



User Information & Authentication – Multiple LDAP Sources

Confidential & Proprietary

Contents

Contents	2
1.0 Introduction.....	3
1.1 About the Multiple LDAP Sources.....	3
1.2 Additional Notes.....	3
2.0 Configuration	4
2.1 Configuring Multiple LDAP Sources	4
2.1.1 Disable use of old ldap configuration	4
2.1.2 Configure Multiple LDAP Authentication Sources.....	4
2.1.3 Configure Academus to Authenticate against the LDAP Sources	4
2.1.4 Configure Academus to Authorize against the LDAP Sources	5
2.1.5 Restart Academus.....	6
2.1.6 Troubleshooting.....	6

1.0 Introduction

1.1 About the Multiple LDAP Sources

Academus by default is configured to authorize and authenticate against its own database. In addition, Academus can be configured to authenticate and authorize against one or many LDAP sources. This document will explain the steps necessary to configure Academus to use multiple LDAP sources.

1.2 Additional Notes

Academus can only be configured to use multiple LDAP (OpenLDAP, SunONE Directory) sources and not multiple Microsoft Active Directory sources.

2.0 Configuration

2.1 Configuring Multiple LDAP Sources

The following steps can be used to configure multiple LDAP sources:

****Best practice: make a backup of the file before editing.**

2.1.1 Disable use of old ldap configuration

In `<ACADEMUS_UNICON_INSTALL_ROOT>/unicon/Academus/portal-tomcat-a/webapps/portal/WEB-INF/classes/properties`

rename `ldap.properties` to `ldap.properties_donotuse`

2.1.2 Configure Multiple LDAP Authentication Sources

In the same directory, open `ldap.xml` and configure it to look something like:

```
<ldapConnections>
  <connection default="true">
    <name>ldap1</name>
    <host> ldap1.domain.net </host>
    <port>389</port>
    <baseDN>o=DevLDS,dc=unicon,dc=net</baseDN>
    <managerDN>uid=admin,ou=administrators,ou=topologymanagement,
      o=netscaperoot</managerDN>
    <managerPW>passwd</managerPW>
    <uidAttribute>uid</uidAttribute>
  </connection>

  <connection>
    <name>ldap2</name>
    <host> ldap2.domain.net </host>
    <port>389</port>
    <baseDN>dc=letnet,dc=net</baseDN>
    <managerDN>cn=PortalCreate,ou=DBQueryAccounts,ou=PortalAccounts,
      dc=letnet,dc=net</managerDN>
    <managerPW>passwd</managerPW>
    <uidAttribute>uid</uidAttribute>
  </connection>
</ldapConnections>
```

where `ldap1.domain.net` is the first LDAP server and `ldap2.domain.net` is the second LDAP server.

2.1.3 Configure Academus to Authenticate against the LDAP Sources

Open `security.properties` in the same directory and configure it to look

something like:

```
# security.properties
root=org.jasig.portal.security.provider.UnionSecurityContextFactory

root.ldapcache_first=org.jasig.portal.security.provider.CacheLdapSecurityContextFactory
securityContextProperty.root.ldapcache_first.connection=ldap1

root.ldapcache_second=org.jasig.portal.security.provider.CacheLdapSecurityContextFactory
securityContextProperty.root.ldapcache_second.connection=ldap2

root.aasimplecache=net.unicon.portal.security.CacheSimpleSecurityContextFactory

principalToken.root=userName
credentialToken.root=password

authorizationProvider=org.jasig.portal.security.provider.AuthorizationServiceFactoryImpl
# eof: security.properties

** Notice that the
securityContextProperty.root.ldapcache_first.connection=ldap1 points at the
<name>ldap1</name> configured in ldap.xml.
```

2.1.4 Configure Academus to Authorize against the LDAP Sources

Edit the PersonDirs.xml config file located in the same directory and add one <PersonDirInfo> block for each LDAP authentication source. Example below, change configuration to suit your environment:

```
<PersonDirInfo>

    <driver></driver>
    <url>ldap://ldap1.unicon.net:389</url>
    <logonid>uid=admin,ou=administrators,ou=topologymanagement,o=netscaperoot</logonid>
    <logonpassword>pass</logonpassword>
    <uidquery>(uid={0})</uidquery>
    <searchquery>(~MATCH_ALL_OP~(uid={0}~WILDCARD_o~)(givenName={1}~WILDCARD_1~)(sn={2}~WILDCARD_2~)(mail={3}~WILDCARD_3~))</searchquery>
    <searchquery2>(&~SEARCH_QUERY~(|~USER_FILTER~))</searchquery2>
    <unionOperator>|</unionOperator>
    <intersectionOperator>&&</intersectionOperator>
    <uidSelect>(uid={~ARG~})</uidSelect>
    <wildcard>*</wildcard>
    <>trueClause></trueClause>
    <usercontext>o=DevLDS,dc=unicon,dc=net</usercontext>

    <attributes>

        <attribute>
            <name>uid</name>
```

```
        <alias>username</alias>
</attribute>

<attribute>
    <name>sn</name>
    <alias>lastName</alias>
</attribute>

<attribute>
    <name>mail</name>
    <alias>mail</alias>
</attribute>

<attribute>
    <name>givenName</name>
    <alias>firstName</alias>
</attribute>

<attribute>
    <name>cn</name>
    <alias>displayName</alias>
</attribute>

<attribute>
    <name>destinationIndicator</name>
    <alias>uPortalTemplateUserName</alias>
</attribute>

<attribute>
    <name>uid</name>
    <alias>user.login.id</alias>
</attribute>

<attribute>
    <name>uid</name>
    <alias>user.login.password</alias>
</attribute>

</attributes>
```

```
</PersonDirInfo>
```

2.1.5 Restart Academus

You will need to restart Academus for the changes to take effect.

2.1.6 Troubleshooting

Tips to help during troubleshooting:

- 1) Most problems encountered when configuring multiple LDAP sources are caused by typographic errors when editing the configuration files. Make sure to double check all your configurations especially check to make sure the XML are all well-formed.

2) Make sure the LDAP sources are accessible from the Academus server.