# Using Directory Server as your Lightweight Directory Access Protocol (LDAP)

**What is LDAP?**

- Lightweight Directory Access Protocol) is an information directory where users and groups can be defined only once and shared across multiple machines as well as across multiple applications
- Also known as X.500 Lite, the protocol enables corporate directory entries to be arranged in a hierarchical structure that reflects geographic and organizational boundaries. Using LDAP, companies can map their corporate directories to actual business processes, rather than arbitrary codes.

**Why do we use it?**

- Was designed to run over TCP or SSL connection, making it ideal for Internet and intranet applications.
- Has simpler functions, making it easier (and, presumably, less expensive) for vendors to implement
- Encodes its protocol elements in a less complex way than X.500, streamlining coding/decoding of requests
- Take responsibility for "referrals" -- LDAP servers return only results (or errors).
- V3 support ensures compatibility with industry standard LDAP based applications
- Eliminates needs for duplicate proprietary directories in our product.
- Reduces TCO for our clientsLearning Management System Release 1.0 requires a LDAP v3 compliant directory.
- The list of supported LDAP products includes:
    - IBM SecureWay® V3.2
    - IBM Directory Server™ V4.1
    - iPlanet V5.0
    - Lotus Domino™
    - Microsoft Active Directory
- Note:
    - If Customers have a security or authentication method other than LDAP, then can actually replace or modify the default JSP's to do the authentication.
        - For example if a client used a 3rd party tool for SSO across their enterprise it could be used to authenticate users. (ex: Netegrity's SightMinder, or Tivoli's Access Manager.)
    - The LMS user management functions assume an LDAP directory is the primary container of user and group information and is still required.

I The VMWARE images have Directory Server installed for use as your LDAP Compliant User Directory.

**A.** Directory Server V5.1 provides a powerful Lightweight Directory Access Protocol (LDAP) identity infrastructure that is the foundation for deploying comprehensive identity management applications and advanced software architectures like Web services.

**1.** Some Key Features:

**a.** SSL Data Encryption

**b.** DB2 UDB 8.1 DataStore – performance, reliability, and data integrity.

**c.** Password Security – expiration, rules, history, ACL Values

**d.** Write-through cache – preventing data loss if server fails

**e.** Fine-grained Access Control – allows self-service and delegated administration.

**f.** Client SDK's – allow fast application development.

**g.** Logging on server events – Audit, Change, and Error logs are provided.

**h.** Robust Replication

**i.** National Language Support (NLS)

**j.** Plug-in support – allowing for choice of authentication methods (SASL, CRAM-MD5

**k.** DSML V2 Support – extends the reach of the directory to web services through XML codingIt's FREE

II Import users as a group via a LDAP Data Interchange Format (LDIF) file

**A.** This file can be provided from a customer's LDAP user directory administrator, or created manually using a text editor.

**1.** A couple of samples are included on the VMWARE image.

**2.** You can quickly edit the data in that file and use it to populate your user directory.

**B.** You should know the following before you start this import.

**1.** Users cannot valid to log on to the LMS while the Directory Server is stopped.

**2.** Depending on the size of your LDIF file this process may take some time.

**3.** The import should not be interrupted once it begins.

**4.** If you have the Directory Management Client Tool open the directory you should close it.

**C.** Launch the **IBM Directory Server Web Admin**

**1.** Open a browser window.

**2.** Enter http://lms/ldap in the address field

**3.** Hit the Enter key.

**4.** Logon:

**a.** Admin ID: "cn=root"

**b.** Password: "password"

5. Expand **Settings** in the left hand navigation frame
6. Click on **Suffixes**
   a. This is where you define your organization
   b. For your installation this is “o=ibm” and has already been defined.
   c. You can only import LDIF files with the organizational suffix defined.
7. Right now your Directory Server should be running. It must be stopped in order to import LDIF files.
   a. Expand the **Current State** folder in the left hand navigation frame
      1) Click on the Start/Stop link in the content frame of the page
      2) You will be presented with a current status and the appropriate action button.
      3) Click on the **Stop** action button.
      4) The content frame will refresh.
   b. When it states that the server is currently stopped you may proceed to the next step
8. Click on the **Database** folder to expand that view
   a. Click on the Import LDIF link to proceed in the content frame.
   b. Manually enter the path on the Directory Server and file name of your LDIF file
      1) This is NOT the local path. The LDIF file must be stored on your Directory Server.
      2) In my environment this file is located on c:\LDAP\directory.ldif
      3) In your VMWARE Session run a search for "*.LDIF" to locate yours if you do not know where it is located.
   c. Click on the **Import** action button.
      1) The content frame will refresh and show you the import progress data.
      2) You will see the following warning messages:
         a) Entry o=ibm already exists
         b) Entry ou=People,o=ibm already exists
         c) Entry ou=Groups,o=ibm already exists
         d) Then in groups of 100 the number of users imported.
         e) When finished you should see “ldif2db: 779 entries have been successfully added out of 782 attempted.”
      3) SUCCESS! You have just added over 782 Groups and Users to the system.
9. The Directory server needs to be restarted in order to use the LMS.
10. Because of the distributed architecture of the LMS stopping and restarting the Directory server will not require you to restart the LMS or any of it’s components.
11. In the upper left hand corner click on the restart button (looks like a circle with a line through it.)
    a. The content frame will refresh.
    b. When it states that the server is “currently running” you are done.

**D.** Click the **Log off** folder in the left hand navigation panel,

**E.** Click the **Log off** action button and close the browser.

**III** Manually Add Groups in IBM Directory Server

**A.** Add Groups individually

**1.** Open the Directory Management Tool on the VMWARE image. (Client side tool)

**2.** Rebind to the database

**a.** Click on the Rebind link in the Directory Tree on the left frame of the Management Tool

1) Select Authenticated
2) Enter "**cn=root**" as the User DN,
3) Enter "**password**" as the User Password
4) Click OK

**b.** The content frame will refresh with a User Tree directory.

1) Expand the **o=ibm** branch
2) Select the **ou=Groups** branch
3) Click Add.
   a) A popup window will appear
   b) Use the dropdown list to change the Entry Type to "**Group"**
   c) Accept the default values for Parent DN.
   d) Change the Entry RDN to "**cn=LMS Enablement**"
   e) Click **OK**
4) Another popup window will open.
   a) Enter "cn=Ed Dussourd" in the "member (Group members)": field
   b) This is a required filed.
   c) Groups cannot exist without at least one member

**c.** Those are the only required fields to add a user in the Directory Server and will be sufficient for use in the LMS.

**d.** Click **Add** now.

**B.** If finished, click the **Exit** action button in the lower left hand navigation section to close the Directory Management tool.

**IV** Manually Add users in IBM Directory Server

**A.** Add users individually.

**1.** Open the Directory Management Tool on the VMWARE image. (Client side tool)

**a.** In the VMWARE session click **Start>Programs>IBM Directory Server 4.1>Directory Management Tool**

**2.** Rebind to the database

**a.** Click on the Rebind link in the Directory Tree on the left frame of the Management Tool

1) Select Authenticated
2) Enter "**cn=root**" as the User DN,
3) Enter "**password**" as the User Password
4) Click OK

**b.** The content frame will refresh with a User Tree directory.

1) Expand the **o=ibm** branch
2) Select the **ou=People branch**
3) Click Add.
   a) A popup window will appear
   b) Accept the default values for Entry Type, and Parent DN.
   c) Change the Entry RDN to "**cn=Mike Smith**"
   d) Click **OK**
4) Another popup window will open.
   a) Enter "Smith" in the "sn(Last name)": field
5) Scroll down to the bottom of the "**Business** tab area
   a) Enter "password" as the user password value.
   b) Passwords are case sensitive.
   c) Validation is not available
6) Click on the "**Other**" tab
   a) Scroll down to the bottom of the field view.
   b) Find the "uid" field
   c) Enter "msmith" as value

**c.** Those are the only required fields to add a user in the Directory Server and will be sufficient for use in the LMS.

**d.** Click **Add** now.

**3.** The user is added, however, the product will demo better if you add more data however

**4.** Scroll down to the bottom of the user list.

**5.** Double click on the User Name – Mike Smith.

**6.** The Edit an LDAP User window opens

**a.** Initials (Initials): "**MPS"**

**b.** On the **Business** tab

1) departmentNumber (Department): "**H2**"
2) employeeNumber: "**L55503**"
3) employeeType (Employee type): "**Full Time**"
4) mail (E-mail):= "**msmith@ldapdemo.com"**
5) manager (Manager): " **cn=George Poirier,ou=People,o=ibm**"
6) telephoneNumber (Office phone): "**555-555-3002**"
7) title (Title) "**Senior Product Specialist**"

**c.** Click on the **Other** tab
1) businessCategory: "**e-Learning**"
2) C: "**USA**"
3) Description: "**Responsible for next generation products**"
4) DisplayName: "**Michael Paul Smith**"
5) GivenName (First Name): "**Michael**"
6) L: "**Cambridge**"
7) O: "**Lotus**"
8) Ou: "**Product Manager**"
9) PostalAddress: "**64431A**"
10) PostalCode: "**02142**"
11) PreferredLanguage: "**English**"
12) St: "**MA**"
13) Street: "**1 Rogers Street**"

**d.** Click on the **Memberships** tab
1) Click **Edit Static Groups**
   a) Select "cn=LMS Enablement,ou=Groups,o=ibm"
   b) Click **Add**
   c) Click **OK**
2) You are returned to the Edit an LDAP User window.
3) Click **OK**

**B.** Repeat the process to add additional users to the user directory

**C.** Tip: For faster and safer results you can duplicate an existing user in the directory tree and modify their information as required.