peoplefluent

PeopleFluent Learning

Single Sign-On Integration Guide

Contents

About this Document

Introduction

The primary objective of this document is to provide information for the implementation of Single Sign-On (SSO) services in PeopleFluent LMS.

Document Information

Revision Information	
Revision Date:	April 25, 2024
Revised Document Version Number:	2.0
Details of Revision:	Initial publication.

PeopleFluent LMS Authentication

A SSO service only requires users to enter a user ID and password information once, and let them subsequently use other applications without the need to login again. A SSO mechanism is useful to these users who need access to multiple systems requiring login.

PeopleFluent LMS supports the following types of SSO solutions:

- The Integrated Windows Authentication - suitable for all organisations that use a Windows-based Intranet environment.
- Security Assertion Markup Language or SAML - a mechanism that provides pure web-based SSO. SAML is more appropriate to those organizations that have an existing commitment to SAML and associated infrastructures.
- The Delegated Authentication - supporting web-based applications also but is a better alternative for those companies that have no experience in SAML.
- WS-Federation Web (passive) requestor profile.

This guide provides basic supplementary information about Active Directory and Lightweight Directory Access Protocol (LDAP) Integration; both are used by the LMS to centralize the storage of user credentials. It also shows how to set up each SSO solution.

This guide is intended for (but not limited to) the LMS administrators who want to install and configure the login adapters for implementing SSO service in the LMS.

Integrated Windows Authentication

Seamless Integration

PeopleFluent LMS provides basic SSO capability by leveraging the Integrated Windows Authentication provided by Microsoft Internet Information Server (IIS). It is tightly integrated with Windows servers and does not require any extra software for implementation, thus providing seamless integration. This solution is a good fit for Windows centric organizations.

Limitations

Although it provides robust integration, it has some limitations:

1. Integrated Windows Authentication is only supported in Microsoft IIS.
2. Integrated Windows Authentication does not work over HTTP proxy connections and firewalls.
3. This solution is only suitable for intranet and IIS web server environments where the client machines are in the same Windows domain.

SSO Login Process

To enable SSO, a special login page "ekpsso.aspx" is used for this purpose. This login page is not visible to the end-user but the administrator should create an entry link to PeopleFluent LMS using this page, or set this page as the default front page of the site.

The login process using ekpsso.aspx is shown below:

1. From some internal website, link to the PeopleFluent LMS Windows SSO start page (e.g. http://< hostname>/LMS/ekpsso.aspx, assuming the default site context is LMS).
2. The code within ekpsso.aspx is able to determine the Windows user ID of the current user. By making use of settings in the configuration file Web.config, it creates an encrypted authentication token which is passed to the LMS. The same encryption key resides in Web.config and the LMS's ekp.properties.
3. If the LMS can decrypt the information sent from ekpsso.aspx, it can safely assume that the user ID is genuine and login the user.

Sample Configuration

Microsoft IIS Web Server Setup

Step 1: Add a Virtual Directory LMS to the Web Server

Important Note:
The name must match the application context name. The default LMS will be used throughout this example.

1. Click **Start** on the Windows desktop, select **Control Panel > Administrative Tools > Computer Management**.

2. Select **Services and Application** and expand **Internet Information Services**. Select **Default Web Site**, right click and select **New**, and then **Virtual Directory**.

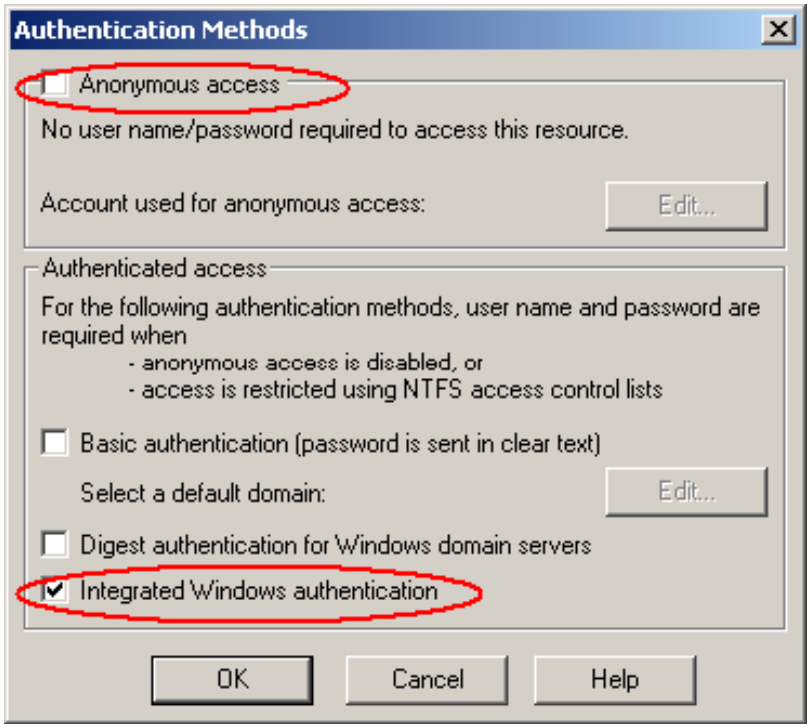
    a. Enter **LMS** as the Virtual Directory Alias.
    b. Select the PeopleFluent LMS document root (Default: \webapps\LMS) as the Web Site Content Directory.
    c. Click **Next** to accept default for Access Permissions.

Step 2: Set the Directory Security of LMS

Warning: If the Integrated Windows authentication is not set, it is equivalent to disabling security checking.

Select LMS virtual directory and set it to use Integrated Windows authentication by right clicking and then select properties. Choose the Directory Security tab folder, and click Edit. Uncheck anonymous access and check the Integrated Windows authentication.

Important Note:
Make sure the Integrated Windows authentication is checked.



Configure LMS to Use Windows SSO

To enable SSO, change the logon page from (default) http://<hostname>/LMS/index.html to http://<hostname>/LMS/ekpsso.asp.

Important Note:
If the application context name is not the default (LMS), the redirect URL in ekpsso.asp has to be changed accordingly.

Enabling ASP.NET v2.0

Version 2.0 of the .NET framework needs to be installed. Even if it has already been installed previously, it should be done again after the installation of IIS to prevent possible errors.

1. Open up the Command Prompt and enter the following commands:cd `%WINDIR%\Microsoft.Net\Framework\v2.0.50727 aspnet_regiis -i`
2. In the IIS console, click the right mouse button on 'Default Web Site' and select 'Properties'. Click the 'ASP.NET' tab. For the ASP.NET version field, choose version 2.0.

ASP.NET Configuration

A configuration file called Web.config accompanies ekpsso.aspx and should be updated accordingly, e.g.

```
<configuration>
 <appSettings>
 <add key="ekpDefaultURL"
value="http://<hostname>/LMS/servlet/ekp/pageLayout" />
 <add key="authenticationKey" value="mysecretkey12345" />
 <add key="authenticationURL" value=
"http://<hostname>/LMS/servlet/ekp?TX=authenticationTokenVerifier"/>
 <add key="authenticationDigestAlgorithm" value="MD5" />
</appSettings>
</configuration>
```

The keys in the configuration file have the following meaning:

- ekpDefaultURL – the page the user will be redirected to after authentication, if the user accesses ekpsso.aspx directly to reach LMS.
- authenticationKey – a secret key used for generating the encrypted authentication token. This must match the value of authentication.key within ekp.properties.
- authenticationURL – once ekpsso.aspx has generated the encrypted authentication token, the user is sent to this LMS URL for authentication and login.
- authenticationDigestAlgorithm – used for generating the encrypted token. This can take one of two values: MD5 or SHA. This must match the value of authentication.digestAlgorithm within ekp.properties.

Protecting Web.config

As Web.config contains sensitive information, it should not be viewable by the public and IIS. By default, it will not serve files with the .config extension. As an added protection, it is standard practice to encrypt sections of the configuration file that contain sensitive data. The .NET framework has a function to carry this out and will automatically decrypt through ASP.NET as and when necessary. To do the encryption, the aspnet_regiis.exe tool should be used. This is located in the Microsoft.NET directory corresponding to the ASP.NET version being used, e.g.

```
cd C:%WINDIR%\Microsoft.NET\Framework\v2.0.50727 aspnet_regiis.exe --pe
"appSettings" --app "/LMS" --prov "DataProtectionConfigurationProvider"
```

The arguments are:

- -pe: the section of the configuration file to be encrypted
- -app: the IIS virtual directory which contains Web.config to be encrypted
- -prov: the name of the encryption provider. The DataProtectionConfigurationProvider uses a machine-based encryption key.

Once encrypted, Web.config will look something like:

```
<configuration>
 <appSettings
configProtectionProvider="DataProtectionConfigurationProvider">
<EncryptedData>
 <CipherData>
 <CipherValue>AQAAANCMnd8BFdERjHoAwE/C1...YEHzqk8kLInCH16mFAAAAAGDGIEk4
309d</CipherValue>
 </CipherData>
 </EncryptedData>
 </appSettings>
</configuration>
```

To undo the encryption:

```
 aspnet_regiis.exe -pd "appSettings" -app "/LMS"
```

The upshot of an encrypted Web.config file is that even if the file should end up in the wrong hands, the authentication key will not be accessible.

LMS Configuration

In ekp.properties, the following configurations must be set, e.g.

```
authentication.key=mysecretkey12345
authentication.service.url=http://<hostname>/LMS/ekpsso.aspx
authentication.digestAlgorithm=MD5
```

The parameters have the following meaning:

- authentication.key – secret key used to validate the encrypted authentication token. This must match the value of authenticationKey within Web.config.
- authentication.service.url – if the user who has not yet logged in attempts to access a secure LMS page which requires a login session, the user is redirected to this URL where an encrypted authentication token would be generated and passed back to the LMS.

- authentication.digestAlgorithm – used for validating the encrypted authentication token. This can take one of two values: MD5 or SHA. This must match the value of authenticationDigestAlgorithm within Web.config.

To enable SSO, change the login page from (default)

`http://<hostname>/LMS/index.html to http://<hostname>/LMS/ekpsso.aspx`

Troubleshooting

The web browser always brings up an authentication box when accessing ekpsso.aspx.

Internet Explorer

Internet Explorer will only pass credentials if the website/domain is designated as a "Local Intranet Zone", i.e. no .com, .net, .org, etc. This is a security restriction with Windows/IE. Your PC will need to be configured to properly pass across the credentials.

Locally on your PC:

1. In IE, click **Tools**, click **Options**, and then click **Security**.
2. Select the zone of **"Local Intranet"**.
3. Press the Sites button and then Advanced.
4. Now add the PeopleFluent LMS URL, e.g. http://<hostname>.

Mozilla Firefox

NTLM authentication must be enabled in Firefox:

1. In Firefox, type "about:config" in the address bar.
2. In the Filter field, type "network.automatic-ntlm-auth.trusted.uris".
3. Double-click the name of the preference that we just searched for.
4. Enter the PeopleFluent LMS URL, e.g. http://<hostname>. If there is more than one URL you want to add, the URLs need to be comma-separated.

IIS Runtime Permission Error

Access is denied.

- **Description**: An error occurred while accessing the resources required to serve this request. You might not have permission to view the requested resources.
- **Error message 401.3**: You do not have permission to view this directory or page using the credentials you supplied (access denied due to Access Control Lists). Ask the Web server's administrator to give you access to 'C:\XXX\Tomcat5.5\webapps\LMS\ekpsso.aspx'.
- **Cause**: ekpsso.aspx is not allowed to run in IIS
- **Solution**: Add "Users" group to ekpsso.aspx


ekpsso.aspx Properties
General
Security
Summary
Group or user names:
Administrators (I-6850-LESTERLI\Administrators)
LOCAL SERVICE
qaqtp2 (qaqtp2@hk.netdimensions.com)
SYSTEM
Users (I-6850-LESTERLI\Users)
Add...
Remove
Permissions for Users
Allow
Deny
Full Control
Modify
Read & Execute
Read
Write
Special Permissions
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

Security Assertion Markup Language (SAML) Autentication

Introduction

PeopleFluent Learning LMS supports the Web Browser SSO profiles of both SAML 2.0 and SAML 1.1, in the role of service provider. It is assumed that the organization using the LMS has already deployed a SAML identity provider. The LMS is known to work with the following identity provider implementations:

- Active Directory Federation Services
- Azure Active Directory
- F5 Networks BIG-IP Access Policy Manager
- Liferay
- McAfee Cloud Identity Manager
- NetIQ Access Manager
- Okta
- OneLogin
- Oracle Identity Federation
- PingFederate
- Salesforce
- Shibboleth
- Workday

PeopleFluent Learning LMS SAML support is based on the Shibboleth 3.x service provider. The LMS supports both SP-initiated and IdP-initiated SSO.

Prerequisites

The Shibboleth SP runs as a Web server module. To date the LMS's SAML support has been tested, and is known to work with the web server configurations listed in the following table:

Shibboleth 2.x Service Provider	Shibboleth 3.x Service Provider
Apache 2.0, 2.2 and 2.4	Apache 2.4
Tomcat 5.5 or higher	Tomcat 8.x

Tomcat requires **mod_proxy_ajp** connector for Apache 2.2 only. For Apache 2.0 or 2.4, use **mod_jk**.

If you are upgrading from Shibboleth 2.x service provider to version 3.x, please review the Shibboleth upgrade documentation.

You must be using a version of Apache that includes SSL support. In order to maintain the security of the environment, it is essential that direct access to Tomcat's AJP connector is blocked at the firewall.

The LMS also supports the Shibboleth service provider with IIS7. Whereas the Shibboleth service provider on Apache passes attributes as environment variables, IIS is not able to pass attributes as environment variables and instead must pass them as HTTP headers, which carries certain security risks. Therefore, take extra care when configuring the LMS with Shibboleth and IIS.

Procedure

1. Download the appropriate Shibboleth 3.x Service Provider (SP) installer from the download site.
2. Install the Shibboleth 3.x Service Provider (SP) as described in the Shibboleth wiki.
3. Check that the SP is running properly by accessing http://localhost/Shibboleth.sso/Status from the actual web server machine. This should return an XML document.
4. Configure etc/shibboleth/attribute-map.xml to specify how the content of SAML assertions is mapped to the LMS user fields. Every Identity Provider is different in terms of the SAML attributes that it will provide. However, some pointers are provided below.

    - In general, attributes can be mapped to any user field that can be set using the LMS's CSV user data loader. As a minimum, you must provide an attribute corresponding with the LMS's UserID field. If you want to enable automatic creation of NTS user accounts, you must also provide attributes corresponding to the LMS's FamilyName and GivenName fields. A Password may be provided, however in general this is not expected; if no value is supplied, direct logins will be disabled for the account.
    - If you are using mod_proxy_ajp, then the value of the id attribute for each <Attribute> element should consist of the name of the corresponding CSV user data loader field name, prefixed with AJP_. Note that these names are case-sensitive. For examples: AJP_UserID, AJP_FamilyName, AJP_GivenName, AJP_Email, AJP_Phone. mod_proxy_ajp will only pass environment variables to Tomcat if their names begin with the AJP_ prefix; it will remove this prefix before passing the environment variable through.
    - If you are using IIS7, or Apache with mod_jk, then the value of the id attribute for each Attribute element should consist of the name of the corresponding CSV user data loader field name without a prefix.

Note:
These names are case sensitive.

Examples:

UserID, FamilyName, GivenName, Email, Phone. If you are using Apache with mod_jk then you will also need to include corresponding JkEnvVar directives in the Apache configuration to ensure that the environment variables are passed through to Tomcat, as in the example below.

```
JkEnvVar UserID JkEnvVar
FamilyName JkEnvVar
GivenName JkEnvVar Email
JkEnvVar Phone
```

- By default the specified attributes will only be used when creating new user accounts; the corresponding fields will not be updated for existing user accounts. You can specify that a particular field should be updated for existing accounts using the value of its corresponding attribute by adding a property named authentication.attribute.{fieldname}.allowUpdate to ekp.properties with the value true. For example, the property below specifies that the Email field should be updated for existing accounts using the value of its corresponding attribute.

  ```
  authentication.attribute.Email.allowUpdate=true
  ```

  The UserID field cannot be updated.

- If you are using multiple assignments, you can control the user's initial assignment after sign-on using an AssignmentID attribute. (Supported in PeopleFluent Learning LMS 14.0 and later.)

- If you are using IIS7 then you must instruct the LMS to read field values from HTTP request headers rather than environment variables, since IIS7 does not support the latter. You can specify that a particular field should be read from the corresponding HTTP request header by adding a property named authentication.attribute.{fieldname}.fromrequestheader to ekp.properties with the value true. You should do this only for fields that have been explicitly mapped to Shibboleth attributes using the etc/shibboleth/attribute-map.xml file as described above. As a minimum, you must add the property below to specify that the UserID field should be read from the corresponding HTTP request header.

```
authentication.attribute.UserID.fromrequestheader=true
```

- In etc/shibboleth/shibboleth2.xml, make the following changes (refer to the Shibboleth 3.x documentation for more information):
    - Configure a <MetadataProvider> element.
        - If the Identity Provider publishes SAML XML metadata, you can simply configure a <MetadataProvider> element that references this metadata, as in the example below.

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="ekp.example.com">
      <Path name="ekp/servlet/ekp/remoteUserAuthenticator"
requireSession="true" authType="shibboleth"/>
    </Host>
  </RequestMap>
</RequestMapper>
```

        - Otherwise, you will need to create the metadata yourself, and then configure a <MetadataProvider> element that references the metadata you created.
    - For the <ApplicationDefaults> element, make the following changes:
        - Configure the value of the entityID attribute to one that's appropriate for your LMS instance. PeopleFluent recommends using a URL with a domain name that you control for the host portion—our general practice is to use https://{LMS-site-hostname}/shibboleth-sp.
        - Add a homeURL attribute with value https:///NTS/servlet/ekp/pa geLayout, replacing with the actual host name that users will use to access the site, and replacing /NTS/ with the actual URL prefix of the LMS site, e.g. homeURL="https://www.example.com/NTS/servlet/ekp/pageLayout".
        - Change REMOTE_USER="eppn" to REMOTE_USER="AJP_UserID" (if using Apache with mod_proxy_ajp) or REMOTE_USER="UserID" (if using IIS7, or Apache with mod_jk)
- Ensure the value of the entityID attribute of the <SSO> element matches the value in the identity provider's metadata.
- If you are using IIS7 you will need to configure the <ISAPI> element as described here. You will also need to configure the <RequestMapper> element to enable Shibboleth authentication for the URL path /ekp/servlet/ekp/remoteUserAuthenticator. The example below was tested with Shibboleth 2.x:

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="ekp.example.com">
      <Path name="ekp/servlet/ekp/remoteUserAuthenticator"
requireSession="true" authType="shibboleth"/>
    </Host>
  </RequestMap>
</RequestMapper>
```

- If you are using Apache, enable Shibboleth authentication for the URL path /NTS/servlet/ekp/remoteUserAuthenticator by adding a <Location> directive like the one shown below either in httpd.conf or the included Shibboleth file:
    - `C:\opt\shibboleth-sp\etc\shibboleth\apache2.config for Apache 2.0`
    - `C:\opt\shibboleth-sp\etc\shibboleth\apache22.config for Apache 2.2`
    - `C:\opt\shibboleth-sp\etc\shibboleth\apache24.config for Apache 2.4`

```
<Location /ekp/servlet/ekp/remoteUserAuthenticator>
 AuthType shibboleth
 ShibRequestSetting requireSession 1
 require valid-user
</Location>
```

- Restart both the web server and the Shibboleth service to ensure the above changes take effect.
- Configure Tomcat to use web server authentication, by adding a tomcatAuthentication="false" attribute to AJP 1.3 connector in <TOMCAT_HOME>/conf/server.xml. The resulting element should look as shown below.

```
<Connector port="8009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" tomcatAuthentication="false" />
```

- Ensure that the property authentication.service.url has the value:

  `/NTS/servlet/ekp/remoteUserAuthenticator in WEB-INF/conf/ekp.properties`

  (Modify the value as appropriate if the URL prefix for the LMS site is not /NTS/.)

  `authentication.service.url=/NTS/servlet/ekp/remoteUserAuthenticator`

- Restart Tomcat to ensure the above changes take effect.
- You can find SAML metadata for the service provider at /Shibboleth.sso/Metadata.

Logout

In a single sign-on environment, it's important that any Logout link behave in a way that is consistent with users' expectations. In general, it's not sufficient for a Logout link merely to end the user's LMS session without also ending his or her sessions with both the Shibboleth service provider and the identity provider. Otherwise, simply accessing any protected LMS page will reinitiate the sign-in process and cause the user to be transparently signed back into the LMS; so, from the user's point of view, clicking the Logout link had no effect.

The simplest solution is to remove the Logout link. This is arguably the best solution, since implementing true single logout is surprisingly hard.

If removing the link is unacceptable, you must ensure that clicking the link causes all of the following to occur:

- End the user's session with the LMS
- End the user's session with the Shibboleth service provider
- End the user's session with the identity provider

Assuming that {idp-logout-url} represents the percent-encoded value of an identity provider URL that ends the user's session, then accessing the URL `/Shibboleth.sso/Logout?return={idp-logo ut-url}` achieves the last two objectives under the default Shibboleth configuration.

For example, if the identity provider logout URL is https://idp.example.com/logout, then you can terminate both the local Shibboleth service provider session and the remote identity provider session by accessing the URL `/Shibboleth.sso/Logout?return=https%3A%2F%2Fidp.example.com%2 Flogout`.

So you need to configure the above URL as the value of the Logout URL field for the root organization. (Go to **Manage Center > Users > Organization Maintenance**, right-click ALL, and select Edit.)

Note that the identity provider still needs to ensure that the user is logged out of any other service providers that have active sessions. This can be hard to achieve reliably, hence the recommendation to simply remove the Logout link.

Delegated Authentication

Introduction

Delegated Authentication is a technique whereby one application relies on a second application to authenticate the end user, thereby avoiding the need for the user to log in to each application separately. Delegated authentication is particularly useful when multiple websites or applications are combined to provide a common service.

An **Authentication Service** is a site that authenticates the end user on behalf of one or more other sites. A **Relying Party** is a site that relies on an authentication service to authenticate the end user.

The LMS can act as either an authentication service or a relying party in a delegated authentication relationship. As an example, consider a portal site that displays a list of the end user's active enrollments (obtained using the LMS's API), but then redirects the user to the LMS to handle tracking when the course is actually launched. Delegated authentication could be used to avoid the need for the user to log into both the portal and the LMS. If the LMS is acting as the authentication service, the user will use an LMS login to access both sites. If the LMS is acting as the relying party, the user will log in through the portal site to access both sites.

Technical Approach

The basic technical approach used is the same whether the LMS is acting as authentication service or relying party. The steps are as follows.

1. The end user attempts to access a protected resource within the relying party. The relying party determines that the user is not yet authenticated.
2. The relying party generates a secure random one-time salt value, and stores it in the user's session.
3. The relying party redirects the user to a distinguished URL within the authentication service (the authentication service URL), including the salt as the value of a query-string parameter named salt. Optionally, the relying part may also provide a query string parameter named callback, whose (URL-encoded) value is a URL that the authentication service should redirect the user to after authenticating the user.
4. If the user is not currently authenticated with the authentication service, the authentication service prompts the user to log in. If the user is already authenticated with the authentication service, this step is skipped.
5. The authentication service redirects the user back to the relying party, using the value of the callback parameter if provided in step 3, or a default URL otherwise. (N.B. The authentication service should check the callback URL against a whitelist of approved sites, in order to prevent arbitrary websites from discovering the user's identity.) The authentication service appends two query string parameters to this URL:

    - `userId`, which is the identifier of the user as established by the authentication service; and
    - `sig`, a hex-encoded cryptographic hash of the string formed by concatenating the user's identifier, a shared secret, and the salt value. (Regardless of whether the LMS is acting as authentication service or relying party, the shared secret is

configured using the `authentication.key` property in the `WEB-INF/conf/ekp.properties` configuration file. The hashing algorithm is configured using the `authentication.digestAlgorithm` property; the default is MD5.)

6. The relying party performs its own computation of the cryptographic hash, and compares the result with the value provided by the query string parameter. Authentication succeeds if and only if the values match.

PeopleFluent LMS as an Authentication Service

In order to use the LMS as an authentication service in a delegated authentication relationship, the relying party should use an authentication service URL formed by appending `servlet/ekp/authenticate` to the base URL of the LMS site. For example, if the LMS site is at http://www.example.com/NTS, then the authentication service URL will be http://www.example.com/NTS/servlet/ekp/authenticate.

The default callback URL for the relying party can be configured using the `authentication.callback.url` property in the WEB-INF/conf/ekp.properties configuration file, as in the example below.

```
authentication.callback.url=http://www.example.com/authcallback.php
```

A specific relying party can override this value by passing a callback URL as the value of a query string parameter named callback, provided that the relying party has been designated as trusted as described here. Note that, as with all parameter values, the value of the callback parameter must be URL-encoded, as in the example below (which also includes the required nonce parameter).

```
servlet/ekp/authenticate?nonce=a6f8a4675a98a54d63d80c0c3b2a4e6c&callback=htt
p%3A%2F%2Fwww.example com%2Fauthcallback.php
```

As an example, an application might be developed that displays a highly-customized view of a learner's training plan including his or her current progress. The application could use delegated authentication to establish the user's identity, and then call the LMS's trainingHistoryXml API function to determine the user's progress in the various courses in their plan so that the training plan can be presented appropriately.

PeopleFluent LMS as an Authentication Service for Multiple Relying Parties

Since each relying party may pass its own callback URL with an authentication request, multiple relying parties can be used with a single LMS instance. For example, multiple portals could be backed by one LMS instance.

PeopleFluent LMS as a Relying Party

In order to have the LMS act as a relying party in a delegated authentication relationship, configure the authentication.service.url property in the `WEB-INF/conf/ekp.properties` configuration file to be the identity provider URL, as in the example below.

The default callback URL for the relying party can be configured using the `authentication.callback.url` property in the WEB-INF/conf/ekp.properties configuration file, as in the example below.

```
authentication.callback.url=http://www.example.com/authcallback.php
```

A specific relying party can override this value by passing a callback URL as the value of a query string parameter named callback, provided that the relying party has been designated as trusted as described here. Note that, as with all parameter values, the value of the callback parameter must be URL-encoded, as in the example below (which also includes the required nonce parameter).

```
servlet/ekp/authenticate?nonce=a6f8a4675a98a54d63d80c0c3b2a4e6c&callbac
k=http%3A%2F%2Fwww.example.com%2Fauthcallback.php
```

As an example, an application might be developed that displays a highly-customized view of a learner's training plan including his or her current progress. The application could use delegated authentication to establish the user's identity, and then call the LMS's trainingHistoryXml API function to determine the user's progress in the various courses in their plan so that the training plan can be presented appropriately.

LMS Authentication

Active Directory Integration

This section describes the steps required in configuring the LMS to use Active Directory (AD) to perform user authentication.

The AD service in the Windows 2000, 2003, and 2008 server provides native LDAP support and it enables other application to use this service through the LDAP interface. The LMS has a built-in login adapter that integrates with the AD to perform user login authentication.

Note:
The following example is based on the Windows 2003 environment.

Configuring Active Directory (AD)

As one of the requirements, all user accounts that exist in the LMS (including the user account for initial binding) must have a corresponding account in AD. Please refer to http://support.microsoft.com/kb/324 753 for details about configuring AD.

Note:
The configurations used in this document are based on the Windows Server 2003 environment.

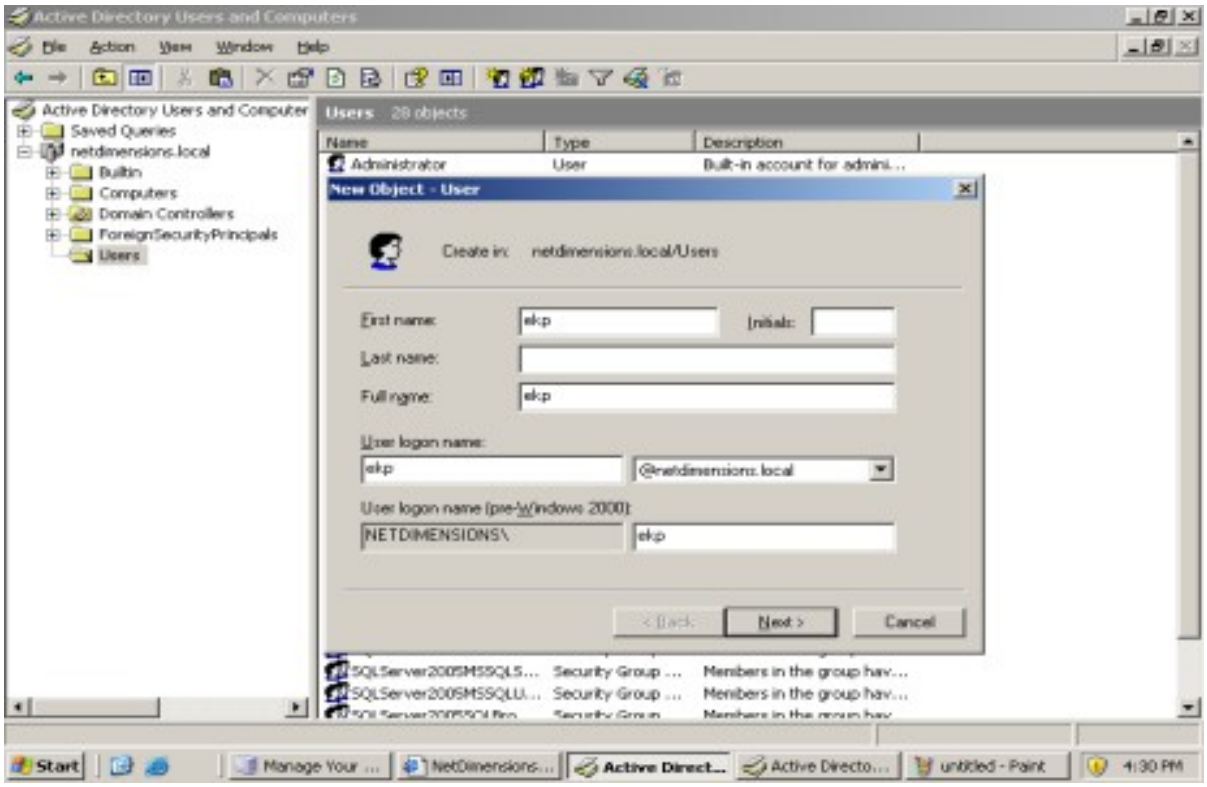
Configuring Domain Name System (DNS)

All users created in the Active Directory must be assigned to a domain name. To configure a Domain Name, please refer to http://support.microsoft.com/kb/814591

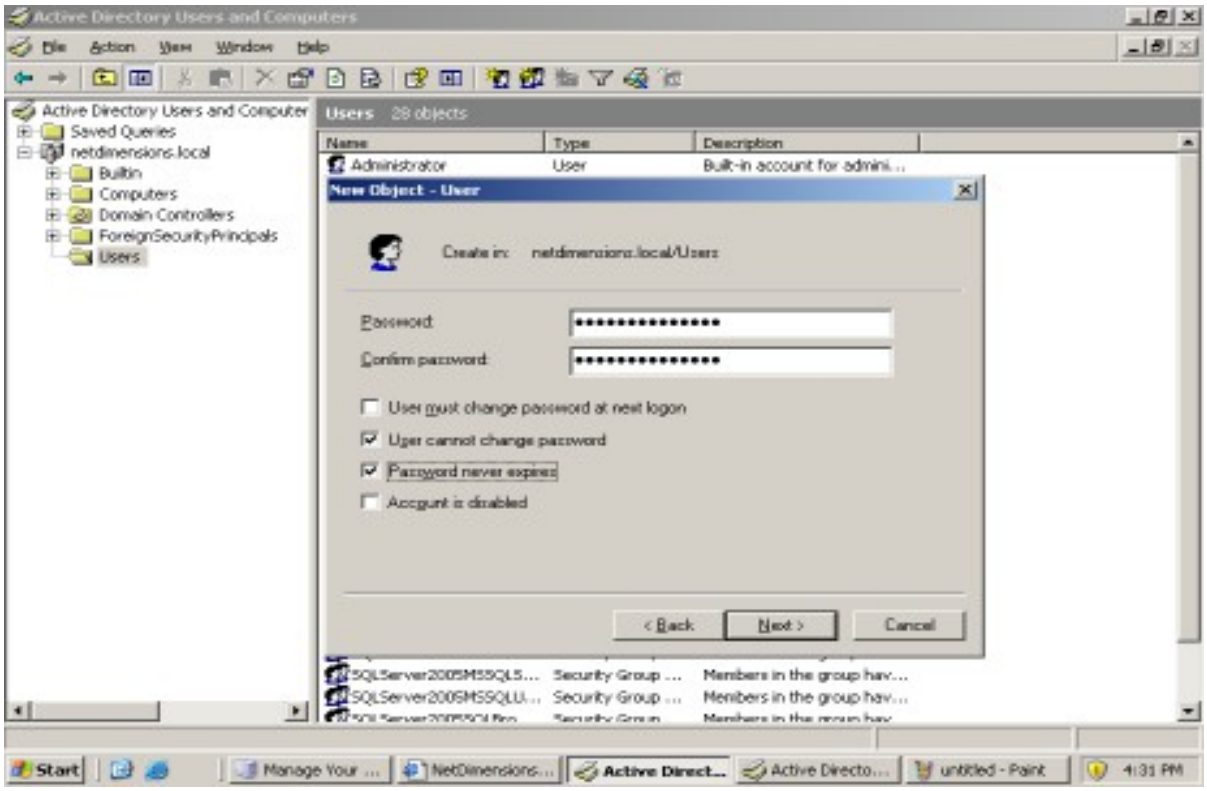
Creating User Account

This section shows the procedures on how to create a new user account into Active Directory

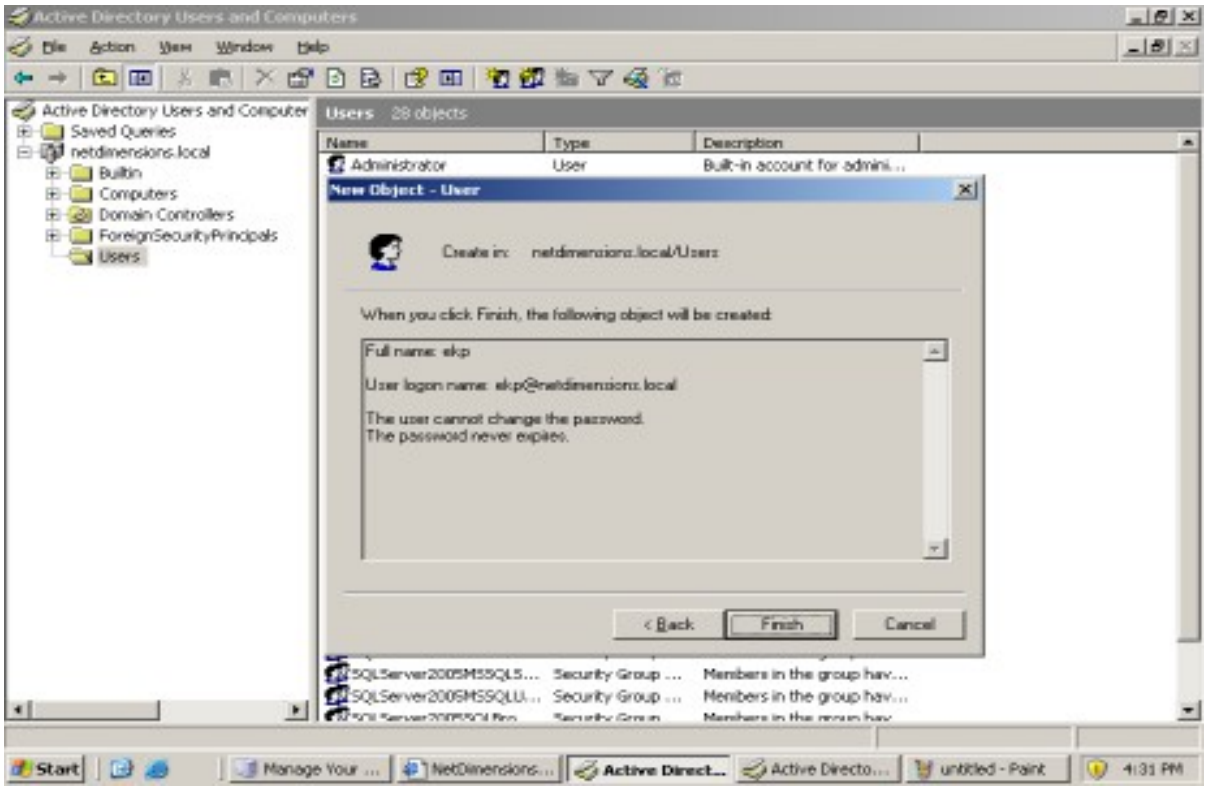
1. Go to **Administrative Tools > Active Directory Users and Computers**, Create a new user "ekp" by selecting **Action > New > User** and enter the name of the user.



2. Enter password for the user and set the options as the following diagram and click **Next**.



3. If the user is created successfully, click **Finish** to continue.



Note:
For details about Adding Users and Computers to the Active Directory, please refer to https://support.microsoft.com/kb/324753

LMS Configuration

In configuring the LMS, the administrator must setup the following:

- Enable the LDAP interface
- Configure User for Initial Binding
- Configure the User to Use External Authentication

Note:
The example below shows the complete configuration of the **ekp.properties**. Those texts in **bold** font style are part of the ekp.properties that enables the LDAP interface. While the texts that are in *italic* shows the setup in configuring user for initial binding.

default.LDAP_Dir=dc=hongkong,dc=netdimensions,dc=com

default.LDAP_HOST1=192.168.99.10

default.LDAP_PORT1=389 default.LDAP_HOST2=192.168.99.12

default.LDAP_PORT2=389 default.LDAP_HOST3=192.168.69.91

default.LDAP_PORT3=389 default.LDAP_TIMEOUT=300

 # Define the active directory DN and password for initial binding.

ldap.useActiveDirectory=true

ldap.activeDirectoryDN=cn=ekp,ou=IT,ou=Users,ou=Hongkong,dc=hongkong,dc=netdimensions,dc=com

ldap.activeDirectoryPassword= ekp_password

The detailed explanation on how the ekp.properties is configured will be discussed on the succeeding sections.

Enable the LDAP Interface

1. Enable the LDAP interface in the LMS by editing the ekp.properties which is located in the **<web- apps>/ekp/WEB-INF/conf** folder.
2. On the ekp.properties put the following settings:

   default.LDAP_Dir=dc=**[domain name]**,dc=**[domain name]**

   default.LDAP_HOST1=**[AD (LDAPserver)]**

   default.LDAP_PORT1=**[port number]**

   default.LDAP_HOST2=**[AD (LDAPserver)]**

   default.LDAP_PORT2=**[port number]**

   default.LDAP_HOST3=[AD (LDAPserver)]

   default.LDAP_PORT3=[port number]

   default.LDAP_TIMEOUT=[port number]

Where:

*default.LDAP_Dir=dc=**[domain name]**,dc=**[domain name]***

Description	Examples
Define the distinguished name of the node connected to the AD.	The example below shows on how to configure the LMS for local host (Intranet) • default.LDAP_Dir=dc=**netdimensions**,dc=**local** The example below shows on how to configure the LMS for LDAP with Domain names • default.LDAP_Dir=dc=**hongkong**,dc=**netdimensions**,dc=**com**

*default.LDAP_HOST1=**[AD (LDAPserver)]***

Description	Examples
Define the primary LDAP server. Entering either the Hostname or the IP address is acceptable.	Sample showing hostname • default.LDAP_HOST1=**win2003-svr** Sample showing IP Address • default.LDAP_HOST1=**192.168.99.10**

default.LDAP_PORT1 (mandatory)

Description	Examples
Define the port number of the LDAP server.	• default.LDAP_PORT1=389

default.LDAP_HOST2=[AD (LDAPserver)]

Description	Examples

Define the second backup LDAP server. Entering either the Hostname or the IP address is acceptable.	Sample showing hostname • default.LDAP_HOST1=**win2003-svr** Sample showing IP Address • default.LDAP_HOST1=**192.168.99.10**

default.LDAP_PORT2 (mandatory)

Description	Examples
Define the port number of the second backup LDAP server.	• default.LDAP_PORT2=**389**

default.LDAP_HOST3=[AD (LDAPserver)]

Description	Examples
Define the third backup LDAP server. Entering either the Hostname or the IP address is acceptable.	Sample showing hostname • default.LDAP_HOST1=**win2003-svr** Sample showing IP Address • default.LDAP_HOST1=**192.168.99.10**

default.LDAP_PORT3 (mandatory)

Description	Examples
Define the port number of the third backup LDAP server.	• default.LDAP_PORT3=**389**

default.LDAP_TIMEOUT

Description
Specify the timeout period in seconds before switching to use.

Note:
LDAP_HOST2 and **LDAP_HOST3** are used to define backup AD servers. The LMS is able to use multiple authentication servers in a daisy-chain fashion. If the first server does not respond to an authentication request, the second is tried, and so on. If your environment does not use backup AD server(s), use the same host as the primary.

The table shows enabling configuring LDAP for local host and for domain name:

Configuring ekp.properties with local host (intranet)	Configuring ekp.properties with domain name.
default.LDAP_Dir=dc=netdimensions,dc=local default.LDAP_HOST1=win2003-svr default.LDAP_PORT1=389 default.LDAP_HOST2=win2003-svr default.LDAP_PORT2=389 default.LDAP_HOST3=win2003-svr default.LDAP_PORT3=389 default.LDAP_TIMEOUT=300	default.LDAP_Dir=dc=hongkong,dc=netdimensions,dc default.LDAP_HOST1=192.168.99.10 default.LDAP_PORT1=389 default.LDAP_HOST2=192.168.99.12 default.LDAP_PORT2=389 default.LDAP_HOST3=192.168.69.91 default.LDAP_PORT3=389 default.LDAP_TIMEOUT=

Configure User for Initial Binding

To enable user for initial binding, in ekp.properties add the following:

- ldap.useActiveDirectory=true
- ldap.activeDirectoryDN=cn=**[user]**,ou=[organization unit],dc=**[domain name]**,dc=**[domain name]**
- ldap.activeDirectoryPassword=**[password]**

Where

ldap.useActiveDirectory	Specifies to use Active Directory

ldap.activeDirectoryDN	Specifies the name of the user for initial LMS binding to the AD, so that directory searches can be done later • [cn] – User account use for initial binding • [ou] – Organizational Unit • [dc] – Domain Component Example: ldap.activeDirectoryDN=cn=**ekp**,ou=users,dc=netdimensions,dc=local
ldap.activeDirectoryPassword	Specifies the password of the user **Note**:**ek p** is the name of the user created in the previous section and **ek p_password** is the password of user **ekp**.

Example:

ldap.useActiveDirectory=true
ldap.activeDirectoryDN=cn=**ekp**,ou=users,dc=netdimensions,dc=local
ldap.activeDirectoryPassword=**ekp_password**

The Distinguished Name string will be determined by how your LDAP is configured.

You can use ADSI Edit on your AD servers to view the format of the DN value assigned to this user ekp – so you would need to specify the same parameters.

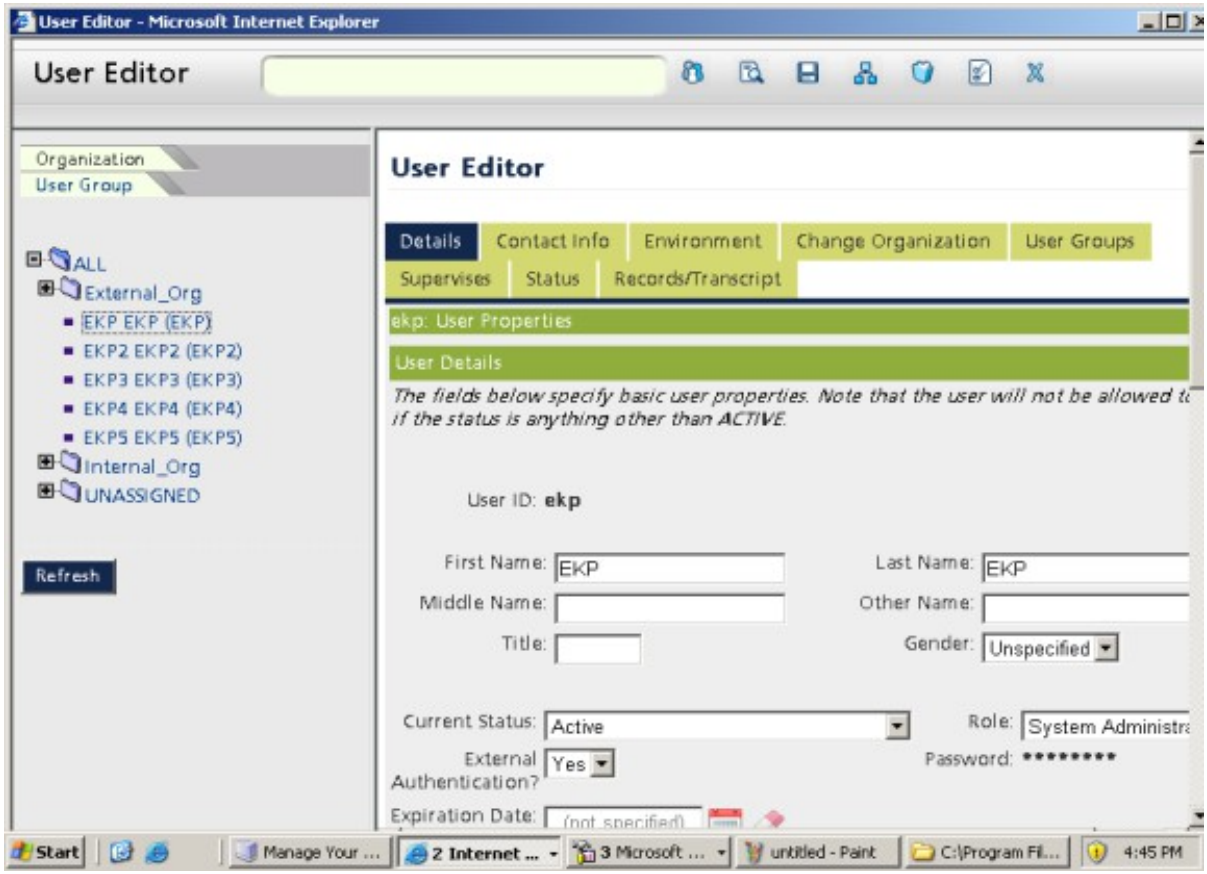
ldap.activeDirectoryDN=cn=ekp,ou=Users,dc=hongkong,dc=netdimensions,dc=com

In larger organizations it could be more complex with multiple OUs for Organizational Units ldap.activeDirectoryDN=cn=ekp,ou=IT,ou=Users,ou=HongKong,dc=hongkong,dc=netdimension,dc=com

Configure the User to Use External Authentication

To complete the LMS configuration, enable the users' external authentication in the User Editor. To do this:

1. Login to the LMS as administrator, go to **Manage > User Manager > User Editor**.



2. Set **External Authentication** to **Yes** for users who want to use AD authentication.

Note:
In order to do the above, the users have to be loaded into the LMS beforehand and the User ID has to match with the user name in the AD. Users with External Authentication set to No will be using default internal authentication, which means that their password is stored in the LMS and at login their user ID/password is checked against this entry instead of authenticated against the AD.

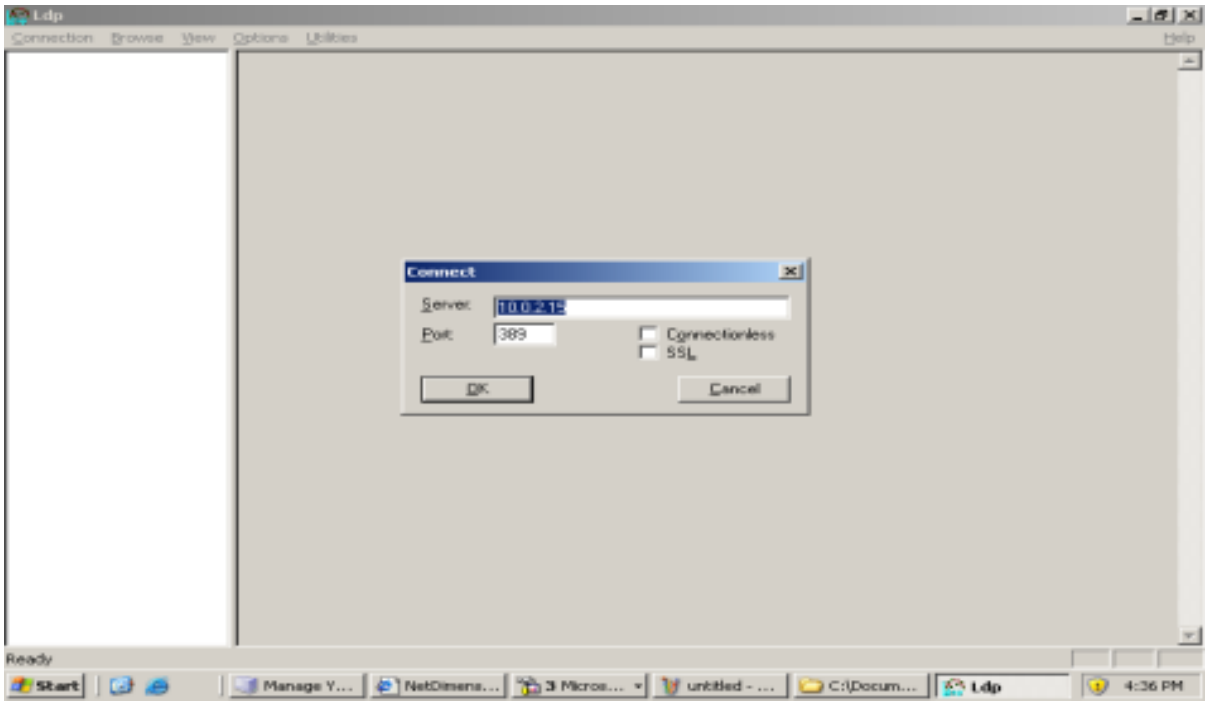
Perform the Initial Binding

Once the server and LMS are properly configured you may perform the initial binding. One of the tools you can use is ldp.exe from

http://www.computerperformance.co.uk/w2k3/utilities/ldp.htm.

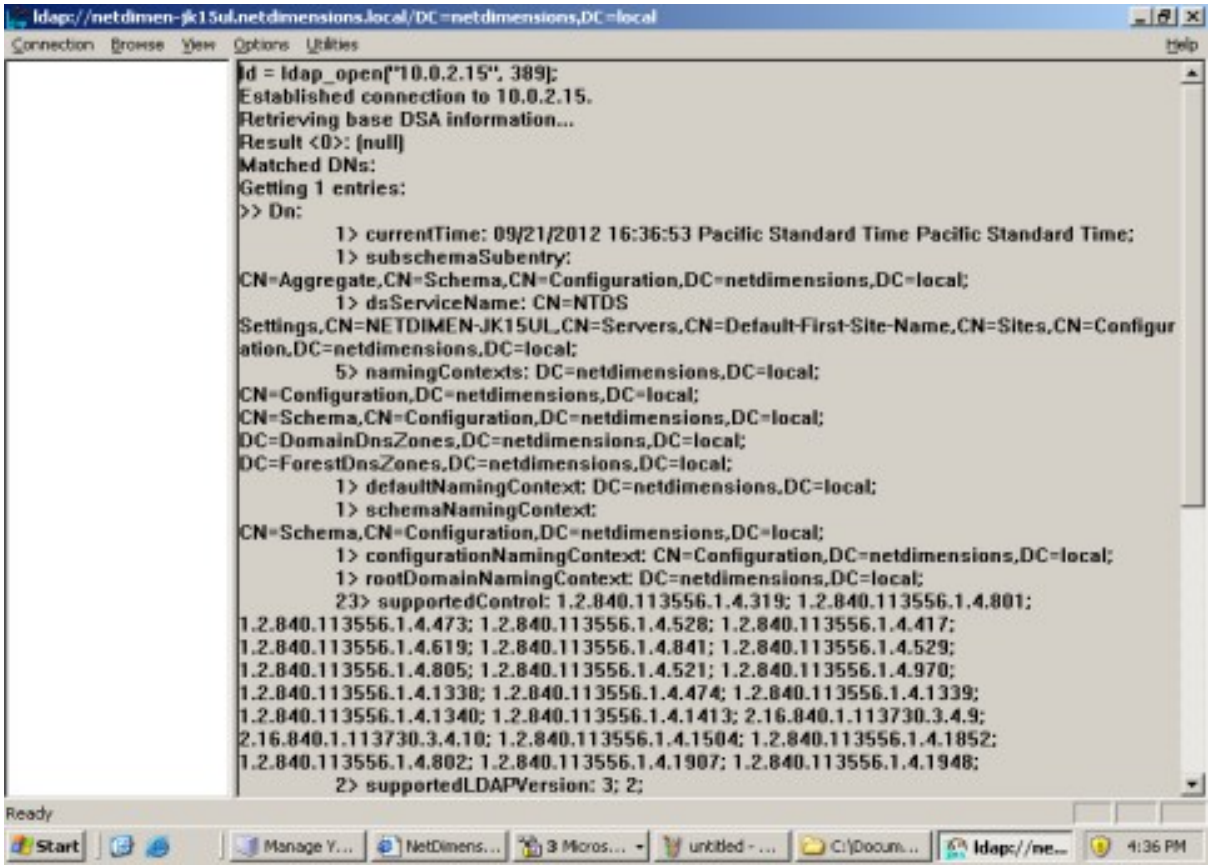
Checking the LDAP Connection

1. On the LDP main menu, go to **Connection > Connect**.



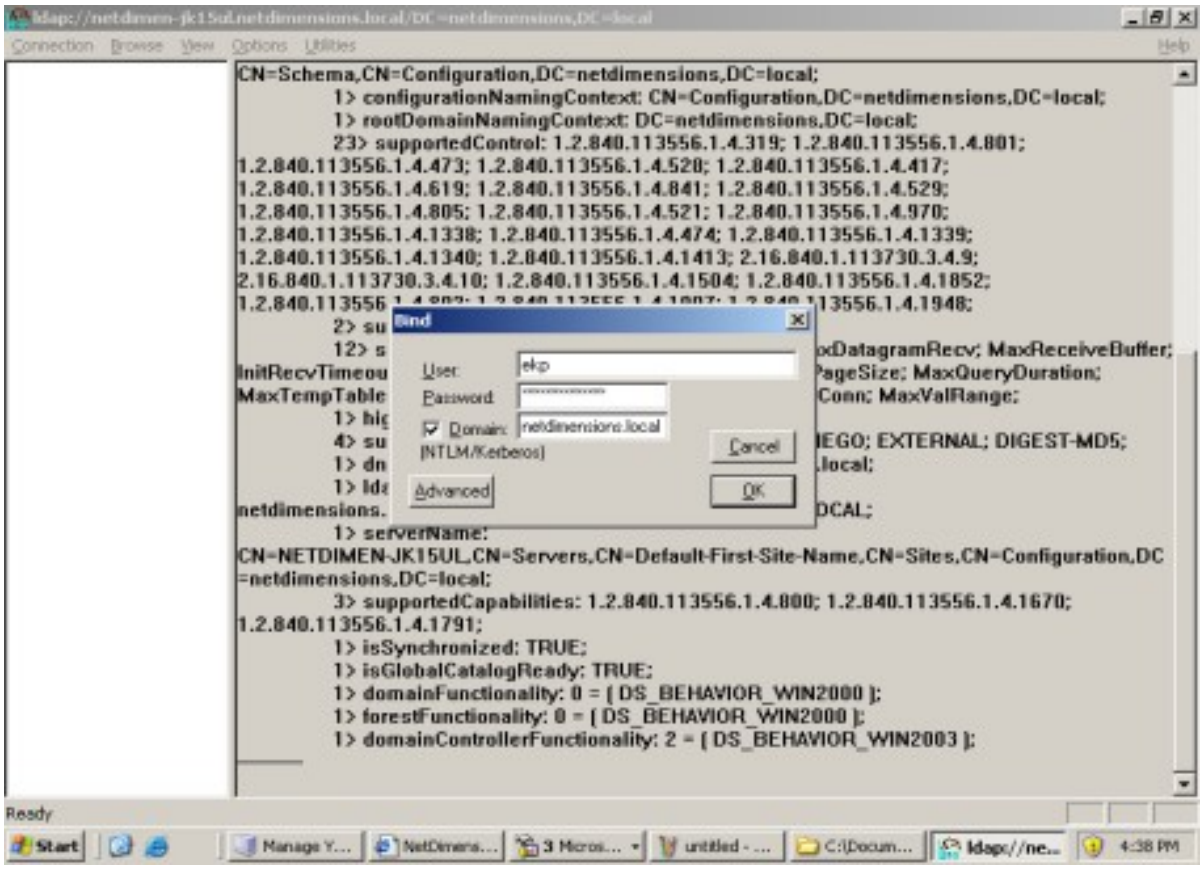
2. Enter the Server and Port number. Then click **OK**.

The message below shows that the connection is successful.



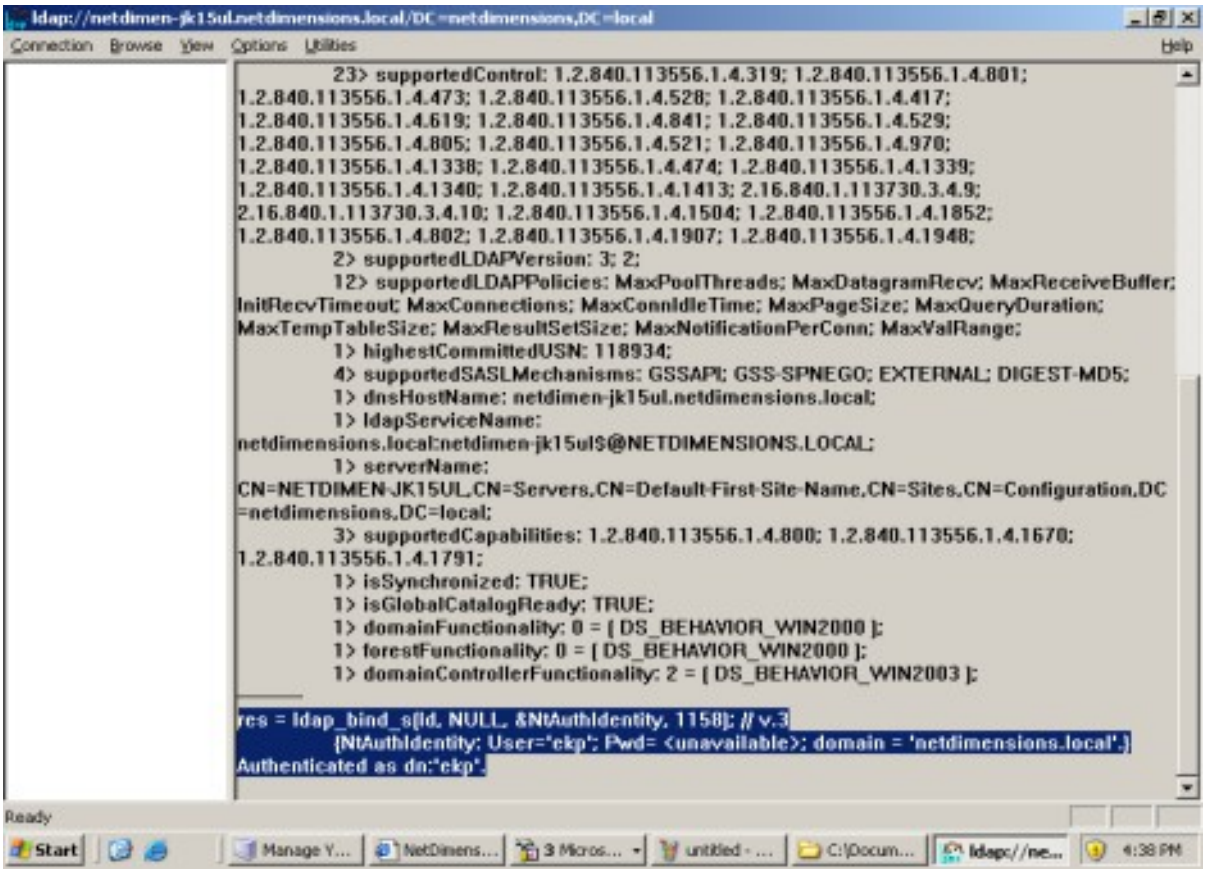
User Initial Binding

1. On the LDP main menu, go to **Connection > Bind**.



3. Enter User, Password, and Domain name.
4. Click **OK**.

The message below shows a successful user authentication (initial binding).



Troubleshooting LDAP Authentication

Checking the LMS Log

Sample of ekp.log Showing Successful LDAP Authentication

```
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: executing sql [SELECT * FROM userstats WHERE userid = ?]
for arguments ('ekp')
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: executing sql [SELECT COUNT(*) FROM messages WHERE
readindicator = 'N' AND userid = ?] for arguments ('ekp')
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: executing sql [UPDATE userstats
SET lastlogon = ?, lastpwchange = ?, nlogons = ?, nattempts = ?, nmsgspending = ?, elapsedloginseconds = ?, nlogouts = ?,
lastAutoEnrollUpdate = ?, first_login = ? , last_crs_offline_auto_enroll = ?, requirepwchange = ?, lastactivedate = ?,
last_job_auto_assign_update = ?, last_job_offline_auto_assign = ? WHERE userid = ?] for arguments ('2012-09-21 16:55:20.9',
'null', 15, 0, 0, 2192, 14, 'null', '2012-09-14 13:30:21.927', 'null', 'N', '2012-09-21 16:55:20.9', 'null', 'null', 'ekp')
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: executing sql [UPDATE auditlogins SET nsecondsactive = ?
WHERE auditkey = ?] for arguments (57, 6206)
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: removing session attribute: 'UserInfoBean'
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: About to obtain a connection for
com.netdimen.core.og@6c7407
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: Obtaining a connection for com.netdimen.core.og@6c7407
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: DEFAULT: Module com.netdimen.core.og@6c7407 allocated
a connection.
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: Obtained a connection for com.netdimen.core.og@6c7407
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: DEFAULT: Module com.netdimen.core.og@6c7407 allocated
a connection.
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: removing session attribute: 'EKPSESSION'
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: About to obtain a connection for login/guest
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: Obtaining a connection for login/guest
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: DEFAULT: Module login/guest allocated a connection.
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: Obtained a connection for login/guest
2012/Sep/21 16:56:18 DEBUG com.netdimen.hc.j.e.d: DEFAULT: Module login/guest allocated a connection.
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: About to obtain a connection for verify/guest
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: Obtaining a connection for verify/guest
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: DEFAULT: Module verify/guest allocated a connection.
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: Obtained a connection for verify/guest
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: DEFAULT: Module verify/guest allocated a connection.
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: Using AD server in:ldap://netdimen-
jk15ul.netdimensions.local:389
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: User ekp found in the directory
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: User DN is:CN=ekp,CN=Users,DC=netdimensions,DC=local
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: Using AD server in:ldap://netdimen-
jk15ul.netdimensions.local:389
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: User login success
2012/Sep/21 16:56:40 DEBUG com.netdimen.hc.j.e.d: executing sql [SELECT * FROM userstats WHERE userid = ?]
for arguments ('ekp')
2012/Sep/21 16:56:41 DEBUG com.netdimen.hc.j.e.d: executing sql [SELECT COUNT(*) FROM messages WHERE
readindicator = 'N' AND userid = ?] for arguments ('ekp')
2012/Sep/21 16:56:41 DEBUG com.netdimen.hc.j.e.d: executing sql [UPDATE userstats
SET lastlogon = ?, lastpwchange = ?, nlogons = ?, nattempts = ?, nmsgspending = ?, elapsedloginseconds = ?, nlogouts = ?,
lastAutoEnrollUpdate = ?, first_login = ? , last_crs_offline_auto_enroll = ?, requirepwchange = ?, lastactivedate = ?,
last_job_auto_assign_update = ?, last_job_offline_auto_assign = ? WHERE userid = ?] for arguments ('2012-09-21
16:56:41.135', 'null', 16, 0, 0, 2192, 14, 'null', '2012-09-14 13:30:21.927', 'null', 'N', '2012-09-21 16:56:41.135', 'null', 'null', 'ekp')
2012/Sep/21 16:56:41 DEBUG com.netdimen.hc.j.e.d: executing sql [SELECT mekp_activation FROM userstats
WHERE userid = ? ] for arguments ('ekp')
2012/Sep/21 16:56:41 DEBUG com.netdimen.hc.j.e.d: About to obtain a connection for pagelayout/ekp
```

Sample of ekp.log Showing Failed LDAP Authentication

```
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  executing sql [SELECT * FROM userstats WHERE userid = ?]
for arguments ('ekp')
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  executing sql [SELECT COUNT(*) FROM messages WHERE
readindicator = 'N' AND userid = ?] for arguments ('ekp')
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  executing sql [UPDATE userstats
SET lastlogon = ?, lastpwchange = ?, nlogons = ?, nattempts = ?,  nmsgspending = ?, elapsedloginseconds = ?, nlogouts = ?,
lastAutoEnrollUpdate = ?, first_login = ? , last_crs_offline_auto_enroll = ?,  requirepwchange = ?, lastactivedate = ?,
last_job_auto_assign_update = ?, last_job_offline_auto_assign = ? WHERE userid = ?] for arguments ('2012-09-21
16:56:41.137', 'null', 16, 0, 0, 2341, 15, 'null', '2012-09-14 13:30:21.927', 'null', 'N', '2012-09-21 16:56:41.137', 'null', 'null', 'ekp')
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  executing sql [UPDATE auditlogins SET nsecondsactive = ?
WHERE auditkey = ?] for arguments (149, 6207)
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  removing session attribute: 'UserInfoBean'
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  About to obtain a connection for
com.netdimen.core.og@1f519ae
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  Obtaining a connection for com.netdimen.core.og@1f519ae
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  DEFAULT: Module com.netdimen.core.og@1f519ae allocated
a connection.
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  Obtained a connection for com.netdimen.core.og@1f519ae
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  DEFAULT: Module com.netdimen.core.og@1f519ae allocated
a connection.
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  removing session attribute: 'EKPSESSION'
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  About to obtain a connection for login/guest
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  Obtaining a connection for login/guest
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  DEFAULT: Module login/guest allocated a connection.
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  Obtained a connection for login/guest
2012/Sep/21 16:59:11 DEBUG  com.netdimen.hc.j.e.d:  DEFAULT: Module login/guest allocated a connection.
2012/Sep/21 16:59:22 DEBUG  com.netdimen.hc.j.e.d:  About to obtain a connection for verify/guest
2012/Sep/21 16:59:22 DEBUG  com.netdimen.hc.j.e.d:  Obtaining a connection for verify/guest
2012/Sep/21 16:59:22 DEBUG  com.netdimen.hc.j.e.d:  DEFAULT: Module verify/guest allocated a connection.
2012/Sep/21 16:59:22 DEBUG  com.netdimen.hc.j.e.d:  Obtained a connection for verify/guest
2012/Sep/21 16:59:22 DEBUG  com.netdimen.hc.j.e.d:  DEFAULT: Module verify/guest allocated a connection.
2012/Sep/21 16:59:22 DEBUG  com.netdimen.hc.j.e.d:  Using AD server in:ldap://netdimen-
jk15ul.netdimensions.local:389
2012/Sep/21 16:59:23 DEBUG  com.netdimen.hc.j.e.d:  User ekp found in the directory
2012/Sep/21 16:59:23 DEBUG  com.netdimen.hc.j.e.d:  User DN is:CN=ekp,CN=Users,DC=netdimensions,DC=local
2012/Sep/21 16:59:23 DEBUG  com.netdimen.hc.j.e.d:  Using AD server in:ldap://netdimen-
jk15ul.netdimensions.local:389
2012/Sep/21 16:59:23 DEBUG  com.netdimen.hc.j.e.d:  LDAP server 1 authentication failed
com.netdimen.auth.login.IncorrectPasswordException
        at com.netdimen.eb.a.a(a.java:14)
        at com.netdimen.auth.login.LDAPLoginAdapter.a(LDAPLoginAdapter.java:2)
        at com.netdimen.auth.login.LDAPLoginAdapter.a(LDAPLoginAdapter.java:14)
        at com.netdimen.tx.auth.login.VerifyLogin.execute(VerifyLogin.java:128)
        at com.netdimen.txserver.TransactionExecutionCommand.b(TransactionExecutionCommand.java:11)
        at com.netdimen.txserver.TransactionExecutionCommand.a(TransactionExecutionCommand.java:29)
        at com.netdimen.txserver.TransactionExecutionCommand.call(TransactionExecutionCommand.java:17)
        at com.netdimen.hc.h.b.a(b.java:7)
        at com.netdimen.txserver.TransactionContainer.a(TransactionContainer.java:126)
        at com.netdimen.txserver.TransactionContainer.a(TransactionContainer.java:231)
        at com.netdimen.txserver.TransactionContainer.a(TransactionContainer.java:109)
        at com.netdimen.core.dh.a(dh.java:93)
        at com.netdimen.core.nb.a(nb.java:4)
        at com.netdimen.core.cc.a(cc.java:66)
        at com.netdimen.txserver.TransactionServlet.a(TransactionServlet.java:32)
```

Additional Resources

Lightweight Directory Access Protocol Version 3

- The IETF LDAPv3 Working Group:

  http://datatracker.ietf.org/wg/ldapbis/charter/

- The LDAPv3 Working Group archived newsgroup:

  http://www.openldap.org/lists/ietf-ldapbis/

- RFC 3377, the current definition of LDAPv3:

  ftp://ftp.rfc-editor.org/in-notes/rfc3377.txt

- LDAP Error Codes:

  http://ldapwiki.willeke.com/wiki/LDAP%20Result%20Codes

Open Group and the Directory Interoperability Forum

- Using VSLDAP – The basis:

  http://www.opengroup.org/openbrand/testing/checklist/guide/use_basics.html

- The Directory Interoperability Forum (DIF):

  http://www5.opengroup.org/idm/

Miscellaneous

- What is Active Directory?

  http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492(v=vs.85).aspx

- Active Directory Application Mode:

  http://www.microsoft.com/en-us/download/details.aspx?id=4201 http://technet.microsoft.com/en-us/library/cc755705(v=WS.10).aspx

- Directory Services Markup Language (DSML):

  http://msdn.microsoft.com/en-us/library/windows/desktop/aa813608(v=vs.85).aspx

- Microsoft Identity Integration Server 2003, Enterprise Edition:

  http://technet.microsoft.com/en-us/library/cc720552(v=ws.10).aspx

- The Microsoft Windows 2000 inetOrgPerson Kit:

  http://msdn.microsoft.com/en-us/library/ms808546.aspx

- LDAP API reference for developers on MSDN:

  http://msdn.microsoft.com/en-us/library/windows/desktop/aa367008(v=vs.85).aspx

For the latest information about Windows Server 2003, refer to the Windows Server 2003 Web site at http://technet.microsoft.com/en-us/windowsserver/bb512919.aspx.

Legal Notice

This document has been created for authorized licensees and subscribers ("Customers") of the software products and associated services of Learning Technologies Group, Inc. by its division PeopleFluent and all of its affiliates (individually and collectively, as applicable, "PeopleFluent"). It contains the confidential and proprietary information of PeopleFluent and may be used solely in accordance with the agreement governing the use of the applicable software products and services. This document or any part thereof may not be reproduced, translated or retransmitted in any form without the written permission of PeopleFluent. The information in this document is subject to change without notice.

PEOPLEFLUENT DISCLAIMS ALL LIABILITY FOR THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT AND MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO ITS ACCURACY OR COMPLETENESS. PEOPLEFLUENT DISCLAIMS ALL IMPLIED WARRANTIES INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. PEOPLEFLUENT DOES NOT GUARANTEE THAT ITS PRODUCTS OR SERVICES OR ANY SAMPLE CONTENT CONTAINED IN ITS PRODUCTS AND SERVICES WILL CAUSE OR ENABLE CUSTOMER TO COMPLY WITH LAWS APPLICABLE TO CUSTOMER. USERS ARE RESPONSIBLE FOR COMPLIANCE WITH ALL LAWS, RULES, REGULATIONS, ORDINANCES AND CODES IN CONNECTION WITH THE USE OF THE APPLICABLE SOFTWARE PRODUCTS,INCLUDING, WITHOUT LIMITATION, LABOR AND EMPLOYMENT LAWS IN RELEVANT JURISDICTIONS. THE PEOPLEFLUENT PRODUCTS AND SAMPLE CONTENT SHOULD NOT BE CONSTRUED AS LEGAL ADVICE.

Without limiting the generality of the foregoing, PeopleFluent may from time to time link to third-party websites in its products and/or services. Such third-party links are for demonstration purposes only, and PeopleFluent makes no representations or warranties as to the functioning of such links or the accuracy or appropriateness of the content located on such third-party sites. You are responsible for reviewing all content, including links to third-party web sites and any content that you elect to use, for accuracy and appropriateness, and compliance with applicable law.

Any trademarks included in this documentation may comprise registered trademarks of PeopleFluent in the United States and in other countries.

Microsoft, Windows, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Oracle and PeopleSoft are registered trademarks of Oracle International Corporation. Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated. All other names are used for identification purposes only and are trademarks or registered trademarks of their respective owners. Portions of PeopleFluent Workforce Communication software may include technology licensed from Autonomy and are the copyright of Autonomy, Inc.Quartz Scheduler is licensed under the Apache License.

Website: peoplefluent.com