



EmerLDAP

LDAP Synchronization Service
Version 2.0

Emerald Management Suite
IEA Software, Inc.

Software License Agreement

By purchasing or installing all or part of the Emerald Management Suite, you indicate your acceptance of the following License Agreement.

Ownership of Software

You acknowledge and agree that the computer program(s) and associated documentation contained with the Emerald Management Suite (collectively, the “Software”) are owned exclusively by IEA Software, Inc. and/or its licensors. The Software contained in the package is protected under copyright laws and all copyright and other intellectual property rights relating to the Software are and remain the exclusive property of IEA Software, Inc. and/or its licensors. You may not rent or lease the Software, but you may transfer the Software and accompanying materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement.

License

IEA Software, Inc. grants to you, and you accept, a limited, non-exclusive and revocable license to use the Software. You agree to use the Software in machine-readable object code form only as authorized in this License Agreement. This License Agreement does not convey any title or interest in the Software to you. You may only use the licensed number of copies of the Software as stated in your purchase agreement.

Scope of License

You may not make any changes or modifications to the Software, and you may not decompile, disassemble, or otherwise reverse engineer the Software. You may not load, rent, lease or sublicense the Software or any copy to others for any purpose. You agree to use reasonable efforts to protect the Software from unauthorized use, modifications, reproduction, distribution and publication. You are not permitted to make any uses or copies of the Software that are not specifically authorized by the terms of this License Agreement. Your adherence to this License Agreement will allow IEA Software, Inc. to continue developing innovative and useful products and providing a high level of customer service and support. If you do not comply with the terms of this License Agreement, your license will be revoked.

Updates and Support

All software updates are available via the IEA Software, Inc. web site. A maintenance contract is available for major version upgrades, which is not included or covered as part of the basic purchase agreement. Technical support is available via E-Mail, support mailing lists, or a purchased telephone support contract.

Trademarks

IEA Software, Inc., Emerald, RadiusNT, and the associated logo(s) are registered trademarks. All images, photographs, animations, audio, video and text incorporated into the Software is owned by IEA Software, Inc., unless otherwise noted by Trademark.

Restricted Rights

The Software is provided with U.S. Governmental Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19 as applicable. The Software is also

protected by International Treaty Provisions. Manufacturer is IEA Software, Inc. Suite 201, West 516 Riverside Spokane, Washington 99201.

Miscellaneous

This License Agreement shall be construed, interpreted and governed by the laws of the State of Washington. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, enforcement of the remaining terms shall not be affected. Failure of either party to enforce any rights or to take action against the other party in the event of any breach of this Licensing Agreement shall not be deemed a waiver of any subsequent enforcement of rights.

Limitations of Liability and Remedies

In no event shall IEA Software, Inc. or its licensors be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential or other damage, even if IEA Software, Inc. or its licensors are advised, in advance, of the possibility of such damages. IEA Software, Inc. and its licensor's entire liability and your exclusive remedy shall be, at IEA Software's option, either (a) return of the price paid, or (b) repair or replacement of the Software. To the maximum extent permitted by applicable law, IEA Software, Inc. and its licensors disclaim all other warranties, either express or implied, including but not limited to, implied warranties with regard to the Software, the accompanying material. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. You may have other specific legal rights which vary from state/jurisdiction to state/jurisdiction.

Should you have any questions concerning this license agreement, please contact IEA Software, Inc. at Suite 326, West 422 Riverside Spokane, Washington 99201 U.S.A. (509) 444-2455.

Credits

Programming by Peter Deacon
Documentation by Dale E. Reed Jr. , Peter Deacon

© 1996-2003 IEA Software, Inc.
All Rights Reserved, World Wide

Table Of Contents

SOFTWARE LICENSE AGREEMENT..... II

1. INTRODUCTION..... 1

2. GETTING STARTED 1

 CONFIGURING EMERALD..... 1

 LDAP SERVER 1

 EXTERNAL SYSTEM..... 1

3. INSTALLING AN EMERDAP SERVER..... 2

 GENERAL 2

 ODBC DATA SOURCES 4

 DIRECTORY SERVER CONFIGURATION 4

 DIRECTORY UPDATE OPTIONS 5

 LOGGING..... 6

 DIRECTORY SYNC CONFIGURATION 7

1. Introduction

The Emerald LDAP Synchronization service (Emerdap) is an interface to the Emerald database that allows synchronization of user information between a LDAP server and the Emerald database. This decreases the challenge of vendors trying to keep up with the database structure or program an ODBC interface into their products that may not be available on some platforms. Tight synchronization alleviates users from having to manage multiple user databases and offers greater scalability and control for all products.

Emerdap will create and remove entries from an LDAP server as they are added and removed from Emerald. It can be configured to keep the two databases exactly the same or make exceptions based on predefined filters.

Note: Some knowledge of LDAP and an LDAP Server is required. We cannot support LDAP server specific problems.

2. Getting Started

Configuring Emerald

Before installing Emerdap you'll need to configure an Emerald External system and associate the Service Types you want synchronized with this system. The Emerald External System Name must match the name of the Emerdap sync server you will be creating later.

LDAP Server

A free LDAP implementation is available from <http://www.openldap.org>.

After installing your LDAP server create a DN (Distinguished Name) to place your Emerald users under. For example ou=users,o=nasa. You can use the ldapadd utility included with some directory servers to add the DN if it does not already exist.

```
ldapadd -h localhost -D 'cn=Directory Manager' -w password
```

```
Ou=users,o=nasa
```

```
Ou=users
```

```
ObjectClass=OrganizationalUnit
```

```
$
```

A Java based LDAP client is also available from <http://www.iit.edu/~gawojar/ldap/>. This Base DN will be used later when configuring your sync server (See [Installing Emerdap](#))

Next create an administrative user that has full access to your Base DN (or use the LDAP root /directory manager account) This user must not have any limitations set on the number of entries a search can retrieve or the amount of time a search operation can take. If Emerdap encounters these search limits database synchronization will fail.

While you're here you may want to turn up the debug level on your LDAP Server to help debug any problems.

External System

Test the system your integrating Emerald and LDAP with to make sure it can connect to your directory server and it's able to read entries within the Base DN you added above.

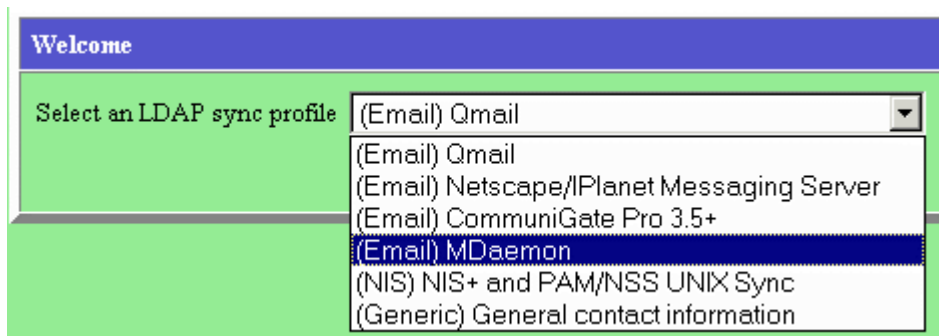
3. Installing an Emerdap Server

Start the Emerdap server in debug mode.

On Win32 platforms select Emerdap (Debug) from the Emerald program group. On UNIX platforms type `./emerdap -debug` from your main Emerald directory (`/usr/local/emerald`)

```
D:\vss\emerdap\debug\emerdap.exe
Debugging Emerald LDAP Sync 2.0.12

Required setting 'Mapped columns' not set
Required setting 'Mapped columns' not set
Starting configuration Web server on TCP port 8012.
```



Your display will have different Sync profiles from what's shown in the picture above. *(If there are no Sync profiles showing check the directory EmerDap is installed to. It should contain an Emerdap sub directory with a file named 'emerdap.ini'. Enter the directory containing this file in the Directory field, then click 'Go'.)*

Now lets get started creating your sync server. Select the proper profile from the Sync profile screen.

General

Installs or removes this sync server from the Windows NT service manager. The 'Service Title' field represents the name of the service listed in service manager. 'Debug' runs the sync server in debug mode within a command window. All messages in this mode are shown in the command window and not logged to disk. Make sure this server is not already running as a service before using the debug option.

General

TO add LDAP support to Qmail see <http://www.nrg4u.com/>

Show advanced options

Server name (Unique name identifying this server)

test

Description

TO add LDAP support to Qmail see <A HREF=http

Configuration server

Enabled

Configuration server port

8012

Service name

Emerdap QMail sync

Service control

Install

Remove

>> Continue

Option	Description
Show advanced	Show advanced sync options
Server name	Emerald external system name of this sync server
Description	Text field describing what this server does
Configuration server	Whether to enable or disable the Emerdap configuration server. Run emerdap from the command line with <code>-config</code> to re-enable.
Configuration server port	TCP Port configuration web server should listen on. The default is 8012
Service name	Service label to show in Windows service manager. (Win32 ONLY)
Service control	Installs or Removes Emerdap as a Windows service. (Win32 ONLY)

As you can see, you have your work cut out for you ☺ If the ‘Help’ button is available in the Sync Configuration section it will share some configuration pointers specific to the sync profile you selected.

ODBC Data sources

Enter the name of the ODBC Data source of your Emerald database. The database server menu use a shared configuration /w other Emerald applications such as Emerald, syslog server, scheduler, Radius... If you have already installed one of these applications database access is already configured and you may skip this step.

Database server TO add LDAP support to Qmail see <http://www.nrg4u.com/>

ODBC datasource: Emerald22 (SQL Server)

Username: sa

Password: *****

Persistent connection: ☒

>> Continue

Directory Server Configuration

Enter your LDAP connect information and Base DN - See [Getting Started](#).

LDAP server TO add LDAP support to Qmail see <http://www.nrg4u.com/>

LDAP host: bluemarble.iea-software.c

LDAP port:

Bind DN: cn=Directory Manager

Bind password: *****

Base DN: ou=bluemarble

SSL enabled: ☐

Netscape 4.x SSL cert:

>> Continue

Option	Description
LDAP Host	LDAP Server hostname
LDAP Port	LDAP Server port number, leave blank to use the default LDAP port.
Bind DN	LDAP bind DN. (An administrative account on the directory server)
Bind Password	LDAP bind password
Base DN	Base DN being synchronized
SSL Cert	Netscape cert7db certificate database file (from Netscape 4.x)
SSL Enabled	Enable secure SSL connection to LDAP Server

Directory Update Options

These options control what and how often to make changes in LDAP based on what has been changed in Emerald.

Sync options
TO add LDAP support to Qmail see <http://www.nrg4u.com/>

Enable Add ☒

Enable Update ☒

Enable Delete ☒

Exclude search filter

Password type {crypt}unixcrypt ▼

Password attribute userPassword

Partial sync (secs) 120

Full sync (secs) 1728000

Partial neg sync (secs) 300

Full neg sync (secs) 172800

>> Continue

Option	Description
Enable Insert	Allow new entry's to be added to the directory.
Enable Update	Allow existing entries to be updated.
Enable Delete	Allow deleted entries and their attributes to be deleted from the directory.
Exclude search filter	An LDAP search filter where a match is used to exclude entries from being updated or deleted. Don't set to disable the exclude filter.
Password type	Password format options such as plain text or unix crypt.

Name of the	The name of the password attribute. Generally 'userPassword'
Partial sync	Seconds between running partial sync (Differential Add/Update)
Full sync	Seconds between running full sync (Complete Add/Update/Delete)
Partial neg sync	Seconds between running partial negative sync (Differential Delete)
Full neg sync	Seconds between running full negative sync (Complete Delete)

Logging

All Errors are logged unconditionally. When first starting the sync server it's a good idea to check all of these and review the output by using the debug option in the [Service Control](#) section. When your confident things are working turn off debugging. Some of these options - especially Search and Update can generate large amounts of debug data.

Logging TO add LDAP support to Qmail see <http://www.nrg4u.com/>

Log file:

Syslog IP:

Debug options:

- ☒ Routines
- ☒ Reads
- ☒ Updates
- ☒ Adds
- ☒ Deletes
- ☐ SQL
- ☐ LDAP
- ☒ Search

>> Continue

Option	Description
Routines	Entering and leaving update functions
Reads	Summary of data read from all sources
Updates	Entries and attributes modified
Adds	New entries and attributes
Deletes	Deleted entries
SQL	SQL specific operations
LDAP	LDAP specific operations
Search	LDAP search operations

Directory Sync Configuration

This section is for advanced users. It allows you to modify defaults for the current sync profile. Please don't make changes to these fields unless you understand their implications. To enable advanced options select 'Show advanced options' from the general section.

Three new sections appear 'LDAP Column mappings', 'Multi-valued attributes' and 'Queries'.

LDAP Column mappings

Column mappings detail how information from the SQL database should be mapped to LDAP attributes.

LDAP column mappings

Mapped columns

uid
userPassword
mailHost
mailAddress
x500uniqueIdentifier

Delete

Primary key

x500uniqueIdentifier

Object classes

organization
posixAccount
organizationalPerson

Delete

Add

>> Continue

Option	Description
Mapped columns	These SQL column names will be mapped to LDAP attributes of the same name.
Primary Key	This Column Name (attribute) becomes the DN of each entry.
Object Class	Object class(es) included in the entry.

Multi-valued attributes

Multi-valued attributes allow mapping multiple values of a field to LDAP. In a relational database of tables containing rows and columns each column can only store a single record per row -- However most directory systems allow an unlimited number of similar attributes per entry. Multi-valued attributes allows you to specify a query to retrieve multiple values from another source. This is only triggered when there is a multi-valued attribute query specified for the column in question and the value of that column in the RDBMS is null. This allows the RDBMS to Detect in advance weather more than one attribute is present and skip having to run this sub-query for entries with 0 or 1 values.

Multi-valued attributes

TO add LDAP support to Qmail see <http://www.nrg4u.com/>

Queries: x500uniqueIdentifier

Queries: cn

Queries: uid

{CALL LDAPmailForwardingAddress(#account

Queries

Queries		TO add LDAP support to Qmail see http://www.nrg4u.com/
Partial sync query (<i>Retreives list of changes since last good call</i>)	<pre>{CALL QMailGetPartial('\$name')}</pre>	
Full sync query (<i>Sets partial sync to retrieve all data</i>)	<pre>{CALL LDAPSetLastModifyDate('reset','\$na</pre>	

Option	Description
Partial sync	Retrieves a list of changed records to compare with the directory servers data.
Full sync	Sets SQLPartialProc to retrieve all records regardless of it's last process date. Don't set to disable Full sync.
Partial time	Sets last call time for Partial sync after a successful run.
Verify delete	Check PrimaryKey does not exist in the database server by returning 'ACK' then delete entry from ldap. Don't set to disable this feature.
Partial neg	A list of PrimaryKeys to delete. Don't set to disable this feature.
Full neg	A list of PrimaryKeys to not delete. Don't set to disable this feature