



LECTRA FASHION PLM - LDAP INTEGRATION & SYNCHRONIZATION PROCESS

Administration Guide

Date of last update: October 2011



Copyright

Lectra PLM Fashion: Copyright ©2006, Lectra and third parties. All rights reserved. This software is owned by Lectra and Lectra's applicable suppliers, and is protected by intellectual property and copyright laws. All rights, title and interest in and to this software, including without limitation all copyrights, patents, trademarks and trade secrets remain at all times exclusively with Lectra, or its applicable suppliers.

Clarity: Copyright©1998-2005 Niku Corporation and third parties. This software is owned by Niku and its suppliers and is protected by United States copyright laws and international treaty provisions.

Trademarks

Niku and the Niku logo are registered trademarks, and Clarity, the Clarity logo, Clarity Studio, Global 2000 Proven, Precision Security, PowerMods, Best Practice Accelerators, PMO Accelerator, CPIC Accelerator, Service Connect, Schedule Connect, and XOG are trademarks of Niku Corporation in the United States and certain other countries. All other trademarks, trade names, and/or product names are used solely for the purpose of identification and are the property of their respective owners.

Lectra® and Lectra Systèmes® are registered trademarks of Lectra.

Internet Explorer is a registered trademark of Microsoft Corporation.

Oracle® is a registered trademark of Oracle Corporation.

Windows NT®, Windows® 2000, and Windows® XP are registered trademarks of Microsoft Corporation. Microsoft® is a registered trademark of Microsoft Corporation.

Any integrated Actuate product remains the property of Actuate.

License

The software is only for limited use. The software is subject to a limited, non-exclusive and non-transferable license of use, for the licensee's own internal business purpose only. The conditions and restrictions of such license are described in Lectra's end-user license conditions of use.

Guarantees

Lectra reserves the right to modify information relating to its products etc., without prior notification, with the aim of improving their reliability and operation.

Publication does not imply that this information is free of all intellectual copyright and does not grant any license over these rights. Furthermore, Lectra shall not be held liable for any consequences arising from the use of this information, for whatever purpose.

The performance measurements and other data referred to in this documentation are approximate and have no contractual value.

Contacts

Call Center Europe : [mailto: callcenter-europe@lectra.com](mailto:callcenter-europe@lectra.com)

Call Center North America : [mailto: Callcenter.Americas@lectra.com](mailto:Callcenter.Americas@lectra.com)

Call Center Asia Pacific : [mailto: callcenter.asia.pacific@lectra.com](mailto:callcenter.asia.pacific@lectra.com)

Call Center Italy : [mailto: callcenter.italia@lectra.com](mailto:callcenter.italia@lectra.com)

Call Center Spain : [mailto: callcenter.sp@lectra.com](mailto:callcenter.sp@lectra.com)



Conventions used in the document



Tip or suggestion



Note



Warning

Contents

1. General Overview	5
1.1 About	5
1.2 Aim of the document	5
1.3 Document conventions	5
1.4 LDAP Mode	6
1.5 LDAP authentication principles	6
1.6 Reminder of LDAP concepts and terminology	7
2. PDM LDAP Repository prerequisites	7
2.1 LDAP tree structure	7
2.2 LDAP access	9
2.3 Information needed by the PLM	9
2.4 Best practices	10
3. LDAP COonFIGURATION	12
3.1 LDAP Synchronizer	12
3.2 PLM Manager	14
4. Name: field of name in LDAPWLP LDAP Configuration	16
4.1 LDAP Configuration	16
4.2 Allowing user to authenticate on LDAP or in the Workflow Management	20
4.3 Restrictions	21
4.4 Enabling LDAP Synchronization FOR WLP modules	21
5. Synchronization	22
6. User Rights	22

1. GENERAL OVERVIEW

1.1 About

Lectra's PLM application authentication process relies on security data stored in the PLM database.

This data can be handled from the PLM Manager. With this tool users can be added or removed.

It may be problematic to handle users individually, e.g. during the PLM installation, with a significant amount of users to enter. PLM supports synchronization of authentication data from the LDAP repository with the PLM database.

From then on PLM can use authentication data (login, password, etc...) from an existing LDAP repository to connect to the PLM platform.

1.2 Aim of the document

The aim of the document is to describe how to configure a PLM solution so that it integrates perfectly with a LDAP repository for authentication process.

1.3 Document conventions



Note



Tips and hints



Warning

1.4 LDAP Mode

When the PLM works in LDAP mode, this information is stored in the AuthenticationConfig entity and can be accessed via the PLM Manager.

This configuration information is read from the database on start-up and is retained while the server is on. If this information is changed, the server has to be restarted to take it into account.

1.5 LDAP authentication principles

The basic principles of PLM integration with LDAP are:

LDAP is the master repository for authentication information, while PLM is servant.

The PLM does not change any data in the LDAP repository

In order to use the LDAP authentication mode, PLM needs to retrieve the security data from the LDAP repository to perform the authentication. This has to be done as simply and transparently as possible.

The objective is: provide a process which avoids any other action except the administration of the security data from the LDAP repository.

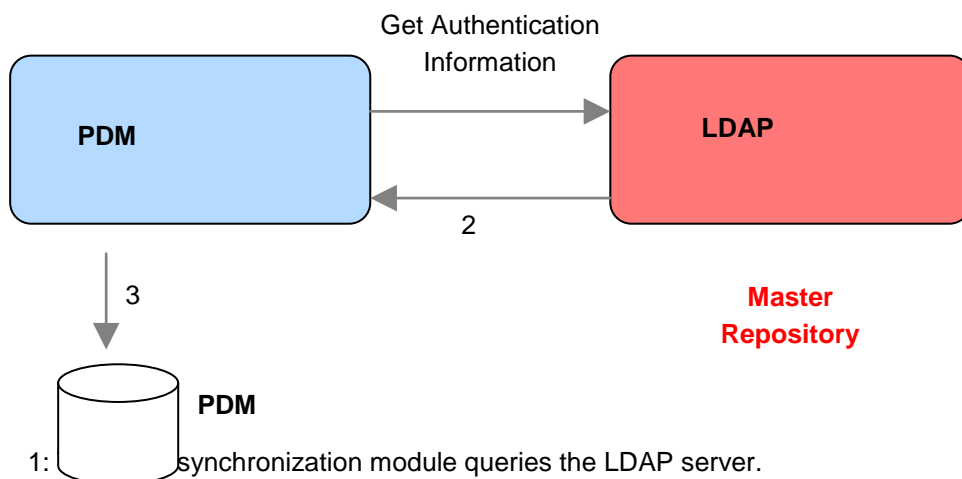
The proposed solution is to perform data synchronization from the PLM with dedicated PLM authentication data localized in a specific node of the LDAP tree. This will be carried out from the PLM Manager.

Adding new users to the PLM will be done by

Creation of the authentication data in the LDAP PLM-specific node,

Activation of the PLM synchronization.

From this point onwards authentication is carried out in the PLM via LDAP.



- 2: The LDAP server returns the list of groups and users listed in the Lectra relative sub tree.
- 3: PDM updates its database by creating/removing/updating security data.

1.6 Reminder of LDAP concepts and terminology

The aim of this section is to act as a reminder of LDAP basic principles.

1.6.1 Terminology

- cn : Common Name
- ou : Organisation Unit
- dn : Distinguished Name
- dc : Domain Component

1.6.2 Concepts

- cn=Joe Smith,ou=East,dc=MyDomain,dc=net. Full definition : distinguished name
- cn=Joe Smith. : Relative Distinguished Name of user "Joe Smith"
- dc=MyDomain,dc=com : DNS domain name (MyDomain.com)
- cn=Users Relative Distinguished Name of container "Users"
- ou=East Organizational Unit where user "Joe Smith" resides

1.6.3 API Example

```
objUser = GetObject("LDAP://aserver/cn=Joe,cn=users,dc=MyDom,dc=com")
```

2. PDM LDAP REPOSITORY PREREQUISITES

The aim of this section is to describe the PDM-dedicated LDAP repository.

2.1 LDAP tree structure

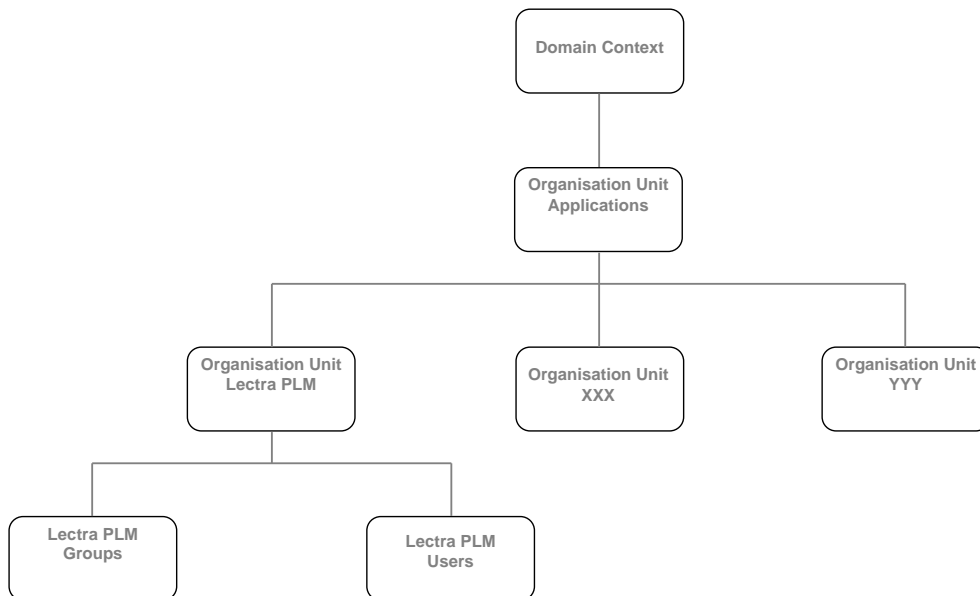
2.1.1 Groups and user location

To start with, PDM needs a specific location in the LDAP tree to get its specific security data. This ensures to cross only the part of the LDAP tree concerned by the synchronization.

Then, in the root PLM location (can be a 'Lectra' folder for instance), the users and the groups must be separately stored: one folder for users another one for groups.

The links between groups and other groups on one hand and between groups and users on the other are retrieved by using a specific attribute in the LDAP group entries, as described below.

Below an example of a LDAP tree structure that would be compliant with the synchronization needs.



2.1.2 Group entry structure

The synchronization is 'group-oriented'.

That means that the synchronization process in the following order :

group presents in the LDAP location

Inner groups and, lastly,

users, in a 'descending way'.

This forces each group entry in the PLM specific LDAP tree node to know its inner groups and its users. So each group entry must have an attribute containing the distinguished name (dn) of its inner groups and users, already created in the LDAP repository.

This attribute can be the same holding the dn of an inner group or the dn of a user: the dn is a LDAP location and, as mentioned earlier, users and groups are not stored in the same location in the LDAP tree.

Here an example of the structure of a group entry in the LDAP tree:

Attribute	Value
objectClass	groupOfUniqueNames

uniqueMember	cn=user1,ou=users,ou=lectraplm,ou=applications,dc=...
uniqueMember	cn=user2,ou=users,ou=lectraplm,ou=applications,dc=...
uniqueMember	cn=group2,ou=users,ou=lectraplm,ou=applications,dc=...
cn	group1

The uniqueMember attribute is used to hold all the group members. Here, group1 contains user1, user2 and the group group2.

2.1.3 User entry structure

A correct mapping must be done between user in PLM data structure and user LDAP entry. So, some specific data must be defined in the LDAP entries so that they can be mapped to in PLM data.

These used pieces of information are:

- name (i.e. login),
- password,
- email
- surname.

If the user PLM data structure changes, the mapping can be changed from the PLM Manager - Security Tool.

2.2 LDAP access

In order to get the data, the PLM must connect to the LDAP repository and so, must have an access with enough rights to read the data involved in the synchronization.

These data being localized in specific tree node, the needed rights are easy to determine.

The PLM has no vocation to change any data in the LDAP repository: the synchronization is performed from LDAP to the PLM. So no write rights are needed.

2.3 Information needed by the PLM

Once the LDAP repository is properly set up, the PLM needs also to be set up with specific information concerning locations of the data to retrieve. This must be provided in the PLM Manager, in the LDAP synchronization settings tab.

Information required is:

The name of the LDAP repository's host (eg ldapserver.eu.lectra.com)

The host port (eg 1528)

The Domain Name (dn) of the user the PLM will use to connect to LDAP with the password.

The users base Domain Name (dn) : different root locations where users to synchronize are stored.

The groups base Domain Name (dn): the root location where all groups to synchronize are stored.

The users and groups object classes that identify each data structure.

For groups data structure, the name of the attribute that all members of the group hold.

The mapping between users and groups LDAP data structure and users and groups PLM data structure: which attributes must be kept from the LDAP data structures to the PLM data structures.

If possible: a filter to identify the users or groups to synchronize.

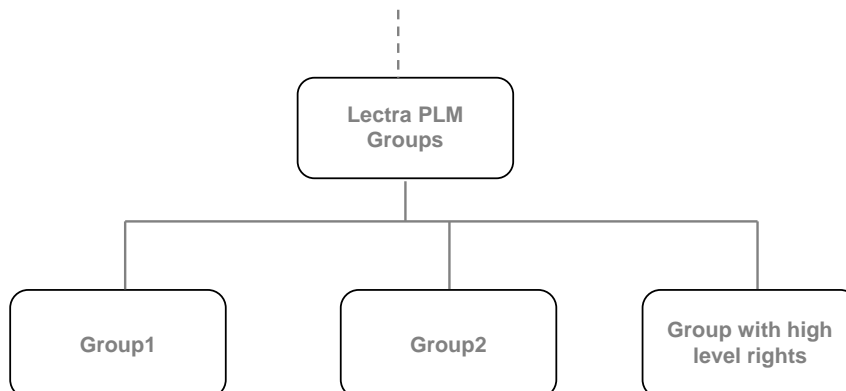
2.4 Best practices

2.4.1 Initial groups right policy

Performing the first synchronization will create the first groups and users in the PLM.

Rights have to be set for the different groups, setting a right access policy on PLM data. The rights allocation needs to be done by a user with sufficient privileges.

In addition to the group structure made by the repartition of different user profiles, you can create another group which will contain specific users authorized to allocate rights.



2.4.2 Multiple users base dn

Technical problems have arisen when requesting data contained in a directory too high in the LDAP tree (i.e.: containing too much data).

The problem occurred during synchronization while PLM synchronization module requested all users contained in the user base dn.

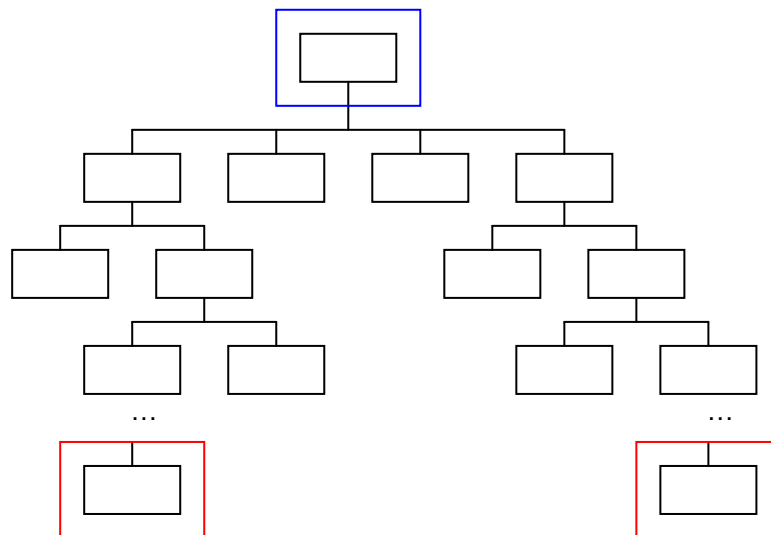
When this user base dn contains too much data, (too high up in the LDAP tree), the LDAP service returns an error. In addition, it is more efficient to do an accurate search and then use the more specific LDAP repertory as user base dn.

This may not always be possible: users may be located in different folders with potentially no parent directory in common or located very high in the tree.

That is why different user base dn's can be used.

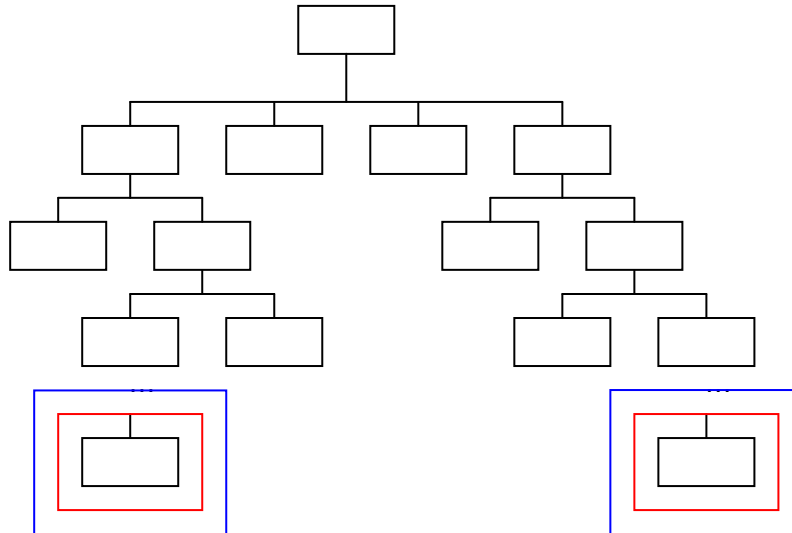
This avoids the problem of finding a convenient common parent directory for all directories containing PLM synchronizable users.

No more problems with too much data requested: base dn's used can be as accurate as possible. Possible case of unique base dn :



- folder containing synchronizable users
- ~~User~~ base dn

Solution with multiple base dn:



3. LDAP CONFIGURATION

3.1 LDAP Synchronizer

3.1.1 Overview

The LDAP synchronizer is a component belonging to the Fashion Integration Platform that is in charge of the PLM Synchronization with a LDAP repository.

LDAP Synchronizer module is generated at Enterprise Integration generation time.

Its role is to provide a way to use Windows to activate the LDAP Synchronization process on the FIP platform.

3.1.2 Contents

This ZIP file contains the following resources :

lib			Folder
ldapsynchronizer.jar	12 679	10 903	Executable Jar
ldapsynchro-config.jar	11 623	9 847	Executable Jar
runsynchro.bat	349	220	MS-DOS Batch
runconfig.bat	392	246	MS-DOS Batch

The lib folder contains all external libraries required for the LDAP synchronizer to work properly.

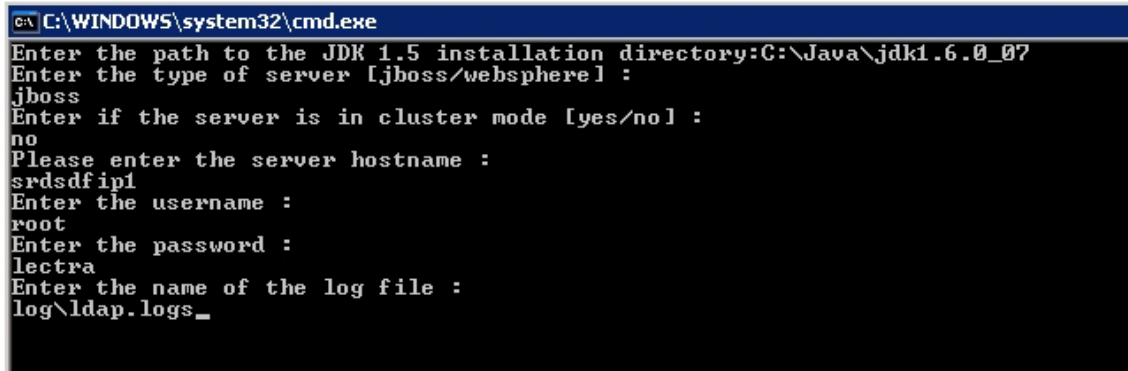
The runconfig.bat lets you specify the path of the JDK to use to run the LDAP Synchronizer

The runsynchro.bat is a script that actually starts the LDAP synchronization.

Process Configuration

The configuration is carried out running the runconfig.bat script.

This script requires some information to be entered in a command prompt as the following screenshot illustrates :



```
C:\WINDOWS\system32\cmd.exe
Enter the path to the JDK 1.5 installation directory:C:\Java\jdk1.6.0_07
Enter the type of server [jboss/websphere] :
jboss
Enter if the server is in cluster mode [yes/no] :
no
Please enter the server hostname :
srdsdfip1
Enter the username :
root
Enter the password :
lectra
Enter the name of the log file :
log\ldap.logs_
```

Once the log file is entered and the user presses Enter, the configuration is completed. The file conf\enterprise.properties is subsequently created :

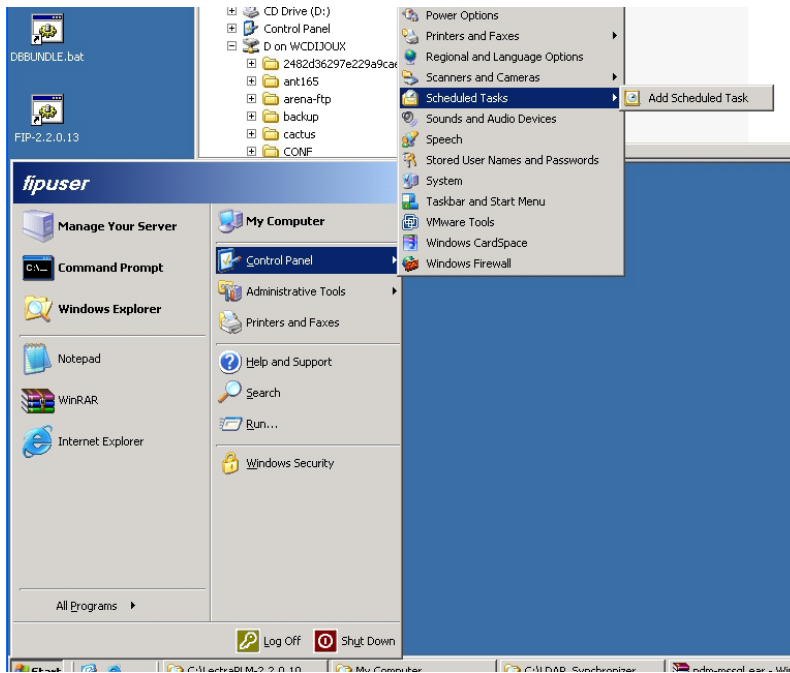
```
# written by PropertiesConfiguration
# Tue Dec 22 17:53:25 CET 2009
    conf.appserver = jboss
env.java.naming.provider.url = jnp://srdsdfip1:1099
conf.jndiname = ejb/EnterpriseHandler
conf.username = root
conf.password = bGVjdHJh
conf.filename = logs\ldap.log
```

This configuration will then be used each time the runsynchro.bat script is started to do the LDAP Synchronization.

3.1.3 Scheduling configuration

Usually, the LDAP Synchronizer is configured so that it runs periodically (e.g. daily).

This is configured in Windows server using the standard scheduler feature:



3.2 PLM Manager

Overview

The PLM Manager enables manual creation, deletion and editing of groups, users or rights. It is also used to allocate rights to users and groups.

In addition, LDAP configuration is also done from the PLM Manager

PLM Manager needs to be installed on an admin workstation.

On connection the basic connection is configured with the :

Server name e.g. srdsdfip1

User name

Password

3.2.1 Configuration

Once connected, the user needs to click on the Security Menu and Configure LDAP sub menu.

LDAP Editor opens.

At first, the server may not be configured with LDAP. The LDAP message appears in red: **No LDAP repository configured**

And in black : Last synchronization : Never

- Server configuration tab:

This tab allows configuring the server and the Authentication from LDAP

- Server Part

Server name (Or IP): Name or Ip of LDAP server

Server port: Port of LDAP server, default value is set to 389

LDAP protocol: Is the LDAP protocol: 'ldaps' for secured LDAP protocol, Otherwise 'ldap'.

- Authentication Part:

Method: the method of authentication: 'Authenticated connection' if use a LDAP user to connected LDAP, Otherwise use 'Anonymous connection'.

If 'Authenticated connection' is selected, LDAP user prefix, DN of reading user and Password are mandatory.

LDAP user prefix: prefix of user in LDAP

DN of reading user: path of user in LDAP

Password: user password in LDAP

- Users Mapping tab

The users mapping can be configured by clicking the Users Mapping tab.

LDAP object class: LDAP object to synchronize with PLM user

LDAP base DN: base DN of users in LDAP

- Synchronization parameters part

All objects that match the filter field are synchronized

- LDAP User Mapping part

It is the map between LDAP user and PLM user.

- Login: LDAP field used for Login
- First name: field of First name in LDAP
- Name: field of name in LDAP
- E-mail address: field of e-mail in LDAP

- Groups mapping tab

The groups mapping can be configured by clicking the Users Mapping tab.

LDAP object class: LDAP object to synchronize with PLM group

LDAP base DN: base DN of groups in LDAP

Membership attribute name: Membership attribute name in LDAP.

- Synchronization parameters part

All objects that match the filter field are synchronized.

- LDAP User Mapping part

It is the map between LDAP group and PLM group.

4. NAME: FIELD OF NAME IN LDAPWLP LDAP CONFIGURATION

This section details the LDAP configuration of the WLP modules (Workflow Management and Line Planning).

It is assumed that resources with the same resource ID as the user's LDAP ID have been defined in the WLP system.

4.1 LDAP Configuration

To set up WLP for LDAP Authentication (see screenshot above)

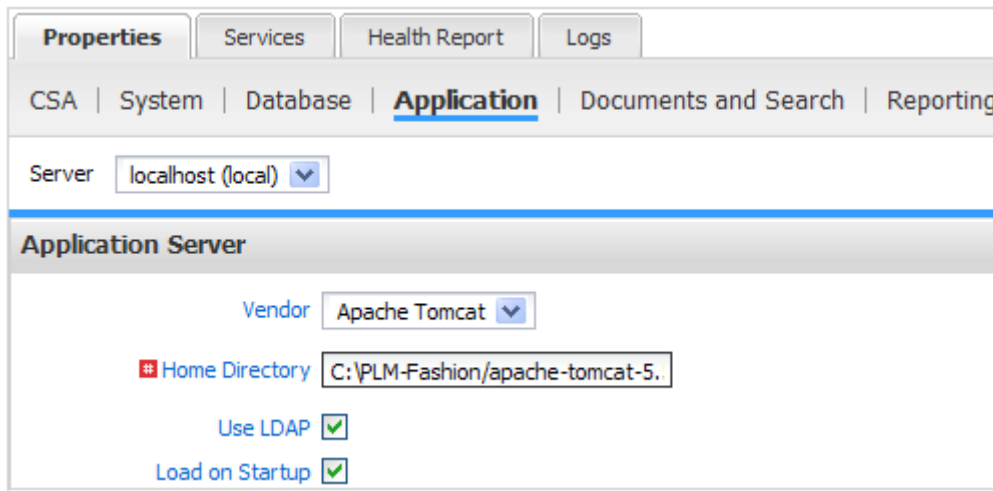
Make sure the WLP Administration service is running (Windows Service "Niku System Admin Server")

Log on into the WLP Administration application (<http://localhost/nsa>) (replace localhost by the name of the server on which the application has been installed.)

Select the server to configure (e.g. localhost)

Click the Application subtab

In the Application Server page, click Use LDAP. (This causes the system to authenticate using information on the LDAP server when users log in.)



The screenshot shows the 'Application Server' configuration page. At the top, there are tabs for 'Properties', 'Services', 'Health Report', and 'Logs'. Below these are navigation links for 'CSA', 'System', 'Database', 'Application' (which is selected), 'Documents and Search', and 'Reporting'. A 'Server' dropdown menu is set to 'localhost (local)'. The main section is titled 'Application Server' and contains the following settings:

- Vendor: Apache Tomcat
- Home Directory: C:\PLM-Fashion/apache-tomcat-5.
- Use LDAP:
- Load on Startup:

Click Save

Click the Security subtab.

In the LDAP Server page, in the URL, enter the LDAP server URL. Note: If your LDAP server is SSL-enabled, use the LDAPS protocol in the URL (rather than the default LDAP protocol).

For instance

“ldap://sdceuces01:389”; “ldap://172.16.35.107:19228”

In Root Context, enter the LDAP naming context

A few examples:

« OU=Employees,OU=Users,OU=Users
Groups,OU=FRA,OU=Subsidiaries,DC=eu,DC=lectra,DC=com »
« dc=eu,dc=lectra,dc=com »

In Search User, enter the username with the appropriate rights for binding to the LDAP server. Must be a fully qualified distinguished name of a LDAP user with read permission.

Examples:

« CN=Chollet Stéphane,OU=Employees,OU=Users,OU=Users
Groups,OU=FRA,OU=Subsidiaries,DC=eu,DC=lectra,DC=com »
« uid=w.zozo,ou=People,dc=eu,dc=lectra,dc=com »

In Password, enter the password; enter it again in Confirm Password.

In Search Filter, enter an optional search filter string (as defined in RFC 2254), except if you choose to use a Group Name (see below)

More information at: <http://www.faqs.org/rfcs/rfc2254.html>



If you choose to use a Group Name (see below), do not use the search filter.

In Date/Time Format, enter the date and time format used by the LDAP server.

For example for Novell eDirectory and IPlanet, use: yyyyMMddHHmmss'Z'

For MS Active Directory, use: yyyyMMddHHmmss'.0Z'

To enable group authentication, in Group Name, enter the group name. For instance:

« CN=WebSpace_Hermes_RW,OU=Sharepoint,OU=Access
Groups,OU=Subsidiaries,DC=eu,DC=lectra,DC=com »

Other example: « cn=PLM_admin,dc=eu,dc=lectra,dc=com »



If group name is specified, authentication and synchronization of users will be done for all users that are part of this group.

Then in Group Identifier, enter the group ID. The value is dependent on the directory server.

For Novell eDirectory and IPlanet, use: uniquemember

For MS Active Directory, use: member

In the section LDAP attribute mapping define the mapping between the WLP system and your Directory Server.

For instance username is often map to sAMAccountName or uid

Full name to display Name or cn

Check your LDAP system to define this mapping

To access the application using alternate authentication methods, check the Allow non-LDAP user's box.

Click Save

At this point your configuration is done and similar to one of the example below (Active Directory or iPlanet).



LECTRA FASHION PLM – LDAP INTEGRATION & SYNCHRONIZATION PROCESS Administration Guide

Properties Services Health Report Logs

CSA | System | Database | Application | Documents and Search | Reporting | **Security** | Background |

Server localhost (local) ▼

Encryption

SSL Keystore
SSL Password
Confirm Password
FIPS 140-2 Mode Enabled

Encrypt Passwords No Encryption
 Using System Key
 Using Custom Key File

Key File

LDAP Server

URL
Root Context
Search User
Password
Confirm Password
Batch Size

Object Class
Search Filter
Date/Time Format
Group Name
Group Identifier
Allow non-LDAP users

LDAP Attribute Mapping

Username
First Name
Last Name

Full Name
Email Address
Modify Time Stamp

Single Sign-on

Token Name
Token Type

Logout URL
Authentication Error URL

Stop and restart all services:

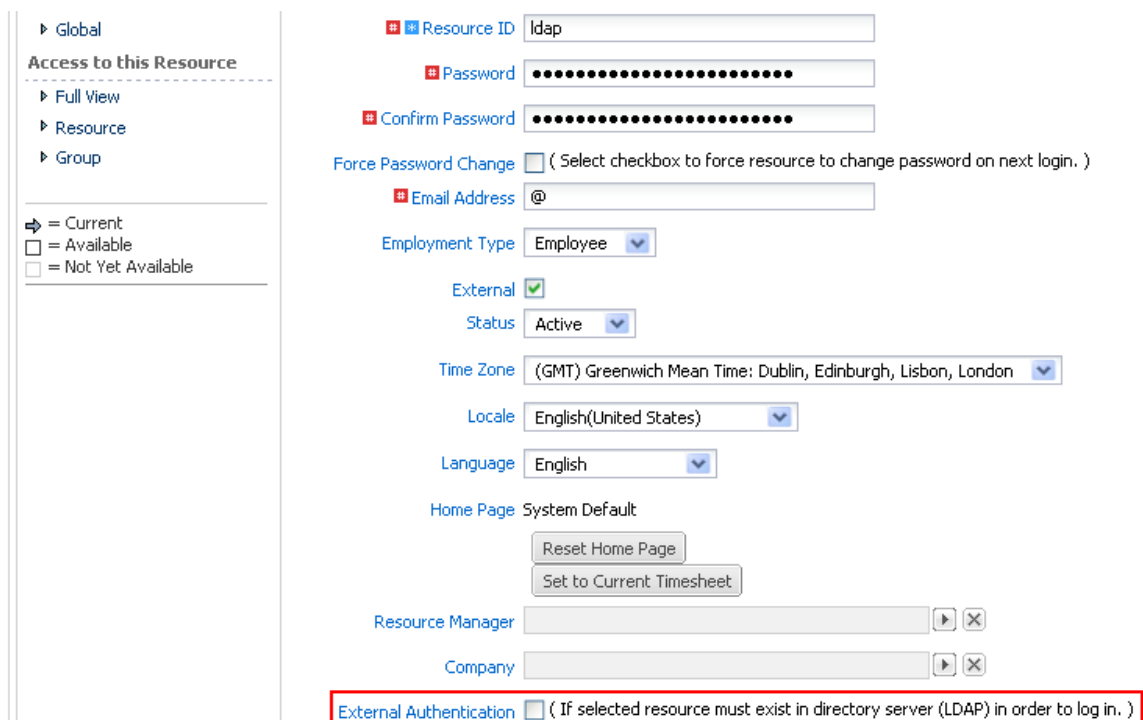
1. On the menu at the left, click All Services.
2. Click the All Services icon to check the box next to each service.
3. Click Stop then Start.

4.2 Allowing user to authenticate on LDAP or in the Workflow Management

If you selected the option “Allow non-LDAP user previously” you allow users defined in the Workflow Management module to authenticate directly in the system without using the LDAP repository.

To allow this you must uncheck the “External” Checkbox when defining a user.

External Authentication means: LDAP authentication.



The screenshot shows the user configuration interface. On the left, there is a navigation menu with 'Global', 'Access to this Resource', 'Full View', 'Resource', and 'Group'. Below the menu are three checkboxes: 'Current' (checked), 'Available', and 'Not Yet Available'. The main configuration area includes fields for 'Resource ID' (ldap), 'Password', 'Confirm Password', 'Force Password Change' (unchecked), 'Email Address' (@), 'Employment Type' (Employee), 'External' (checked), 'Status' (Active), 'Time Zone' ((GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London), 'Locale' (English(United States)), 'Language' (English), 'Home Page' (System Default) with 'Reset Home Page' and 'Set to Current Timesheet' buttons, 'Resource Manager', and 'Company'. At the bottom, the 'External Authentication' checkbox is unchecked and highlighted with a red box, with the text '(If selected resource must exist in directory server (LDAP) in order to log in.)' next to it.

4.3 Restrictions

The Workflow Management module supports the use of only one LDAP Domain and a LDAP group that is not "nested".

4.4 Enabling LDAP Synchronization FOR WLP modules

In addition to LDAP authentication, the WLP system supports one-way synchronization with an LDAP server. In this configuration, information from the directory server is synchronized with the WLP database. No information (including first, last names and email addresses) is sent from the WLP system to the directory server.

4.4.1 Configuration

To synchronize the LDAP and WLP servers:

- Log into WLP Application (<http://localhost/niku>) with administration rights (you must be able to view and execute Jobs).
- On the menu at the left, under Personal, click Reports and Jobs.
- Click the Jobs tab.
- In the Available Job Filter page, in Job Type, enter "LDAP", and then click Filter.
- Choose one of the following jobs:
 - To create users in WLP that have been newly created in the LDAP directory server, click LDAP - Synchronize New and Changed Users.
 - To deactivate users in WLP that have been removed from the directory server, click LDAP - Synchronize Obsolete Users.
- If you only want to synchronize the servers once, check the box next to Immediate and skip to step 8.
- To set up a synchronization job that runs on a recurring basis:
 - Check the box next to Scheduled.
 - (Optional) If you want to set up a schedule and also have the job run immediately, also check the box next to Immediate.
 - In Start Date, click the calendar icon and select the first day you want the job to run. If you selected Immediate above, select today's date.
 - In Start Time, select the time to start the job each time it runs.
 - Click Set Recurrence.
 - To have the job run weekly, click Weekly, then check the box next to the day of the week you want the job to run. If desired, select the months you want the job to run. In Recur Until select the last date you want the job to run.
 - To have the job run monthly, click Monthly, then enter the date you want the job to run each month. If desired, select the months you want the job to run; in Recur Until select the last date you want the job to run.

- To set the job frequency using a Unix crontab-like format, click Use UNIX crontab entry format and then enter the crontab parameters.
- Click Submit.

4.4.2 Checking the LDAP synchronization logs

Logs about the LDAP synchronization are available in the folder `niku_home/logs/ldapsync` where `niku_home` is where you choose to install the WLP system (recommended path: `c:\lectra\plm\clarity`)

- Log files related to New and Changed Users jobs are:
- `ldapusers_nm_*.xml`: List of users found in the directory server to be synchronized with Clarity.
- `ldapsync_nm_*.xml`: List of Success/Error/Warning messages for this sync job.
- Log files related to Synchronize Obsolete Users job are:
- `ldapusers_ia_*.xml`: List of users to be inactivated in WLP.
- `ldapsync_ia_*.xml`: List of Success/Error/Warning messages for this sync job.

5. SYNCHRONIZATION

Once the configuration is completed, you must restart the server for the configuration changes to be taken into account.

If you change the configuration, you must reenter the password and you must restart the server.

Once the server has been restarted, you can open the PLMManager to:

- Check your LDAP connection, by opening LDAP configuration Security menu, configure LDAP sub menu.
- Test LDAP connection by clicking on Test button
- Synchronize by clicking on Synchronize button to activate the synchronization.

6. USER RIGHTS

After synchronize, you must define rights in the PLMManager for users and groups.