Lukas|kyle.lukas1@marist.edu] (2008-04-29 16
INFO: edu.marist.login.LDAPSynchronizer@39d81561.updateUserData(): UserEdit [Stuart|Homcy|stuart.homcy1@marist.edu] (2008-04-2
INFO: edu.marist.login.LDAPSynchronizer@72cd69d5.updateUserData(): UserEdit [Soraya|Peralta|soraya.peralta1@marist.edu] (2008-
INFO: edu.marist.login.LDAPSynchronizer@49fe6f1a.updateUserData(): UserEdit [Kevin|Keating|kevin.keating1@marist.edu] (2008-04
INFO: edu.marist.login.LDAPSynchronizer@12af4d52.updateUserData(): UserEdit [James|Campbell|james.campbell1@marist.edu] (2008-
INFO: edu.marist.login.LDAPSynchronizer@71b94d77.updateUserData(): UserEdit [David|Pulikowski|david.pulikowski1@marist.edu] (2
r)
INFO: edu.marist.login.LDAPSynchronizer@3b884f7e.updateUserData(): UserEdit [Kimberly|White|kimberly.white1@marist.edu] (2008-
INFO: edu.marist.login.LDAPSynchronizer@7fe09bf9.updateUserData(): UserEdit [Ashley|Blanding|ashley.blanding1@marist.edu] (200
INFO: edu.marist.login.LDAPSynchronizer@70c21df9.updateUserData(): UserEdit [Arabia|Jennings|arabia.jennings1@marist.edu] (200
INFO: edu.marist.login.LDAPSynchronizer@32b70f32.updateUserData(): UserEdit [Marcy|Jordan|marcy.jordan@marist.edu] (2008-04-29
INFO: edu.marist.login.LDAPSynchronizer@402ff78d.updateUserData(): UserEdit [Rob|O'Neill|rob.oneil1@marist.edu] (2008-04-29 16
INFO: edu.marist.login.LDAPSynchronizer@33bc7e98.updateUserData(): UserEdit [Hazel|Christian|hazel.christin1@marist.edu] (2008
INFO: edu.marist.login.LDAPSynchronizer@65984394.updateUserData(): UserEdit [David|Mamorella|david.mamorella@marist.edu] (2008
INFO: edu.marist.login.LDAPSynchronizer@76cdcef4.updateUserData(): UserEdit [Gabriela|Mogrovejo|gabriela.mogrovejo@marist.edu]
```



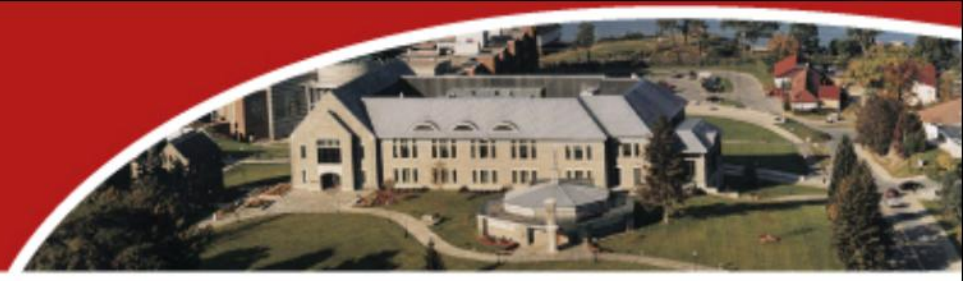
Future Thoughts

- CAS needs to pass role information in order to use GroupProvider.
- Possibly make LDAPSynchronizer a singleton to improve performance (must consider concurrency issues)



Resources

- eduPerson Object Class
  - http://www.educause.edu/content.asp?PAGE_ID=949&bhcp=1
- Expired Password Integration
  - http://ja-sig.org/wiki/display/CAS/Expired+Password+Integration
- Clustering CAS
  - http://www.ja-sig.org/wiki/display/CASUM/Clustering+CAS
- CAS 4 Roadmap
  - http://www.ja-sig.org/wiki/display/CAS/CAS+4+Roadmap
- Yale CAS-NG Presentation
  - http://www.yale.edu/tp/CASNG.ppt
- Sakai CAS Filter
  - Jen Bourey, Yale



Questions?