

The page features several decorative squares of varying sizes and colors (blue and grey) scattered across the background. The largest blue square is in the top left corner. Other blue squares are located in the middle left, bottom right, and bottom center. Grey squares are located in the middle left and middle right.

LDAP Change Password Channel Configuration Guide

Contents

1.0 Introduction.....	4
1.1 What is the LDAP Change Password Channel?	4
2.0 Configuration	5
2.1 Publishing the Channel	5
2.2 OpenLDAP Example.....	6
2.3 Active Directory Example	6

1.0 Introduction

1.1 What is the LDAP Change Password Channel?

The LDAP Change Password channel allows portal administrators to easily give LDAP or Active Directory users the ability to change their password on the LDAP or Active Directory server. The channel is not published by default but is included with the base Academus installation.

2.0 Configuration

2.1 Publishing the Channel

The LDAP Change Password channel is configured completely by its publishing parameters. This allows you to publish multiple instances of the channel if needed (for example, if you have two distinct LDAP servers you are authenticating against). Additionally, no property files have to be adjusted and the portal does not need to be restarted after the channel is published. The standard publishing parameters for this channel are as follows:

Channel Type: Custom
 Channel Title: LDAP Change Password
 Channel Name: LDAP Change Password
 Channel Functional Name: ldap-change-password
 Channel Description: A channel to allow users to change their LDAP passwords
 Channel Timeout: 20000
 Channel Secure: No
 Channel Class: net.unicon.portal.channels.ldapchangepw.CLdapChangePW

There are a number of channel publishing parameters that allow you to customize the behavior of this channel. These have been described in the table below:

Parameter	Description	Example
LDAPHost	This is the URL to the LDAP/Active Directory server.	For an OpenLDAP over an unencrypted connection: ldap://niobe.unicon.net:389 For an Active Directory over SSL. Idaps://deploy1.unicon.net:636
LDAPBaseDN	This is the base DN to authenticate against. This is the container under which users will be searched for. Users that exist above this container will not be found.	CN=Users,DC=uniconsystest
LDAPUser	This is the user the channel will use to make password changes. This user must have the ability to change a password on the LDAP server.	CN=Tom Dinchak, CN=Users, DC=uniconsystest
LDAPPass	This is the password for the user specified by LDAPUser.	Example: secret
isSSL	Is the channel connecting to LDAP/Active Directory over SSL? "yes" or "no" (if not specified the default is "no"). Note: This should always be "yes" for Active Directory.	
isActiveDirectory	Are we connecting to an Active Directory? "yes" or "no" (if not specified the default is "no").	
hashType	This is the hash format of user passwords in LDAP. Valid settings are "SHA-1" or "none" (if not specified the default is "SHA-1"). The "none" setting will not hash the passwords and they will be stored in plain text. This can be expanded to support more formats (MD5, etc). Note: this is only used with LDAP, not with Active Directory.	
askForCurrent	Should we ask for the user's current password before authorizing the password change? "yes" or "no" (if not specified the default is "no").	

2.2 OpenLDAP Example

The example configuration below will work with an OpenLDAP server or any LDAP server that uses OpenLDAP's method of password management:

```
LDAPHost:          ldap://niobe.unicon.net:389
LDAPBaseDN:        dc=unicon,dc=net
LDAPUser:           cn=Manager,dc=unicon,dc=net
LDAPPass:          secret
isSSL:             no
isActiveDirectory: no
hashType:          SHA-1
askForCurrent:     yes
```

2.3 Active Directory Example

The example configuration below will work with an OpenLDAP server or any LDAP server that uses OpenLDAP's method of password management:

```
LDAPHost:          ldaps://niobe.unicon.net:636
LDAPBaseDN:        dc=unicon,dc=net
LDAPUser:           cn=Manager,dc=unicon,dc=net
LDAPPass:          secret
isSSL:             yes
isActiveDirectory: yes
askForCurrent:     yes
```

Note that the hashType parameter is not used in Active Directory configuration. Also, Active Directory has fairly strict requirements on who can change passwords. You must connect to the Active Directory server over SSL (ldaps protocol) as a domain administrator account, or an account that has the proper rights to change a user's password. Additionally, you will have to import the Active Directory server's SSL certificate into Academus' JVM keystore.