

Setting up an XMPP System

Using Isode's M-Link XMPP Server and Swift XMPP Client to set up an instant messaging system suitable for 1:1 and Multi-User chat. Includes setting up message archives for end-user access.

Contents

Introduction	3
Objectives	3
Using Isode Support	4
Preparation	5
Isode Products	5
Product Activation Key	5
Server Addresses	5
Edit the Hosts File	5
Use DNS Settings	5
Creating an M-Link XMPP Service using Isode's M-Vault Directory Server	6
Starting M-Link Console	6
Starting the Wizard	6
Create a Directory for User Information	7
Creating an M-Link XMPP Service using Microsoft's Active Directory	12
Starting M-Link Console	12
Starting the Wizard	12
Create a Directory for User Information	13
Configuring your M-Link Service	18
Adding a Multi-User Chat (MUC) Domain	18
Adding a Persistent MUC Room	19
Setting 1:1 and Multi-User Chat Archive Locations	19
Adding Users (M-Link + M-Vault Configuration only)	20
Testing with the Swift XMPP Client	22
Archive Browsing using M-Link Console	25
What Next?	27
Other Evaluations	27
Whitepapers	27
Copyright	28

Introduction

This guide details the process for creating an instant messaging and multi-user chat system using Isode's M-Link User Server and Swift XMPP Client. The M-Link User Server is one of a family of XMPP products which comprises:

- M-Link User Server (XMPP Server)
- M-Link Edge (XMPP Boundary Guard)
- M-Link IRC Gateway (XMPP/IRC Gateway)
- M-Link Constrained Networks (XMPP Messaging for low-bandwidth and/or high-latency networks)
- Swift (multi-platform XMPP client)

M-Link products are widely deployed in the Government, Military, and Intelligence markets.

Use of TLS: Due to UK Export Controls we are unable to provide Evaluation Licenses to certain Geographic regions that would allow the use of TLS so this guide will not configure any TLS. Should you wish to use TLS please contact your Account Manager and if you are located in an approved region we can provide a license (MAC Address of Server required) and additional instructions for configuring TLS.

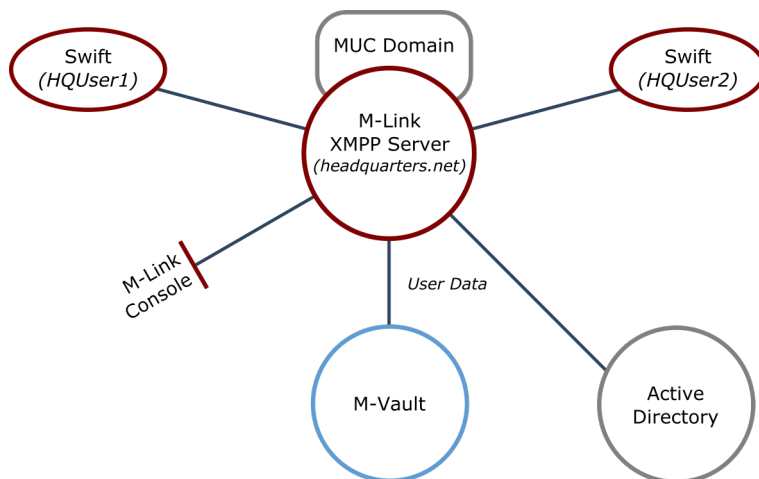
Objectives

By the end of this guide you will have:

1. Created an XMPP server (headquarters.net) on a single-node for 1:1 chat using either Isode's M-Vault Directory Server or Microsoft's Active Directory to hold user information.
2. Set up a multi-user chat domain for the XMPP server and created a permanent multi-user chat (MUC) room.
3. Set up archives for both multi-user and 1:1 chats.
4. Created users for the XMPP service and tested 1:1 and multi-user chat.

You'll use the M-Link Console (MLC) management GUI to set up your system. MLC is Isode's central tool for XMPP system Configuration and Operational management for all products in the M-Link family.

The diagram which follows shows the main elements of the system.



For the purposes of this evaluation we have assumed this is a "clean" installation of M-Link User Server on to a physical or virtual machine. If you have previously installed an M-Link product on the hardware or VM you are using for this evaluation, please make sure you have completely uninstalled that version before proceeding.

Using Isode Support

You will be given access to Isode support resources when carrying out your evaluation. Any queries you have during your evaluation should be sent to support@isode.com. Please note that access to the Self-Service Portal for web-based ticket submission and tracking is not available to evaluators.

Preparation

You should visit www.isode.com/products/supported-platforms.html to discover which operating systems are supported for Isode evaluations. Please note that in addition to the server platforms listed, we support the use of Isode servers on Windows 8, Windows 8.1 and Windows 10 for simple evaluations and demonstrations.

Isode Products

Product downloads are held in a password-protected section of the Isode website. If you have not already done so you should apply for a username/password by filling in the form located at www.isode.com/evaluate/evalrequest.html.

Products can be obtained by clicking on the links in the “Download Links” section of the Evaluation page (www.isode.com/evaluate/evaluate-xmpp.html). The downloads page will give installation instructions specific to your platform.

Product Activation Key

Isode server products require a valid Product Activation Key from Isode before they will run correctly. Keys are issued by Isode Customer Services. If you haven't already been sent a Key when requesting access to the evaluation files, please send a message to request one to support@isode.com remembering to specify which Isode server products you need a Key for.

By default, the file you receive needs to be placed in `\Isode\etc\` (Windows) or `/etc/isode/` (Linux), renamed 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.

Server Addresses

M-Link Console 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 have two options to ensure correct functioning of MLC (M-Link Console).

Edit the Hosts File

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
```

Use DNS Settings

Alternatively, you can use DNS instead of the Hosts file, to use DNS 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 M-Link XMPP Service using Isode's M-Vault Directory Server

M-Link uses an LDAP Directory Server to hold user information. In this section we're going to use Isode's M-Vault for this purpose. Skip this section if you are using Microsoft's Active Directory for this purpose.

Starting M-Link Console

In Windows click Start, and from the Programs menu, select 'Isode 17.0 > M-Link Console'. In Linux execute the following command:

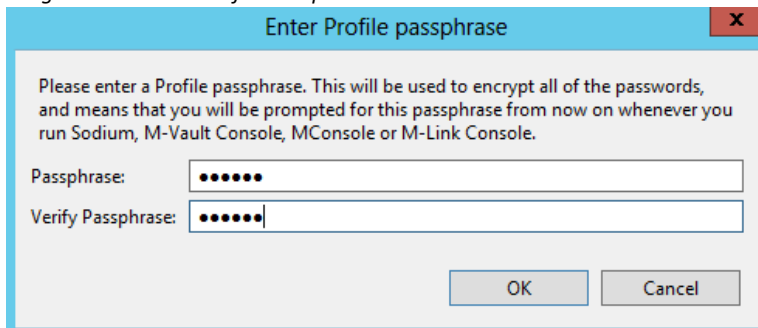
```
% /opt/isode/bin/mlc
```

If you're running Windows 7, 8 or 10 you will need to run Isode Management tools (like MLC) as an Administrator. You can do this by right-clicking on the program icons and choosing "Run as administrator" from the pop-up.

Starting the Wizard

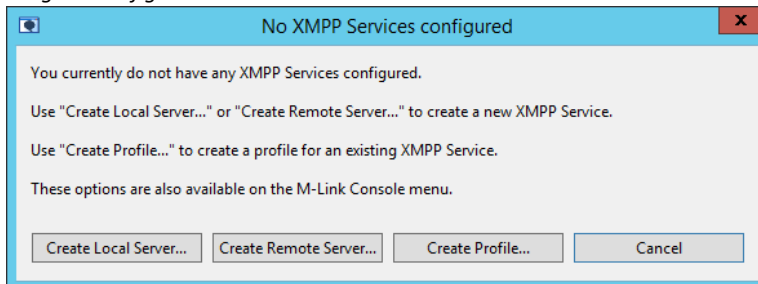
If this is the first time you've used any of the Isode management GUI tools, you will not yet have Isode profile settings saved and will be asked if you wish to encrypt your bind profile (answer "Yes") and will then prompted to set and confirm a password for that profile (Image 1).

Image 1: Enter Bind Profile Passphrase



If you have already created an Isode bind profile as part of another evaluation, you will be prompted for your passphrase. Once you have created the profile, or entered your passphrase, click [OK] and MLC will launch. If you don't currently have any XMPP services configured, you'll be prompted to create one (Image 2).

Image 2: Configure XMPP Services



In the next screen (Image 3) you'll be prompted to specify the **Domain Name** and **Display Name**

for your IM service, in this guide we're using "Headquarters.net". Enter this value for both fields and then click [Next].

Image 3: Specify the domain

Create a Directory for User Information

Whilst M-Link could use an existing directory server to hold user information, in this guide you'll create a new one. In the next screen, Image 4, choose the "Create a new directory and use that" radio button and fill in a name for the Administrator. Click [Next].

Image 4: Directory for User Information

Accept the defaults in the DIT structure configuration screen (not shown) and click [Next] again.

In the **Password configuration** screen (Image 5), Administrator and M-Link Server passwords will be automatically generated. Either change these to values you'll remember or make a note of the auto-generated ones (by ticking "show") before clicking [Next] again.

Image 5: Password configuration

Create Directory Server

Password configuration
Passwords are auto-generated, but can be modified here if required

Administrator's Password: cn=Mlink Admin,cn=Users,o=XMPP
Password: Show

M-Link Server's Password: cn=M-Link server for headquarters.net,cn=Users,o=XMPP
Password: Show

Record user authentication times (authTimestamps)

Password Hashing
Hashed passwords are more secure, but are not compatible with password-based SASL mechanisms other than PLAIN, LOGIN and SCRAM-SHA-1.
Note that while non-hashed passwords may be recovered from the DSA database, hashed passwords are NOT recoverable.
 Hash all passwords using SCRAM-SHA-1

MLC will create and display Bind profile name and file system location for the Directory (Image 6). Accept the defaults in these two fields and click [Next].

Image 6: Bind Profile Names & Filesystem Location

Create Directory Server

Bind Profile Names and Filesystem Location
Use the suggested values, or enter your own

Management bind profile name: Used to manage the DSA in M-Vault Console

The folder which will contain the directory server's database and configuration (this folder will be created in order to initialize the DSA):

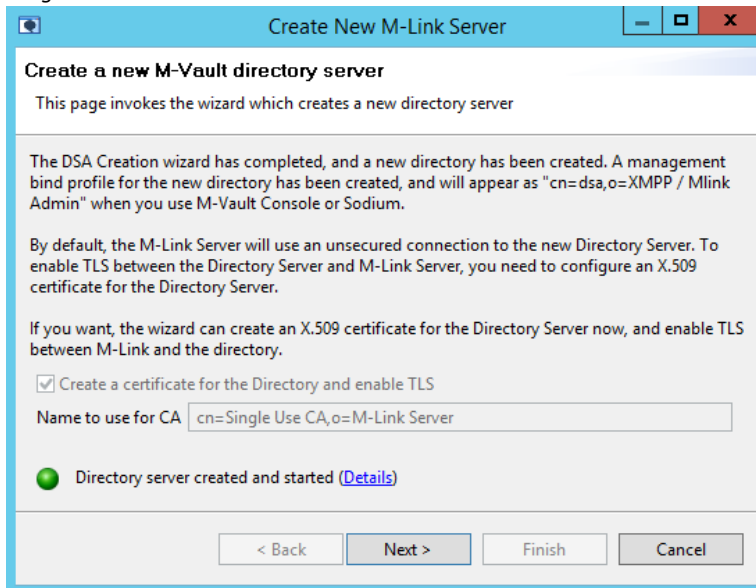
On the next two screens, **Address Configuration & Confirm Details** (not shown) accept the defaults and click [Finish] at the end.

You've now completed the directory creation process.

This directory will be used to hold user information for your XMPP service.

In the next screen (Create a New M-Link Server – Image 7) click on [Next] to begin the process of creating the M-Link XMPP Server.

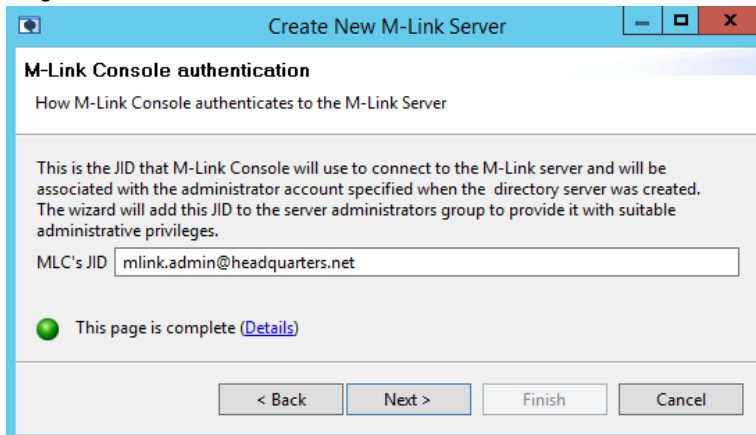
Image 7: Create a New M-Link Server



MLC is an XMPP client and needs to use an identity to connect to M-Link, as does any XMPP client. By default, it will use the identity of the initial operator/Administrator we set earlier (see Image 4).

The first stage in M-Link Server creation will pre-fill that identity (Image 8), accept this default and click [Next].

Image 8: M-Link Console authentication



In the **M-Link Server directory Paths** and **Archive Server Details** screens (not shown) accept the defaults and click [Next].

In the **Http Connection Details for Archive Server** screen (Image 9), accept the defaults and click [Next].

Image 9: Http Connection Details for Archive Server

Create New M-Link Server

Http Connection Details for Archive Server

Use this page to provide http host and port to be used by M-Link Console for connecting to the Archive Server

The Archive server maintains chat archives for the M-Link Service. To allow M-Link Console to access archives via Archive, you need to provide the HTTP host and port of the Archive server for this M-Link Service.

Archive Server's HTTP details

Archive Http Host:

Archive Http Port:

Page is complete [\(Details\)](#)

M-Link encrypts sensitive configuration data using a passphrase, in the next stage (Image 10) a random passphrase will be set. It's important that you make a note of this passphrase or change it to something else. Click **[Next]**.

Image 10: M-Link Server password

Create New M-Link Server

M-Link Server password

The password used by all the cluster members

The M-Link Server encrypts sensitive configuration data using a passphrase.

The passphrase is REQUIRED whenever a new server is added to a clustered configuration. So you MUST make a note of it if you anticipate adding cluster nodes.

The passphrase must be at least 16 characters and contain a mixture of digits and upper and lower case letters.

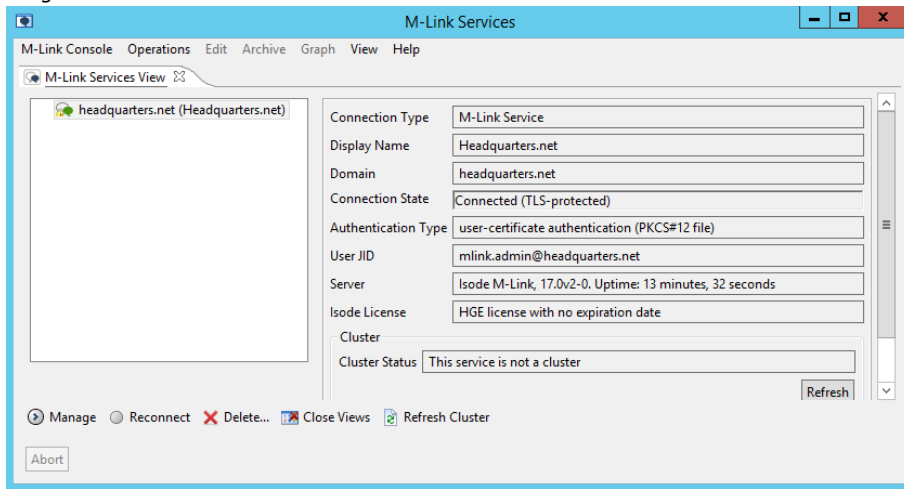
Passphrase: Show

This page is complete [\(Details\)](#)

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 (Image 11) and you'll see that your M-Link Service, 'Headquarters.net', is now active.

Image 11: M-Link Services



Creating an M-Link XMPP Service using Microsoft's Active Directory

M-Link uses an LDAP Directory Server to hold user information. In this section we're going to use Microsoft's Active Directory for this purpose.

If you have an AD certificate for Client and Server Authentication on your Active Directory server, you will require a TLS (HGE) License for your M-Link Server, without this you will not be able to complete your M-Link configuration.

Starting M-Link Console

In Windows click Start, and from the Programs menu, select 'Isode 17.0 > M-Link Console'. In Linux execute the following command:

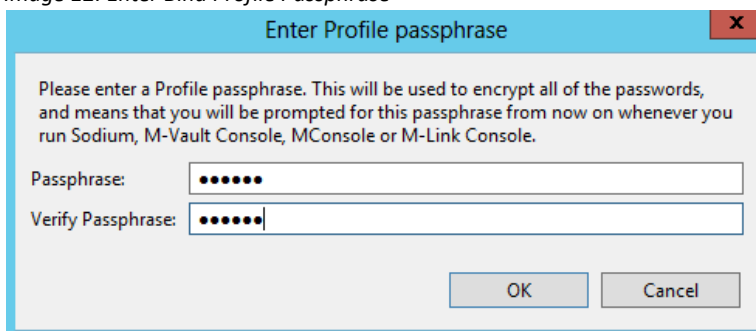
```
% /opt/isode/bin/mlc
```

If you're running Windows 7, 8 or 10 you will need to run Isode Management tools (like MLC) as an Administrator. You can do this by right-clicking on the program icons and choosing "Run as administrator" from the pop-up.

Starting the Wizard

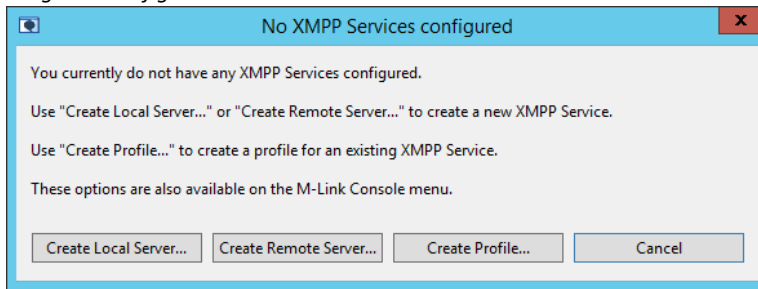
If this is the first time you've used any of the Isode management GUI tools, you will not yet have Isode profile settings saved and will be asked if you wish to encrypt your bind profile (answer "Yes") and will then prompted to set and confirm a password for that profile (Image 12).

Image 12: Enter Bind Profile Passphrase



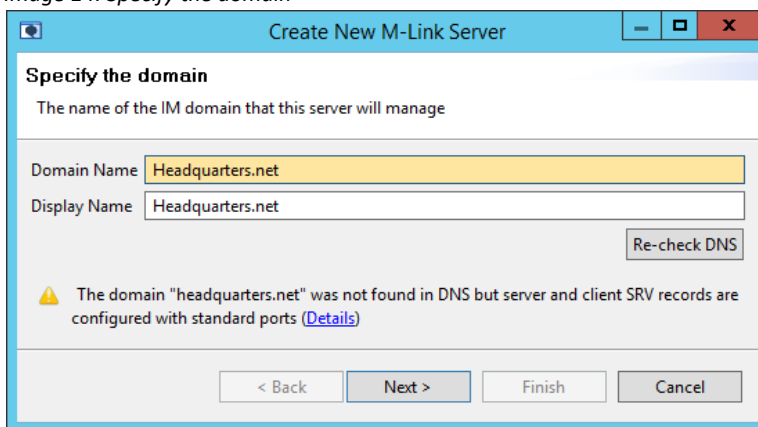
If you have already created an Isode bind profile as part of another evaluation, you will be prompted for your passphrase. Once you have created the profile, or entered your passphrase, click [OK] and MLC will launch. If you don't currently have any XMPP services configured, you'll be prompted to create one (Image 13).

Image 13: Configure XMPP Services



In the next screen (Image 14) you'll be prompted to specify the **Domain Name** and **Display Name** for your IM service, in this guide we're using "Headquarters.net". Enter this value for both fields and then click [**Next**].

Image 14: Specify the domain



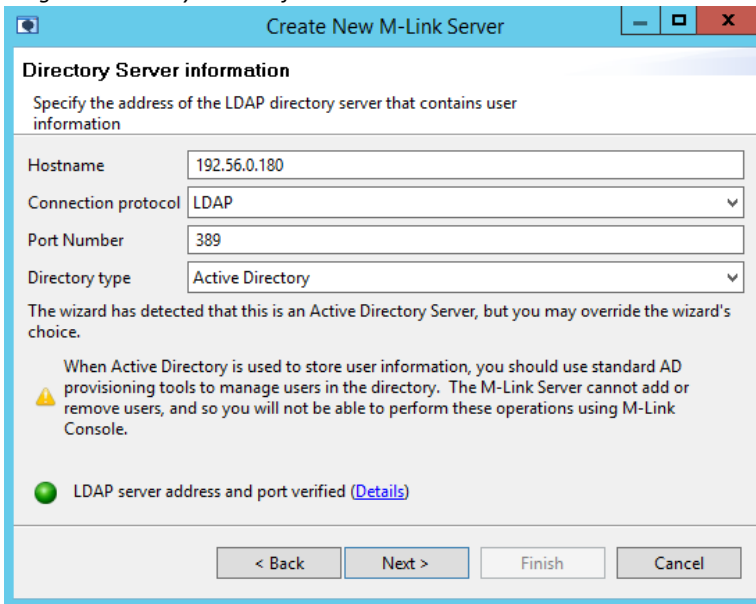
Create a Directory for User Information

At the **Directory user information screen** (Image 15) select the "Use an Existing Directory" radio button 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 (Image 15).

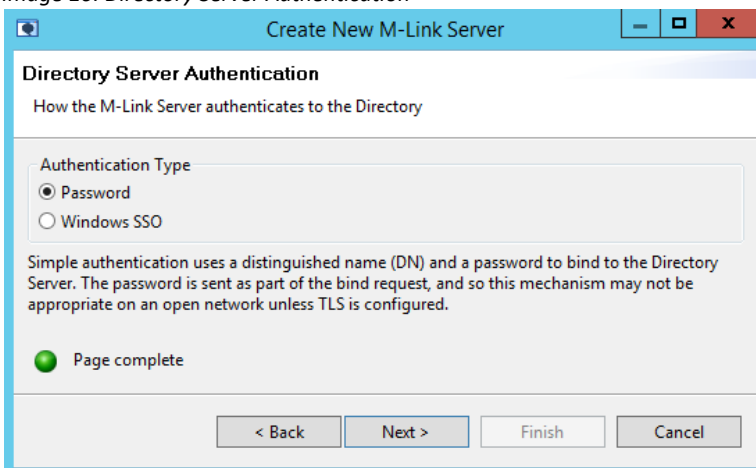
The wizard will also attempt to determine the directory type (i.e. Active Directory) automatically. You will not be able to proceed past this step unless you can supply details of a directory that is contactable. Click [**Next**] once you have established connection with AD.

Image 15: Directory Server information



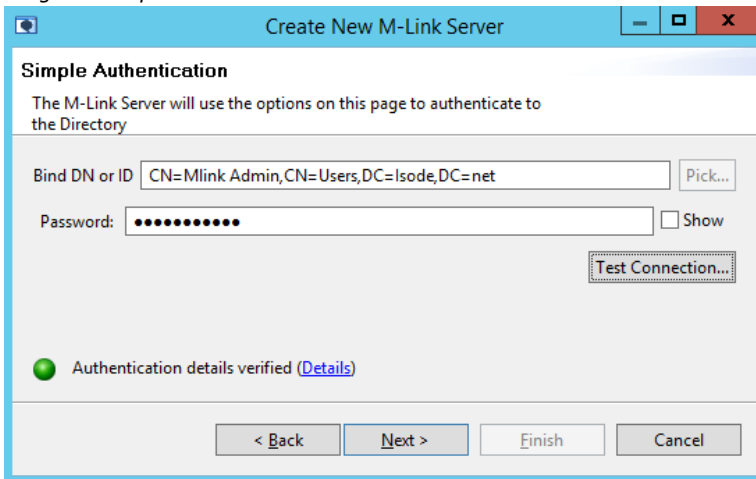
For the purposes of this evaluation, at the **Directory Server Authentication** screen (Image 16).

Image 16: Directory Server Authentication



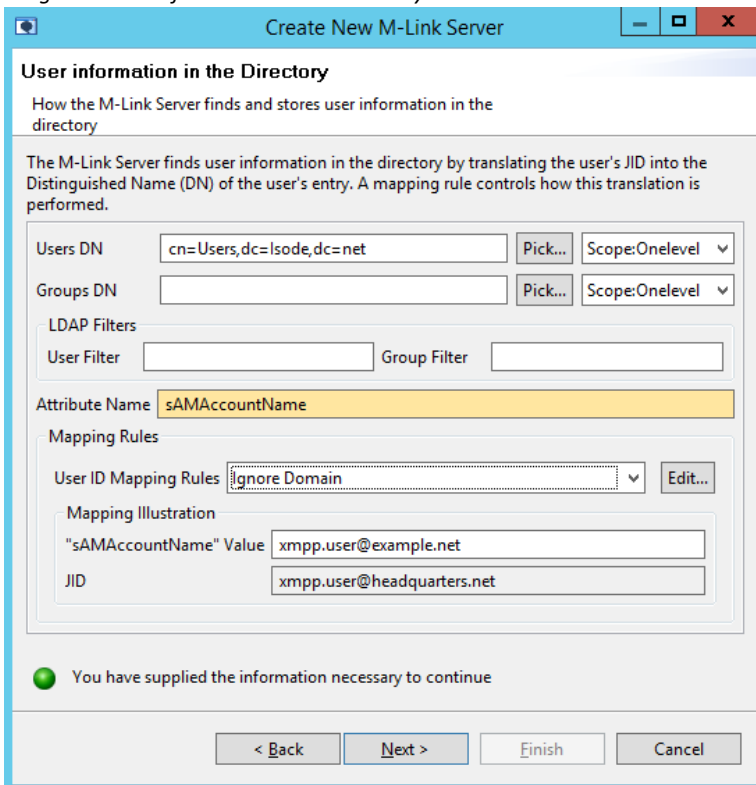
At the **Simple Authentication** screen (Image 17) type in a bind name of a user in AD, this is case sensitive. Click [Next] and at the Peer and LDAP Trust Anchors screen (not shown) click [Next] again.

Image 17: Simple Authentication



At the **User information in the Directory** screen (Image 19), the “Users DN” should already be populated with the correct DIT structure of your AD environment. If it is not correct, type in the DIT structure manually. In “Attribute Name” type in “sAMAccountName,” select the “Ignore Domain” option from the “User ID Mapping Rules” drop down menu, Click [Next] and [Next] again at the “Read User Passwords” screen (not shown).

Image 18: User information in the Directory



At the **M-Link Console authentication** screen (Image 19) type in a user from AD you want to authenticate with, the example that follows is using the same user as in the Simple Authentication screen. You can select any user you want as long as they are in the same DIT structure defined in the Search Users DN, click [Next].

Image 19: M-Link Console authentication

M-Link Console authentication

How M-Link Console authenticates to the M-Link Server

M-Link Console needs to connect to the M-Link Server using an operator JID. This page lets you specify the JID and password which will be used. The wizard will add this JID to the server administrators group to provide it with suitable administrative privileges.

MLC's JID

The password corresponding to the supplied JID, as stored in the directory. M-Link Console will store these credentials in your bind profile file, and use them when connecting to the server

Password: Show

The page is complete but cannot be verified by the wizard ([Details](#))

Accept the defaults in **M-Link Server Directory Paths** screen, the **Archive Server Details** screen (not shown) and the **Http Connection Details for Archive Server** screen (Image 20), clicking [Next] through all.

Image 20: Http Connection Details

Http Connection Details for Archive Server

Use this page to provide http host and port to be used by M-Link Console for connecting to the Archive Server

The Archive server maintains chat archives for the M-Link Service. To allow M-Link Console to access archives via Archive, you need to provide the HTTP host and port of the Archive server for this M-Link Service.

Archive Server's HTTP details

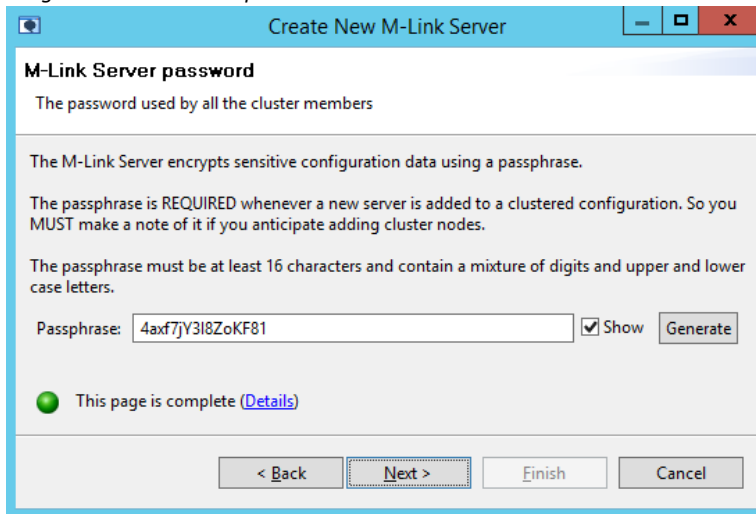
Archive Http Host

Archive Http Port

Page is complete ([Details](#))

M-Link encrypts sensitive configuration data using a passphrase, in the **M-Link Server password** screen (Image 21) a random passphrase will be set. It's important that you make a note of this passphrase or change it to something you will remember. Click [Next].

Image 21: M-Link Server password



The final screen (not shown) will confirm the configuration you've just created. Click [**Finish**] and MLC will save your configuration and start M-Link.

Configuring your M-Link Service

In the next section we're going to configure the XMPP service for use, including adding Users and a Multi-User Chat (MUC) domain.

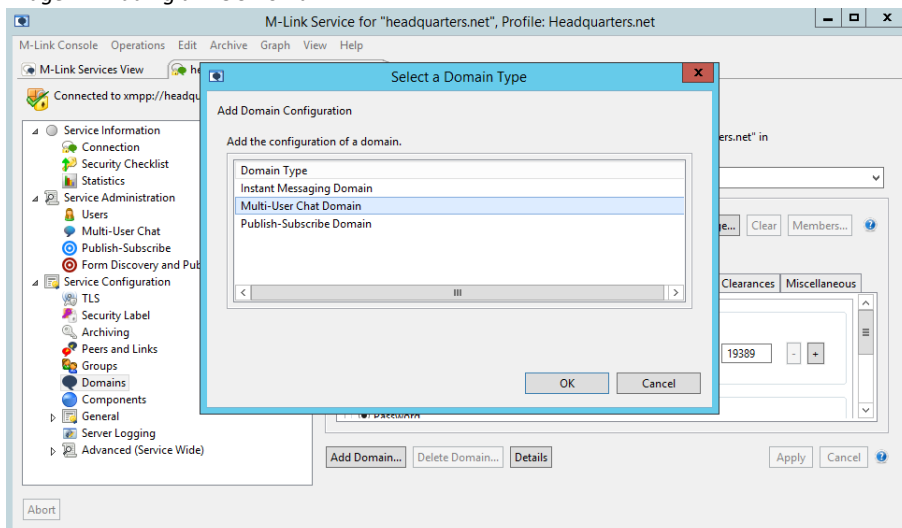
Adding a Multi-User Chat (MUC) Domain

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.

In MLC, 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.

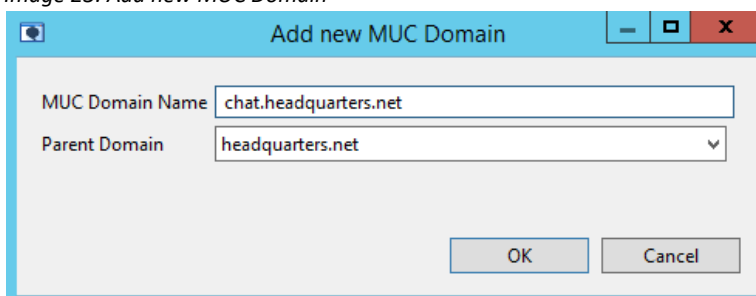
Expand **Service Configuration** from the left-hand pane, select **Domains** and then click the [**Add domain**] button. In the resulting pop-up (Image 22) select 'Multi-User Chat Domain' and click on [**OK**].

Image 22: Adding a MUC Domain



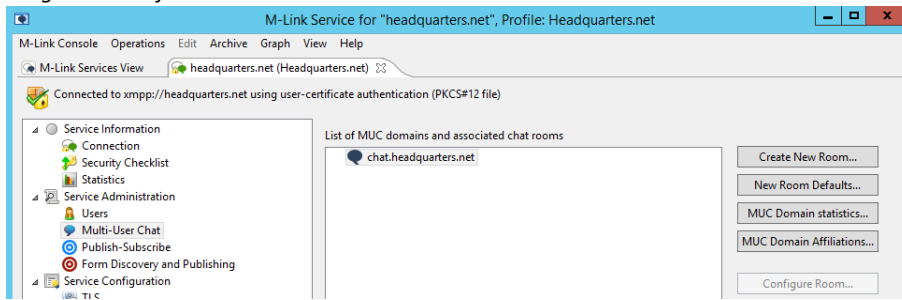
In the **Add new MUC Domain pop-up** (Image 23) fill in the muc domain name “chat.headquarters.net” and the parent domain name “headquarters.net” and click [**OK**] to confirm the changes.

Image 23: Add new MUC Domain



Back in the main MLC screen, expand **Service Administration** and select **Multi-User Chat** (Image 24), you'll now see the MUC domain associated with headquarters.net.

Image 24: List of MUC domains



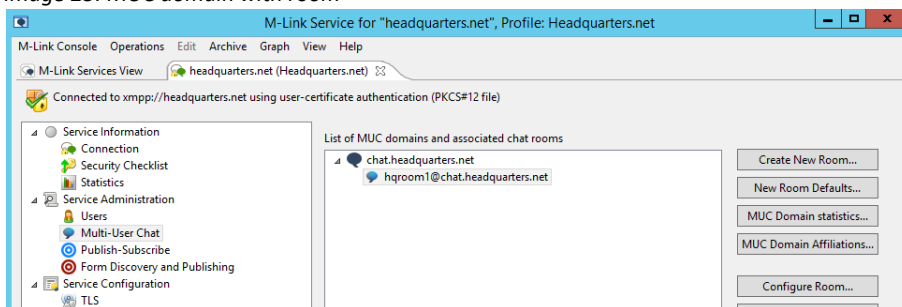
Note: We've created one MUC domain for the headquarters.net service however, a service can contain multiple MUC domains. You may for instance wish to create different MUC domains to match requirements of your organization's security policy, with an entire MUC domain reserved for users of a certain security 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 service 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 New Room]** button. Give the room a name but at this stage don't apply a password or customize the room settings.

Click on **[OK]** and, after the confirmation message, the new room will appear in the administration screen (Image 25).

Image 25: MUC domain with room



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]**.

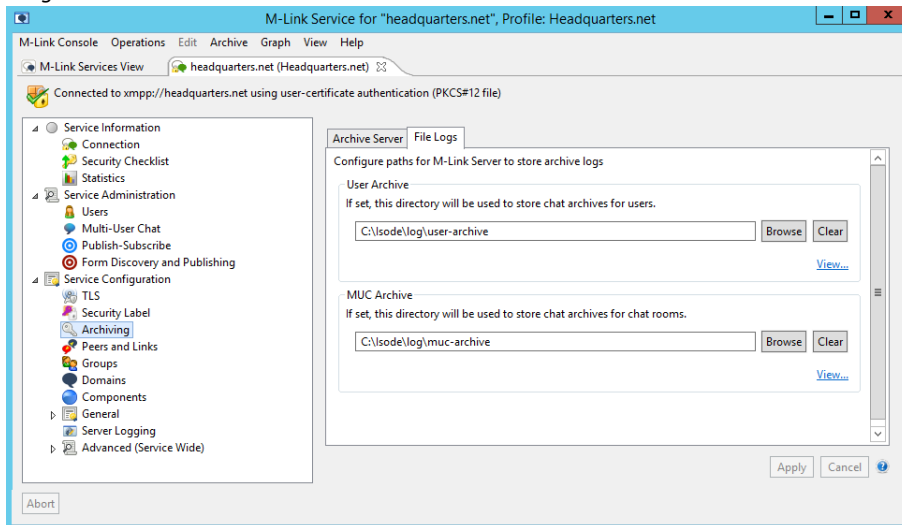
Setting 1:1 and Multi-User Chat Archive Locations

A common administrative requirement is for archives to be kept of both 1:1 chat sessions and multi-user chat sessions. In this section we'll set locations for storing those archives.

If you have a Windows OS browse to C:\Isode\log and create the following folders user-archive and muc-archive. If you have a Linux OS, browse to: \var\isode\log

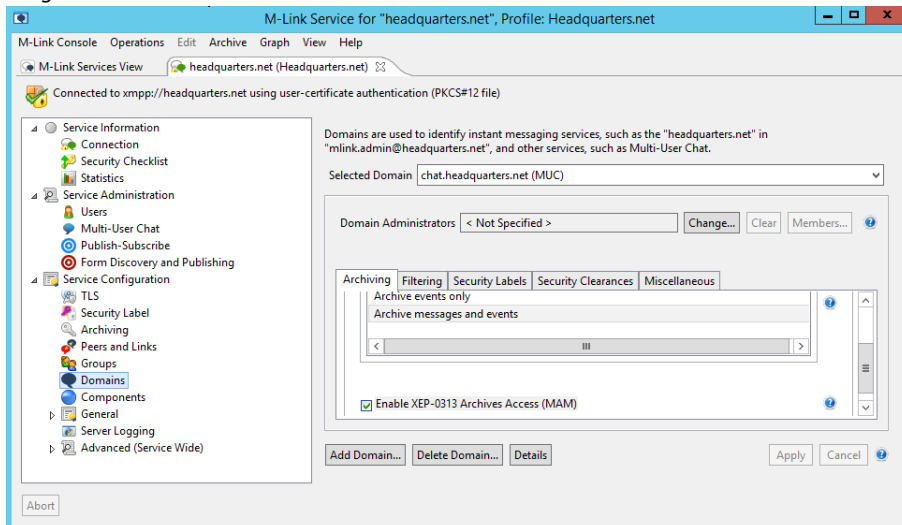
Expand **[Service Configuration]**, select **[Archiving]** and click on the File Logs tab. Browse to the folder you just created for user and MUC archives (Image 26), click **[Apply]**.

Image 26: Archive Locations



Go to “Domains” within “Service Configuration”, select the headquarters.net domain, click “Archive messages and event” and tick the “Enable XEP-0313 Archives Access (MAM)”, click [Apply] and then repeat this process for the chat.headquarters.net domain (Image 27). You’ll need to restart the server (by choosing “Restart local M-Link Server” from the “Operations” menu) to enable Archive browsing.

Image 27: Archive Domains



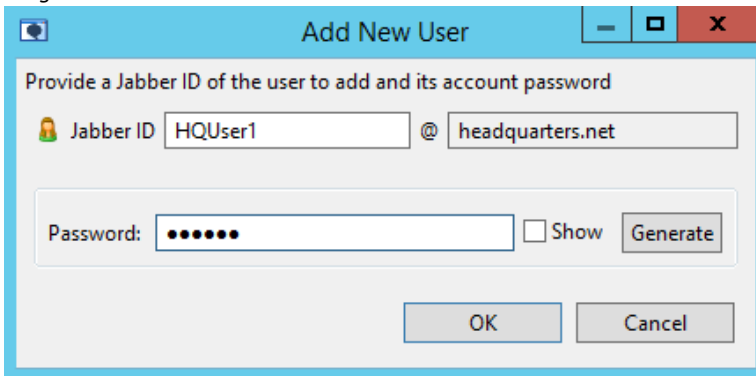
Adding Users (M-Link + M-Vault Configuration only)

We now have an XMPP service, running on one node with a single MUC domain. Within that MUC domain we have a single permanent MUC room.

We do not currently have any users of the XMPP service. In many situations you'd connect to an existing Directory (such as Isode's M-Vault or Active Directory) for user information but here we're going to use MLC to create new user entries in the M-Vault directory we've already set up. Select "Service Administration/Users" in the left pane and click on [Add User].

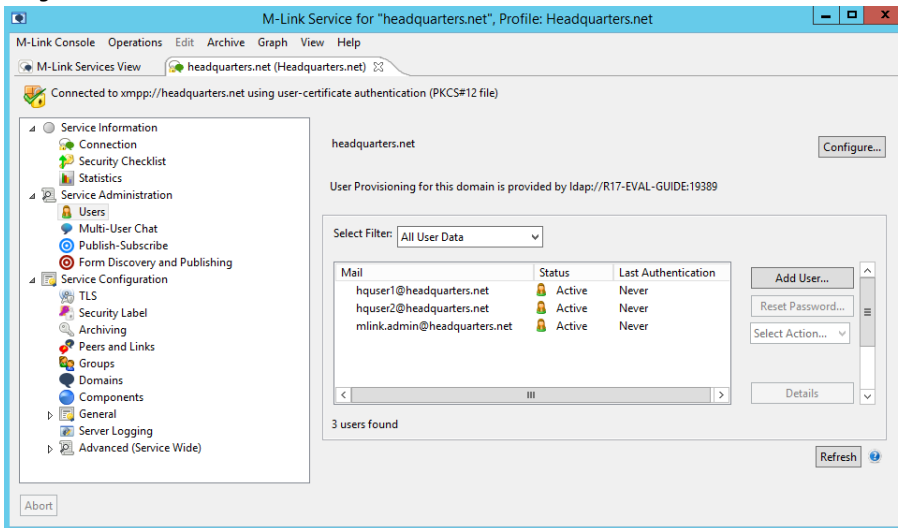
The minimum required information for each user is Jabber ID and password. Add the users “HQUser1@headquarters.net” and “HQUser2@headquarters.net” and make a note of the passwords you set.

Image 28: Add New User



Click on [OK] after setting up each user to be returned to the main MLC screen (Image 29).

Image 29: Users



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.

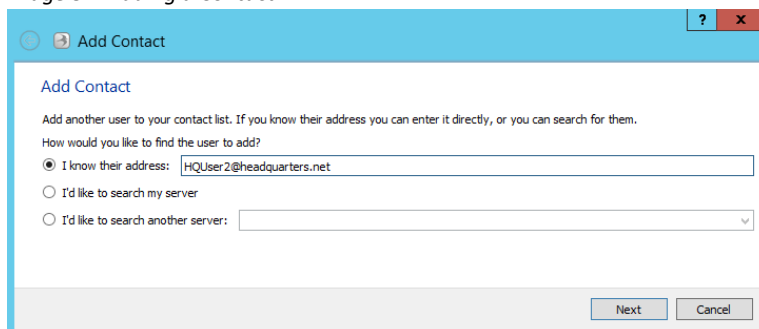
Launch Swift and log in using the address and password details for “*HQUser1@headquarters.net*”.

Image 30: Logging into Swift



You can run multiple copies of the Swift client, so launch Swift again, this time logging in as “*HQUser2@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 (Image 31).

Image 31: Adding a Contact

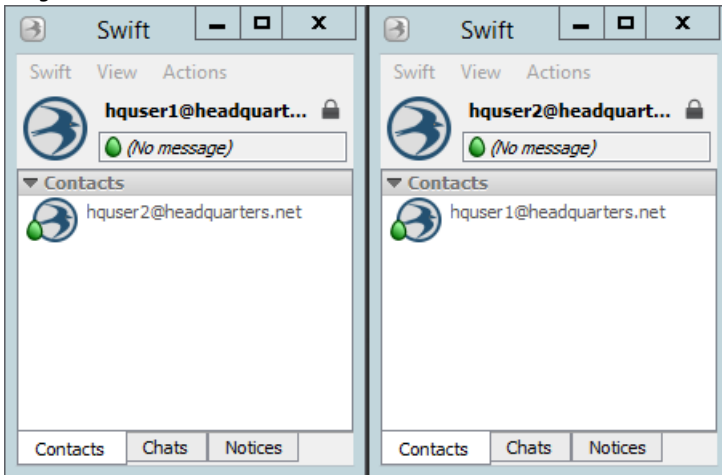


Click [**Next**] and give the contact a name (or select their JID as the name for your roster) and click Finish. We're not going to create any group contacts at this stage.

When the HQUser2 user receives and accepts the request, each will appear in the other's roster

(Image 32) and you can now engage in 1:1 chat between your two users.

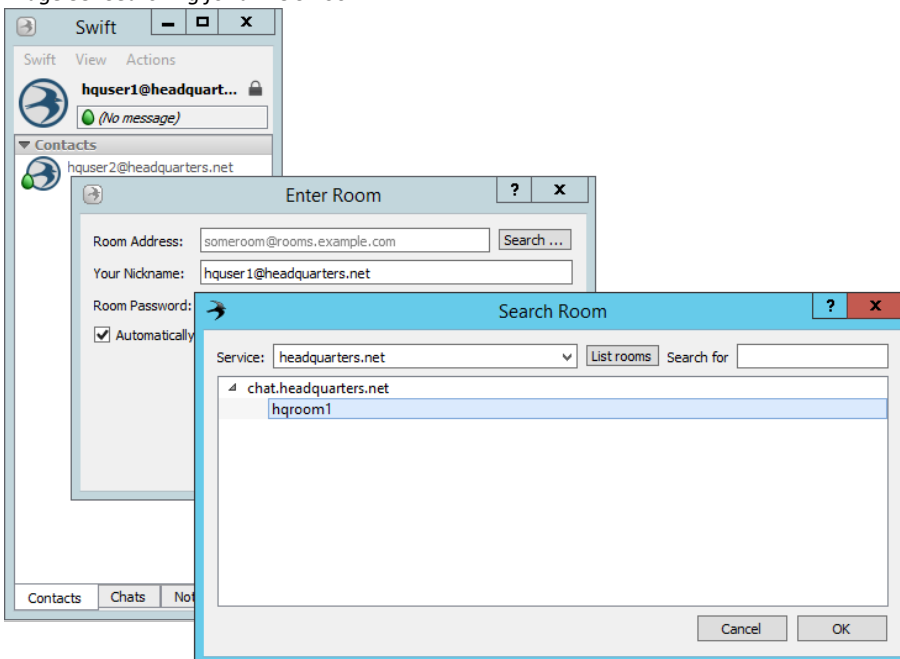
Image 32: User Rosters



***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 (Image 33).

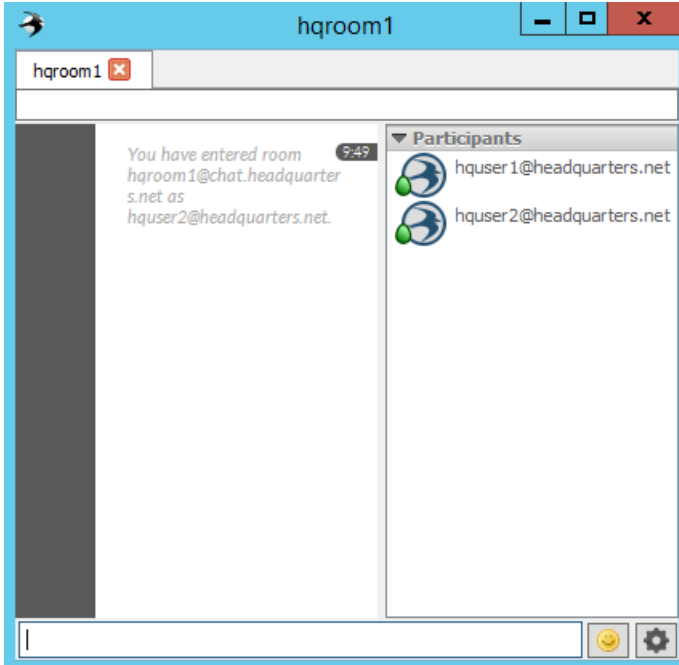
Image 33: Searching for a MUC Room



Select “hqroom1” and click [**OK**] to enter. In Image 34 you can see the MUC room from the

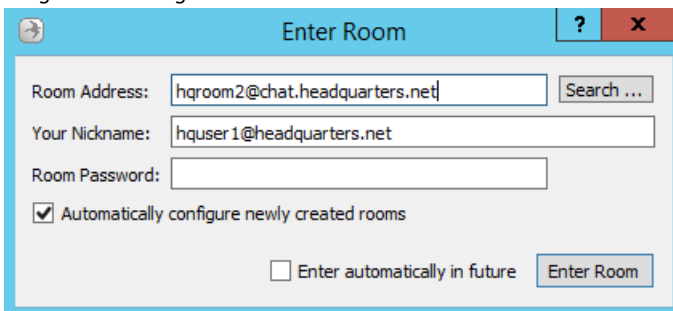
perspective of “*HQUser1@headquarters.net*” once both users have entered the room. You'll note that both are listed as 'Participants' in the room as the room was created (& would therefore be moderated by) “*HQUser2@headquarters.net*”, the admin user that MLC is logged in as.

Image 34: MUC Room



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 Image 35 we've created a new room called “*hqroom2@chat.headquarters.net*”

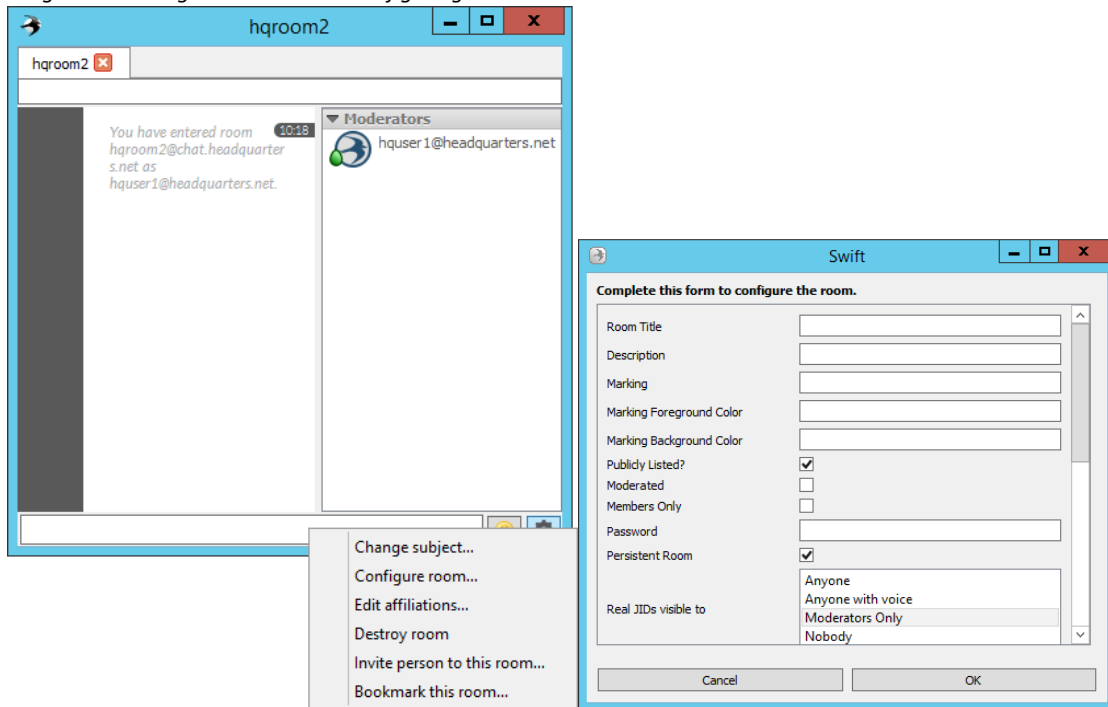
Image 35: Creating a MUC Room



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).

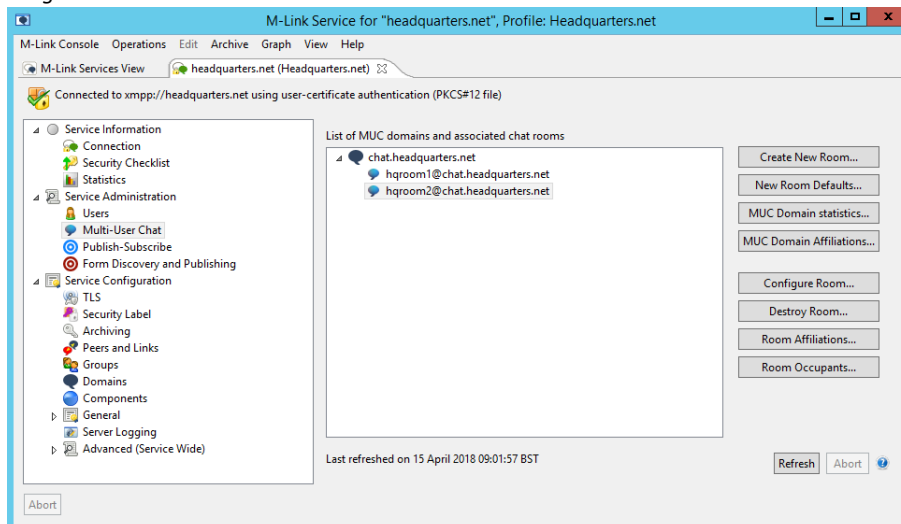
As moderator, the creator of the room can configure the room so that it becomes permanent by accessing the [**Configure Room...**] menu option from the settings icon. In the resulting XMPP form, the room can be made persistent (Image 36).

Image 36: Entering a MUC Room & Configuring as a Moderator



Switching back to the Multi-User Chat screen in MLC, you can see that this new room is now displayed, after clicking the **[Refresh]** button, in Image 37.

Image 37: New MUC Room

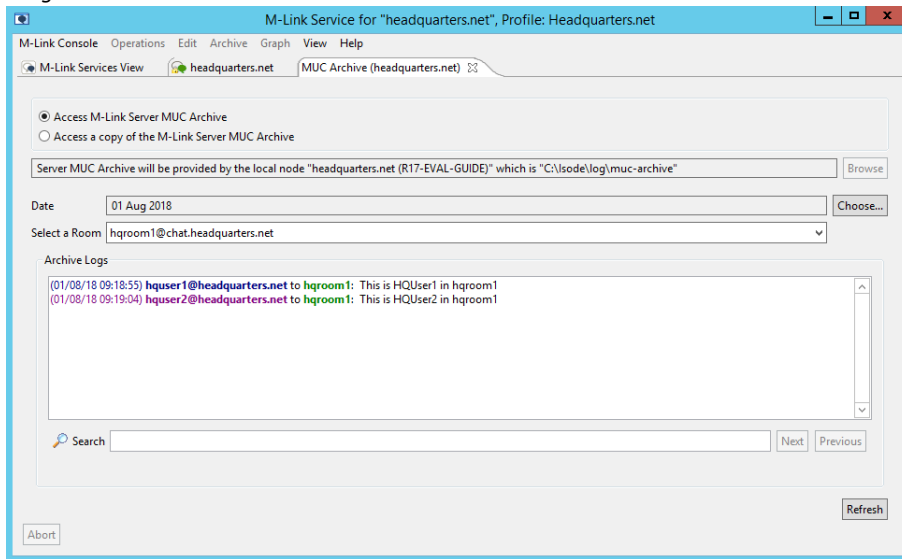


Archive Browsing using M-Link Console

Earlier we set locations for storing logs of 1:1 and Multi-User Chat. On the assumption that you've now engaged in chat between the users of the XMPP service we can use MLC to browse archives of those conversations. In MLC expand **[Service Configuration]**, select **[Archiving]** and click on the File Logs tab (as you did to set up archive locations) but this time click on 'view' next to MUC archive to bring up the search screen.

Select the "Access M-Link Server MUC Archive". 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 (the contact with whom the user was chatting). In Image 38, the `hqroom@chat.headquarters.net` has been selected, showing the room history.

Image 38: Archives



What Next?

More information on the M-Link User Server can be found on the Isode website at www.isode.com/products/m-link.html.

Information on the Swift XMPP client can be found at www.isode.com/products/swift.html.

Detailed configuration and operational information on all variations of M-Link can be found in the M-Link Administration Guide available from the Isode website at www.isode.com/support/help.html.

Other Evaluations

This guide is one of three relating to Isode's XMPP products:

- [Setting up an XMPP System for 1:1 and Multi-User Chat \(this guide\)](#)
- [Connecting XMPP and IRC Chat Services](#)
- [XMPP for Constrained Network Environments](#)

Information on all of these evaluations can be found at www.isode.com/evaluate/evaluate-xmpp.html. For XMPP evaluations outside of the scope of these guides, please contact us.

Whitepapers

Isode regularly publishes whitepapers on technical and market topics related to its products. A full list of these can be found at www.isode.com/whitepapers/.

Copyright

The Isode Logo and Isode are trade and service marks of Isode Limited.

All products and services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations, and Isode Limited disclaims any responsibility for specifying which marks are owned by which companies or organizations.

Isode software is © copyright Isode Limited 2002-2018, All rights reserved.

Isode software is a compilation of software of which Isode Limited is either the copyright holder or licensee. Acquisition and use of this software and related materials for any purpose requires a written licence agreement from Isode Limited, or a written licence from an organization licensed by Isode Limited to grant such a licence.

This manual is © copyright Isode Limited 2018.