QuercusPlus 2.5
LDAP Adapters

Configuration Guide

Published: 11th April 2008

DOCUMENT HISTORY

Version	Date	Author	Description
1.0	11-04-2008	Jan Navratil	Document created

TABLE OF CONTENTS

1 SUMMARY

1.1 Scope

- This technical document describes how to configure QuercusPlus LDAP Adapters for industry leading LDAP servers.

1.2 Audience

- Application administrator / DBA
    - To install, configure and maintain the software
    - Administrative experience with preferred LDAP server and Oracle Database is required
- Integration architects
    - To help when designing institution wide identity management solution
    - Detail understanding of the LDAP technology is assumed

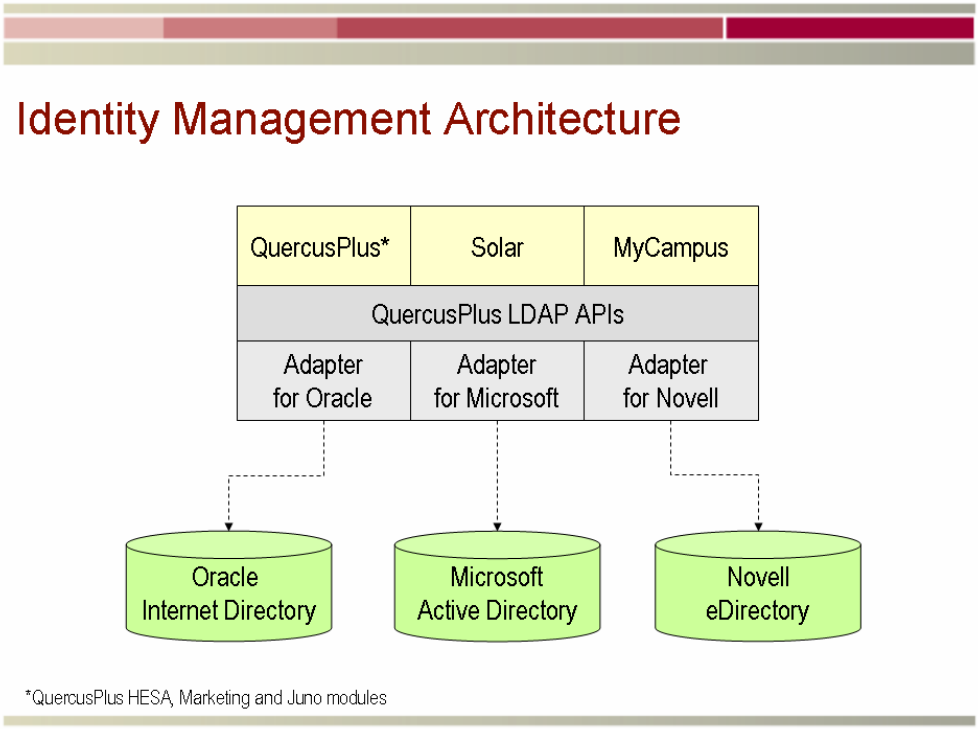
1.3 Additional Documentation

- CampusIT Data Sheet: Identity Management (February 2008)
    - Summarizes Benefits and features of the solution
- CampusIT Release Notes
    - SU1271 – to install the QuercusPlus patch
- QuercusPlus Identity Management Configuration Guide
    - This document – how to configure adapters

1.4 Architecture Overview

The architecture is based on set of authentication and authorization API introduced initially in QuercusPlus version 2.0. This API is used across all CampusIT solutions including Solar and is delegating authentication and authorization services to the Oracle Internet Directory.

Additional logical layer of Adapters was introduced as part of the API to handle specific requirements of each identity management system repository. The API itself has not been changed: All applications can immediately take advantage of new features without any upgrades.



The mechanism to link user account in Oracle Internet Directory with records in QuercusPlus system has been improved to be both more flexible and robust. Traditionally QuercusPlus person ID Number was the only attribute to link QuercusPlus with Oracle Internet Directory. New solution allows to use any unique identifier as a link (Person ID Number is still the default option). Even when person ID number is used to establish the link subsequent changes to the ID in QuercusPlus would not cause link to become broken.

1.5 Limitations

- Please note end user accounts for CampusIT QuercusPlus Backoffice (Forms) and Oracle Discoverer can be integrated only with Oracle Identity Directory using Oracle Single Sign On.
- This configuration is not discussed in this document (Oracle SSO).

2 PREREQUISITES

2.1 Components

- CampusIT QuercusPlus 2.5.0.4 or higher (patch SU1271)
- Identity Management Adapters Configuration Scripts (SU1308)
- Oracle Database[1] 10g Release 1 or Release 2 (with the latest patch[2])
- One of following identity management repositories (LDAP)
    - Oracle Internet Directory 10g Release 1 or Release 2
    - Microsoft Active Directory 2000 or 2003
    - Novell eDirectory version 8.8

2.2 Accounts/passwords

- Quercus database (QUERCUS)
- Administrative account on the LDAP server
- Privileges to create or modify Oracle Wallet (only for SSL communication)

2.3 Skills[3]

- Oracle database administration (including Oracle Wallet for SSL)
- Administration of selected LDAP server (Oracle, Microsoft, Novell)

[1] Running on the Microsoft Windows, Sun Solaris or Linux operating systems. This guide assumes MS Windows so please make relevant alternations where appropriate (file paths).

[2] Latest Oracle database patch is strongly recommended as there are known issues with LDAP operations over SSL with initial versions. The latest database patches are 10.1.0.5 respective 10.2.0.3+ at time of writing of this document.

[3] CampusIT can provide technical consultancy to speed-up the implementation.

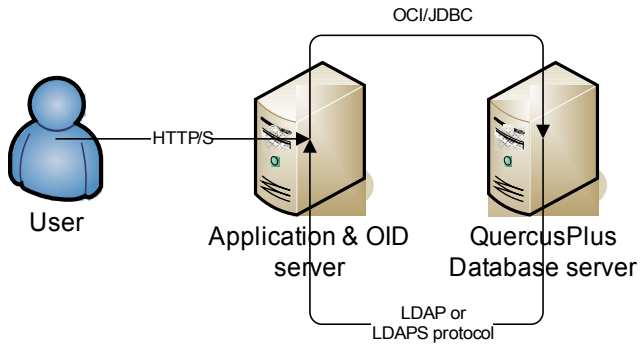
3 Configuration Overview

3.1 Connection between database and LDAP server

- New enhancements and features (identity management adapters) allow configuring identity management to support various requirements.
- The purpose of this section is demonstrating some of them.

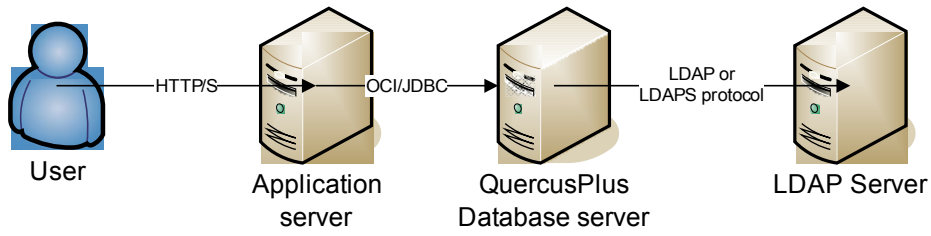
3.1.1 Simple deployment with an Oracle Internet Directory

- The first figure represents the simplest possible scenario when CampusIT solution is deployed on the LAN.
- The Oracle Application server acts as both HTTP and LDAP server.



3.1.2 Simple deployment with non Oracle LDAP server

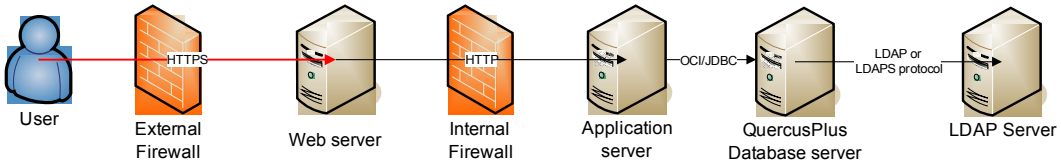
- Alternation of previous figure when there is dedicated server for LDAP server – typical situation when Microsoft Active Directory or Novell eDirectory servers are used.



3.1.3

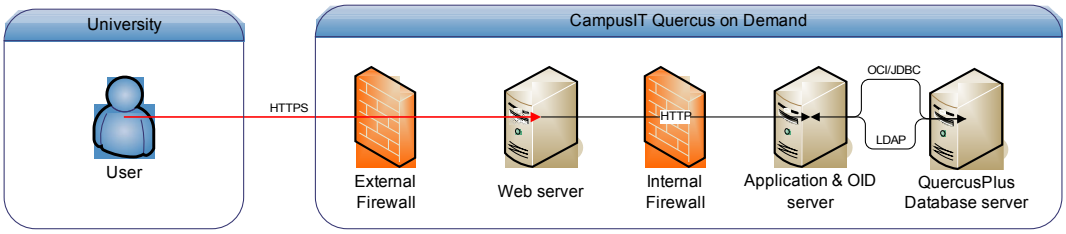
3.1.4 Advanced deployment with non Oracle LDAP server

- More complex situation when CampusIT solution is made available over the Internet.
- Please note LDAP server is not exposed on the internet.



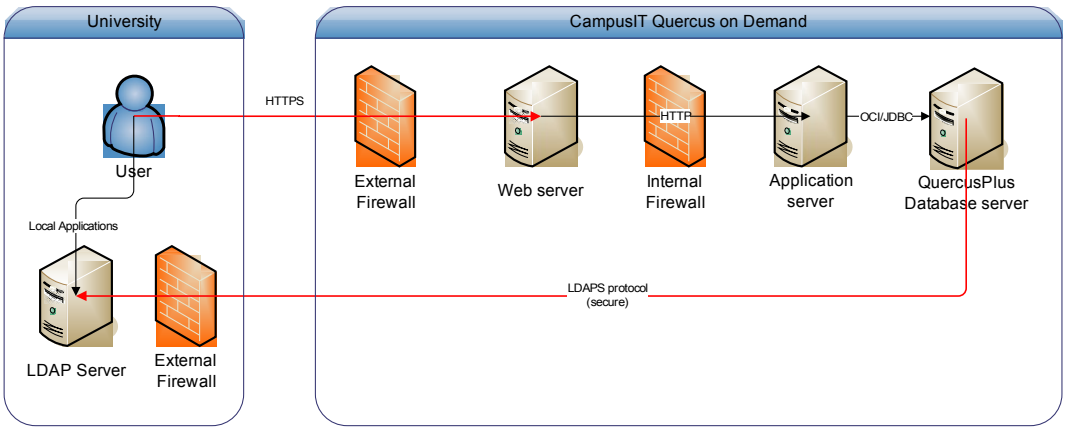
3.1.5 Quercus on Demand (standard deployment)

- This scenario represents institution using CampusIT solution as a hosted service. Identity management is part of hosted solution.



3.1.6 Quercus on Demand with Local identity management system

- This scenario represents institution using CampusIT solution as a hosted service however fully integrated with their own (local) identity management system.
- Communication over Internet is always secure (SSL).

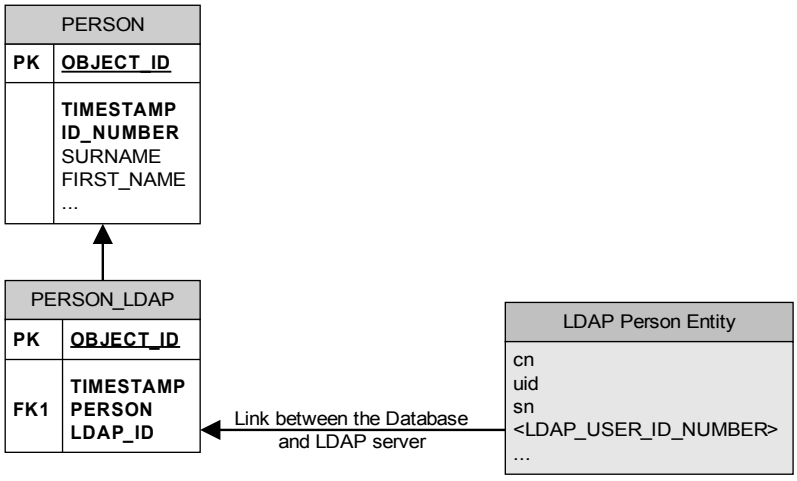


3.2 Association between QuercusPlus and LDAP records

- Once physical connectivity is established as discussed in 3.1 the logical link between database records and user credentials needs to be established using unique user identifier.

3.2.1 Data model

- The link between database and LDAP server is based on unique LDAP_ID person identifier.
- This unique ID is attached to every PERSON in the Quercus database thru PERSON_LDAP table.
- The PERSON_LDAP.LDAP_ID is automatically populated when new PERSON record is created with the value of PERSON.ID_NUMBER
- The LDAP_ID is not changed when ID_NUMBER is subsequently changed in QuercusPlus.
- The same value must be defined as part of LDAP Person Entity. The name of the LDAP attribute is typically “employeenumber”. The name of this attribute can be customized by LDAP Adapter parameter.
- It is possible to use other unique LDAP attributes (like “uid”) to link records as LDAP_ID is defined as VARCHAR2(30). In this situation additional mechanism must be implemented to populate (update) LDAP_ID when new person is created.



3.3 LDAP Adapters API

- The Adapters are implemented in following QuercusPlus baseline objects
    - Package OC_LDAP
      Low level procedures to communicate with a LDAP server
    - Package OC_LDAP_USER
      User centric functionality to authenticate, authorize and retrieve details about the user from the LDAP server
    - Package OC_PARAM
      To manage parameters required for API and LDAP adapters
- The API including specific LDAP Adapters is part of CampusIT QuercusPlus baseline so there is no additional installation required when any mentioned functionality is to be used for the first time – apart of the configuration steps discussed later in this document.
- Note: Please note QuercusPlus LDAP adapters for Microsoft and Novel requires special licence and support agreement with CampusIT prior using in the production environment.

3.4 Understanding Security

- Standard LDAP communication protocol is not encrypted. This represents potential risk during user authentication as password is transferred as a plain-text over the network.
- When connection between database and LDAP server is over un-trusted network (like Internet) it's mandatory so use encryption to maintain appropriate security level.
- LDAPS (secure LDAP) protocol is using common SSL technology based on server certificate to encrypt all communication between LDAP server and application.
- Please keep in mind establishing SSL connection is relatively time consuming operation. The negative performance impact is however minimalized as CampusIT applications are caching attributes retrieved from the LDAP for user session duration.
- Following simplified figure illustrates the situation
    - User → Application (not discussed in this document)
    - Application → LDAP

3.5 Tools

- It's assumed administrator is familiar with native management tools for used Identity management system.
- CampusIT can also recommend open source tool "LDAP Browser and Editor" http://www-unix.mcs.anl.gov/~gawor/ldap/

4 Oracle Internet Directory

- This chapter is step-by-step guide to setup OID as your identity management system.
- If you are already using OID as your identity management system you probably don't make any changes to the configuration at all.
- You may however want to enable SSL communication (see Step 5).

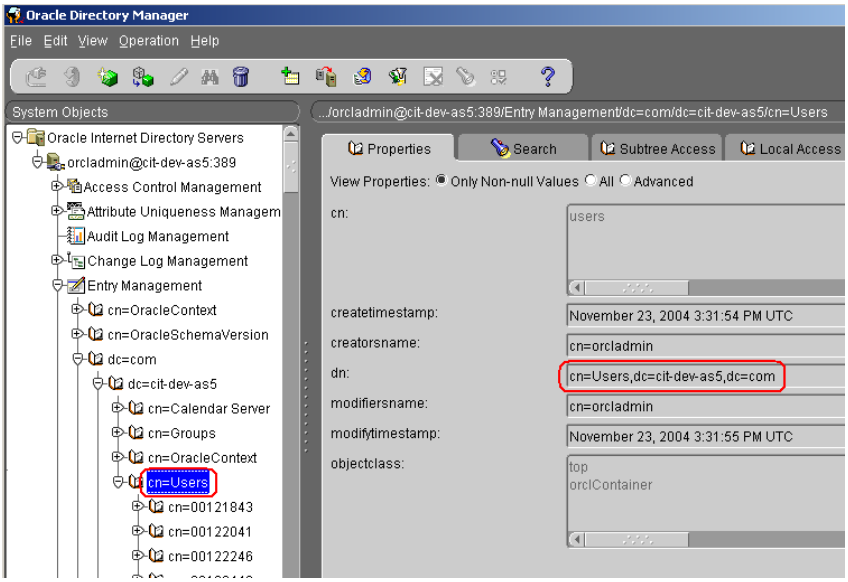
4.1 Connection between database and OID server

4.1.1 Step 1 – Collect required details

- All LDAP parameters can be viewed and managed using Solar Control Centre however initial setup must be done using command line as you can't login into the Solar control centre before initial LDAP setup is completed.
- Please make sure you have and understand the following details for your environment

Parameter	Sample of value	Description
LDAP_SERVER_HOST	myldapserver	Host name of the LDAP server
LDAP_SERVER_PORT	389	Port number of the LDAP server (common values are 389 or 636)
LDAP_USER_BASE	cn=Users,dc=university,dc=org	User search base in the LDAP It's specific to each installation of Oracle Application Server
LDAP_USER_ID_NUMBER	employeenumber	Name of property in LDAP user profile holding ID (link to PERSON_LDAP.LDAP_ID)
LDAP_GROUP_BASE	cn=Groups,dc=university,dc=org	Group search base in the LDAP It's specific to each installation of Oracle Application Server
LDAP_ADMIN_USER_NAME	cn=orcladmin	User name of an LDAP admin account. Leave blank when LDAP server doesn't require authentication (see step 4).
LDAP_ADMIN_PASSWORD	password	Password of the LDAP admin
LDAP_WALLET	file:d:\wallet	Location of Oracle Wallet (e.g. "file:d:\wallet"). Leave blank when SSL communication is not required.
LDAP_WALLET_PASSWORD	password	Password for the Oracle Wallet

- You can use Oracle Directory Manager to find LDAP_USER_BASE & LDAP_GROUP_BASE



4.1.2 Step 2 – Check Network connectivity

	Step	Description
1	Make sure the LDAP server is accessible from the database server on specified port	
2	Windows C:\> telnet myldapserver 389 Unix [oracle@cit-dev-db1 ~]$ telnet 192.168.62.156 389 Trying 192.168.62.156... Connected to 192.168.62.156. Escape character is '^]'.	You can use any LDAP tool to test the connectivity Make sure you are running the test from the database server!
3	If connection fails you have to investigate if LDAP server is running and/or your network configuration allows connection from the database server	

4.1.3 Step 3 – Basic configuration

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_set_oracle	
3	Enter LDAP parameters when prompted	LDAP_SERVER_HOST LDAP_SERVER_PORT LDAP_USER_BASE LDAP_GROUP_BASE
4	Run the basic diagnostic script: SQL> @ldap_ping	
5	Ping LDAP server (myldapserver:389) SSL mode is OFF **Connected !** OK	The response should look like this.
6	The configuration of the Oracle OID LDAP Adapter is now completed and it's ready for use. It's however recommended to complete the harness test as mentioned in Step 6	

4.1.4 Step 4 – Admin account credentials (optional)

- This step can be skipped in most cases as it is required only when you
  - Use automated user account creation functionality as part of Solar services. Please contact CampusIT is you are not sure.
  - Configure OID to block anonymous searches (default option allows anonymous searches)
- You don't have to use super user admin account (cn=oracle). You can create special admin account with privileges limited to user account management in the specified LDAP User Base.

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_admin	
3	Enter LDAP parameters when prompted	LDAP_ADMIN_USER_NAME LDAP_ADMIN_PASSWORD
4	Run the basic diagnostic script: SQL> @ldap_ping	
5	Ping LDAP server (myldapserver:389) SSL mode is OFF **Connected !** **Authenticating user (cn=orcladmin)** **Authenticated !** OK	The response should look like this.

4.1.5 Step 5 – Enabling secure communication (optional)

- The SSL is not enabled by default on Oracle Internet Directory. It's required to enable it on the server first and then configure QuercusPlus.

	Step	Description
1	Activate SSL on the Oracle Internet Directory server	See Oracle Metalink Note 315847.1 "Configuration and Test of OID with SSL"
2	Copy certificate of the certification authority used to generate your SSL certificate for OID into database Oracle Wallet as a Trusted certificate. Make sure you save the certificate in the "Base-64 encoded X.509" format prior importing into Oracle Wallet Manager.	Oracle Wallet Manager
3	Login to the QuercusPlus database as a QUERCUS user	
4	Run the script: SQL> @ldap_enable_ssl	
5	Enter LDAP parameters when prompted	LDAP_SERVER_PORT LDAP_WALLET LDAP_WALLET_PASSWORD
6	Run the basic diagnostic script: SQL> @ldap_ping	
7	Ping LDAP server (myldapserver:636) **SSL mode is ON** **Connected !** OK	The response should look like this.

4.1.6 Step 6 – Final end-to-end test (harness)

- Before running this test make sure you have user created in an LDAP Directory with all required attributes as listed in 3.2
- You can also test membership of user in the group

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_test	
3	Enter LDAP parameters when prompted	USER_NAME USER_PASSWORD USER_GROUP
4	============================ == User record as in LDAP == ============================ DN = cn=joe.blog,cn=users,dc=cit-dev-as5,dc=com First Name = Joe Surname = Blog Email = joe.blog@mail.com User ID = 1987578 Authenticated = YES Group Member = YES	The results should look like These details should match values you entered when you have created the user in OID.
6	Congratulations ! You have successfully completed configuration of Oracle Internet Directory LDAP Adapter.	Feel free to contact CampusIT to provide technical assistance when you run into any difficulties with this configuration.

5 Microsoft Active Directory

5.1 Connection between database and MS AD server

5.1.1 Step 1 – Collect required details

Please consider following unique features and limitations:

5.1.1.1 MS AD schema doesn't have "employeenumber" attribute

You need to decide what identifier will be used to link to Quercus records:

- If you wish to use QuercusPlus LDAP ID you need to extend your LDAP schema with a new attribute to store the value of PERSON_LDAP.LDAP_ID
- If you prefer to use existing unique keys in MS AD as a link (e.g. "sAMAccountName") you would need to update records in PERSON_LDAP table as illustrated in section 3.2 of this guide.
- The name of the LDAP attribute is stored in QuercusPlus as the LDAP_USER_ID_NUMBER parameter.

5.1.1.2 Anonymous searches are not allowed

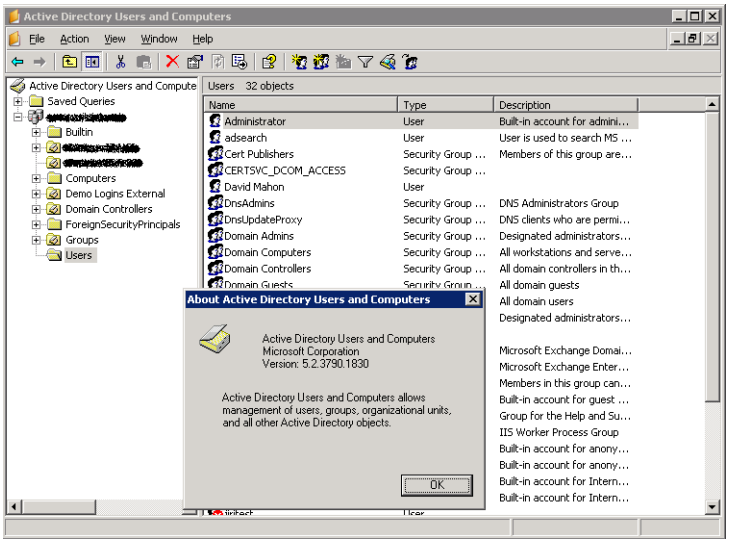
- MS AD doesn't allow searches with anonymous connection.
- You would need to provide credentials for LDAP_ADMIN to allow QuercusPlus LDAPAdapter to work.
- You can create dedicated system user account in MS AD for this purpose with limited priviledges (read-only).

- Please make sure you have and understand the following details for your environment

Parameter	Sample of value	Description
LDAP_SERVER_HOST	myldapserver	Host name of the LDAP server
LDAP_SERVER_PORT	389	Port number of the LDAP server (common values are 389 or 636)
LDAP_USER_BASE	CN=Users,DC=university,DC=org	User search base in the LDAP
LDAP_USER_ID_NUMBER	myuseridattribute	Name of property in LDAP user profile holding ID (link to PERSON_LDAP.LDAP_ID)
LDAP_GROUP_BASE	CN=Groups,DC=university,DC=org	Group search base in the LDAP It's specific to your Microsoft Active Directory installation

LDAP_ADMIN_USER_NAME	CN=ADSearch,CN=Users,DC=university,DC=org	MS Active Directory does require authentication even for searches in the directory by default.
LDAP_ADMIN_PASSWORD	Password	Password of the LDAP admin
LDAP_WALLET	file:d:\wallet	Location of Oracle Wallet (e.g. "file:d:\wallet") on the database server. Leave blank when SSL communication is not required.
LDAP_WALLET_PASSWORD	password	Password for the Oracle Wallet

- You can use “Microsoft Active Directory Users and Computers” console to find LDAP_USER_BASE & LDAP_GROUP_BASE



5.1.2 Step 2 – Check Network connectivity

	Step	Description
1	Make sure the LDAP server is accessible from the database server on specified port	
2	Windows C:\> telnet myldapserver 389	You can use any LDAP tool to test the connectivity Make sure you are running the test from the database server!
3	If connection fails you have to investigate if LDAP server is running and/or your network configuration allows connection from the database server	

5.1.3 Step 3 – Basic configuration

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_set_microsoft	
3	Enter LDAP parameters when prompted	LDAP_SERVER_HOST LDAP_SERVER_PORT LDAP_USER_BASE LDAP_GROUP_BASE LDAP_USER_ID_NUMBER LDAP_ADMIN_USER_NAME LDAP_ADMIN_PASSWORD
4	Run the basic diagnostic script: SQL> @ldap_ping	
5	Ping LDAP server (myldapserver:389) SSL mode is OFF **Connected !** **Authenticating user (CN=ADSearch,CN=Users, DC=university,DC=org)** **Authenticated !** OK	The response should look like this.
6	The configuration of the Microsoft Active Directory Adapter is now completed and it's ready for use. It's however recommended to complete the harness test as mentioned in Step 6	

5.1.4 Step 4 – Enabling secure communication (optional)

- The SSL communication is not enabled by default on Microsoft Active Directory Server. Oracle Internet Directory.
- It's required to enable it on the server first and then configure QuercusPlus LDAP Adapter.

	Step	Description
1	Activate SSL on the Microsoft Active Directory server	See Microsoft Knowledge Base document **247078** "How To Enable Secure Socket Layer (SSL) Communication over LDAP for Windows 2000 Domain Controllers"
2	Copy certificate of the certification authority used to generate your SSL certificate for MS AD into database Oracle Wallet as a Trusted certificate. Make sure use save the certificate in the "Base-64 encoded X.509" format prior importing into Oracle Wallet Manager.	Oracle Wallet Manager
3	Login to the QuercusPlus database as a QUERCUS user	
4	Run the script: SQL> @ldap_enable_ssl	
5	Enter LDAP parameters when prompted	LDAP_SERVER_PORT LDAP_WALLET LDAP_WALLET_PASSWORD
6	Run the basic diagnostic script: SQL> @ldap_ping	
7	Ping LDAP server (myldapserver:636) **SSL mode is ON** **Connected !** OK	The response should look like this.

5.1.5 Step 5 – Final end-to-end test (harness)

- Before running this test make sure you have user created in an MS AD with all required attributes as listed in 3.2
- You can also test membership of user in the LDAP group

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_test	
3	Enter LDAP parameters when prompted	USER_NAME USER_PASSWORD USER_GROUP
4	============================ == User record as in LDAP == ============================ DN = cn=test1,cn=users,dc=university, dc=org First Name = Joe Surname = Blog Email = test1@mail.com User ID = 1987578 Authenticated = YES Group Member = YES	The results should look like These details should match values you entered when you have created the user in MS AD.
5	Congratulations ! You have successfully completed configuration of Microsoft Active Directory LDAP Adapter.	Feel free to contact CampusIT to provide technical assistance when you run into any difficulties with this configuration.

6 NOVELL E-DIRECTORY

This chapter is step-by-step guide to setup NED as your identity management system.

6.1 Connection between database and NED server

6.1.1 Step 1 – Collect required details

- All LDAP parameters can be viewed and managed using Solar Control Centre however initial setup must be done using command line as you can't login into the Solar control centre before initial LDAP setup is completed.
- Please make sure you have and understand the following details for your environment

Parameter	Sample of value	Description
LDAP_SERVER_HOST	myldapserver	Host name of the LDAP server
LDAP_SERVER_PORT	389	Port number of the LDAP server (common values are 389 or 636)
LDAP_USER_BASE	CN=Users,O=university	User search base in the LDAP It's specific to each installation of Oracle Application Server
LDAP_USER_ID_NUMBER	employeenumber	Name of property in LDAP user profile holding ID (link to PERSON_LDAP.LDAP_ID)
LDAP_GROUP_BASE	CN=Groups,O=university	Group search base in the LDAP It's specific to each installation of Oracle Application Server
LDAP_ADMIN_USER_NAME	CN=admin,O=university	User name of an LDAP admin account. Leave blank when LDAP server doesn't require authentication (see step 4).
LDAP_ADMIN_PASSWORD	Password	Password of the LDAP admin
LDAP_WALLET	file:d:\wallet	Location of Oracle Wallet (e.g. "file:d:\wallet"). Leave blank when SSL communication is not required.
LDAP_WALLET_PASSWORD	password	Password for the Oracle Wallet

6.1.2 Step 2 – Check Network connectivity

	Step	Description
1	Make sure the LDAP server is accessible from the database server on specified port	
2	Windows C:\> telnet myldapserver 389 Unix [oracle@cit-dev-db1 ~]$ telnet 192.168.62.156 389 Trying 192.168.62.156... Connected to 192.168.62.156. Escape character is '^]'.	You can use any LDAP tool to test the connectivity Make sure you are running the test from the database server!
3	If connection fails you have to investigate if LDAP server is running and/or your network configuration allows connection from the database server	

6.1.3 Step 3 – Basic configuration

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_set_novell	
3	Enter LDAP parameters when prompted	LDAP_SERVER_HOST LDAP_SERVER_PORT LDAP_USER_BASE LDAP_GROUP_BASE
4	Run the basic diagnostic script: SQL> @ldap_ping	
5	Ping LDAP server (myldapserver:389) SSL mode is OFF **Connected !** OK	The response should look like this.
6	The configuration of the Novell e-Directory LDAP Adapter is now completed and it's ready for use. It's however recommended to complete the harness test as mentioned in Step 6	

6.1.4 Step 4 – Admin account credentials (optional)

- This step can be skipped in most cases as it is required only when you
  - Use automated user account creation functionality as part of Solar services. Please contact CampusIT is you are not sure.
  - Configure NED to block anonymous searches (default option allows anonymous searches)
- You don't have to use super user admin account. You can create special admin account with privileges limited to user account management in the specified LDAP User Base.

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_admin	
3	Enter LDAP parameters when prompted	LDAP_ADMIN_USER_NAME LDAP_ADMIN_PASSWORD
4	Run the basic diagnostic script: SQL> @ldap_ping	
5	Ping LDAP server (myldapserver:389) SSL mode is OFF **Connected !** **Authenticating user (cn=orcladmin)** **Authenticated !** OK	The response should look like this.

6.1.5 Step 5 – Enabling secure communication (optional)

- The SSL is enabled by default on Novell eDirectory server.

	Step	Description
1	Copy certificate of the certification authority used to generate your SSL certificate for NED into database Oracle Wallet as a Trusted certificate. Make sure use save the certificate in the "Base-64 encoded X.509" format prior importing into Oracle Wallet Manager.	Oracle Wallet Manager
2	Login to the QuercusPlus database as a QUERCUS user	
3	Run the script: SQL> @ldap_enable_ssl	
4	Enter LDAP parameters when prompted	LDAP_SERVER_PORT LDAP_WALLET LDAP_WALLET_PASSWORD
5	Run the basic diagnostic script: SQL> @ldap_ping	
6	Ping LDAP server (myldapserver:636) **SSL mode is ON** **Connected !** OK	The response should look like this.

6.1.6 Step 6 – Final end-to-end test (harness)

- Before running this test make sure you have user created in an LDAP Directory with all required attributes as listed in 3.2
- You can also test membership of user in the group

	Step	Description
1	Login to the QuercusPlus database as a QUERCUS user	
2	Run the script: SQL> @ldap_test	
3	Enter LDAP parameters when prompted	USER_NAME USER_PASSWORD USER_GROUP
4	============================ == User record as in LDAP == ============================ DN = cn=joe.blog,o=university First Name = Joe Surname = Blog Email = joe.blog@mail.com User ID = 1987578 Authenticated = YES Group Member = YES	The results should look like These details should match values you entered when you have created the user in NED.
5	Congratulations ! You have successfully completed configuration of Novell eDirectory LDAP Adapter.	Feel free to contact CampusIT to provide technical assistance when you run into any difficulties with this configuration.

7 REFERENCE

7.1 Configuration Parameters

Parameter	Sample of value	Description
LDAP_SERVER	ORACLE_OID MICROSOFT_AD NOVELL_ED	Type of LDAP server in use (ORACLE_OID, MICROSOFT_AD, NOVELL_ED)
LDAP_SERVER_HOST	myldapserver	Host name of the LDAP server
LDAP_SERVER_PORT	389	Port number of the LDAP server (common values are 389 or 636)
LDAP_USER_BASE	cn=Users,dc=campusit,dc=net	User search base in the LDAP It's specific to each installation of Oracle Application Server
LDAP_USER_ID_NUMBER	employeenumber	Name of property in LDAP user profile holding ID (link to PERSON_LDAP.LDAP_ID)
LDAP_GROUP_BASE	cn=Groups,dc=campusit,dc=net	Group search base in the LDAP It's specific to each installation of Oracle Application Server
LDAP_ADMIN_USER_NAME	cn=orcladmin	User name of an LDAP admin account.Leave blank when LDAP server doesn't require authentication for searches and you active operations (changes to the LDAP schema) are not used.
LDAP_ADMIN_PASSWORD	password	Password of the LDAP admin user
LDAP_WALLET	file:d:\wallet	Location of Oracle Wallet (e.g. "file:d:\wallet"). Leave blank when SSL communication is not required.
LDAP_WALLET_PASSWORD	password	Password for the Oracle Wallet

7.2 Configuration Scripts

Script name	Description	Parameters
ldap_set_oracle.sql	Configures Oracle Internet Directory Adapter	LDAP_SERVER_HOST LDAP_SERVER_PORT LDAP_USER_BASE LDAP_GROUP_BASE
ldap_set_microsoft.sql	Configures Microsoft Active Directory Adapter	LDAP_SERVER_HOST LDAP_SERVER_PORT LDAP_USER_BASE LDAP_GROUP_BASE LDAP_USER_ID_NUMBER LDAP_ADMIN_USER_NAME LDAP_ADMIN_PASSWORD
ldap_set_novell.sql	Configures Novell eDirectory Adapter	LDAP_SERVER_HOST LDAP_SERVER_PORT LDAP_USER_BASE LDAP_GROUP_BASE
ldap_admin.sql	Configures LDAP server administrator credentials	LDAP_ADMIN_USER_NAME LDAP_ADMIN_PASSWORD
ldap_enable_ssl.sql	Enable secure communication with the LDAP server (sets LDAPS protocol)	LDAP_SERVER_PORT LDAP_WALLET LDAP_WALLET_PASSWORD
ldap_disable_ssl.sql	Disable secure communication with the LDAP server (sets LDAP protocol)	LDAP_SERVER_PORT
ldap_ping.sql	Basic diagnostic utility to check connectivity	N/A
ldap_show.sql	List of all LDAP parameters including current values	N/A
ldap_test.sql	End to end test utility to validate functionality including lookup for user details,	USER_NAME USER_PASSWORD USER_GROUP
ldap_trace.sql	Low level diagnostic utility	To be used when requested by CampusIT Helpdesk staff.