Isode

# XMPP Instant Messaging (with Active Directory)

*Quick setup of Isode's XMPP Server, M-Link, using Microsoft's Active Directory for user account provisioning*

# Objectives

This document is intended for those beginning an evaluation of Isode's XMPP Server product, M-Link. During this evaluation we will:

- Configure Active Directory for use with M-Link (note that this guide does not cover installation and initial setup of Active Directory: you should refer to your AD documentation in order to achieve this).
- Set up an XMPP Service (headquarters.net) on a single-node for 1:1 chat.
- Set up a Multi-User Chat (MUC) domain for headquarters.net and create a permanent MUC room.
- Set 1:1 and Multi-User Chat Archive Locations
- Test 1:1 Chat & MUC with AD users and with the Swift XMPP Client.

We'll be using 2 Isode products: M-Link (to provide the XMPP service) and Swift (an Open Source XMPP Client which Isode provides commercial support contracts for). For the purposes of this evaluation guide we have assumed that this is a 'clean' installation of M-Link R16.3. You'll interact with M-Link using:

- M-Link Console (MLC): a GUI management tool that enables configuration and management of an M-Link system.
- Swift: An open source multi-platform XMPP client.

> **Note for Windows Users**
>
> If you're running Windows 7/8 or 10 you will need to run Isode Management tools as an Administrator. You can do this by right-clicking on the program icons and choosing 'Run as administrator' from the pop-up.

## Installation Requirements

You should visit [www.isode.com/products/supported-platforms.html]to discover which operating systems are supported for Isode evaluations. Evaluation downloads (excluding documentation) are held in a password-protected section of the Isode website. If you have not already done so you should apply for password access by filling in the form located at [www.isode.com/evaluate/evalrequest.html].

## Obtain Isode Server Products

Many Isode management tools are written in Java. You should install Java before installing the Isode packages. You can obtain the required packages (Java SE 8 – JRE) from [www.oracle.com/technetwork/java/javase/downloads/index.html].

After obtaining password access to the Isode binary files you should download and install M-Link, following the instructions on the download page for your platform. The number of packages required will vary depending on platform. Server downloads are listed at [www.isode.com/evaluation/].

> **Note for Linux Users**
>
> On Linux platforms you should create an M-Link runtime user account 'mbox'. After installation you should change the ownership of the /etc/isode directory to this user.

## Obtain the Swift XMPP Client

Swift for Windows, Linux and Mac OSX can be downloaded from [www.swift.im].

## Evaluation License File

Isode server products require a valid license from Isode before they will run correctly. Licenses are issued by Isode Customer Service. If you haven't already been sent a license when requesting access to the evaluation files, please send a message to request a license to [pre-sales@isode.com] remembering to specify which Isode server products you need a license file for.

By default the license file you receive needs to be installed in \Isode\etc\ (Windows) or /etc/isode/ (Linux) as 'license.dat'. You may have chosen an alternative installation directory when installing the software, in which case you will have to place the license file there.

## Edit the Hosts File

MLC recognizes real server addresses rather than the 'localhost/machinename' designations you'll be using if you set up this evaluation on your local machine.

You will therefore need to edit your hosts file (found at /Windows/System32/drivers/etc/hosts on Windows and /etc/hosts on Linux) to include a line that adds a references between the localhost address and the domain name you'll be using for this evaluation. In this document we're using the domain name 'headquarters.net' so your hosts file will need to include the line:

> *127.0.0.1 headquarters.net*

## DNS Settings

In order for Active Directory to find your Mlink Server you will need to set up SRV records within DNS. SRV records are set up for every domain that you host, pointing to every node of the cluster on port 5269, and that for the chat domains you should also have _xmpp-client._tcp set up pointing to 5222. If you're running non-standard ports replace 5269 and 5222 as appropriate. Below is an example:

> *_xmpp-server._tcp.headquarters.net IN SRV 5 33 5269 xmpp.mydomain.com.*
> *_xmpp-client._tcp.headquarters.net IN SRV 5 33 5222 xmpp.mydomain.com.*

# Creating an XMPP Service

M-Link uses a directory to hold user information. You're going to use Active Directory for this purpose, although you could instead use Isode's own M-Vault LDAP Directory (a separate evaluation guide covers setting up M-Link using M-Vault).

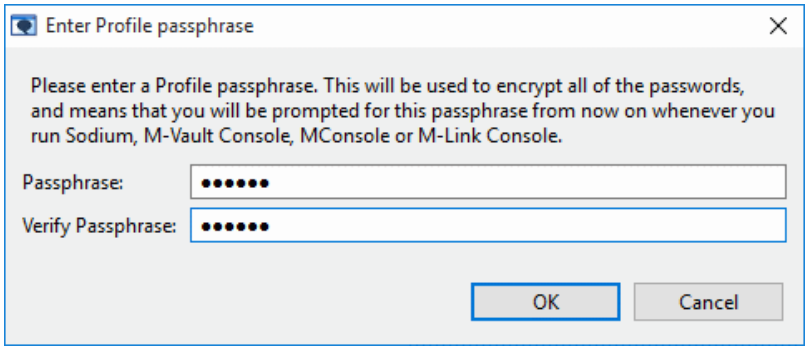
## Starting M-Link Console

In Windows click Start, and from the Programs menu, select 'Isode 16.3 > M-Link Console'. In Linux execute the following command:

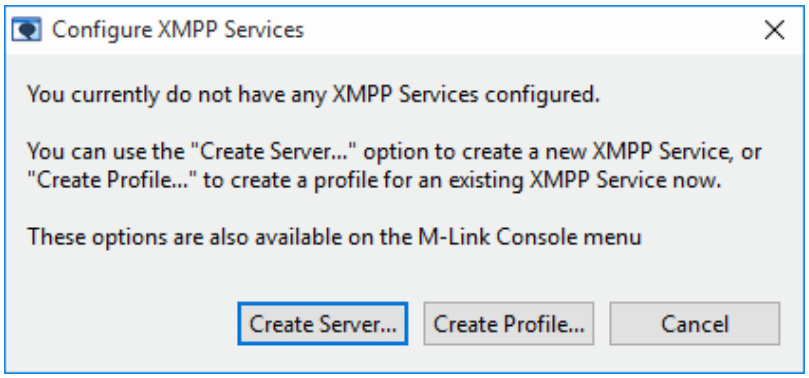
> *% /opt/isode/bin/mlc*

## Starting the Wizard

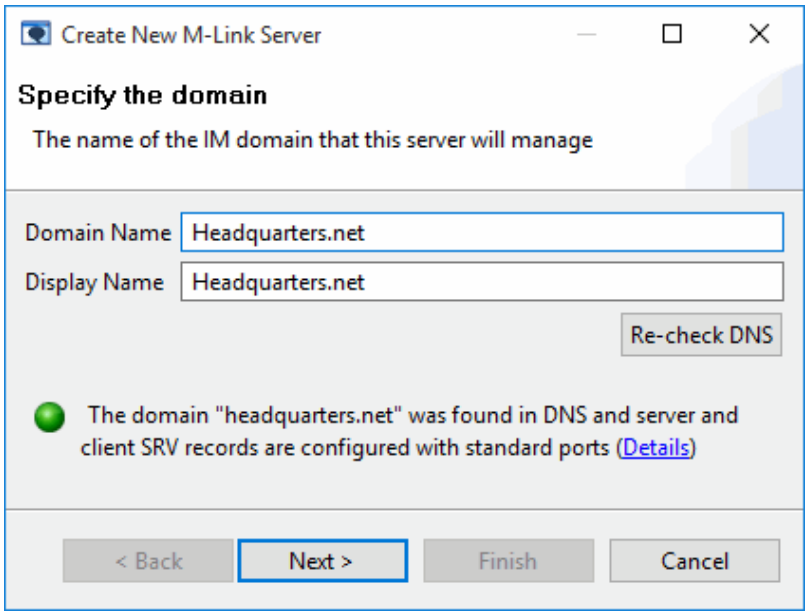
If this is the first time you've used any of the Isode management GUI tools, you will not yet have Isode profile settings saved. If this is the case you'll be asked if you wish to encrypt your bind profile (Yes) and then prompted to set and confirm a password for that profile.




If you have already created an Isode bind profile as part of another evaluation, you will be prompted for the passphrase. Once you have created the profile, MLC will launch. If you don't currently have any XMPP services configured, you'll be prompted to create one:




Choose **[Create Server...]** in the next screen specify the Domain Name and Display Name for your IM domain. In this case we're using 'headquarters.net' for both.

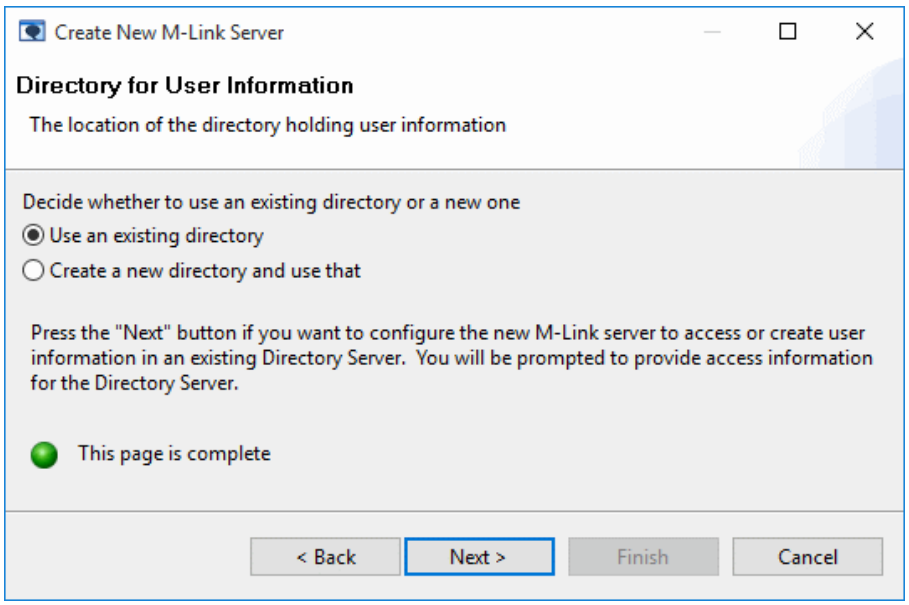



Click on **[Next >]** and you'll be prompted for information on the Directory that will be used to hold user information.

## Specifying a Directory for User Information

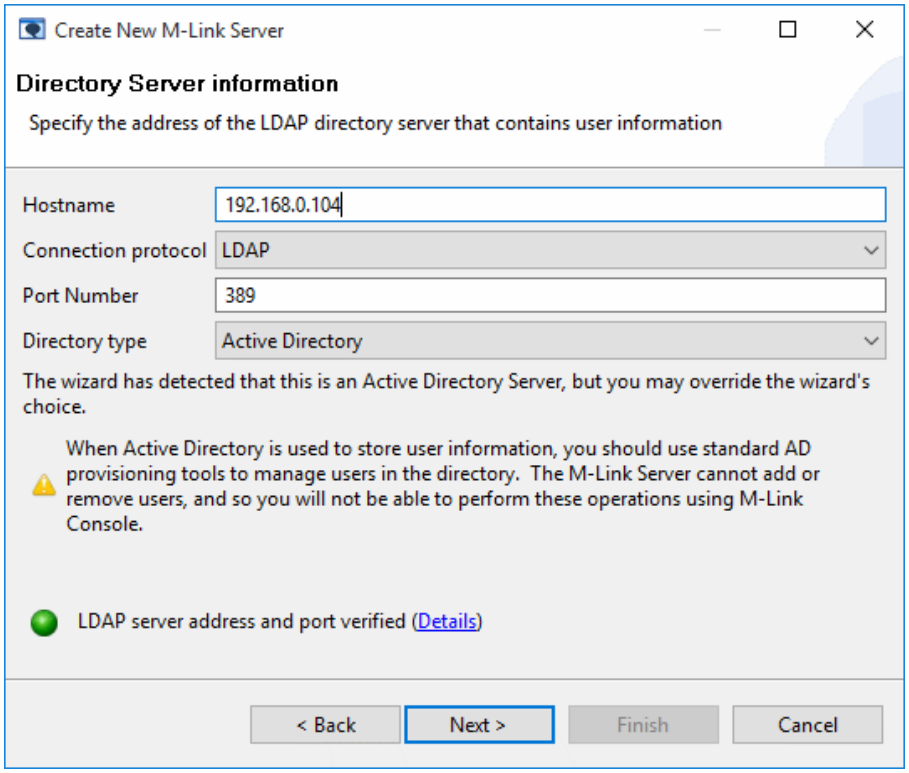
As mentioned earlier M-Link can use an existing directory for user account information but for the purposes of this evaluation we're going to create a new one.

We're going to be using an existing Active Directory installation so select the **[Use an existing directory]** option and click on **[Next>]**.

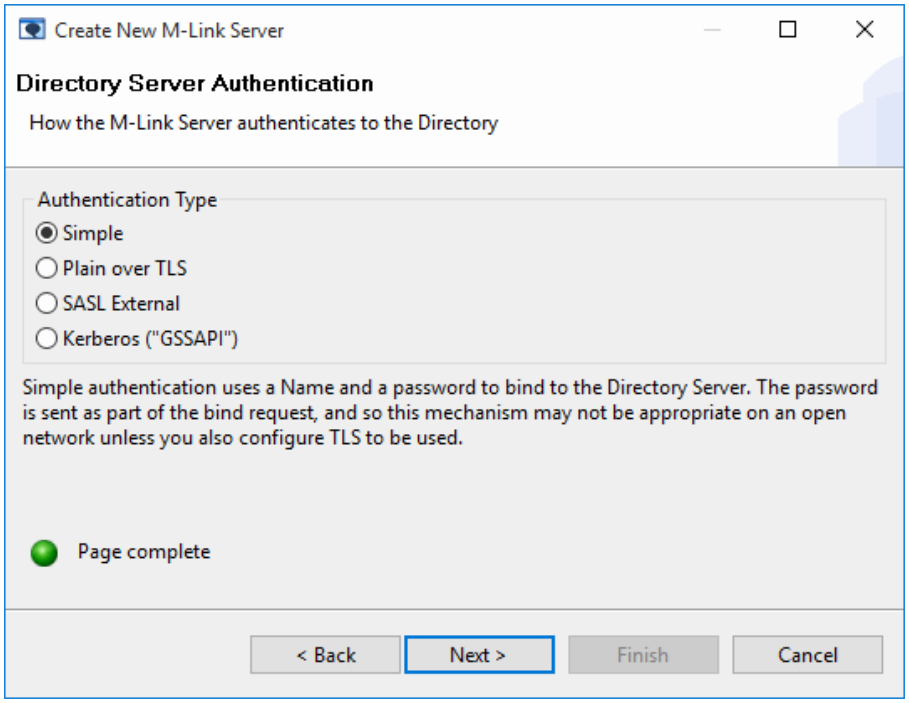



You'll be prompted to supply the address of the Active Directory server you'll be using. When you do, an anonymous connection attempt will be made in order to establish if the directory is online and accessible. The wizard will also attempt to determine the directory type (i.e. Active Directory) automatically. You will

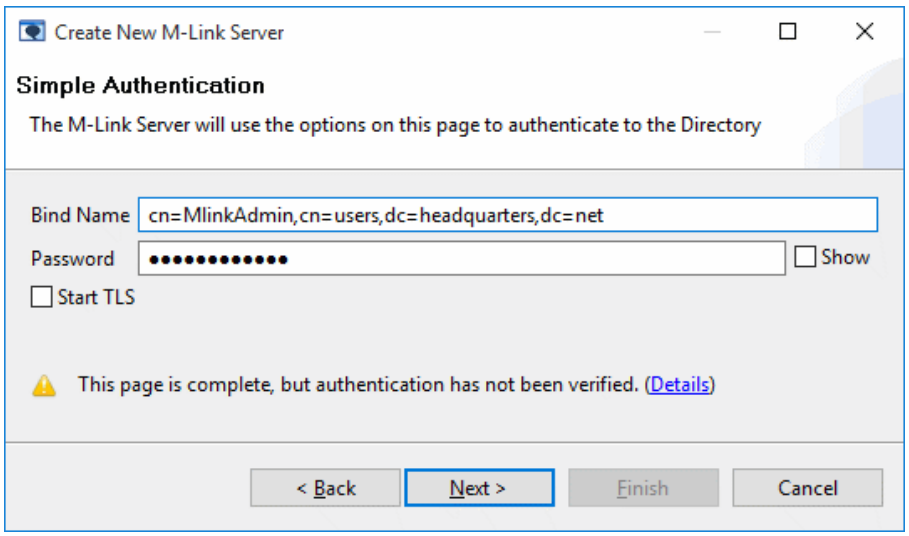
not be able to proceed past this step unless you can supply details of a directory that is contactable. Click **[Next>]** once you have established connection with AD.



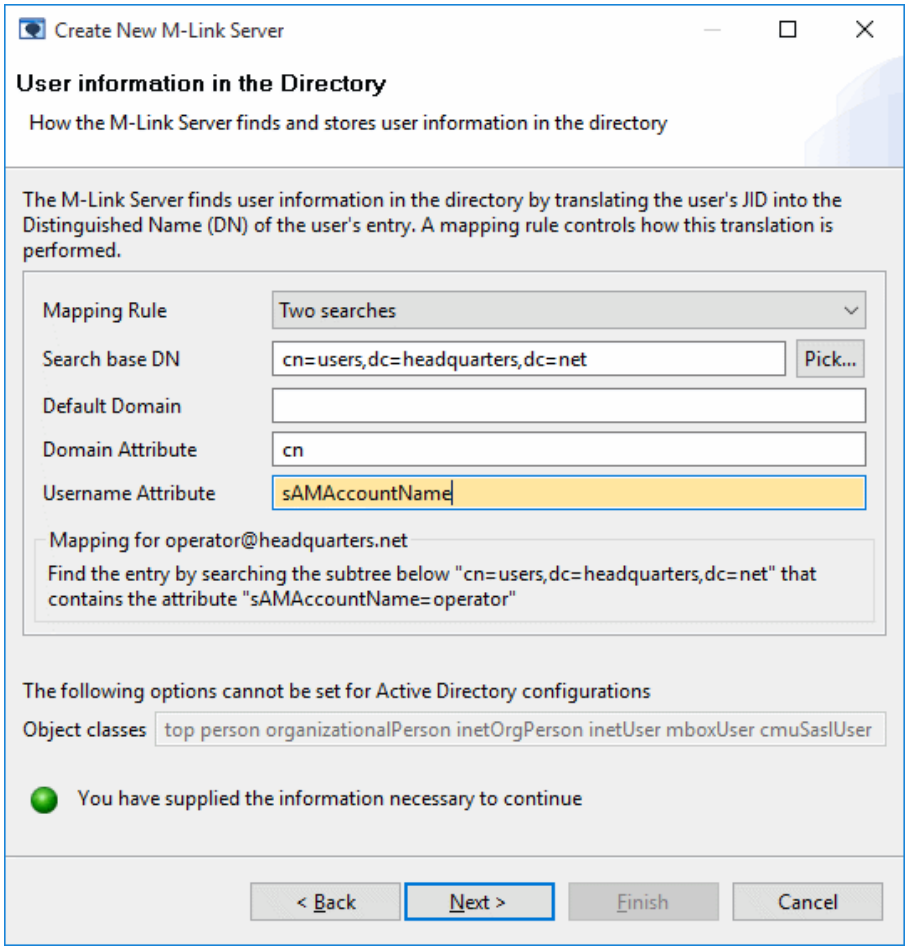

For the purposes of the evaluation, at the Directory Server Authentication screen select "Simple". Click [**Next**>].

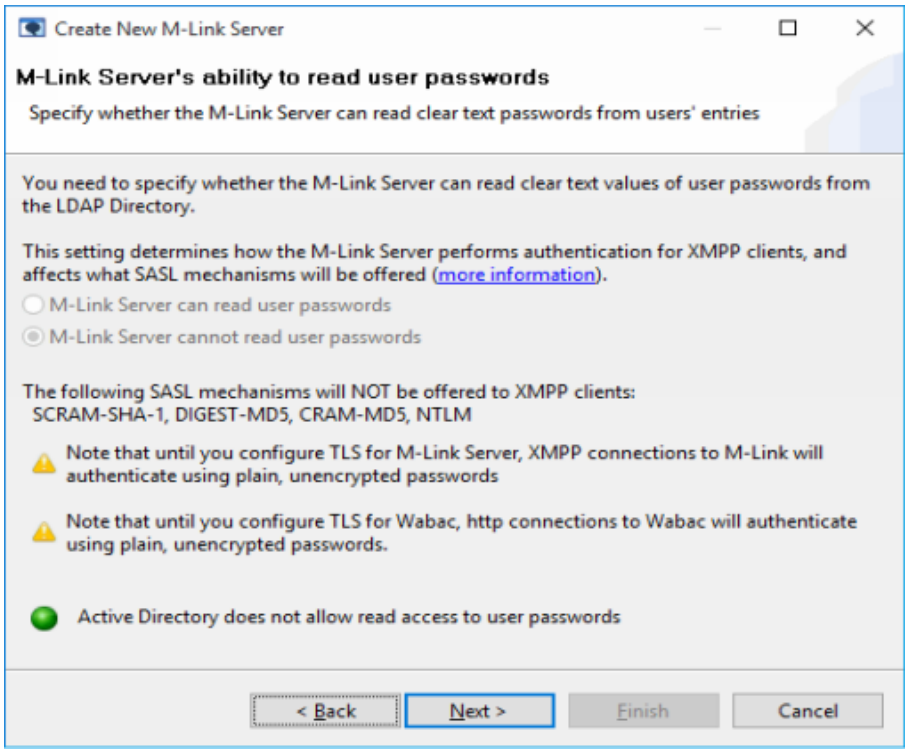



Enter the Bind DN and Password of the AD account that you want to be the M-Link Admin. Click [**Next**>]




You'll be asked where user entries should be found/stored inside AD and which attribute will be used to store the user JIDs. Select "Two Searches" from the SASL Mapping Rule drop-down, define the 'Search Base DN' as in the screenshot below and choose a Username Attribute, in our example we've used "sAMAccountName" as the Username Attribute and click on **[Next >]**.

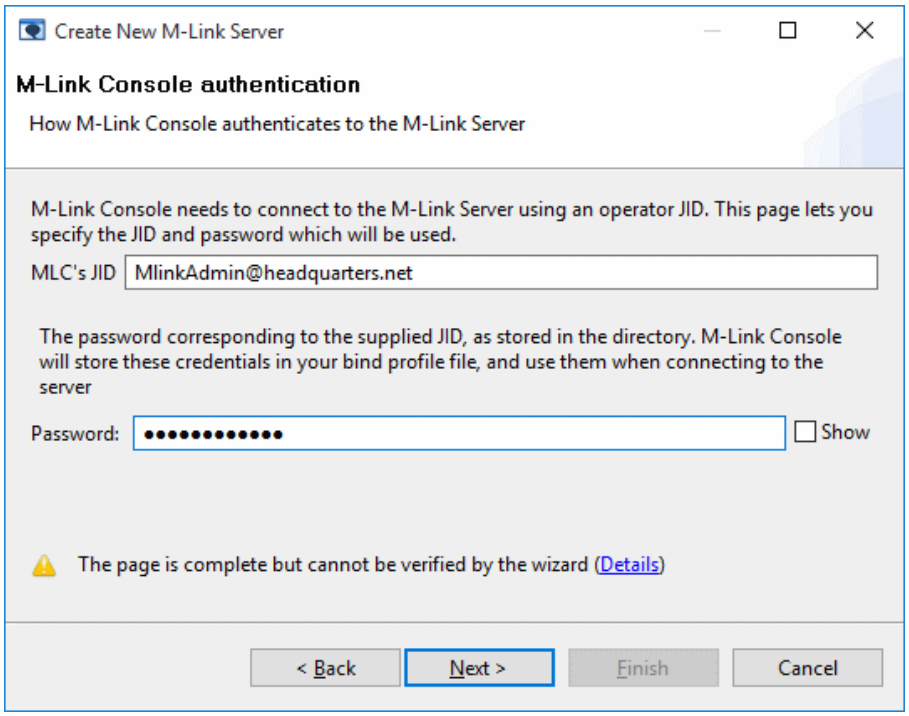




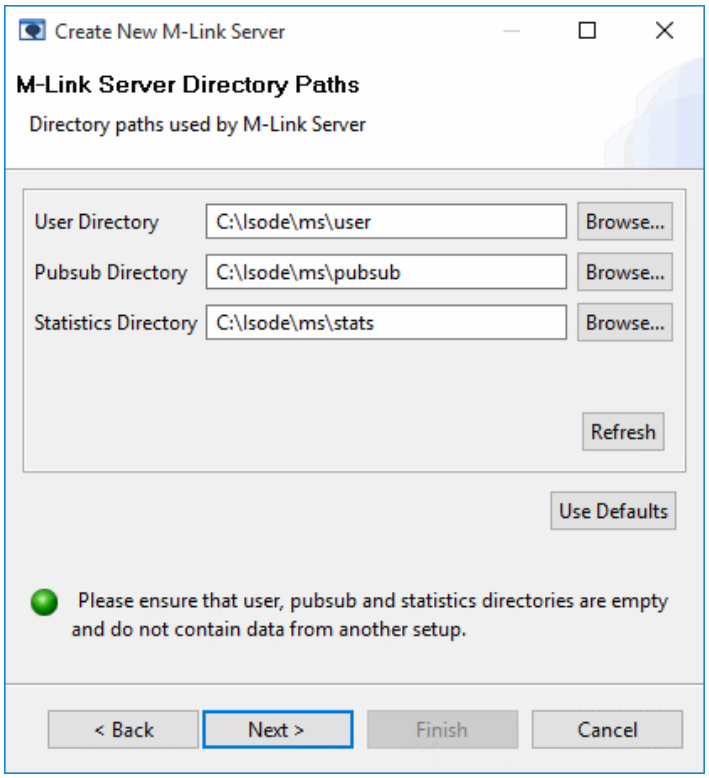

The next screen is used to determine if the M-Link Server has access to user passwords stored in the directory. Active Directory does not allow access to user passwords so click **[Next >]** again to skip this step.

## Create a new M-Link Server

MLC is an XMPP client and needs to use an identity to connect to M-Link, as does any XMPP client. When the server is created, the JID you specify here will be a member of the Operator group, so MLC will be able to administer the server. MLC will use the Mlink Operator AD account created earlier, so enter the JID and password details as below: Click [**Next**>].



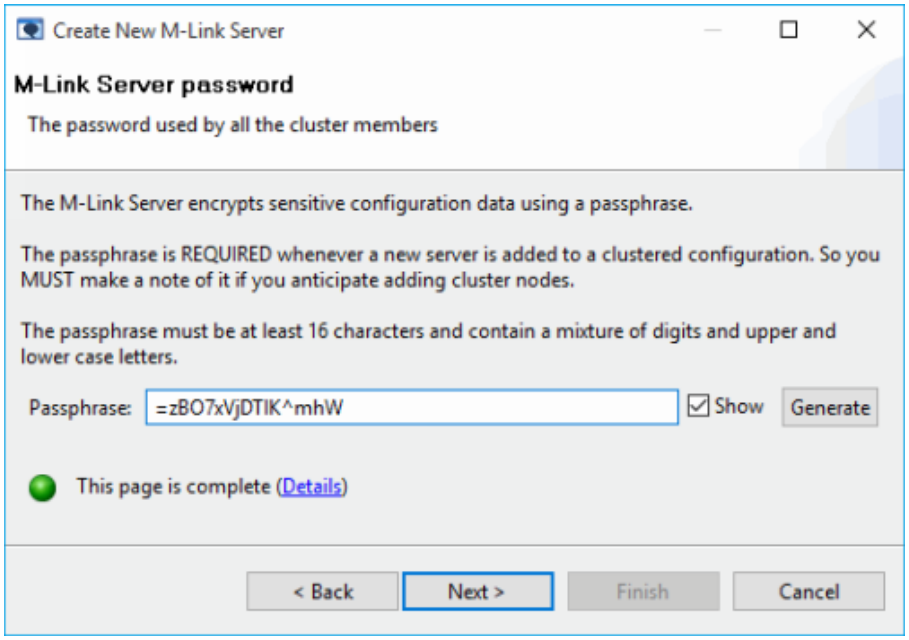

In the following screen you'll be prompted to set locations for User, Pubsub and Statistics data. Use the defaults, as follows, and click [**Next**>].



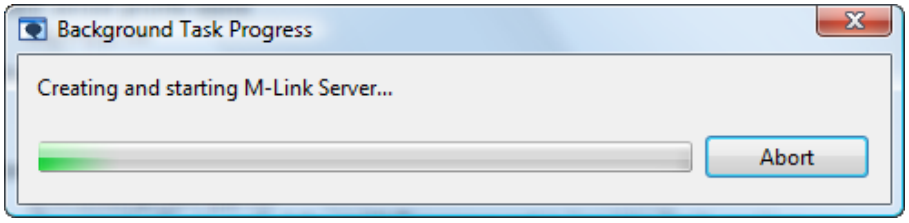

At the Archive Server Database Details screens, use the defaults and click [**Next**>].

M-Link encrypts sensitive configuration data using a passphrase, in the ext step a random passphrase will be

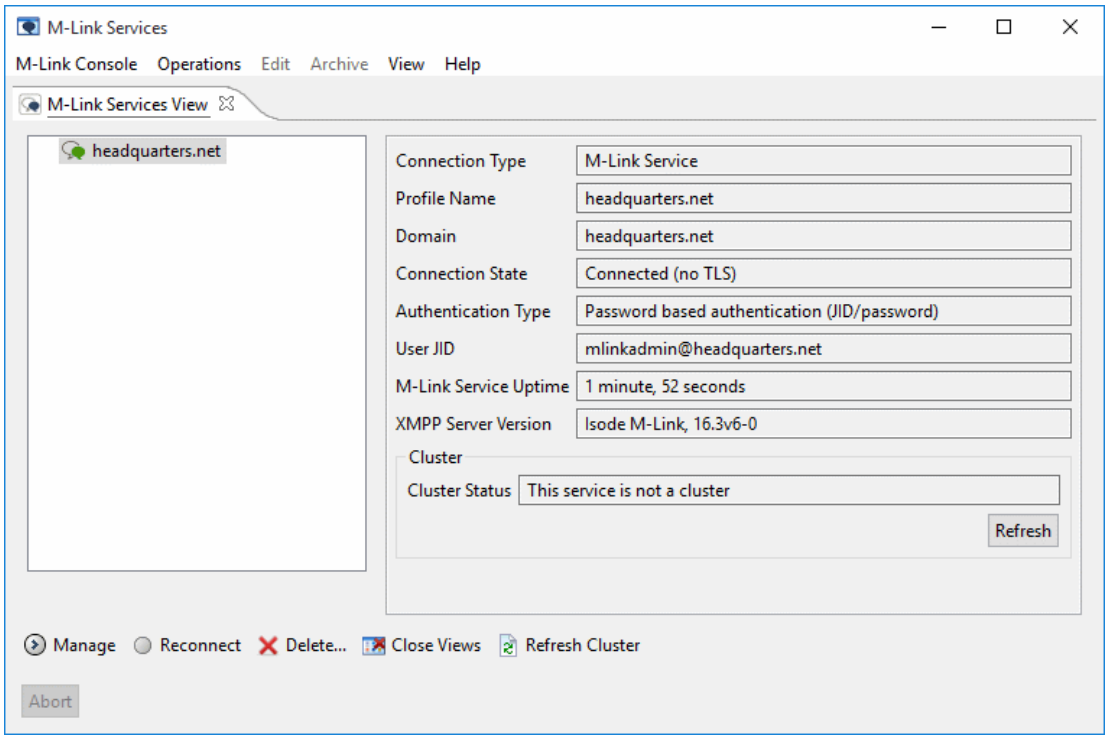
set. It's important that you make a note of this passphrase. Click [**Next**>].




Click on **[Next >]** and the final screen will confirm the configuration you've just created. Click **[Finish]** and MLC will save the configuration and start M-Link.




After completing the Wizard process, you'll be dropped back into the main MLC screen and you'll see that your M-Link Service, 'headquarters.net', is now active.

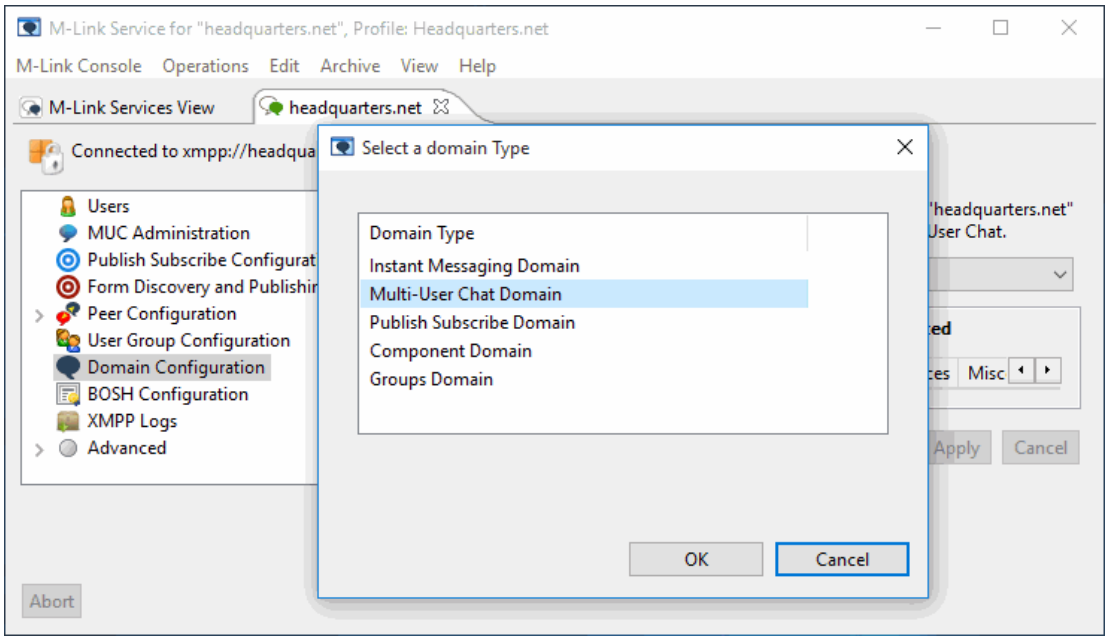



## Adding a Multi-User Chat (MUC) Domain

The XMPP Service we've set up will allow 1:1 instant messaging by default. In order to enable multi-user chat we need to set up a multi-user chat domain within which chat rooms can be created.

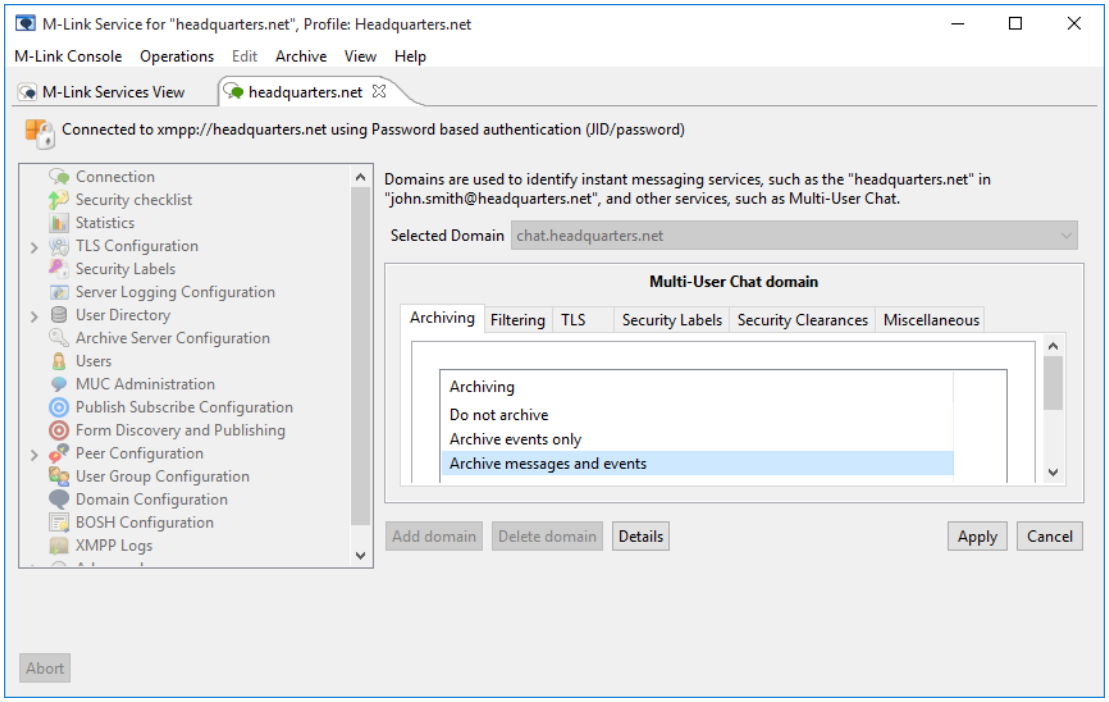
Highlight the XMPP Service, right-click and select **[Manage]** from the menu. You can also use the **[Manage]** menu item at the bottom of the MLC screen to achieve the same effect.

Select **[Domain Configuration]** from the left-hand pane and then click on **[Add domain]**. In the resulting pop-up select 'Multi-User Chat Domain' and click on **[OK]**.

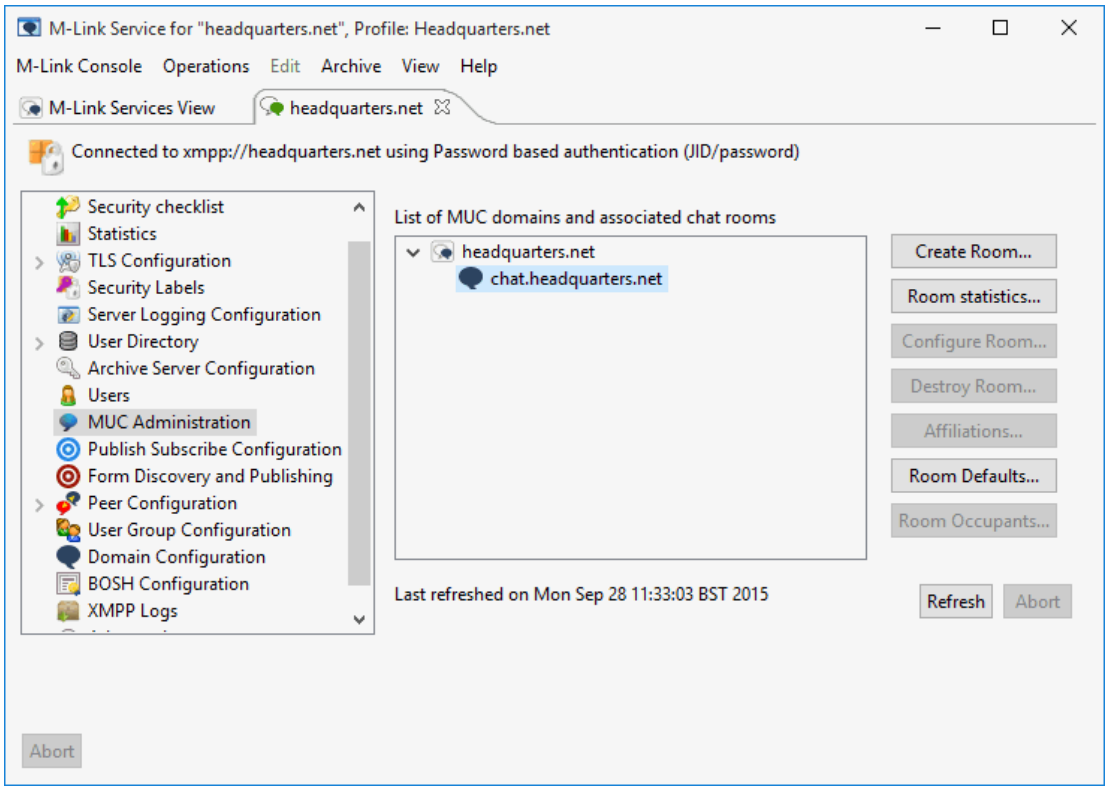



Fill in the Domain Name (chat.headquarters.net) and Parent Domain Name (headquarters.net) and click on **[ OK]** to confirm the changes.

On the Archiving tab, select [**Archive messages and events]**, then click on **[Apply]** to commit these changes.




Now select **[MUC Administration]** from the left pane and you'll now see the MUC domain associated with headquarters.net.

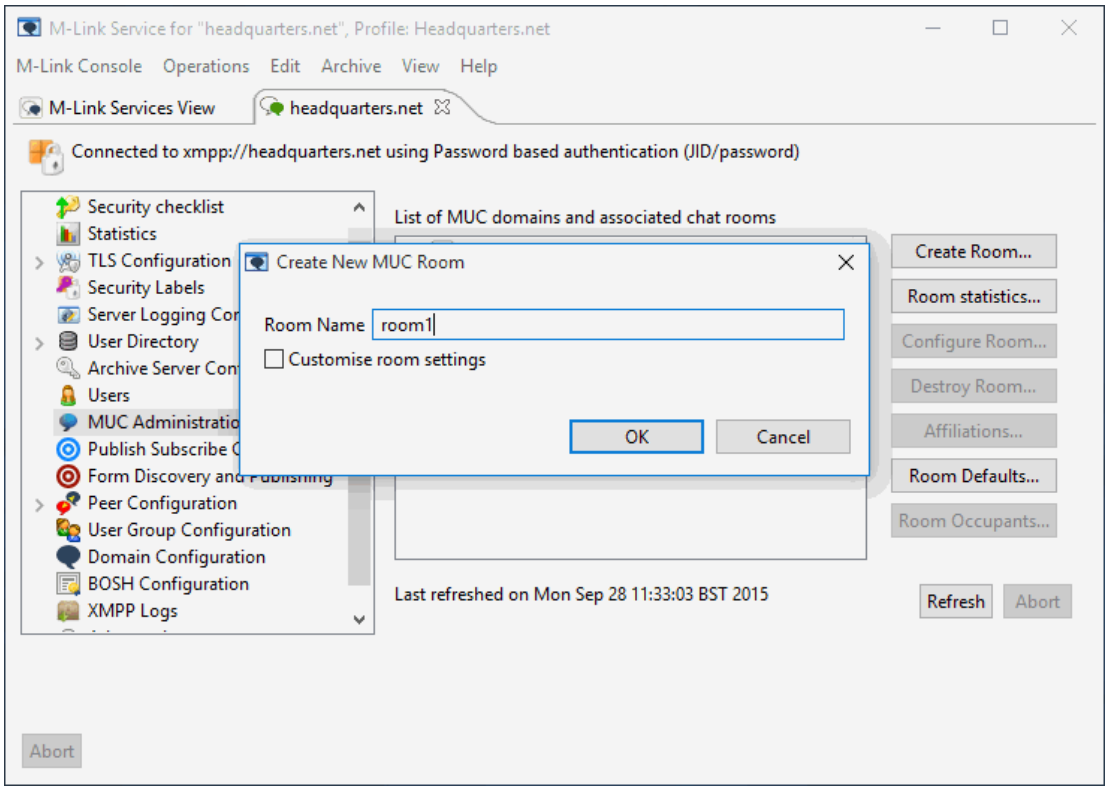



**Note**

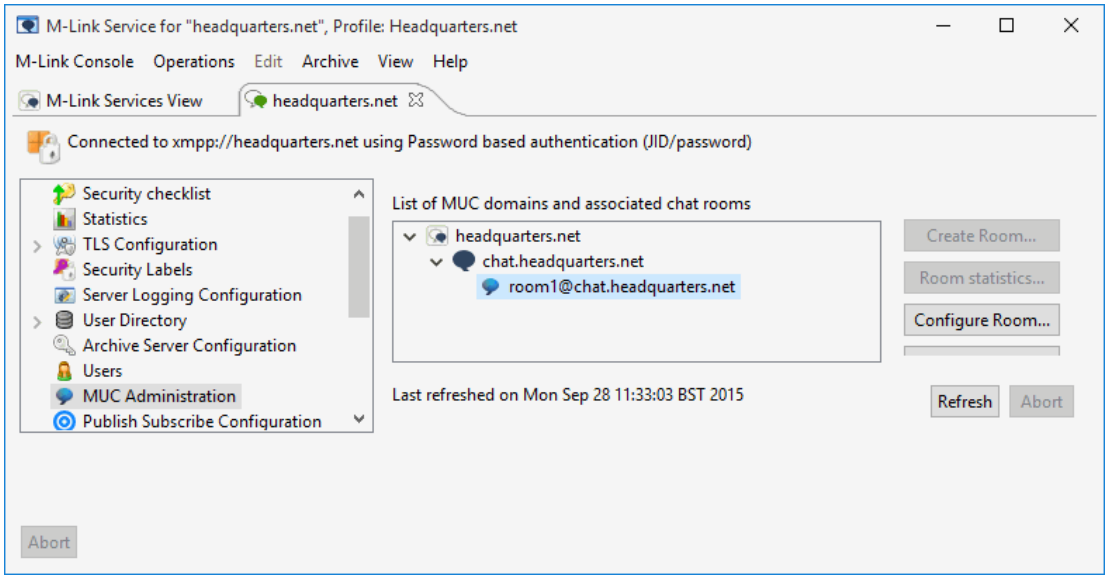
We've created one MUC domain for the headquarters.net service however, a service can contain multiple MUC domains. You may for instance wish to create different MUC domains to match requirements of your organization's security policy, with an entire MUC domain reserved for users of a certain security clearance, rather than applying security clearances to individual MUC rooms. See the M-Link Administration Guide for more information on Security Policy.

## Adding a Persistent MUC Room

Now that we've created a MUC domain, the servicemuc- can host MUC rooms. We're going to create a single persistent MUC room. This type of room will persist through server re-starts. Highlight the 'chat.headquarters.net' domain and click on the **[Create Room...]** button. Give the room a name but at this stage don't apply a password or customize the room settings.




Click on **[OK]**. After the confirmation message the new room will appear in the administration screen.

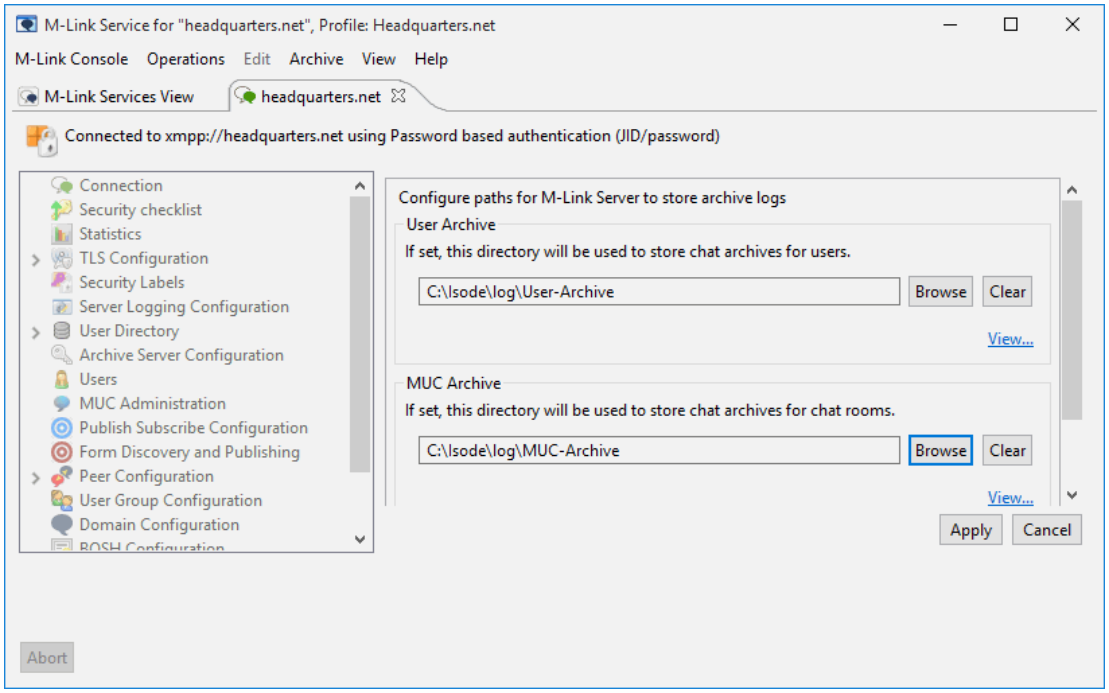



Although we're not going to add any special configuration options to the room at this stage, you can see what options are currently available for room configuration by highlighting the room and clicking on **[Configure Room]**.

## Setting 1:1 and Multi-User Chat Archive Locations

A common admin requirement is for archives to be kept of both 1:1 and MUC chat sessions. In this section

we'll set locations for storing those archives. Select the XMPP Logs option from the left-hand pane and set locations for User and MUC Archives using the fields provided on the right. Click on **[Apply]** to commit these locations.




You'll need to switch back to the M-Link Services View tab and **stop** and **start** the service (from the Operations menu) to activate logging.

# Testing with the 'Swift' XMPP Client

A number of free XMPP clients are available but for the purposes of this evaluation we're going to use the 'Swift' client. Instructions for obtaining and installing Swift for your platform an be found at [www.isode.com/evaluation/swift/].

## Installing and Using Swift

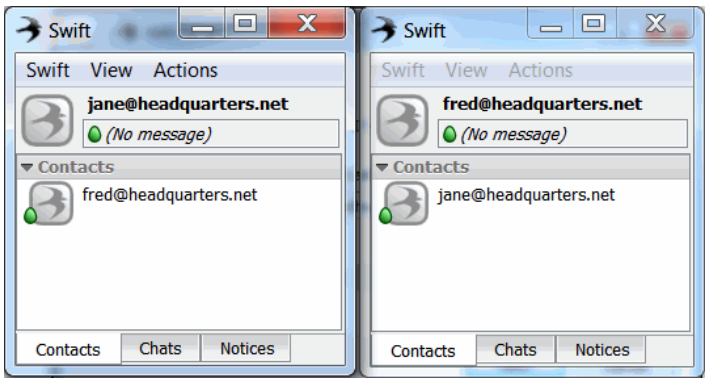
Install and run Swift. When starting Swift use the address and password details for "jane@headquarters.net" to log in.


You can run multiple copies of the Swift client, so launch Swift again, this time logging in as "fred@headquarters.net". Once you've logged in as both users, you'll see that they have empty rosters. From either of these users, select **[Add Contact]** from the **[Action]** menu in Swift and fill in the JID of the other user.

> **Note**
>
> These instructions assume that you are either using Swift on the same machine as that which is running your server software, (& that it is therefore taking advantage of the Hosts file changes you made earlier to resolve the @headquarters.net address) or you are using SRV records within DNS to resolve the @headquarters.net address. If you are using Swift on a different machine and are not using SRV records, click on the Connection Options links under the Connect button to specify the IP address of the system hosting M-Link.

Click **[Next]** and give the contact a name (or select their JID as the name for your roster) and click Finish. We're not going to create any group contacts at this stage.  When the Jane Brown user receives and accepts

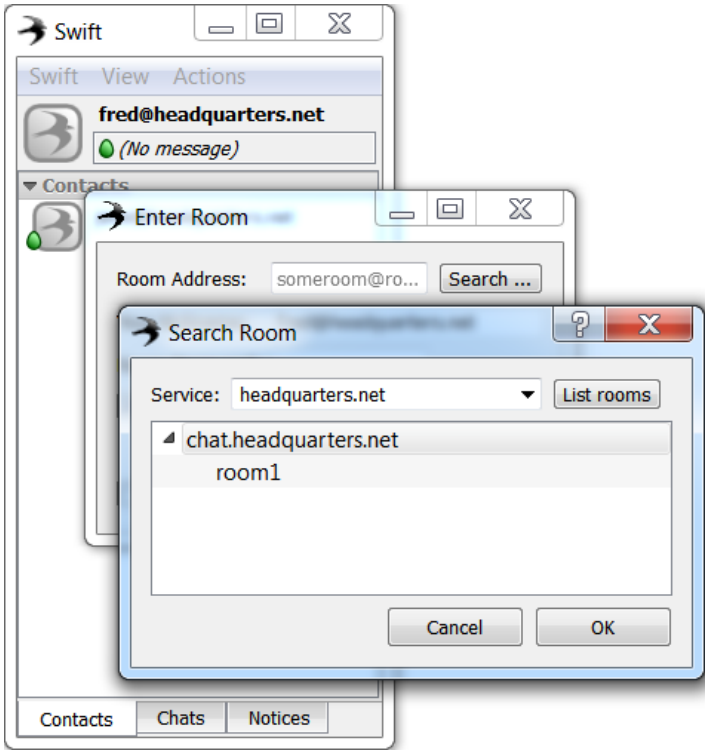
the request, each will appear in the other's roster.



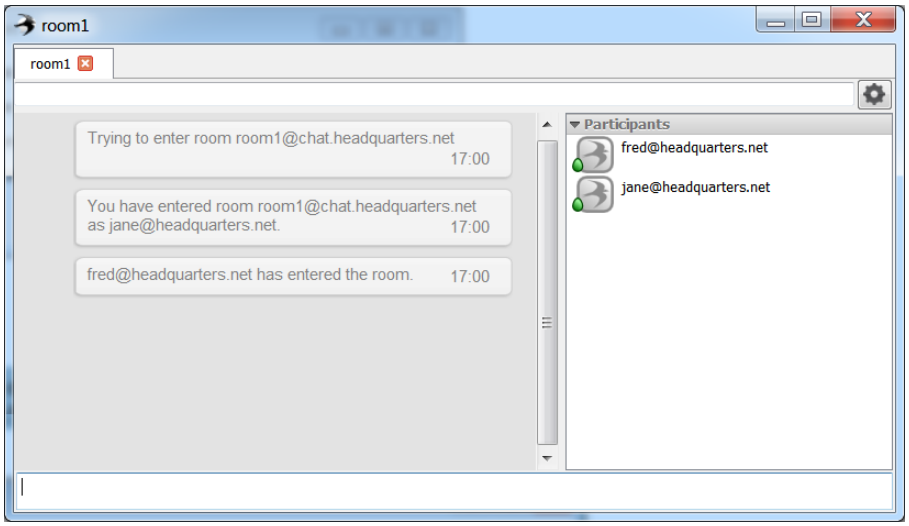

You can now engage in 1:1 chat between your two users.

> **Further Reading: Roster Prepopulation**
>
> If you have a large group of users who require large or defined rosters of contacts, setting them up this way can be very time consuming. M-Link supports using group information from a directory, to support roster prepopulation and authorization. Groups can be based on SASL userids, on an LDAP search, or on an X.500 style group held either in the configuration or in the authentication directory. More information can be found in the M-Link Administration Guide (see the final section of this document for links).

Earlier we set up a persistent chat room using MLC. In order to enter that room select **[Enter Room...]** from the **[Actions]** menu and then click on the **[Search...]** button.



Select room1 and click **[OK]** to enter. In the screenshot below you can see the MUC room from the perspective of "jane@headquarters.net" once both users have entered the room.

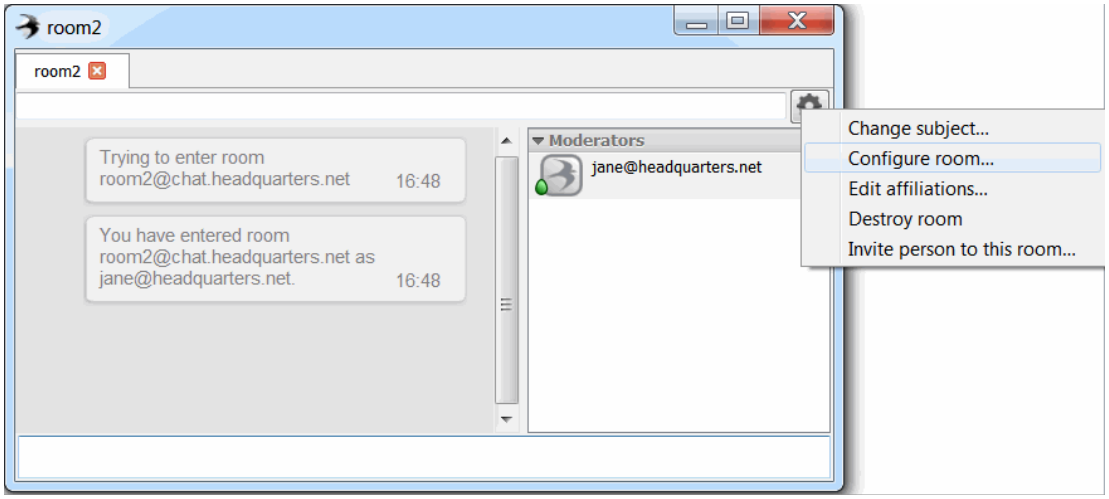



You'll note that both are listed as 'Participants' in the room as the room was created (& would therefore be moderated by) "john.smith@headquarters.net", the admin user that MLC is logged in as.

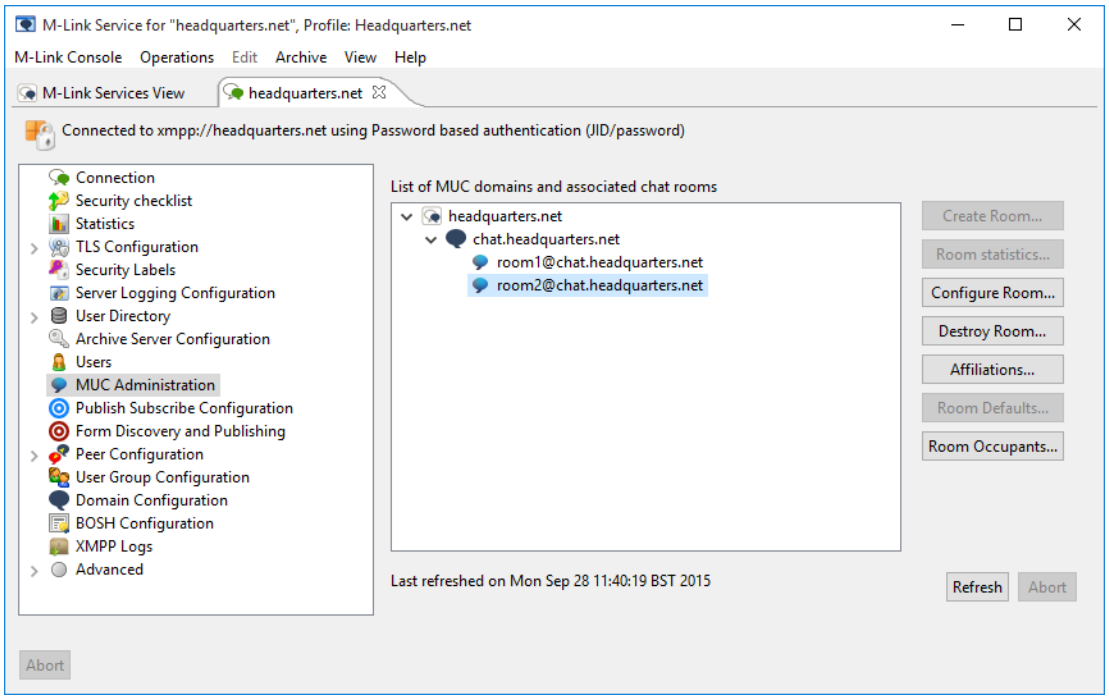
Your two users can create, as moderators, their own rooms within Swift (or many other XMPP clients) by selecting **[Enter Room...]** from the **[Actions]** menu and using the Room field to name the new MUC room. In the screenshot below we've created a new room called "room2@chat.headquarters.net"

Clicking on **[Enter Room]** will bring the creator into the room as a Moderator, with access to configuration options for that room. Rooms created in this way are ad-hoc chat rooms (that is, they will not persist once the last participant leaves or through a server restart).

As moderator, the creator of the room can configure the room so that it becomes permanent by accessing the **[Configure Room...]** menu option from the settings icon, as below. In the resulting XMPP form, the room can be made persistent.

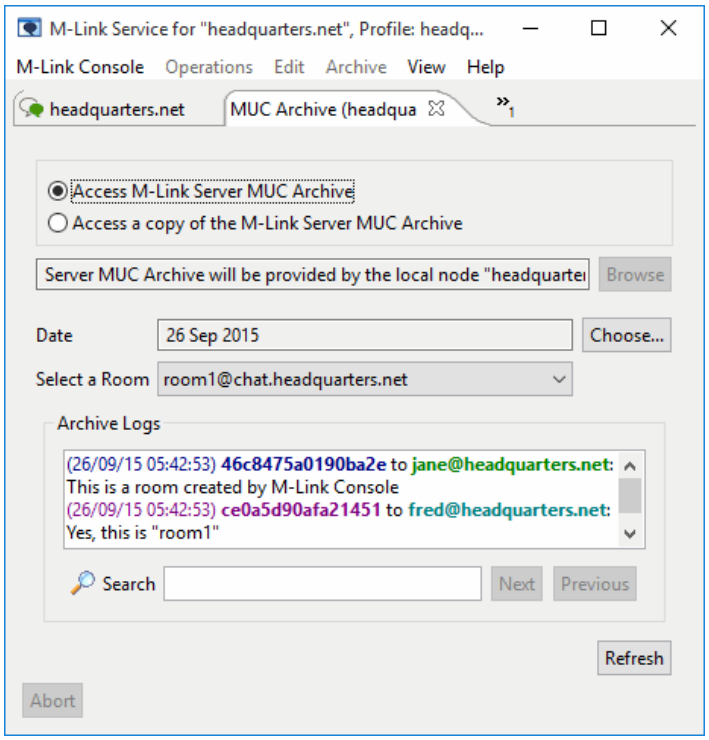



Switching back to the MUC Administration screen in MLC, you can see that this new room is now displayed (after clicking the **[Refresh]** button.




## Archive Browsing using M-Link Console

Earlier we set locations for storing logs of 1:1 and Multi-User Chat and we can use MLC to browse chat archives. In MLC Choose 'XMPP Logs' (as you did to set up archive locations) but this time click on 'view' to bring up the search pop-up. MUC logs can be searched by a combination of Date and Room. 1:1 chat logs can searched by any combination of Date, User and Contact.



# What next/other resources

## Help us improve our Evaluation Guides

Producing evaluation guides that are easy to follow and that help evaluators get started with our products is important to us. Please help us improve this guide by emailing us at customer-service@isode.com.

## Product Information

While following this guide you have installed M-Link (XMPP Server) and M-Vault (LDAP/X.500 Directory Server). For more information on these server products and the MLC Management tool, follow the links below:

- M-Link: [www.isode.com/products/m-link.html]
- M-Vault: [www.isode.com/products/m-vault-directory.html]
- M-Link Console: [www.isode.com/products/m-link-management.html]

## Further Evaluations

Evaluations of other Isode products are available from [www.isode.com/evaluate/index.html].
One further XMPP evaluation guide, which follows directly on from this one, is "XMPP for Constrained Link Environments". Isode messaging products, including M-Link, have special functionality to optimize operation over constrained links (such as HF Radio and SatCom). By the end of this new evaluation guide you will have:

- Configured two M-Link servers on separate hosts to communicate using Isode's optimized server-to-server protocol over TCP and/or over STANAG 5066 (HF Radio).
- Learned how to filter traffic types over the link.
- Set up a Federated Multi-User Chat (FMUC) room.

The guide is available from [www.isode.com/evaluate/xmpp-constrained-links.html].

## Documentation

This guide has covered only the basic functionality of Isode's M-Link server. To extend your system and explore the capabilities of M-Link further you should read the Administration Guide available from the Isode website in PDF format. The M-Link Administration Guide, together with all other Isode documentation is available from [www.isode.com/support/docs.html].

## Whitepapers

Isode regularly publishes whitepapers relevant to XMPP. All whitepapers can be searched from the whitepaper index page on the Isode website at [www.isode.com/whitepapers/index.html].

# Copyright