

# LDAP



For Version 7.4.4.\*

There is a bug with the openJDK 1.8 which is installed with 7.4.4.\* . The patch for this is contained in the link below.

[Follow Instructions in the README\\_7.4.4.x\\_patch.txt](#)

## 1. Configuring LUNA

### Introduction

The configuration for LUNA is done in the luna-security.xml (7+) file located in the following place

- <LUNA Install Directory>/tomcat/luna\_apps/luna.war/WEB-INF



### For 7.4.4.0+ and Active Directory LDAP

For clients who use Active Directory, they will have to set a flag to "1" in luna-security.xml:

```
<property name="trustStorePath" value=""/>
<property name="activeDirectory" value="1"/>
```

In the section that follows, only sections that are pertinent to the configuration are shown.

### Active Directory LDAP example

```
<!--
The properties of ldapAuthenticationSearch need to be specified in the
same way as Insight User Manager 6.x. See the InsightUserServer.dat file.
Example for Active Directory
-->
<bean id="ldapAuthenticationSearch" class="com.luna.insight.client.security.ldap.LDAPAuthenticationSearchImpl">
  <property name="ldapUserAttribute" value="insightUser" />
  <property name="ldapURL" value="ldap://ldap.luna.edu" />
  <property name="baseDN" value="dc=luna,dc=edu" />
  <property name="loginSSL" value="0" />
  <property name="trustStorePath" value="" />
<!--
Example for LDAPS:
<property name="ldapUserAttribute" value="insightUser"/>
<property name="ldapURL" value="ldaps://ldap.luna.edu"/>
<property name="baseDN" value="dc=luna,dc=edu"/>
<property name="loginSSL" value="1"/>
<property name="trustStorePath" value="C:/myStoreFile">
-->
</bean>
```

Assigning credentials by pattern matching in user's DN for Active Directory LDAP

The ldapSearchFilters and credentialsConditions properties work in the same way as ldapAuthenticationSearch.

In the following example, pattern matching is applied to the DN returned after applying the search filter (sAMAccountName=(0)), where sAMAccountName is the login name for every user.

This is done in the order from top to bottom, and when there is a match, the corresponding credential under "mappedValues" is assigned and the rest of the conditions are ignored. If there is no match, it is assigned a default credential ID set above.

Regular expression can be used in conditions.

Syntax for "conditions":  
<attribute value>=<pattern>

For example, in condition "distinguishedName=CN=admin,OU=Art History\*", we are trying to match the <attribute value> "distinguishedName" against the <pattern> "CN=admin,OU=Art History"

Example DN's and expected results from the credential mappings set below:

**admin will get credential 4**

distinguishedName: CN=admin,OU=Art History Department,OU=College of Letters and Science,DC=luna,DC=edu

**jsmith will get credential 3**

distinguishedName: CN=John Smith,OU=Art History Department,OU=College of Letters and Science,DC=luna,DC=edu

**janderson will get credential 3**

distinguishedName: CN=Jenny Anderson,OU=Art History Department,OU=College of Letters and Science,DC=luna,DC=edu

**jdoe will get credential 3**

distinguishedName: CN=Jane Doe,OU=English Department,OU=College of Letters and Science,DC=luna,DC=edu

**jemerson will get credential 2**

distinguishedName: CN=Jill Emerson,OU=French Department,OU=College of Letters and Science,DC=luna,DC=edu

**NOTE:**

For Windows Active Directory, it should be enough to specify only 1 entry, (sAMAccountName={0}) in ldapSearchFilters. Unlike OpenLDAP, specifying complicated or wrong search condition for Active Directory results in time-out and considerable system delay. The syntax of ldapSearchFilter\_x is based on RFC 2254. See: <http://www.ietf.org/rfc/rfc2254.txt>

```
<!-- Example for Active Directory
-->
<bean id="ldapCredentialsMap" class="com.lunaimaging.insight.core.domain.authenticators.ldap.LdapCredentialsMap"
>
  <property name="ldapSearchFilters">
    <list>
      <value>(sAMAccountName={0})</value>
    </list>
  </property>
  <property name="ldapSearchAttributes">
    <list>
      <value>insightUser</value>
    </list>
  </property>
  <property name="conditions">
    <list>
      <value>distinguishedName=English Department</value>
      <value>distinguishedName=CN=admin,OU=Art History*</value>
      <value>distinguishedName=Art History*</value>
      <value>distinguishedName=College of Letters and Science</value>
    </list>
  </property>
  <property name="mappedValues">
    <list>
      <value>3</value>
      <value>4</value>
      <value>3</value>
      <value>2</value>
    </list>
  </property>
</bean>
```

## Open LDAP example

```

<bean id="authenticatorSearchLDAP" class="com.lunaimaging.insight.core.domain.authenticators.
LdapSearchAuthenticator">
  <property name="defaultCredentialsId" value="2" />
  <property name="ldapAuthenticationSearch">
    <ref bean="ldapAuthenticationSearch" />
  </property>
  <property name="ldapSearchMap">
    <ref bean="ldapCredentialsMap" />
  </property>
</bean>
<!--
The properties of ldapAuthenticationSearch need to be specified in the
same way as Insight User Manager 6.x. See the InsightUserServer.dat file.
Example for OpenLDAP:
-->
<bean id="ldapAuthenticationSearch" class="com.luna.insight.client.security.ldap.LDAPAuthenticationSearchImpl">
  <property name="ldapUserAttribute" value="insightUser" />
  <property name="ldapURL" value="ldap://ldap.luna.edu" />
  <property name="baseDN" value="dc=luna,dc=edu" />
  <property name="loginSSL" value="0" />
  <property name="trustStorePath" value="" />
  <!--
Example for LDAPS:
<property name="ldapUserAttribute" value="insightUser"/>
<property name="ldapURL" value="ldaps://ldap.luna.edu"/>
<property name="baseDN" value="dc=luna,dc=edu"/>
<property name="loginSSL" value="1"/>
<property name="trustStorePath" value="/usr/local/insight/LunaImaging/myStoreFile">
-->
  <property name="ldapSearchFilters">
    <list>
      <value>(uid={0})</value>
    </list>
  </property>
  <property name="ldapSearchAttributes">
    <list>
      <value>insightUser</value>
    </list>
  </property>
  <property name="ldapSecurityPrincipal" value="{0}" />
  <property name="ldapSecurityPrincipalAttributes" value="dn" />
</bean>

```

#### Assigning credentials by pattern matching in user's DN for OpenLDAP

The `ldapSearchFilters` and `credentialsConditions` properties work in the same way as `LdapAuthenticationSearch`.

OpenLDAP:

In the following example, pattern matching is applied to the DN returned after applying the search filter (`uid=(0)`), where `uid` is the login name for every user.

This is done in the order from top to bottom, and when there is a match, the corresponding credential under `"mappedValues"` is assigned and the rest of the conditions are ignored. If there is no match, it is assigned a default credential ID set above.

Regular expression can be used in conditions.

Syntax for "conditions":

```
<attribute value>=<pattern>
```

for example, in `"dn=uid=admin,ou=Art History"`,

we are trying to match the `<attribute value>` `"dn"` against the `<pattern>` `"uid=admin,ou=Art History"`

Example DN's and expected results from the credential mappings:

**admin will get credential 4**

```
dn: uid=admin,ou=Art History Department,ou=College of Letters and Science,dc=luna,dc=edu
```

**jsmith will get credential 3**

dn: uid=jsmith,ou=Art History Department,ou=College of Letters and Science,dc=luna,dc=edu

**janderson will get credential 3**

dn: uid=janderson,ou=Art History Department,ou=College of Letters and Science,dc=luna,dc=edu

**jdoe will get credential 3**

dn: uid=jdoe,ou=English Department,ou=College of Letters and Science,dc=luna,dc=edu

**jemerson will get credential 2**

dn: uid=jemerson,ou=French Department,ou=College of Letters and Science,dc=luna,dc=edu

The syntax of LdapSearchFilter\_x is based on RFC 2254. See: <http://www.ietf.org/rfc/rfc2254.txt>

```
<bean id="ldapCredentialsMap" class="com.lunaimaging.insight.core.domain.authenticators.ldap.LdapCredentialsMap"
>
  <property name="ldapSearchFilters">
    <list>
      <value>(uid={0})</value>
    </list>
  </property>
  <property name="ldapSearchAttributes">
    <list>
      <value>insightUser</value>
    </list>
  </property>
  <property name="conditions">
    <list>
      <value>dn=English Department</value>
      <value>dn=uid=admin,ou=Art History*</value>
      <value>dn=Art History*</value>
      <value>dn=College of Letters and Science</value>
    </list>
  </property>
  <property name="mappedValues">
    <list>
      <value>3</value>
      <value>4</value>
      <value>3</value>
      <value>2</value>
    </list>
  </property>
</bean>
```