Access Control[1]

- **I** Base installation:
  - **A.** Access control is enabled by default in the LMM settings.xml file, and should be left that way.
  - **B.** When the LMS was installed an administrative user was defined. For the VMWARE image that user is lmsadmin.
  - **C.** For security and administrative purposes this is the only user who can manage Access Controlled features.
  - **D.** To give other users access to the two catalog folders and resources, you'll need to log in to the LMM as the admin user, lmsadmin/password, and make the changes outlined below depending on your installation needs..
    - **1.** In a Beta/Pilot environment you will likely want to change the ACL from "LdapId=lmsadmin" to "LdapId=*". This will give all users access to the Location Resources.
    - **2.** In a true deployment you would likely want to leave this administrative user in place and create additional Access Controls to manage catalogs and resources.
- **II** **Beta/Pilot environment**
  - **A.** Change the ACL from "LdapId=lmsadmin" to "LdapId=*" in three default locations
  - **B.** This has already been done for you in the VMWARE image provided at the LMS-Enablement Session, but you need to be aware of these steps for other installations that you may conduct.
  - **C.** **Log on to the LMM.**
    - **1.** Launch the LMS
      - **a.** http://lms.mindspan.com/lms-lmm.
    - **2.** Logon to the system as an administrator
      - **a.** Click the Log In link in the upper right corner of the browser.
      - **b.** Enter "**lmsadmin**" as the username
      - **c.** Enter "**password**" as the password.
      - **d.** Click the **Log In** action button on that form.
    - **3.** ALL Views are available to a System Administrator, but would not be for a Course Administrator in a true environment. In the interest of time, we have included both roles here because they are so intertwined.
  - **D.** **Click on Settings Tab**
    - **1.** In the **Deployment** section
      - **a.** Click LMM Server link
        - 1) Click General Settings link.
          - a) Click on the **Location Access Control** sub-tab to specify the default access control settings for location.
          - b) Click on the **Edit** link in the far right corner of the table.
            - i) Leave Match Type as **Attribute**
            - ii) Set Match String to "**UserId=***"
            - iii) Click **Save**

---

[1] If you put an invalid Match String for the ACL then you may put system into an unrecoverable state. Be very careful in the past this has caused us to have to rebuild the databases.

E. **Click on Course Catalog Tab**
  1. In the **Offerings Catalog** section
    a. Click on the Manage Offerings Catalog link
      1) Click on The Offerings Catalog folder Icon 📁
        a) Click the Access Control tab
        b) Click on the **Edit** link in the far right corner of the table.
          i) Leave Match Type as **Attribute**
          ii) Set Match String to “**UserId=***”
          iii) Click **Save**

F. **Click on Course Catalog Tab**
  1. In the **Offerings Catalog** section
    a. Click on the Manage Offerings Catalog link
      1) Click on The Offerings Catalog folder Icon 📁
        a) Click the Access Control tab
        b) Click on the **Edit** link in the far right corner of the table.
          i) Leave Match Type as **Attribute**
          ii) Set Match String to “**UserId=***”
          iii) Click **Save**

III Configurations that should be made only in a true deployment or upon customer request.

A. Log in to the LMS system as lmsadmin/password

B. Go to the **Course Catalog** tab
  1. Click on the Manage Offerings Catalog link from the Course Catalog menu.
  2. There are a few options on this screen
    a. **Search** by Keyword
    b. Advanced Search
    c. Offerings Catalog link.
  3. Modify the ACL for the Masters Catalog by clicking the Folder Icon. 📁
    a. You are presented with two tabs
      1) Folder Details
      2) Access Controls
    b. On the first tab, **Folder Details**, notice that you have the following command buttons:
      1) **Edit**
      2) **Delete**
      3) **Move Folder**
      4) **Copy Folder**
    c. With the exception of Edit. You should never attempt to Delete, Move, or Copy the Top most node of either Catalog.

C. First we want to ensure that all students can open to the first level (immediate children of the Offerings Catalog).
  1. Click on the **Access Control** tab
    a. Notice that you have system defined Access Control based on the parameters entered on install.
    b. In the VMWARE image it should read “LdapId=lmsadmin”.
    c. Click **Add**

2. A popup window launches with four fields.
  - **a.** Level
    - 1) **Read** – users with this permission can view contents of folders and enroll in courses
    - 2) **Write** – users with this permission can:
      - a) View content
      - b) Add/Remove content.
    - 3) **Manage** – users with this permission can:
      - a) View content
      - b) Add/Remove content
      - c) Create / Copy / Move / Delete the folder
      - d) Modify Access Control permissions
  - **b.** Scope
    - 1) **All Children** – Permissions associated with this ACL carry to the all subsequent levels
    - 2) **Immediate Children** - Permissions associated with this ACL carry to the next level only.
  - **c.** Match Type
    - a) **User** – specific to a user defined in the LDAP
      - i) **Match String Examples**:
      - ii) cn=Nana Strose,ou=Groups,o=ibm
      - iii) Nana Strose/People/ibm
      - iv) */Springfield/Acme
      - v) *,ou=Springfield,o=Acme
    - b) **Group** – specific to a group defined in the LDAP
      - i) **Match String Examples**:
      - ii) cn=HarrisAdministrators,ou=Groups,o=ibm
      - iii) HarrisAdministrators/Groups/IBM
    - c) **Attribute** – specific to a logical statement
      - i) **Match String Examples**:
      - ii) LdapId=georgep
      - iii) o=ibm
  - **d.** Accept the default for Level – "**Read**"
  - **e.** Select "**Immediate Children**" for the Scope
  - **f.** Select "User" from the Match Type dropdown list
  - **g.** Enter **"*"** in the Match String field. This will allow all users to open the Course Catalog and read it's children.
  - **h.** Click **Save** to complete the process and return to the previous screen.
  - **i.** Notice that a new access control has been added and you now have a new link Add Entry. This link allows you to specify additional ACL's to this Read level

D. Second we want to designate a group of users who can write to the first level (immediate children of the Offerings Catalog).
  - **1.** Click on the **Access Control** tab
    - **a.** Notice that you have system defined Access Control based on the parameters entered on install.
    - **b.** In the VMWARE image it should read "LdapId=lmsadmin".
    - **c.** Click **Add**

    2. A popup window launches with four fields.
        a. Change the default for Level – "**Write**"
        b. Select "**Immediate Children**" for the Scope
        c. Select "**Group**" from the Match Type dropdown list
        d. Enter **"LMS Team/Groups/ibm"** in the Match String field. This will allow all users on the LMS Team to write to the offerings catalog
        e. Click **Save** to complete the process and return to the previous screen.
        f. Notice that a new access control has been added and you now have a new link Add Entry. This link allows you to specify additional ACL's to this Read level

E. Lastly, we want to designate that only one user has access to Manage All folders

    1. Click on the Edit link in the far right corner of the default access control.
        a. A popup window launches with only two fields
        b. Leave Match Type as "**Attribute**"
        c. Change Match String to "**LdapId=lmsadmin**"
        d. <u>Before</u> you click **Save** Check your syntax… check it again, and verify your last check. (Changing the manage level for all children to an invalid user will lock you out of the course catalog management function.)
        e. <u>Click **Save** only after you have validated it.</u>
        f. Notice that a new access control has match string has been updated.

IV Log out.

A. Confirm you settings.

B. If you find that you can not access the immediate children of the offerings catalog then a mistake has been made in the Access Control settings.

    1. Log on as lmsadmin to correct the issue.

C. Challenge set Access Controls for the sub folders.

V Correcting ACL Matching String Errors

A. If a mistake is made and you are locked out of an access controlled feature.

    1. Open LMM database,
        a. Connect to the ACL table and look for the applicable entry.
        b. Depending on changes you have made you will want to find the appropriate record to modify:
            1) "MAST" which maps to the Masters Catalog
            2) "OFFR" which maps to the Offerings Catalog
            3) "ROOM" which maps to the Resources ACL
        c. Identify key, or "OID" associated with the record and write it down.
    2. Connect to the "ACLCriteria" table
        a. Find the match the OID you wrote down with the key under acl_oid in this table.
        b. This identifies the entry you will want to change

B. Launch the DB2 command window.

C. Enter the following commands
  1. Db2 connects to the LMM with user db2admin/password
  2. db2 update aclcriteria set match_string='LdapId=*' where oid='99000000000000300ACRT' (this key must match the oid identified earlier.)
  3. Db2 terminate
D. Launch the LMS to determine if your changes were successful.

VI Mapping of ACL names and LDAP fields.

Name to use in ACL	Name in LDAP
BusinessCategory	businessCategory
CommonName	cn
City	l (L)
Country	c
DepartmentNumber	departmentNumber
EmployeeType	employeeType
LdapId	uid
Manager	manager
Organization	o
OrganizationUnit	ou
State	st
Title	title
Userid	uid

The mapping above is based on the data contained in your Settings.xml file. Here is a sample from another installation. If you examine the code section below you will see how the string values used in the ACL settings for the LMS are matched to the LDAP attribute.

```
<objectclass name="inetOrgPerson">
        <mapping name="Address_1" ldapAttribute="postalAddress"/>
        <mapping name="Address_2" ldapAttribute="postalAddress"/>
        <mapping name="BusinessCategory" ldapAttribute="businessCategory"/>
        <mapping name="City" ldapAttribute="l"/>
        <mapping name="CommonName" ldapAttribute="cn"/>
        <mapping name="Country" ldapAttribute="c"/>
        <mapping name="DepartmentNumber" ldapAttribute="departmentNumber"/>
        <mapping name="Description" ldapAttribute="description"/>
        <mapping name="DisplayName" ldapAttribute="displayName"/>
        <mapping name="EmailAddress" ldapAttribute="mail"/>
        <mapping name="EmployeeNumber" ldapAttribute="employeeNumber"/>
        <mapping name="EmployeeType" ldapAttribute="employeeType"/>
        <mapping name="FirstName" ldapAttribute="givenName"/>
        <mapping name="Initials" ldapAttribute="initials"/>
        <mapping name="LastName" ldapAttribute="sn"/>
        <mapping name="LdapId" ldapAttribute="uid"/>
        <mapping name="Manager" ldapAttribute="manager"/>
        <mapping name="Organization" ldapAttribute="o"/>
```

```
    <mapping name="OrganizationalUnit" ldapAttribute="ou"/>
    <mapping name="PhoneNumber" ldapAttribute="telephoneNumber"/>
    <mapping name="PostalCode" ldapAttribute="postalCode"/>
    <mapping name="State" ldapAttribute="st"/>
    <mapping name="Title" ldapAttribute="title"/>
    <mapping name="UserId" ldapAttribute="uid"/>
</objectclass>
```