MLINKADM-17.0

M-Link Administration Guide

Isode

Table of Contents

1 Software version

This guide is published in support of Isode M-Link R17.0. It may also be pertinent to later releases. Please consult the release notes for further details.

2 Readership

This guide is intended for administrators who plan to configure and manage *Extensible Messaging and Presence Protocol* (XMPP) services using Isode M-Link R17.0.

3 How to use this guide

You are advised to read through Chapter 1, *Isode M-Link Overview* before you start to set up your XMPP service. You may also want to review Appendix L, *Glossary* as you come across technical terms you are not familiar with.

4 Typographical conventions

The text of this manual uses different typefaces to identify different types of objects, such as file names and input to the system. The typeface conventions are shown in the following table and subsequent note.

Object	Examples
Applications	M-Link Server
Literals (domain names, IP addressses, DNs, etc.).	`example.com`, `192.0.2.1`, `cn=Example`
File and folder (directory) names	*C:\isode*
Commands and program options	**unique_id** `--verbose`
GUI elements	**Label**, **Menu**, **Menu Item**, **Sub-Menu**
User input	`hello!`
Citation, glossary terms, and cross references	[[RFC6120]], *Glossary term*, Section 4, “Typographical conventions” (cross reference).
Additional information to note, or a warning that the system could be damaged by certain actions.	Notes are additional information; cautions are warnings.

Note: This is an example of a note.

5 File system place holders

Where directory names are given in the text, they are often place holders for the names of actual directories where particular files are stored. The actual directory names used depend on how the software is built and installed. All of these directories can be changed by configuration.

Certain configuration files are searched for first in *(ETCDIR)* and then *(SHAREDIR)*, so local copies can override shared information.

The actual directory defaults vary, depending on whether the platform is *Windows* or *Unix*. The following table provides the platforms-specific defaults.

Name	Place holder for the directory used to store...	Windows	Unix
(ETCDIR)	System-specific configuration files	*C:\Isode\etc*	*/etc/isode*
(SHAREDIR)	Configuration files that may be shared between systems	*C:\Program Files\Isode\share*	*/opt/isode/share*
(BINDIR)	Programs run by users	*C:\Program Files\Isode\bin*	*/opt/isode/bin*
(SBINDIR)	Programs run by the system administrators	*C:\Program Files\Isode\bin*	*/opt/isode/sbin*
(LIBDIR)	Libraries	*C:\Program Files\Isode\bin*	*/opt/isode/lib*
(DATADIR)	Storing local data	*C:\Isode*	*/var/isode*
(LOGDIR)	Log files	*C:\Isode\log*	*/var/isode/log*
(MSDIR)	M-Link working directory	*C:\Isode\ms*	*/var/isode/ms*
(MSUSERDIR)	M-Link user data directory	*C:\Isode\ms\user*	*/var/isode/ms/user*

6 Support queries and bug reporting

A number of email addresses are available for contacting Isode. Please use the address relevant to the content of your message.

- For all account-related inquiries and issues: customer-service@isode.com. If customers are unsure of which list to use then they should send to this list. The list is monitored daily, and all messages will be responded to.
- For all licensing related issues: license@isode.com.
- For all technical inquiries and problem reports, including documentation issues from customers with support contracts: support@isode.com. Customers should include relevant contact details in initial calls to speed processing. Messages which are continuations of an existing call should include the call ID in the subject line. Customers without support contracts should not use this address.
- For all sales inquiries and similar communication: sales@isode.com.

Bug reports on software releases are welcomed. These may be sent by any means, but electronic mail to the support address listed above is preferred. Please send proposed fixes

with the reports if possible. Any reports will be acknowledged, but further action is not guaranteed. Any changes resulting from bug reports may be included in future releases.

Isode sends release announcements and other information to the Isode News email list, which can be subscribed to from the address: http://www.isode.com/company/contact.html

7 Export controls

Many Isode products use protocols and algorithms to encrypt data on connections. If you license the higher grade encryption (HGE) Isode products they are subject to UK Export controls.

You must ensure that you comply with these controls where applicable, i.e. if you are licensing or re-selling Isode products outside the Community with the HGE option selected.

All Isode Software is subject to a license agreement and your attention is also called to the export terms of your Isode license.

Note: An HGE-TLS license is generally required to allow M-Link Server use of *TLS* as it will not generally allow use of TLS with low-grade encryption.

Chapter 1 Isode M-Link Overview

This chapter gives an overview of Isode M-Link.

This chapter contains the following sections:

1.1 About M-Link Server

Isode M-Link is an Isode product providing a standards-compliant *Extensible Messaging and Presence Protocol* (XMPP) server called M-Link Server. It supports a range of capabilities:

- *Instant Messaging* and Presence (IM&P),
- *Multi-User Chat* (MUC),
- *Personal Eventing Protocol* (PEP),
- *Components*,
- *Publish-Subscribe* (PubSub), and
- XMPP over *Bidirectional-streams Over Synchronous HTTP* (BOSH).

The remainder of this section summarizes some additional capabilities of M-Link Server.

1.1.1 Multiple XMPP service domains

Any Isode M-Link deployment, whether a single server or a cluster, may service many domains, including multiple IM, MUC, and PubSub domains. This is described in Chapter 3, *Domains*.

1.1.2 Chatrooms and multiparty chat sessions

Isode M-Link supports the configuration of one or more Multi-User Chat service domains, described in Chapter 9, *Multi-User Chat*, allowing several users or clients to join a single conversation in a controlled environment.

This chapter also covers Federated MUC (FMUC), which enables several MUC rooms to be federated into a single logical room. The chapter also describes Isode M-Link Gateway capability to the IRC (Internet Relay Chat).

Chatroom configuration and history may be persisted on-disk, allowing collaboration to continue seamlessly through service disruption and restarts.

1.1.3 Federation with other XMPP servers and Isode M-Link Edge

M-Link Server supports federation with other XMPP servers. Standard federation is fully connected. Isode M-Link also supports an XMPP Trunking architecture where servers are

connected indirectly. The Isode M-Link Edge configuration of XMPP supports indirect interconnection of servers. Isode M-Link uses Peer Controls to configure connections to remote servers, which can use optimized protocols for high latency networks and HF Radio.

This is all described in Chapter 8, *M-Link Edge, Peers and Links*.

1.1.4 Policy-driven security labels

Isode M-Link supports *Security Labels in XMPP* [*XEP-0258*] for clients such as Swift. Isode M-Link also supports *Cross Domain Collaborative Information Environment - Client Chat Protocol* (CDCIE-CCP) capable clients such as TransVerse. Security Labels are described in Section H.2, “SIO Options”.

1.1.5 Application-level gateway capabilities

Isode M-Link provides XMPP *application-level gateway* capabilites including content filtering, border guard integration, and cross security domain services. These capabilities can be deployed *at the edge* of an enterprise network using separate M-Link Servers, called M-Link Edge Servers, then those providing core XMPP services.

1.1.6 Management through Ad-Hoc Commands

Isode M-Link supports through Ad-Hoc Commands [*XEP-0050*] including a large subset of the service administration commands [*XEP-0133*]. Any authorized XMPP client supporting Ad-Hoc Commands can be used to access these commands. For the complete list of Ad-Hoc Commands, see Appendix G, *Ad-Hoc Command Reference*.

1.1.7 Components

Isode M-Link supports Components as specified in [XEP-0114].

1.2 About M-Link Console

The M-Link Console (MLC) provides administrators with the ability to deploy and operate M-Link Server instances using a *graphical user interface* (GUI). M-Link Console is an XMPP client. It can manage both *local* and *remote* M-Link Server instances. When managing local M-Link Server instances, M-Link Console offers additional capabilities. M-Link Console use is discussed throughout this guide. To get started, see Chapter 2, *M-Link: Getting Started*

1.3 About M-Link Archive Server

The M-Link Archive Server records XMPP traffic in database. This database can be used by XMPP clients using Message Archive Management (MAM) facilities. Administrators are also provided an HTTP interface to perform administrative tasks. These capabilities are discussed in Chapter 15, *Archive Management*.

1.4 About M-Link FDP Gateway

The M-Link FDP Gateway is an application that can discover forms using Form Discovery and Publishing (FDP) and forward them to an entity on the XMPP network. M-Link FDP Gateway is discussed further in Chapter 11, *M-Link FDP Gateway*.

1.5 About M-Link Web Application

M-Link Web Application are applications that run within a web browser. The applications allow an administrator to perform various administration tasks, view server statistics, and browse message archives. Applications for interacting with the FDP service are also provided. The M-Link Web Application are described in Chapter 20, *M-Link Web Application*.

Chapter 2 M-Link: Getting Started

This chapter discusses M-Link Server creation.

This chapter contains sections on the following topics:

2.1 About M-Link Server and M-Link Console

As described in Chapter 1, *Isode M-Link Overview*, M-Link Server is an *XMPP* server and M-Link Console is a tool which provides a *graphical user interface* (GUI) for creating and managing M-Link Server instances.

This section provides a brief introduction to terminology which will help you better understand subsequently provided materials.

A single M-Link Server instance, or multiple M-Link Server instances cooperatively, can provide an XMPP service for an XMPP domain or set of domains. The terms M-Link Server or *node* are to refer to a particular M-Link Server instance. The term M-Link service or *service* are used to refer to the M-Link Server instance(s) providing a particular XMPP service. When multiple M-Link Server instances are cooperatively providing an XMPP service, the *service* (or M-Link service) is said to be provided by a *cluster* of *node*s (or M-Link Server instances).

The distinction between *service* and *node* is important to understand in the configuration of M-Link service as some settings may apply *service* wide while others are *node* specific.

When loading its configuration, M-Link Server first initializes each configuration option to a hard coded default. Secondly, it loads options which have been set in the *service* configuration such that any option set *service* wide overrides the option's default value. Finally it loads options which have been set in the *server*'s *node* specific configuration such that an option in the *node* specific configuration overrides the option's *service* wide and/or default value.

2.2 Installing an Isode license file

In order to create or start an M-Link Server or M-Vault Server instance on a host system, the license for the respective product is required. The functionality of M-Link Console is also restricted in absence of an appropriate license.

Where M-Link Server and M-Link Console and, if used, M-Vault Server are to be ran on the same host system, all relevant licenses are provided by Isode in single file. This file needs to be copied to *(ETCDIR)/license.dat*. on the host system. Otherwise, each system hosting a product component will each have their own license file.

Questions regarding licensing should be directed to licensing@isode.com.

2.3 Starting and stopping M-Link Server

The M-Link Server can be started and stopped in the following ways:

- M-Link Console can be run locally on the same computer as the M-Link Server. More on this in Section 2.6, “Getting started with M-Link Console (MLC)”.
- Other operating system specific methods are described in Section A.1, “Running as Operating System Service”.

2.4 M-Link Server runtime user

When running on Unix, if the M-Link Server is started as 'root', it will then drop privileges to run as another user specified in Section H.1.16, “Runtime User ID”. All files in the Section H.1.1, “Users Root Directory”, Section H.1.112, “Publish-Subcribe Directory”, Section H.1.111, “Queues Statistics Directory”, Section H.1.113, “MUC Audit Archive Directory”, Section H.1.114, “User Audit Archive Directory” and Section H.1.5, “Telemetry Log Directory” are created as this user so it should be ensured that the directories have correct ownership and permissions. More on this in Section A.1.1, “Linux”.

On Windows, the M-Link Server runs as Windows service(s) under the `LocalSystem` account. More on this in Section A.1.2, “Windows”.

2.5 M-Link Server Administrators

Certain users have administrative rights and can perform configuration of the XMPP service. Such administrators, like any other M-Link Server users, use an XMPP client to connect

to the M-Link Server. There are two types of M-Link Server administrator: *Server* administrators and *Domain* administrators.

2.5.1 Server Administrators

A special *Server Administrators* group (see Section H.1.50, “Server Administrators”) defines which users are server administrators: members of the server administrators group have complete control over configuration for the whole service. An M-Link Server requires the server administrators group to contain at least one member; this administrator can add other users to the server administrators group.

A member of the server administrators group has special privileges including:

- use of the service administration (XEP-0133) and similar administrative commands.
- joining all chatrooms on the system and get the same rights as the owner.
- access to the archive of the M-Link Archive Server.
- viewing on-demand statistics.
- live session monitoring.
- creation and configuration of domains.

When M-Link Console is used to configure and create a new M-Link service then it automatically makes the initial administrator be a member of the server administrators group. Subsequently, when M-Link Console connects to the M-Link service using the credentials of that administrator, all administration facilities will be available.

2.5.2 Domain Administrators

Every domain may have a group associated with it, whose members are *Domain Administrators* for that domain. Server administrators can always manage the domain, whether or not a domain administrators group is specified. Note that domain administrators do not have the ability to create or delete domains, only to administer domains that have been created by a service administrator. See Chapter 3, *Domains* for more information about domain administration.

2.6 Getting started with M-Link Console (MLC)

2.6.1 Starting MLC

To start M-Link Console:

- On Unix systems, run **/opt/isode/bin/mlc**.

  Note that if M-Link Console is used to create, start or stop the M-Link Server on the local computer, then it needs to be run as `root` or the *runtime user ID* (see Section 2.4, “M-Link Server runtime user”).
- On Windows systems, select **M-Link Console** from within the **Isode** group of the Windows **Start** menu.

  Note that if M-Link Console is used to create, start or stop the Windows services corresponding to M-Link Server and M-Vault Server on the local computer, then it needs to be run with Administrator privileges or a user with the relevant permissions to manage these Windows services.

For most other M-Link Server administration, M-Link Console can be run locally on the same computer as the M-Link Server or remotely on a different computer.

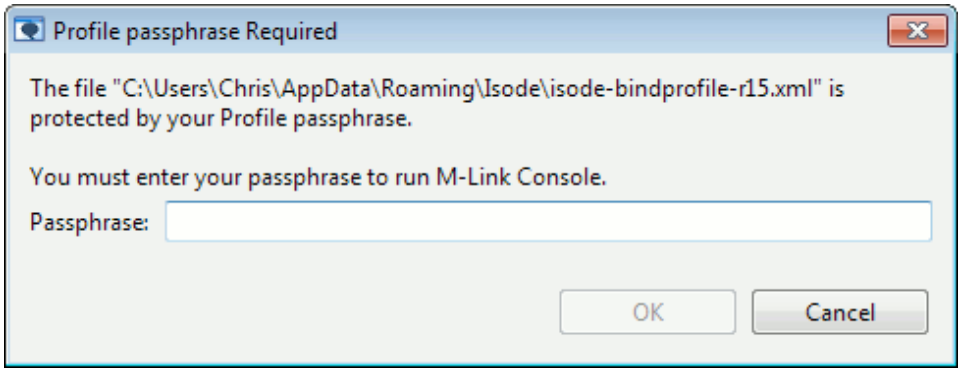
2.6.2 Profile passphrase

If you have not previously run any of the Isode management GUI tools, you will not yet have saved an Isode profile. If this is the case, you will be prompted at first launch of M-Link Console to create a new passphrase for encrypting profiles.

Figure 2.1. Prompt to create new profiles file

If you have already created an Isode profile (sometimes called a 'Bind profile'), you will be prompted for the passphrase.

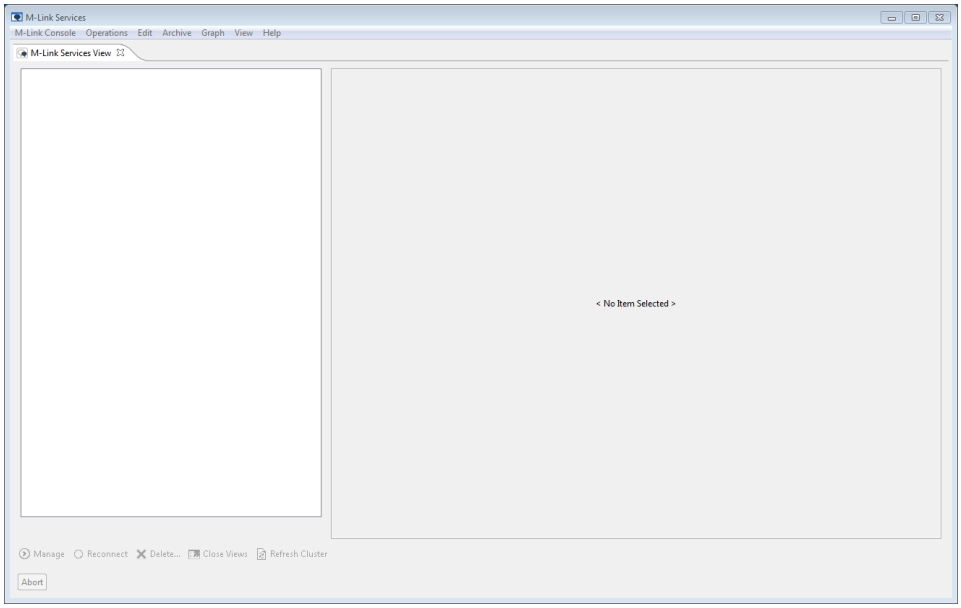
Figure 2.2. Prompt to unlock an existing profile



2.6.3 M-Link Services View

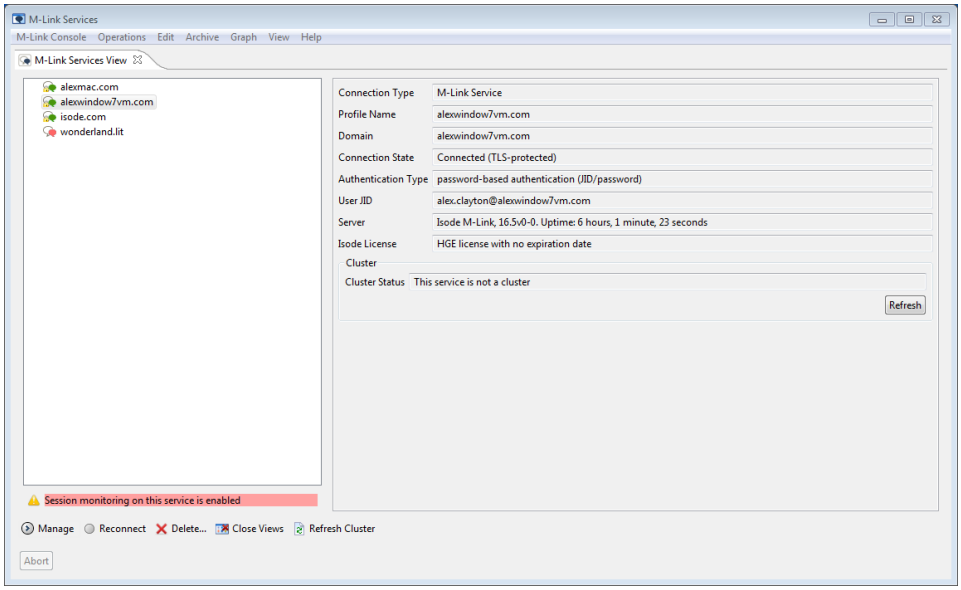
Once you have unlocked the profiles, M-Link Console will launch and display the **M-Link Services View** with the existing list of M-Link service profiles configured in M-Link Console. This list will be empty if no profiles have been configured. You can also open this view using **View** → **M-Link Services**.

Figure 2.3. M-Link Services View with no M-Link service profiles



After configuring a list of services that you wish to monitor or manage, the services will appear as shown below:

Figure 2.4. M-Link Services View with three service profiles



The left pane of the view contains a list of all M-Link services for which a profile has been created as described in Section 2.9.1, “Adding, modifying or deleting M-Link Console profiles”.

M-Link Console attempts to connect to all listed services, and the display will reflect the state of the connection. The color of an icon indicates connection status:

- green: a connection is established,
- amber: a connection is being attempted, and
- red: a connection could not be established.

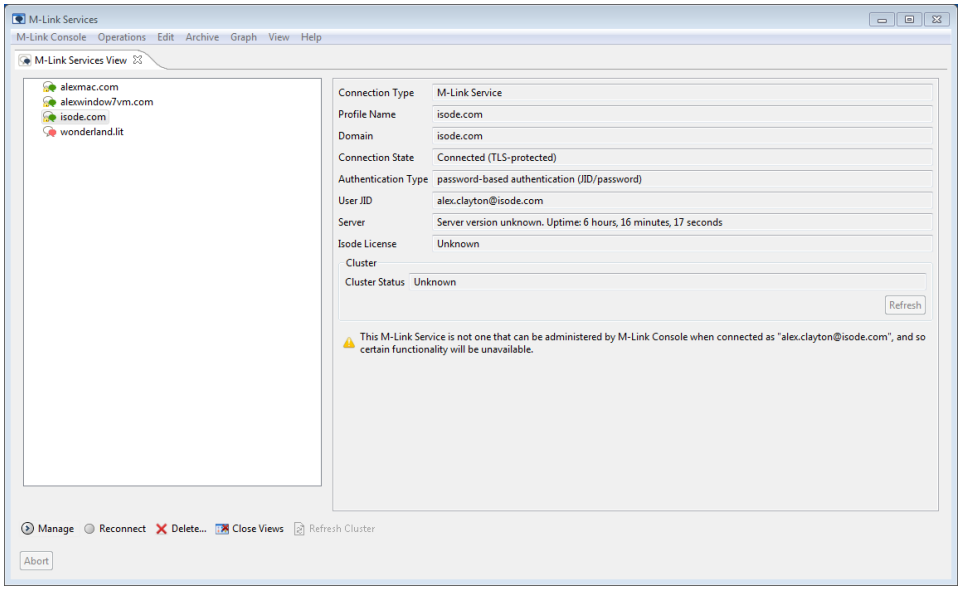
A golden padlock overlaying the icon is used to indicate a connection is protected by TLS.

In the screenshot above, three of the services have active connections with TLS protection; the other has no connection.

When a service in the left pane is selected, the right pane shows a summary page for the selected service.

You can use M-Link Console to monitor any M-Link service that you are able to connect to, regardless of whether you have administrative rights to manage the service. The next screenshot shows what happens when the user does not have administrative rights for the selected service.

Figure 2.5. Viewing a service without having administrative rights



2.7 Create an M-Link Server

2.7.1 Create an M-Link Server

M-Link Console is able to set up a new M-Link service, which it does by generating configuration data that the M-Link Server will read when it starts. Please note that on Unix, the user running M-Link Console should have the correct ownership and permissions of the directory *(`ETCDIR`)/servpass* if it exists and if it does not exist then the user should have the correct permissions to create it.

If you want to create the new M-Link Server on the same system as M-Link Console is running (a *local* server), then the configuration and initialization of the server will all be done by M-Link Console.

If you want to create the new server on different system (a *remote* server), then M-Link Console will generate configuration data and give instructions on how to deploy and use it on the remote system in order to get the new M-Link Server running there. See Section 2.8, “Create an M-Link Server on a remote host” for more information about managing remote servers.

In each case (*local* and *remote*), the **Create M-Link Server** wizard will prompt you for the information required to create and start a new server, and it will add an M-Link Console profile so that M-Link Console can administer the server and access the full range of configuration options when the server is running.

An M-Link service relies on an LDAP Server to store information about the users of the service, and so an important part of service setup is providing information to M-Link Console about where the LDAP Server is, and how it should be accessed.

If you already have an LDAP Server that contains user information, or is suitable for doing so, you can provide these details to the wizard. When you are creating a *local* M-Link Server, and you do not already have a suitable LDAP Server configured, then M-Link Console can create a new M-Vault Server for you (provided you have an appropriate version of Isode M-Vault installed and licensed).

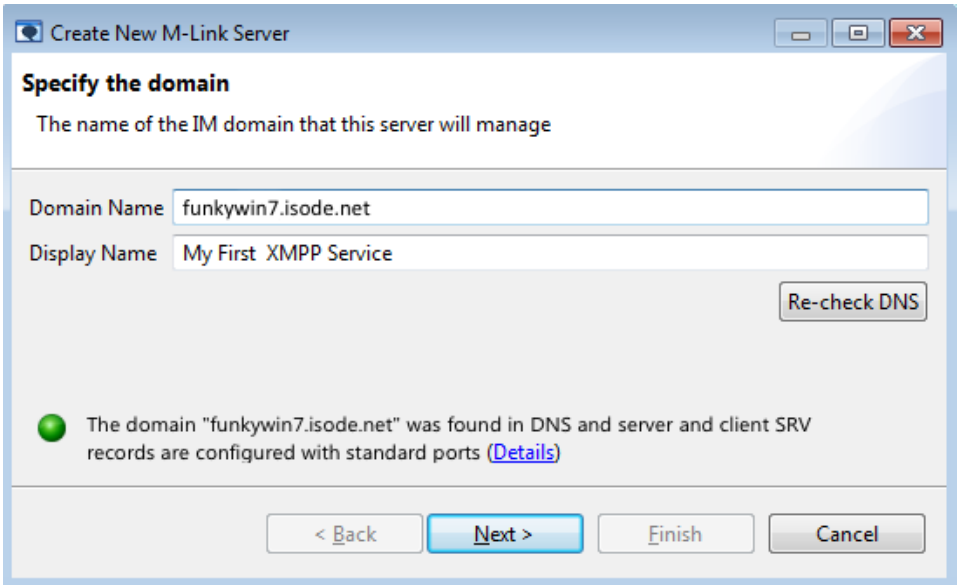
The wizard will attempt to ensure that any LDAP Server you specify does exist and is reachable, because an M-Link Server will not allow clients (including M-Link Console) to connect to it when the LDAP Server is unavailable.

In order to be able to access user information, an M-Link Server needs to be able locate the LDAP Server, authenticate itself to the LDAP Server with a suitable level of authentication, and needs to know how to obtain user information for the Directory.

Depending on whether you use a new or existing LDAP Server, the wizard may be able to supply some of the above information automatically.

To launch the **Create New M-Link Server** wizard to create a new server on the local host system, select **Create Local M-Link Server...** from the **M-Link Console** menu on the **M-Link Services** view (see Section 2.6.3, “M-Link Services View”).

Figure 2.6. Specifying the domain name

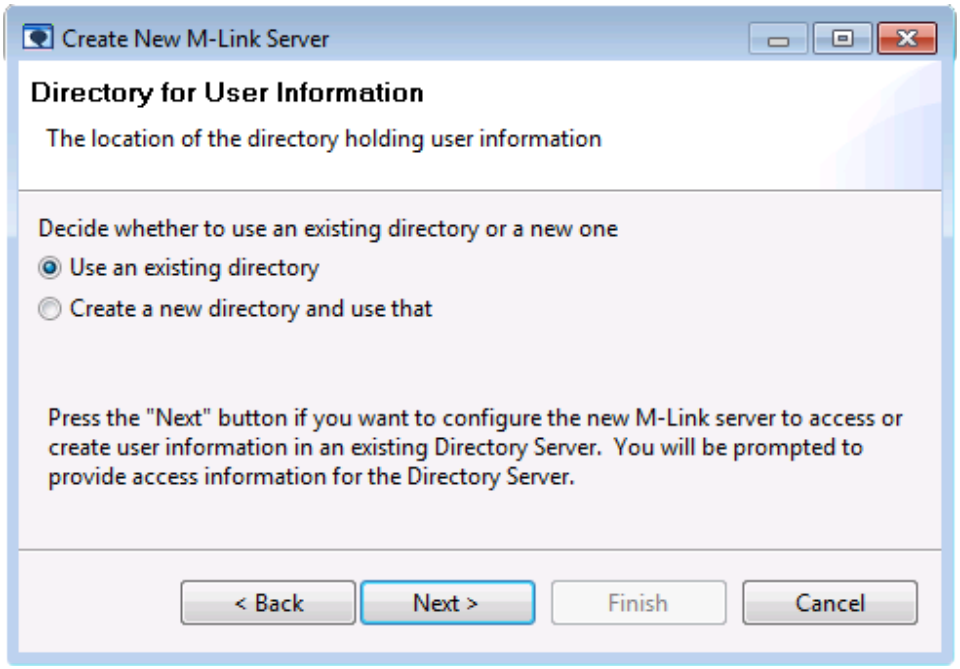


When you specify the domain name for the server, M-Link Console will check to see whether *DNS* resource records, including SRV resource records, are configured. Typically, SRV resource records would be configured to make it easy for clients and other XMPP services to find this M-Link service, but the server itself does not require them, and so the wizard will allow you to proceed even if warnings are displayed (in some cases, for example, it may be that DNS configuration will be done later) but you should review them in case they are being shown because you mistyped the domain name. See Section 2.9.5, “DNS Configuration” for information about how to configure DNS.

After specifying the domain name for the service, M-Link Console requires that you specify configuration for the LDAP Server. How you configure this information depends on whether you are using an existing LDAP Server, or want to create a new M-Vault Server for this purpose. Both options are described below.

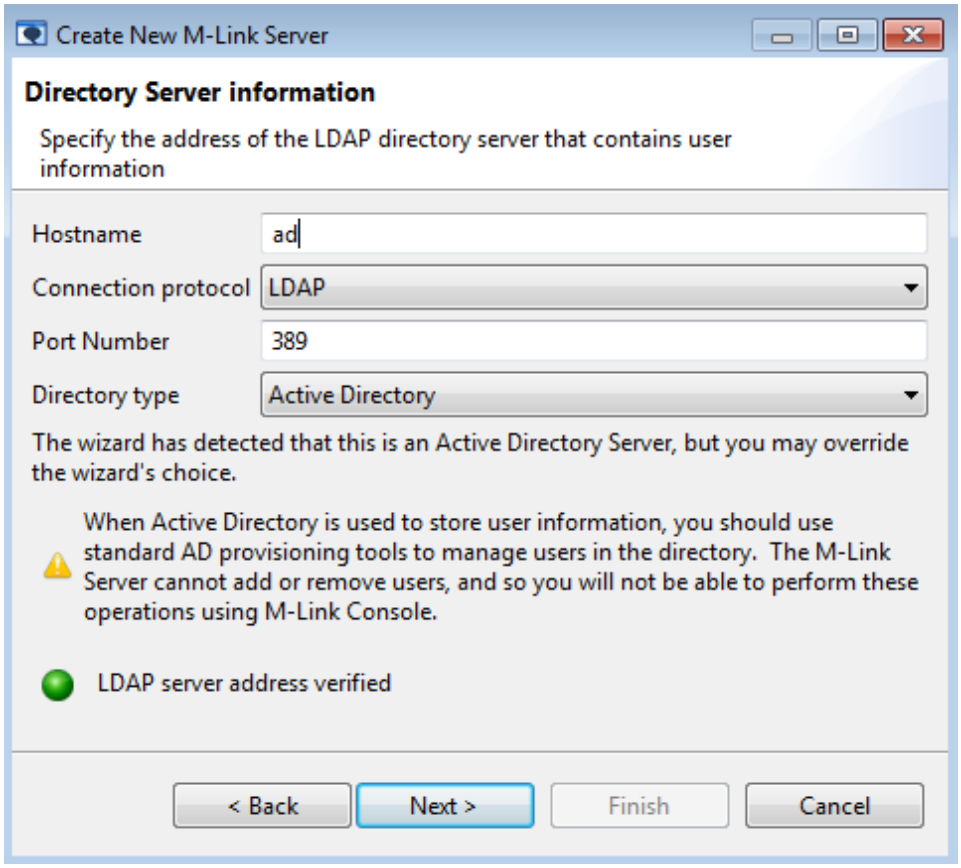
2.7.2 Configuring the new M-Link Server with an existing LDAP Server

Figure 2.7. Choosing to use an existing LDAP Server



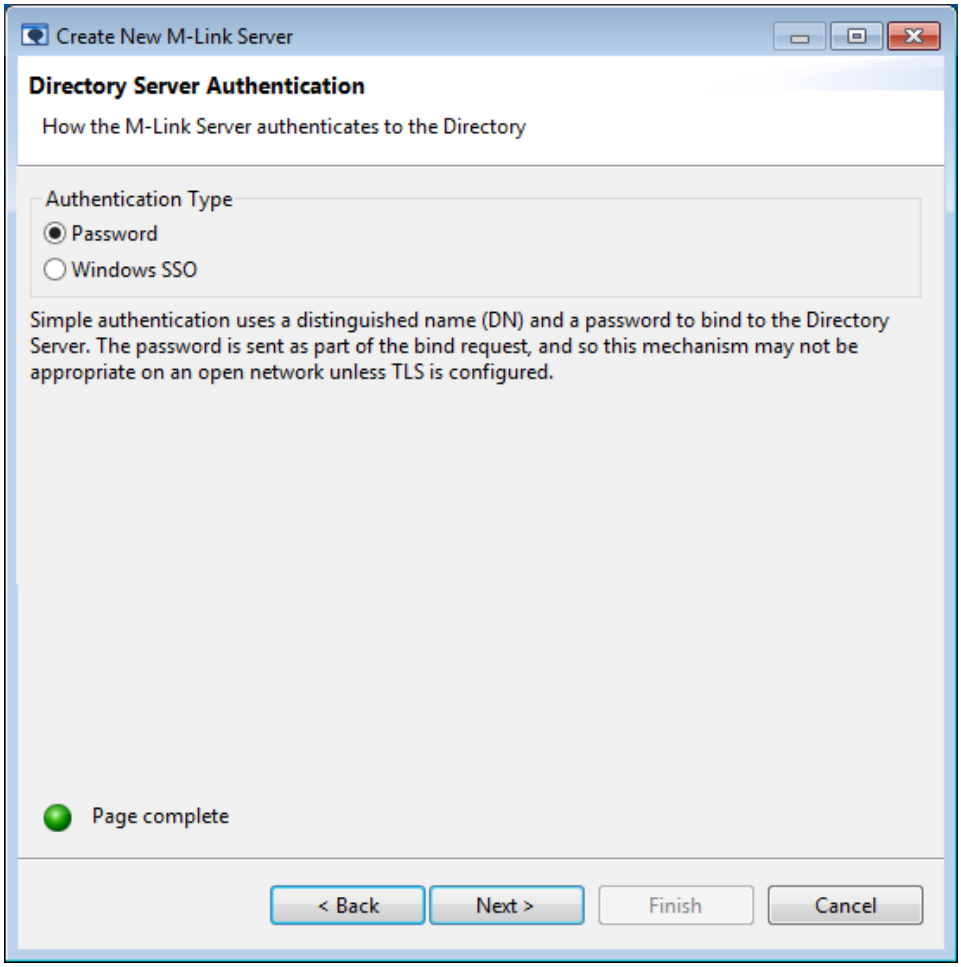
After choosing to use an existing LDAP Server the wizard will prompt you to supply its address. When you do this, the wizard will attempt to make an anonymous connection to the LDAP Server, in order to establish that it is online and accessible. The wizard also needs to know whether the *Directory* is an Active Directory (and will attempt to determine this automatically).

Figure 2.8. Specifying the existing LDAP Server's address



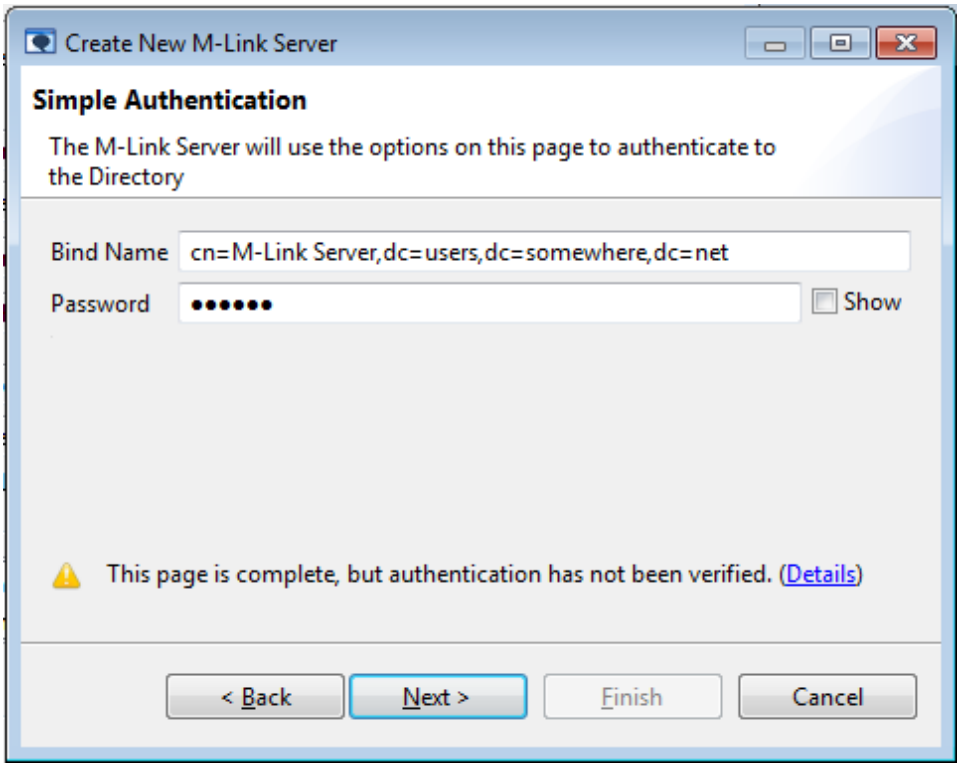
The wizard allows you to choose various types of authentication, each of which may require different parameters.

Figure 2.9. Choosing authentication type



Different authentication types require different sets of parameters. The wizard will attempt to verify any authentication parameters you provide, but in some cases will not be able to do this.

Figure 2.10. Specifying authentication details

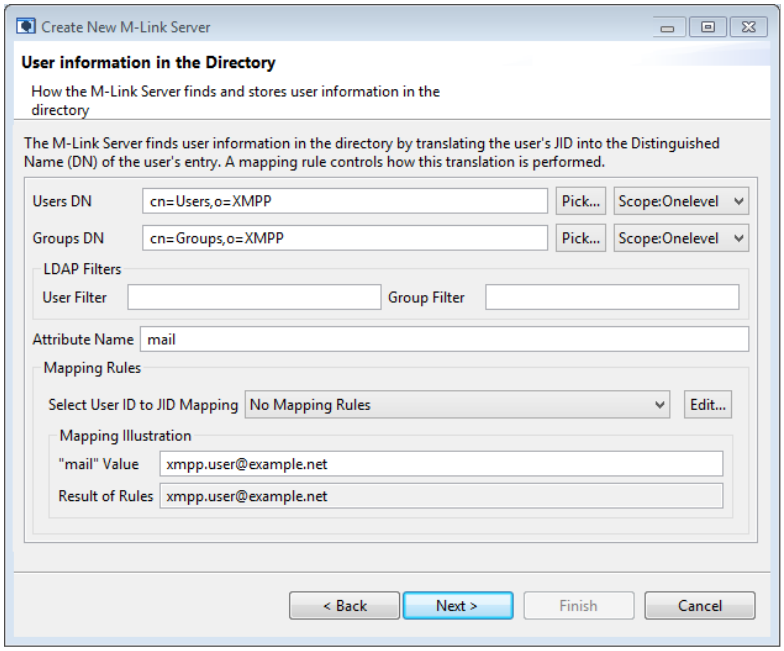


Once you have provided valid authentication details, the next wizard page is used to configure how the M-Link Server locates information inside the Directory. Specifically:

- when determining which directory entry corresponds to a given user, the M-Link Server maps the user's ID into a JID by using *Mapping Rules* and then performs a directory search, looking at entries below the *Users DN*, for the entry which contains the JID in the attribute named by *Attribute Name*. An extra *User Filter* may be specified to customise the exact search. See Section 3.2.3.2, “Mapping Configuration” for more information.

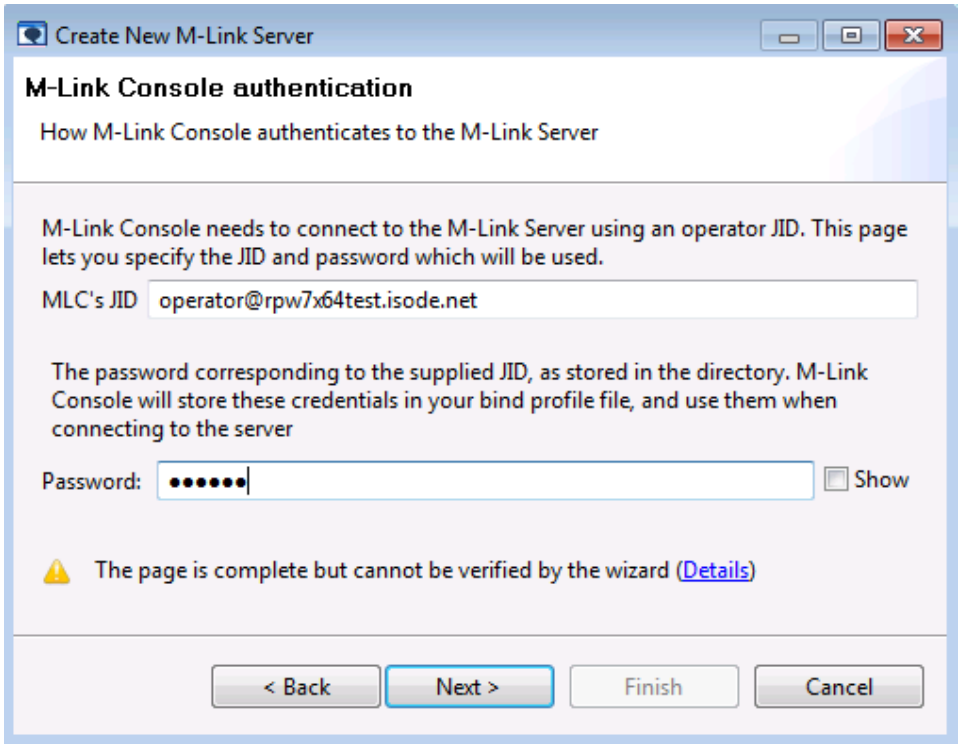
  As you update the user configuration on the wizard page, the wizard will show you how such mapping will affect the search for a given entry. In the screenshot below, the configuration specified will mean that a user with the JID `xmppuser@example.net` will be associated with the Directory entry that matches the search filter `mail="xmppuser@dexample.net"`. If you are not certain what mapping should be used here, then you should consult with the person responsible for administering the LDAP Server.
- when resolving the members of a directory groups, the M-Link Server searches the directory, looking at entries below the *Groups DN* for any entry that contains *member* or *uniqueMember* attributes. An extra *Group Filter* may be specified to customise the exact search. See Section 3.2.3, “User Directory configuration for IM domains” for more information.

Figure 2.11. User information in the Directory



The next page lets you specify the JID and password of an administrator that M-Link Console will use when it connects to the new M-Link service. When the server is created, the JID that you specify here will be a member of the *operator* group (see Section 2.5, "M-Link Server Administrators"), who can use M-Link Console to administer the M-Link service.

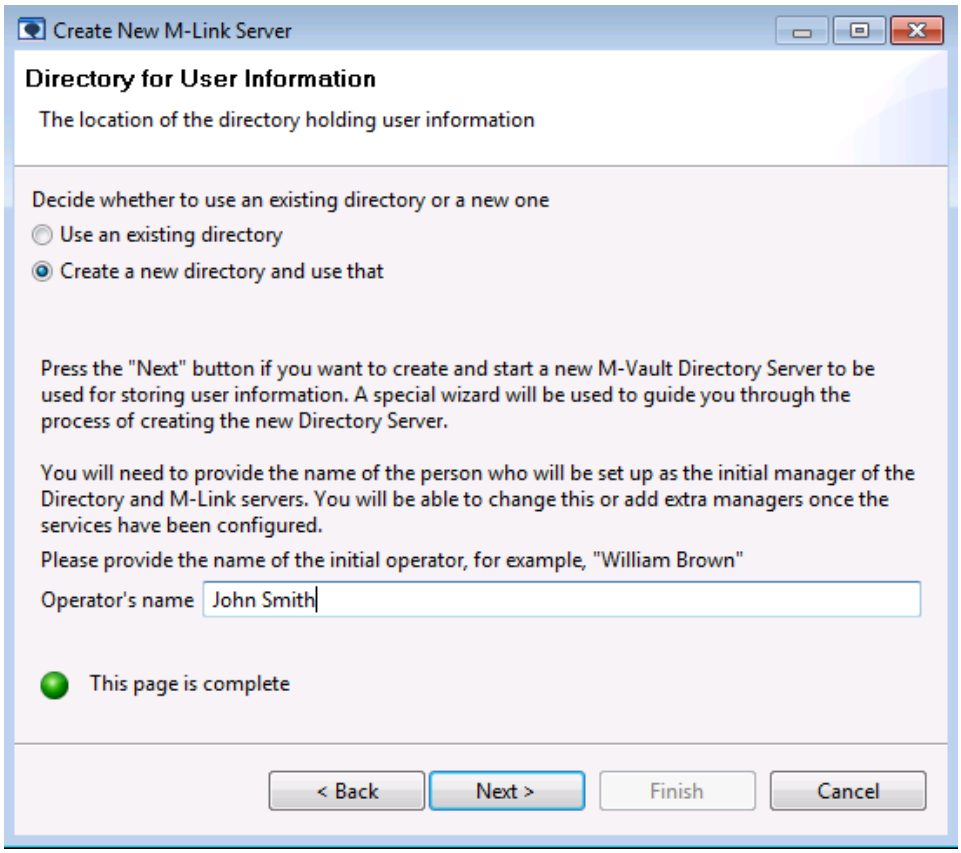
Figure 2.12. M-Link Console's JID and password



The final pages of the wizard are the same as those for a configuration where a new LDAP Server has been created; see Section 2.7.4, "Remaining steps".

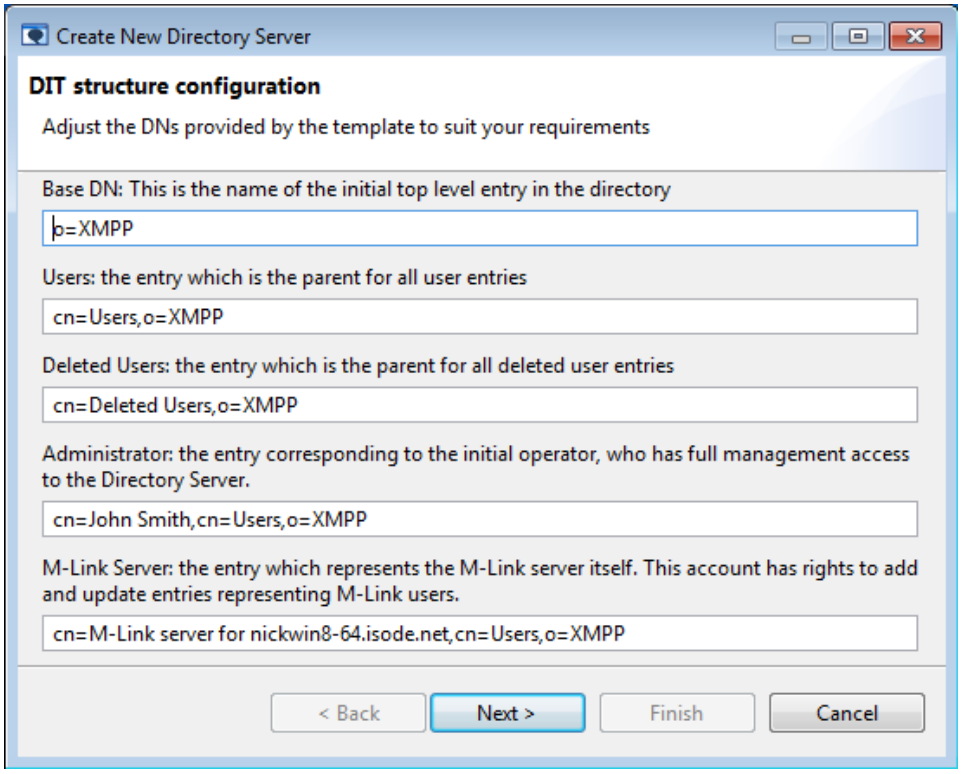
2.7.3 Creating a new M-Vault Server for the new M-Link Service

Figure 2.13. Choosing to create a new M-Vault Server



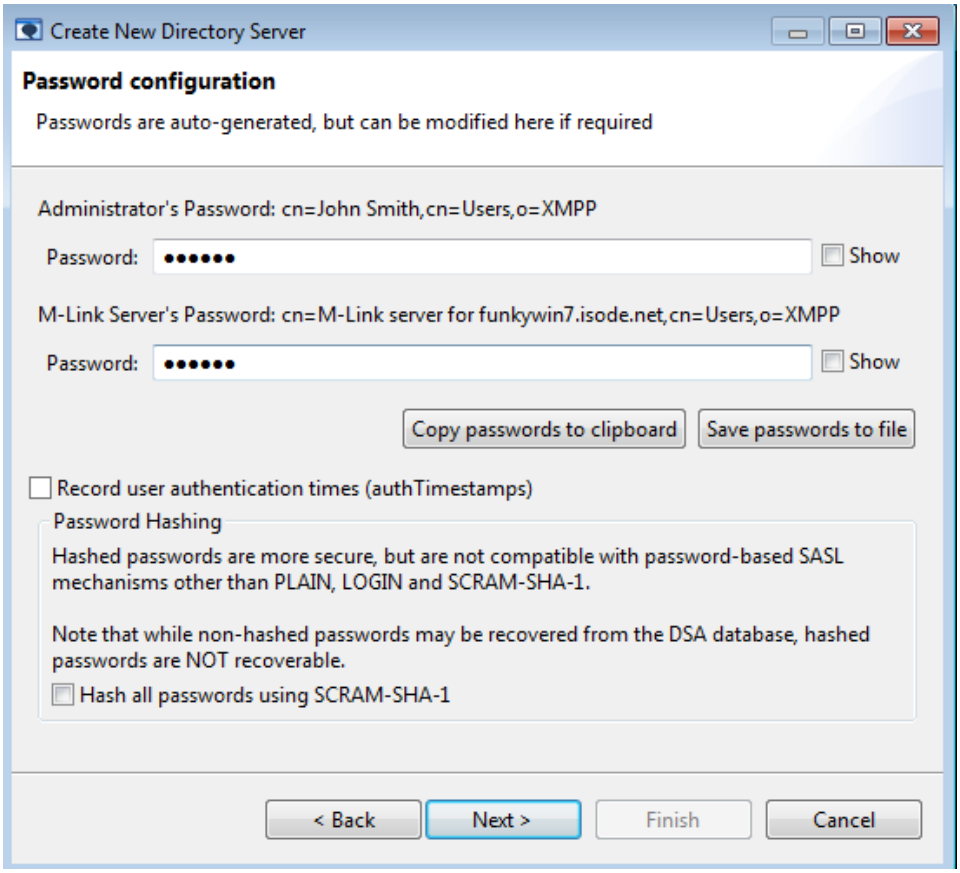
If Isode M-Vault is installed and licensed on your system, you can choose to create a new M-Vault Server. When you choose this option, you will be prompted to supply the name of the initial administrator for the M-Link Server. This user will be added in the Directory provided by M-Vault Server.

Figure 2.14. DIT Configuration in the new Directory



The **Create New Directory Server** wizard will take you through the process of creating and starting a new M-Vault Server instance. This wizard is template-driven, using files in the *(SHAREDIR)/mlink-dsa-setup* directory. The default template will create a M-Vault Server containing a user entry for the administrator JID used by M-Link Console when it connects to the new service and one for the M-Link service itself, which needs to authenticate to the directory server in order to access and update user information.

Figure 2.15. Password Configuration in the new Directory server

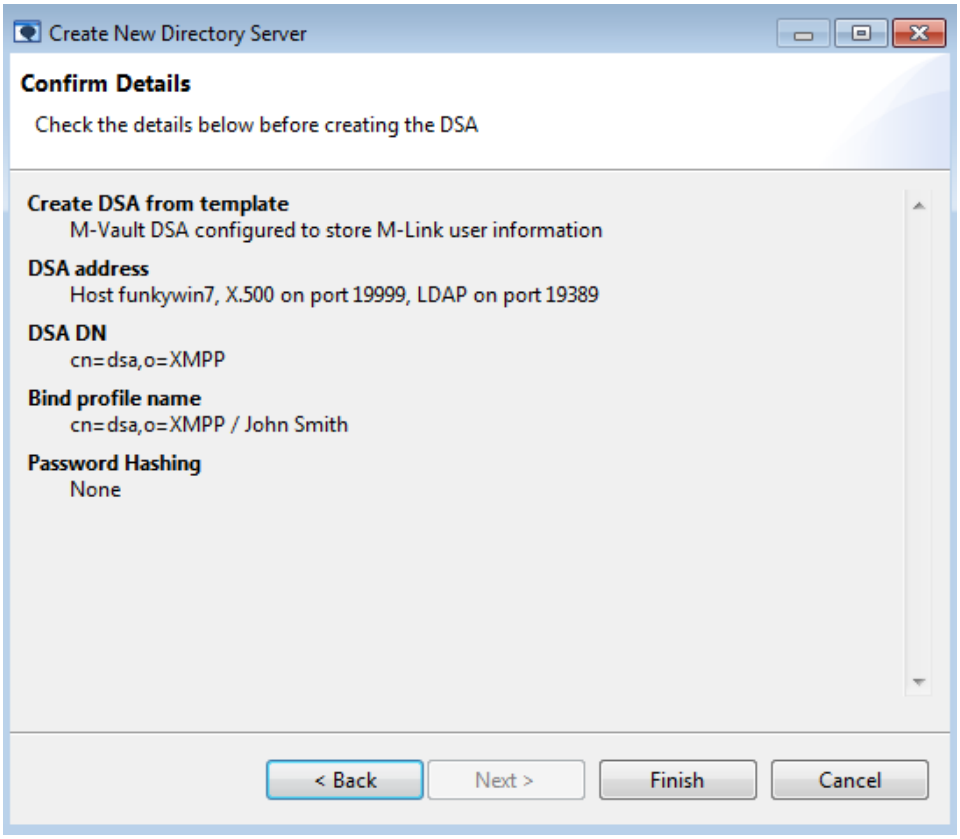


The administrator's password will be associated with JID used by M-Link Console (see Figure 2.17, “JID for M-Link Console”). M-Link Console will store the administrator's password in the service profile that gets created for the new M-Link service.

The M-Link Server's password is used by the M-Link Server to authenticate itself to the M-Vault Server. After the M-Link Server has been configured, M-Link Console keeps no record of it.

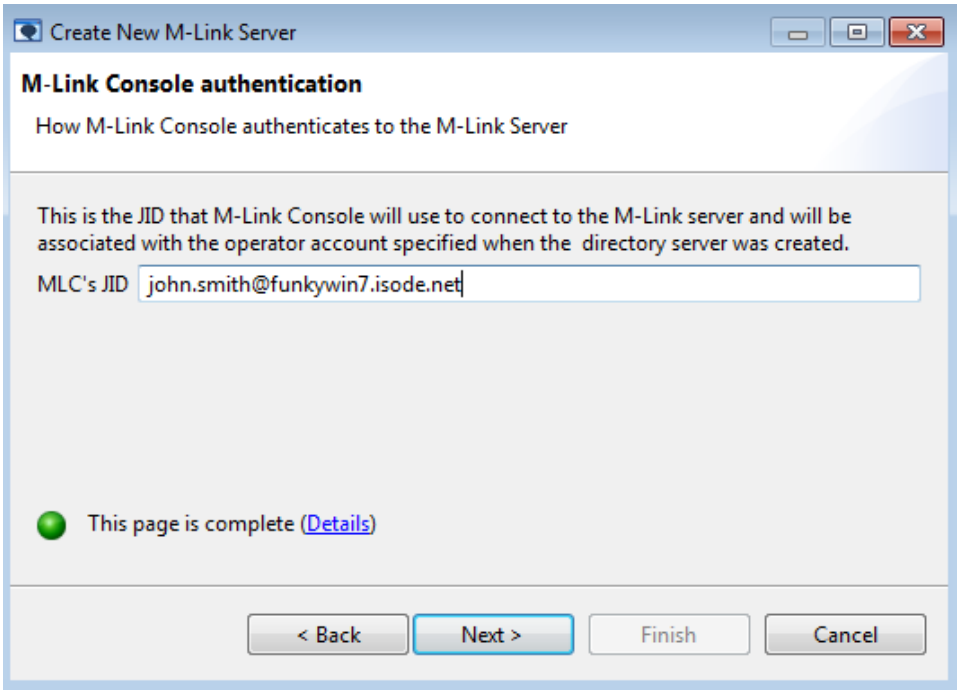
The **Record user authentication times** checkbox will determine whether the directory server records the time every time a user authenticates. As well as being displayed when using user provisioning, this information allows the directory server to enforce limits such as password and account lifetime for users.

Figure 2.16. Confirm Details page



At the end of the **Directory Server Creation** wizard, a page will summarize the creation details you have provided and ask you to confirm them before finishing the creation process. The wizard creates a new bind profile which will appear in M-Vault Console and Sodium so that these applications will be able to connect to and manage the new directory server. The new bind profile will also be used by M-Link Console in order to perform user provisioning operations (see Section 6.2, “ User Provisioning in M-Link Console”.

Figure 2.17. JID for M-Link Console



After the new M-Vault Server has been created and started, the **Create New M-Link Server** wizard will ask you to supply the JID of the M-Link service administrator. A value is suggested based on the name of the user you provided when creating the M-Vault Server.

2.7.4 Remaining steps

2.7.4.1 Runtime Username and Permissions

> **Note:** This section is applicable to Unix installations. If you are running on Windows, you may skip this section.

After either creating a new directory server, or providing details about an existing Directory Server, the next wizard page will ask you for:

- The *username* for the M-Link Server process (see Section 2.4, “M-Link Server runtime user”).

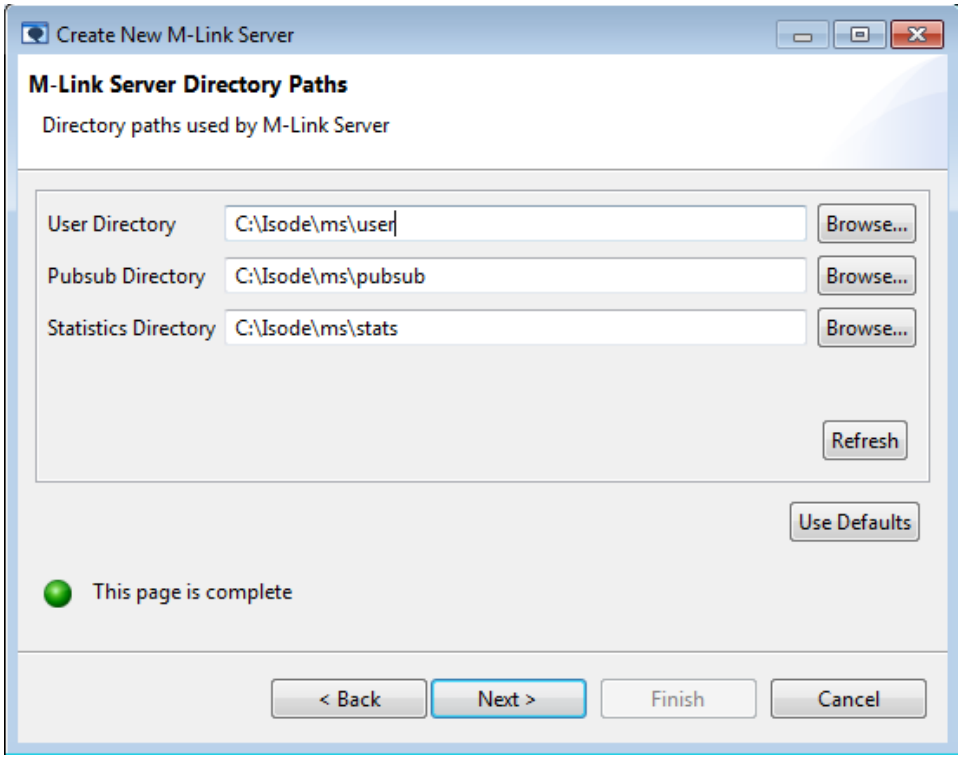
Note that the screenshot below reflects a Windows installation, where no *username* is required.

2.7.4.2 Directory Paths

The page asks you to specify location of directories that the new M-Link Server requires. All the directory paths must be configured; the wizard will suggest values for you but you may change them as desired:

- The *runtime directory* (see Section H.1.4, “Runtime Directory”) will only be asked for servers running on Unix system
- The *user directory* (see Section H.1.1, “Users Root Directory”)
- The *pubsub directory* (see Section H.1.112, “Publish-Subcribe Directory”).
- The *statistics directory* (see Section H.1.111, “Queues Statistics Directory”)

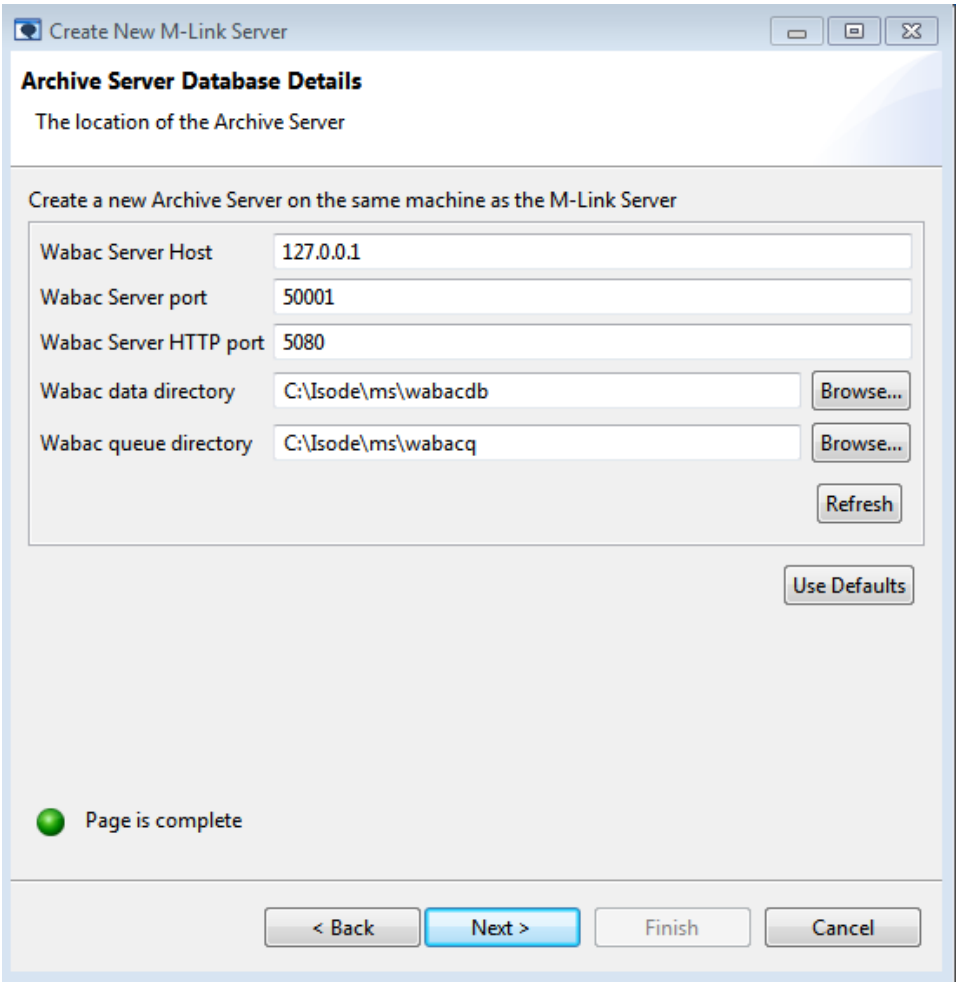
Figure 2.18. M-Link Server directories



2.7.4.3 M-Link Archive Server Database Details

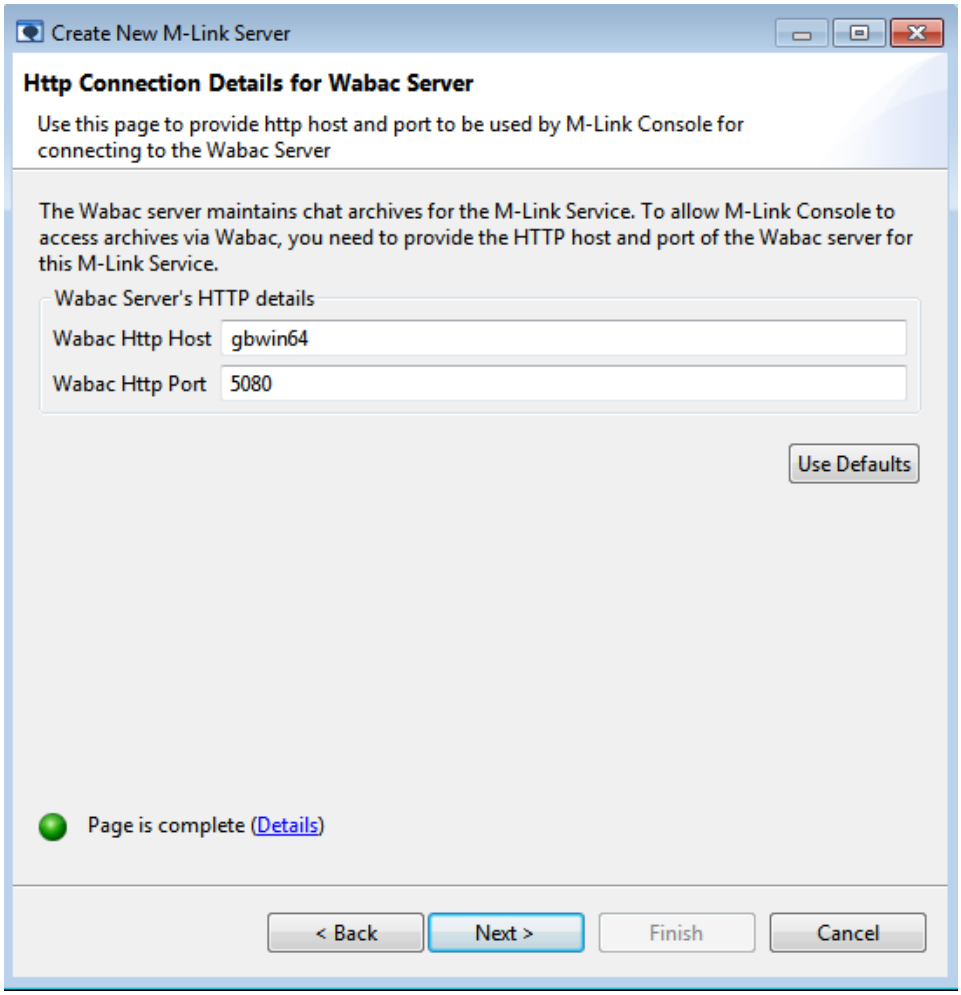
On pressing the **Next** button, the wizard will ask you about the configuration details of the M-Link Archive Server (see Chapter 15, *Archive Management*) as shown in figure below. The description of the configuration parameters for M-Link Archive Server can be found in the appendix starting from Section H.1.135, “Archive Server Host”.

Figure 2.19. M-Link Archive Server Database Details



Pressing the **Next** button will display the wizard page for configuring the HTTP host and port for M-Link Console to connect to the M-Link Archive Server (as shown in the figure below). These details will be stored in the profile for the M-Link service. In the absence of M-Link Archive Server's HTTP details, M-Link Console will not be able to use the services of the archive server.

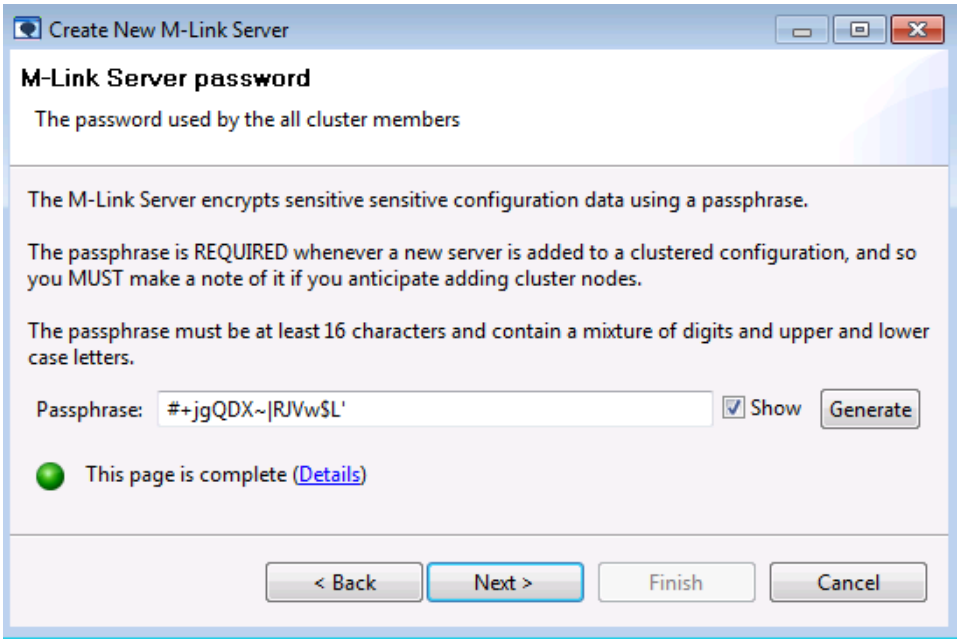
Figure 2.20. HTTP Connection Details for Archive Server



2.7.4.4 M-Link Passphrase

The last piece of information required is the *M-Link Server passphrase*. You must make a note of this password if you intend to create a clustered configuration as you will be required to enter it for any new cluster node that you add.

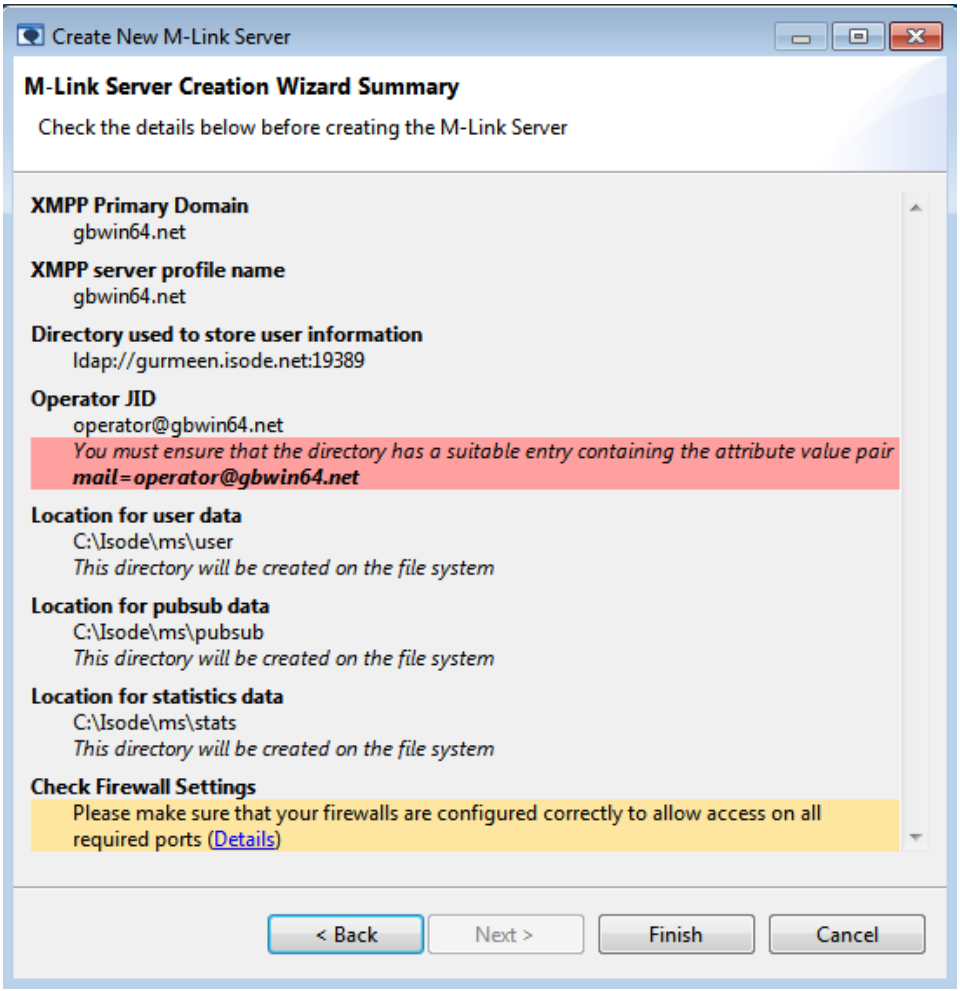
Figure 2.21. M-Link Server passphrase



2.7.4.5 Summary Page

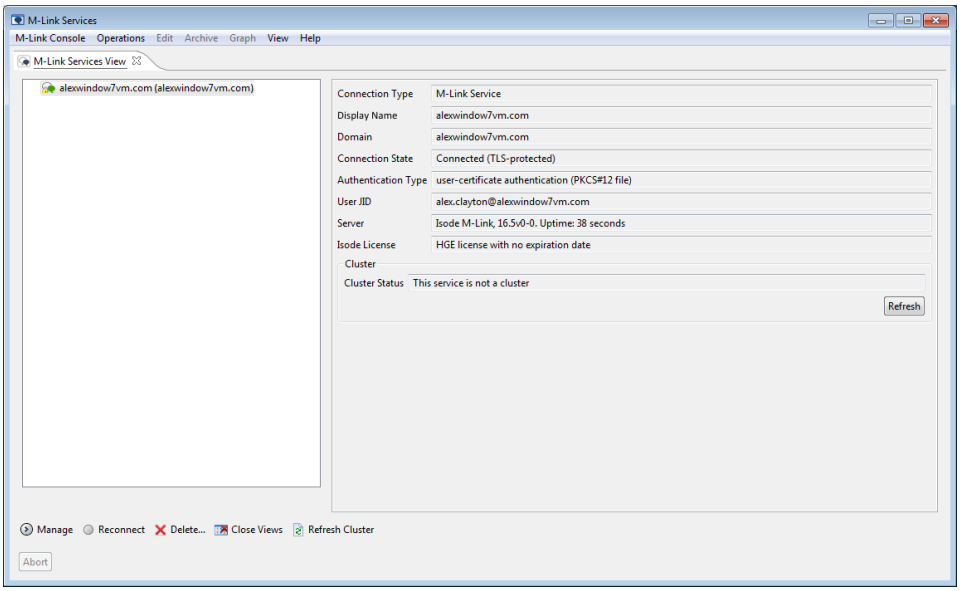
Finally, the wizard will display a summary page before the new M-Link Server is created and started. If you created a new LDAP Server, the wizard will update the contents of the Directory according to the JID that was specified for the administrator. If you used an existing Directory Server, the summary page will indicate what actions you may need to perform to ensure that the administrator JID can be found in it.

Figure 2.22. Summary Page



Once you press the **Finish** button, the wizard will configure and start the new M-Link service, which will run as a process on the local system. The new service will appear in the services view, and as soon as the service has been started, M-Link Console will connect to it. Selecting the new service will cause the information about the service to be displayed in the right hand pane:

Figure 2.23. Newly created service



2.8 Create an M-Link Server on a remote host

This section discusses how to create and manage remote M-Link Server instances using M-Link Console.

2.8.1 Background

M-Link Console is a Java application which uses a GUI to interact with the user. This means that you cannot use M-Link Console on a system where Java is not installed, or where there is no graphical console available. In order to be able to create and manage an M-Link Server in such cases, you need to run M-Link Console from a suitable alternate system, and treat the M-Link Server as a remote M-Link Server.

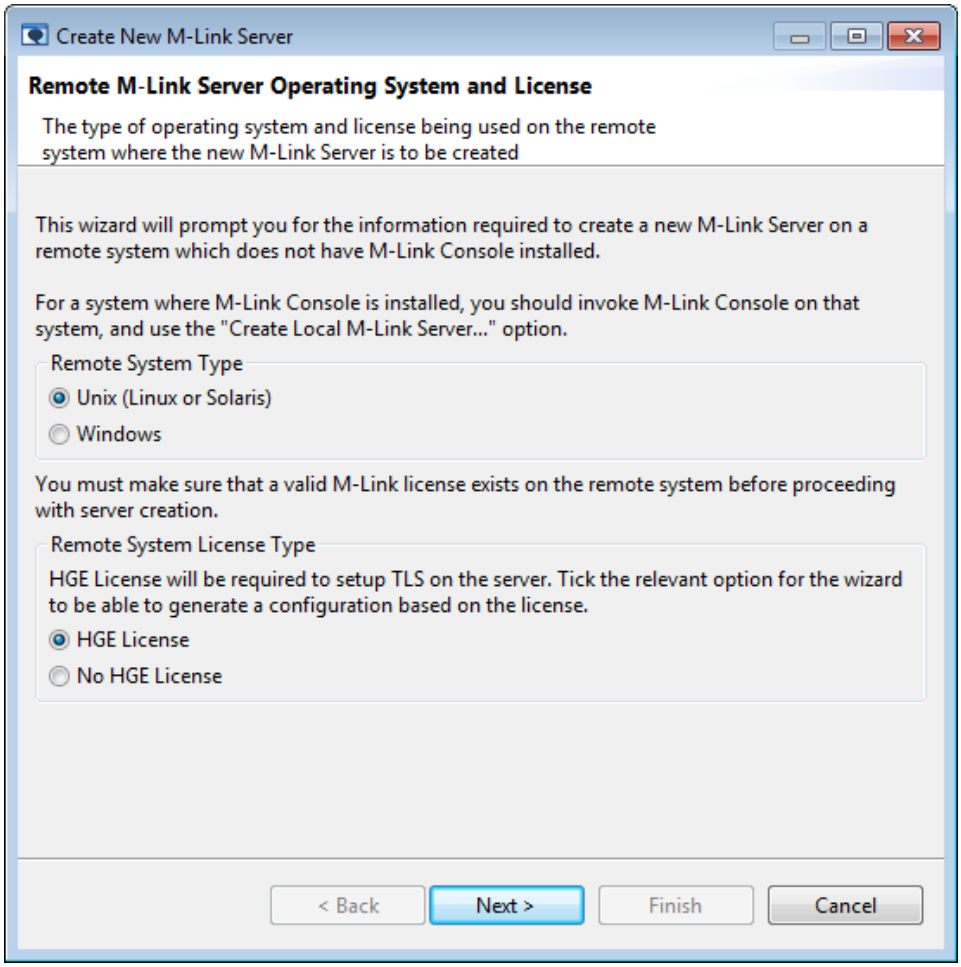
Normally, M-Link Console interacts directly with the M-Link Server and associated tools in order to configure, start and stop it. For a remote M-Link Server, M-Link Console has no direct access to the system where the server runs. This means that in situations where direct access is required (for instance to stop and start the server), M-Link Console relies on there being an administrator who has such access on the remote system.

2.8.2 Using M-Link Console to set up a remote server

Using M-Link Console to create an M-Link Server on another system, requires you to provide much the same information as would be needed when creating a server on the local system (see Section 2.7, “Create an M-Link Server”). In most cases, the wizard pages which are shown are identical. Similarly, you can use M-Link Console to create a cluster member on another system.

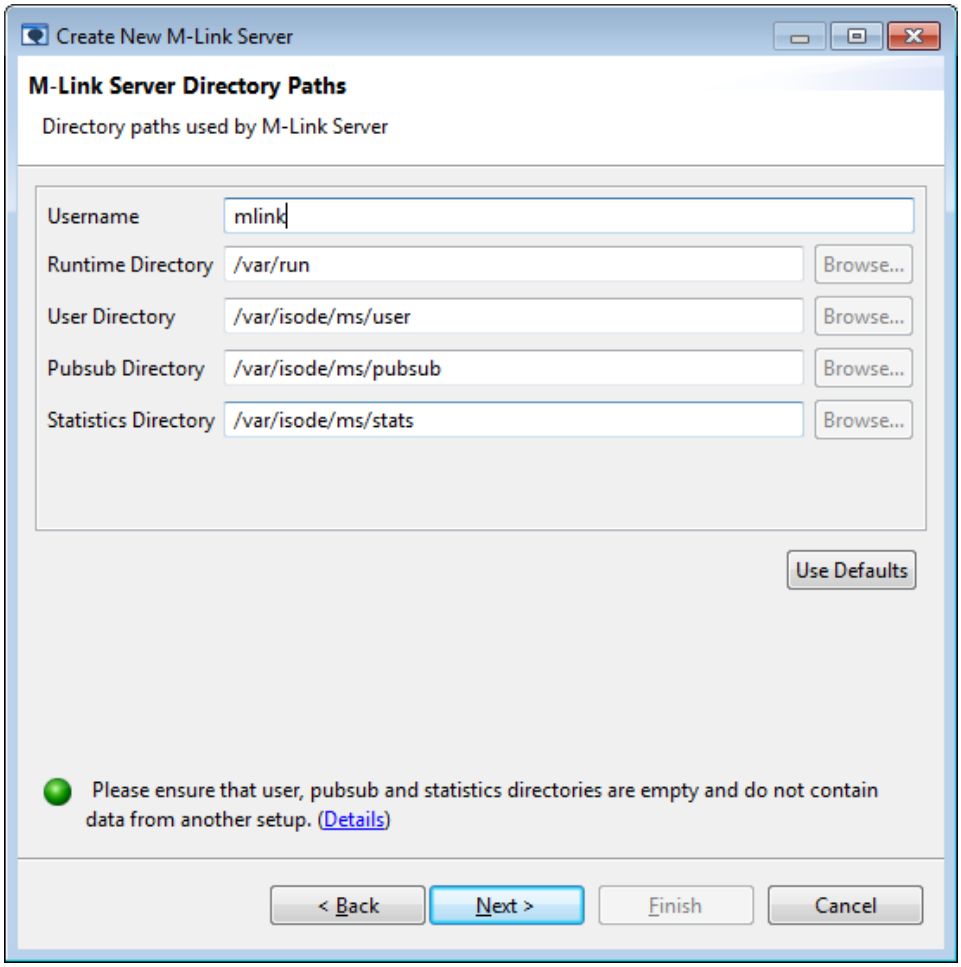
To begin the process, use **Create Remote M-Link Server...** from the **M-Link Console** (or **New Remote Cluster Node...** from the **Operations** in the case of a cluster node). M-Link Console needs to know the operating system used on the remote system, because that determines the format of file paths which it needs to use; and whether the remote system has an HGE license:

Figure 2.24. Specifying the remote system type



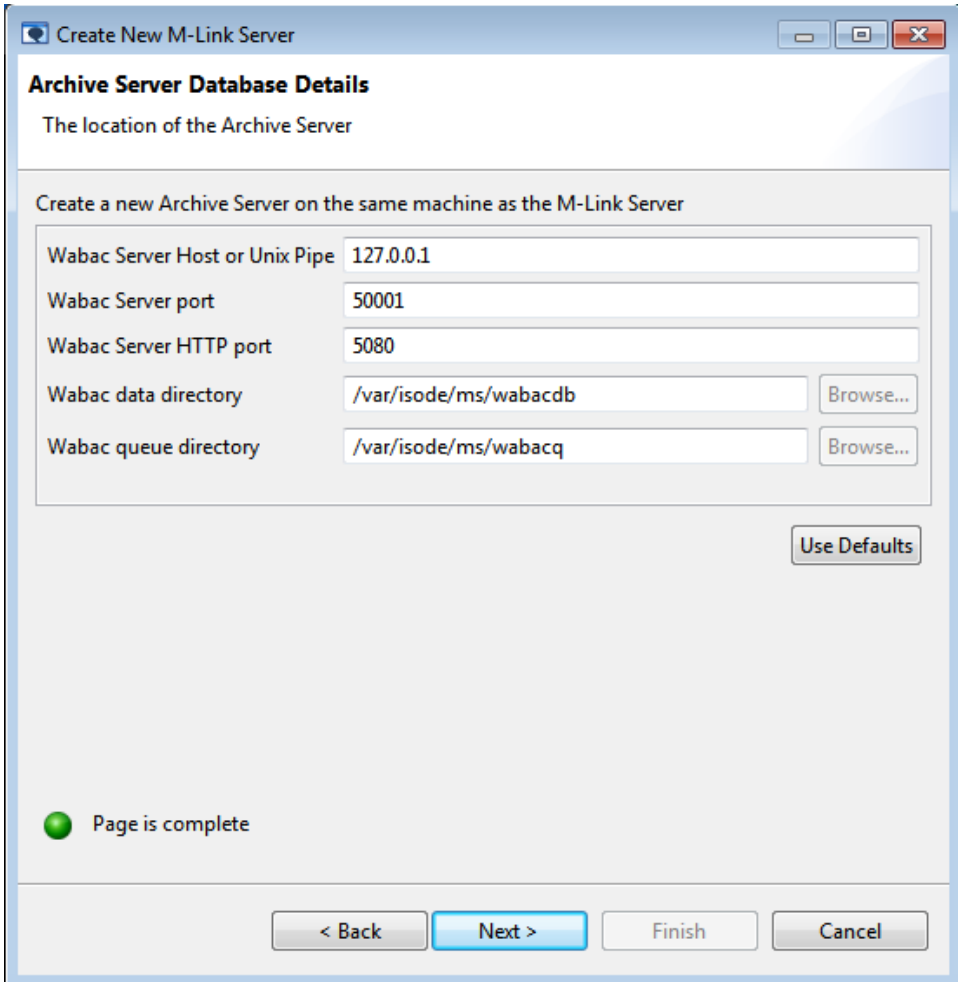
After this, you will be presented with the same set of wizard pages as shown in Section 2.7, “Create an M-Link Server”. In most cases the pages are identical, although since M-Link Console is not running on the same system as the server, some of the checks that the wizard would otherwise attempt are not performed (for example, M-Link Console has no way to determine whether the remote system is able to access the LDAP Server). Similarly, M-Link Console cannot access the filesystem which will be used by the M-Link Server, and so when you are asked to specify the directory paths used by the server, the **Browse** buttons are disabled, and a **Use Defaults** can be used to generate values suitable for the remote system:

Figure 2.25. Specifying the remote system directory paths



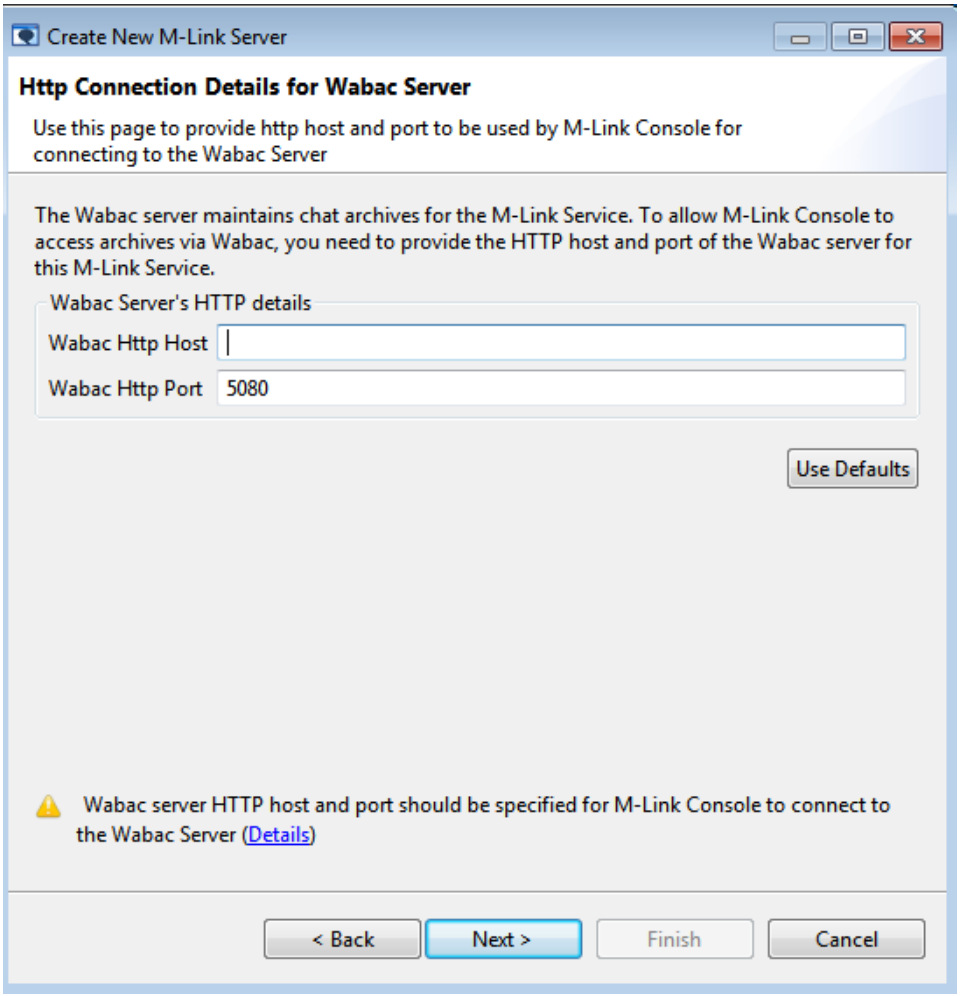
Similarly, the wizard will ask you to provide the details of the M-Link Archive Server (see Chapter 15, *Archive Management*) on the remote system.

Figure 2.26. Specifying the remote system Archive Server details



In order for M-Link Console to connect to the M-Link Archive Server, you will need to configure the details of HTTP server and port for connecting to the M-Link Archive Server.

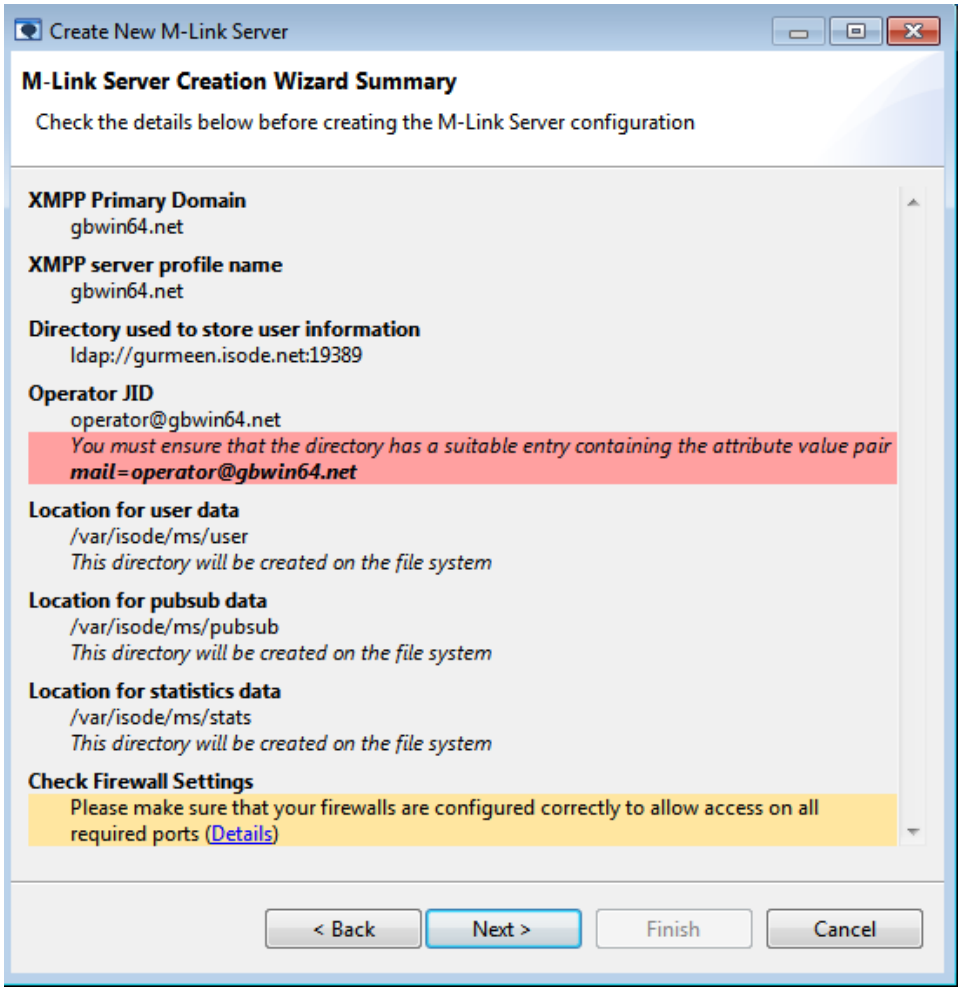
Figure 2.27. HTTP connection details for M-Link Archive Server



Once M-Link Console has all the information required, it will be ready to generate the server's configuration file. Since the configuration file contains sensitive data, you need to provide a server passphrase which is used to encrypt the configuration (see Figure 2.21, “M-Link Server passphrase”).

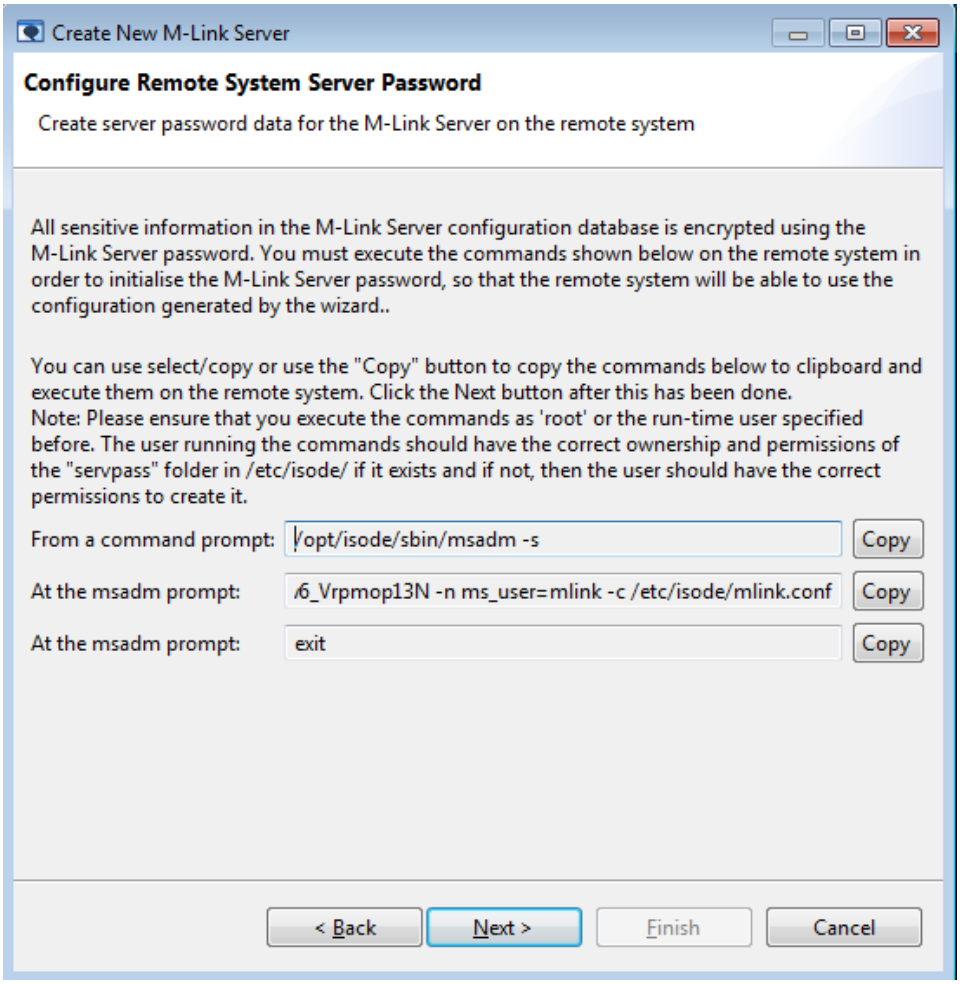
The wizard will show a summary page which allows you to check the details for the new remote server:

Figure 2.28. Remote server details summary



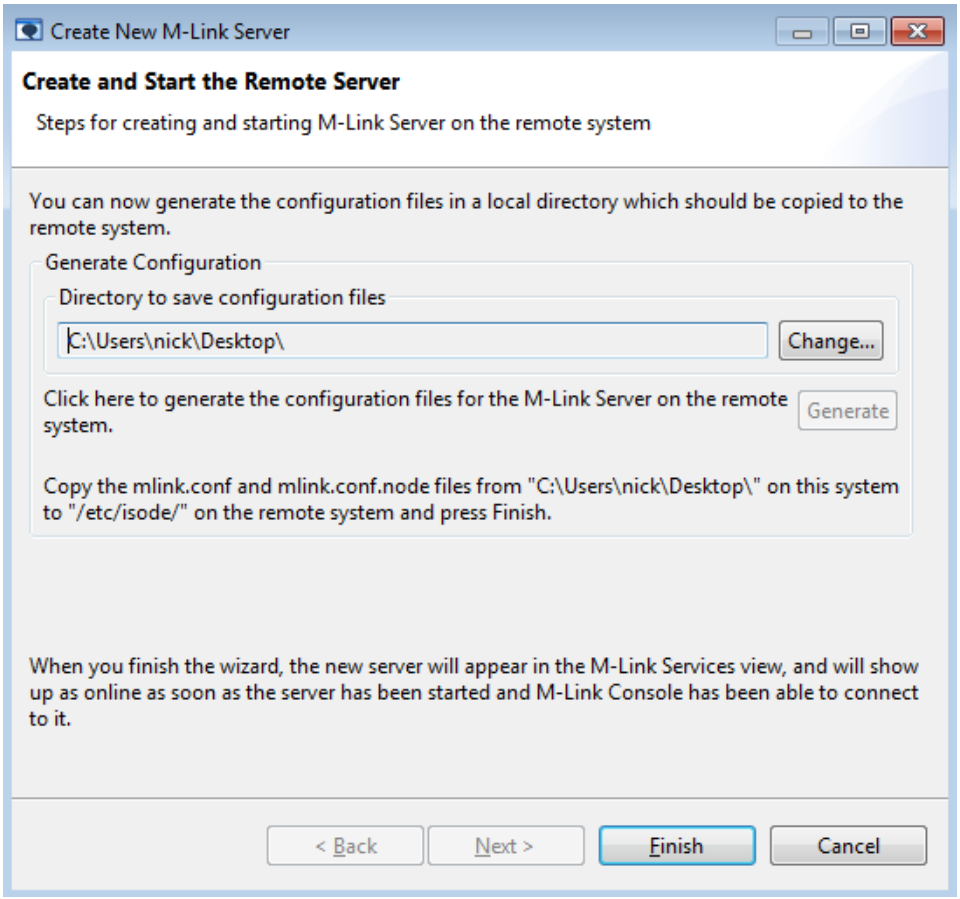
The wizard will then generate commands that need to be entered on the remote server that will initialise an encrypted version of the configuration for the new server.

Figure 2.29. Configuring server password for remote server



Finally, the wizard will generate the configuration files for the new server, which will already be encrypted using the server passphrase, so that you can copy them to the remote system:

Figure 2.30. Generating configuration files for remote server



2.8.3 Other Considerations

Once a remote server has been configured and started, then M-Link Console can connect to it and manage it in the same way as it would a local server. There are some things that are not possible with a remote server though:

- You cannot start or stop the remote server using M-Link Console. These operations must be carried out by a suitably privileged administrator logged in to the server system. See Section A.1, “Running as Operating System Service” for information about using the command line to do this.
- Certain configuration parameters (such as logging configuration) contain file or directory paths which are typically only meaningful for the system where the server is running. Since M-Link Console has no direct access to the remote system, you will be unable to access these files.
- If you are using M-Link Console to manage a server on the local system, then you only need to install a license file on that system (see Section 2.2, “Installing an Isode license file”). For a remote server, a suitable license must be installed on the remote system (otherwise the M-Link Server will not start). M-Link Console does not require a license to run, but encryption functionality will be unavailable unless an HGE-TLS license (see Section 7, “Export controls”) has been installed on the system where M-Link Console is running. In practice, this means that attempts to connect to a server that is using TLS will need to to specify **Allow "PLAIN" without TLS** - normally, M-Link Console will not use authentication methods which send plaintext passwords unless the connection is secured with TLS. This option may be used to override this behaviour.

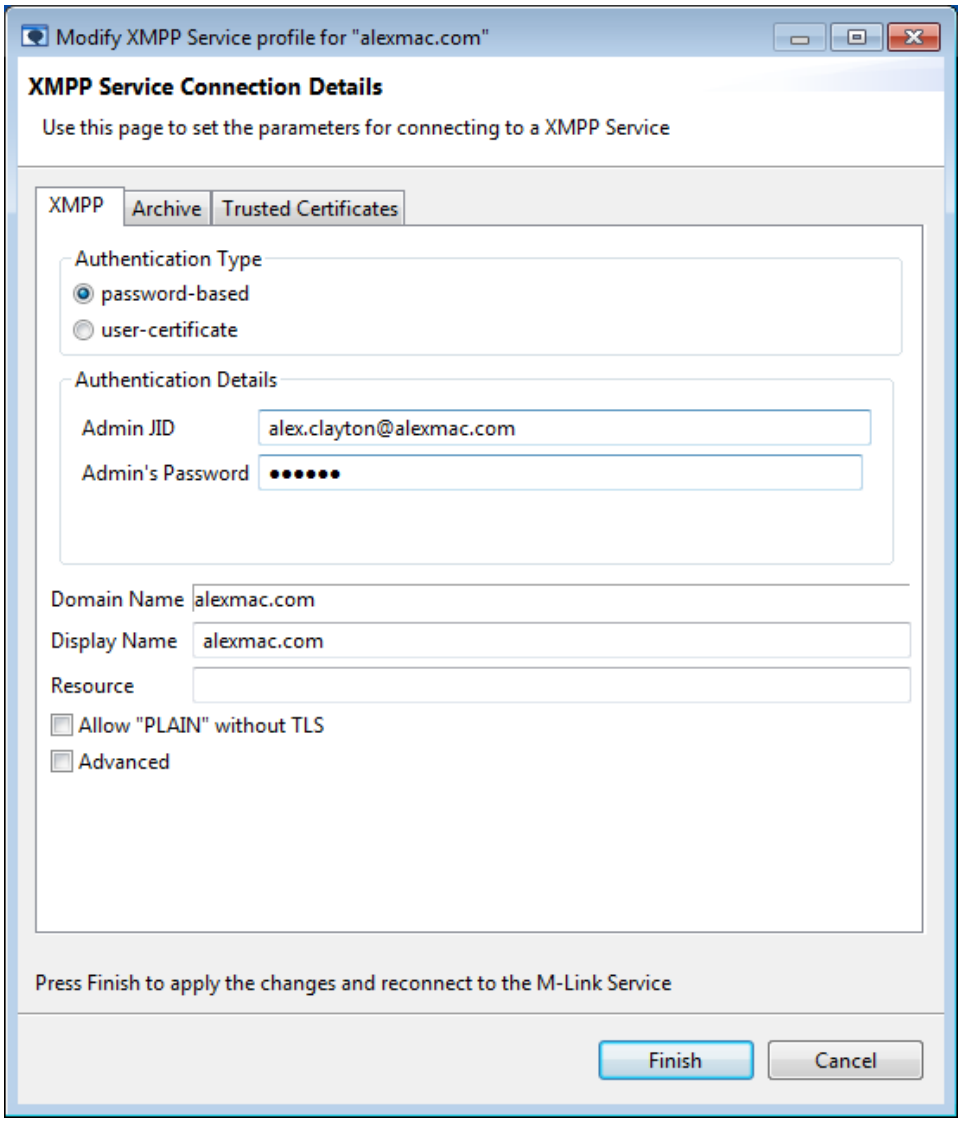
2.9 Additional Topics

2.9.1 Adding, modifying or deleting M-Link Console profiles

The services view contains information about all the XMPP services that are stored in the profile file. A profile will be created by M-Link Console for any M-Link Server that you created.

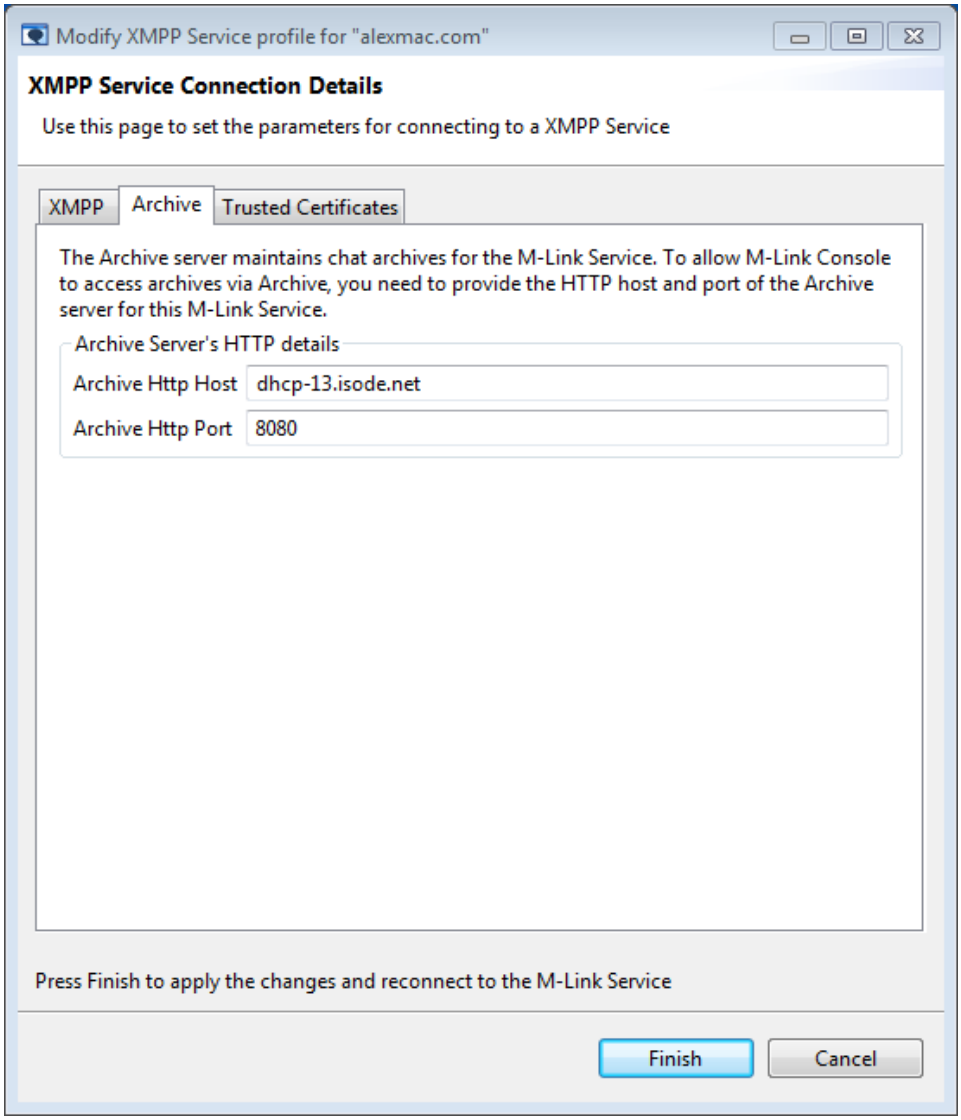
You can also add profiles for XMPP services that already exist (either on the local system or on remote systems). To do this, use **M-Link Console → Create Profile for existing XMPP Service...**, and enter details about the XMPP service. The dialog displays a set of tabs for configuring authentication and other details. The first tab is used for the configuration of authentication details. The example below shows a profile configured to use *Password based* authentication (*User certificate* authentication is described in Section 2.9.2, “Certificate Based Authentication”). For simple authentication, a JID and password are required.

Figure 2.31. Profile for an existing service (simple authentication)



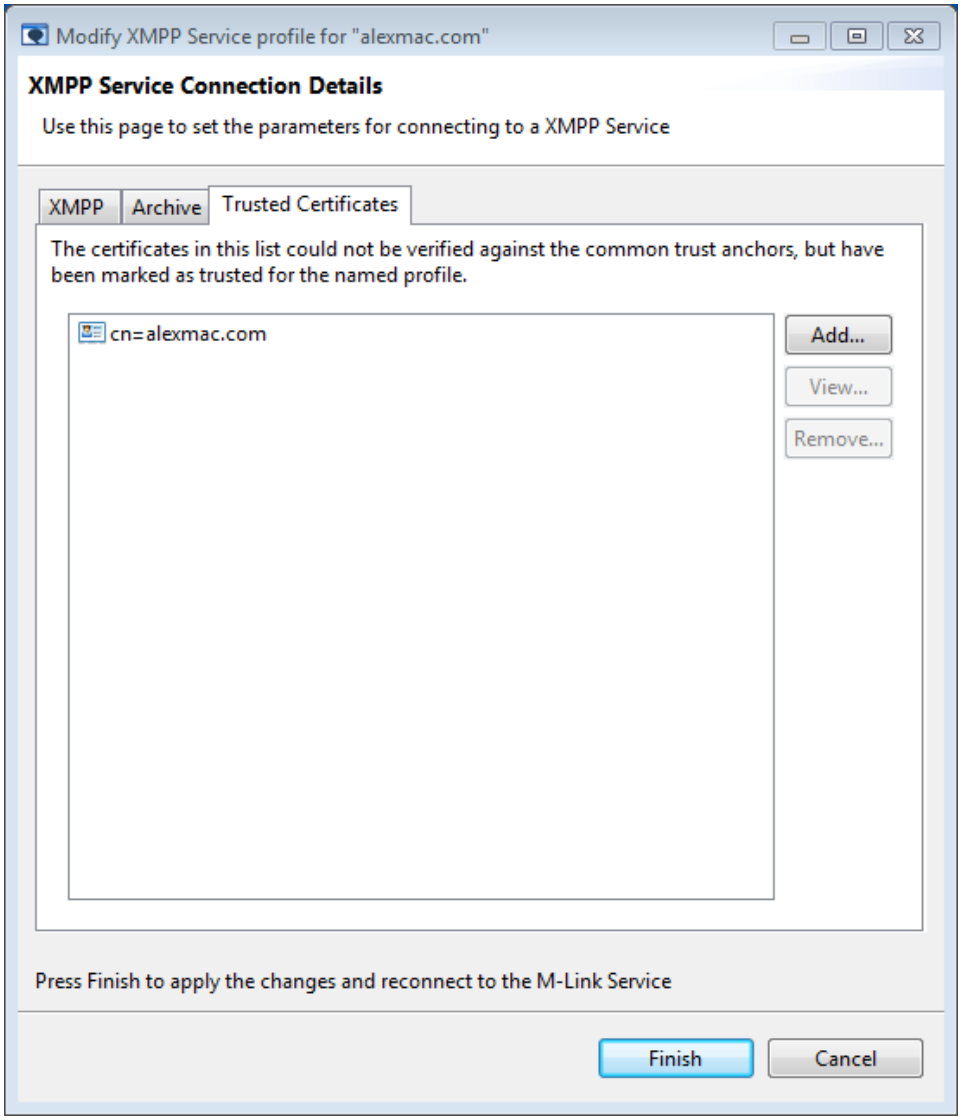
The **Archive** tab is used for configuring the details of HTTP server and port for connecting to the M-Link Archive Server. M-Link Console will use these details to connect to the M-Link Archive Server for archiving services (see Section 15.7.2, “Using Archive Services in M-Link Console”).

Figure 2.32. HTTP connection details of Archive Server



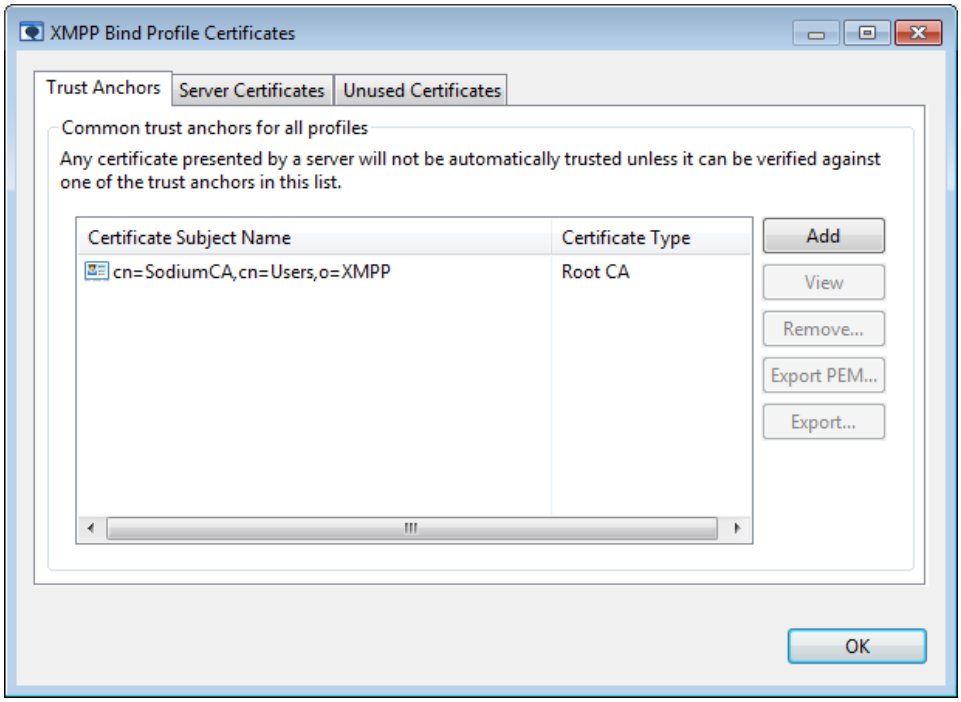
The **Trusted Certificates** tab is used for pinning server certificates in order to trust connection to the server configured with one of certificates listed here. Certificate pinning is used in certain situations where it is not possible to verify server certificates using the configured trusted root CA certificates (see Figure 5.16, “Untrusted Server Certificate Dialog”).

Figure 2.33. Trusted Certificates for Profile



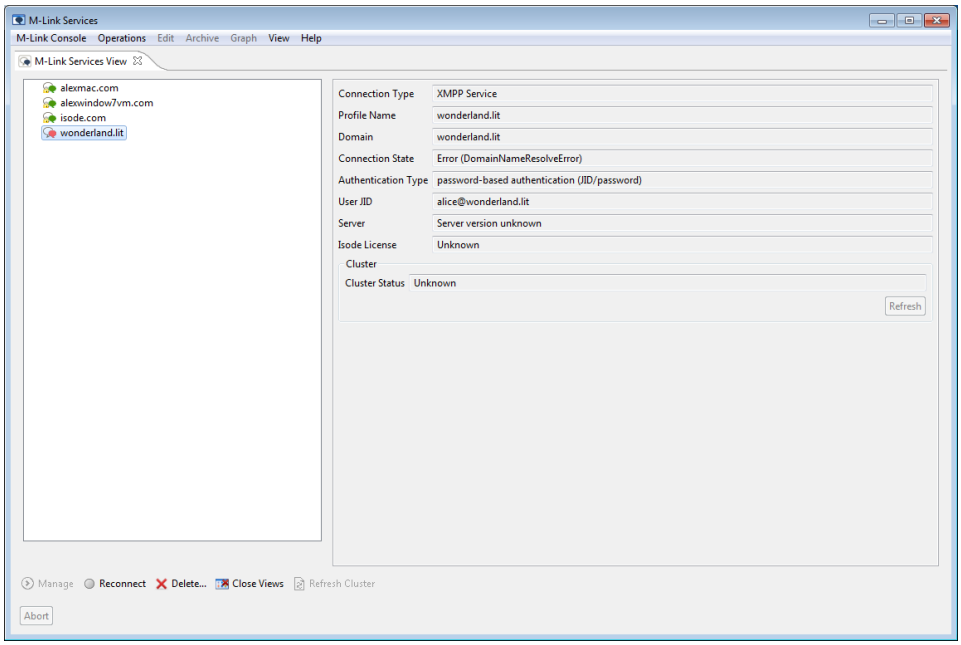
However, the ideal way to ensure secure trusted connections is by configuring the root CA certificates that you trust, using the **M-Link Console → Manage Trusted Certificates...** option. On selecting the menu, a dialog to configure certificates will appear as shown below:

Figure 2.34. Configuring Trusted Certificates



When you press **Finish**, M-Link Console will add a new profile and show the service on the Services view. It will then attempt to connect to the service, using the administrator JID and Password that you supplied. If M-Link Console is unable to establish a connection, a red icon will be displayed, and the **Connection State** will contain an error message.

Figure 2.35. A service that is unavailable



You can modify an existing profile (for example, to correct a mistyped JID or password) by using **M-Link Console** → **Connection Details...**, or remove a profile altogether using the **Delete...** button on the toolbar.

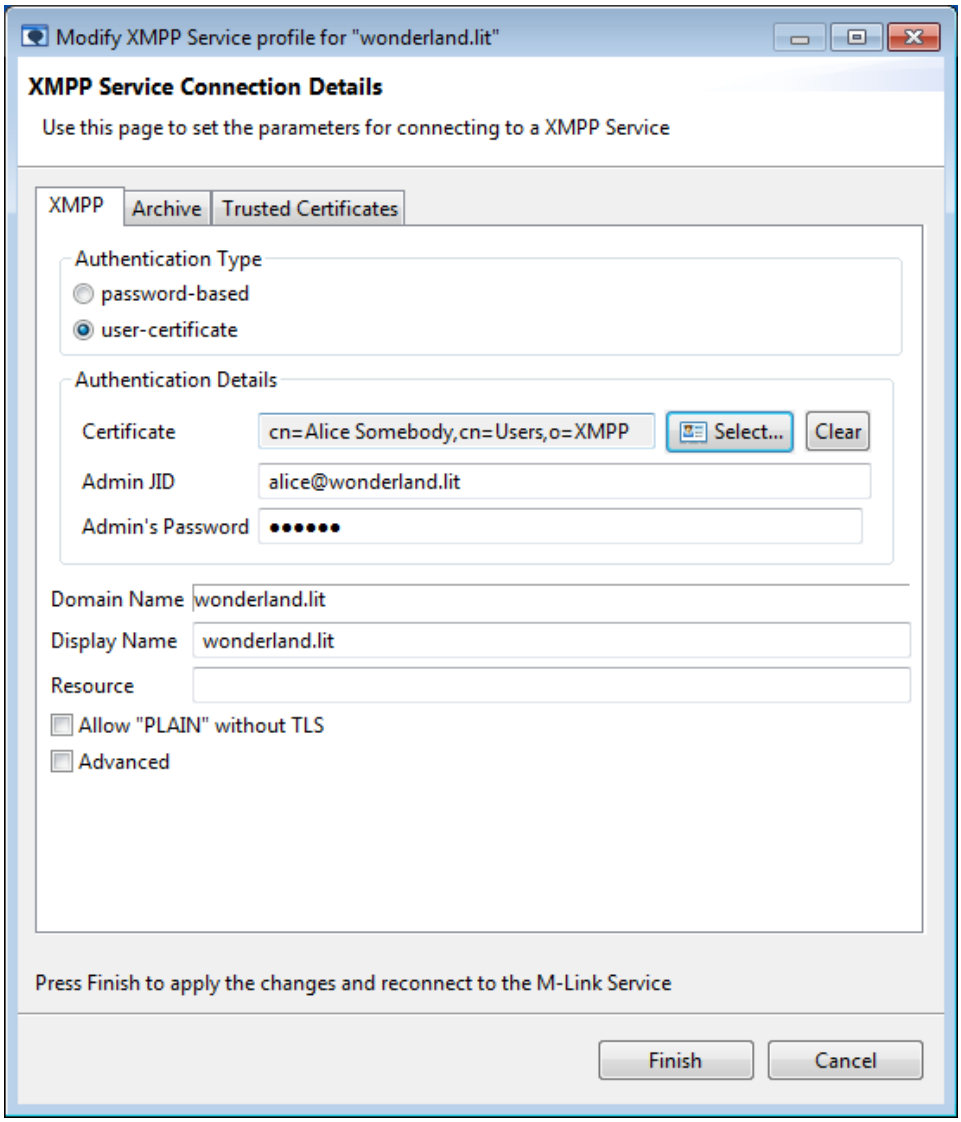
2.9.2 Certificate Based Authentication

You may configure M-Link Console to connect to a server using *User certificate* authentication. In this case, a client certificate is sent to the server over a TLS-protected

connection, and the server determines what access to allow based on information in the certificate. Certificate based authentication is therefore only usable in cases where the server is configured to allow TLS and suitable trust anchors have been configured.

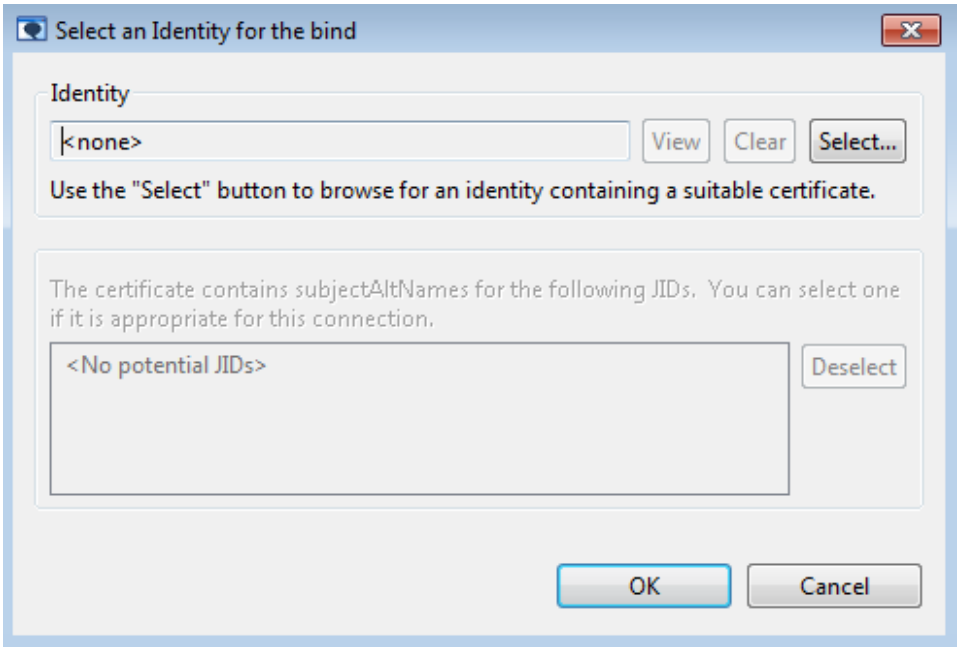
When the **User certificate** option is selected in the **XMPP Service Connection Details** dialog, any existing certificate that has been configured will be shown:

Figure 2.36. Profile for Certificate Based Authentication



Clicking on the **Select...** button invokes the **Select Identity** dialog, which will show you information about the current certificate (if there is one):

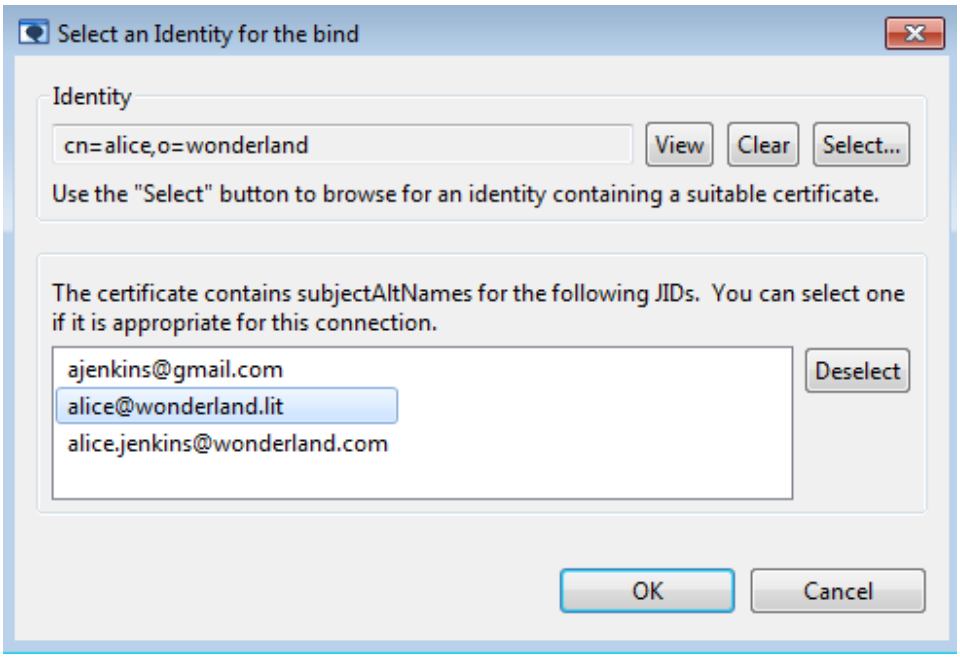
Figure 2.37. Select Identity Dialog for Certificate Based Authentication



To choose the certificate that you want to use, click on the **Select...** button. This will invoke the **Browse Identities** dialog box, as shown below. The **PKCS#12 files** tab lets you browse the filesystem and select a file containing a suitable identity.

Once you have selected an identity and clicked **OK**, the **Select Identity Dialog** will display the identity you chose, as well as showing any subject alternative names from the certificate which contain JIDs:

Figure 2.38. Selecting a JID from a certificate



If any of them is suitable, you can choose an appropriate JID from the list (if none is suitable, you can enter a JID by hand later). Once you have done this, click **OK** to return to the **XMPP Service Connection Details** dialog.

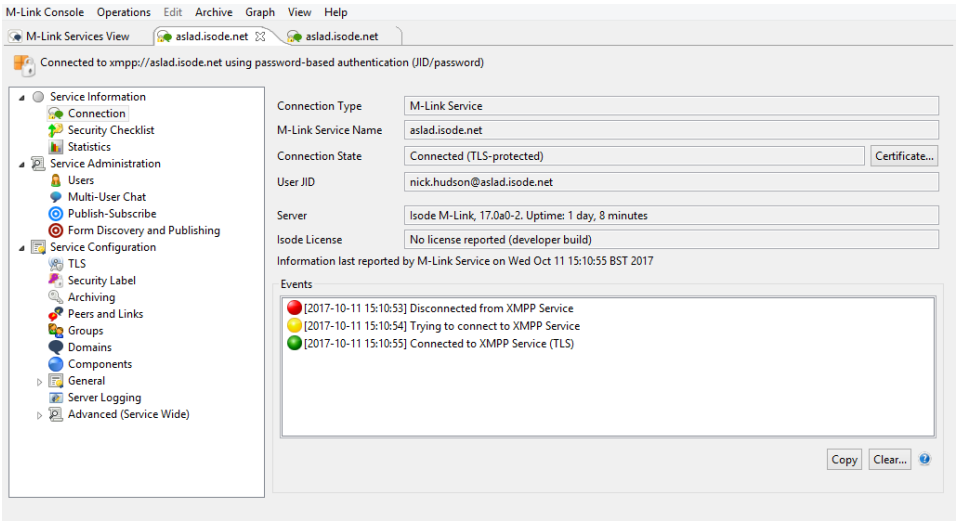
When you press **Finish** for a profile using certificate based authentication, M-Link Console will add a new profile and show the service on the Services view. It will then attempt to connect to the service using the certificate.

2.9.3 Service View

M-Link Console displays the *service* configuration in the *service* view. It retrieves the *service* configuration from whichever node responded when M-Link Console connected to the XMPP service (in a clustered configuration, there may be more than one node). The basic service view shows settings which are configured service-wide.

You can open a *service* view for any service which appears in the services view, by selecting it and clicking on the **Manage** button. The screenshot below shows a typical service view.

Figure 2.39. XMPP Service View

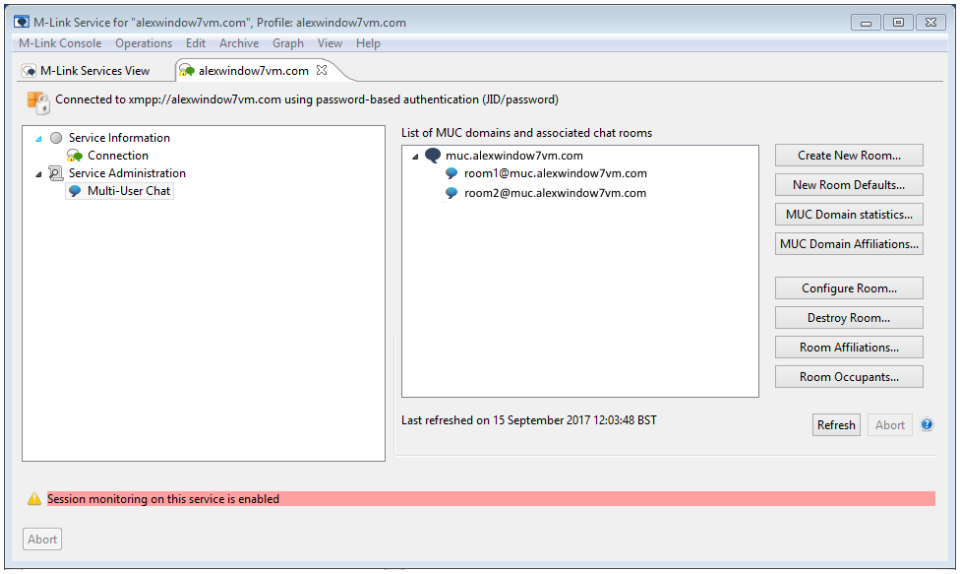


The left-hand pane of the view shows a list representing the different types of information which M-Link Console can control. When an item in the list is selected, the right-hand pane will show the options corresponding to that section.

When the *Connection* item is selected (as shown above), the right-hand pane shows information about the service, including an *Events* list, which contains information when M-Link Console has lost and attempted to regain its connection to the service, and so can be used to tell when the service may have been unavailable.

The other items in the left-hand pane typically correspond to configuration which is only permitted for users who are members of the server administrators group (see Section 2.5.1, “Server Administrators”). When M-Link Console authenticates as a user who is a domain administrator, then a restricted set of configuration is shown, corresponding to the domains that the user is allowed to manage. The screenshot below shows the view that would appear for a user who is domain administrator for a single MUC domain.

Figure 2.40. XMPP Service View for a Domain Administrator



If M-Link Console authenticates as a user who is neither a service nor group administrator, then no configuration options will be shown.

M-Link Console provides a number of editors arranged into three categories:

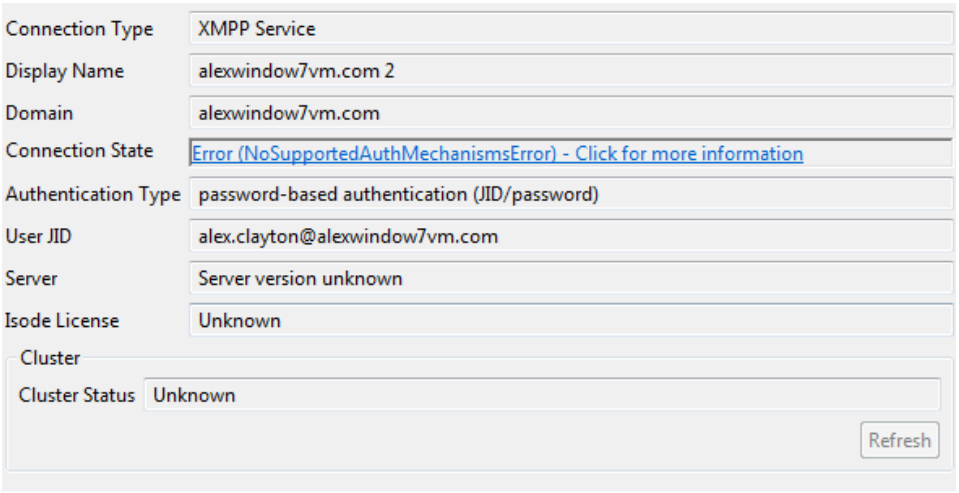
- **Service Information**
  - The **Connection** editor is described in Section 2.9.3, " Service View".
  - The **Security Checklist** editor displays the results of a set of tests based on the current configuration, and suggests any changes that may help to increase security. The Security Checklist is described in Section 16.2, " Security Checklist".
  - The **Statistics** editor displays statistical information returned by the service. Statistics are described in Chapter 17, *Statistics*.
- **Service Administration**
  - The **Users** editor is described in Chapter 6, *M-Link User Management*.
  - The **Multi-User Chat** editor is described in Section 9.5, " MUC Administration using M-Link Console".
  - The **Publish-Subscribe** editor is described in Section 10.4, " Using M-Link Console to manage Publish-Subscribe services".
  - The **Form Discovery and Publishing Administration** editor is described in Section 10.5, " Using M-Link Console to manage Form Discovery and Publishing".
- **Service Configuration**
  - The **TLS** editor is described in Chapter 5, *Configuring TLS*.
  - The **Security Label** editor is described in Chapter 7, *Security Labels in XMPP*.
  - The **Archiving** editor is described in Chapter 15, *Archive Management*.
  - The **Peer and Link** editor is described in Section 8.5, " Peer Configuration" and Section 8.10, "Configuring Links".
  - The **Groups** editor is described in Chapter 4, *Configuring Groups*.
  - The **General** editorallows configuration of client and server connections, BOSH (Chapter 12, *XMPP over BOSH*) and cluster communication (Chapter 14, *Clustering*).
  - The **Domain** editor is described in Chapter 3, *Domains*.
  - **Server Logging** editor is described in Chapter 18, *Monitoring the M-Link Server*.
  - The **Advanced** editor is described in Section F.1, "Advanced Configuration using MLC".

If you are managing a cluster, then the service view will show extra information. Clustering is described in Chapter 14, *Clustering*.

2.9.4 No Supported Authentication Error Message

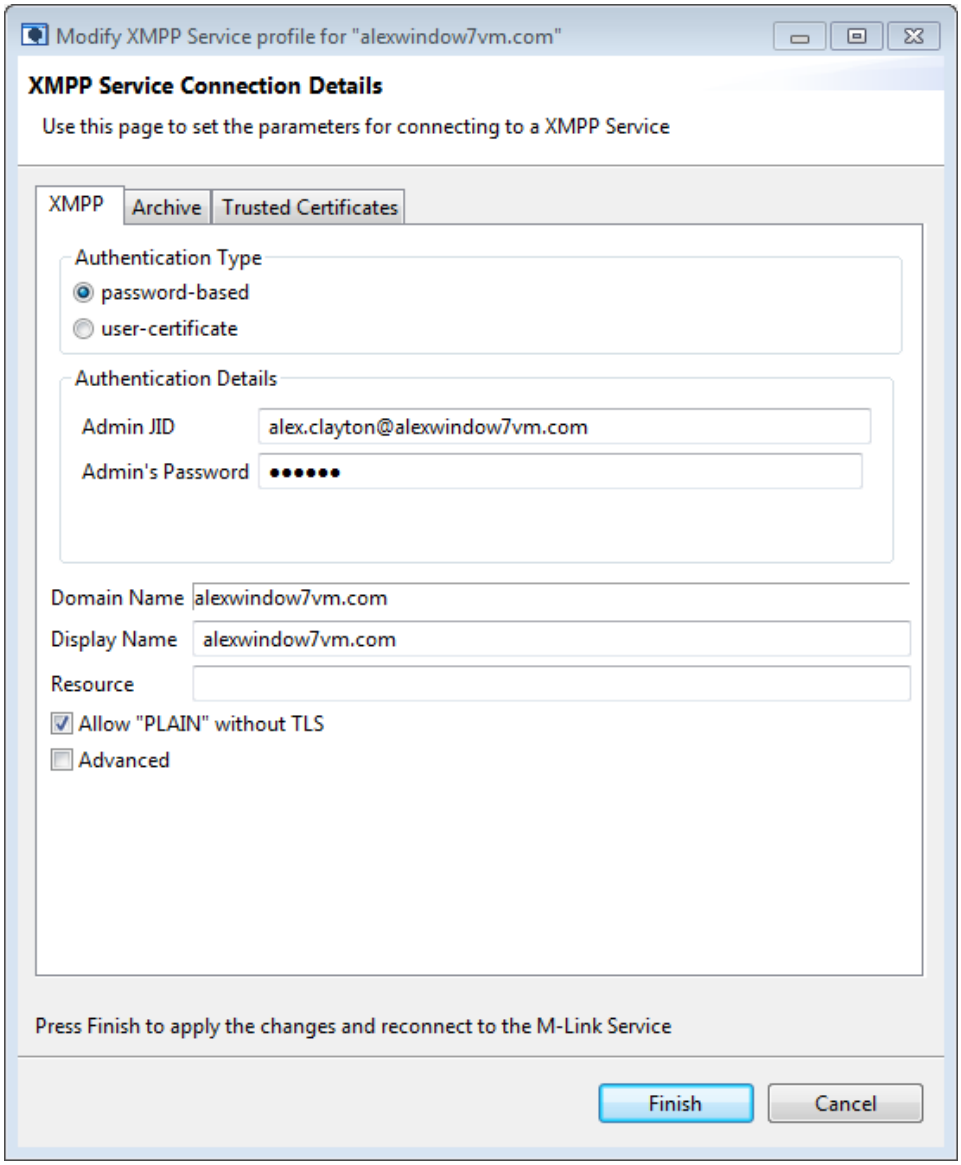
When connecting to a service, M-Link Console will avoid authentication mechanisms where credentials are sent in clear text. Typically this is done by establishing a TLS connection before sending authentication information. If TLS cannot be established, and there are no authentication mechanisms available which protect the user's credentials, then the connection will fail, and **NosupportedAuthMechanismsError** will be displayed in the **Connection State** field of the **Services View**.

Figure 2.41. No Supported Authentication Mechanisms Error



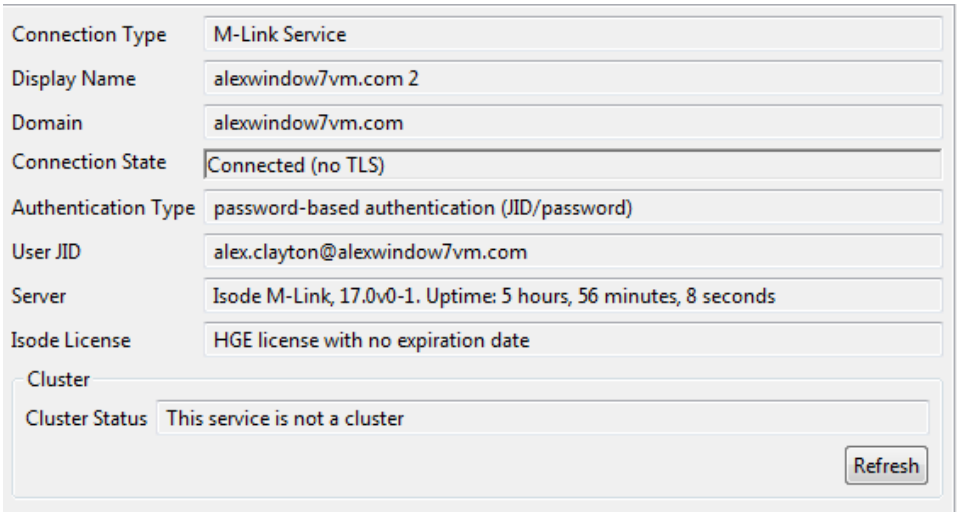
In this case it is recommended that the server should be reconfigured to enable TLS (see Chapter 5, *Configuring TLS*). If this is not possible then the bind profile for the service can be configured to allow plain text passwords to be sent when TLS has not been established. This can be done by opening the **Connection Details** for the profile (see Section 2.9.1, “Adding, modifying or deleting M-Link Console profiles”) and enabling the **Allow "PLAIN" without TLS** checkbox.

Figure 2.42. Enable Allow "PLAIN" without TLS



M-Link Console should now be able to connect to the server but the connection will not be secured. The identity of the server will not be verified and the confidentiality of the authentication exchange as well as XMPP traffic will not be protected. In particular, the user's name and password will be exposed along with all instant messaging and presence information.

Figure 2.43. Connecting to a server after allowing Allow "PLAIN" without TLS



2.9.5 DNS Configuration

XMPP clients and servers typically use the *Domain Name System* (DNS) to determine the IP addresses and TCP ports of XMPP servers they need to connect to. For XMPP Client-to-Server (C2S) the following discovery approach is typically used.

Clients first look for SRV resource records for the XMPP domain they wish to connect to. Each SRV resource record for a domain provides a location (a domain name and a port) for the service (e.g., XMPP C2S). Multiple SRV resource records may be published for each service. In addition to the service location, each SRV resource record has a priority and a weight. Preference of two SRV resource records is given to one with the lower priority value or, in the case the equal priority, to the resource record with the higher weight. The location's domain name is resolved to a set of IP addresses using normal A and AAAA lookup. Depending on the client's configuration, if both IPv4 and IPv6 are supported, preference may be given to one or the other. Otherwise, IP addresses are typically tried in the order provided by the Domain Name System, which may or may not change with each lookup.

If SRV resource records are not published for the domain, clients and servers will resolve the domain name to a set of IP addresses and connect to each using the default port for the protocol. This is accomplished by looking for A and AAAA resource records for IPv4 and IPv6 addresses respectively, possibly with CNAME resolution when necessary. As above, this resolves to a set of IP addresses. Depending on the client's configuration, if both IPv4 and IPv6 are supported, preference may be given to one or the other. Otherwise, IP addresses are typically tried in the order provided by the Domain Name System, which may or may not change with each lookup.

In deployments where DNS is not available, clients will often use other host-to-IP address lookup systems, such as those provided by a hosts file. These typically behave similarly to DNS with only A and AAAA resource records. Configuration of alternative host-to-IP address lookup systems is not detailed in this guide.

To illustrate proper configuration of DNS, consider an XMPP service consisting of a three node cluster providing Instant Messaging service for the domain *`example.com`*, where the cluster nodes are named *`node1.example.com`*, *`node2.example.com`*, and *`node3.example.com`*. The nodes have IPv4 addresses *`192.0.2.1`*, *`192.0.2.2`*, and *`192.0.2.3`* respectively. The nodes have IPv6 addresses *`2001:DB8::1`*, *`2001:DB8::2`*, and *`2001:DB8::3`* respectively. We assume the XMPP C2S protocol is available on its default port, `5222`. Additionally we'll assume this IM service is not co-located with other `example.com` services such as WWW.

Note that these examples utilize the Domain Name System *zone file* format specified in [*RFC 1035*] (§ 5) and [*RFC 1034*] (§ 3.6.1). Furthermore,the examples assume placement in the zone *example.com*:

```
$ORIGIN example.com.
```

Each node should have an appropriate resource records for addressing purposes:

```
node1 IN A 192.0.2.1
node1 IN AAAA 2001:DB8::1
node2 IN A 192.0.2.2
node2 IN AAAA 2001:DB8::2
node3 IN A 192.0.2.3
node3 IN AAAA 2001:DB8::3
```

SRV resource records can then be provided. Here we've given equal preference to each node in our cluster.

```
_xmpp-client._tcp IN SRV 1 1 5222 node1
_xmpp-client._tcp IN SRV 1 1 5222 node2
_xmpp-client._tcp IN SRV 1 1 5222 node3
```

While the domain naming each node allow for users to manually configure their client to connect to any one of the three nodes, it is often desirable to provide a domain which they can use to have the client connect to any of the nodes. The following resource records creates *xmpp.example.com* for this purpose as well as other purposes discussed below.

```
xmpp IN A 192.0.2.1
xmpp IN AAAA 2001:DB8::1
xmpp IN A 192.0.2.2
xmpp IN AAAA 2001:DB8::2
xmpp IN A 192.0.2.3
xmpp IN AAAA 2001:DB8::3
```

If the DNS servers providing the example.com zone support CNAME round robins, the *xmpp.example.com* A and AAAA resource records can be replaced with:

```
xmpp IN CNAME node1
xmpp IN CNAME node2
xmpp IN CNAME node3
```

For clients using XMPP over BOSH, clients can discover the BOSH URL using the [*XEP-0156*] discovery method. See the Chapter 12, *XMPP over BOSH* for a discussion of BOSH URLs. To support this discovery in our example, the following TXT resource record is published:

```
_xmppconnect IN TXT (
     "_xmpp-client-xbosh=https://xmpp.example.com:5280/bosh" )
```

This resource record relies on domain *xmpp.isode.com* previously configured.

As we assumed the IM service is not co-located with other example.com services, note that we don't publish any A and AAAA resource records for the XMPP nodes at *example.com*. We also do not use *example.com* in the BOSH URL.

If a WWW service is available at the URL `https://example.com` or `http://example.com`, host-meta data can be published using either XML or JSON.

XML host-meta example:

```
<?xml version='1.0' encoding=utf-9'?>
<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'>
   ...
   <Link rel="urn:xmpp:alt-connections:xbosh"
       href="https://xmpp.example.com:5280/bosh" />
   ...
<XRD>
```

JSON host-meta example:

```
{
   ...
   "links": [
      ...
      {
        "rel": "urn:xmpp:alt-connections:xbosh",
        "href": "https://xmpp.example.com:5280/bosh"
      },
      ...
    ]
}
```

For XMPP S2S the following discovery approach is similar to XMPP C2S. For the IM domain, the following would be published assuming S2S is available on the default port, `5269`:

```
_xmpp-server._tcp IN SRV 1 1 5269 node1
_xmpp-server._tcp IN SRV 1 1 5269 node2
_xmpp-server._tcp IN SRV 1 1 5269 node3
```

Additionally, DNS SRV records should be created for each other XMPP domain accessible by other XMPP servers. For instance, assuming a Multi-User Chat service domain of *`muc.example.com`* and Publish-Subscribe service at *`pubsub.example.com`*, the following additional resource records should be published:

```
_xmpp-server._tcp.muc IN SRV 1 1 5269 node1
_xmpp-server._tcp.muc IN SRV 1 1 5269 node2
_xmpp-server._tcp.muc IN SRV 1 1 5269 node3

_xmpp-server._tcp.pubsub IN SRV 1 1 5269 node1
_xmpp-server._tcp.pubsub IN SRV 1 1 5269 node2
_xmpp-server._tcp.pubsub IN SRV 1 1 5269 node3
```

2.9.6 Removing the M-Link Server

To cleanly remove an M-Link Server install:

- Using M-Link Console use it to stop the server, otherwise use the relevant operating system specific method described in Section A.1, “Running as Operating System Service”.
- If M-Link Console has a profile for the service, delete it.
- Delete the *`(MSDIR)`* directory.
- If using Windows, remove the Windows service as described in Section A.1, “Running as Operating System Service”.

To cleanly remove an M-Vault Server instance that may have been created by M-Link Console, run the command:

```
(SBINDIR)/dsa-setup delete -ppfile text-file-containing-bind-profile-pwd
         -dsa DSA-DN dsa-folder
```

Example use is shown below:

Unix

```
# /opt/isode/sbin/dsa-setup delete -ppfile secret.txt
  -dsa "cn=dsa,o=XMPP" /var/isode/d3-db
```

Windows

```
# C:\>"C:\Program Files\Isode\bin\dsa-setup.bat" delete
  -ppfile C:\secret.txt -dsa "cn=dsa,o=XMPP" C:\Isode\d3-db
```

Lastly uninstall the Isode M-Link and Isode M-Vault packages.

Chapter 3 Domains

This chapter describes how M-Link Console can be used to view, modify, create and delete domains.

3.1 Overview

In XMPP, domains are used to identify *Instant Messaging* (IM) services, such as the `example.com` in `joe@example.com`. As well as Instant Messaging domains, an M-Link service can also have *Multi-User Chat* (MUC) and *Publish-Subscribe* (PubSub) domains. *Server* Administrators have full control over domains (including creating and deleting them). Each domain has an optional *Domain* Administrators group, whose members may make changes within the domain.

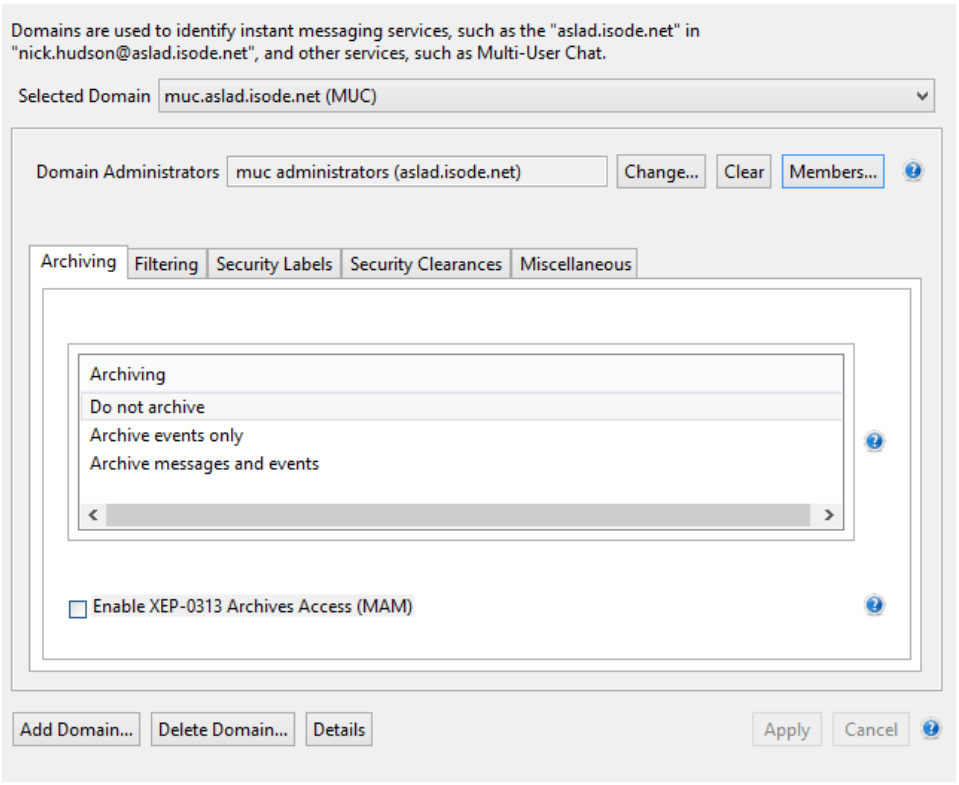
For the purposes of Service Discovery (see [*XEP-0030*]), MUC and PubSub domains are organised using a hierarchy which places them “beneath” IM domains, but while it may be useful to configure a service so users of a given IM domain have visibility only to domains “beneath” it, the M-Link service does not impose any such access controls by default.

3.2 Using M-Link Console to manage domain configuration

M-Link Console provides a customised editor to manage domain configuration. Domain configuration always applies to the whole service, and cannot be overridden for any particular node. This editor is only available to users who are members of the Service Administrators group.

Selecting the **Domain** editor in the service view (In the **Service Configuration** section) will display an editor that allows you to select from the configured domains. The **Selected Domain** selection includes the name and type of each domain:

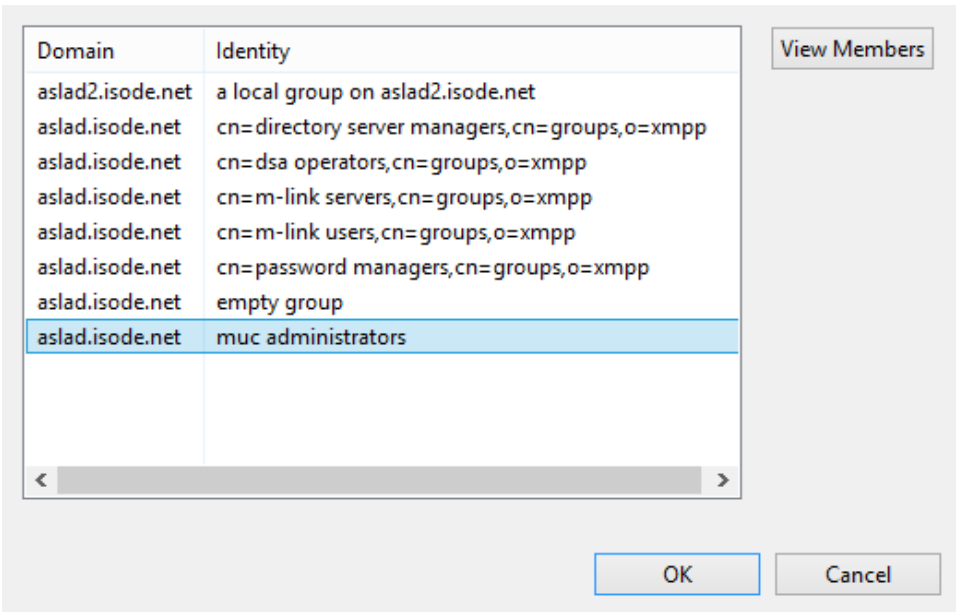
Figure 3.1. Domain configuration editor showing a MUC domain



3.2.1 Domain Administrators

Server Administrators always have the ability to make any configuration change to any domain. A domain may (but does not have to) have a designated *Domain* Administrators group. Members of the domain administrators group have access to service administration for the domain, although they cannot make any changes to the domain itself. To select a domain administrators group, use the **Change...**, which will display a dialog showing available groups:

Figure 3.2. Selecting a Domain Administrator group



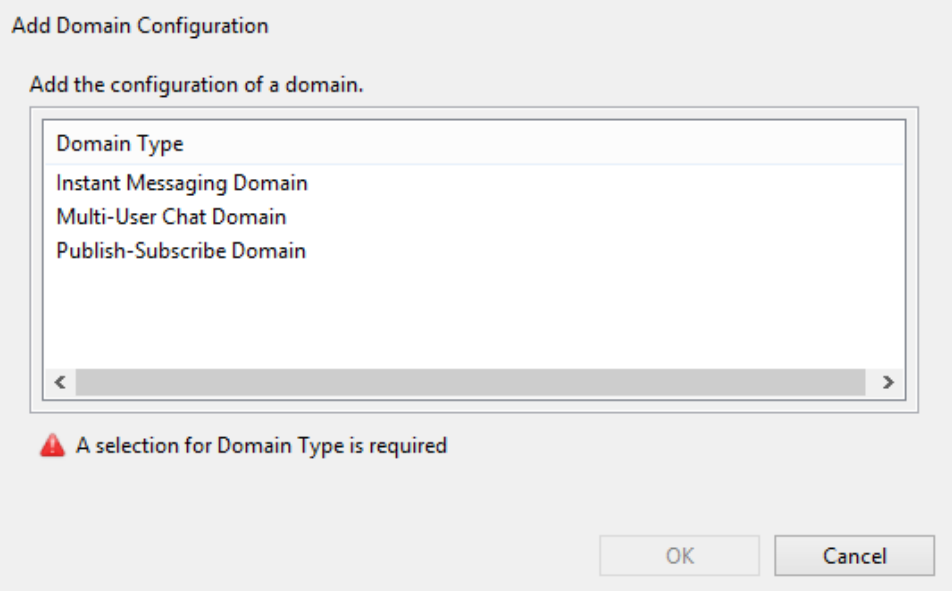
The dialog shows all available groups (both Local and Directory groups), together with the name of the IM domain where each group has been defined (see Section 4.1,

"Overview"). The group used as the Domain Administrator group for a domain can belong to any IM domain. When displaying a selected group, MLC includes the domain name in the **Domain Administrators** selector (to distinguish cases where different IM domains may have groups with the same name).

3.2.2 Adding and Configuring Domains

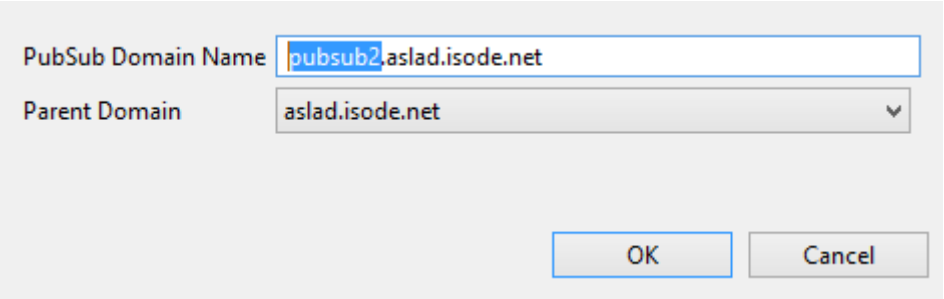
To add a domain, click on **Add domain** button and choose a domain type.

Figure 3.3. Select Domain Type



The wizard will prompt you for the name of the new domain. In the case of MUC and PubSub domains, you also need to choose a parent domain; MLC will suggest a name for these domains which contains a suffix matching the parent domain. Isode recommends following the suggested naming convention to make administration less confusing, but there is no requirement that you do this.

Figure 3.4. Choose Domain Parent and Name



After selecting the domain type and name, you have the opportunity to configure options for the domain before creating it, including specifying the Domain Administrators group. The options will be displayed in the configuration tabs and may vary depending on the type of domain being added (see Figure 3.1, "Domain configuration editor showing a MUC domain" above). Individual fields inside the editor will display tooltips with extra information about the parameters they correspond to.

Once the details for the new domain have been completed, use the **Apply** button to create the domain. The new domain will appear in the **List of domains**, and you can subsequently use this control to select which of the configured domains you want to view, modify or remove.

The tabs shown inside the domain editor are:

- The **Authentication** tab is displayed for IM domains and is used to configure the location of the Directory Server that contains user information for this IM domain. See Section 3.2.3, “User Directory configuration for IM domains”.
- The **Mapping** tab is displayed for IM domains and is used to configure the how user information for this IM domain is found inside the Directory Server. See Section 3.2.3, “User Directory configuration for IM domains”.
- The **Archiving** tab is used to configure whether archiving is performed on the domain. (See Section 15.4, “Archive Data and Configuration” for more information).
- The **Filtering** tab is used to specify filters that are used to constrain traffic to and from this domain. For information about how filtering works, see Section 8.8, “Peer Filtering”.
- The **Security Labels** tab allows you to configure a security label. Note that you cannot set this value unless security policy for the server has been configured. See Chapter 7, *Security Labels in XMPP*) for more information.
- The **Security Clearances** tab is used configure clearances for this domain. Note that you cannot set this value unless a security policy for the server has been configured. See Chapter 7, *Security Labels in XMPP* for more information.
- Other options for domain configuration (which may vary based on domain type) are shown in the **Miscellaneous** tab.

3.2.3 User Directory configuration for IM domains

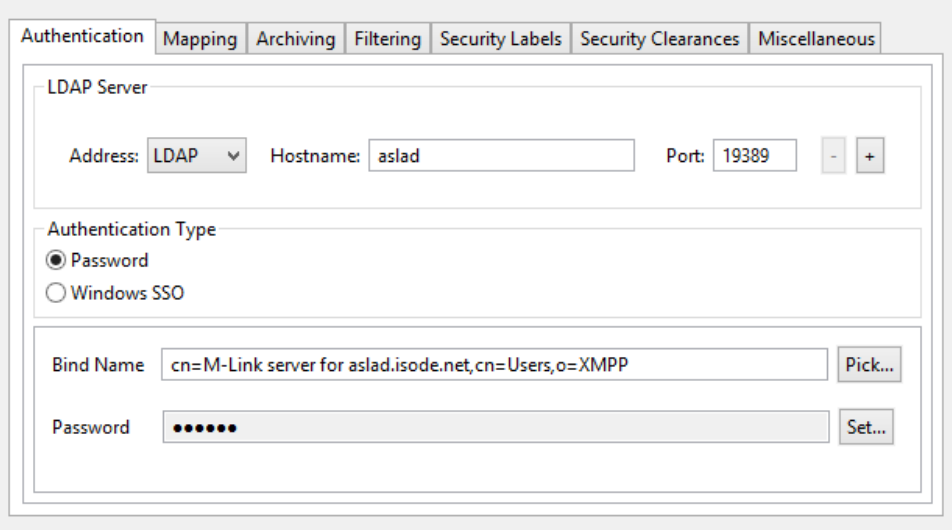
Each IM domain is associated with an LDAP directory which is used:

- to provide a database of users that are allowed to use the domain.
- as the source of Directory Groups (see Section 4.1, “Overview”) for the domain.

3.2.3.1 Authentication Configuration

The **Authentication** tab is used to configure how the M-Link service connects to the directory:

Figure 3.5. Authentication tab



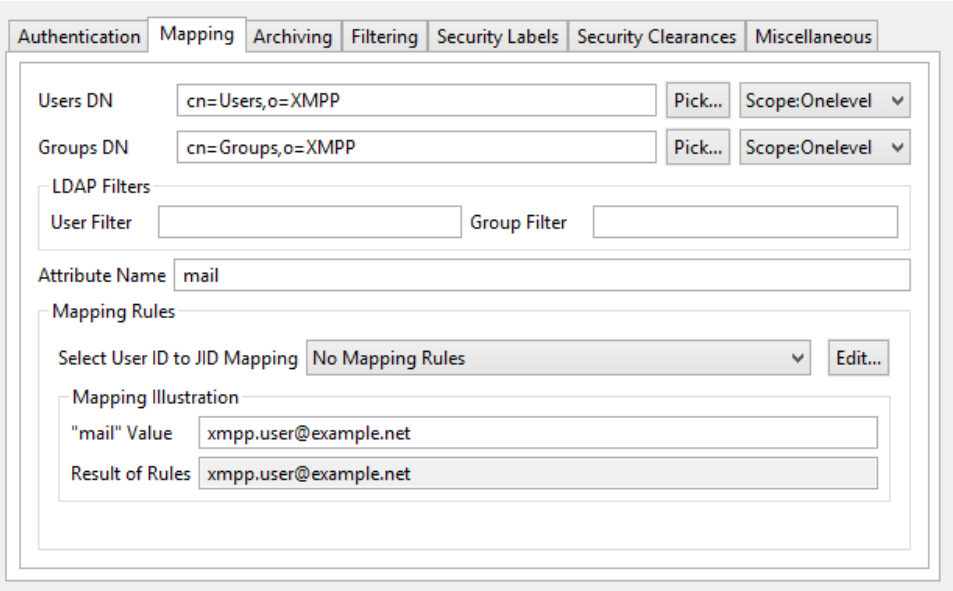
For **Password** based authentication, a bind name and password are required. This password is stored in encrypted form, and so although you can change the password value, you cannot view any saved value.

For Windows SSO (Single Sign On), no bind credentials need to be configured on this tab, and the M-Link service uses it's designated Service Principal Name (SPN) to authenticate to the specified Active Directory.

3.2.3.2 Mapping Configuration

The **Mapping** tab is used to configure how the M-Link service locates and processes information inside the directory for users and groups:

Figure 3.6. Mapping tab



To locate user entries, the M-Link service performs a search of the directory, starting at the location specified in **Users DN**. Depending of the value for **Scope**, the search includes only entries directly beneath the **Users DN** (*Onelevel*), or all entries at any depth below **Users DN** (*Subtree*).

The *Directory Groups* (see Chapter 4, *Configuring Groups*) exposed by this IM domain correspond to entries in the Directory Server which are found by searching beneath this **Groups DN** in the directory. Any entries representing groups will be exposed by this IM domain as directory groups, with members corresponding to values of *member* or *uniqueMember* attributes inside the directory entry.

The **User Filter** and **Group Filter** allow you to add extra constraints to the search performed to find user entries. For example, to include only users in the “engineering” organization, a suitable user filter might be `(o=engineering)`; to exclude groups that are located in “London”: the group filter could be set to `(!(l=london))`.

Inside the directory, each user entry has an attribute containing a user ID. By default, the `mail` attribute is used for this, but this is configurable by changing **Attribute Name**.

The M-Link service performs mapping on user ID values found in the Directory to derive JIDs which will be used to identify those users to XMPP.

Typically, the user ID inside the directory will be identical to the JID for that user, and so no mapping is required. For cases where the user IDs do not correspond to JIDs that are appropriate for this IM domain, you can create a custom mapping rule to convert the user ID in the directory into a suitable JID. The dialog shows the effect of any rule you configure.

Chapter 4 Configuring Groups

This chapter discusses how M-Link Console can be used to view, modify, create and delete groups for an M-Link service.

4.1 Overview

Groups are used to define sets of users: a group name can be used to refer to all of the users it contains.

There are two types of groups: *Local* Groups, which contain a list of user JIDs, and *Directory* Groups, whose members are populated with the result of a Directory search operation, so that their contents can automatically reflect changes to the user database.

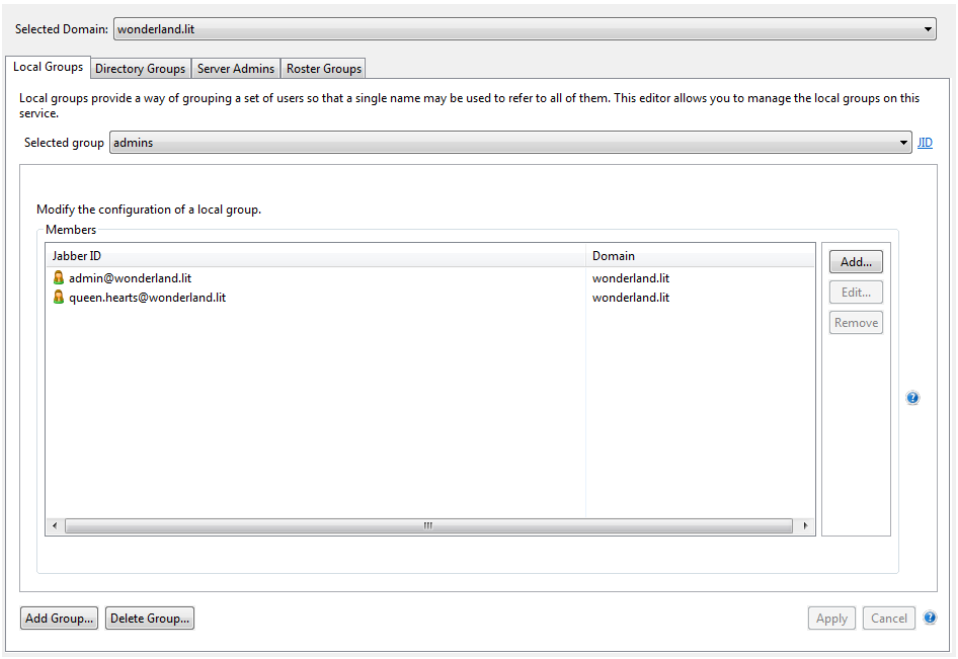
Each group belongs to an IM domain, but its visibility is not restricted to the domain where it is defined. Internally, groups have a JID which is unique for the entire M-Link service. For local groups, part of that JID is a *group name* which is used by MLC when displaying them. Although group names must be unique within any given domain, there is nothing to prevent multiple domains having groups with the same group name. However, this may make it harder for an administrator to distinguish them, and so is not recommended. Directory groups are identified using Distinguished Names (DNs).

4.2 Using M-Link Console to manage group configuration

M-Link Console allows you to manage group configuration using a special editor which only appears for the members of the *Server* Administrators group. Group configuration applies service-wide, and cannot be overridden on individual cluster nodes.

Select **Groups** in the service view to see information about what groups are currently configured:

Figure 4.1. Group configuration editor showing Local Group "administrators"



If the service has more than one IM domain configured, the **Selected domain** selector can be used to pick the IM domain. Four tabs will be shown:

1. The **Local Groups** tab lets you create, delete and modify Local Groups for the selected IM domain. The **Selected group** shows the names of the Local Groups, and allows you to select an existing group to manage. To see the full JID of a given group, click on the **JID** link next to the selector.

   The **Members** box shows existing members of the group. You can add new members by entering or removing JIDs from the box: each JID should occupy a separate line.

   The **Delete group...** allows you to delete the selected Local Group.

   The **Add group...** adds a new Local Group.
2. The **Directory Groups** tab displays which groups (if any) are supplied by the directory for the selected IM domain, and lets you view the members of those groups. All of this information needs to be configured within the directory, and this editor simply provides a way to view the configuration, but not make any changes to it. The configuration which controls how an IM domain uses the directory, see Chapter 3, *Domains*.
3. The **Server Admins** tab shows which group is designated as the *Server* Administrators group. This configuration applies to all domains, and so will display the same information regardless of which IM domain has been selected.

   This tab allows you to view members of the designated Server Administrators group, and you can also change which group should be used as the Server Administrators group.

   Note that misconfiguring the Server Administrators group can result in being locked out from the server: M-Link Console will not allow you to set the Server Administrators group to an empty value, but cannot prevent e.g. configuring a group that subsequently is removed or emptied of members. Care should be taken when making changes to this value.
4. The **Roster Groups** tab shows which roster groups have been configured for the selected IM domain. A “Roster Group” refers to an existing local or directory group in the same domain, and causes all members of that group to be added to each others rosters. The Roster Group's name may, depending on the type of client used, be visible to users in their XMPP clients.

Chapter 5 Configuring TLS

This chapter discusses how to manage TLS configuration of an M-Link service.

5.1 Background

Transport Layer Security (TLS), formally known as Secure Socket Layer (SSL), can be used to provide communication security, namely data integrity and encryption, between M-Link Servers and the clients and servers it communicates with. M-Link Server's use of TLS is not limited to XMPP. Its use in LDAP and various other application protocols is also supported.

An M-Link service's use of TLS requires that you configure identity information, namely an X.509 *certificate* and a private key, then the M-Link service will be able to provide TLS in XMPP and other communications. This identify information is referred to as the server's *identity*. You can select an identity using M-Link Console by referring to a PKCS#12 or PEM file. It is recommended that this file also include a complete *chain* of *CA* certificates.

It is recommended that TLS be configured at the *service* level to the greatest extent possible. However, there are certain cases where *node* configuration must be used. In particular, when it is desirable for each M-Link Server providing an M-Link service to have a separate *identity*, the *identity* must be set at the *node* level.

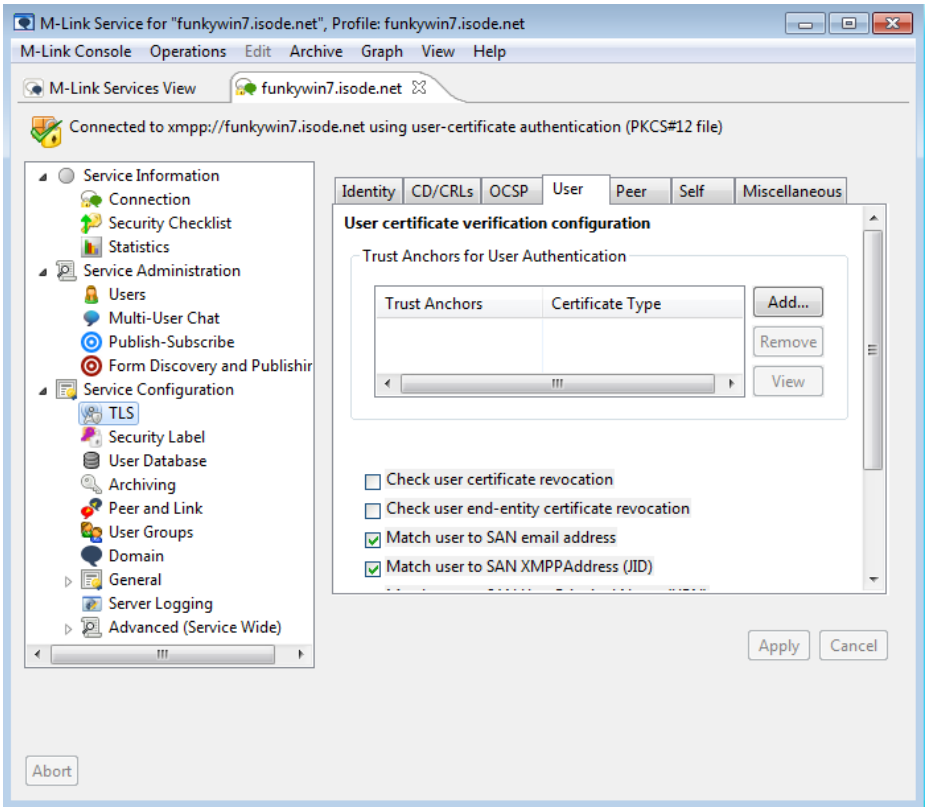
5.2 Steps to configure TLS for an M-Link Server

TLS is configured using M-Link Console in the following steps.

1. In the *service* view, select the **TLS** editor and then select the **Identity** tab. For a clustered service, setting an identity on the TLS tab will set the same identity for all nodes. In order to set a separate identity for each node, an Identity needs to set for each node by setting it on the *Node* item.

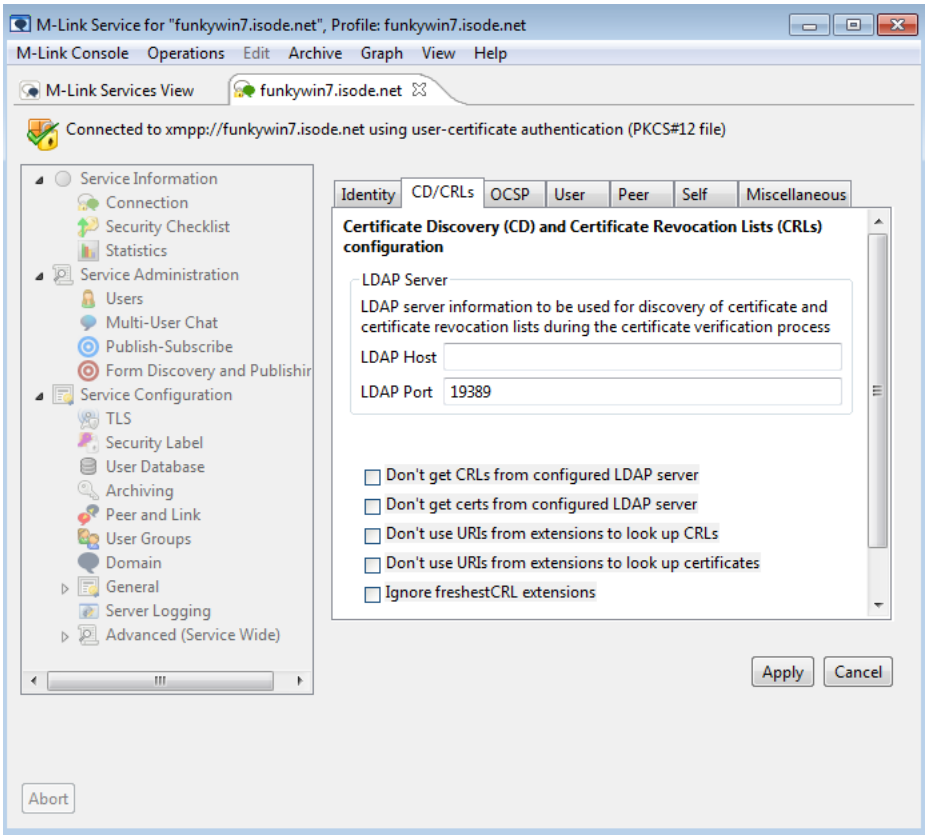
   Note that for a clustered configuration, node's identity will take precedence for a node when an identity has been set up on the Identity tab of the service TLS editor as well.

Figure 5.1. TLS Identity editor



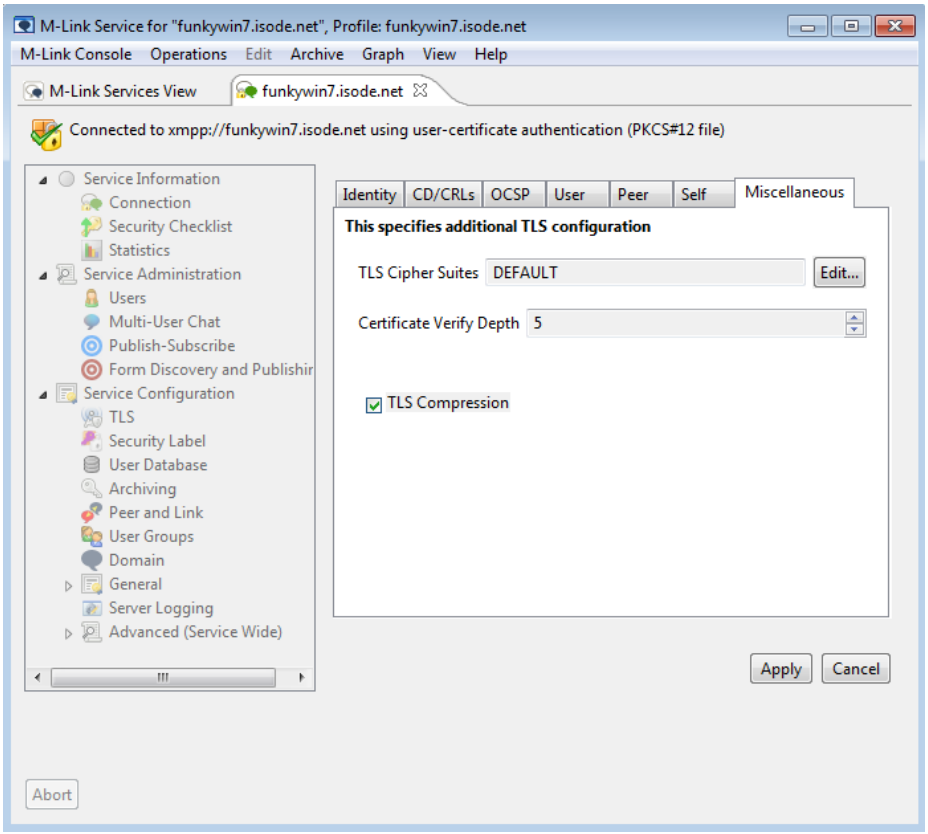
2. The **Identity** tab allows you to select or create an identity for the server to use:
   - **PKCS#12...** enables you to browse the filesystem for an identity which has been created previously.
   - **PEM...** allows you to load in an identity from a file containing concatenated PEM representations of certificates and a private key
   - **Create...** starts a wizard to create a new identity. The wizard is initialised with a subject DN corresponding to the M-Link Server itself. This process is explained below (see Section 5.3, “Creating a new identity for the M-Link Server”
   - **Resume...** is enabled if you have already generated a certificate request and now need to finish creating the identity.
   - If an identity is configured, then you use the **Trust for C2S** or **Trust for S2S** check box to trust the CA certificate in the TLS Identity for all 'client to server' or 'server to server' connections respectively. The server certificate can be added to the list of trusted certificates for inter node communications in a cluster by selecting the **Trust for self** button.
3. Use the **User** tab to specify CA certificates that serve as *Trust Anchors* for XMPP client connections and the **Peer** tab to specify CA certificates that will serve as *Trust Anchors* for peer server connections during certificate verification. The **Self** tab is used for configuring the certificates for intra service communications (e.g. authentication between cluster nodes when the certificates are different for each node).
4. In the *service* view, click the *TLS* editor and select the **CD/CRLs** tab to configure where the M-Link Server should look for Certificate Revocation Lists and Certificates to be used for certificate verification and CRL checking. Note that the other flags on this tab are not dependent on the configuration of the LDAP Host and Port.

Figure 5.2. Certificate Discovery and CRL Checking Configuration



5. Use the **OCSP** tab to configure an OCSP URI and OCSP responder certificate to be used for checking status of certificates using Online Certificate Status Protocol. The flags on this editor can be set or unset to tune the OCSP configuration.
6. The miscellaneous tab allows you to modify the TLS Cipher Suites and rest of the TLS related attributes for the service.

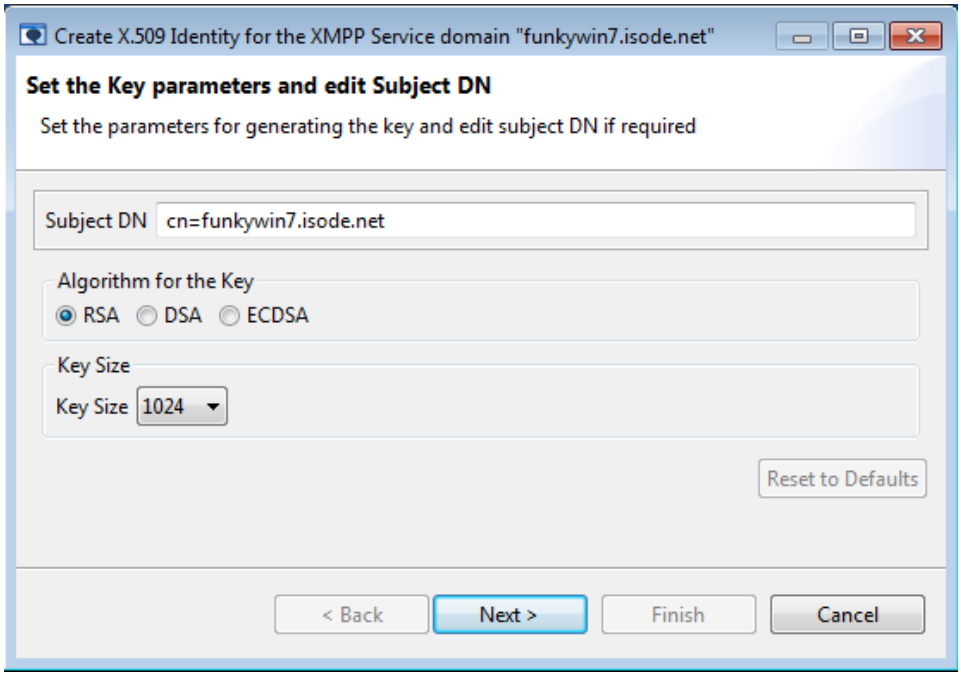
Figure 5.3. Miscellaneous TLS Attributes



5.3 Creating a new identity for the M-Link Server

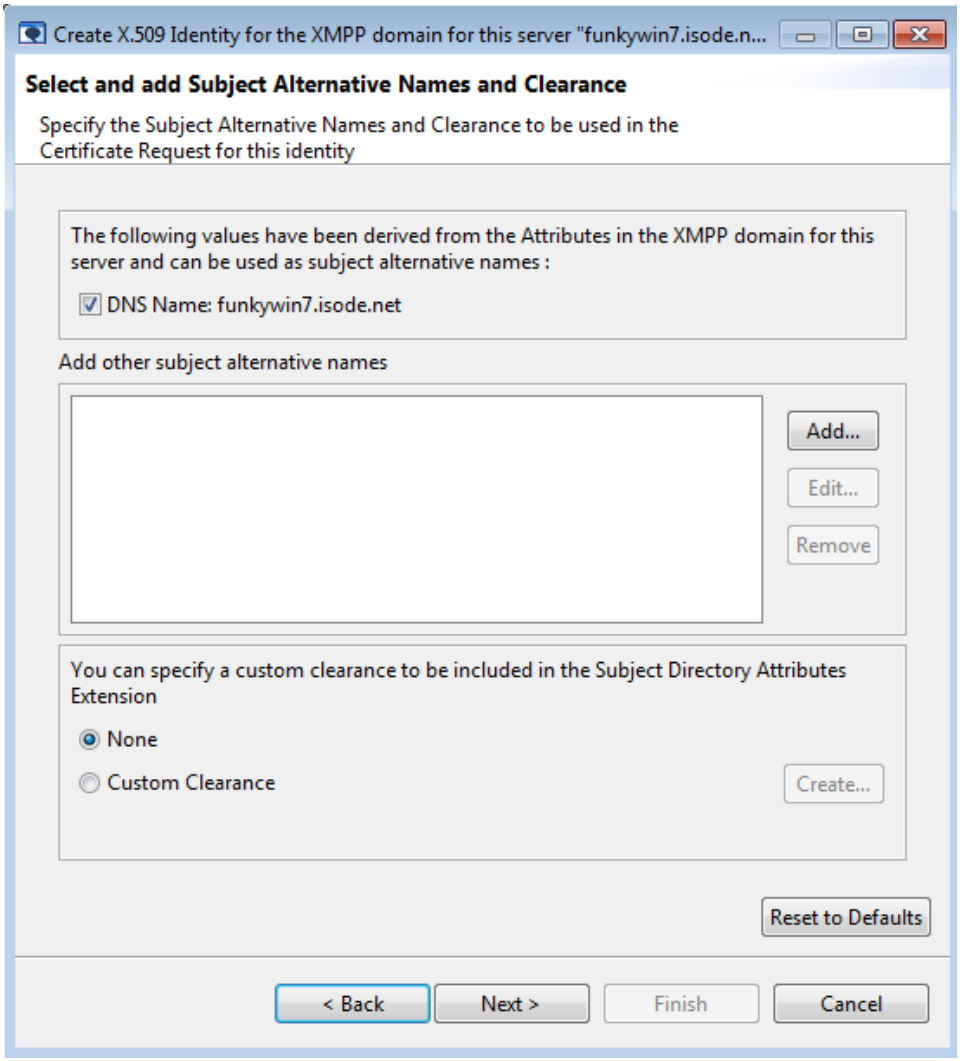
Clicking on the **Create...** button in the *Identity* tab will start a wizard which will take you through the process of creating an identity, by generating a private key and a *Certificate Signing Request* (CSR) which can be sent to a Certification Authority for signing:

Figure 5.4. Starting the identity wizard



The wizard provides default values for the key parameters and CSR subject name, using the domain of the M-Link Server. You can change the subject name to any distinguished name. Click **Next** to advance to the next wizard page:

Figure 5.5. Choosing subject alternative names and clearance values



The wizard will suggest a set of subject alternative name values to be included in the CSR, based on values that most clients will expect to see. You can choose not to include the suggested values (by unchecking the box next to any value) or you can add extra subject alternative names if required.

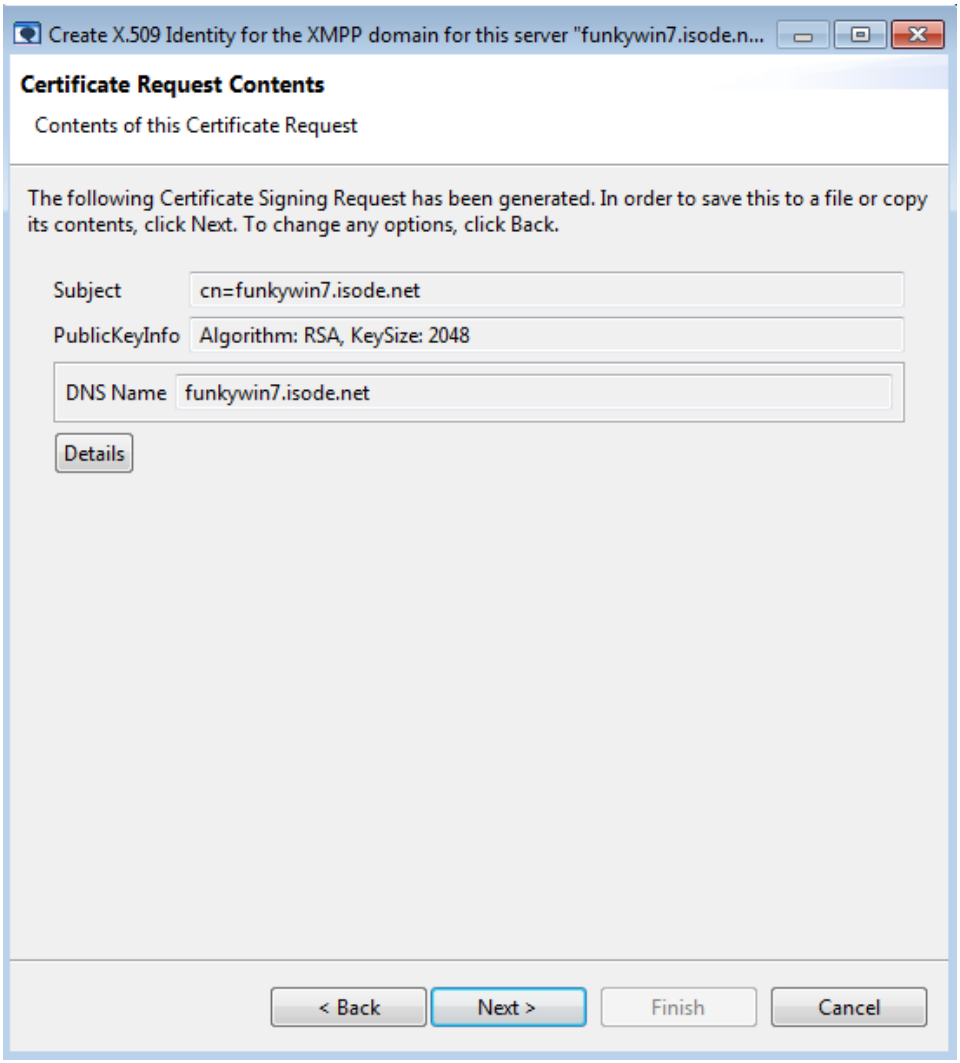
Note: The certificate should at least contain subject alternative name of type DNS Name, for each XMPP service domain (e.g., IM, MUC, pubsub, groups) for S2S TLS authentication to work for the domain.

You can also include a clearance value in the subject alternative name by clicking on the **Create** button. See Chapter 7, *Security Labels in XMPP* for more information on security clearances.

Note: Including subject alternative name and clearance values inside the CSR is no guarantee that they will appear in the certificate; the final contents of the certificate are determined by the policy of the issuing Certificate Authority.

Click **Next** to advance to the next wizard page:

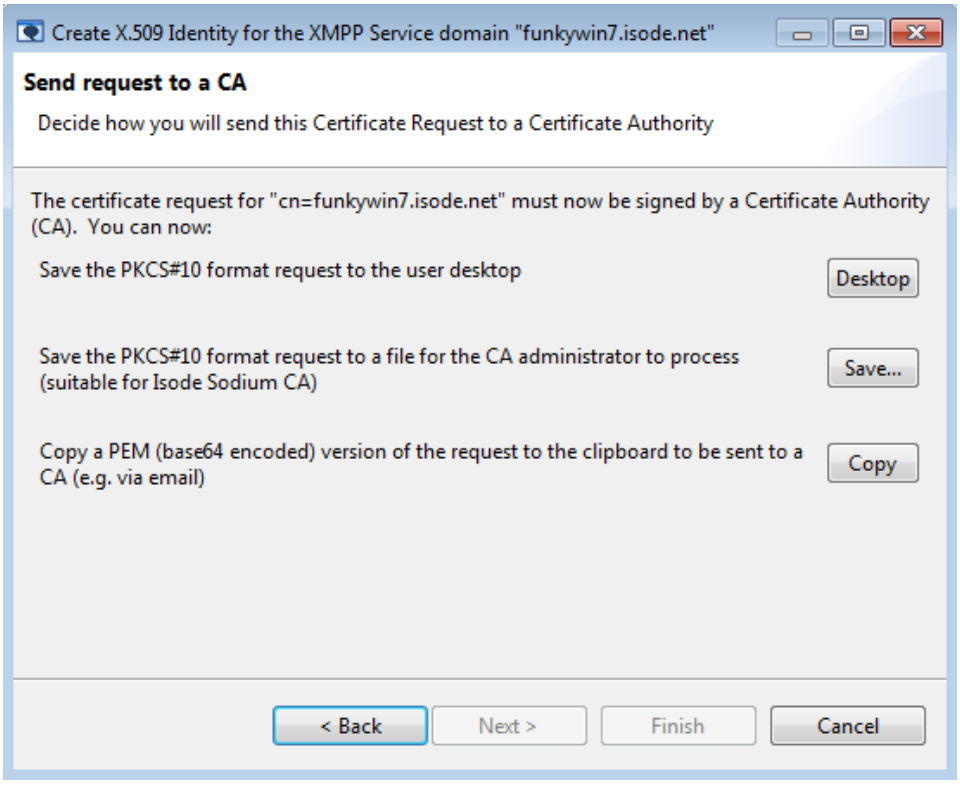
Figure 5.6. CSR summary



A summary is shown. If the details are correct, click **Next**.

The CSR now needs to be passed to a CA for signing:

Figure 5.7. How to contact the Certificate Authority

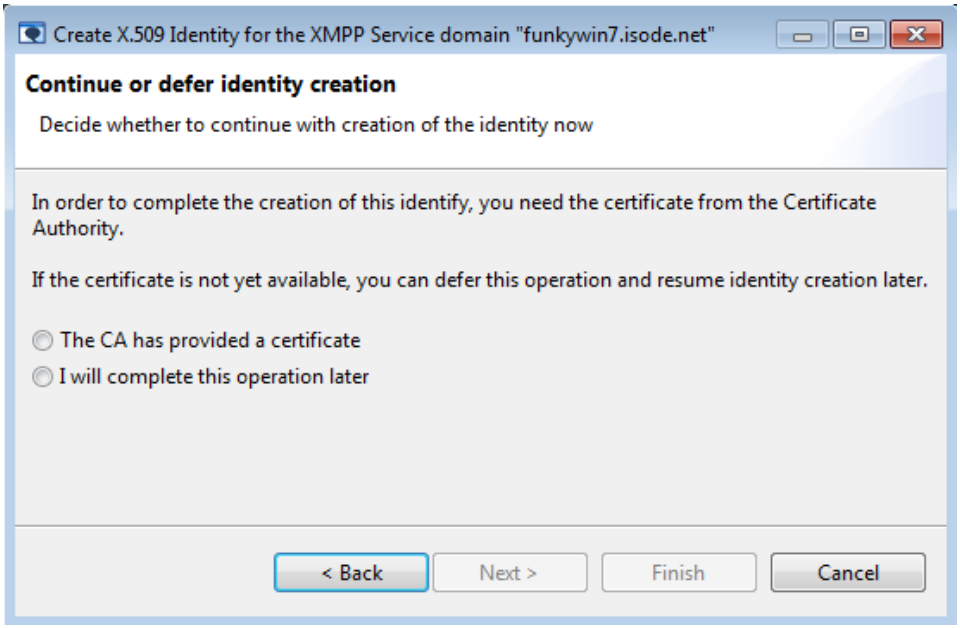


You have three options:

- (Windows only) Click **Desktop** to save the request as a file on your desktop, which can then be passed to a CA.
- Click **Save** to save the request as a PKCS#10 format file in a location of your choice. This is useful if you are using Sodium CA to issue certificates and have created a default location for the CA to collect CSRs and return certificates.
- Click **Copy** to copy the request to the clipboard. This can then be pasted into an email message.

Click **Next**.

Figure 5.8. Continue or defer identity creation



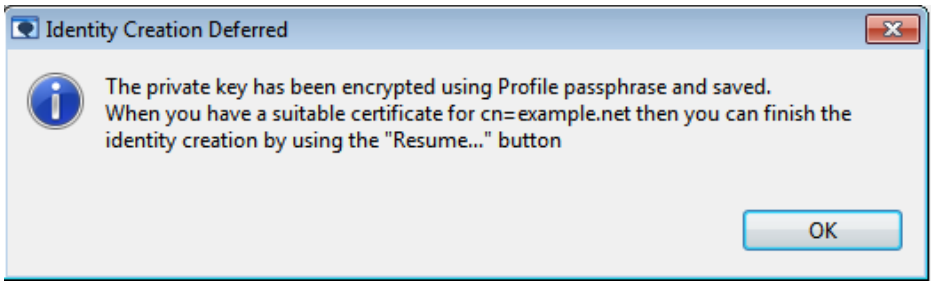
You now have two options:

- **The CA has provided a certificate**: choose this option if the CA is able to issue the certificate while you are waiting.

  Click **Next**. The wizard will continue as described in Section 5.4, “Completing identity creation”.
- **I will complete this operation later**: choose this option to save the information you have recorded as a *deferred identity*. Deferred identity information is protected by your profile passphrase and preserved between M-Link Console sessions.

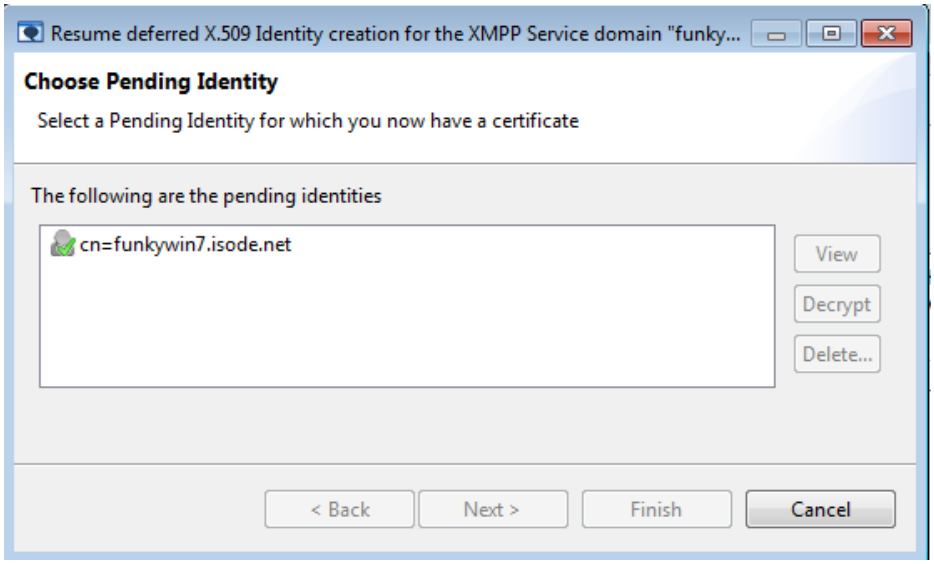
  Click **Finish** to close the wizard and complete the operation later. Click **OK** to acknowledge the message.

Figure 5.9. Deferring identity creation



Once the certificate has been supplied by the CA, you can use the **Resume...** button to carry on with TLS configuration:

Figure 5.10. Choosing a deferred identity creation

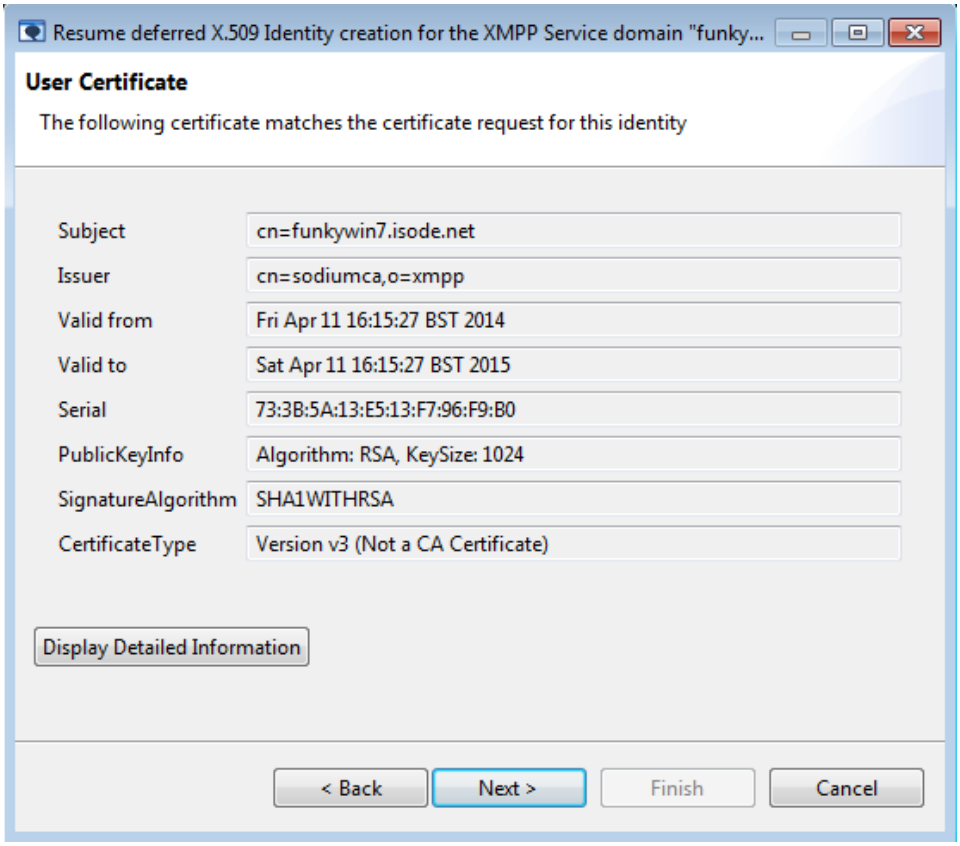


The wizard will attempt to locate, and then will display, the certificate issued by the CA (see Section 5.4, “Completing identity creation”).

5.4 Completing identity creation

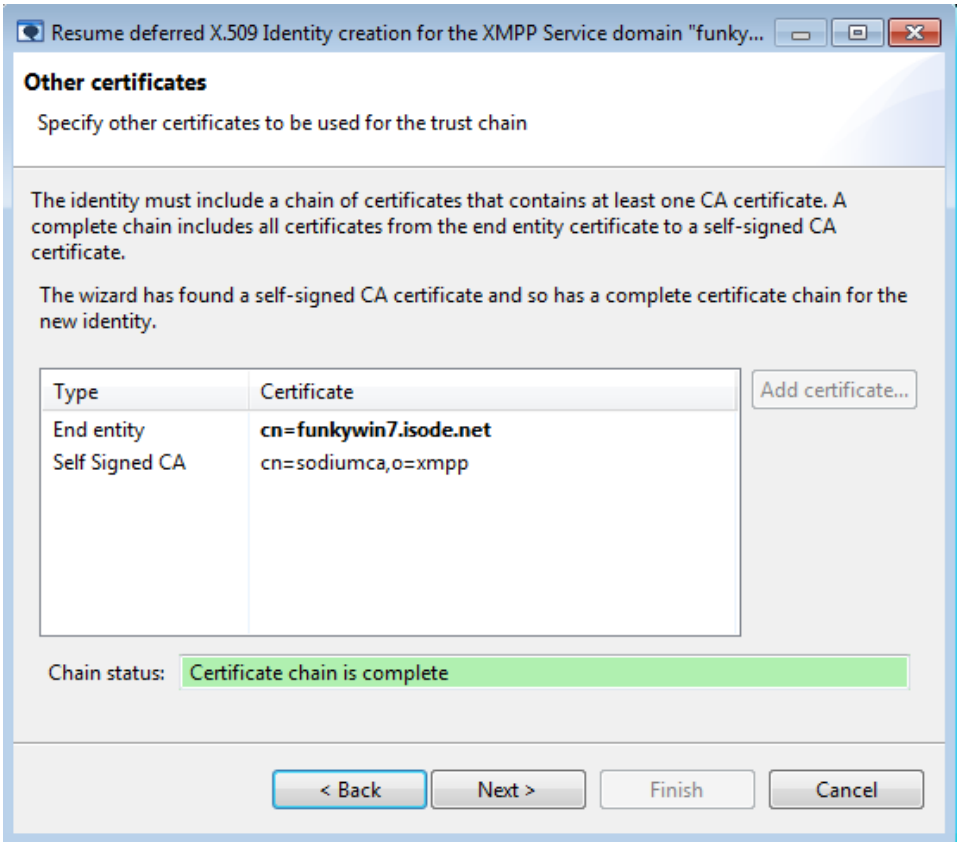
The wizard displays the certificate that has been issued by the CA:

Figure 5.11. M-Link Server's certificate



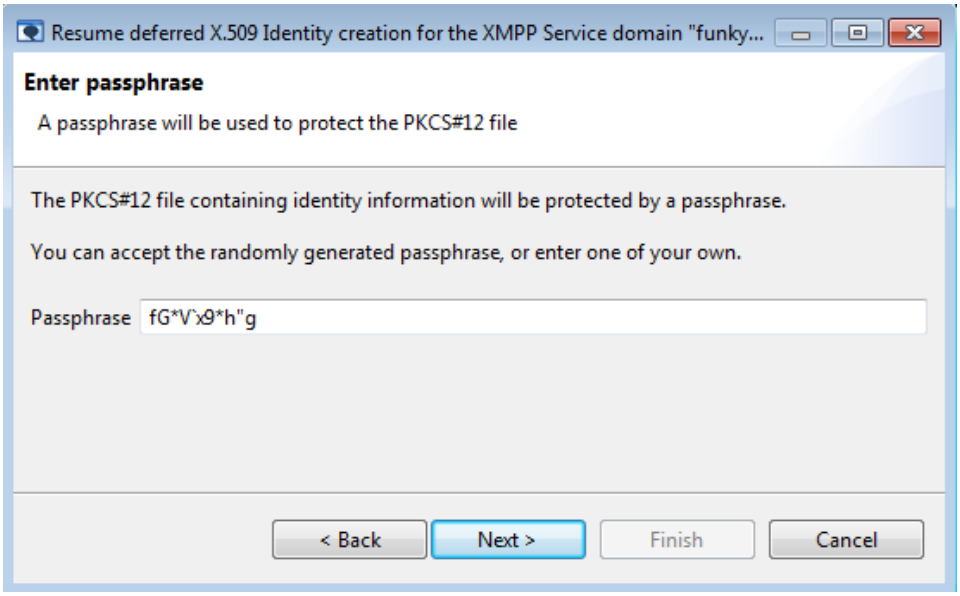
Click the **Next** button:

Figure 5.12. Certificate Trust Chain



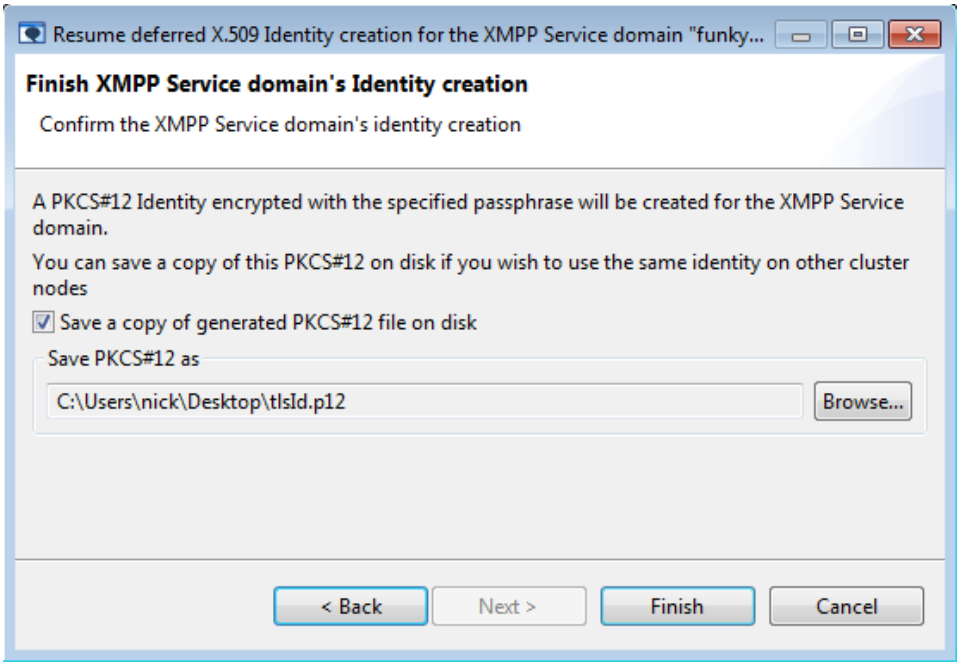
The wizard displays the trust chain for the certificate. Certificates in the trust chain are included in the identity. If the chain is incomplete, then you can add further certificates to it. Click **Next**:

Figure 5.13. Identity passphrase



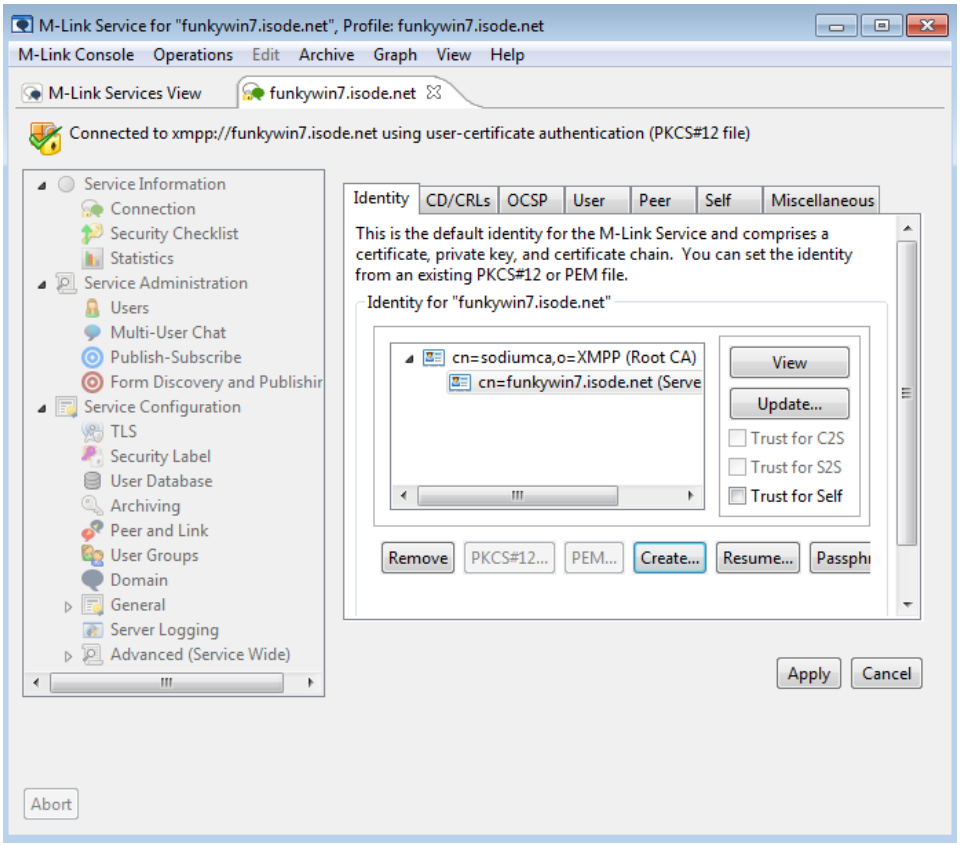
The wizard will create a new PKCS#12 file to contain the identity. Since the identity contains the server's private key, it will be encrypted. The wizard suggests a passphrase for this, you can accept the suggested value or provide your own passphrase. It is advisable to make a note of the passphrase, because it will be required if you use the same identity again (which may happen if you are configuring an M-Link cluster where all nodes share the same identity, (see Figure 14.4, “TLS configuration required when joining a cluster”)), or if you ever want to re-encrypt an existing server identity (for example, following a security breach). On clicking **Next** the following page will appear:

Figure 5.14. Finish creating the identity



The wizard prompts you to finish identity creation. Click on the **Finish** if you are ready to configure the identity, and the *TLS Identity* editor will be updated to show the server certificate:

Figure 5.15. Certificate ready to be used

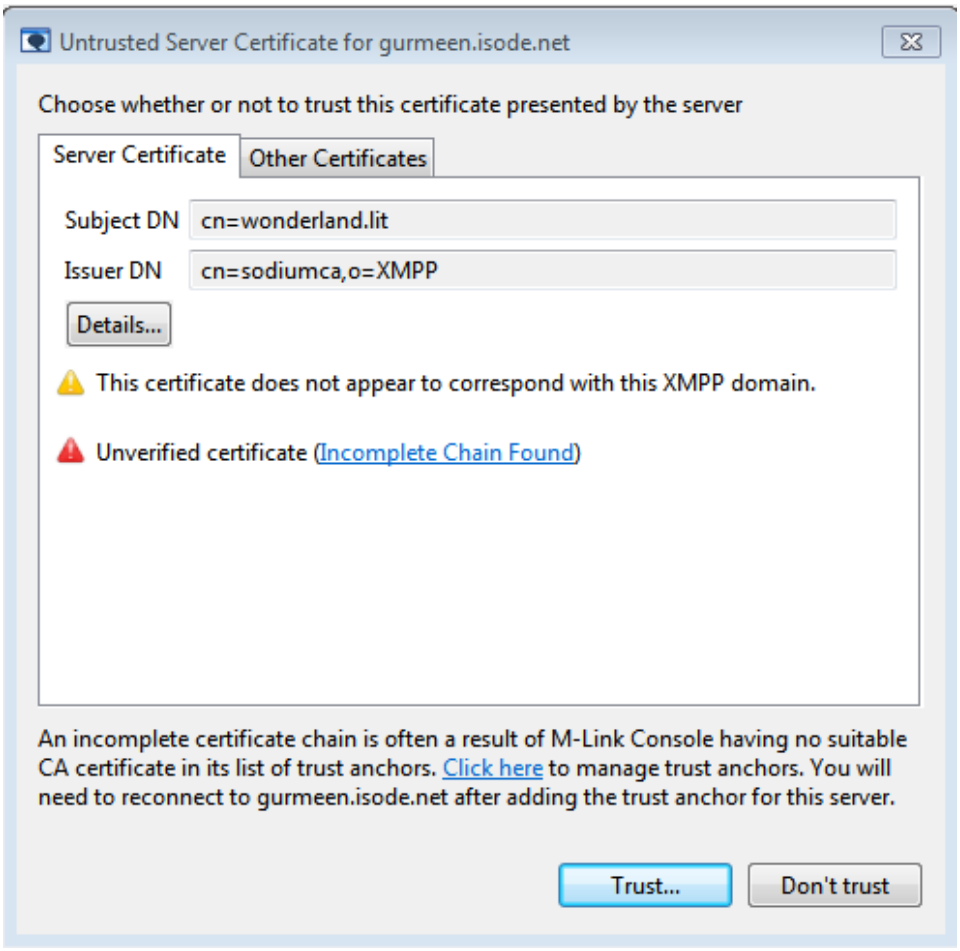


The editor shows that the server identity has been created, and that the certificate is ready, although it is not yet in use by the server. To tell the server to start using the new identity, click on the **Apply** button.

The new server identity will not be used until the server has been restarted. You can use **Operations → Stop all local M-Link Servers**, and then **Operations → Start local M-Link Server** in the *M-Link Services View* to do this.

Once the server has restarted, M-Link Console will re-connect to it. At this stage, you may see a warning dialog:

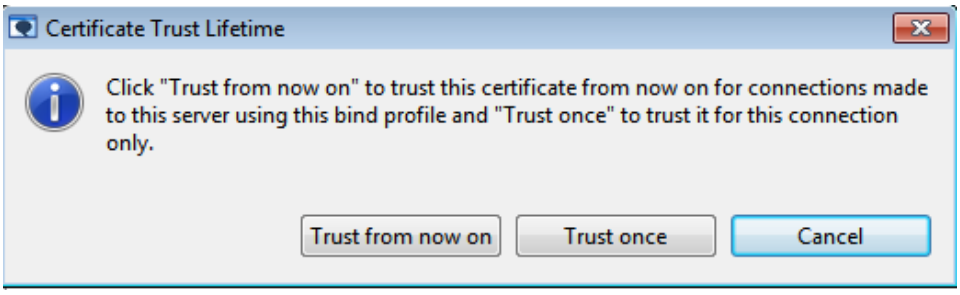
Figure 5.16. Untrusted Server Certificate Dialog



This warning indicates that the certificate used by the server is one that M-Link Console has not previously been told to trust. Assuming this certificate is the one that you have just configured, you can use the **Trust** button to tell M-Link Console to accept this certificate for this particular server.

Clicking the **Trust** button presents you with a choice of whether to trust this certificate only once or for lifetime of the profile.

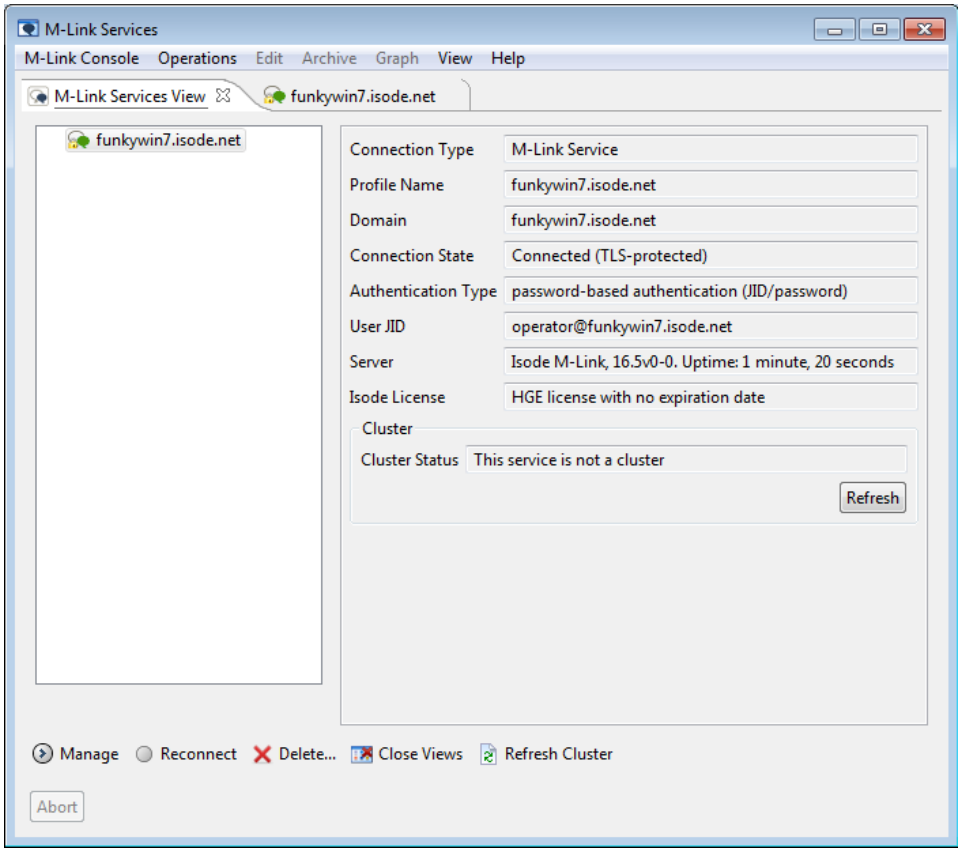
Figure 5.17. Certificate Trust Lifetime Dialog



You can also choose to use certificate verification by configuring the root CA certificate that issued this certificate chain using the **M-Link Console → Manage Trusted Certificates...** option (see Figure 2.34, “Configuring Trusted Certificates”).

Once TLS connection has been established, M-Link Console will show padlock icons and *Connection State* in the service view:

Figure 5.18. TLS connection established



Chapter 6 M-Link User Management

This chapter discusses provisioning of user, user authentication and authorization, and groups.

6.1 User Management

6.1.1 M-Link's use of a Directory to store user information

Information about each user of an M-Link service is stored in an LDAP Directory. Any user of the M-Link Service must have an entry inside the LDAP Directory, and the M-Link Server will use information from the Directory to perform authentication for any user that connects to M-Link.

A single M-Link service may be configured to host multiple IM domains. Each IM domain has its own set of users, and has separate LDAP configuration.

Configuration for each IM domain in an M-Link service therefore includes:

- How the M-Link Server connects to the LDAP Directory: where the LDAP Directory is, and what credentials the M-Link Server needs to use when connecting to it (including any TLS configuration)
- How the M-Link service maps user information in the directory into a JID that corresponds to the IM domain in question.

6.1.2 User Management and Provisioning

The M-Link service itself does not provide any functionality to add, remove, or modify user entries inside the user directory: such tasks are the responsibility of a user administrator who has suitable directory access.

The *Users* editor in M-Link Console displays information about users in a given IM domain. *Server* Administrators may view user information for any IM domain; *Domain* Administrators may only view user information for an IM domain if they are a member of the Domain Administrator group for that domain.

Information shown in the Users view is normally restricted to basic information returned by the M-Link service: it is possible to list users, search for users, and display basic information about the user (see Section 6.2.3, “Searching for and viewing existing users”).

When an Isode M-Vault directory is used to provision information for XMPP users, M-Link Console can access the Directory Server directly, which means that it can provide more detailed information about users, as well as being able to make changes to the user database such as creating, deleting and locking users etc.. User provisioning from M-Link Console is discussed in Section 6.2, “ User Provisioning in M-Link Console”.

When user information is kept in a Directory Server that is not managed by the administrator of the M-Link service (such as an Active Directory), then M-Link Console cannot be used to add, remove and modify users: these tasks will be accomplished by a suitable administrator using, e.g., the Active Directory toolset.

When using M-Link Console to create a new M-Link Server that uses an M-Vault directory server, then the wizard will set up appropriate configuration to allow M-Link Console to perform user provisioning, based on the responses given (see Section 2.7, “Create an M-Link Server” and Section 3.2.3, “User Directory configuration for IM domains”).

6.2 User Provisioning in M-Link Console

This section describes how M-Link Console can be used to provide user provisioning for an IM domain on an M-Link service

6.2.1 Overview

M-Link Console can be used to provide user provisioning for any IM domain for an M-Link service via the *Users* Editor. This editor is able to connect directly to the LDAP Directory used to provision users for the domain and allows the viewing and managing users on the service.

This editor can be used to Lock, Unlock, Delete and Restore users, as well as provide information about why a user may have been locked out from the service. In addition it can be used to add new users to the directory and purge old stale accounts from the directory completely. Finally it also provides facilities for removing redundant data from the service for users that have been deleted or purged.

6.2.2 Configuration

This section describes how to configure M-Link Console to provide user provisioning.

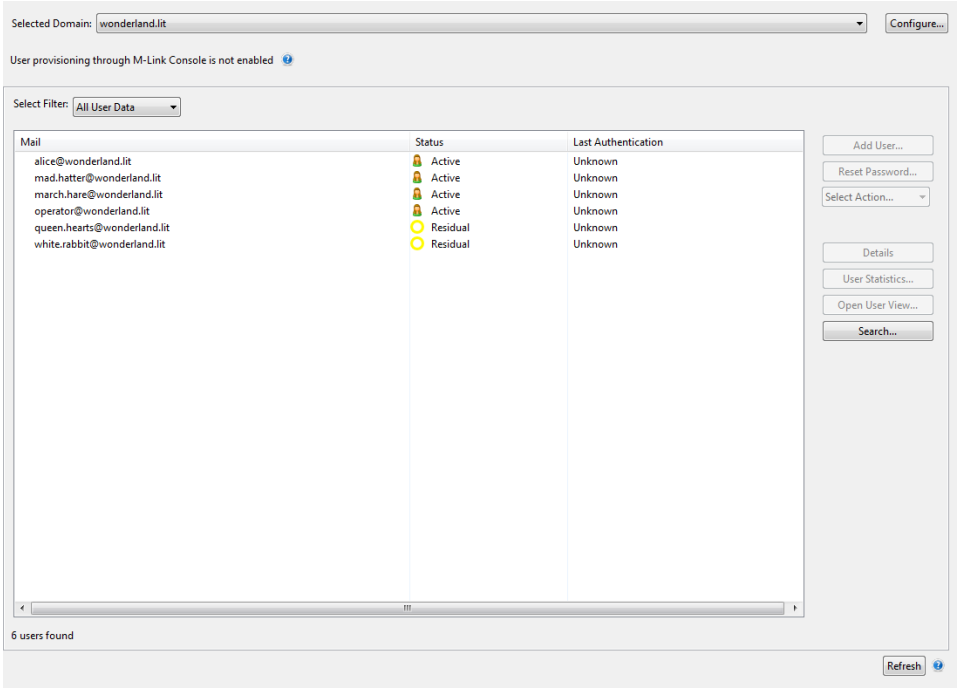
For M-Link Console to perform User Provisioning for an IM domain, it requires information about the directory including bind information, so it can connect to the directory, and topological information about the directory (namely, the location of entries representing active and deleted users). This information is a superset of the configuration used by the M-Link Server itself when it is reading user information.

When a new M-Link service is created via the wizard (see Section 2.7, “Create an M-Link Server”), then for a configuration using M-Vault, M-Link Console will automatically configure this information in the bind profile for the initial IM domain of the service.

M-Link Console provides the ability to add or modify user provisioning configuration for an existing IM domain. This is useful for users who are IM domain administrators (that is, they have management responsibility for one or more IM domains, but are not members of the Server Administrators group).

To view or modify LDAP user provisioning configuration for M-Link Console open the *Users* editor.

Figure 6.1. Users editor with no directory configuration

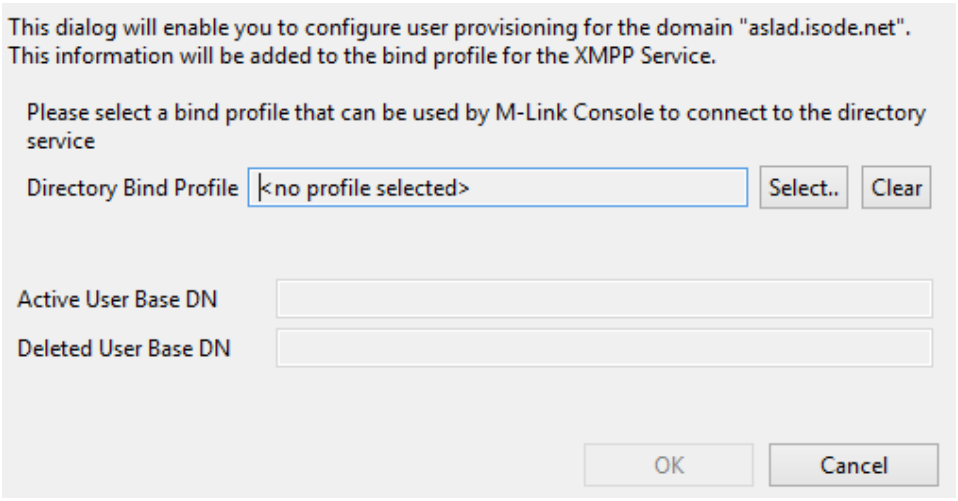


The Users editor shows information for the selected IM domain. If no directory configuration has been specified, then the contents of the view are obtained from the M-Link service and provides:

- A list of currently active users (either a complete list or one based on a search filter)
- A list of users which are no longer active but for which the M-Link service still has residual data (see Section 6.2.3, “Searching for and viewing existing users”)
- The ability to find more detailed user information, including roster information for any active user
- A count of the number of users who match the currently selected filter. This can be used to work out the total number of active users or the number of users for which residual data exists.

To add or modify directory configuration, use the **Configure...** button:

Figure 6.2. Configure User Provisioning Dialog

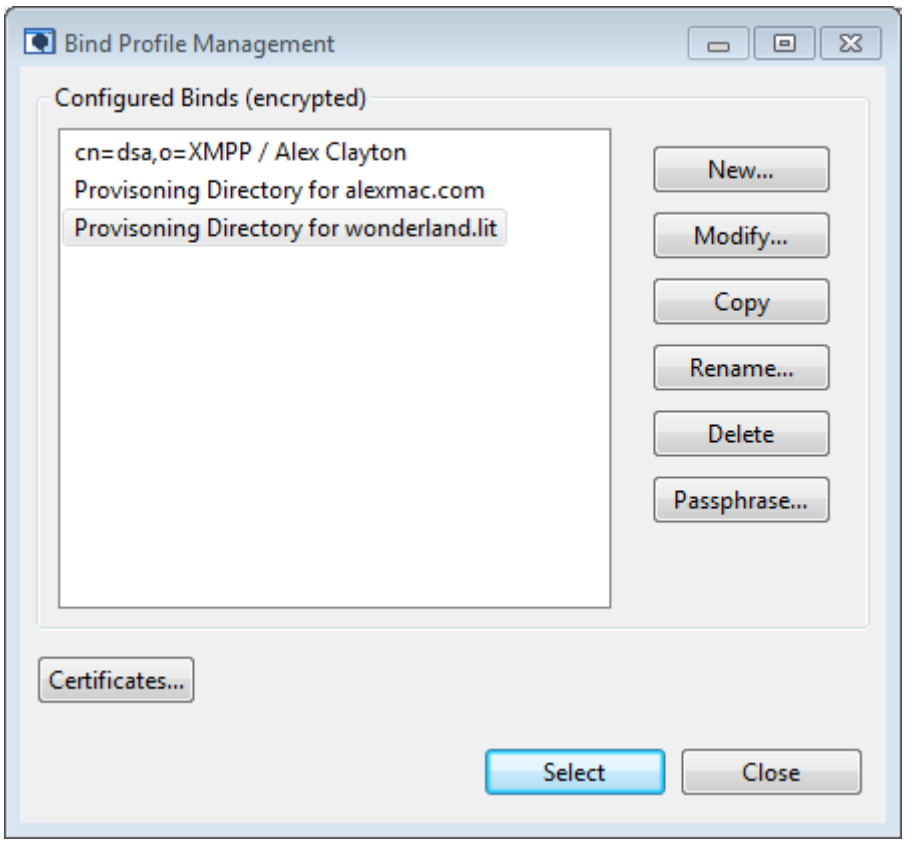


The dialog will require the following fields to be filled in:

- **Directory Bind Profile**
- **Active User Base DN**
- **Deleted User Base DN**

The **Directory Bind Profile** specifies the bind profile M-Link Console will use to bind to the LDAP directory. Press **Select** to bring up the **Bind Profile Management** dialog which will allow the selection of the bind profile to use.

Figure 6.3. Bind Profile Management Dialog

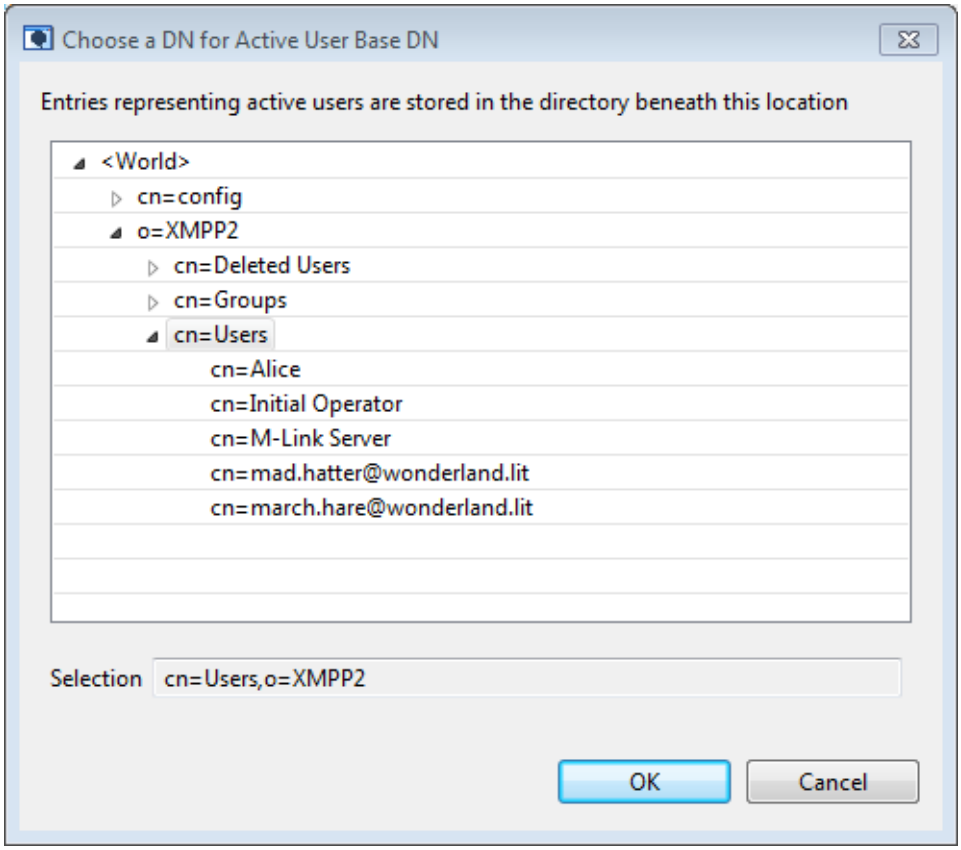


This bind profile should be capable of binding to the directory with sufficient access to be able to read and write from the *Active* and *Deleted* user trees.

Once Selected M-Link Console will attempt to use the profile to bind to the directory and warn if this is not possible.

If a bind is successful **Pick** buttons will become visible next to the **Active User Base DN** and **Deleted User Base DN** fields. Selecting these will bring up a **DN Selection Dialog**.

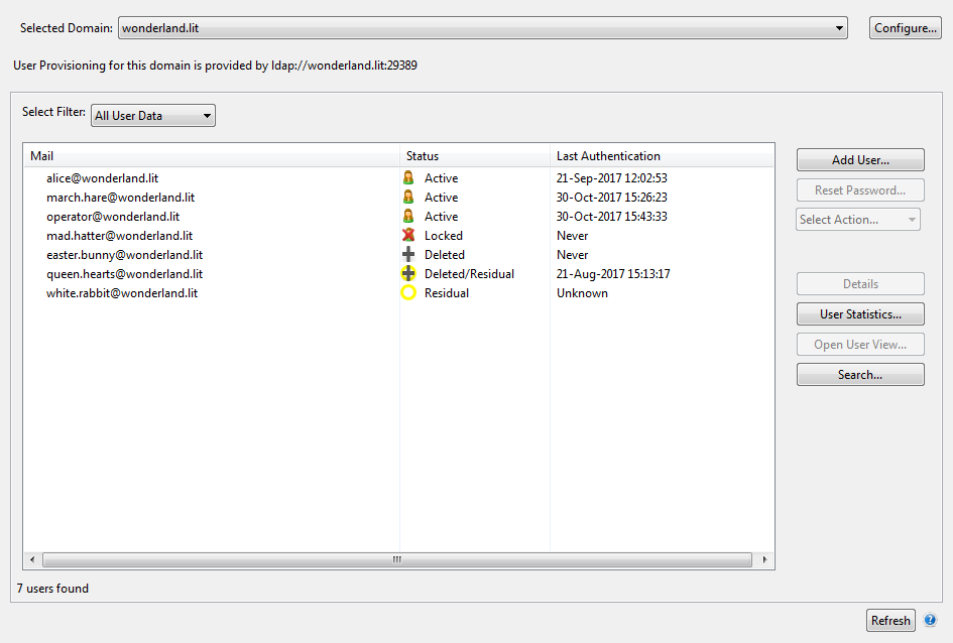
Figure 6.4. DN Selection Dialog



For each of the fields select the appropriate DN in the directory, that is, for the **Active user Base DN** select the location below which user entries will be stored, and for the **Deleted User Base DN** select the location beneath which entries for *Deleted Users* will be stored.

Once all details are entered either press **OK** in the **Configure User Provisioning** dialog or **Finished** in the **Connection Details** dialog to confirm the changes. These will now be written to the M-Link Console bind profile for the service and M-Link Console will now be able to access the directory for user provisioning, and the Users editor window will reflect the information from the directory:

Figure 6.5. Users editor with directory configuration



6.2.3 Searching for and viewing existing users

When directory configuration has been specified, the table listing users provides the following information:

Mail
: This contains the JID of the user on the service.

Status
: This represents the status of a user, which can be either:

- an *Active* user entry is one that is in appears beneath the designated *Users* subtree in the directory, and will be visible to the M-Link service which means that the user will be able to authenticate to this IM domain.

  For cases where M-Link Console is not configured to connect to the provisioning directory, *active* users will include all users that the M-Link server has knowledge of. Depending on the how the provisioning directory is configured, this may mean that the list includes users who would be prevented from authenticating (e.g. if the directory regards the user account as *expired*, it may still appear as an *active* user so far as the M-Link service is concerned).
- a *Locked* user entry appears beneath the *Users* subtree, but is locked (either as a result of password policy or because the administrator has manually locked the account). Such users are visible to the M-Link service but will be prevented from logging in to the service when they try and authenticate.

  Extra information about why a user is locked is available with the **Details** button (see Section 6.2.6, “Viewing details for a user”).
- a *Deleted* user entry appears beneath the *Deleted Users* subtree in the directory, and as such will not be visible to the M-Link service. Such users will not be able to log in to the M-Link service
- *Residual* entries appear when a user is not visible to the M-Link service but where the M-Link service can see roster information relating to that user. The most likely situation where this will occur is when an active user is deleted, leaving their roster behind (or where other users still refer to the deleted user in their roster)

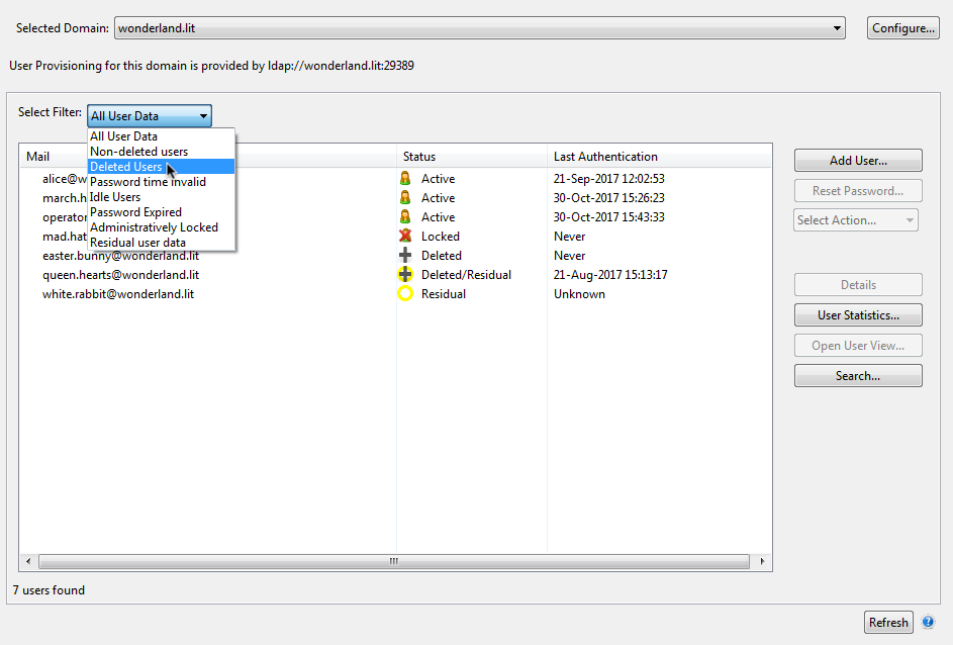
Last Authentication
: This displays the time the user last authenticated to the user directory, which (unless the directory is being used to provision other services) will also be the time that the

user last authenticated successfully to the M-Link service. This requires the User Directory to have been configured to store Authentication Timestamps.

Clicking on the column headers will sort the entries by that column.

The list of users shown can be filtered by selecting from the **Select Filter** combo box.

Figure 6.6. Select Filter



This will reduce the users shown in the list to only those that match the given filters. The available filters are:

All Users
: Displays all users.

Non-deleted user
: Displays all users who are visible to the server i.e. the *Active* and *Locked* users.

Deleted Users
: Displays all *Deleted Users*, i.e. users under the deleted users node in the directory.

Password time invalid
: Users whose passwords are out of the validity period according to their entry in the directory.

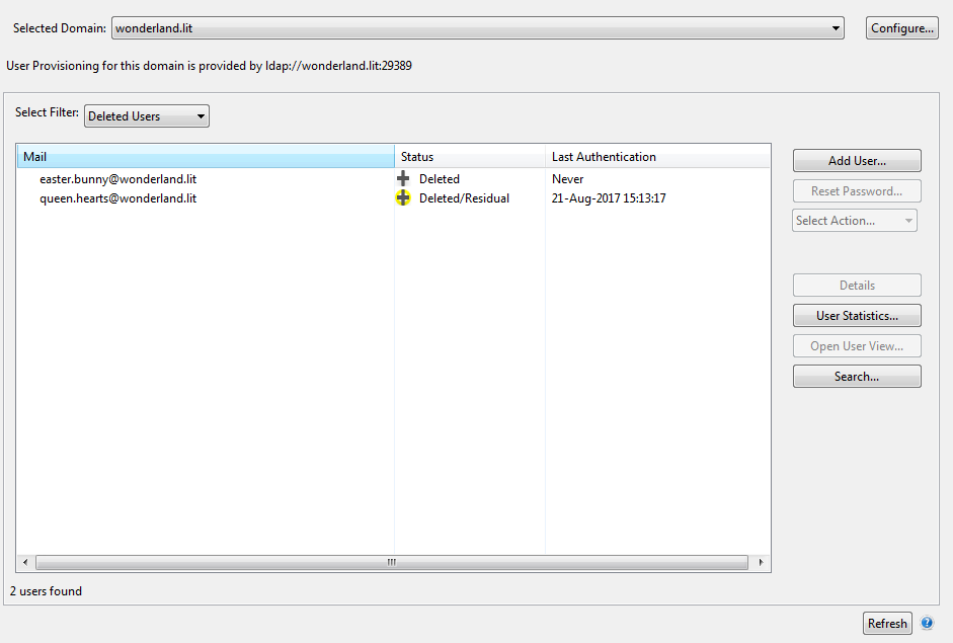
Idle Users
: Users whose password has become idle according to the directory's password policy.

Password Expired
: Users who password has expired according to the password policy.

Administratively Locked
: Users who have been manually locked by an administer.

Residual user data
: Deleted or Purged users who still have residual data on the M-Link Service.

Figure 6.7. Using a Filter



Note some of these will not be applicable depending on whether a password policy is set and how it is configured for the directory.

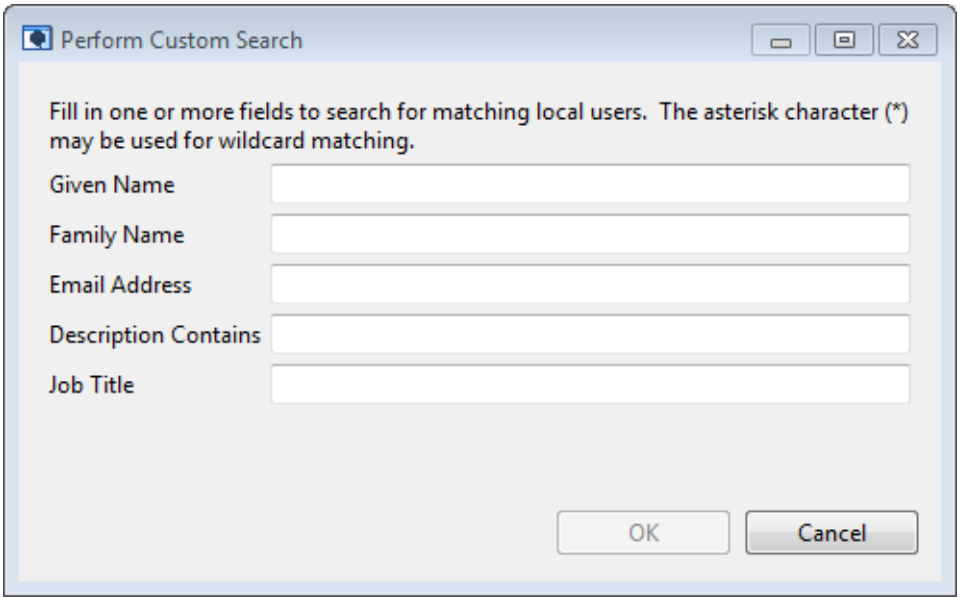
A new search can be performed at any time be pressing the refresh button.

6.2.4 Custom user search

In addition to the standard filters described above a custom search may be performed for the users on the service. This consists of string matching against fields provided by either the M-Link service or LDAP directory. This search may be performed regardless of whether directory information is configured for the domain.

To perform a custom search select the **Search…** button which will bring up the **Perform Custom Search** dialog.

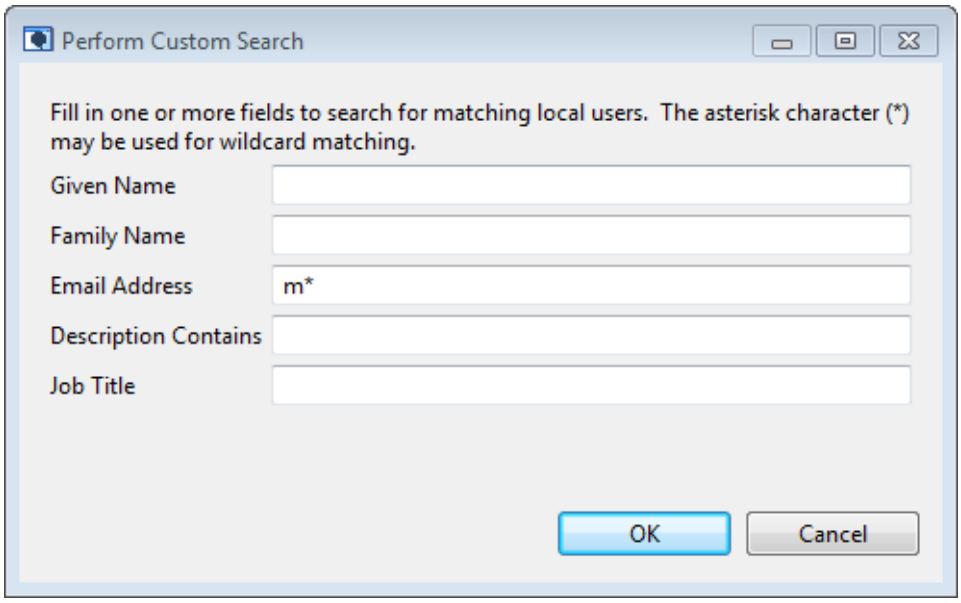
Figure 6.8. Perform Custom Search dialog



The fields in the dialog are **Given Name**, **Family Name**, **Email Address**, **Description contains** and **Job Title**, representing corresponding fields for the users' entries in the directory. Each field can be filled in with a string to match against, with * used for wild card matching.

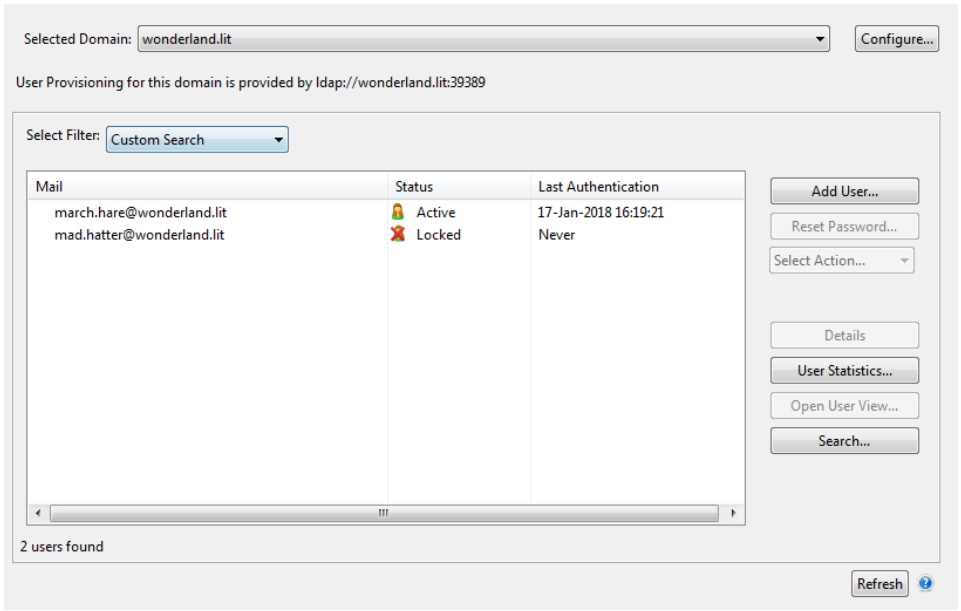
The fields **Given Name**, **Family Name**, **Email Address**, and **Job Title** are matched using exact matches, i.e. the search string has to match exactly; the **Description Contains** field, as the name implies, the match is made if the description contains the given string. Any fields left blank will not be searched against.

Figure 6.9. Search to find all users whose email begins with m



To run the search enter the required fields and select 'OK'. M-Link Console will then perform the search and the results will be displayed in the list. The **Select Filter** combo will have its text changed **Custom Search** to indicate that it is displaying the results of a custom search.

Figure 6.10. Results from a Custom Search

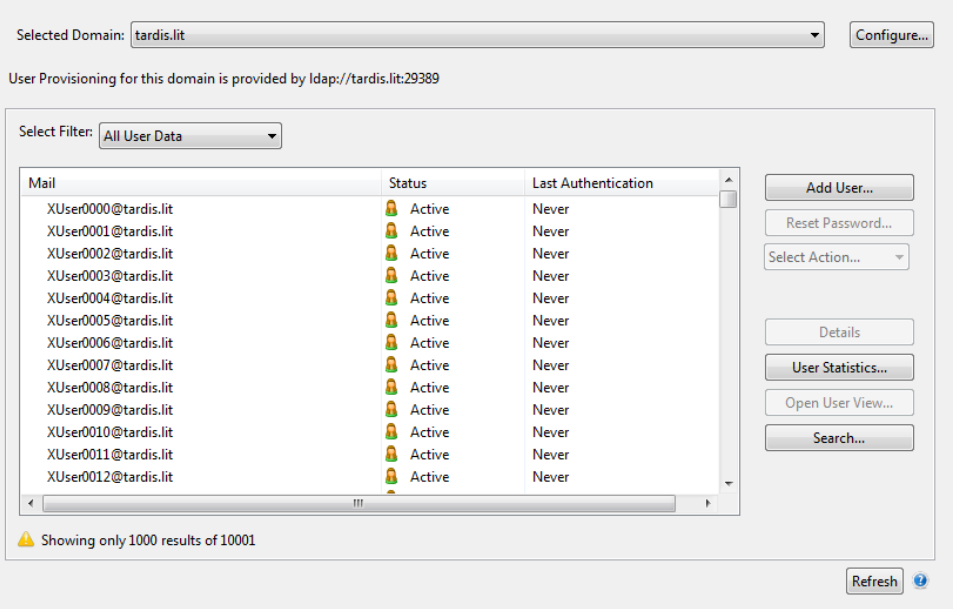


To clear the search results any other filter from the **Select Filter** combo box.

6.2.5 Dealing with large numbers of users

M-Link Console imposes a limit of 1000 users to display in the user list at any one time; if the result set is ever more then this then only 1000 users will be shown and the user count message will be updated to demonstrate that not all the results have been displayed.

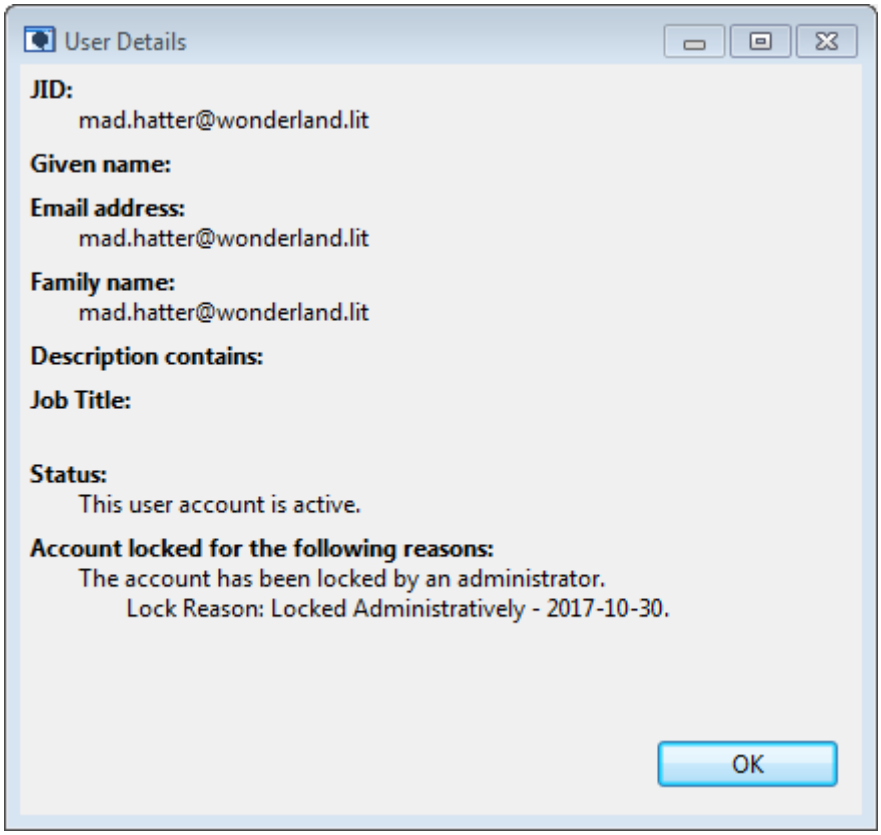
Figure 6.11. User List when over 1000 entries available



6.2.6 Viewing details for a user

More details can be seen for a user by either double clicking them, or selecting them and then pressing the **Details** button found to the right of the table. This brings up a **User Details** dialog for the user.

Figure 6.12. User Details Dialog

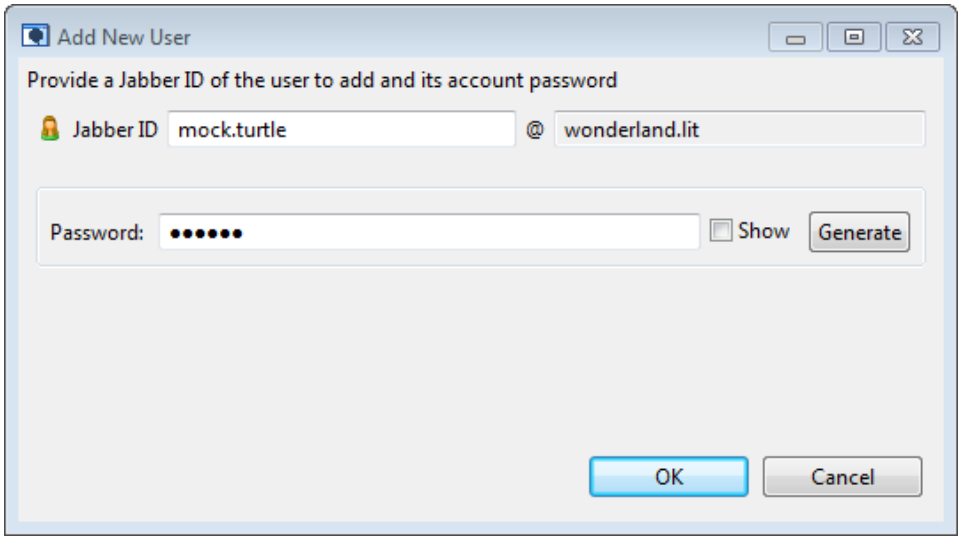


This contains information on the user's JID and Status. If they are locked it will give the list of all reasons the account was locked; if the M-Link service has residual data for the user, that will be reported here.

6.2.7 Adding a new user

New users can be added to the directory by selecting the **Add User...** button found to the right of the table. This will bring up the **Add New User** dialog.

Figure 6.13. Add New User Dialog

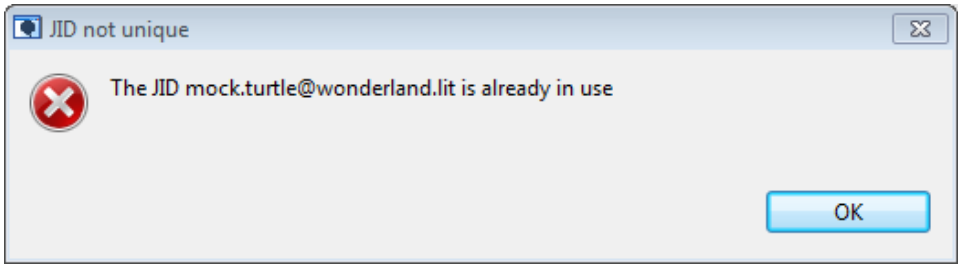


Enter the required JID for the new user in the **Jabber ID** field. The domain part of the JID will be set to the current IM domain.

An initial Password for the user should be entered into the password field. If needed a random one can be generated via the **Generate** button.

Once a valid JID and password are entered click **OK** to complete the dialog. M-Link Console will check that the user (either active or deleted) with the given JID does not already exist. An error message will be displayed if it already exists and return you to the **Add New User** dialog.

Figure 6.14. User Exists Error Message

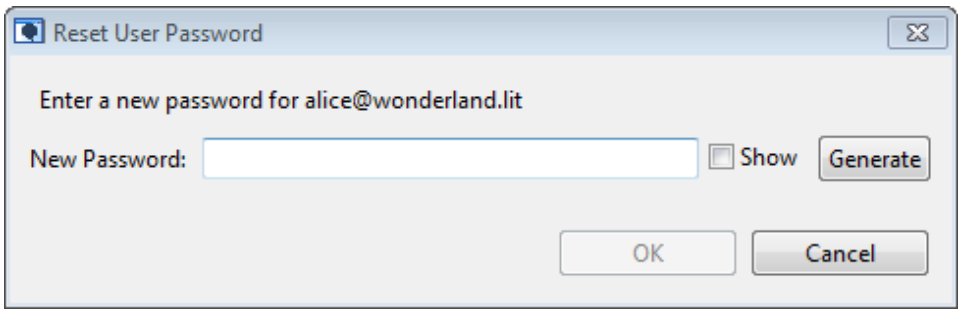


If there is no existing user with that name then M-Link Console will create a new user in the directory. A new search will then be performed and the new user will appear in the user list.

6.2.8 Reset a users Password

The password of a selected user can be changed by selecting the **Reset Password** Button found to the right of the table. This opens the **Reset User Password** dialog.

Figure 6.15. Reset User Password Dialog

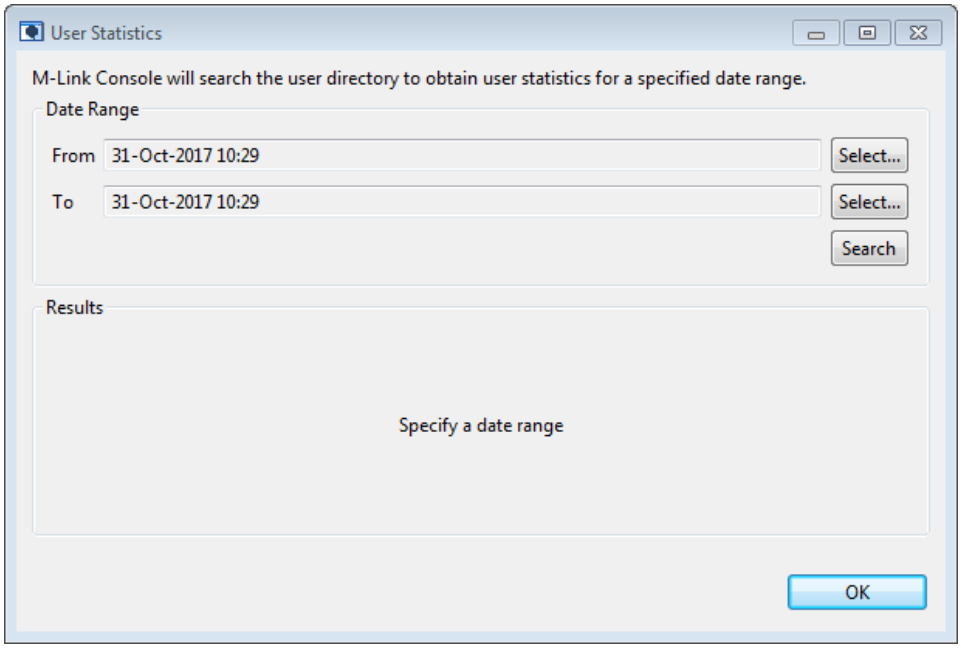


Enter a new password for the user in **New Password**. A random password can be generated by clicking on the **Generate** button, setting the **Show** check box will make the password visible. On selecting **OK** M-Link Console will write the updated password value to the directory before performing a new search.

6.2.9 User Statistics

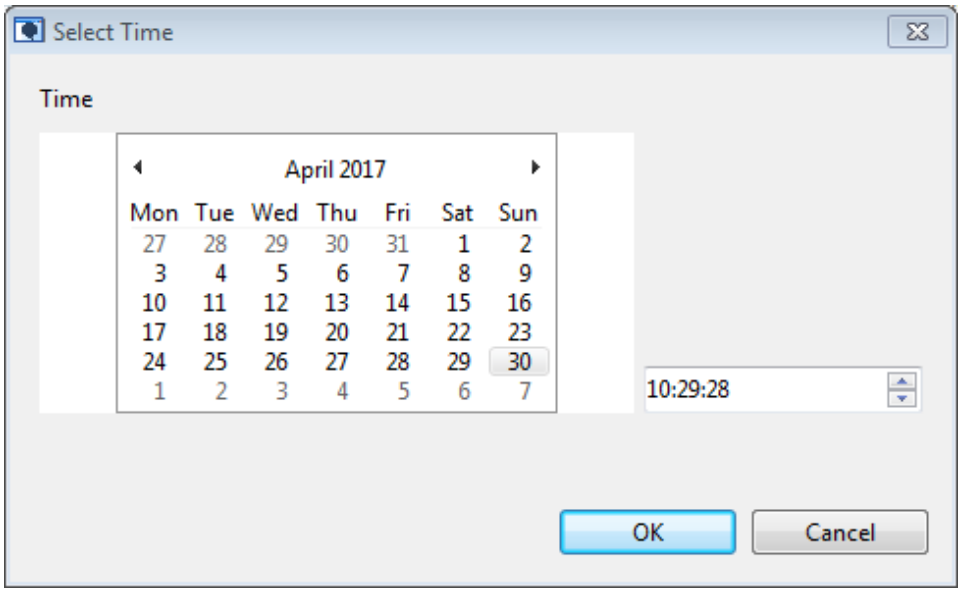
M-Link Console is able to provide information on the number of user accounts created and deleted in a given date range. This is done by doing a search for accounts created or deleted on the directory server, so it only available if user provisioning information is set for the domain. To access the feature select the **User Statistics...** button, this will open the *User Statistics* dialog.

Figure 6.16. *User Statistics* dialog



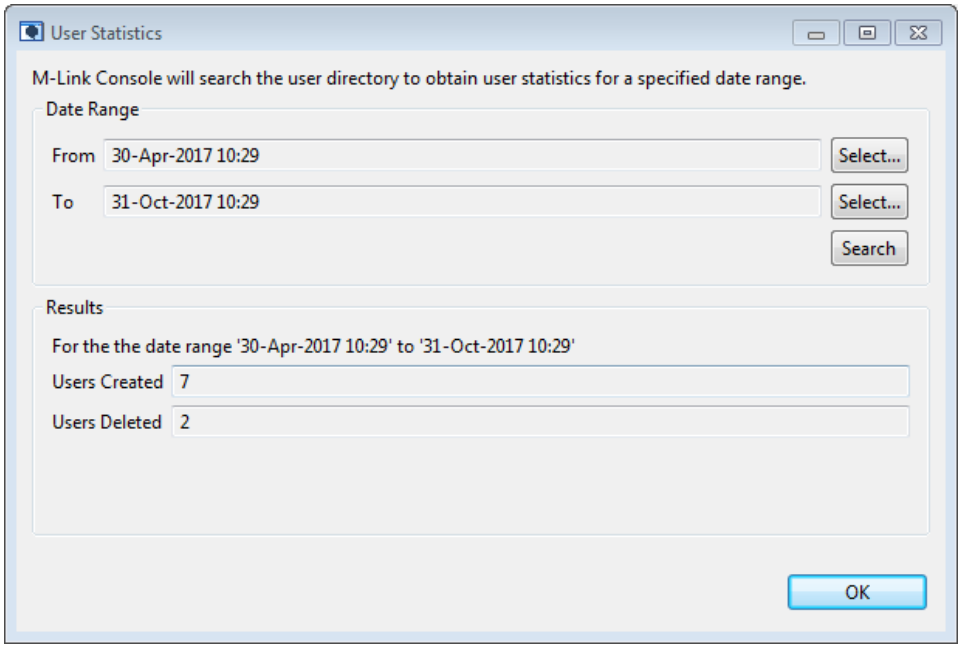
In the dialog the **Date Range** for which the statistics should be retrieved needs to be set. This can be done by modifying the **From** and **To** by selecting the **Select..** button for either to bring up the *Select Time* dialog.

Figure 6.17. *Select Time* dialog



Once the desired **Date Range** is set the **Search** buttons should be selected to send the request to get the statistics. When this returns the results will be displayed in the bottom half of the dialog.

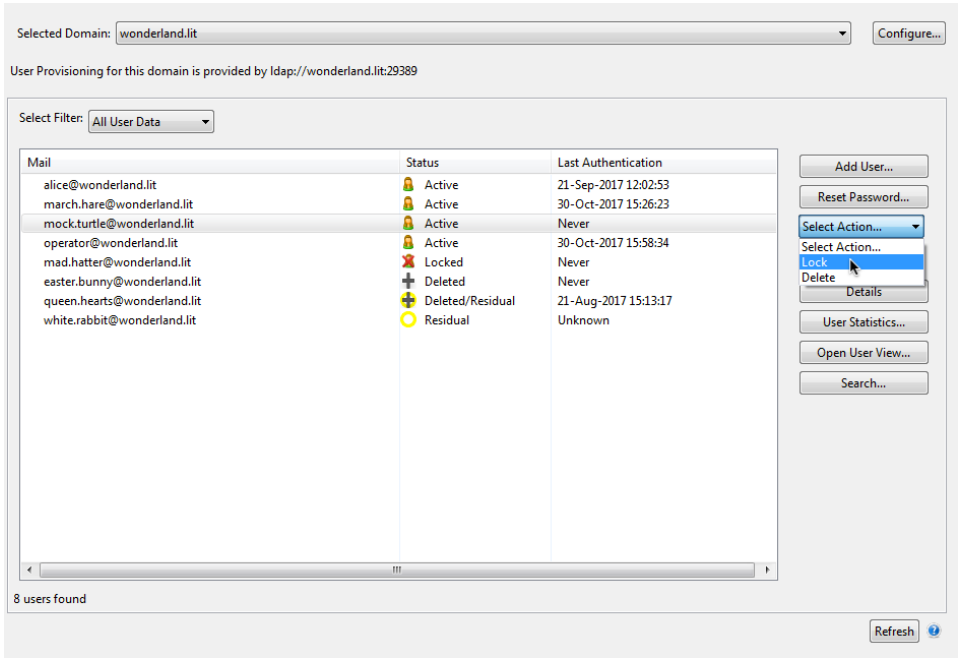
Figure 6.18. Results being shown in the *User Statistics* dialog



6.2.10 Other Actions

The remaining actions: Lock, Unlock, Delete, Restore, Purge and Cleanup are accessed via the **Select Action...** drop-down button:

Figure 6.19. Select An Action



Once the action is finished a new search will performed to get any updates that occurred to the user list as the result of the action.

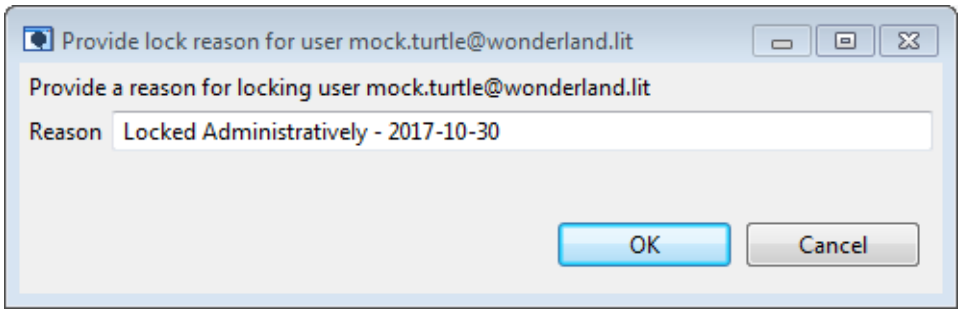
The **Select Action...** button is context aware and will only show actions valid for the current selection, which may be a single or multiple selected users, though an action can only be performed on a selection of users if it is valid for all users in a selection.

The remainder of this section details each of these actions in brief.

6.2.10.1 Lock

This adds an administrative lock to the user(s) account to prevent them from logging into the service and directory. When selected a **Provide Lock Reason** dialog will be presented.

Figure 6.20. Provide Lock Reason Dialog



A reason for locking the user(s) can be added here that will be stored in the directory.

6.2.10.2 Unlock

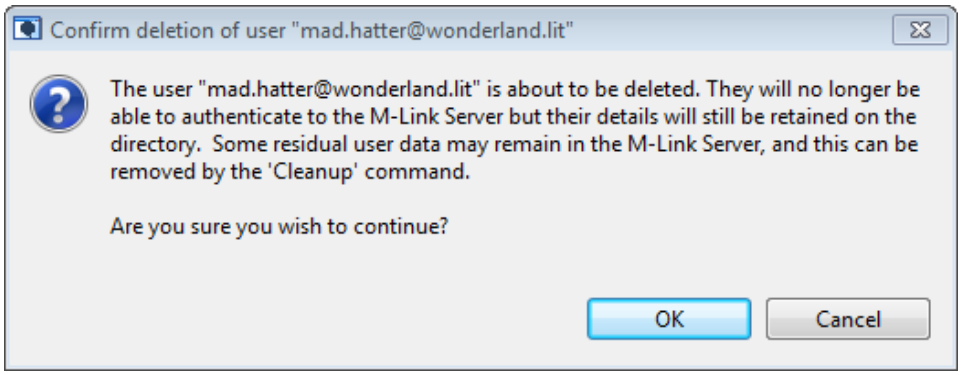
This removes an Administrative Lock (see Section 6.2.10.1, “Lock”) from the selected user(s).

6.2.10.3 Delete

This deletes the selected user(s) by moving them from the *Active User* tree in the directory to the *Deleted User* tree. Although the users have been removed from the perspective of the M-Link Server, information about them will still exist in the directory (and M-Link Console will prevent you creating a new user with the same JID).

When selected a confirm dialog will be shown to confirm that the user(s) should be deleted.

Figure 6.21. Confirm Delete Dialog



6.2.10.4 Purge

When a user is deleted their information is still retained in the directory, this information can be removed from the directory by selecting the Purge action. This will Purge all entries for the selected user(s) from the directory, no more information will exist for them on the directory though some may still exist on the M-Link Server (see Section Cleanup). Once purged the user data is irrecoverable.

When selected a confirm dialog will be shown to confirm that the user(s) should be purged.

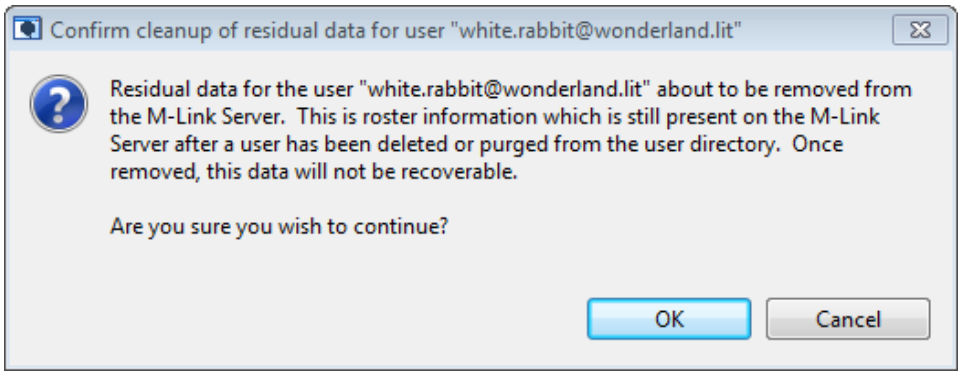
Figure 6.22. Confirm Purge Dialog

6.2.10.5 Cleanup

If a user is Deleted or Purged some residual data may still exist for them on the M-Link Server. This may be stuff such as XMPP roster information for the user. If this is the case then the user list table will describe the user as having an *Residual* or *Deleted/Residual* status. This residual data can be removed from the Server by performing a Cleanup operation. Note that this action is irreversible and once deleted the data can not be restored.

When selected a confirm dialog will be shown to confirm that the users data should be cleaned up.

Figure 6.23. Confirm Clean Up Dialog



6.3 Windows Single Sign-On Configuration

This section describes how to integrate an M-Link Server with Active Directory in support of Windows Integrated Single Sign-On.

Windows Integrated Single Sign-On (Windows SSO) allows as user, once signed into Windows system joined to an Active Directory (AD) domain, to access any resource in the network that is integrated an AD service for that domain. This integration utilizes *Kerberos V5* technology.

M-Link Server supports the *Simple Authentication and Security Layer* Kerberos V5 ("*GSSAPI*") authentication mechanism which can be used to support Windows Integrated Single Sign-On. This Windows Integrated Single Sign-On support relies on the M-Link Server being deployed on a Windows host system that has joined an AD domain. It also requires that M-Link is configured to get user information from Active Directory.

6.3.1 SPN and AD Domain Naming

Services that can be used for Windows SSO are identified by an Service Principal Name (SPN). XMPP Server SPNs are of the form `xmpp/`*`im-domain`* where *`im-domain`* is the instant messaging domain of an XMPP service, for example `xmpp/example.com`. It is anticipated that this convention will be standardized for XMPP.

In order to enable SSO for a given IM domain, the SPN needs to be correctly set for the IM domain. Once this is done, M-Link will offer SSO for that domain. If multiple IM domains are configured in M-Link, SPNs need to be set for each IM domain for which SSO is desired.

It is recommended that IM domains are chosen to be either the same as the AD domain on which M-Link is running or as a subdomain. While this is not required, it will facilitate SSO where the XMPP client is running on a different AD domain, as it enables the client to discover the AD domain supporting the desired M-Link server. For example, with an AD Domain `example.com` a likely IM domain is `example.com` with SPN `xmpp/example.com`. Another possible IM domain for this AD domain is `xmpp.example.com` with SPN `xmpp/xmpp.example.com`.

6.3.2 M-Link Server Account

To support Windows SSO, an M-Link Server must be hosted on a Windows system that has joined an Active Directory domain.

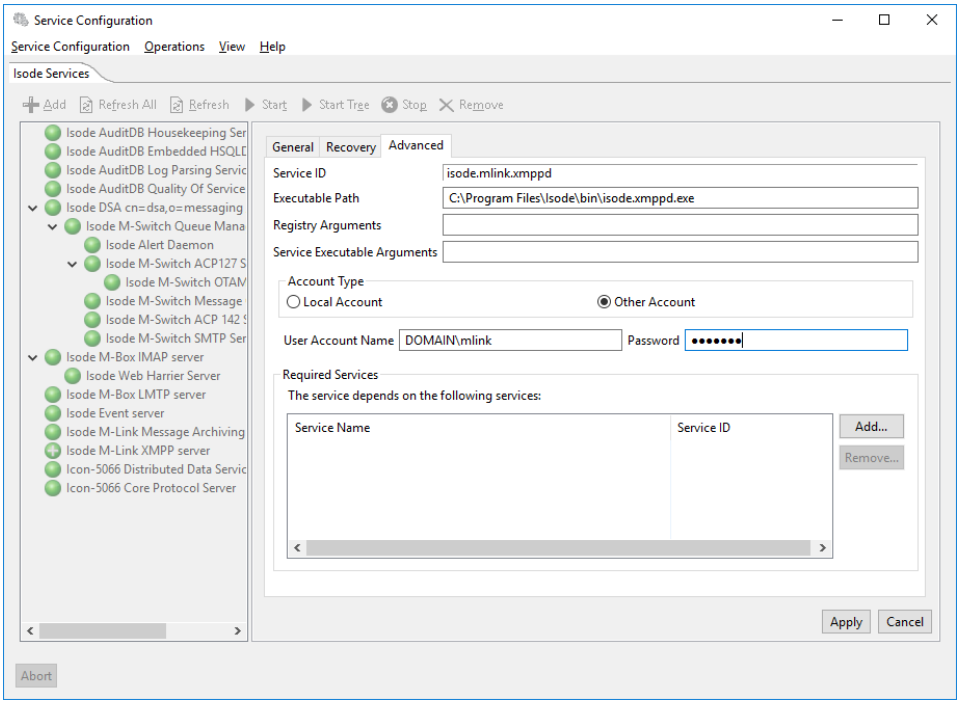
M-Link Server's default installation is set up as a Windows service under the `LocalSystem` account. It is recommended that a special Windows Managed Service Account is used to run M-Link and that SPNs are associated with this special account. This provides Windows operational benefits. It also provides two SSO security benefits:

1. The XMPP SPNs will only be available to M-Link.
2. M-Link will not have access to other SPNs created for other services.

To do this create a Windows Managed Service Account using standard Windows tools, which will assign appropriate privileges to the account. For a clustered M-Link configuration all severs must run in the same AD domain and one Managed Service Account must be used for all the M-Link servers. The SPN is associated with the Managed Service Account.

Isode Service Configuration tool can be used to set the Windows Service Account to run M-Link as shown below.

Figure 6.24. Set Windows Service Account



In the example the account `DOMAIN/mlink` is used. The password needs to be entered to set the configuration but is not stored by Isode tools.

6.3.3 Setting the SPN

This section illustrates how to use the Windows **setspn** command to set and manage necessary SPNs.

Where the SPN is assigned to a Windows account (recommended), use the **setspn** `-U` flag. For example, to assign the SPN `xmpp/example.com` to the user `mlink`, use the command:

```
C:\>setspn -U -S xmpp/example.com mlink
```

To view the the SPNs assigned to user `mlink`. use the command:

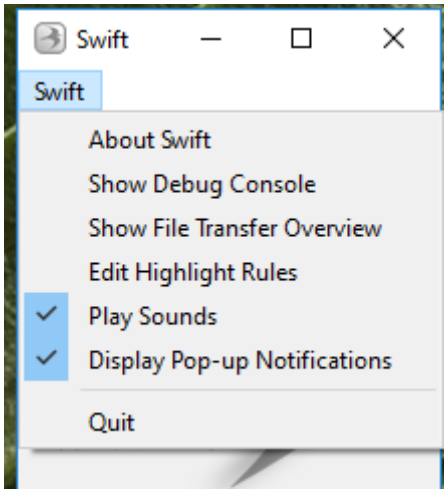
```
C:\>setspn -U –l mlink -l
```

Further details on use of the **setspn** command are provided in Microsoft documentation.

6.3.4 Testing that SSO is Being Offered

To validate that SSO is being correctly offered by M-Link for an IM domain, the best approach is to connect with a client to M-Link and examine the protocol trace. This can be done easily using the Isode Swift client. Prior to connection select **Show Debug Console** as shown below.

Figure 6.25. Show Debug Console in Swift



Protocol trace will appear in a special window. The first point to check is the first message sent from client to M-Link and the `to` field which is set to the IM domain. In the following example this is `example.com`.

```
<!-- OUT 2017-11-16T18:57:48 -->
<?xml version="1.0"?><stream:stream xmlns="jabber:client"
 xmlns:stream="http://etherx.jabber.org/streams"
 to="example.com" version="1.0">
```

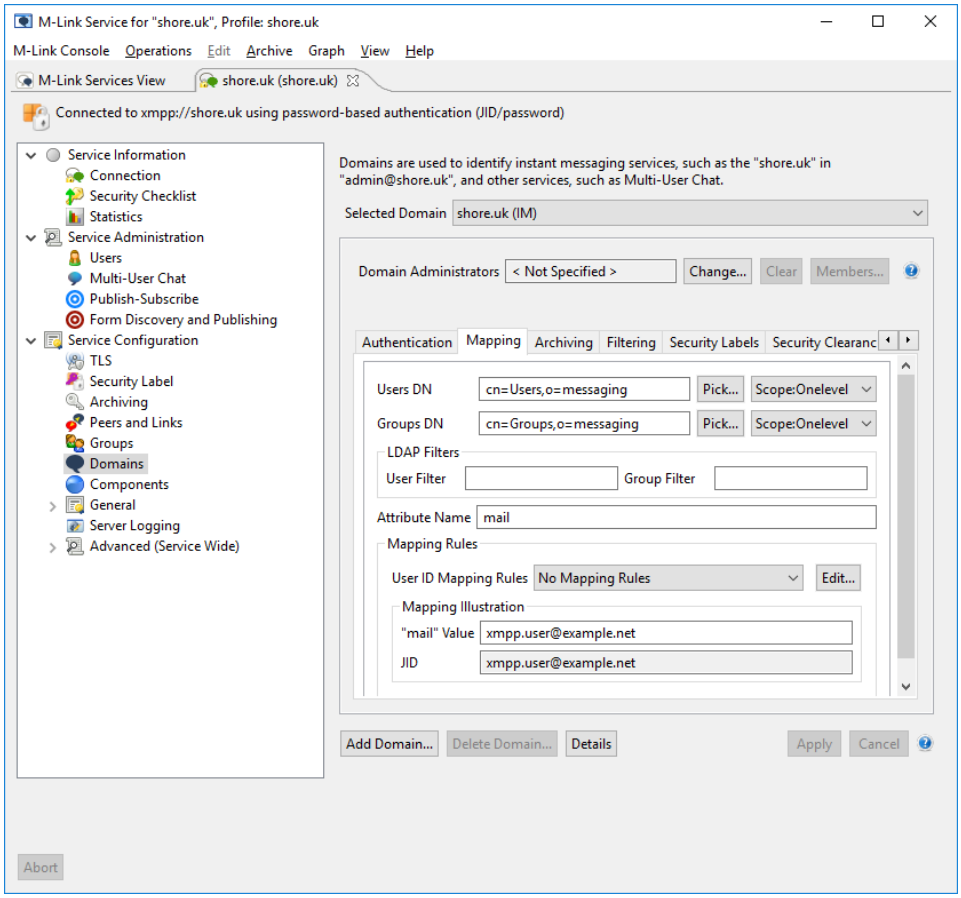
The second point to check is the `<stream:features>` response from M-Link, which will typically be the third message back from M-Link (after TLS negotiation). If this includes `<mechanism>GSSAPI</mechanism>` then SSO is enabled. The following example shows a response with SSO enabled.

```
<!-- IN 2017-11-16T18:57:48 -->
<?xml version='1.0'?><stream:stream xmlns='jabber:client'
 xmlns:stream='http://etherx.jabber.org/streams' from='isode.com'
 id='e364738402164a23' version='1.0'><stream:features>
 <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
 <mechanism>GSSAPI</mechanism><mechanism>PLAIN</mechanism>
 </mechanisms></stream:features>
```

6.3.5 Configuring JID Mappings for an IM Domain

When M-Link authenticates a user using Windows SSO, it will determine the JID to be used based on the Windows authentication information and on M-Link configuration. Windows SSO Authentication (Kerberos) will determine a User Principal Name to identify the client. M-Link will use this to determine the AD directory entry associated with the user. M-Link will then use information from this directory entry to determine the user's JID. This is configured with the IM Domain Mapping tab shown below.

Figure 6.26. IM Domain Mapping



The user's JID is derived from a directory attribute. This can be any attribute, but one of a small number will typically be chosen:

`mail`
: This is the default. It is an attribute that will usually be set and it is often desirable to have email address and JID the same.

`jid`
: This is a specific attribute to set JID. This enables completely flexible specification of a JID for each user and may be useful when other attributes do not give the desired mapping.

`SAMAccountName`
: A standard Windows account name to identify users.

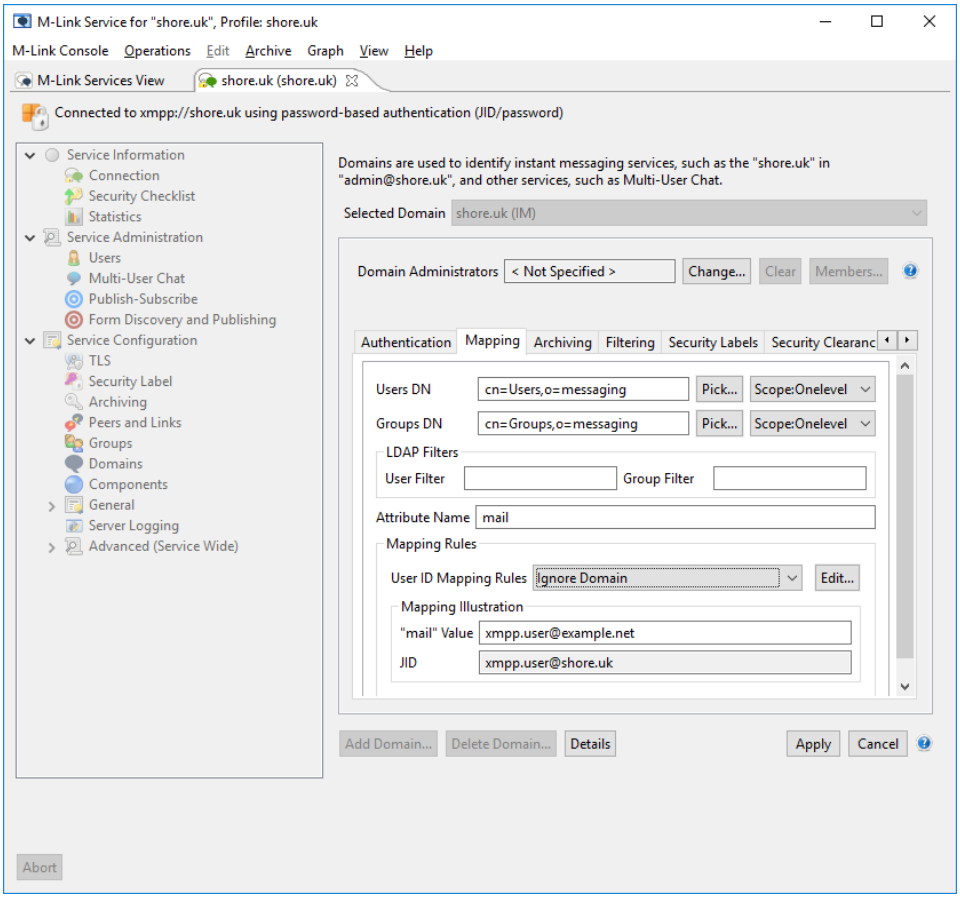
`UserPrincipleName`
: The Kerberos Principal Name of the user.

There is some post-processing done on the attribute to ensure that a valid JID is always derived:

1. Any characters not valid in a JID, such as space, are mapped or stripped.
2. If the attribute is a simple string (e.g., as in `SAMAccountName`) the configured IM domain value is added.

Additional mappings may also be configured, as shown below.

Figure 6.27. Additional Mappings



The mapping that may be useful in SSO setup is **Ignore Domain**. This will remove the domain that is included in the attribute and replace it with the configured IM domain. The UI illustrates the mapping that will take place.

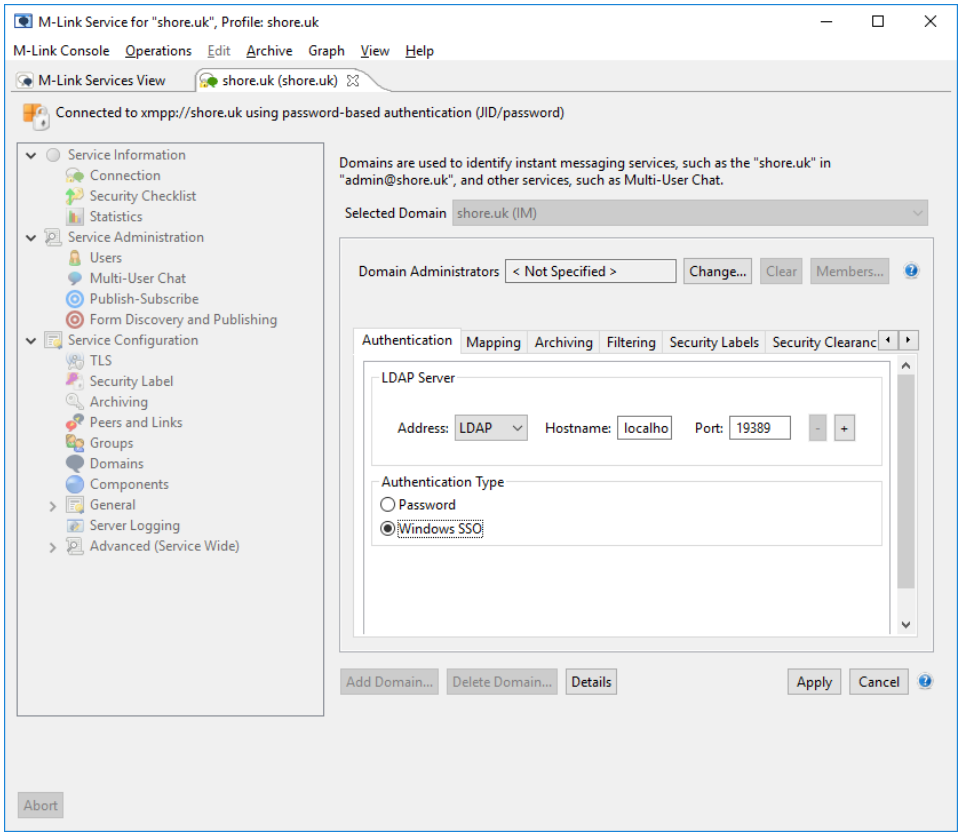
6.3.6 Testing SSO

Now that the server is fully configured, SSO can be tested with any XMPP client that supports SSO. An XMPP client that correctly supports SSO will only prompt for the IM Domain and the JID will be set by the server.

6.3.7 SSO Configuration for M-Link Access to Active Directory

In a setup using SSO, it will usually be desirable to configure M-Link access to AD to use SSO. This can be done by selecting Windows SSO for the IM domain, as shown below.

Figure 6.28. Set Authentication Type



Chapter 7 Security Labels in XMPP

This chapter discusses M-Link configuration of security labels.

7.1 Overview

In an environment using security labelling, there are a number of elements which allow user-friendly control of the sensitivity of a particular object, and which objects and users are allowed to see that object.

M-Link supports both the newer, XSF standards-track *XEP-0258*, and the older form of security labels used by the CDCIE system, including the TransVerse client. Setting up both requires a number of items to be configured. A policy is required for the server to evaluate labels and clearances, and a server itself will most likely need a clearance, and may be labelled.

7.2 Concepts

A number of concepts are key to understanding M-Link's handling of security labels.

7.2.1 Security Policy

A Security Policy defines what sensitivity levels and categories exist, and more generally what they mean, and how they interrelate. M-Link is informed of the key functional aspects via a Security Policy Information File, or SPIF, which is in the Open XML SPIF [http://www.xmlspif.org/] format.

7.2.2 Security Label

A Label embodies a particular sensitivity, and is attached to the object with that sensitivity. For example, a Confidential message would have a Confidential label present, and a Confidential chatroom would have a label present in its configuration.

Applying a label to a server restricts those who can connect to those with sufficient clearance.

Labels include a Display Marking which provides a human-readable form of the machine-readable label as well as information about which colors XMPP clients should use when presenting the label to human.

7.2.3 Security Clearance

Applying a clearance to an object enables it to handle labelled information. For example, server clearances are used to prevent messages labelled with a high sensitivity label from being accepted by the server, and to restrict a "top secret" server to only handling top secret data.

7.2.4 Catalogs

Catalogs are used to provide a working set of useful labelling options to security label capable clients which are not policy-aware. If no catalog is provided, then clients will be unable to label messages unless they are policy-aware - typical clients are not.

For example, chatroom configuration forms provide a simple list of labels and clearances so that a user may simply pick from a list instead of providing a label or clearance in native form.

7.3 System Wide Configuration

To enable security labelling, a SPIF must be configured at minimum (see Section H.2, “SIO Options”). It is also recommended to configure both a label catalog and a clearance catalog.

Neither catalog needs to be exhaustive, and the catalogs are filtered down as appropriate.

FLOT injection can be enabled to support clients which do not have native support; this will inject the display marking of a label into the message’s text.

7.4 User Configuration

Users should have clearances defined for them.

Clearances are refreshed on each authentication by the user.

7.5 Object Configuration

7.5.1 Server

Servers also may have clearance, which will cause any messages not passing the clearance to be rejected. Note that the absence of a clearance simply disables this check; a default clearance is not used.

A label will prevent user connections by users without the requisite clearance. If a user’s clearance is found to be insufficient at authentication time, then all the user’s existing sessions are also terminated.

Finally, a default label acts as a default of last resort; if no more specific default label can be found for a message with no label of its own, this label will be used.

7.5.2 Service Domain

Service domains, such as IM, MUC, and PubSub domains, may also have Clearances, Labels, and Default Labels associated with them. This is detailed in Section H.3, “Domains Options”.

7.5.3 Chatrooms

MUC Chatrooms may also have clearances, labels, and default labels, as seen in Chapter 9, *Multi-User Chat*.

7.5.4 Peers

Peers have clearances and default labels - the default label controls the inbound messages.

Peers may also have FLOT, and various relabelling options set as described in Section H.6, “Peers Options”. This may be used to setup multi-site security policies, or to hide the labelling from external sites.

7.6 Security Label Configuration using M-Link Console

Security Labels are described in the Isode Whitepaper available at http://www.isode.com/whitepapers/security-labels-clearance.html. *XEP-0258* describes the use of security labels in XMPP.

> **Note:** M-Link Console cannot be used for configuration of security labelling for a clustered or remote configuration. If you intend to create or update an M-Link cluster with security labelling or configure security labelling on the M-Link server remotely, then please contact Isode support.

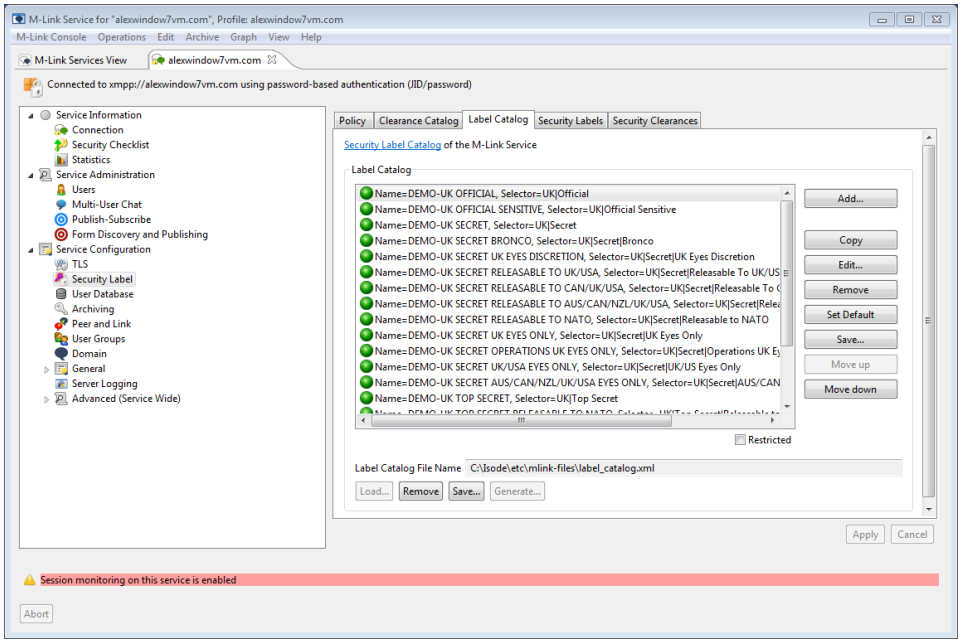
7.6.1 Setting up Security Policy

The security policy is represented as an SDN.801c SPIF in the Open XML SPIF format. To configure the security policy, select the “Security Labels” editor on the Service View of the local M-Link Server. Load the security policy XML file using the **Load...** button. Isode provides sample security policies which are called policy.xml. These can be found in *(SHAREDIR)/security-label/example-data/<sample-folder>*. A README.txt file in *(SHAREDIR)/security-label/example-data/* gives details about the policies in the sample folders. Click Apply to save the security policy for the server. You will now be able to create security labels and clearances. The above folders also contain sample clearance XML, label XML, clearance catalog XML and label catalog XML files. The server will need a restart to honour the security policy.

7.6.2 Setting up Catalogs

Security label and clearance catalogs are collections of security labels and clearances respectively. M-Link Console enables you to create and manage catalogs using the catalog editors. If a catalog is available as an XML file, it can be loaded using the **Load...** button. Once loaded, the editor displays the catalog as a collection of labels or clearances, each of which can be displayed and edited. The figure below displays a security label catalog which is very similar to the clearance catalog.

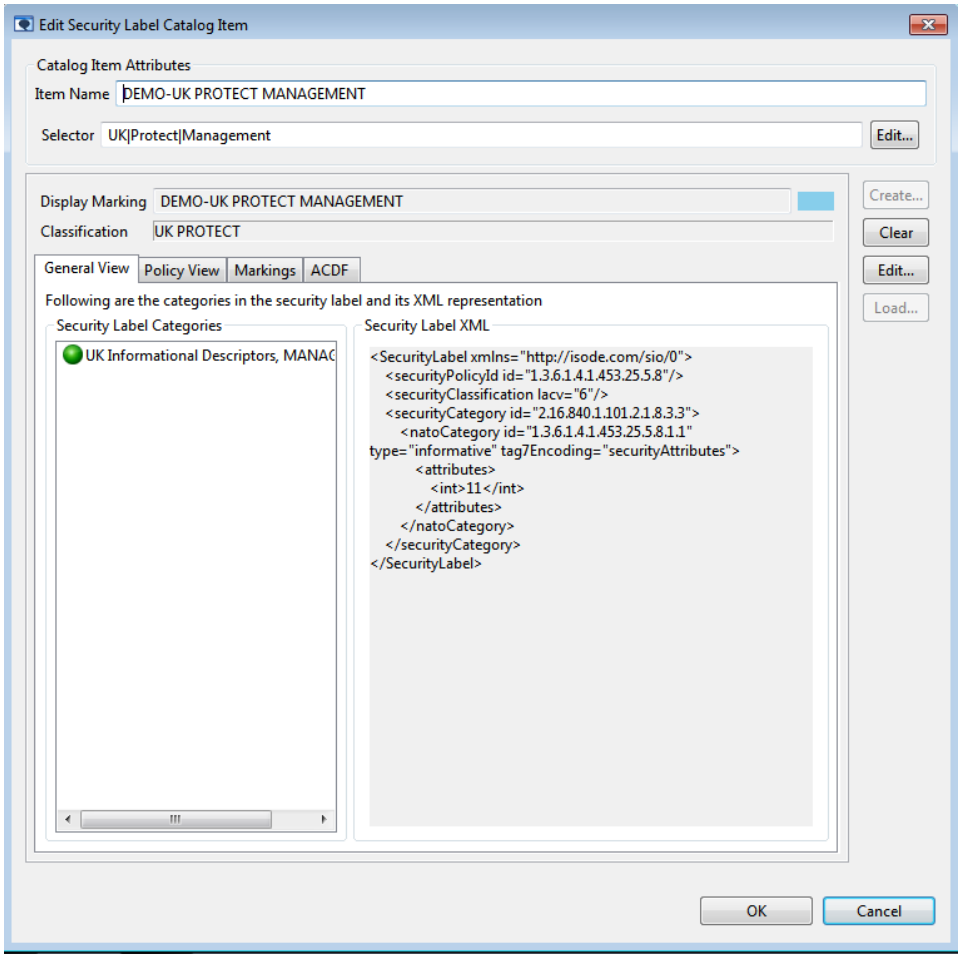
Figure 7.1. Security Label Catalog



The buttons on the right hand side of the Catalog editor provide various options to edit the labels or clearances in the catalog. Click **Add...** to add a new label or clearance to the catalog, or **Edit...** to edit an existing label or clearance in the catalog. The **Set Default** button can be used to specify a label or a clearance as the default item in the catalog. The catalog items can be rearranged in the catalog using the **Move up** and **Move down** buttons. The check button **Restricted** can be used to set the *restricted* status which advises the policy-aware applications to restrict users to only use items of the catalog.

The following editor will appear when adding or editing a new label item in the catalog (similar editor will appear for a clearance item).

Figure 7.2. Security Label Catalog Item

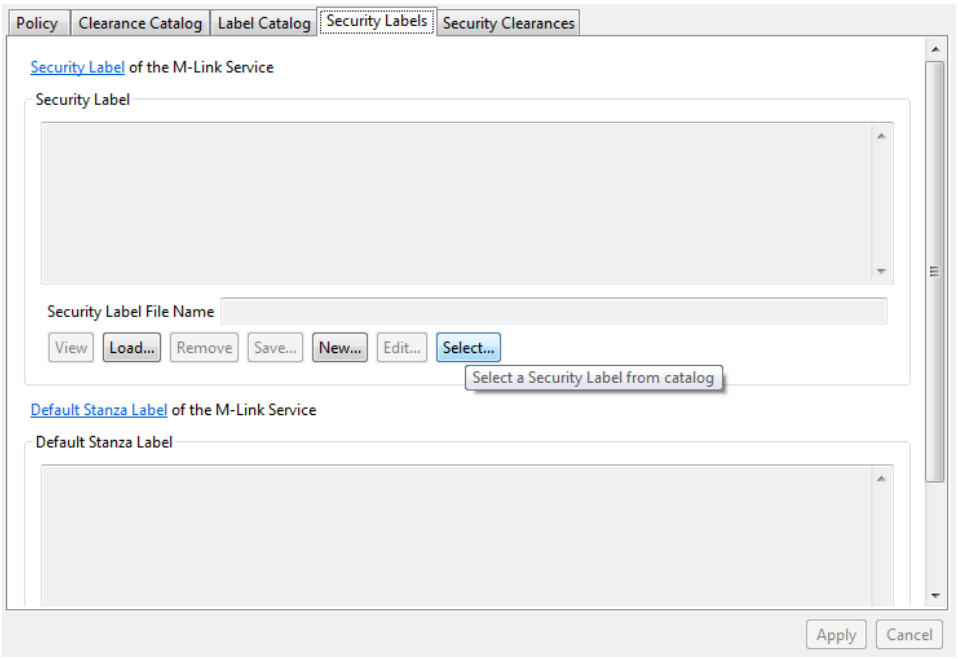


Create... button can be used to create a new label/clearance using the configured security policy. This button will only be enabled if the label or clearance is empty. **Edit...** button will allow editing the existing label/clearance which will only be enabled when the label/clearance has been created using the configured security policy. Use the **Load...** button to load a label/clearance from an XML file. The **Item Name** identifies the label/clearance in the catalog. The **Selector** is used for arranging the catalog items in a User Interface. The value of this attribute represents the item's placement in a hierarchical organization of the items. If one item has a selector attribute, all items should have a selector attribute. Selectors are strings separated by "|".

7.6.3 Applying Labels and Clearances

Once a security policy has been configured, a security label and/or a clearance can be applied to the M-Link Server. Click **Load...** to load a label from an XML file, **New...** to create a new label using the configured security policy or **Select...** to select a label from the label catalog. Similar options are available on the clearance tab for creating and setting clearances on the service.

Figure 7.3. Selecting a Security Label

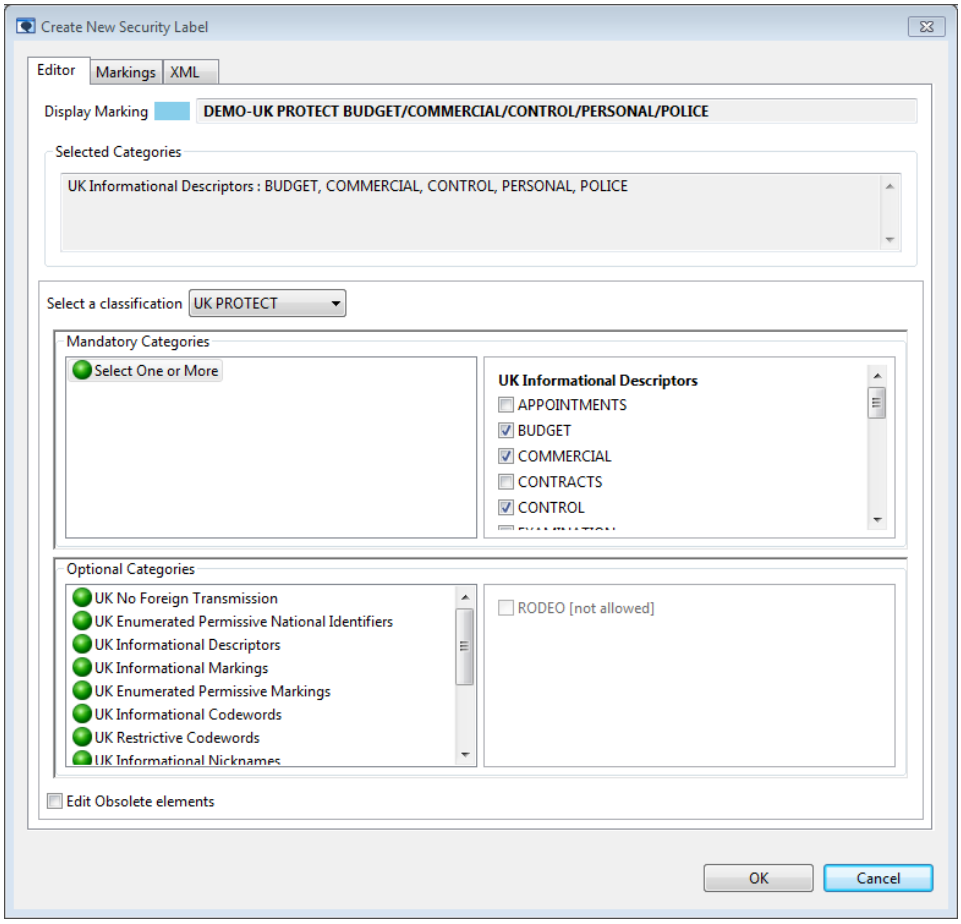


Note: Make sure that the bound M-Link User (administrator) has a suitable clearance before applying a label or default label to the Service or domain. Insufficient clearance of the administrator may result in lockout if a label or default label is applied.

7.6.3.1 Editing Security Labels

The following editor will appear when either the **New...** or **Edit...** button is selected for creating or editing security label (see Figure 7.2, “Security Label Catalog Item” and Figure 7.3, “Selecting a Security Label”).

Figure 7.4. Security Label Editor



In order to create a new security label, first select a classification from the drop-down list. Note that classification cannot be changed when editing an existing label. Selecting a classification may or may not require inclusion of certain categories. The required categories if any will be displayed as a list in the **Required Categories** pane. The **Optional Categories** pane lists all the categories in the configured policy, from which the user can select certain categories to be added to the label. A category in the Required/Optional Categories list is selected if the user selects a button from the options in the pane on the right hand side of the category group. Once a category is selected, it appears in the list of Added Categories.

The categories which are disallowed based on the selection of a certain category or classification, will be disabled automatically on the editor. The obsolete categories will be allowed for editing, based on whether **Edit obsolete elements** is selected or not.

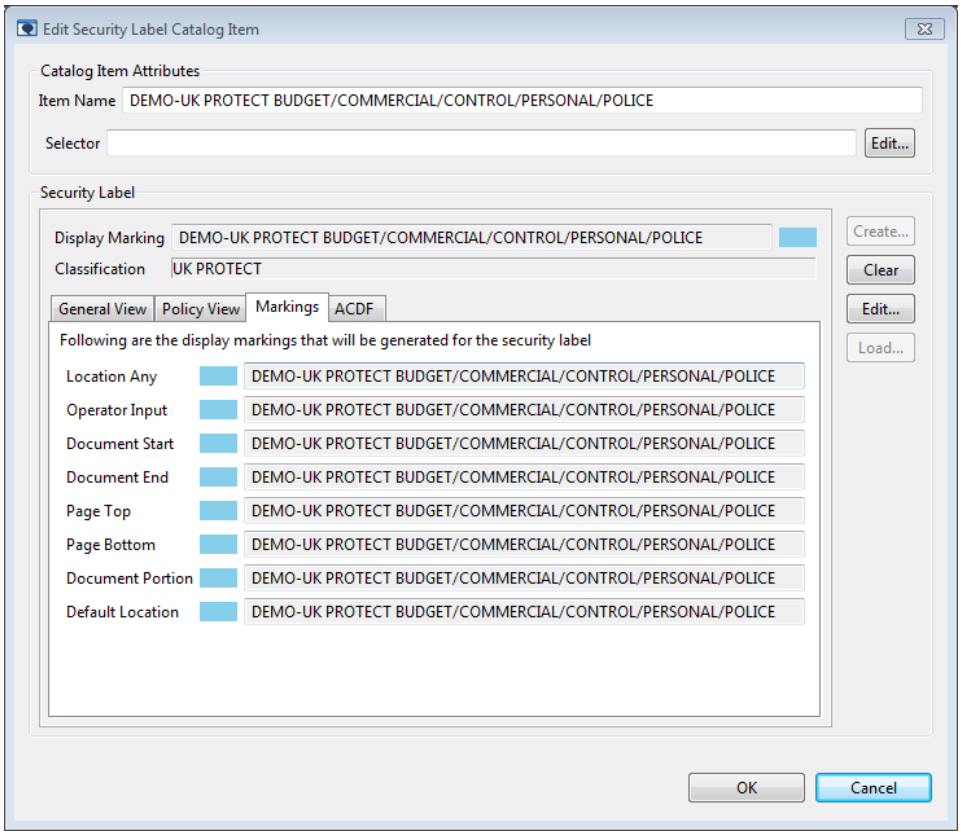
If selection of a classification mandates some categories to be selected which appear on the **Required Categories** section, a solid green circle indicates that the requirement for the required category item have been fulfilled by the selection of categories in that group. An empty green circle will indicate that the requirement for the item is not valid and still requires you to select categories in that group. Required categories are a subset of the **Optional Categories** and once selected, will also appear selected on the **Optional Categories** pane. This will simplify label creation by highlighting the items that need reviewing.

Selection rules of a category group determine whether it allows selection of single or multiple categories in the group. For single category selection, the categories are displayed using radio buttons, and for multiple category selection they are displayed as check-boxes.

The added categories and the XML format of the security label will get updated on the editor as the label is edited.

The markings get updated on the **Markings** tab when a valid combination of categories has been selected as shown in the figure below.

Figure 7.5. Security Label Markings

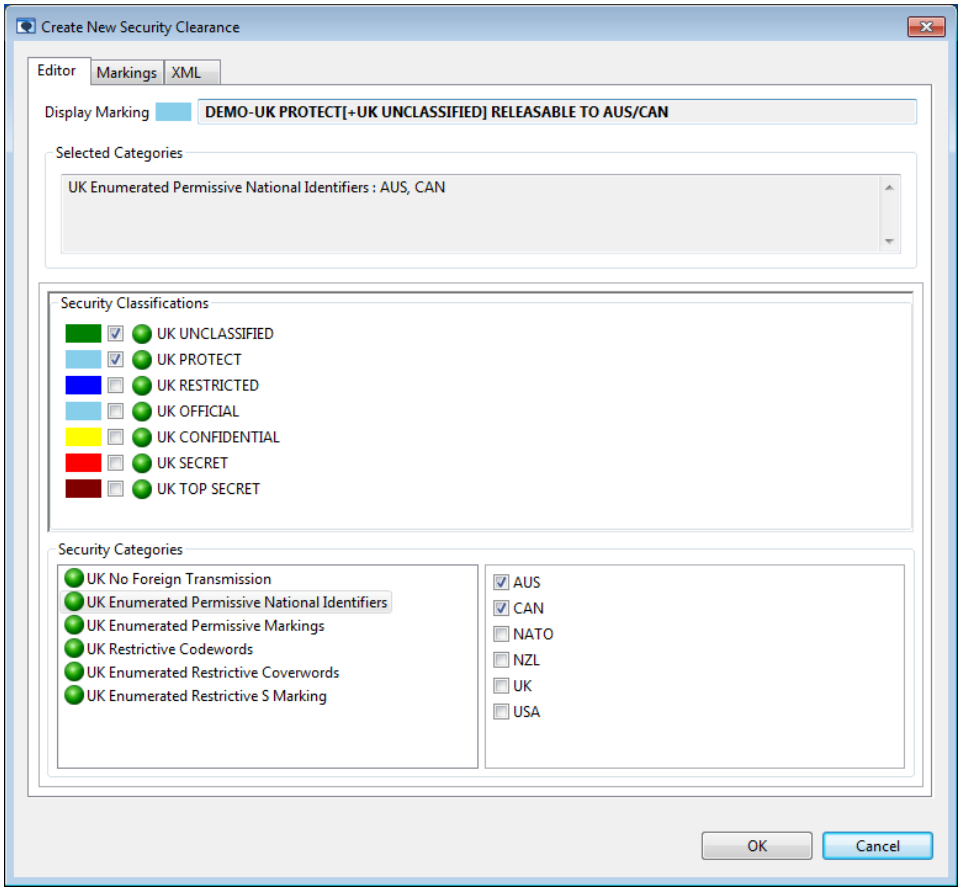


Note: Rules for label editing are based on SDN.801c and are configured in the security policy.

7.6.3.2 Editing Security Clearance

Once a security policy has been configured, a clearance can be created. The following editor will appear when either the **New...** or **Edit...** button is selected for creating or editing security clearance from the clearance editor or a clearance catalog item editor. These are similar to the ones for security label editor (see Figure 7.2, “Security Label Catalog Item” and Figure 7.3, “Selecting a Security Label”).

Figure 7.6. Clearance Editor

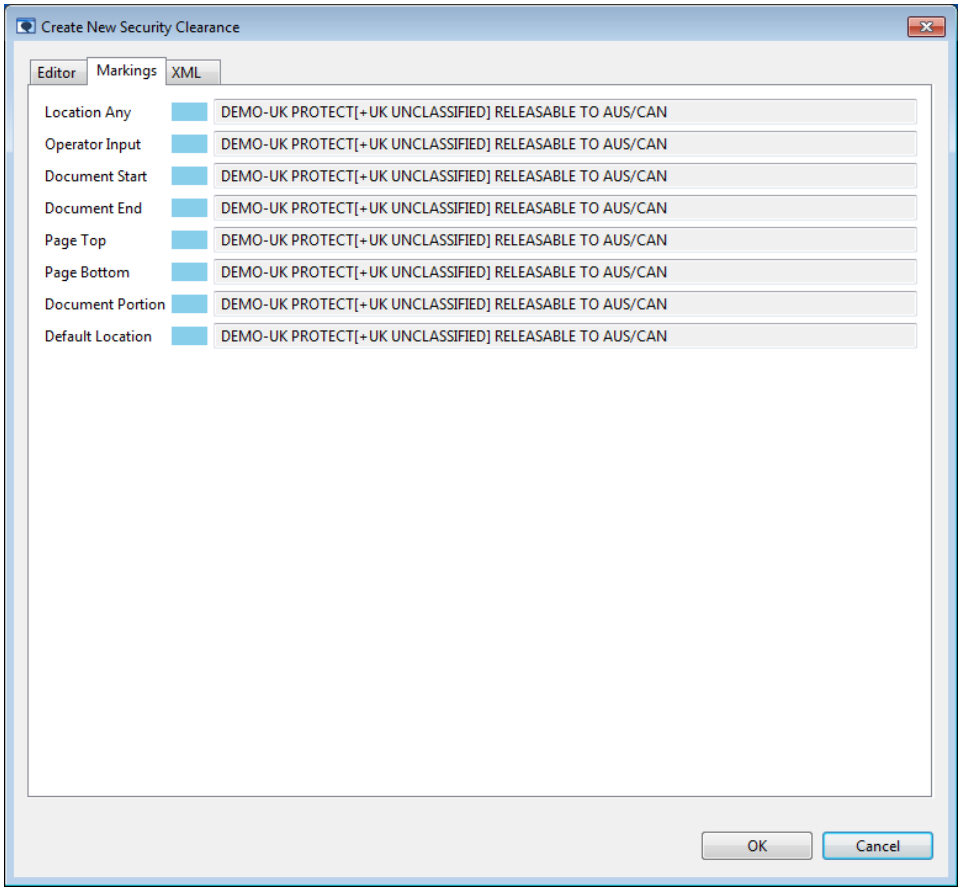


One or more classifications can be selected from the **Security Classifications** pane to be added to the clearance. The **Security Categories** pane lists all the categories in the configured policy, from which the user can select certain categories to be added to the clearance.

The added categories and the XML format of the security clearance will get updated on the editor as the clearance is edited.

The markings get updated on the **Markings** tab as and when the clearance is modified:

Figure 7.7. Clearance Markings

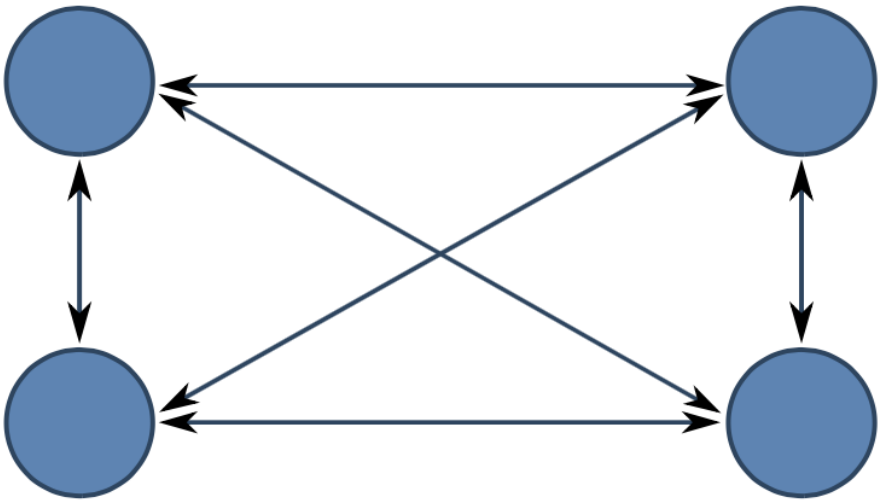


Chapter 8 M-Link Edge, Peers and Links

This chapter introduces the M-Link Edge product, explains what XMPP trunking is, and how M-Link peers can be used to support it. It also shows use of *links* to support operation with XML Guards and operation over constrained links, including HF Radio using STANAG 5066.

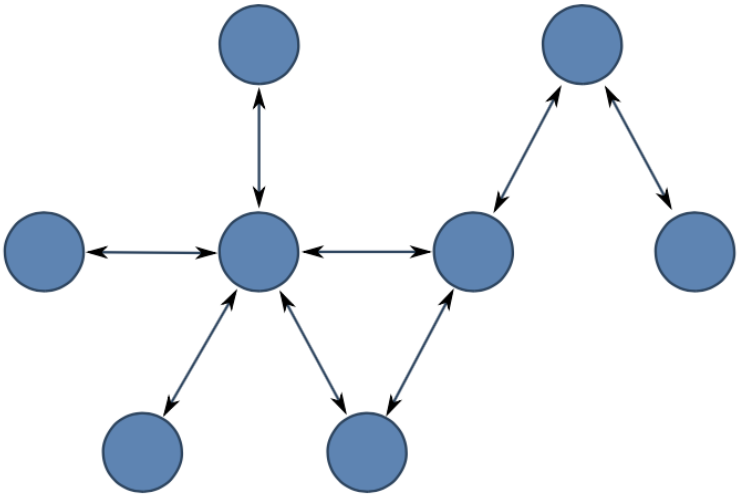
8.1 XMPP Trunking and Peer Controls

Figure 8.1. Standard XMPP Server Configuration



In a standard XMPP configuration, XMPP servers are fully interconnected, as shown in Figure 8.1, “Standard XMPP Server Configuration”. This model works well for open XMPP deployments on the Internet. However, it does not work so well for cross domain, organizational boundary and constrained link scenarios.

Figure 8.2. XMPP Trunking



The model of XMPP Trunking, shown in Figure 8.2, “XMPP Trunking” extends the standard XMPP model to allow for configurations where servers are not fully connected. This structure enables XMPP messages to be switched through intermediate servers.

Peer Controls is the mechanism used by M-Link to enable configuration of an XMPP Trunking architecture. By default, M-Link will use DNS to determine which server to connect to, which will lead to a fully connected approach. A Peer Control provides configuration for a domain to direct M-Link to connect to a specific peer.

Further information on XMPP Trunking and use of M-Link Peer Controls is provided in the Isode white paper “Providing XMPP Trunking with M-Link Peer Controls” https://www.isode.com/whitepapers/xmpp-trunking.html

8.2 Peers and Links

M-Link peer controls apply to domains and are checked prior to DNS being used. There are three types of peer control configuration:

1. Single Specific Domain. This is used to force routing for a specific domain.
2. Domain plus all sub-domains.
3. Default. This forces routing of all traffic to this peer control, unless there is another peer control. This is helpful in configurations where all traffic is handled with peer controls.

This combination provides full flexibility to configure arbitrary XMPP trunking configurations.

When a peer control is in place, it is possible to configure specific actions for the peer:

- Traffic filtering, which enables removal or modification of traffic to and for the peer.
- Security Label checking against a configured security clearance for the peer.
- Security label mapping.

Traffic to a peer configured with peer control may flow in a number of ways:

- Using standard S2S. Here the peer control is simply used to control traffic flow, and optionally use custom TLS configuration for the peer. The other options use special protocols.
- XEP-0361 "Zero Handshake Server to Server Protocol" operating over TCP (see Section 8.11, “XEP-0361 Zero Handshake Links”). This protocol is designed to support constrained bandwidth links with high latency, where standard S2S will lead to performance problems. It is also used to connect XML Guards.
- STANAG 5066. This provides operation of HF Radio using XEP-0361 in conjunction with XEP-0365: "Server to Server communication over STANAG 5066 ARQ". See Section 8.12, “STANAG 5066 Links”

8.3 M-Link Edge

M-Link Edge is an M-Link server with no local users that is used in boundary and cross-domain configurations to check and potentially modify traffic. M-Link Edge will often be used in conjunction with an XML Guard to provide cross-domain protection and may use XEP-0361 to communicate with the XML Guard.

M-Link and M-Link Edge are both provided by the same underlying technical product, but are sold as different products. Note that XEP-0361 may not be used with a standard M-Link deployment that supports local users.

8.4 Constrained Network Configurations

There are two further M-Link product variants used in support of constrained networks. These variants will always use XEP-0361: "Zero Handshake Server to Server Protocol" and may use XEP-0365: "Server to Server communication over STANAG 5066 ARQ" for HF Radio.

The two product variants are:

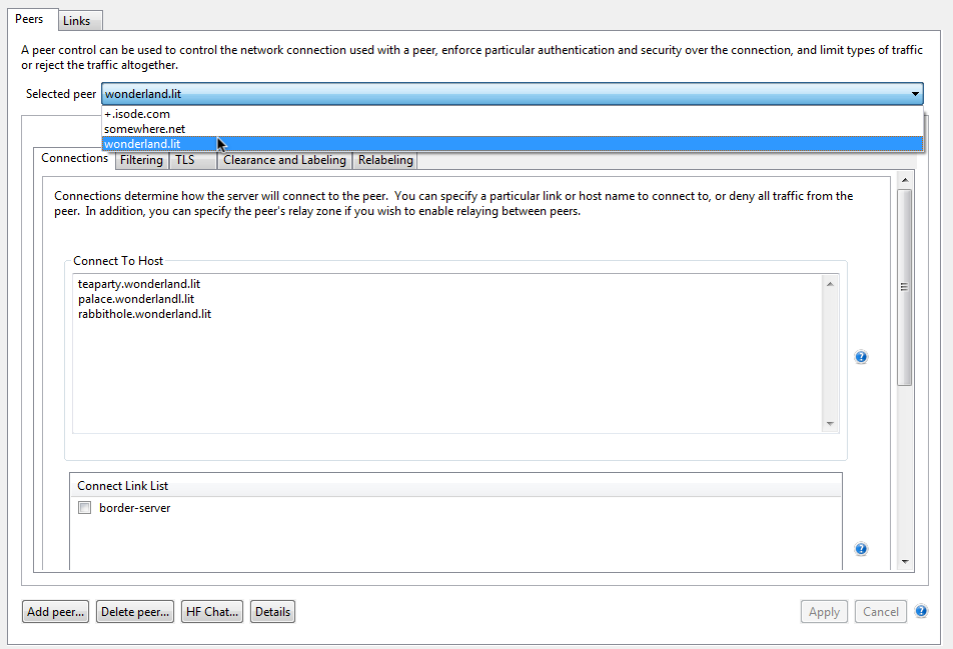
1. M-Link Constrained Network Server. This is an M-Link server supporting local users that only communicates using XEP-0361 and does not use standard S2S. This is used to support local users on a system which only communicates over constrained networks.
2. M-Link Constrained Network Gateway. This is an M-Link server with no local users. On one side it communicates with M-Link Mobile servers using XEP-0361. On the other side it will communicate with federated XMPP servers using standard S2S. It may also communicate with an XML Guard.

8.5 Peer Configuration

M-Link Console allows you to manage peer and link configuration using the **Peer and Link** editor. This only appears for *Server* administrators, and will only offer server-wide configuration (as opposed to node specific configuration - see Chapter 14, *Clustering*).

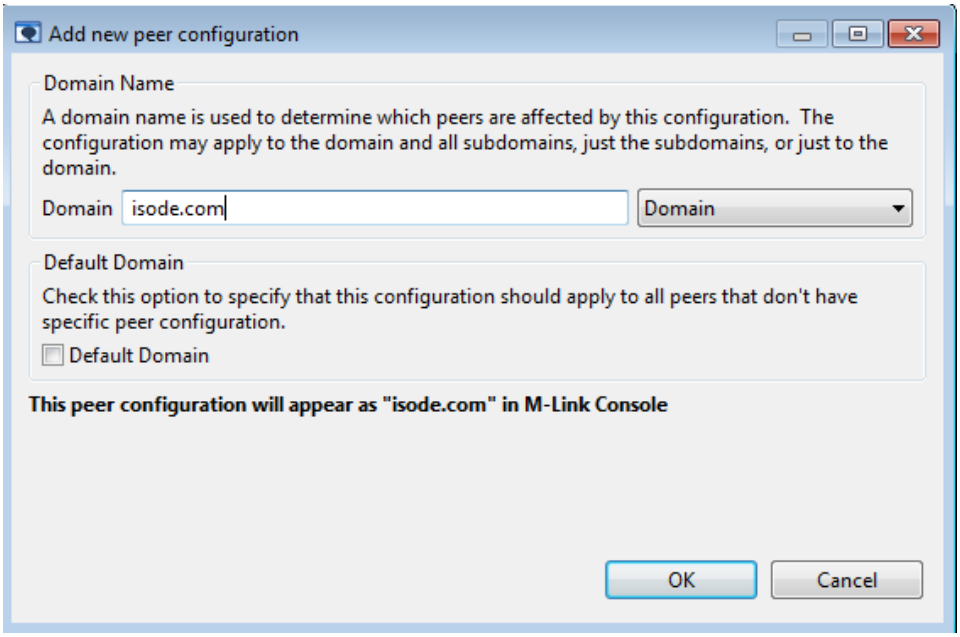
Select *Peer and Link* in the service view and then select the **Peers** tab. The **Selected Peer** selection box can then be used to choose which of the configured peers to see the details of:

Figure 8.3. Viewing peer configuration



To add information about a peer, click on the **Add peer** button. You will be prompted to supply a domain name, and to specify whether this peer configuration applies just to the domain in question, or whether it applies also to subdomains:

Figure 8.4. Adding a peer



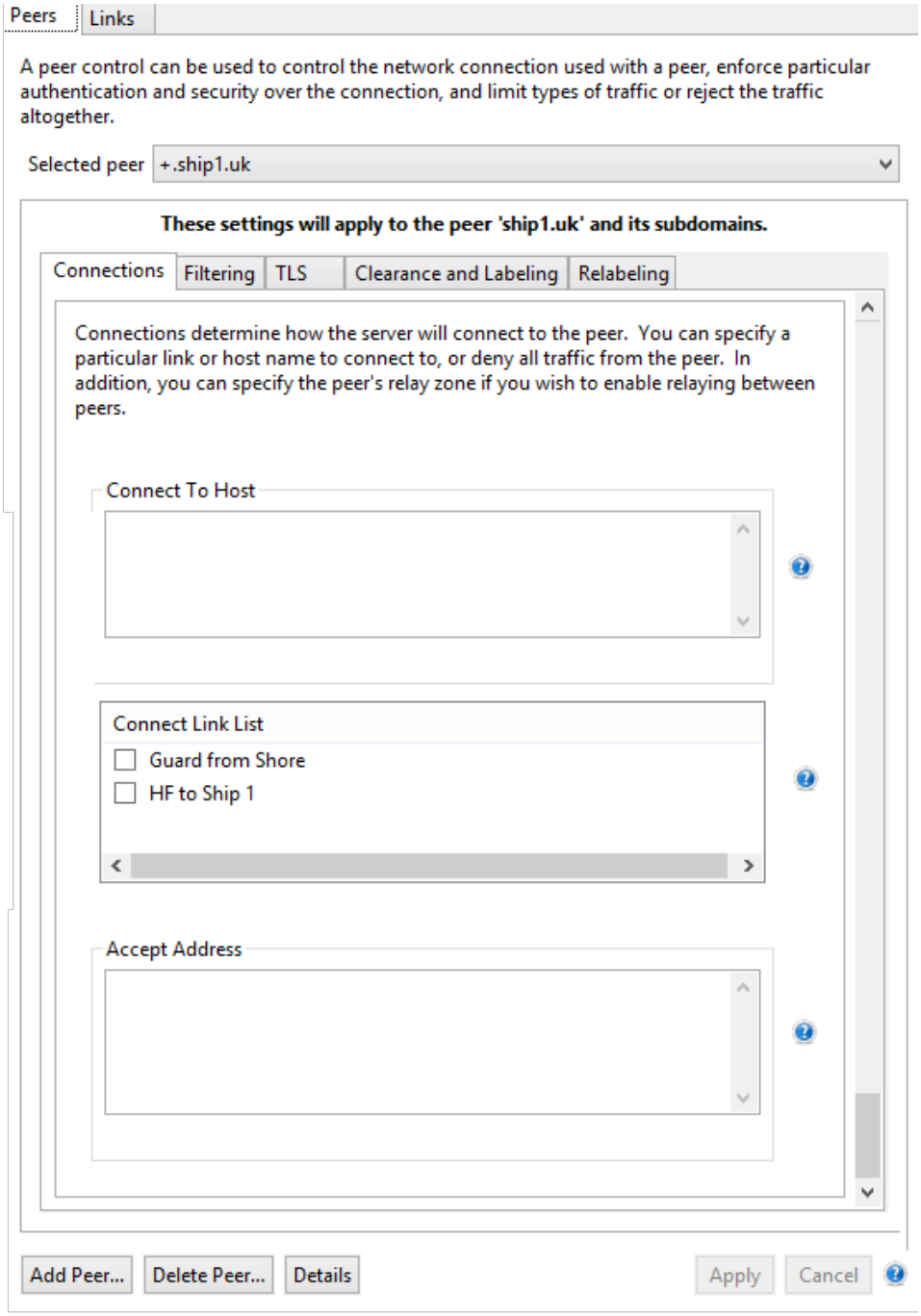
Before adding the new peer, M-Link Console allows you to set any peer configuration using the same set of tabs as previously mentioned. Once the configuration is complete, use the **Apply** button to add the new peer.

The various configuration options for the peer are separated into the following tabs:

- The *Connections* tab can be used if you want to direct connections for this peer to a specific host/IP address (rather than relying on the default lookup for the domain). If any links are configured (see Figure 8.14, “Link configuration editor with no links configured”), you can choose one of those links.
- The *Filtering* tab is used to specify filters that are used to constrain traffic between this M-Link Service and the specified peer. See Section 8.8, “Peer Filtering” below.
- The *TLS* tab is used to configure whether the peer must use TLS, and if so whether it must use strong authentication. Any certificate supplied by the peer will be verified against the server's Trust Anchors (see Section 5.2, “Steps to configure TLS for an M-Link Server”), or match the *Server Certificate* shown in this tab.
- The *Clearance and Labelling* is used to configure the security clearance of the peer and the security labels used for messages to and from the peer. See Chapter 7, *Security Labels in XMPP* for more information on security labels and clearances.
- The *Relabelling* tab allows you to configure options related to the relabelling policy for this peer. See Section H.6, “Peers Options” for more information.

8.6 Connection Configuration

Figure 8.5. Configuring Peer Connections



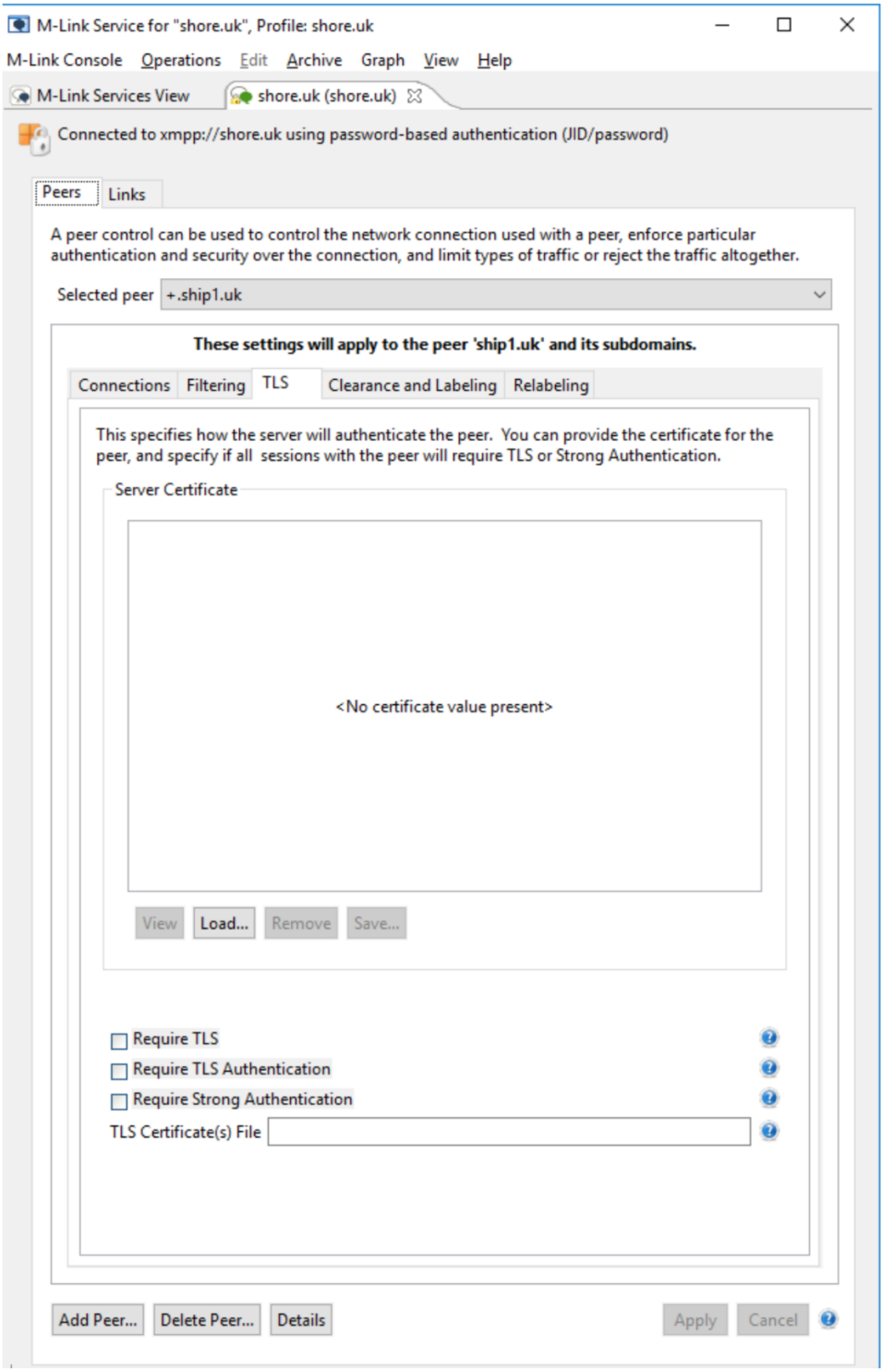
The Connections tab of a Peer enables control of connections when standard S2S is used. The **Connect to Host** allows configuration of the host that is connected to, overriding DNS lookup. See Section H.6.2, “Connect To Host”.

The Connect Link List shows links that may be used to control how traffic for the peer is routed. See Section H.6.3, “Connect Link List”.

Accept Address lists permissible addresses for S2S connections from the domain. See Section H.6.10, “Accept Address”.

8.7 Authentication with Standard S2S

Figure 8.6. Configuring Peer Authentication



Configuration of peer authentication for a peer using standard S2S is configured using the TLS tab for the peer. The key options on this tab are:

- Server Certificate. This can be used to specify PEM-formatted certificates which are sufficient to authenticate the peer. This is referred to as *Certificate Pinning*. It is only needed where an appropriate trust anchor is not configured for M-Link.
- Require TLS. If this is selected, use of TLS is enforced for the peer.
- Require TLS Authentication. If this is selected, the server requires authenticated TLS in sessions it initiates with the peer.
- Require Strong Authentication. If this is selected, peers connecting to this server must assert a valid X.509 certificate.
- TLS Certificate File. This option, if set, overrides values specified in the "Server Certificate", by specifying the names of files which contain PEM formatted certificates to authenticate the peer.

The following subsections provide more details on this authentication.

8.7.1 Inbound authentication

S2S Authentication in M-Link is handled by first attempting to use any presented certificate to authenticate the peer.

M-Link expects a peer to provide a *from* attribute on the stream to identify itself; this will be used as the requested identity and validated against the certificate. Note that a peer must have already provided a version attribute in order to trigger the offer of features (including TLS).

If there is no *from* attribute, then the certificate is examined to see if there exists any jid which may validate; in either case, SASL EXTERNAL is offered. Note that the tests are performed at the point where TLS is negotiated, not after the stream is restarted subsequently, and as such it’s possible for a peer to provide a from attribute only after the certificate has already been evaluated, and therefore too late.

Also, we only offer SASL EXTERNAL (and indeed trust the certificate at all) if CRL checking passes – this means that if CRL checking is on, and we cannot find or use the CRL (it contains unknown critical extensions, or the CRL DP points to an unknown protocol or unreachable destination) then the certificate will not be trusted.

However, whether or not we trust the certificate, if a peer presents the certificate configured in its peer control and requests that domain, then it will be trusted; however in this case, it MUST use a *from* attribute on the stream in order to be offered SASL EXTERNAL.

The remote peer formally requests to use the identity in one of three ways:

8.7.1.1 SASL EXTERNAL with no authorization identifier.

In this case, M-Link uses either the stream’s *from* attribute, or – if there is none – a default extracted from the certificate. It is possible, in the case of wildcards for example, that no such authorization identifier exists, in which case the SASL exchange fails.

If the stream’s *from* attribute is used, this authorization identifier will be checked against the certificate prior to returning a `<success/>`. (Since this identifier may have changed after the initial test earlier, of course).

8.7.1.2 SASL EXTERNAL with an authorization identifier.

In this case, M-Link will validate the requested authorization identifier against the certificate and fail if the certificate does not match.

8.7.1.3 db:result with a from

If a Server dialback request (see *XEP-0220*) is received and the peer is requesting a domain for which the certificate will authenticate it, then an actual dialback is not performed (i.e., no `db:verify` is sent) and the request is immediately accepted. This is known as “dialback without dialback”.

If the requested domain (the from attribute on the db:result) is not verifiable via the TLS certificate, then the dialback proceeds as normal – if strong authentication is not required for the peer.

To require this, you will need to configure strong authentication, and then set the Require TLS (Section H.6.5, “Require TLS”) and Require Strong Auth (Section H.6.7, “Require Strong Authentication”) settings both to true.

8.7.2 Outbound authentication

This is simpler. At the point of authentication, however offered by the peer, M-Link will check that the peer’s domain is validated by the certificate – either by being present in a trusted certificate or via configuration.

8.7.3 M-Link authentication to peers

If M-Link is able to verify the peer it’s connecting to via TLS, it will still use dialback if required to authenticate itself. M-Link’s configuration on strong auth requirements therefore only affects its requirements for the remote peer to authenticate to M-Link, and will not enforce that M-Link use SASL EXTERNAL as a client.

If M-Link is offered SASL EXTERNAL, it will always use it, and will always include an authorization identifier. This will always be the same as the stream *from* attribute. This is technically counter to the strict reading of the specifications; however we have found that this aids (and never harms) interoperability.

8.8 Peer Filtering

This section describes filtering that may be configured for a peer using the *Filtering* tab.

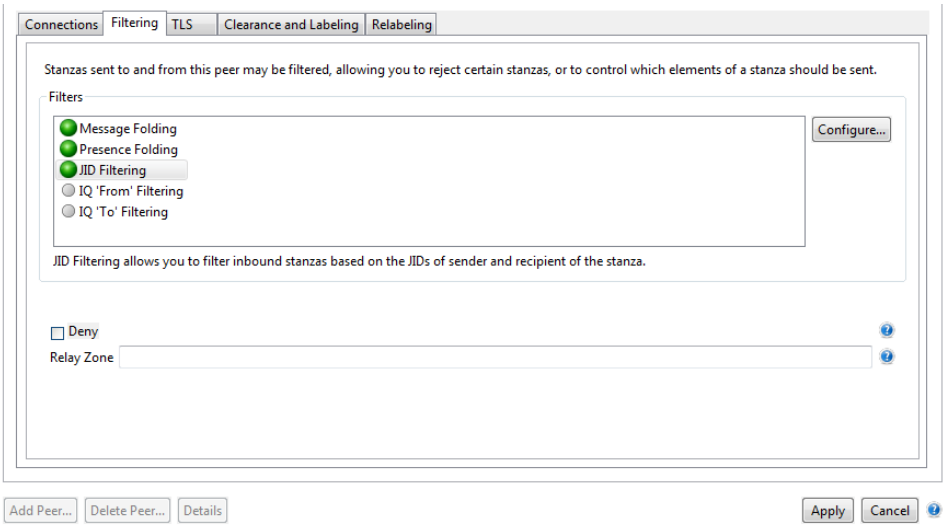
Filtering can also be configured on domains, and this section is the reference for this capability. Note that only JID and IQ filtering can be applied to a domain. The message and presence folding capabilities are not available for domains.

The M-Link Server supports filtering configuration for any peer, which allows you to specify which stanzas (or stanza elements) should be discarded when data is exchanged with that peer. One typical case where this may be useful is when network capacity is constrained: for example, on a slow link it may make sense to set up a filter to strip all presence stanzas. Another use of filters is to control which stanzas from the peer are discarded, based on the JID of the sender and recipient of the message.

The M-Link Server provides various configuration parameters that determine how filtering is performed. These parameters are described in Section H.6, “Peers Options”. As well as allowing you to change the value of these parameters directly, the editor in M-Link Console also provides some *pre-set* options: if you select one of these, then M-Link Console will set the configuration parameter(s) appropriate for that option.

There are five types of filtering supported by M-Link. The **Filtering** tab will indicate which, if any, has been configured, and allow you to manage them:

Figure 8.7. Viewing Filters for a peer

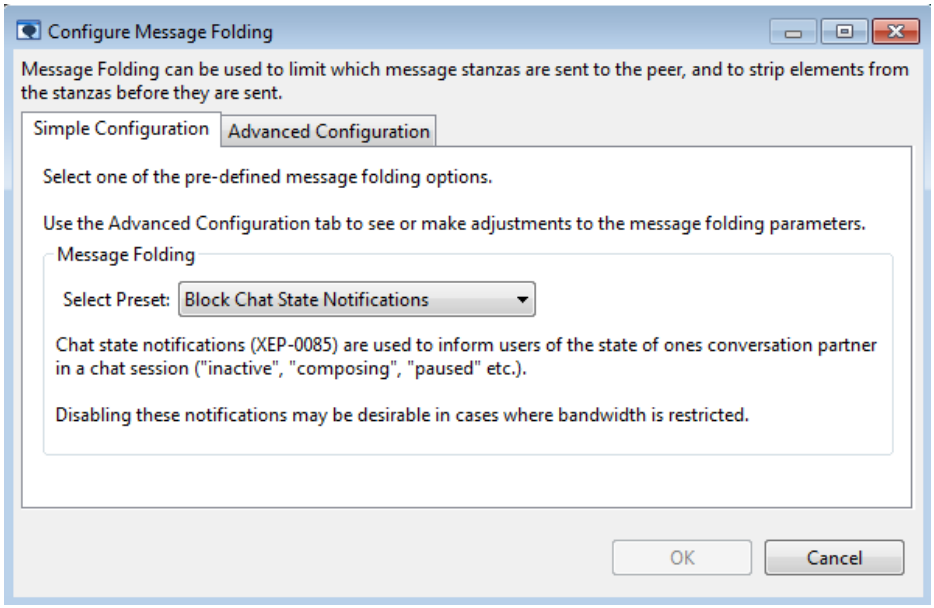


The filter types are:

- *Message Folding* allows you to control which payload elements of a `<message> ... </message>` stanza are sent to the peer.

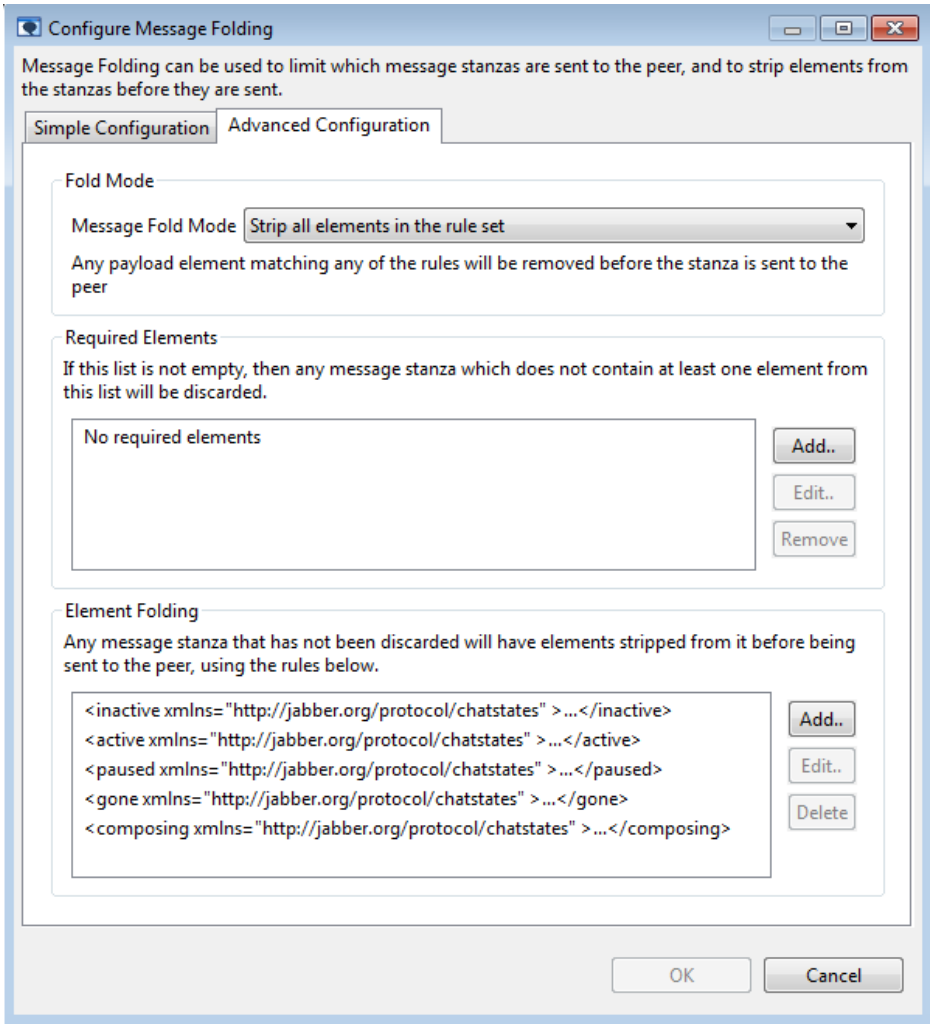
  The editor provides various pre-sets for this option; in each case, selecting a pre-set will display an explanation of its meaning:

  Figure 8.8. Choosing message folding pre-set

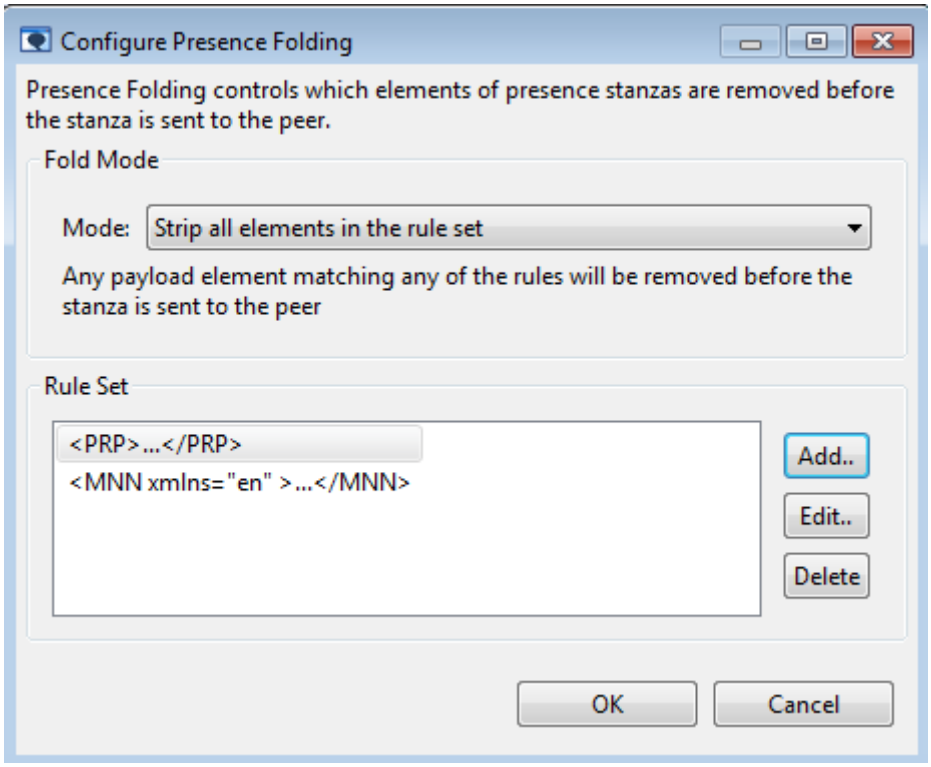
  By switching to the **Advanced** tab, you can see the effects of any chosen preset; you can also use this tab to fine-tune the configuration:

Figure 8.9. Advanced view of "Block Chat State Notifications"



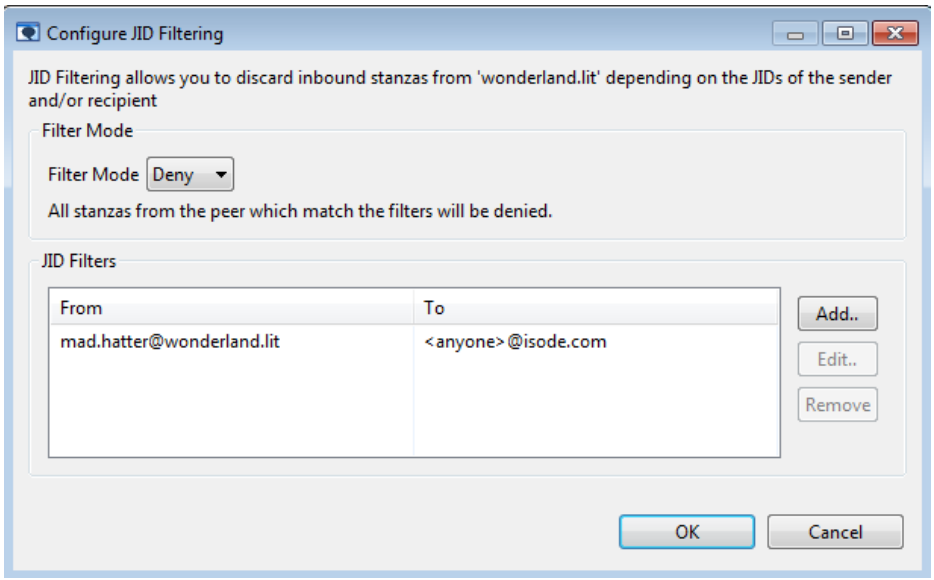
- *Presence Folding* allows you to control which payload elements of a `<presence> ... </presence>` stanza are sent to the peer. You can discard presence stanzas altogether, or configure a filter that will allow or discard specified payload elements from presence stanzas:

Figure 8.10. Presence Folding configuration



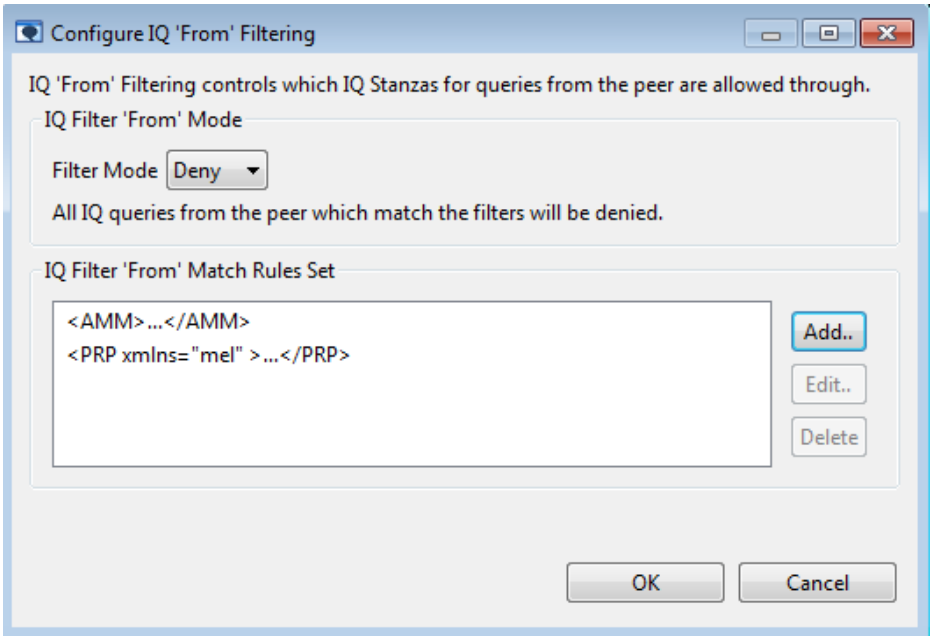
- *JID Filtering* allows you to control which incoming stanzas from the peer should be discarded, based on the JIDs of the sender and recipient. In the example below, any stanzas from `mad.hatter@wonderland.lit` sent to any JID with a domain of `isode.com` will be discarded (and any other stanzas will be permitted):

Figure 8.11. Configuring a JID filter



- *IQ 'From' Filtering* and *IQ 'To' Filtering* allow you to filter IQ stanzas from and to the peer, based on their payload elements:

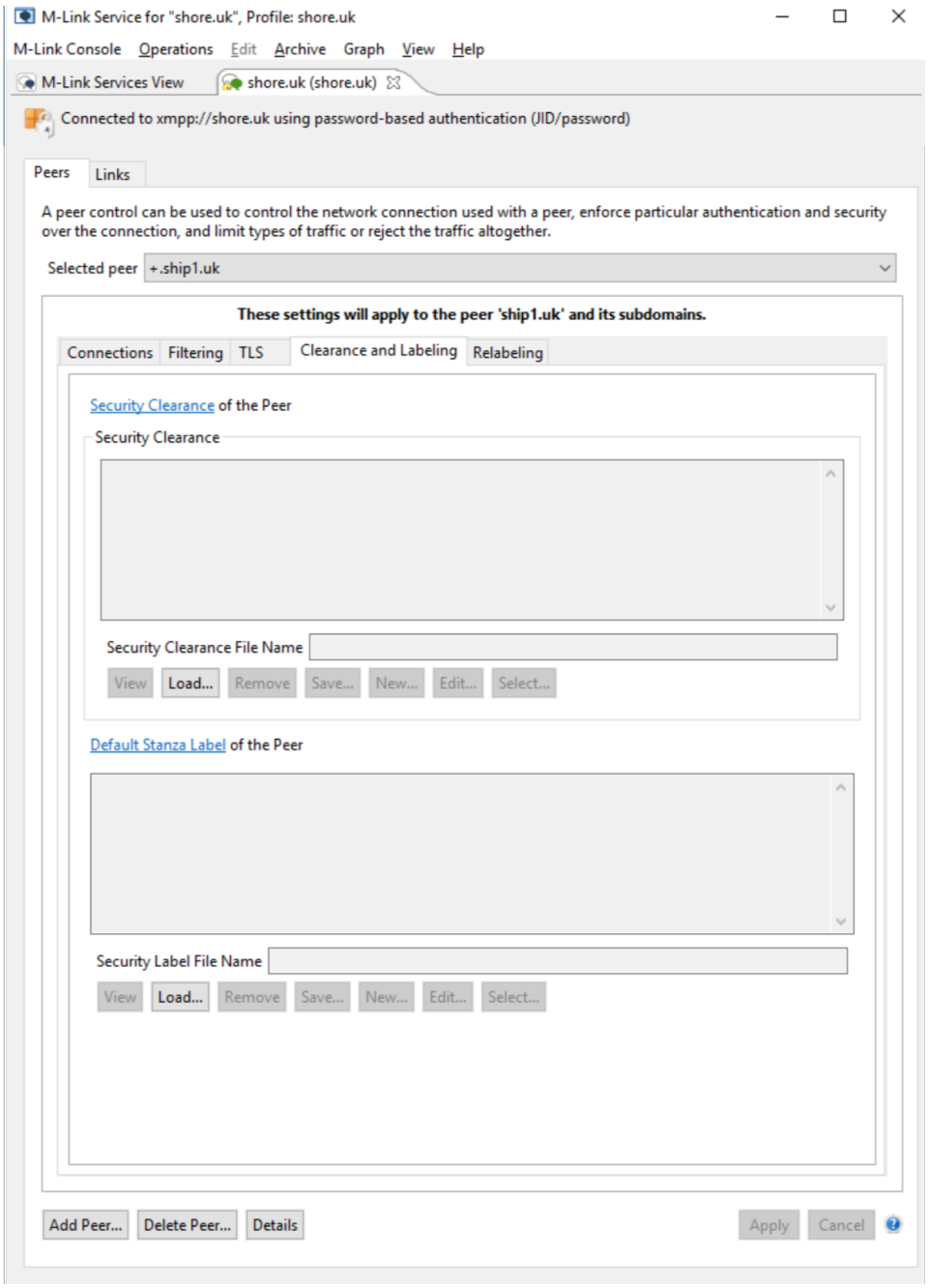
Figure 8.12. Configuring an IQ filter



8.9 Clearance, Labelling and Relabelling

Controls on peers based on security labels and security clearances can be configured for each peer. A general overview of M-Link security label and security clearance capabilities is provided in Chapter 7, *Security Labels in XMPP*.

Figure 8.13. Clearance and Labelling



The Clearance and Labeling tab for a peer allows setting of:

- Security Clearance. If set, this is used to check the security label on all stanzas passing through. If the access control check fails, messages are rejected.
- Default Stanza Label. If set, this specifies a security label which will be added to any messages which do not have a security label. This can be helpful when a security label is required on all messages.

8.10 Configuring Links

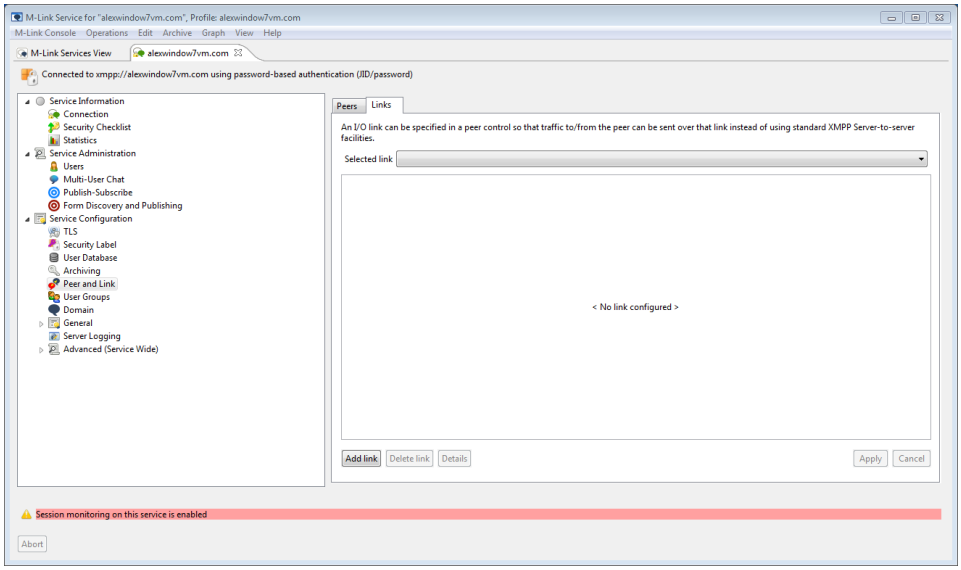
M-Link Console can be used to configure links of two types:

1. XEP-0361 Zero Handshake links
2. STANAG 5066 Links for HF Radio using XEP-0361 and XEP-0365

Links are configured as independent objects in M-Link. M-Link peers may be configured to use a link. If no links are configured for a peer, standard S2S is used.

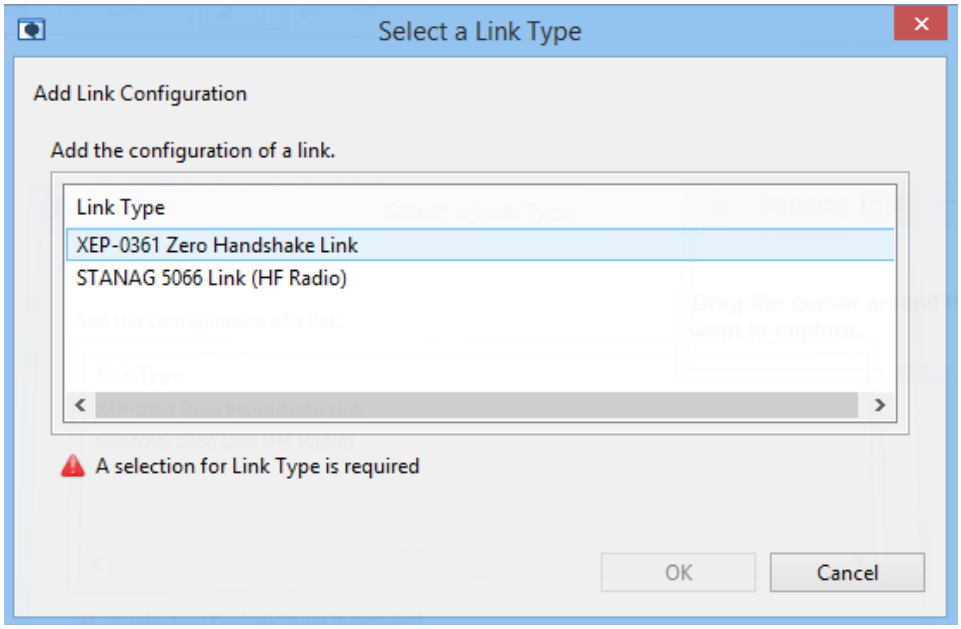
Select the **Links** tab in the Peer and Link editor to see information about the links that are currently configured:

Figure 8.14. Link configuration editor with no links configured



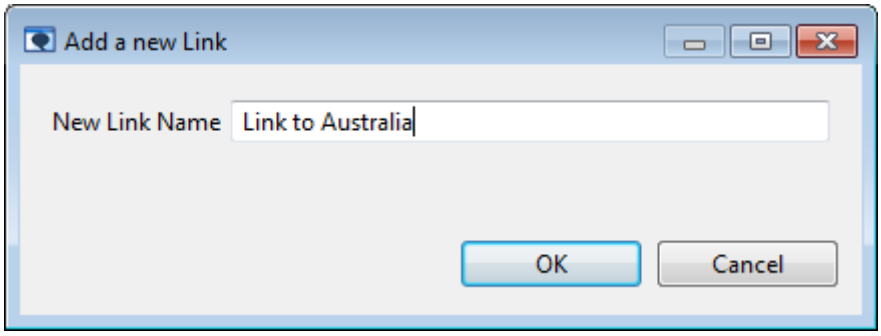
To create a new link, click on the **Add link** button, and choose a link type:

Figure 8.15. Selecting a link type



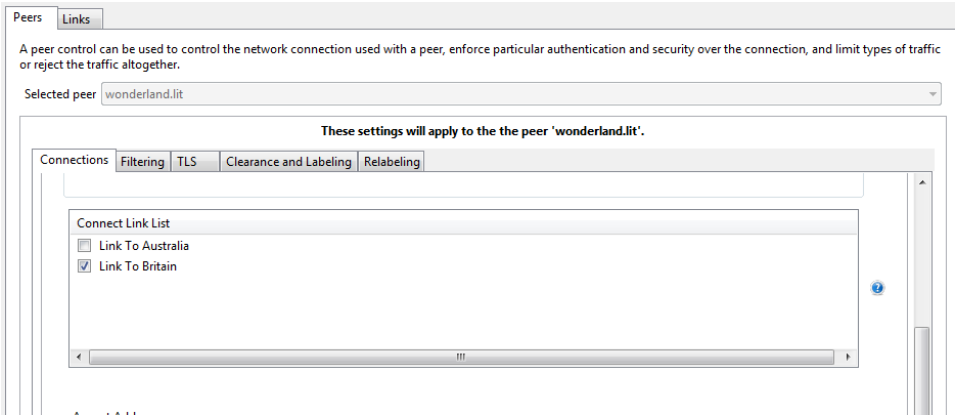
You will then be prompted to enter a name for the new link:

Figure 8.16. Enter a name for the link



If you have any links configured, then they will appear in the *Connect Link List* section of the Peer editor. By default, a peer configuration will not be associated with a link, but you can change a peer's configuration to select one or more links (multiple links may be specified for failover purposes). Note that a single link may be used in multiple peer configurations.

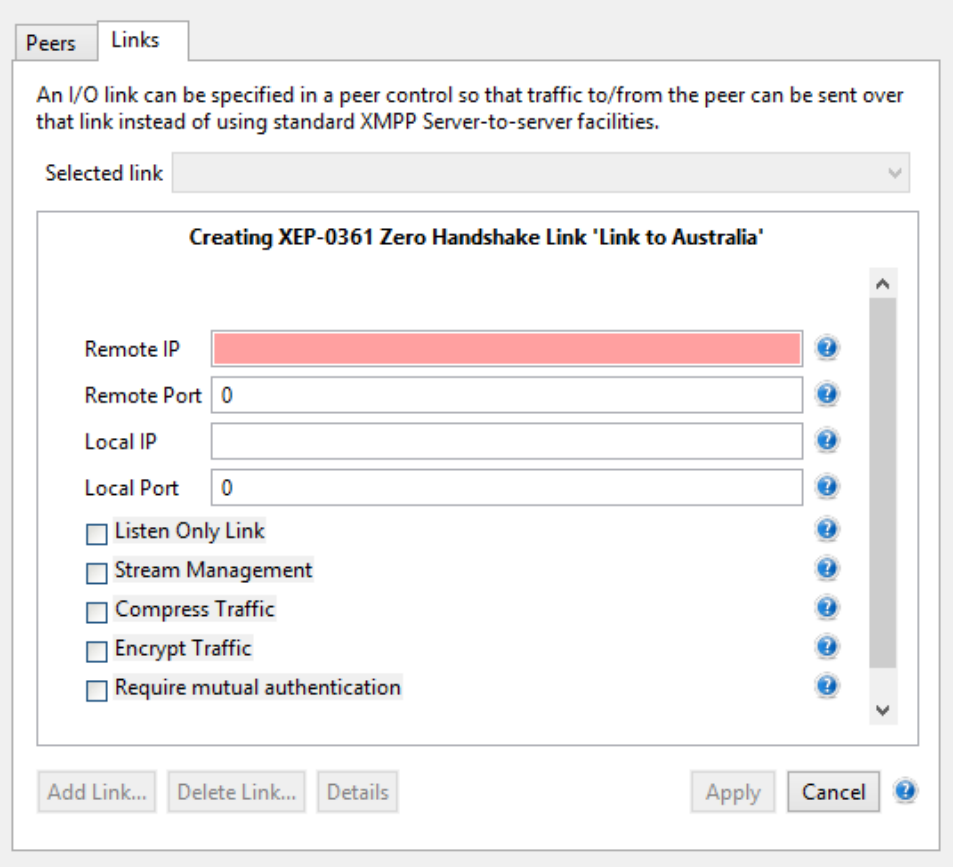
Figure 8.17. Configuring a peer with a specific link



8.11 XEP-0361 Zero Handshake Links

The options for configuring a XEP-0361 Zero Handshake Server to Server protocol link are shown below:

Figure 8.18. Configuring a XEP-0361 link



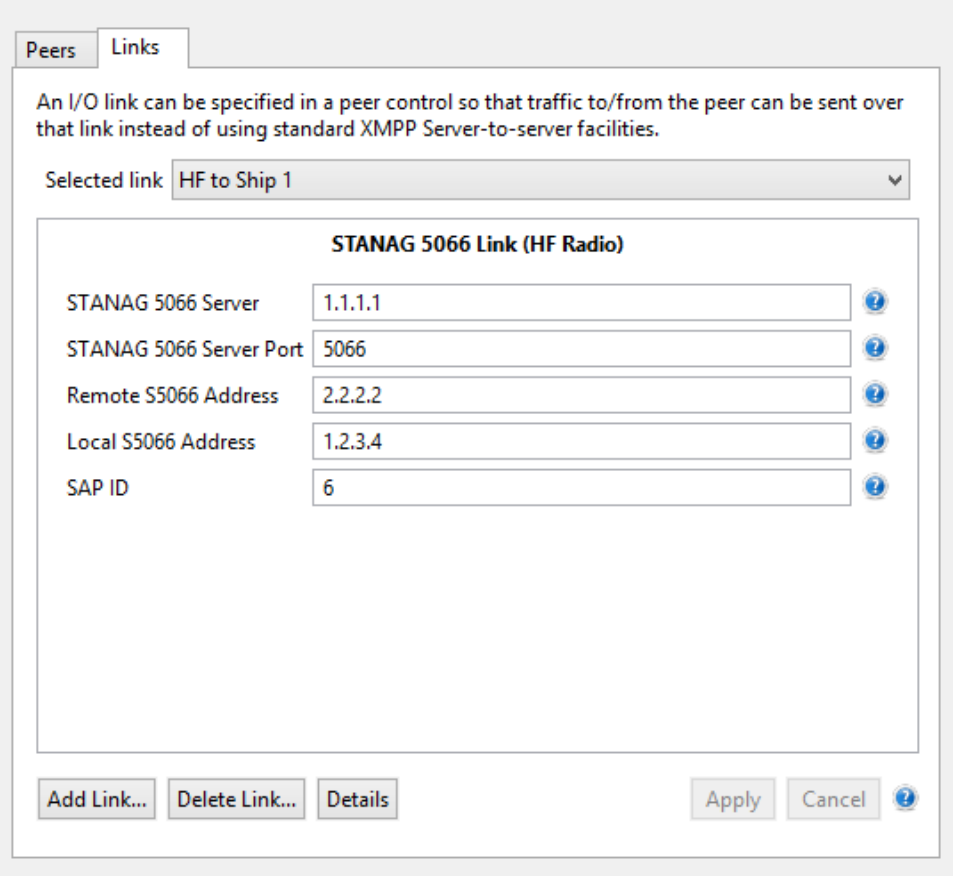
The parameters for a XEP-0361 link are set as follows:

- Remote IP: the IP address of the peer
- Remote Port: the port used by the peer
- Local IP: the IPv4 or IPv6 address that the local server listens on
- Local Port: the port that the local server listens on
- Listen Only Link: a link that accepts connections but does not initiate them
- Stream Management: Whether XEP-0198 stream management is enabled
- Compress Traffic: whether or not traffic is compressed
- Encrypt Traffic: enables TLS encryption. Note that this will add TLS handshakes to the connection.
- Require Mutual Authentication. Use two way strong authentication for the peer

8.12 STANAG 5066 Links

A STANAG 5066 link is used to support HF Radio connections using XEP-0361 and XEP-0365 "Server to Server communication over STANAG 5066 ARQ". The link is configured as shown below:

Figure 8.19. Configuring a STANAG 5066 (HF Radio) link



The parameters for a STANAG 5066 link are set as follows:

- STANAG 5066 Server: the IP address where the STANAG 5066 Server is running
- STANAG 5066 Server Port: the STANAG 5066 server port, which will usually be 5066
- Remote S5066 Address: the STANAG 5066 node address of the peer
- Local S5066 Address: the STANAG 5066 node address of the local system
- SAP ID: the STANAG 5066 SAP ID used - usually 6 (RCOP).

Chapter 9 Multi-User Chat

This chapter explains the M-Link Server implementation of Multi-User Chat rooms.

9.1 Overview

Multi-User Chat (MUC) rooms allow several entities to communicate together, whether by simple text messages or more complex structured XML. They have both affiliations – long-term, persistent, relationships between users and the room – and roles – short-term relationships between room occupants and the room.

M-Link Server is a relatively full-featured implementation of [*XEP-0045*] and supports persistent rooms if configured.

9.2 Persistent rooms

Rooms are persisted in the Publish-Subscribe config directory, using a simple XML format, and their history is persisted as a directory of atomically managed files.

These files and directories should not be managed directly, but instead a capable XMPP client should be used to create a room under a MUC domain and manage it.

9.3 Creating and configuring rooms

Although persistent rooms can be precreated in XML, the simplest method for creating chatrooms is to simply use a standard XMPP client. Rooms are, by default, made as partial copies of a special room with the node-name `template-room`, which can be changed to provide useful defaults.

9.3.1 Room configuration options

Room configuration options are listed in Appendix I, *MUC Room Settings Reference*. They are identified by the data form (see [*XEP-0004*]) field variable name, and also include the descriptive name used by M-Link in the form.

If FMUC or IRC gatewaying support is enabled, additional options related to these features will also be present. See Section 9.6.2, “Configuring federation of a MUC room” and Section 9.7.1, “Enabling IRC Gateweying for the server” for details of these

Form names beginning with `muc#` are standardized as part of [*XEP-0045*], and more details will be found there.

9.3.2 Affiliations

This section explains the default rights and roles of affiliations. No affiliations or roles are allowed to manipulate users of a higher affiliation or role, hence a Administrator cannot kick an Owner or Super from a room.

9.3.2.1 Super

Server administrators and Domain administrators of the MUC domain (see Section 2.5, “M-Link Server Administrators”), will automatically be Owners of any chatroom they join on the server. Owners of the template-room will automatically be owners of rooms they join on the same server.

This automatic owners are, internally, treated as 'Super', with a role of 'Super', which are presented as 'Owner' and 'Moderator' respectively.

They do not appear on room affiliation lists, and these affiliations are temporary only.

9.3.2.2 Owner

Room owners conceptually have complete control of the room. They will be made Moderators on joining the room.

9.3.2.3 Administrator

Administrators conceptually manage the room, and can view and change affiliations equal to or lower than theirs. Like owners, they will be made Moderators on joining the room.

9.3.2.4 Members

Members have a long-term relationship with the room, and will always become Participants when they join a room, allowing them to post messages in the chatroom itself. If made Moderator, then they can manipulate users with affiliations equal to or less than their own.

9.3.2.5 Outcast

These are conceptually banned from the room, and cannot join the room.

9.3.2.6 None

Anyone without an affiliation – even after domain matching – will be assigned the default role when they join the room. This is typically indirectly set either by the 'Moderated' or 'Members Only' settings to be either Participant, Visitor, or None. The latter setting will not allow them to join the room.

Note that 'Moderated' and 'Members Only' settings are mutually exclusive.

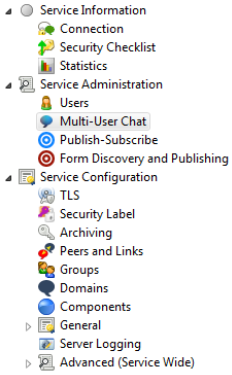
9.4 The template room

Each MUC service has a special room, called template-room, which can be used to set certain service-wide settings. Room affiliations on this room are special, and room settings are copied to newly created rooms, allowing the provision of defaults. Finally, service-wide settings are also found here.

9.5 MUC Administration using M-Link Console

M-Link Console provides some basic functionality for MUC administration via the **Multi-User Chat** editor editor. This is accessible to all *Server* administrators and any *Domain* administrators of one or more MUC domains. To open the editor select it from the left hand side of the **Service** view, it can be found under the **Service Administration** sub heading.

Figure 9.1. Selecting the Multi-User Chat editor



Once selected the editor will show a tree consisting of the list of MUC domains the user can administrate with the list of rooms on that domain underneath. For a *Server* administrator this will be a list of all the MUC domains on the server, for a *Domain* administrator this will be the list of the MUC domains they are set as an administrator for.

Figure 9.2. Editor for a *Server* administrator

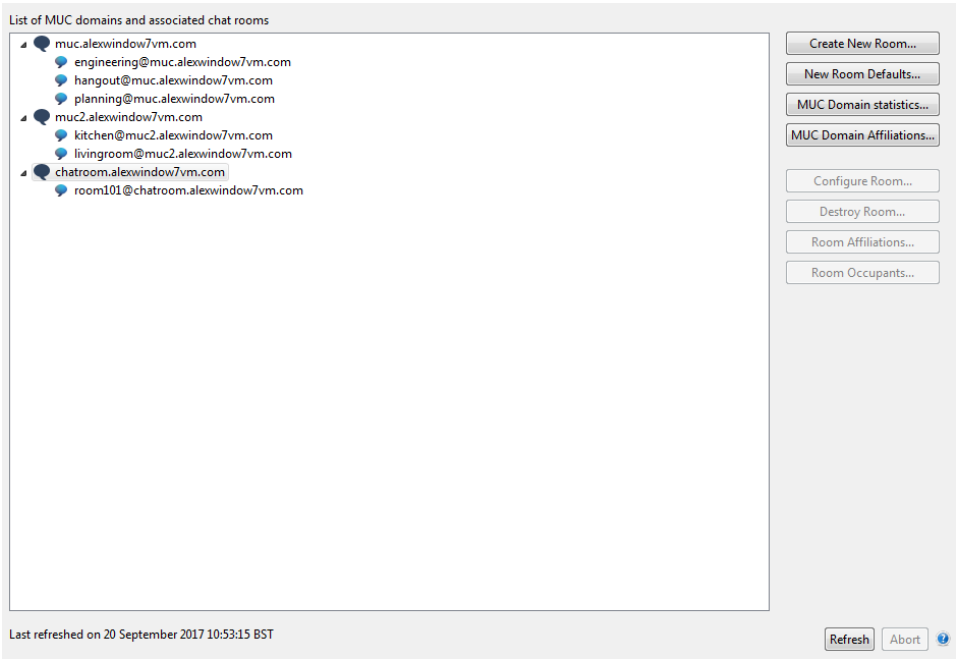
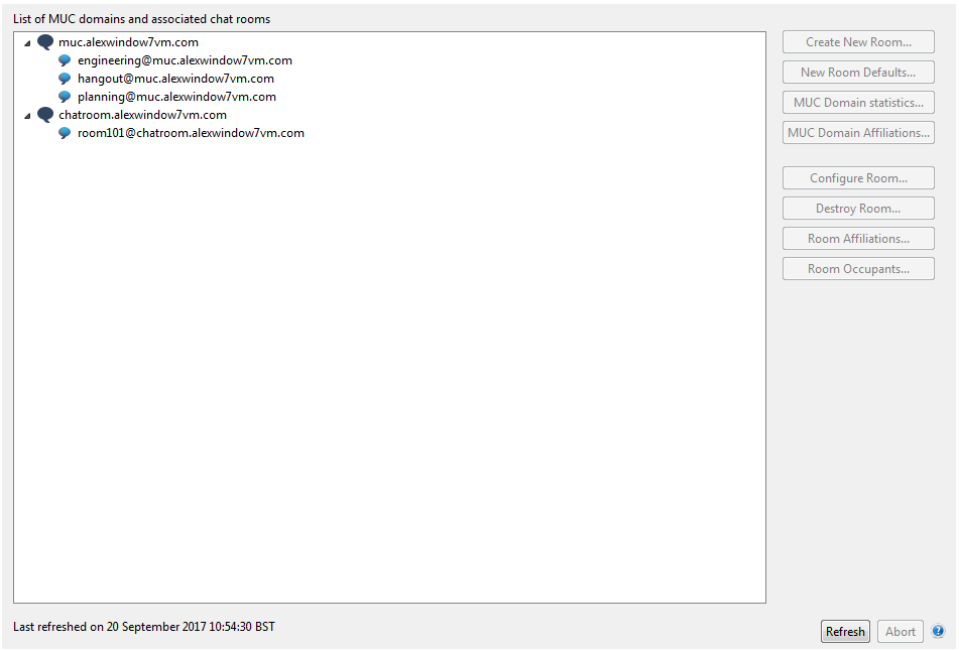
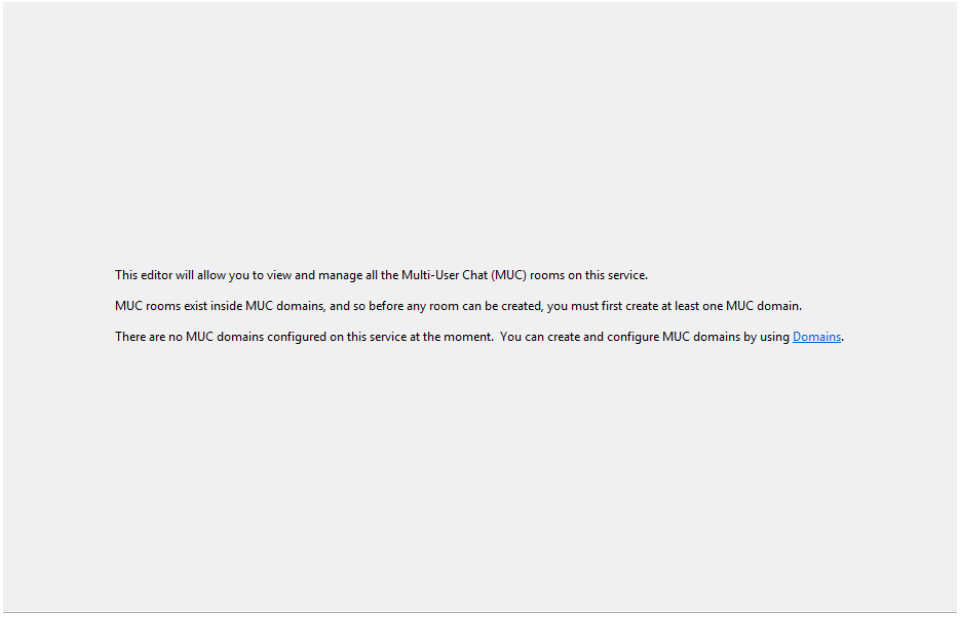


Figure 9.3. Editor for a *Domain* administrator



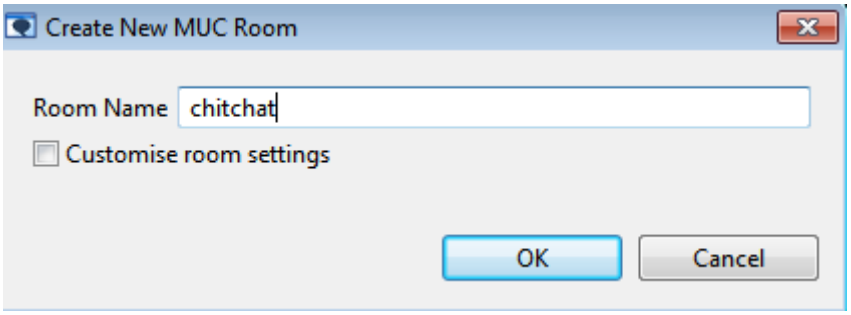
If no MUC domains are present on the server then the *Server* administrator will instead see a different view, informing them of the fact and directing them to the domain editor (Chapter 3, *Domains*).

Figure 9.4. *Server* administrator view when there are no MUC domains



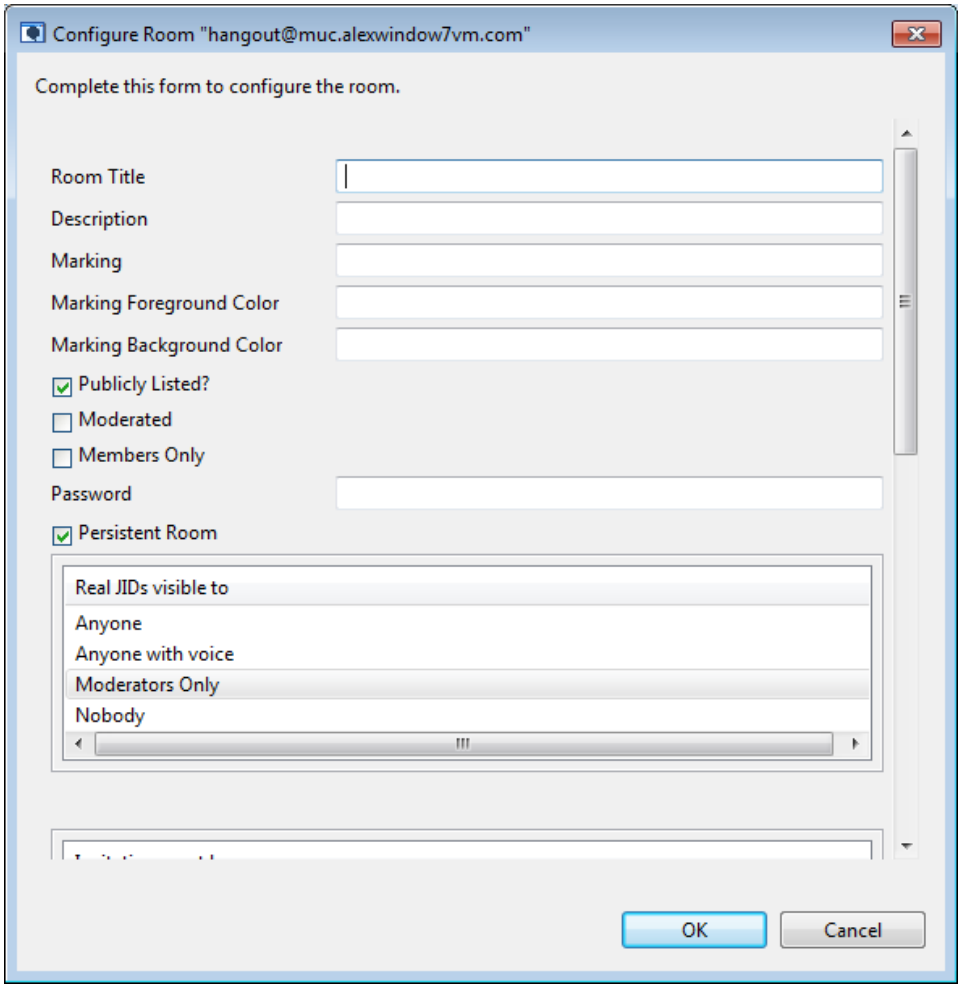
Persistent chat rooms can be created under a MUC domain, if one exists, by selecting the MUC domain and clicking the **Create Room...** button. The default room settings will be used unless the **"customise room settings"** has been selected, in which case a dialog will be displayed to allow configuration of all room settings (see Figure 9.6, “Chat Room Configuration”).

Figure 9.5. Creating a Chat Room



An existing chat room can be reconfigured using the **Configure Room...** button which presents the form shown below (the form fields are described in Section 9.3.1, “Room configuration options”).

Figure 9.6. Chat Room Configuration



Default configuration parameters for all the rooms created in a MUC domain can be configured using the **Room Defaults...** button. The button is enabled when a MUC domain is selected on the tree. On clicking the button a configuration form will be displayed to allow setting the default parameters.

An existing chat room can be destroyed using the **Destroy Room...** button. Only authorised users are able to destroy rooms.

9.5.1 Affiliations Administration using M-Link Console

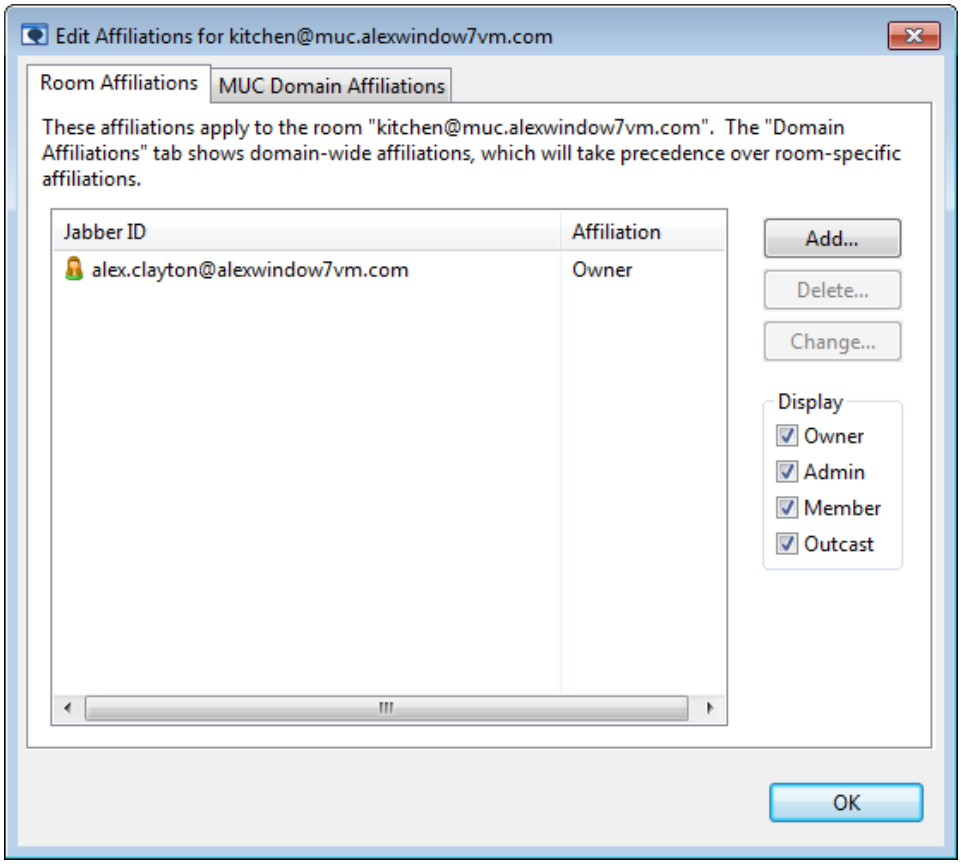
M-Link Console allows you to view and edit MUC room affiliations. Affiliations control user privileges in a MUC room, and apply whenever a user attempts to visit the room. More information about Affiliations can be found in Section 9.3.2, “Affiliations”. The following affiliations are defined:

1. Owner
2. Admin
3. Member
4. Outcast
5. None (the absence of an affiliation)

M-Link Console can be used to specify affiliations on a room on on a domain wide level. Domain wide affiliations will take priority over room specific affiliations. So if user has an affiliation set on both the room and the domain, the one on the domain will apply.

To edit the affiliations on a room select it then click on the **Room Affiliations...** button. This will bring up the affiliation editor for that room.

Figure 9.7. MUC Room Affiliations

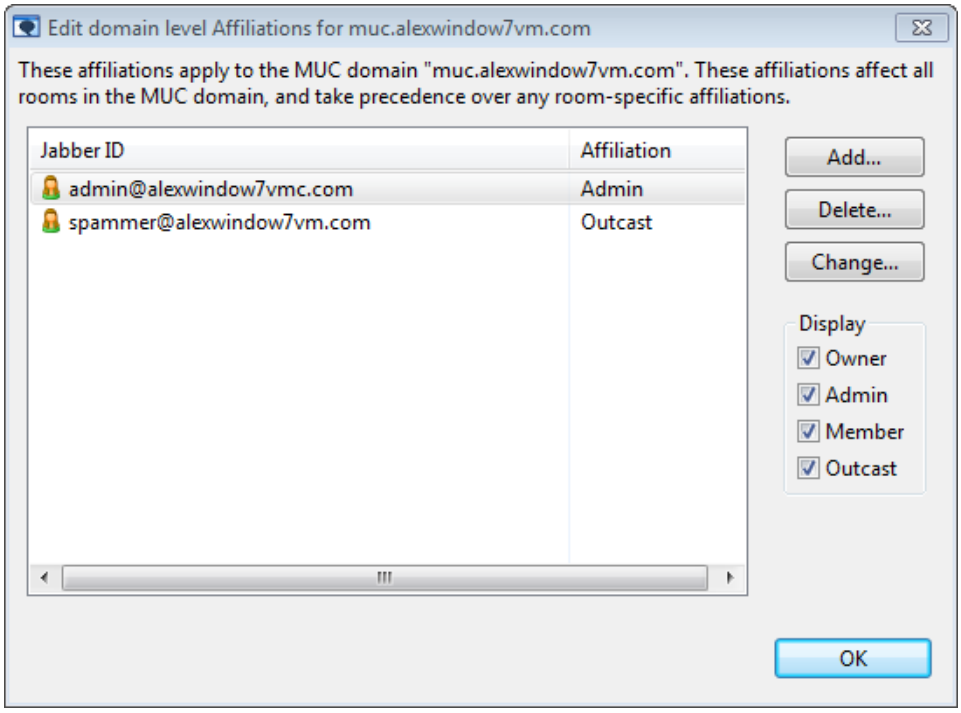


Click the **Add...** button to add a user to a specific affiliation; **click Change...** button to modify the affiliation of selected user; and **Delete...** button to remove any affiliations for the selected user.

You can also view (but not edit) the domain level affiliations for the room's domain using the *MUC Domain Affiliations* tab

To edit the affiliations on a domain select either the domain or a room on the domain then press the **MUC Domain Affiliations...**. This will bring up the MUC Domain Affiliation editor which can be used similarly to the Room Affiliation Editor.

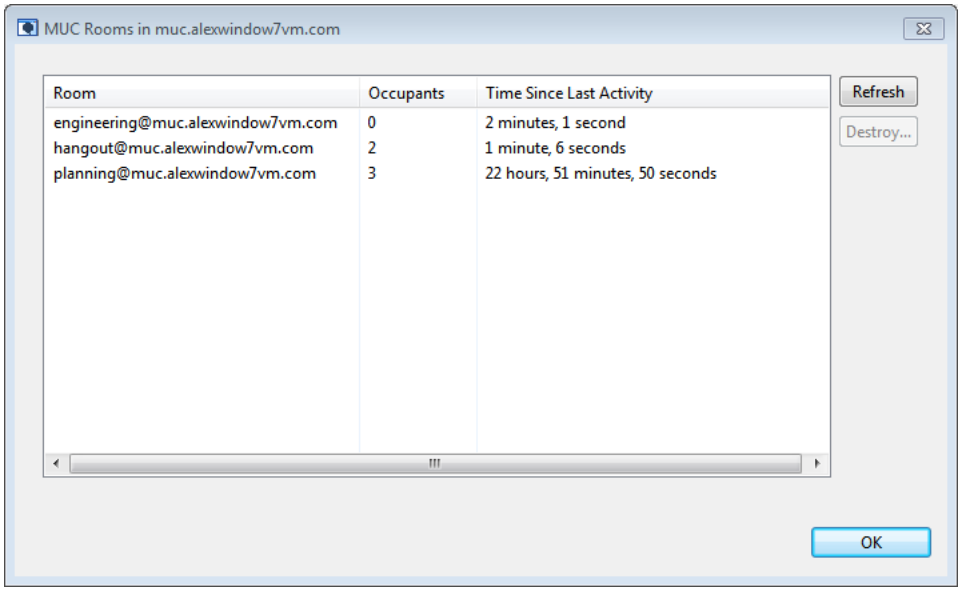
Figure 9.8. MUC Domain Affiliations



9.5.2 Room Statistics and Room Occupants

The **Room statistics...** button will be enabled when any MUC domain is selected, and when clicked it will display a dialog with information that may be useful for room administration:

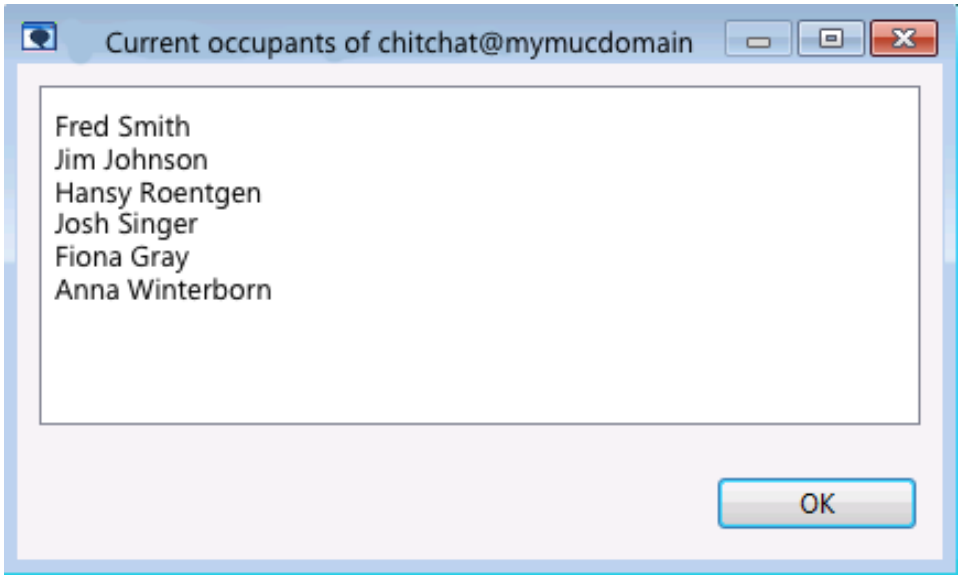
Figure 9.9. MUC Room Statistics



Viewing room statistics may help to identify MUC rooms which are moribund; by sorting the list of rooms with the **Time Since Last Activity**, you can quickly identify rooms that have been inactive for long periods of time, and - if appropriate - destroy those rooms using **Destroy...**.

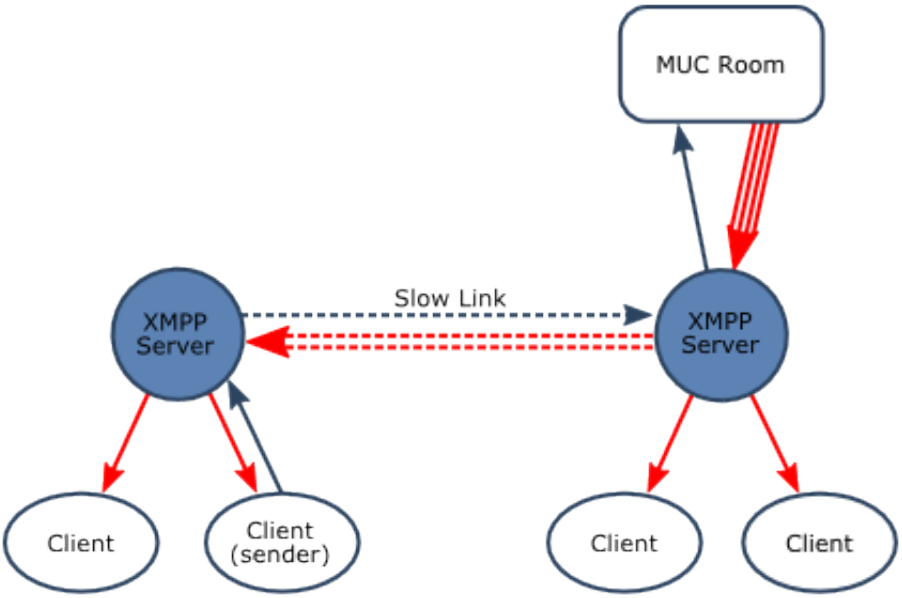
The **Room occupants...** button will be enabled when any MUC is selected, and when clicked it will display a dialog showing the current list of room occupants:

Figure 9.10. MUC Room Occupants



9.6 Federated MUC (FMUC)

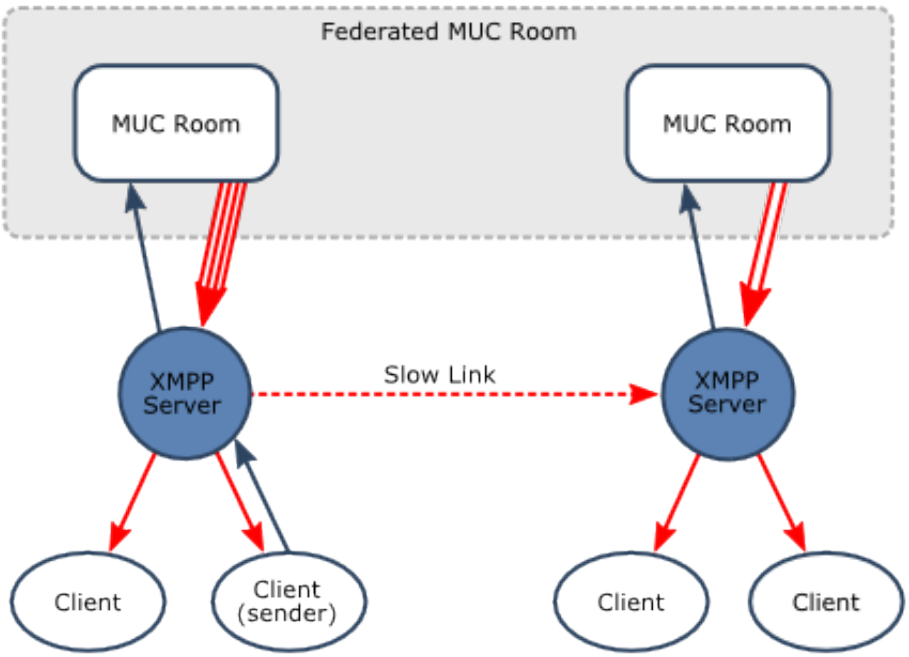
Figure 9.11. Standard MUC Architecture



Although XMPP provides a service federated over multiple servers, standard MUC rooms operate on a single server. This centralized MUC model works well in many situations, but is not ideal in all environments. In particular:

- Where there is a constrained link between a pair of servers, operating a MUC room on one server with clients on both servers leads to inefficient operation, as illustrated in the diagram above. It also prevents operation of remote clients when the link is not working.
- In a cross-domain environment, it is undesirable to have clients directly accessing a MUC room in the remote domain

Figure 9.12. Federated MUC Architecture



Federated MUC (FMUC), specified in *XEP-0289*: Federated MUC for Constrained Environments (https://xmpp.org/extensions/xep-0289.html), addresses these issues. FMUC enables MUC rooms on multiple servers to federate and provide a single MUC room. This provides optimized performance for constrained links, as shown in the diagram above. More information on FMUC is provided in the Isode whitepaper "Federated Multi-User Chat: Efficient and Resilient Operation over Slow and Unreliable Networks", available at https://www.isode.com/whitepapers/federated-muc.html.

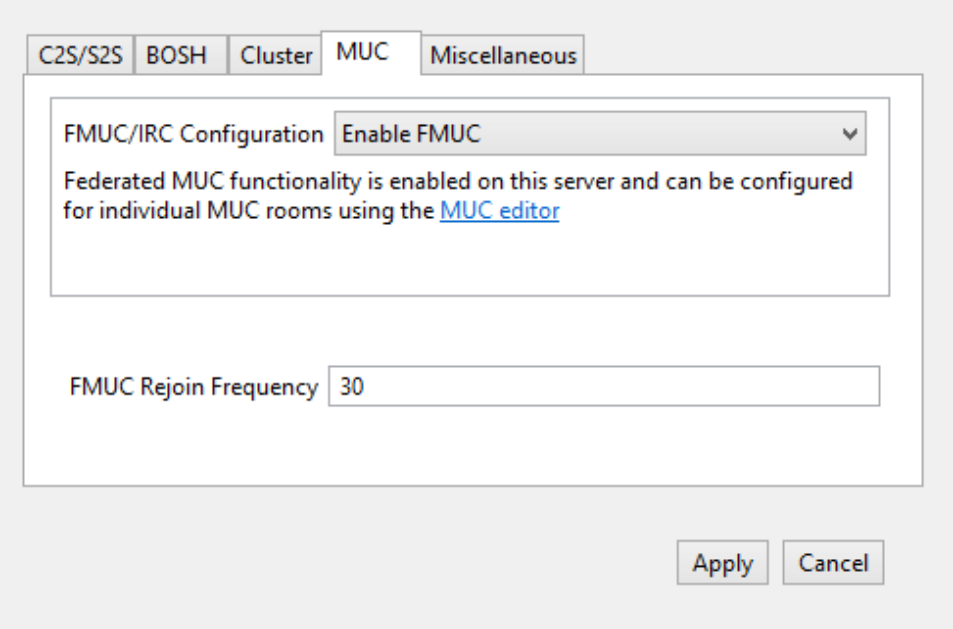
FMUC is enabled server-wide (see Section 9.6, “Federated MUC (FMUC)”); individual MUC rooms can be configured to participate in a federated FMUC room, simply by including the names of the federated rooms to which messages are sent. FMUC is simply configured using a set of standard MUC rooms that will work together.

FMUC configuration is per-room, but first requires FMUC to be enabled for the server.

9.6.1 Enabling FMUC for the server

To allow MUC rooms to be federated first enable the FMUC functions of the server. Using M-Link Console select the **General** editor and go the the **MUC** tab; then select the **Enable FMUC** option from the **FMUC/IRC Configuration** combo. Once selected the **FMUC Rejoin Frequency** will be configurable in the provided text box.

Figure 9.13. Enabling FMUC for the server

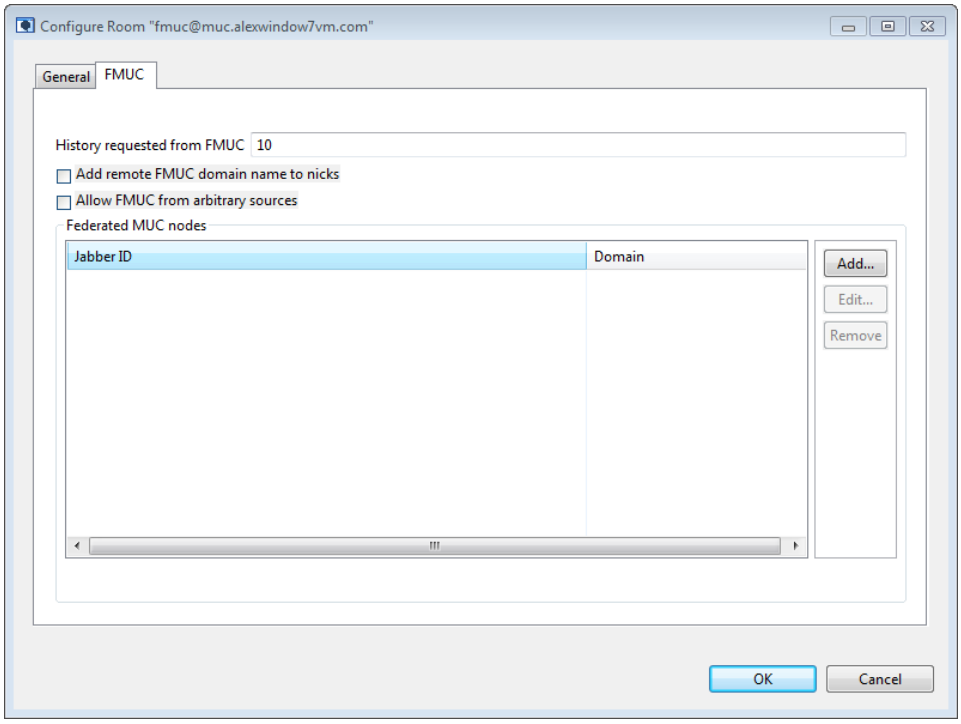


Selecting **Apply** will cause the server to be updated, a restart may be required for the settings to be applied.

9.6.2 Configuring federation of a MUC room

Once FMUC is enabled on the server then M-Link Console will allow the managment for FMUC configuration of a MUC room through the **Multi-User Chat** editor. To enable federation for a MUC room, open the room configuration dialog for the room as described in Section 9.3, “Creating and configuring rooms”, then select the **FMUC** tab, this will display the FMUC configuration form for the MUC room.

Figure 9.14. Configuring FMUC for a room



Two key fields of this form are:

- "**Allow FMUC from arbitrary sources**" will, if enabled, accept requests to start federating from any other MUC, irrespective of whether it is in the configured node list or not.
- "**Federated MUC nodes**" is a list of the MUCs that this MUC is configured to federate with - note that while it is possible to federate with many nodes, there must be no 'loops' in the config (that is: it must be an acyclic graph). So to have the rooms *demo@conference.example.com* and *sample@rooms.server.local* federate you would add *sample@rooms.server.local* to the **Federated MUC nodes** list of *demo@conference.example.com*, and add *demo@conference.example.com* to the **Federated MUC nodes** list of *sample@rooms.server.local*.

Once the required configuration is set, select **OK** to save the settings.

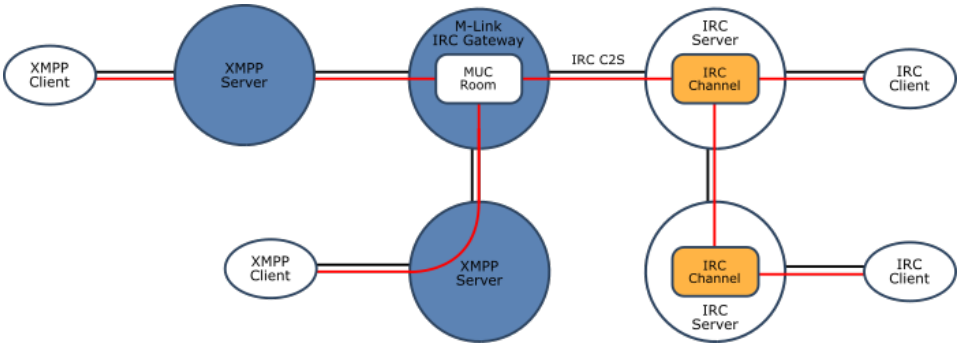
9.6.3 Things to note

- When a federated MUC becomes unavailable it may take some time before the link is considered 'dead' and remote occupants in the MUC are marked as having left the room. It is possible for occupants of different nodes of an FMUC room to see messages arrive in a slightly different order when either messages are sent at the same time or the network link between servers is slow.
- You can only federate between local and remote MUC rooms, you cannot federate between two MUC rooms hosted on the same M-Link instance.
- If FMUC is enabled for the server, anyone able to create a MUC room can then configure it to federate with a remote host - this provides a mechanism for potential abuse if your users are not trusted.

9.7 IRC Gateways

Internet Relay Chat (IRC) is a widely deployed real time text chat service. Although IRC can used for 1:1 user chat, it is primarily used for group chat, using "channels". M-Link provides a capability to interconnect XMPP with IRC, as illustrated below.

Figure 9.15. M-Link IRC Gateway



The M-Link IRC gateway works by associating an IRC channel with an XMPP MUC room. This gives a number of advantages:

- XMPP users joining a normal MUC room, where the room happens to have IRC participants in it, do not need to be aware of IRC in any way
- IRC users operate in a normal channel and receive messages from XMPP users who appear to them as IRC channel members
- Straightforward migration from IRC to XMPP can be achieved, with the IRC Gateway being removed once there are no longer any IRC users.

Further details on the architecture, and comparison to other approaches, is available in the Isode whitepaper "Interconnecting XMPP and IRC", available at https://isode.com/whitepapers/interconnecting-xmpp-and-irc.html

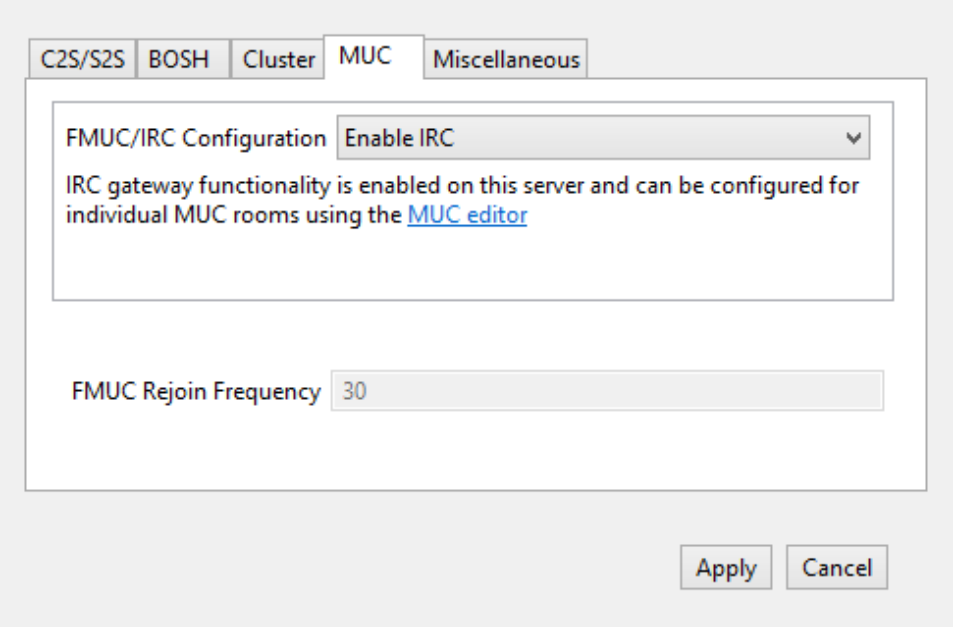
Once IRC Gateway functionality has been enabled for an M-Link service (see Figure 9.16, “Enabling IRC Gatewaying for the server”), individual MUC rooms can be configured to IRC channels as required (see Figure 9.17, “Configuring IRC Gatewaying for a MUC room”).

IRC gatewaying is per-room, but first requires the gateway to be enabled for the server.

9.7.1 Enabling IRC Gatewaying for the server

To enable the IRC Gateway functions of the server using M-Link Console select the **General** editor and go the the **MUC** tab; then select the **Enable IRC** option from the **FMUC/IRC Configuration** combo.

Figure 9.16. Enabling IRC Gatewaying for the server

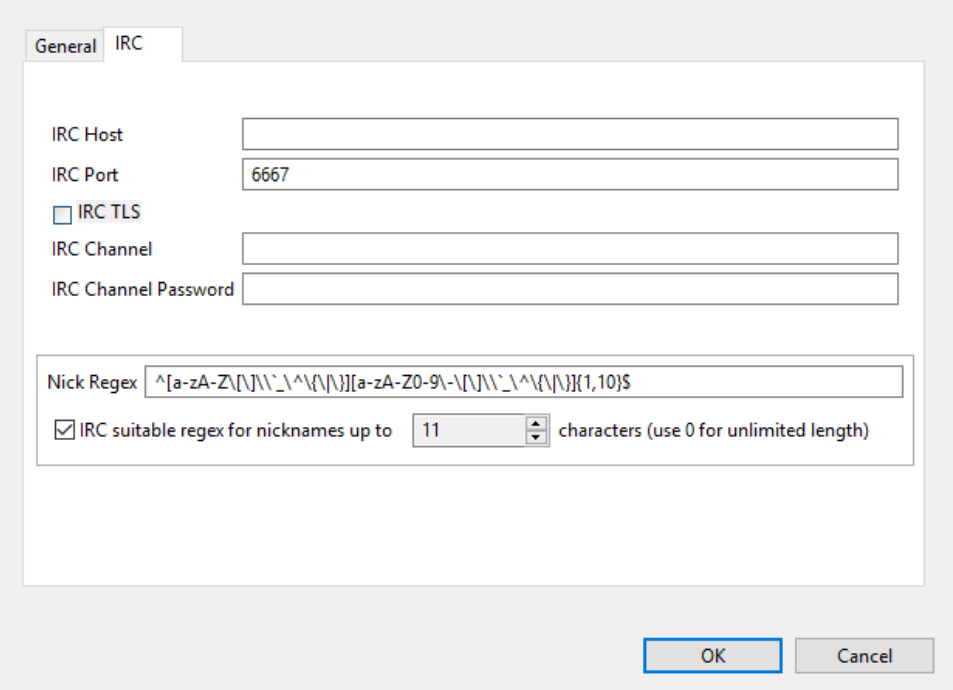


Selecting **Apply** will cause the server to be updated, a restart may be required for the settings to be applied.

9.7.2 Configuring gatewaying of a MUC room to an IRC channel

Once IRC Gatewaying is enabled on the server the management of the gatewaying for a given MUC room can be configured in M-Link Console via the **Multi-User Chat** editor. To enable or configure gatewaying of a MUC room, bring up the configuration dialog for the room as described in Section 9.3, “Creating and configuring rooms” and select the **IRC** tab. In the displayed form set the **IRC Host**, **IRC Port**, **IRC TLS**, **IRC Channel** and **IRC Channel Password** to the appropriate values for the IRC server and channel you want the MUC to gateway onto.

Figure 9.17. Configuring IRC Gatewaying for a MUC room



IRC places additional restrictions on names in a channel beyond those that XMPP places on names in a MUC and as such it is useful to set a limit for the nicknames of users in the MUC to those that are supported by IRC. This can be done by setting an appropriate regular expression for the room's **Nick Regex**. M-Link Console can generate a regex that matches the typical requirements for IRC nicknames, or you can enter a regex manually. For an IRC server which is configured to accept nicknames consisting of one letter/special character followed by up to eight letter/digit/special characters (in accordance with RFC 2812), then an appropriate regexp would be *^[a-zA-Z\[\]\\`_\^\{\|\}][a-zA-Z0-9\-\[\]\\`_\^\{\|\}]{1,8}$*

9.7.3 Things to note

- Only the MUC messages and occupancy are gatewayed - direct interactions between occupants such as private messages and file transfers are not supported.
- FMUC and IRC gatewaying can not be enabled for the same MUC room.
- All MUC configurations gatewaying a room onto an IRC channel should set the IRC TLS option exactly the same way when these are for the same IRC server - e.g. you should not have one room using TLS and another using non-TLS if both rooms gateway to the same IRC server.
- All MUC configurations gatewaying a room onto an IRC channel should refer to IRC servers in a consistent way. When referring to an IRC server, always refer to it in exactly the same way in the configuration of different MUC rooms - e.g. you should not refer to it as 'irc' in one room, 'irc.isode.net' in another and '172.16.3.101' in another if these are all the same server. It is legal to have different MUCs gatewaying to different servers - e.g. one room can gateway to 'irc.isode.net' and another to '172.16.3.101' as long as these are not different addresses for the same IRC server.

Chapter 10 Publish-Subscribe, PEP, and FDP

This chapter discusses configuration of M-Link Publish-Subscribe and related services.

10.1 Overview

Publish-Subscribe (PubSub) [*XEP-0060*] provides a powerful *publish-subscribe* facility via XMPP. Isode M-Link aims to provide a complete PubSub implementation.

The *Personal Eventing Protocol* (PEP) [*XEP-0163*] provides a personal variant of PubSub typically used for rich presence use cases.

Internally, M-Link Server uses PEP for various storage tasks, including private XML storage [*XEP-0049*] and offline messages [*XEP-0160*].

Form Discovery and Publishing (FDP) [*XEP-0346*] is implemented using PubSub and provides a mechanism to allow the XMPP Server to store a list of form templates that can be enumerated and retrieved by an FDP-aware client.

10.2 Service configuration

User specific data is stored within the users' personal directories on the filesystem, as given by the user directory (see Section H.1.1, “Users Root Directory”).

Service data for PubSub domain is stored in the directory tree defined by Section H.1.112, “Publish-Subcribe Directory”.

10.3 Node configuration

Node configuration is as per the standard.

10.4 Using M-Link Console to manage Publish-Subscribe services

M-Link Console can be used to administrate *Publish-Subscribe* (PubSub) services using the **Publish-Subscribe Administration** editor. Note that to be able to setup PubSub nodes, you must have at least one PubSub domain configured (see Section 3.2, “Using M-Link Console to manage domain configuration”).

Applications using PubSub will typically create nodes using some application-specific naming convention. A new PubSub node will initially have an *owner* affiliation matching that of the creator's JID; additional affiliations may be added later. Apart from administrators, only users who have appropriate affiliations may make changes to a given PubSub node (see Figure 10.5, “Managing PubSub node affiliations”).

PubSub nodes hold application-specific data in the form of one or more items, each of which is an XML fragment. The XMPP service itself does not impose any constraints on the contents or format of these items (other than that they be valid XML). So while M-Link Console is able to view the contents of PubSub nodes, it will not be able to validate this information, or to render it in any form other than raw XML.

In most cases, you will use M-Link Console to view the current PubSub setup: to see what nodes exist and see who is subscribing to individual PubSub nodes. While it is possible to use the editor to add, change or delete PubSub nodes and their contents, this ought only to be done if you have an understanding of the impact of such changes on any applications which may be using the PubSub configuration in question.

The editor uses a tree structure to display all the PubSub domains (blue icons) which the user can administrate. For a *Server* Administrator this will be all the PubSub domains on the server, for a *Domain* Administrator it will be the PubSub domains they are an administrator of. Individual PubSub nodes inside the domains are displayed with green icons:

Figure 10.1. PubSub view for *Service* Administrators

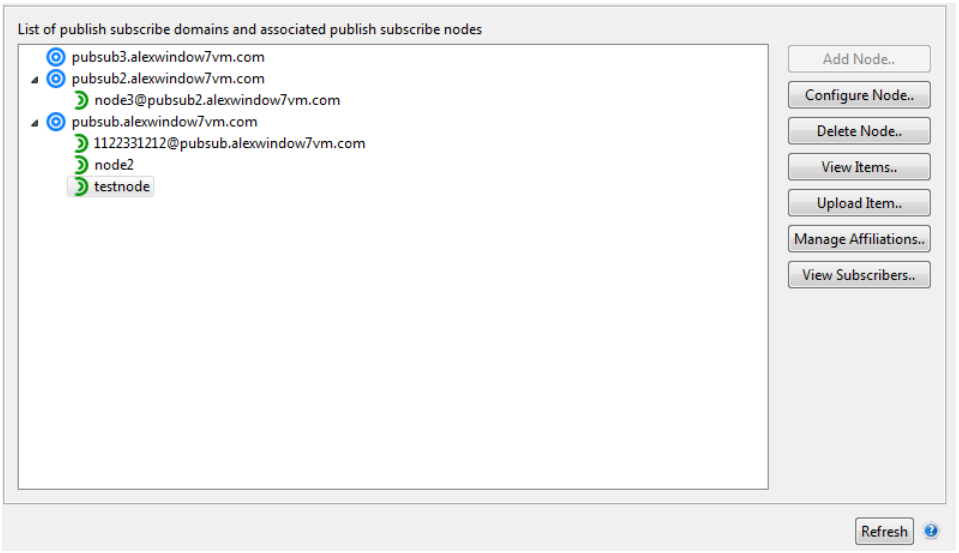
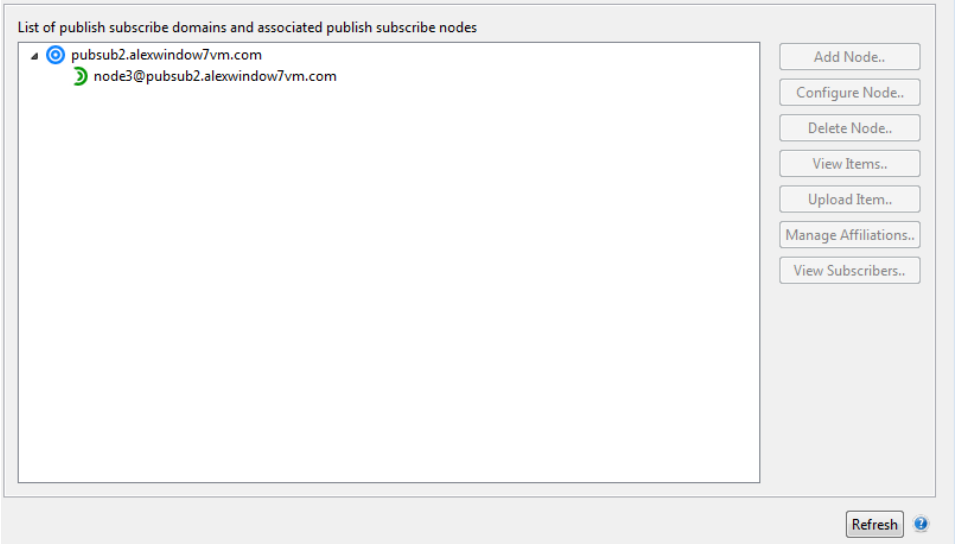
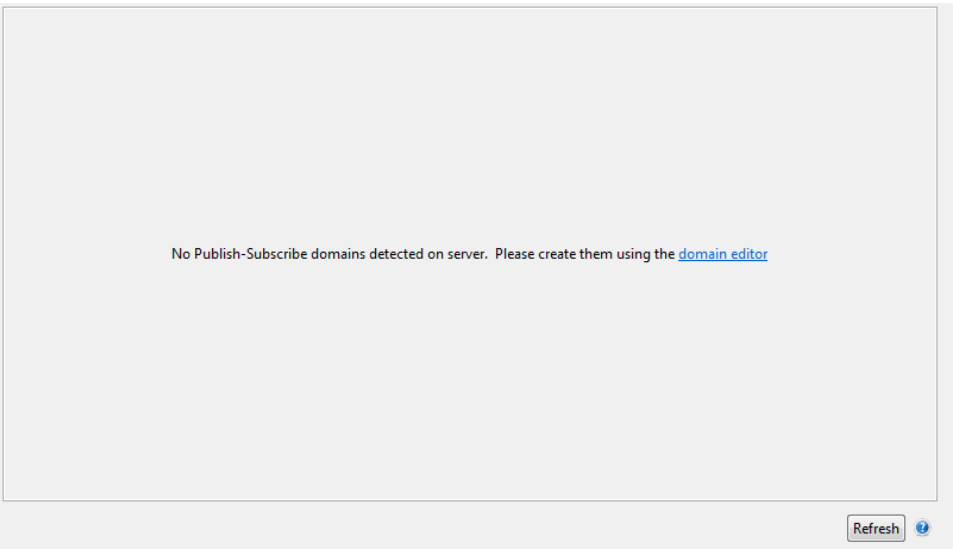


Figure 10.2. PubSub view for *Domain* Administrators



If no PubSub domains are present on the server then the *Server* administrator will instead see a different view, that informs them of the fact and directs them to the domain editor (Chapter 3, *Domains*).

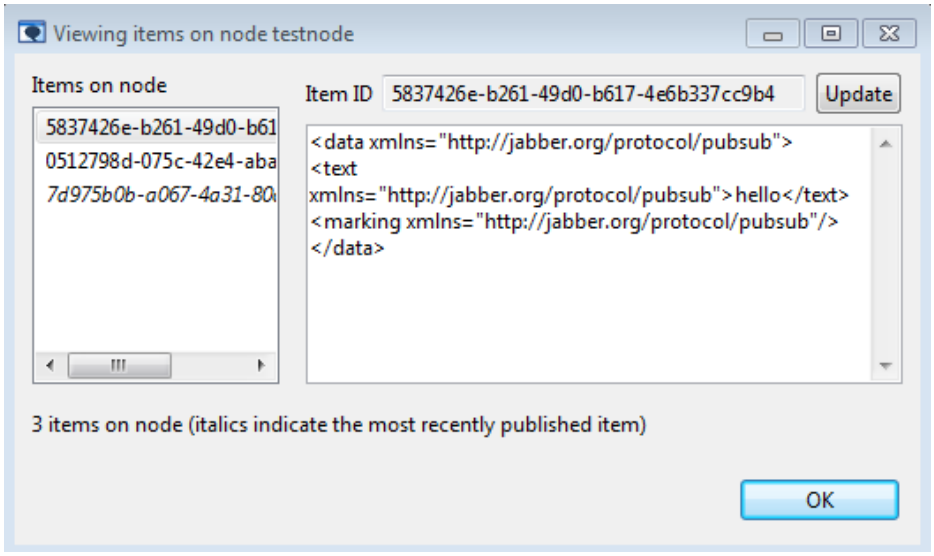
Figure 10.3. PubSub view for when no domains are configured



Selecting a PubSub node enables various options:

- Using **Configure Node..** allows you to view or modify the current configuration of a PubSub node - for example, to change the maximum number of items stored on the node.
- **Delete Node..** will delete the selected node, as well as any items that were stored on the node.
- **View Items..** allows you to display the contents of the selected PubSub node. Items on a PubSub node are identified by an *Item ID*, and have an XML payload. If multiple items are stored on the node, there is no guarantee as to what order the items will be displayed (the collection of items is a set rather than a sequence), but M-Link Console will indicate which item was the most recently published one using italics.

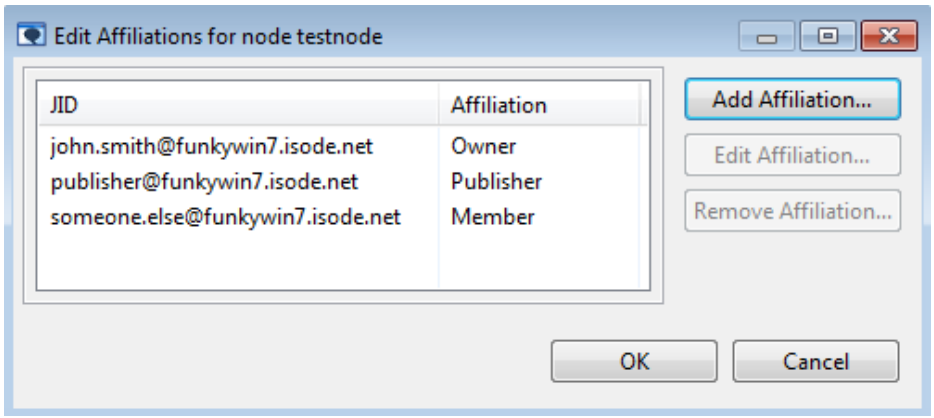
Figure 10.4. Viewing items on a PubSub node



M-Link Console allows you to replace the contents of any existing item by selecting it and then using the **Update** button.

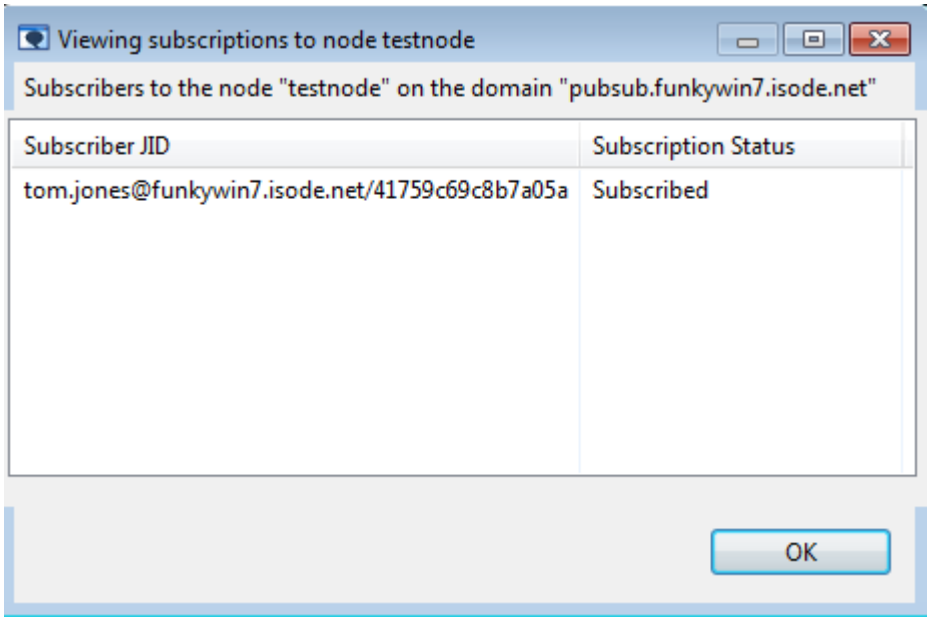
- **Upload Item..** allows you to upload a new item to the selected node. This operation may result in an existing item being removed (if the number of items on the node is already at the maximum number for that node). M-Link Console will prompt you for the name of a file whose contents are to be uploaded, and will check that the file contents are XML, but beyond that it performs no validation on the data.
- **Manage Affiliations..** allows you to view and configure the list of users who are allowed to make changes to the selected node. Initially, a newly created node will have a single owner affiliation corresponding to the JID of its creator.

Figure 10.5. Managing PubSub node affiliations



- **View Subscribers..** will display a list showing all the current subscribers. This may be a useful check to perform if you are considering deleting a PubSub node.

Figure 10.6. Viewing subscribers to a PubSub node



10.5 Using M-Link Console to manage Form Discovery and Publishing

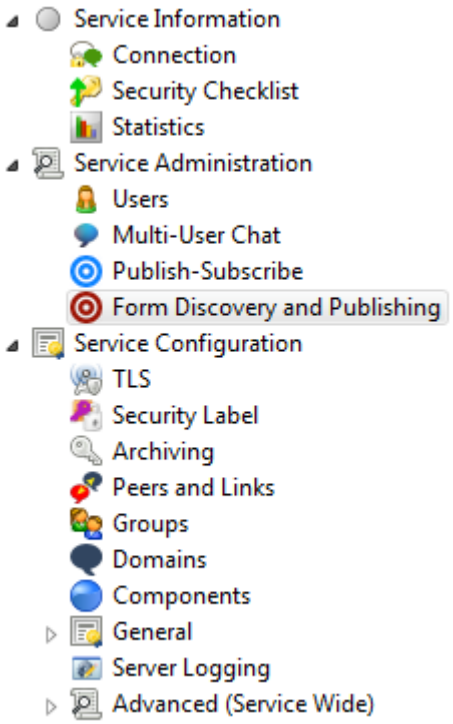
Form Discovery and Publishing (FDP) is supported by M-Link Server and can be configured by M-Link Console. FDP is implemented using PubSub.

FDP provides a mechanism to allow the XMPP Server to store a list of form templates that can be enumerated and retrieved by an FDP-aware client. Such a client may allow a user to choose from the list of form templates, and then present a chosen template in a way that lets the user "fill in" the form. Once a user has filled in a form, it is submitted back to the XMPP Server, which will notify any interested entities that a new copy of that form has been submitted, allowing them to request a copy of the filled in form.

A commonly used example is the case of a MEDEVAC (Medical Evacuation), following a casualty in the field. When such an event occurs, many people need to take actions (from lawyers to helicopter pilots) and many more may need to be informed. With FDP, an arbitrary number of entities can register an interest, so that whenever someone submits a completed MEDEVAC form, all of those interested partied will immediately be notified.

M-Link Console provides the **Form Discovery and Publishing** editor that allows an administrator to manage FDP configuration. The editor can be found under the **Service Administration** heading. It will be available for all *Service* Administrators and any *Domain* administrators who are administrators of one or more FDP Domains.

Figure 10.7. Selecting the Form Discovery and Publishing editor



Since FDP is implemented using PubSub, any FDP configuration will be visible in M-Link Console's PubSub editor (see Section 10.5.7, “Viewing FDP configuration in the PubSub editor”). However, since the PubSub editor has no special knowledge of FDP and cannot validate FDP-specific configuration changes, it is recommended that you do not use the PubSub editor to make changes to FDP configuration.

When selected the editor gives a tree view listing all the FDP domains the user can administrate with the domains FDP topics underneath. For a *Server* administrator this will be all FDP domains on the service, for a *Domain* Administrator it will be the FDP domains they can administrate.

Figure 10.8. Form Discovery and Publishing edior for *Server* administrator

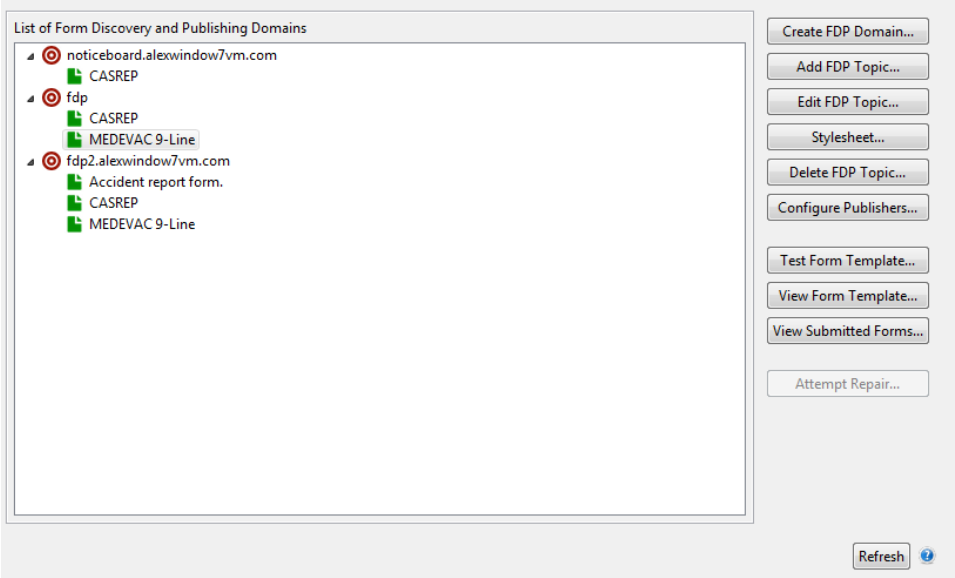
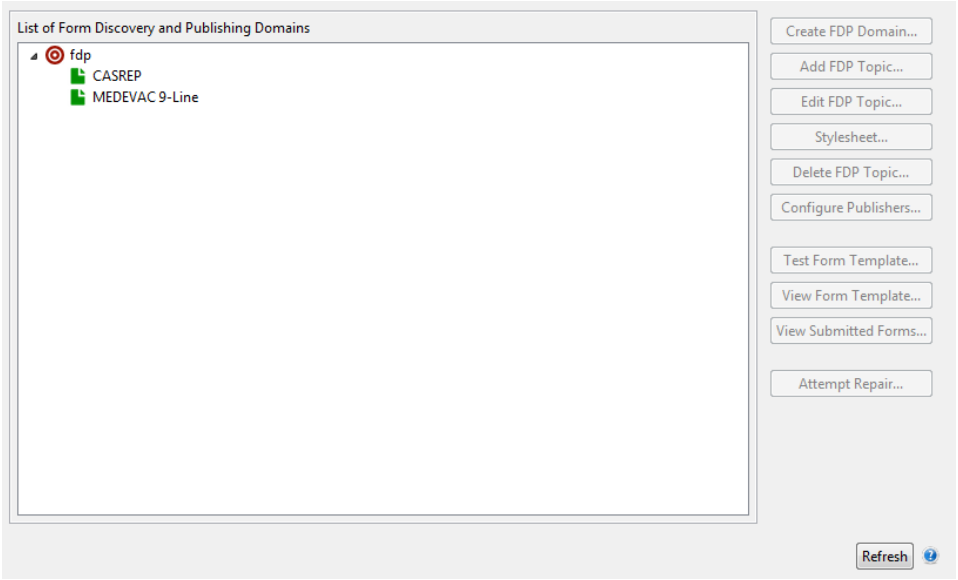
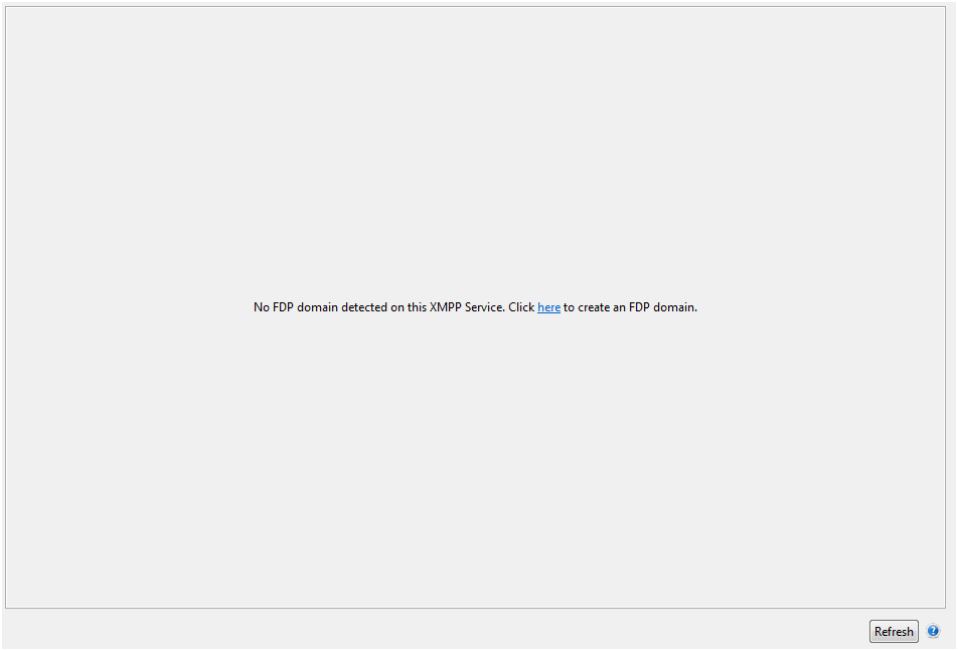


Figure 10.9. Form Discovery and Publishing edior for *Domain* administrator



If no FDP domains are configured on the service, then the *Server* Administrator will see a message informing them of this fact which will include a link to open the **Create FDP Domain** dialog (see Section 10.5.1, “Creating an FDP domain”).

Figure 10.10. Form Discovery and Publishing edior when no FDP domains configured



The functionality provided by M-Link Console for managing FDP includes:

- Creating an FDP domain (see Section 10.5.1, “Creating an FDP domain”)
- Adding and removing FDP topics (see Section 10.5.2, “Adding and removing FDP topics”)
- Editing existing FDP topics (see Section 10.5.3, “Editing existing FDP topics”)
- Testing an FDP template (see Section 10.5.4, “Testing an FDP template”)
- Viewing existing form templates and viewing submitted forms (see Section 10.5.5, “Viewing existing FDP topics”)

- It is also possible to view "raw" FDP configuration from within the PubSub editor (see Section 10.5.7, “Viewing FDP configuration in the PubSub editor”).

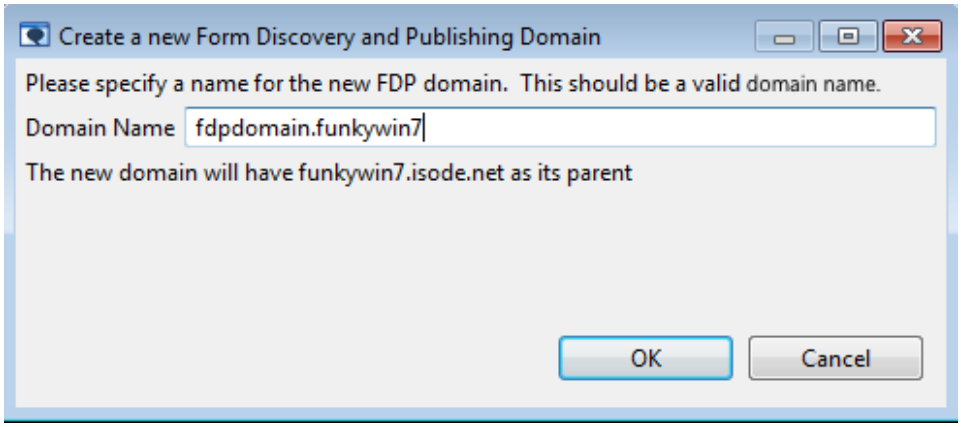
10.5.1 Creating an FDP domain

FDP form templates and submitted forms are held inside an "FDP domain" and so you must create an FDP domain before you can load form templates.

As specified in [*XEP-0346*], an "FDP domain" is a normal PubSub domain which has a type of `urn:xmpp:fdp:0`. You could create an FDP domain by by creating an PubSub domain and then setting its type via the the **Domains** editor (see Section 3.2, “Using M-Link Console to manage domain configuration”).

However, M-Link Console's FDP editor provides the ability to create FDP domains automatically, without the need to set the type. This can be accessed by selecting the **Create FDP Domain...** button or selecting the link in the no FDP domains configured view described above. This will open the **Create FDP Domain** dialog.

Figure 10.11. Creating a new FDP domain

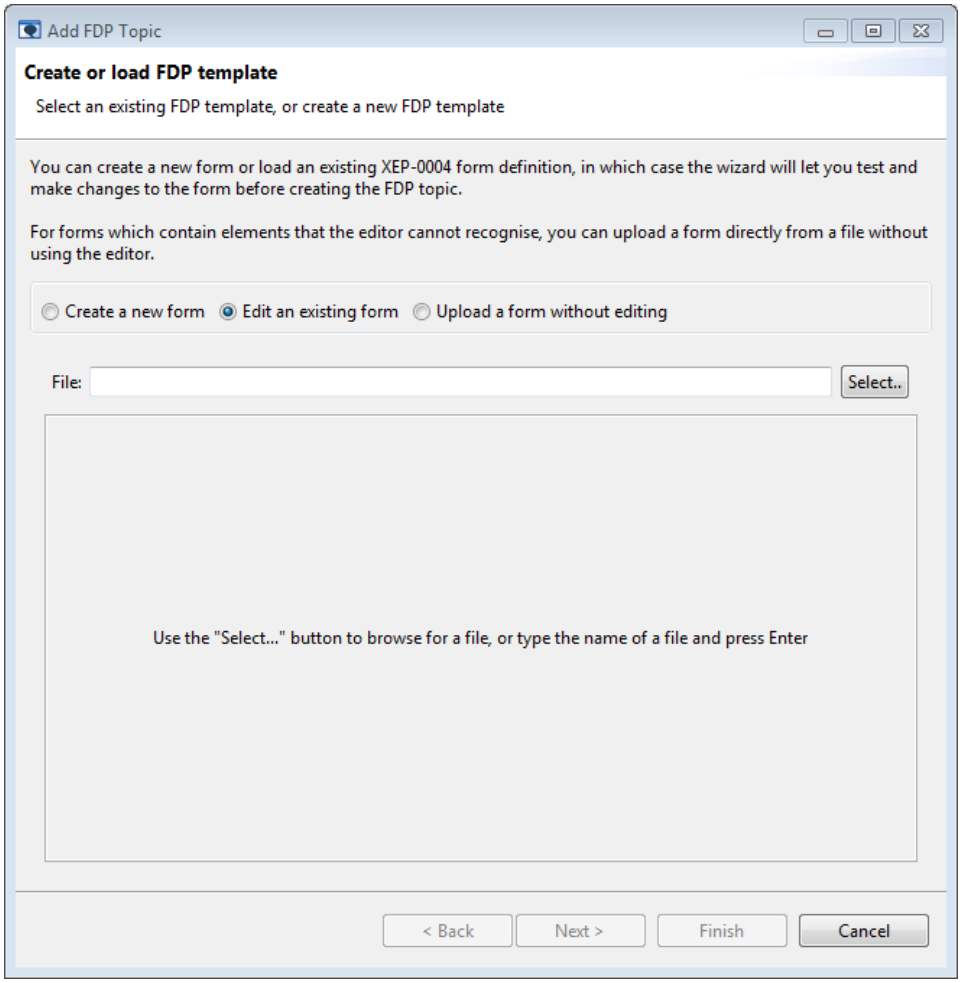


The domain name you choose can be any valid domain name, but typically will be one that is meaningful for users of FDP on this XMPP service. Once the domain has been created, it will appear in the tree view (it will also be shown by the Domain and PubSub editors), and you can add new FDP form templates.

10.5.2 Adding and removing FDP topics

An FDP domain contains zero or more FDP topics, where each topic contains two pubsub nodes: a *template* node that contains the form template, and a *submitted* node that will contain a number of filled in forms submitted by FDP-aware applications. The *template* and *submitted* node pair for any given form are called an FDP *topic* by M-Link Console.

Figure 10.12. The add FDP topic wizard



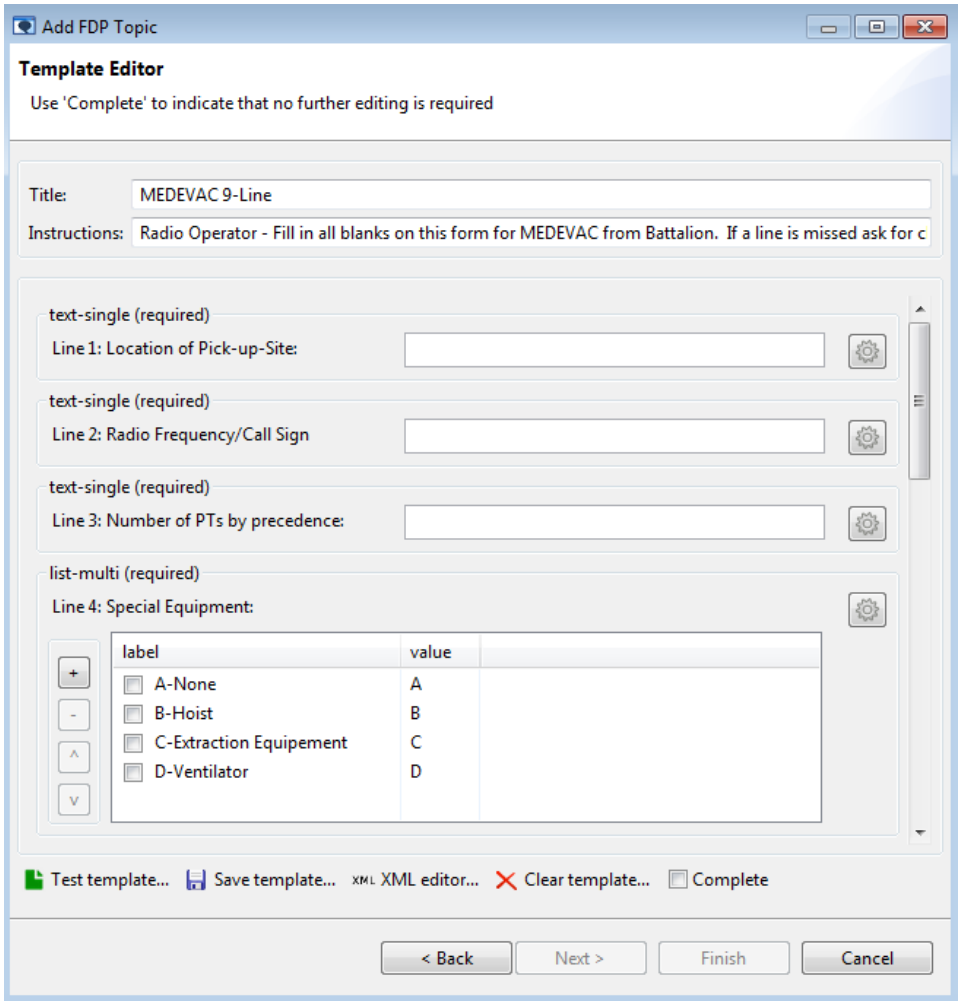
The **Add FDP Topic...** wizard is used to create a new topic. This allows you to upload or create an FDP template, before configuring the topic and uploading it.

10.5.2.1 Using the FDP template editor

After opening the wizard, a selection page is displayed. Here you have the option to upload and edit an existing FDP template, create a new FDP template, or upload an existing FDP template without editing it

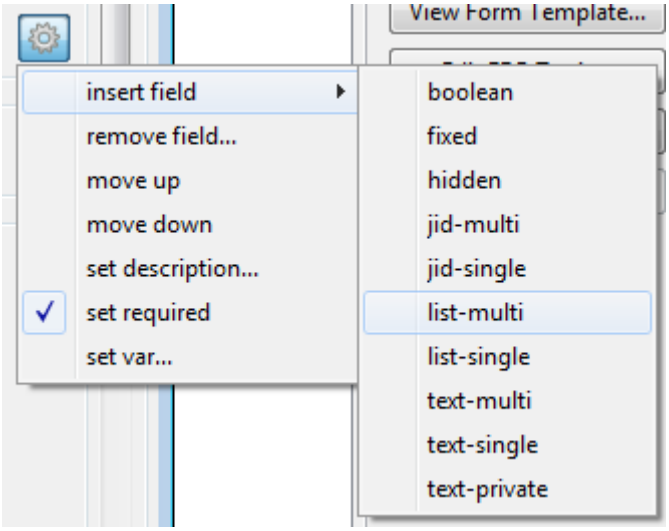
When loading an existing template, the specified XML file *must* be a valid XML document, meeting the requirements for a XEP-0004 data form. If the provided template is invalid, M-Link Console will present an error dialog, indicating the cause of the error if possible. In this case you will be unable to proceed with the selected template and it should be fixed manually before trying to load the file again. If the FDP template is valid, M-Link Console will display a preview of the selected file and allow you to proceed. If you did not select *Upload a form without editing* then the selected file will be loaded in the editor.

Figure 10.13. The FDP template editor showing a MEDEVAC 9-Line FDP template



The editor will display a visual representation of the form as it might be presented by an FDP client. Using the **Add field...** button displayed at the bottom of the editor content area, you can append fields to the currently displayed template. Fields must be of a specific type, and any fields of an unknown type will be rendered as a text-single field, as per XEP-0004. Inserting fields is possible by selecting the configuration icon, displayed to the right of each field and navigating to the **add field** menu. By specifying a field type from this menu, for example 'text-single', a new form field of the specified type will be inserted after the selected field.

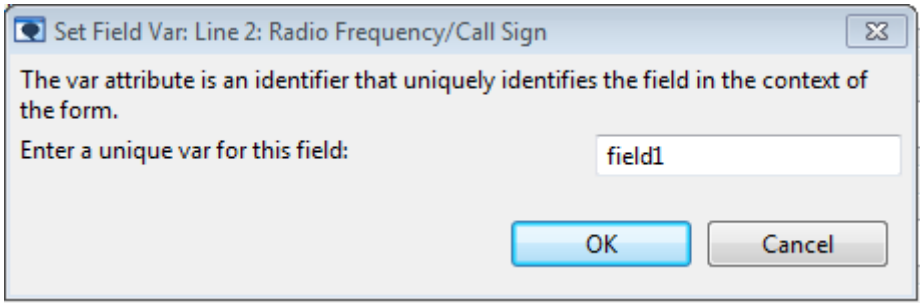
Figure 10.14. FDP template editor field options



As well as inserting fields, the configuration menu contains options to remove and modify fields. By selecting **remove field...**, a dialog will be presented asking you if you want to remove the currently selected field. You can also change the position of the field by moving it up or down, using the **move up** and **move down** options.

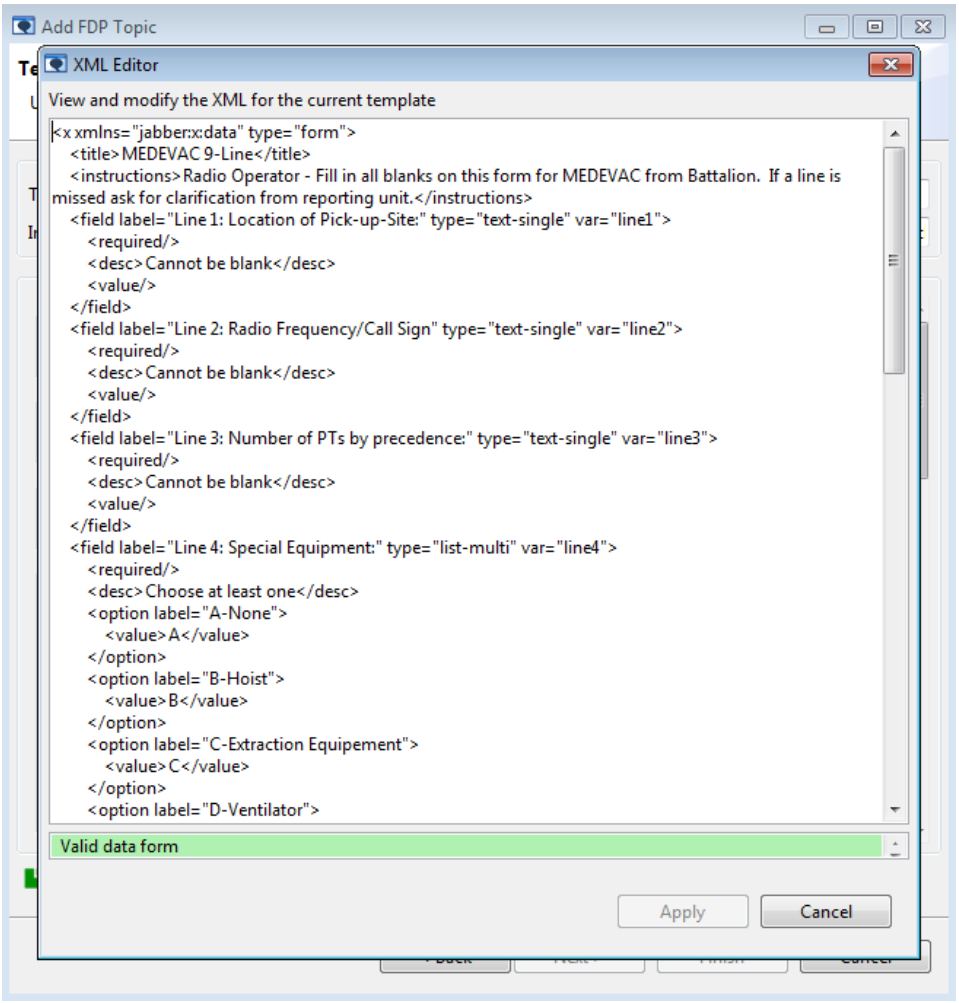
Selecting the **Clear template...** button will present a dialog asking if you want to clear the current template. Selecting **OK** will clear the currently displayed field, removing all existing fields, selecting **Cancel will cancel the operation without modifying the template.**

Figure 10.15. Editing a var attribute for a form field



Selecting the **set var...** option opens a dialog to edit the 'var' attribute for the current field. The var attribute is an identifier for the field which *must* be unique, invalid var attributes will not be permitted. Selecting **set description...** opens a dialog to edit the description for the current field. This is often displayed as a tooltip by the FDP client. Selecting the **set required...** option will present a dialog to specify whether the selected field is mandatory or optional, the required status is indicated in the title above each field.

Figure 10.16. The XML editor dialog for an FDP template



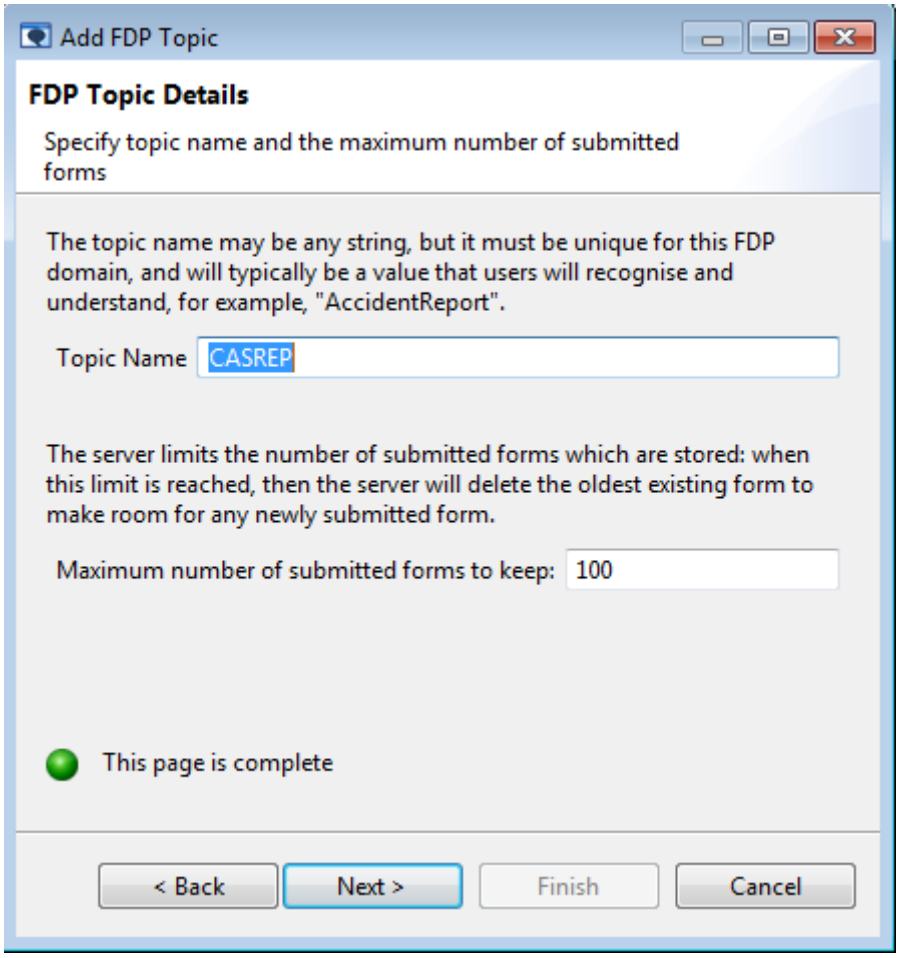
The **XML editor...** button opens an editor, allowing you to view and modify the XML for the current form. The editor will attempt to validate any XML you provide. If the XML provided is invalid, a warning or error message will be presented and you will be unable to apply any changes. It is only possible to click **Apply** when *all* the XML is valid. When you have finished making changes to the XML, select **Apply** and the changes will be applied to the currently displayed form.

10.5.2.2 Configuring the Topic

Once you have finished making changes to the template, check the **Complete** box and select the **Next** button to proceed to the next page.

On the next page, you can specify a name for the new FDP topic, and configure the maximum number of submitted forms the XMPP server should retain. It is possible to adjust this maximum value once the topic has been created (see Section 10.5.7, “Viewing FDP configuration in the PubSub editor”). It is also possible to edit the template for an existing node once the topic has been created (see Section 10.5.3, “Editing existing FDP topics”).

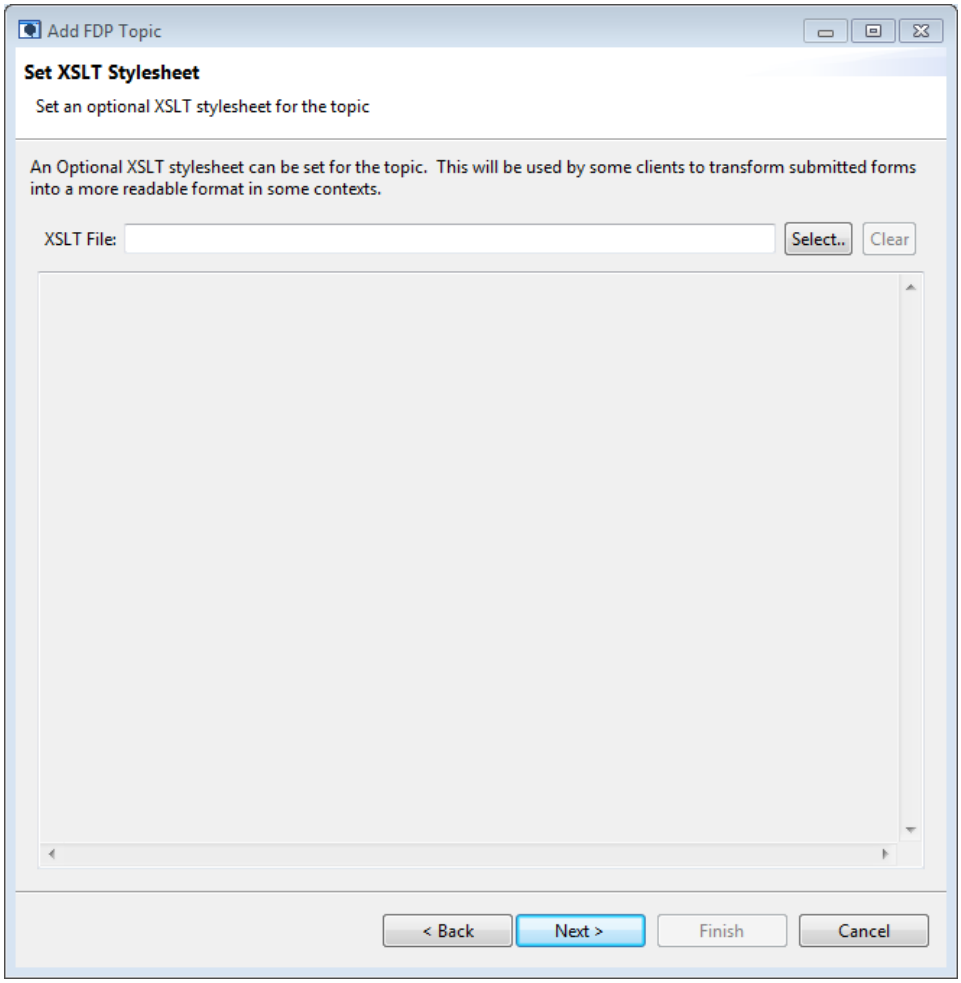
Figure 10.17. FDP Topic Details



10.5.2.3 Set the *XSLT Stylesheet*

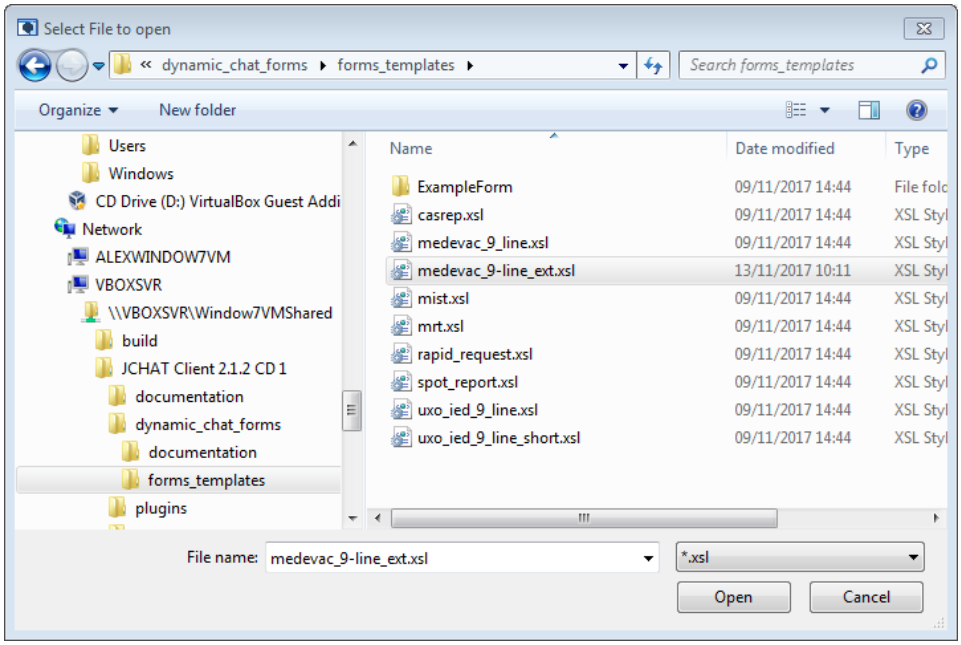
The next page lets you set an *XSLT stylesheet* for the *topic*. This may be used by some clients (such as the NATO JChat client) to transform submitted *FDP forms* into another format. This is an optional field and not required, initially it is unset, and the page is displayed as shown below.

Figure 10.18. Set XSLT Stylesheet - No sheet selected



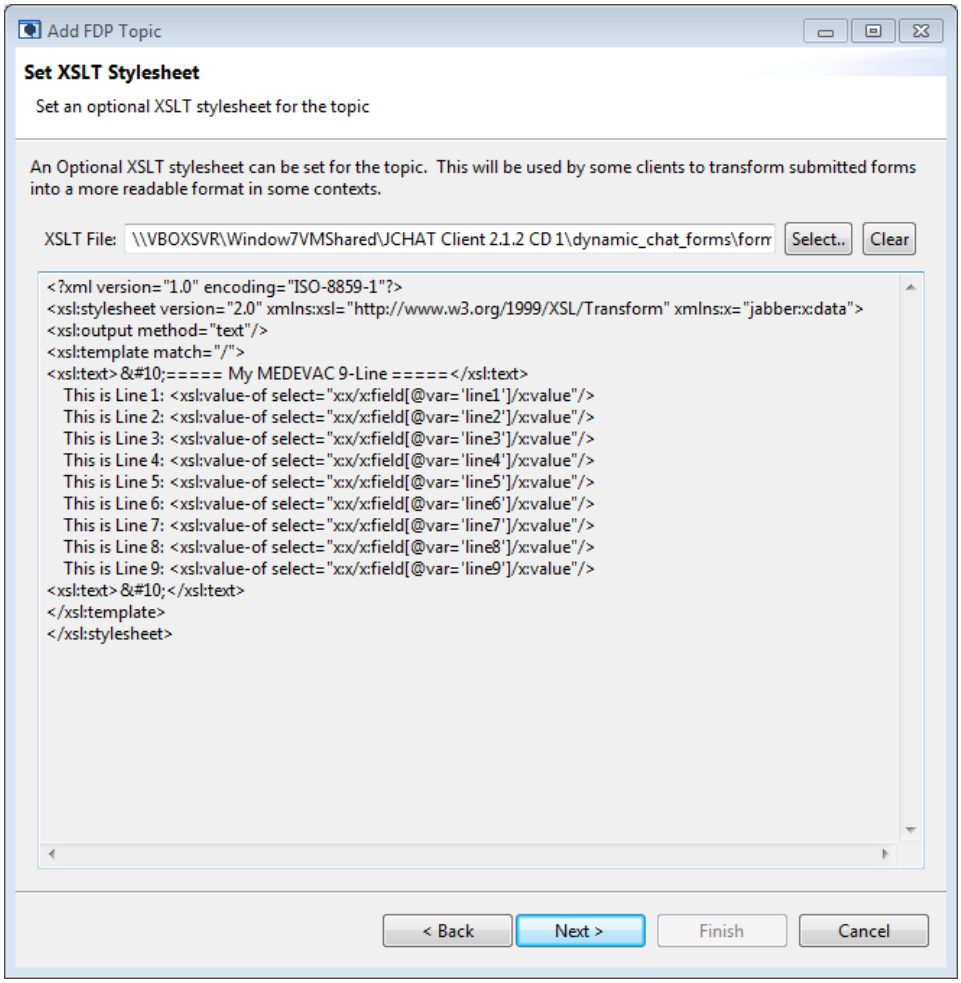
To set an *XSLT stylesheet* select the **Select** button to bring up the **Select XSLT File dialog**.

Figure 10.19. Select XSLT File dialog



Browse the the location of the required *XSLT* file in the file browser and select it. The selected *stylesheet* will then be displayed in the editor.

Figure 10.20. Set XSLT Stylesheet - Showing selected stylesheet

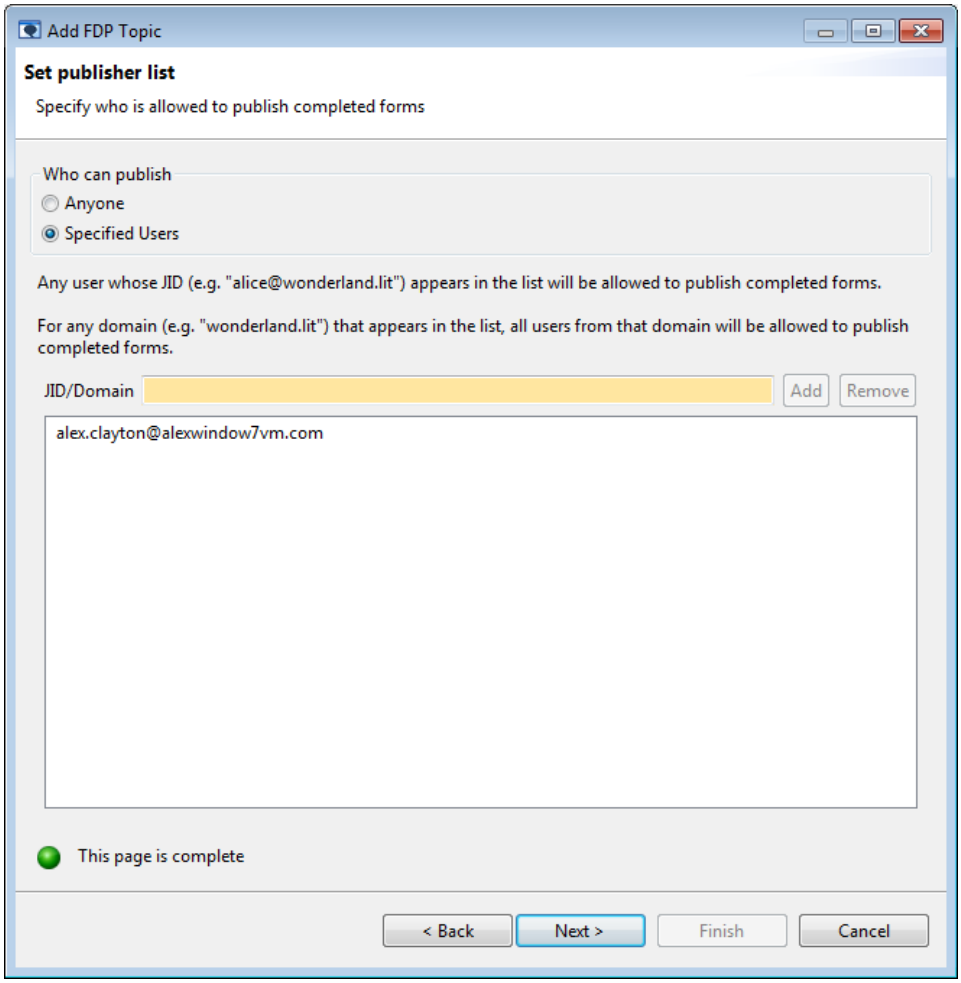


If needed you can change the selected *XSLT stylesheet* by selecting the **Select...** button again, or clear the selection by selecting the **Clear** button. Once satisfied select the **Next** button to select the next page.

10.5.2.4 Specify completed form publishers

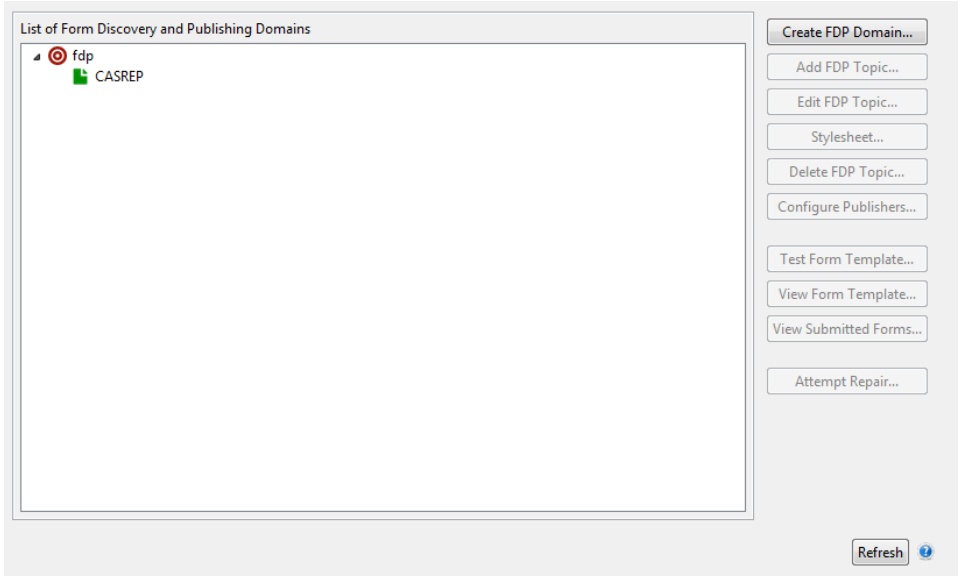
The next page lets you configure who is allowed to publish completed forms. This can either be a whitelist of specified users or it can be set to allow anyone to publish them. By default it will be set to specified users with only the topic creator allowed to publish. These options can be configured now or at any subsequent time, using the **Configure Publishers...** button, or by using the **Edit FDP Topic...** wizard.

Figure 10.21. Specifying who can publish completed FDP forms



On completion of the wizard, M-Link Console will create the necessary PubSub nodes to contain both the FDP form template and any submitted forms, and then show the new topic in the editor, beneath the FDP domain:

Figure 10.22. FDP editor showing a single FDP Topic



When any FDP topic is selected, you can delete the topic using the **Delete FDP Topic...** button. Note that if you delete an FDP topic, then both form template and *all stored submitted forms* for that topic will be deleted.

10.5.3 Editing existing FDP topics

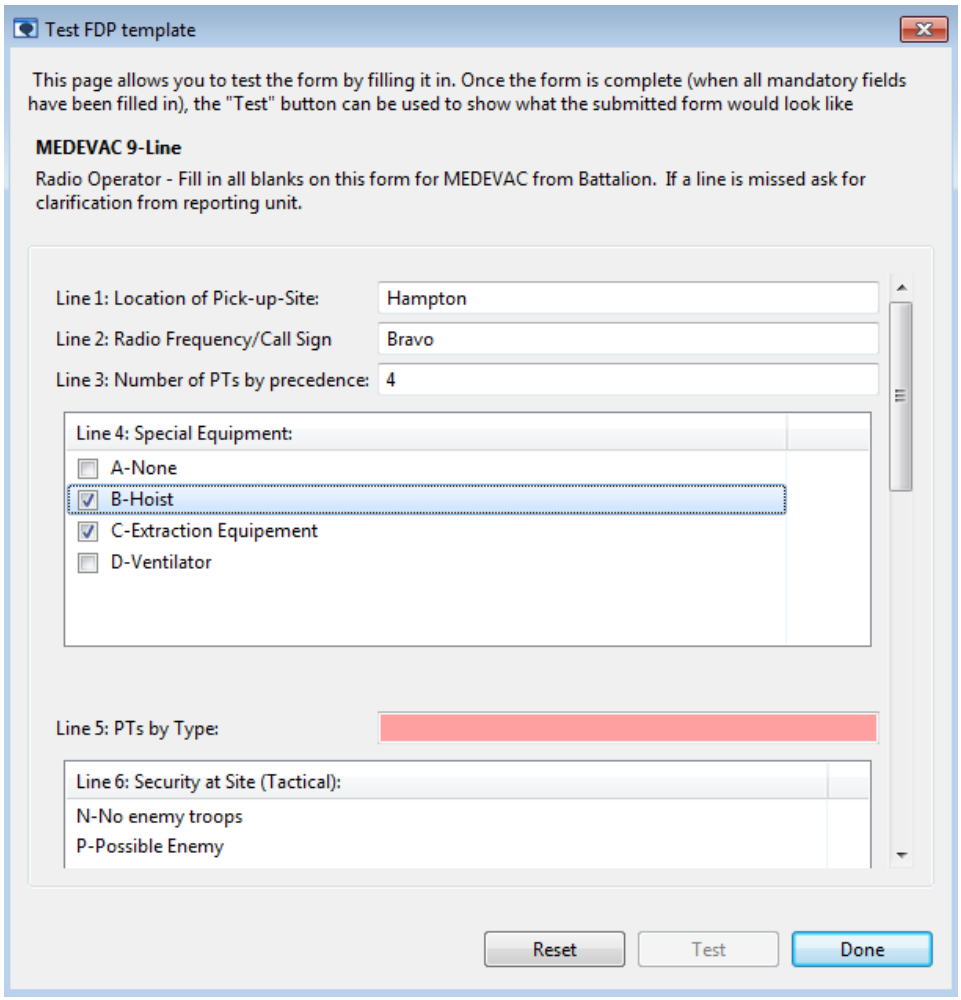
M-Link Console also provides a wizard to edit existing FDP topics. To edit an existing topic, select the topic from the FDP menu and select the **Edit FDP Topic...** button. This will open an editor and load the template for the selected topic. From this editor, you are able to modify the selected topic. By selecting the **XML editor...** button, you will be able to view and edit the XML for the selected template. When you have finished editing the template, check the **Complete** check-box. At any stage, you can either press the **Finish** button to skip subsequent configuration and apply the changes, or the **Next** button to continue making changes to the selected topic.

Selecting **Next** opens a page for configuring the maximum number of forms retained by the server. Pressing **Next** again opens a page where you can edit the publishers configured to submit forms for the selected node.

The final page of the wizard contains a summary page. This page will display a warning message if the template has been modified, or if the server submitted-form-limit has been reduced. If the template has been changed, the original FDP submit node becomes invalid. This means that any previously submitted forms may not render correctly with the new template if you apply the changes. If the submitted-form-limit has been reduced, the server will remove the oldest existing submitted form until the number of items has been reduced to the new limit. Clicking **Finish** will apply any changes to the FDPTopic. Clicking **Cancel** will return you to the FDP menu cancelling any changes.

10.5.4 Testing an FDP template

Figure 10.23. Testing FDP templates



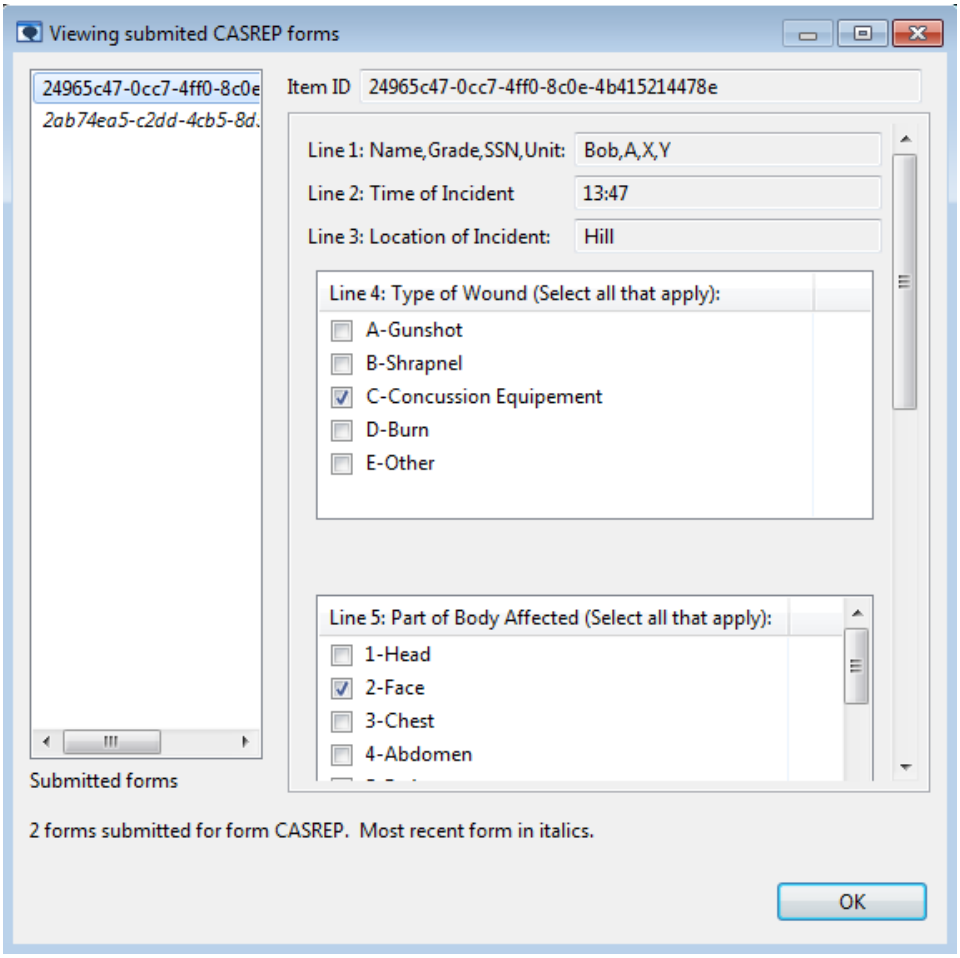
M-Link Console provides a dialog to test an FDP topic's template, and view a sample submitted form. To do this, select the **Test Form Template...** option from the FDP menu. This will open a dialog containing the selected topic's template. Here you can fill in the fields for the template and view the resulting submitted form by selecting the **Test** button. Selecting the **Reset** button clears any user input.

10.5.5 Viewing existing FDP topics

After selecting an FDP topic, you are able to view the topic's form template (as shown in ...) and also to view the contents of any forms which have been submitted. The maximum number of submitted forms stored for any topic is limited, and is configured when the topic is created (see Figure 10.17, “FDP Topic Details”). To view the forms which have been submitted for a given topic, use the **View Items...** button.

M-Link Console displays a window containing the list of IDs corresponding to the forms that have been submitted (on the left), which you can use to view any of the submitted forms (the list is not held in any particular order, although the most recently submitted form will have an ID shown in italics). The selected submitted form is shown in the right hand side of the window:

Figure 10.24. Viewing submitted FDP forms



Because M-Link Console's FDP editor has knowledge of the structure of data in the *template* and *submitted* nodes, it is able to use this to render the submitted form in a helpful way. It is possible to view submitted form information from the PubSub editor (see Section 10.5.7, "Viewing FDP configuration in the PubSub editor") although in this case any data will be rendered in its raw, unformatted form.

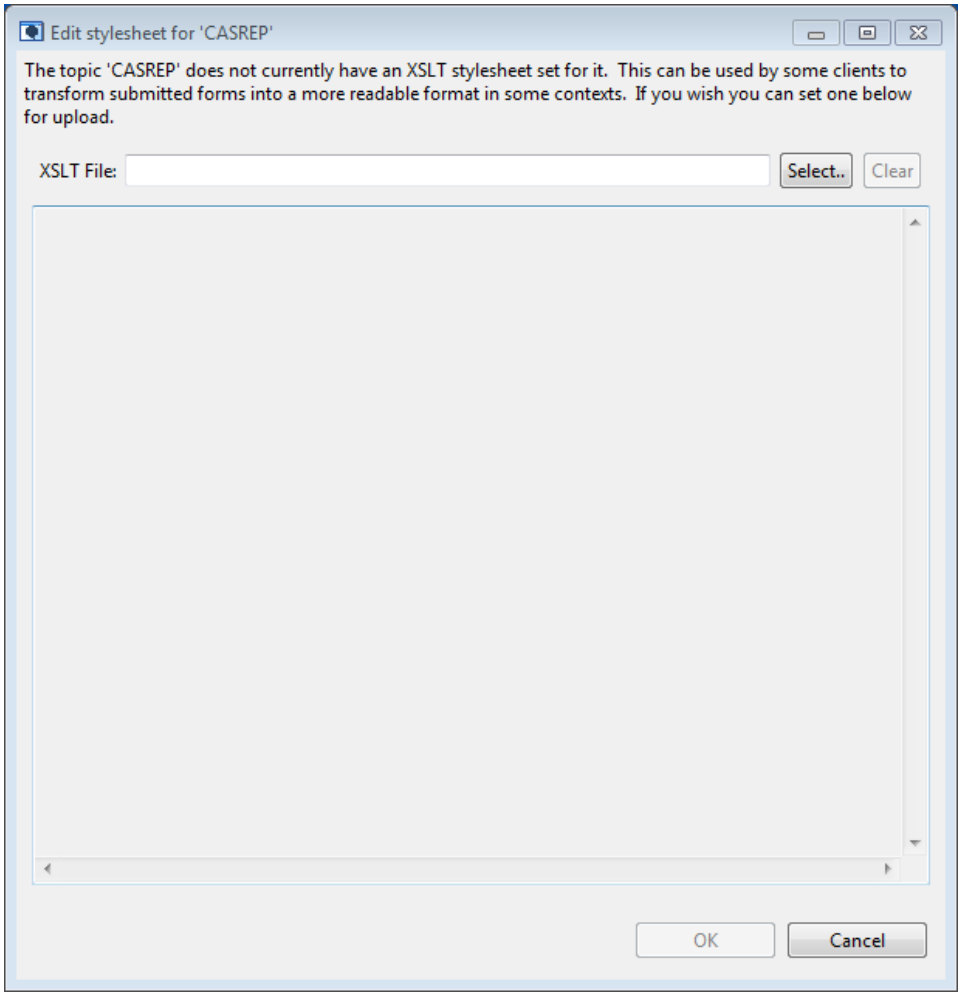
10.5.6 Viewing and editing the *XSLT Stylesheet* for an *FDP Topic*

Each *FDP Topic* can have an *XSLT stylesheet* associated with it. This is an optional value that clients may use to transform submitted *FDP forms* into another format.

The *XSLT stylesheet* can be set during the creation of *FDP Topic* (see Section 10.5.2.3, "Set the *XSLT Stylesheet*"). Alternatively it can be viewed (if set) and edited via the **Edit stylesheet dialog**.

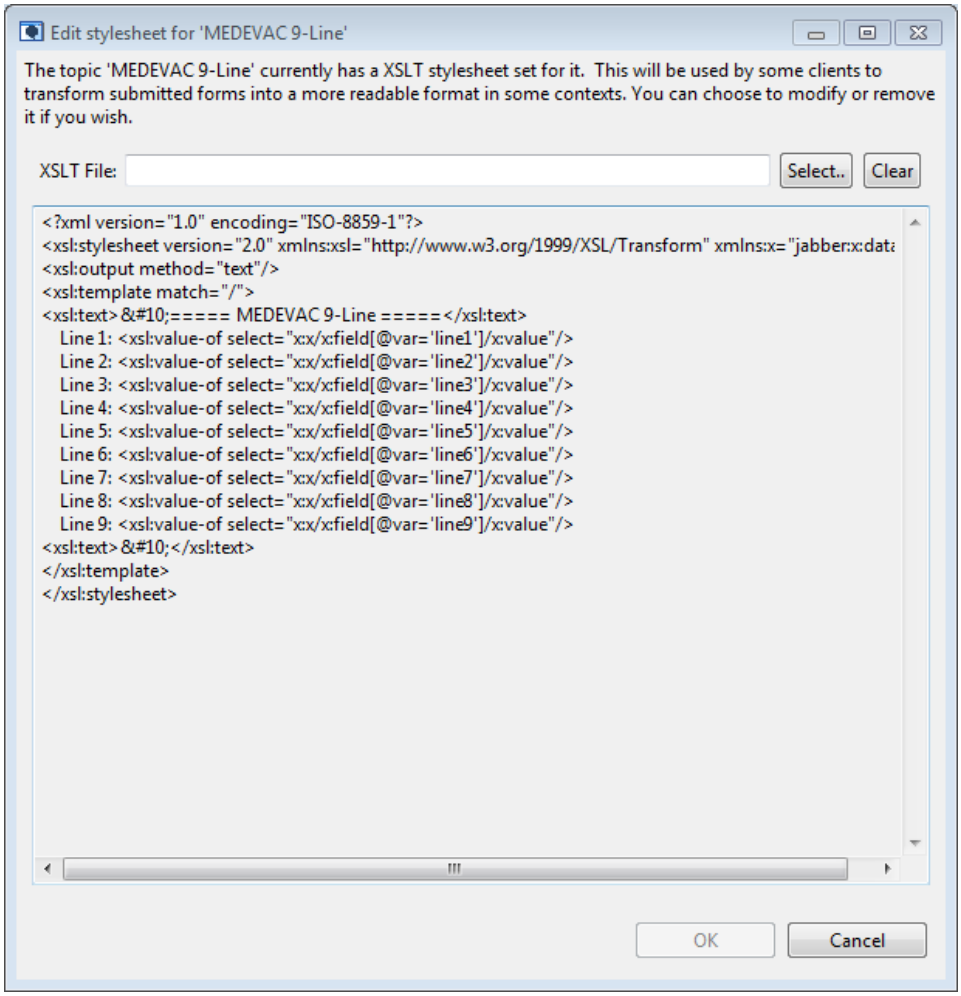
This dialog can be opened by selecting an *FDP Topic* and then pressing the **Stylesheet...** button. For a *Topic* without a *stylesheet*, the dialog will be displayed with an empty stylesheet as shown below. The **Select...** button can be used to launch a file browser to select an *XSL file* to upload. To save changes select the **OK** button.

Figure 10.25. Edit Stylesheet Dialog for *Topic* with no *stylesheet*



For a *Topic* which already has an *XSLT Stylesheet* selected the dialog will show the contents of that stylesheet. Here the **Select...** button can be used to open a file browser for selecting a new stylesheet, or the **Clear** button can be used to remove the stylesheet. As before use the **OK** button to save the changes.

Figure 10.26. Edit Stylesheet Dialog for *Topic* with a *stylesheet*

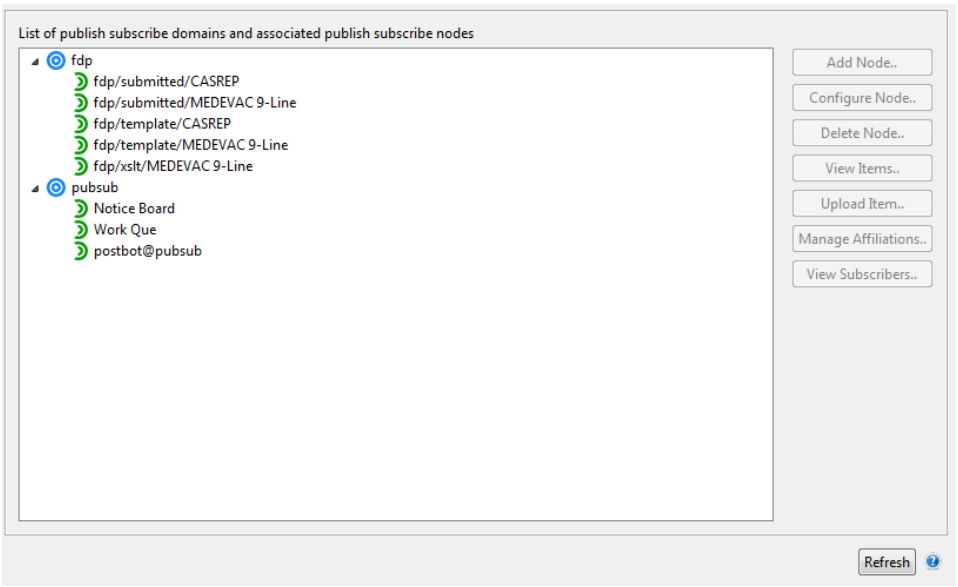


10.5.7 Viewing FDP configuration in the PubSub editor

Since FDP is implemented using PubSub, any FDP topics that you configure will appear as PubSub nodes that will be visible in M-Link Console PubSub editor. In normal usage, it will not be necessary to use the PubSub editor to manipulate FDP configuration, but there may be cases where it is useful to do so, and this section describes the appearance of FDP information when viewed in the context of the PubSub editor.

When using the PubSub editor, an FDP topic will appear as two separate nodes, as shown below:

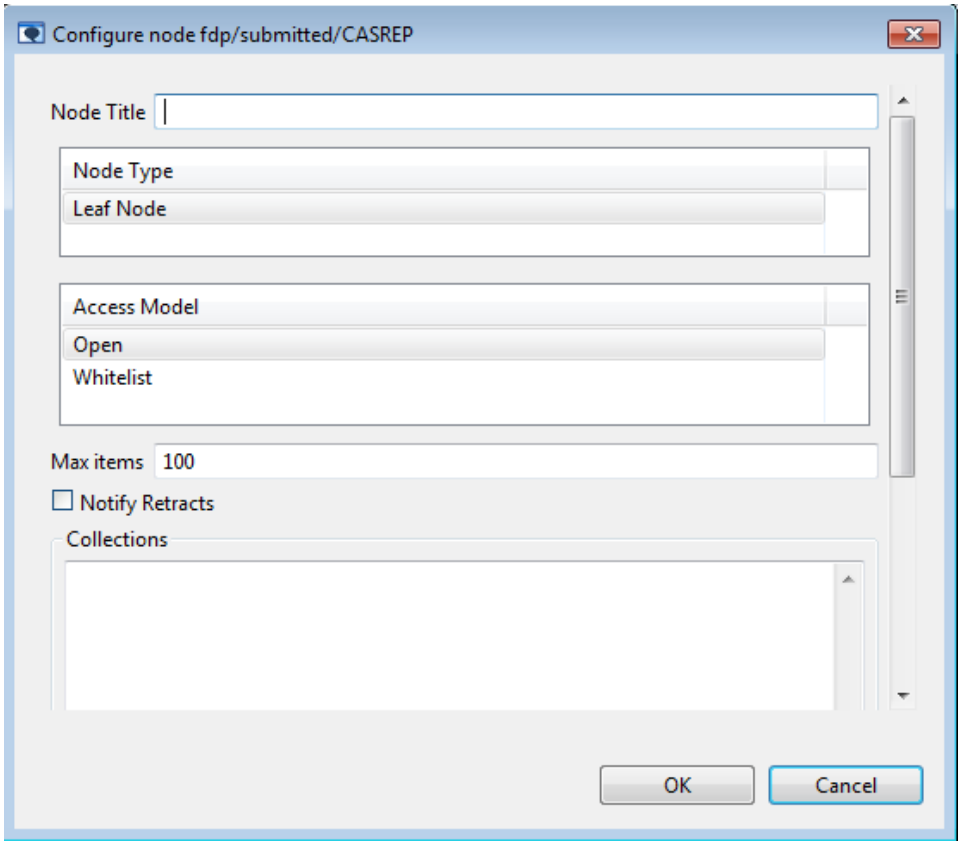
Figure 10.27. FDP Topic shown in PubSub editor



Beneath the FDP PubSub domain, each FDP topic is represented by a number of nodes (*/template*, */submitted* and optional */xslt*). The items on these nodes can be viewed inside the PubSub editor using the **View Items...** button although since the PubSub editor has no special knowledge of FDP forms, the template and submitted values will be rendered as raw XML (see Figure 10.4, “Viewing items on a PubSub node”).

Some functions in the PubSub editor may be useful in the context of FDP, such as the **View Subscribers...** option, which could be used to find out whether any clients are currently monitoring a given FDP topic. It is also possible to use the **Configure Node...** to examine or change options: specifically, you can change the **Max Items** for a */submitted* node:

Figure 10.28. Viewing PubSub configuration for an FDP "submitted" node



Chapter 11 M-Link FDP Gateway

This chapter describes the M-Link FDP Gateway.

11.1 Introduction

The M-Link FDP Gateway is a simple application that can discover forms using Form Discovery and Publishing (FDP) (as defined in [*XEP-0346*]) and forward them on to a target JID. When run, the application connects to a specified FDP domain and subscribes to the subscription node of a given FDP topic. Whenever it receives notification of the publication of a form, it will serialize the form into a XMPP <message/> *stanza* and send it to the target JID.

The M-Link FDP Gateway is robust enough to survive disconnections from the server due to network failures or server restarts, because it maintains a list of which forms it has processed. This prevents the sending of duplicate messages for the same submitted form, and also allows the M-Link FDP Gateway to determine which forms may have been submitted to the XMPP server while it was not connected to the server, so that it can "catch up" when a connection is established.

Note that the M-Link Server maintains a list of the most recent *n* published forms for each topic, where *n* is a configurable value (see Figure 10.17, “FDP Topic Details”). Once the list is full, then the server will delete old forms to make room for new ones. When the M-Link FDP Gateway loses its connection to the server, it will check this list as soon as it reconnects, so that it will be able to forward any forms that it might otherwise have missed.

In most cases, a "max items" value of `100`, as used by M-Link Console when configuring FDP topics, will be adequate; in cases where very many forms are being submitted, you may want to consider using a larger value.

If the M-Link FDP Gateway finds, when it connects to the server, that the list of published forms has been completely re-filled since it last looked, then it will log a warning, and you should consider raising the "max items" value on the server for the topic concerned.

11.2 Installation

The M-Link FDP Gateway will be installed automatically when you install Isode M-Link. It can be found in the Isode Java classes directory with the file *isode-fdpgateway.jar*

11.3 Configuring the XMPP service

The M-Link FDP Gateway requires an XMPP service to connect to, and an FDP topic to subscribe to. The topic will need to be on a correctly configured FDP domain (as per

[*XEP-0346*]). The submit node for the topic should be configured to allow the login JID used by the M-Link FDP Gateway (see Section 11.4.1, “M-Link FDP Gateway Parameters”).

If you have M-Link Console installed, you can use it to create and configure the FDP domain and topics. This can be done using the **Form Discovery and Publishing Administration** editor in the service view. New domains can be created using the **Create FDP Domain…** wizard, and topics created using the **Add FDP Topic…** wizard. When using these wizards the created domains and topics will be created correctly for use with the M-Link FDP Gateway, and will not require further configuration.

11.4 Running the M-Link Console

M-Link FDP Gateway can be run either from the command line (or from a script) or as a Windows service. In either case it will need to be configured by passing it a number of parameters. When run from the shell these parameters can be passed to it directly, as command line arguments, or passed inside an XML configuration file. When run as a Windows service then the parameters must be provided via an XML configuration file.

11.4.1 M-Link FDP Gateway Parameters

The list of parameters and their meanings are described below:

- `login-jid <jid>`

  (Required)

  This is the JID the M-Link FDP Gateway will use to authenticate to the the XMPP server. It should be a valid JID that is a user on the target XMPP service. The user should have permission to subscribe to the submit node of the specified FDP topic.

  The login JID used by the M-Link FDP Gateway should not be used by any other clients.
- `login-password <password>`

  (Required)

  This is the password associated with the `login-jid`.
- `fdp-domain <fdpDomain>`

  (Required)

  This should be the FDP domain that `fdp-topic` is on. It should be a properly configured FDP domain (see Section 11.3, “Configuring the XMPP service”).
- `fdp-topic <fdpTopic>`

  (Required)

  The FDP topic to connect to. This should be a properly configured FDP topic that is on the specified `fdp-domain`. The specified `login-jid` should be able to be allowed to subscribe to its submit node.
- `target-jid <targetJID>`

  (Required)

  This is the JID that the serialised forms will be sent to. It should be a valid JID, and correspond to an existing user.

The M-Link FDP Gateway does not have any way of validating the target JID. Therefore it is strongly recommended you confirm that the intended user is receiving the forms when first configuring the M-Link FDP Gateway.

- `serialize-mode <mode>`

  (Required)

  When serialising the forms the M-Link FDP Gateway can either convert them into text and include them in the <body/> element of the <message/> stanzas, or just include the form payload in the <message/> stanza. When included in the <body/> element, any XMPP client connected as the `target-jid` will see the forms forwarded on to it as messages from the `login-jid`. If the forms are included inline as part of the payload, then a specialized client will be required to interpret them.

  The serialize-mode parameter specifies which of these two options will be used. Use `SERIALIZE` to serialize them into the <body/> element, and `RAW` to include them inline in the <message/> stanza.

- `data-directory <dataDirectory>`

  (Required)

  The M-Link FDP Gateway maintains a list of the items that it has sent. This prevents it sending duplicate items and allows it to determine if it has missed any items when it reconnects. A copy of this list is saved to the filesystem. The data directory parameter specifies the directory this data should be saved to. It does not have to be an existing directory: the M-Link FDP Gateway will try to create the directory if it does not exist, but the user running the M-Link FDP Gateway must have permission to create and write to the directory.

- `certs-file <pinnedCertificateFile>`

  (Optional)

  The name of a file that contains one or more PEM format certificates which will be trusted by M-Link FDP Gateway when checking the certificate presented by an XMPP server when a TLS connection is established. For more information on TLS and certificates, see Section 11.7, “TLS”).

- `ta-file <trustedRootCAsFile>`

  (Optional)

  The name of a file that contains one or more PEM format CA certificates which will be trusted when performing certificate verification on any certificate presented by an XMPP server when a TLS-protected connection is established. For more information on TLS and certificates, see Section 11.7, “TLS”).

- `get-items-threshold <value>`

  (Optional)

  As elsewhere described the M-Link FDP Gateway maintains a list of all the submitted forms that it has processed. Items are only removed from this list when it is determined that no copy exists on the server (forms on the server are purged to make room for new ones when the "max items" is reached). The M-Link FDP Gateway will ask the server for its current list of submitted forms every so often, so that it can purge old items from its cache.

  By default, this refresh operation will be performed after every 10 forms received as publish subscribe notifications, but this can be configured by setting the `get-items-threshold` parameter.

- `plain-without-tls <value>`

(Optional)

When the M-Link FDP Gateway authenticates to a server which is holding FDP information, it will normally only use a plain text password authentication mechanism when TLS has been established. This means that when connecting to a server that does not offer TLS, but which requires plain text authentication, the M-Link FDP Gateway will fail to connect. In this case, the log file will report a message similar to the following:

```
2018-02-25 16:08:38 - Unable to connect, reattempting connection..
```

The `plain-without-tls` option may be specified in this case to relax the restriction which otherwise prevents the connection. Note that in thie case, the password will be transmitted in the clear over the wire. Disabling TLS is not recommended unless M-Link FDP Gateway is operating on the same host system as M-Link Server

11.4.2 Providing parameters via command line

When it is being run from the command line (or script), the parameters for the gateway can be passed to it as command line parameters. This can be done as follows:

The parameters should be listed after the command that runs the gateway, with each parameter paired with the value it should be set to. Each parameter should prefixed with two dashes (--) and followed by the value for the parameter. If the value contains any spaces then the value should be enclosed in quotation marks.

Here is a sample command for starting the M-Link FDP Gateway from the command line (or from within a script) on a Unix system where the parameters are provided via the command line. This is a single command, but the lines have been split for readability.

```
% /opt/isode/bin/fdpgateway
--login-jid mad.hatter@wonderland.lit
--login-password secret
--fdp-domain fdpdomain.wonderland.lit
--fdp-topic "MEDEVAC 9-Line"
--target-jid march.hare@rabbit.hole
--serialize-mode SERIALIZE
--data-directory /home/user/documents/fdpGatewayDir
--get-items-threshold 25
--certs-file /home/user/fdpgateway/servercert.pem
```

This command causes M-Link FDP Gateway to attempt to connect to the server *`wonderland.lit`*, authenticating as *`mad.hatter@wonderland.lit`* with a password of *`secret`*. If the server uses TLS, then any certificate that it sends will be compared with the contents of */`home/user/fdpgateway/servercert.pem`*, and the connection will only proceed if the file contains the server certificate (see Section 11.7, “TLS”). Once connected, it will attempt to subscribe to the FDP topic *`MEDEVAC 9-Line`* which it will expect to find in the Publish-Subscribe domain *`fdpdomain.wonderland.lit`*. Using and updating its cache in */`home/user/documents/fdpGatewayDir`*, it will determine whether there are any un-forwarded forms held on the server, and it will send these, and subsequently any newly published forms, to *`march.hare@rabbit.hole`*.

For every 25 forms it forwards, it will purge its local cache by asking the server at *`wonderland.lit`* which old forms have expired.

11.4.3 Providing parameters via XML File

Paramters can be passed to M-Link FDP Gateway as part of a XML file. This can be done when the gateway is running from the shell or when its being run as a Windows service. The XML must follow a specific Isode defined structure that is described below.

There should be a single top level `<gateway_configuration version="1">` element, this must contain an `version` attribute set to `1`. The `<gateway_configuration>` element can contain one or more `<profile>` elements, each one representing one configuration for the gateway. Each configuration can be run as separate instances of the gateway (see Section 11.8, “Deploying more than one M-Link FDP Gateway” for more information of running multiple gateways). Each `<profile>` should contain the parameters for that configuration as separate child elements, with the element's contents set to its required value. The profile can have an `id` attribute that will be used to distinguish it from the others.

Here is a sample XML for a two separate configurations of the M-Link FDP Gateway on a Unix type system:

```
<gateway_configuration version="1">

<profile id="Profile 1">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password>secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>march.hare@rabbit.hole</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<data-directory>/home/user/documents/march-hare</data-directory>
<get-items-threshold>25</get-items-threshold>
<certs-file>/home/user/fdpgateway/servercert.pem</certs-file>
</profile>

<profile id="Profile 2">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password>secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>alice@wonderland.lit</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<data-directory>/home/user/documents/march-alice</data-directory>
<get-items-threshold>25</get-items-threshold>
<certs-file>/home/user/fdpgateway/servercert.pem</certs-file>
</profile>

</gateway_configuration>
```

If using *`Profile 1`* M-Link FDP Gateway will to attempt to connect to the server *`wonderland.lit`* , authenticating as *`mad.hatter@wonderland.lit`* with a password of *`secret`*. If the server uses TLS, then any certificate that it sends will be compared with the contents of */home/user/fdpgateway/servercert.pem*, and the connection will only proceed if the file contains the server certificate (see Section 11.7, “TLS”). Once connected, it will attempt to subscribe to the FDP topic *`MEDEVAC 9-Line`* which it will expect to find in the Publish-Subscribe domain *`fdpdomain.wonderland.lit`*. Using and updating its cache in */home/user/documents/march-hare*, it will determine whether there are any un-forwarded forms held on the server, and it will send these, and subsequently any newly published forms, to *`march.hare@rabbit.hole`*.

`Profile 2` will behave similarly but send will send its forms to *`alice@wonderland.lit`* and store its cache in */home/users/documents/alice*.

Another example, this time configured for a Windows system, can be found in *(SHAREDIR)/examples/fdpgateway-params.xml.sample*.

11.4.4 Launching the gateway using an XML File

When running from the shell the XML file (see Section 11.4.3, “Providing parameters via XML File”) can be specified by passing it as the `--xml-file` command line parameter. Optionally the profile to use within that file can be passed as the `--profile` parameter. If no profile is specified the gateway will load with the first profile it finds in the file. For example:

Here is a sample command for starting the M-Link FDP Gateway with an XML file on a Unix system. This is a single command, but the lines have been split for readability.

```
% /opt/isode/bin/fdpgateway
--xml-file /home/user/documents/gateway-params.xml
--profile "Second Profile"
```

This command will run the gateway using the parameters contained in profile `Second Profile` located in the XML file */home/user/documents/gateway-params.xml*

For instructions on passing the configuration file to the gateway when it is run as a Windows service see Section 11.4.5, “Running the gateway as a Windows service.”.

11.4.5 Running the gateway as a Windows service.

It is possible to run the M-Link FDP Gateway from the command-line on a Windows system, but more typically it will be configured as a Windows service. This will require a XML file configuration similar to the one described above, but with the *id* attribute of *profile* required. Here is an example configuration file for a Windows system:

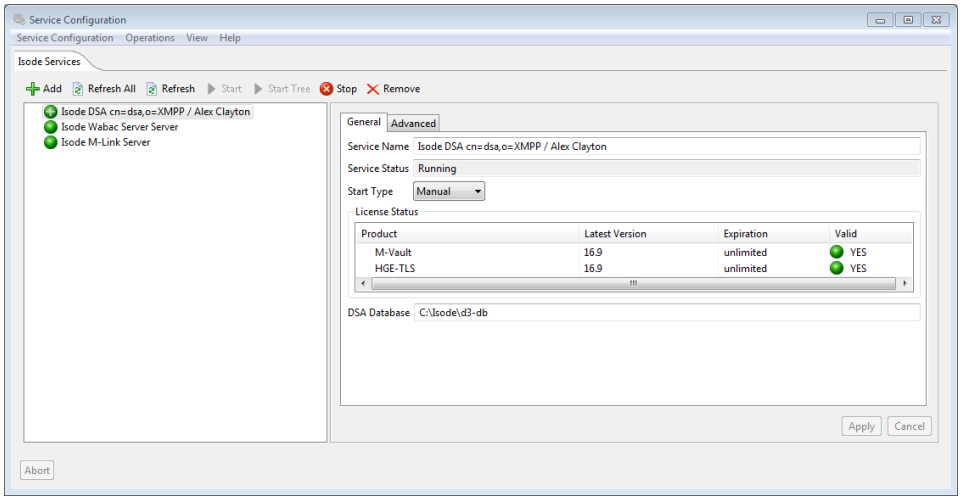
```
<gateway_configuration version="1">

<profile id="Profile 1">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password>secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>march.hare@rabbit.hole</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<!-- File paths on windows that contain backslash characters
must be escaped as in the example below -->
<data-directory>C:\\fdpgateway</data-directory>
<get-items-threshold>25</get-items-threshold>
<certs-file>C:\\fdpgateway\\servercerts.pem</certs-file>
</profile>

</gateway_configuration>
```

This file should be saved to *(ETCDIR)/fdpgateway-params.xml*. A sample file is supplied in *(SHAREDIR)/examples/fdpgateway-params.xml.sample*, this can be copied to the location and modified for the appropiate configuration.

Once the file *(ETCDIR)/fdpgateway-params.xml* is in place, you can configure and create a Windows service that will run the M-Link FDP Gateway.

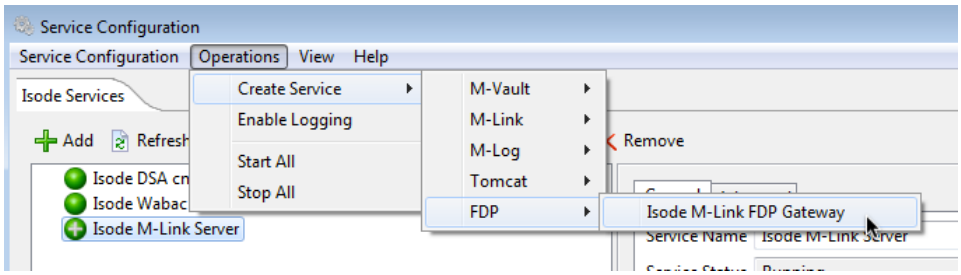
To create a Windows service to run the M-Link FDP Gateway open the **Isode Service Configuration** tool.

Figure 11.1. Isode Service Configuration tool.



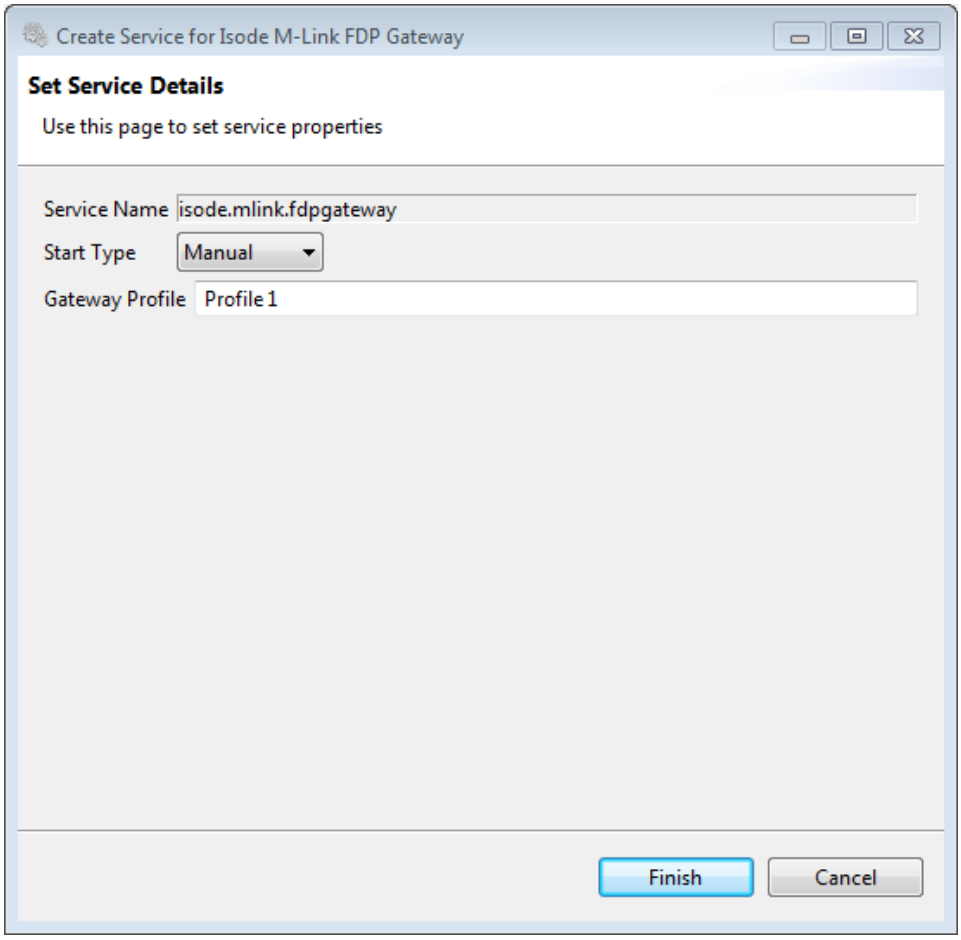
Select *Operations-> Create Service-> FDP-> Isode M-Link FDP Gateway*.

Figure 11.2. Select *Operations-> Create Service-> FDP-> Isode M-Link FDP Gateway*



This will open the *Create Service for M-Link FDP Gateway* dialog.

Figure 11.3. *Create Service for Isode M-Link FDP Gateway* dialog



The fields in the dialog are:

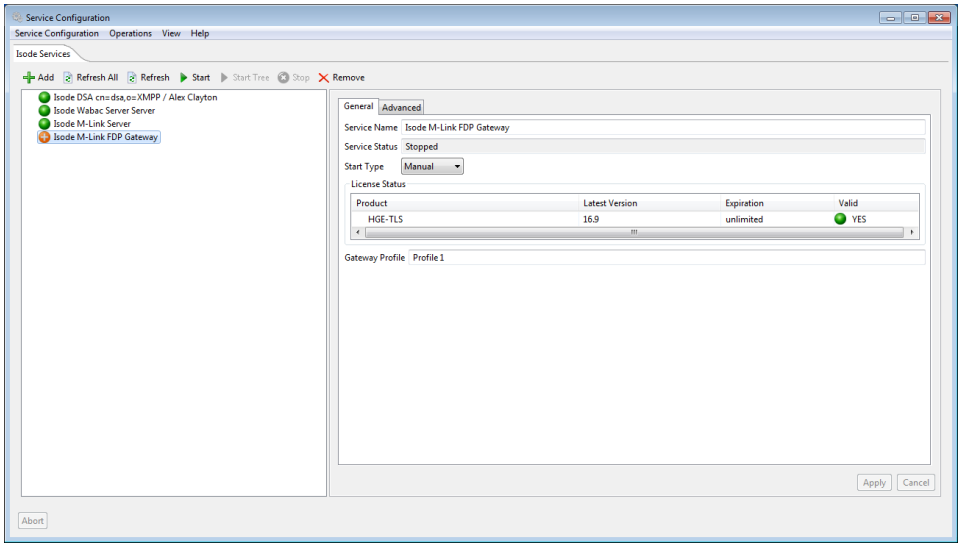
Service Name
: This is the name the service will appear as in the *Isode Service Configuration* tool. It is automatically generated and can not be edited.

Start Type
: This determined whether the service will need to be manually started, or whether it will start automatically when Windows starts. It defaults to *Manual* which means the service will have to be manually started by the user. It can be changed to *Automatic* so that the service starts when Windows or *Disabled* to disable the service.

Gateway Profile
: This will need to be set to the name of the gateway profile in `(ETCDIR)/fdpgateway-params.xml` that should be run.

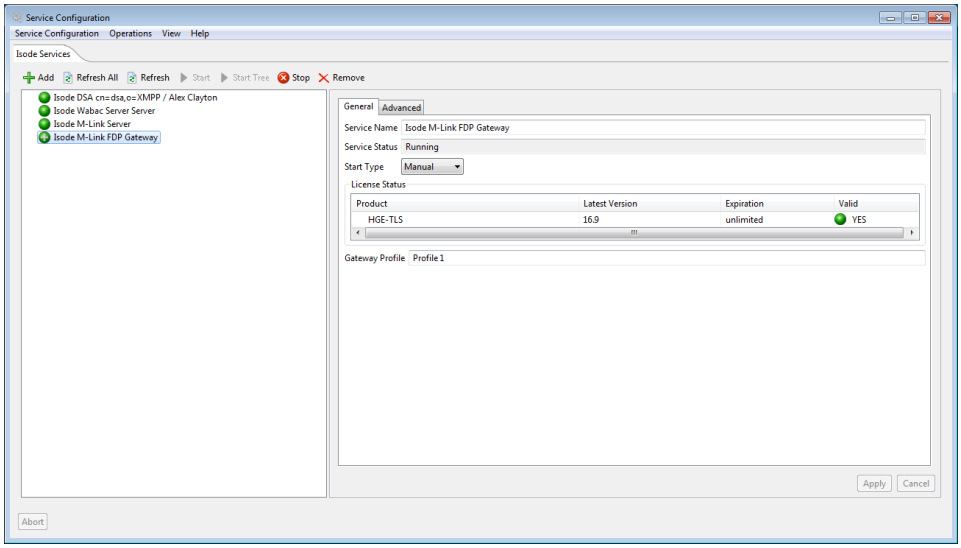
Once all the fields are entered, click finish and the new M-Link FDP Gateway service will be created and added to the *Isode Service Configuration tool*.

Figure 11.4. New service for M-Link FDP Gateway



The service can then be started by clicking the *start* button on the tool bar

Figure 11.5. New M-Link FDP Gateway service started



More information about the **Isode Service Configuration** tool may be found *M-Vault Administration Guide*.

11.5 Logging

The M-Link FDP Gateway logs information to a log file about its progress. This information is by default logged to the gateway's log file which can be found in *`(LOGDIR)`/fdpgateway-eventXXXX.log*. Logging can be configured by modifying the *fdpgatewaylogging.xml* in the *`(SHAREDIR)`*.

11.6 Recommendations

The M-Link FDP Gateway requires a large number of parameters to configure, and typically these will be contained in a script which could be configured to run automatically, for example when the machine is turned on or the user logs in.

When using a script in this way, it is recommended that you first run the script manually, to ensure everything has been configured correctly.

11.7 TLS

When connecting to an XMPP server, the M-Link FDP Gateway will use TLS if the server supports it. In the case of a server supporting TLS, it is typical for the server to send its certificate, and M-Link FDP Gateway will check any server certificate before proceeding with a connection.

A TLS connection will only proceed if the certificate presented by the server is *trusted*. There are two ways that you can configure trust:

1. By storing copies of specific certificates ("pinning") that you know belong to a server that M-Link FDP Gateway is connecting to. The `certs-file` option can be used to name a file that contains pinned certificates: if a server presents a certificate which matches any pinned certificate, the connection is allowed to proceed.
2. If the `ta-file` option is used, then the file specified is considered to contain a set of trusted CA certificates. This means that any certificate presented by the server will (if it is not a "pinned" certificate) be subject to certificate verification, using the specified CA certificates as trust anchors.

   This mechanism may be useful if you do not want to trust a specific server certificate (because it is subject to change, or not yet known) but you do know what CAs are trustworthy (and will be used to issue the server's certificate).

If a certificate presented by the server does not pass either of the above tests, then the connection to the server will fail.

If server certificate verification fails, then the service will fail to start, and an error message will be written to the gateway log file (see Section 11.5, “Logging”). This error message will contain the PEM encoding of the certificate which could not be verified. If it is appropriate, then you can copy this PEM encoding into a file and use the `certs-file` configuration option to point to this file. Having done this, then the next time the M-Link FDP Gateway is started, it will trust the server certificate.

11.8 Deploying more than one M-Link FDP Gateway

It is possible to have multiple M-Link FDP Gateway instances running at once, which may be useful in case where there are several FDP forms of interest. Care should be taken to use different `data-directory` for each instance, but it is reasonable to have multiple instances of the application to send different forms to one user, or multiple instances which watch the same form with each one forwarding information to a different user.

The examples below show how to use configuration to deploy two instances of the M-Link FDP Gateway, first using the command-line arguments, then using a XML configuration file specified on the command line and finally using separate Windows services.

In all examples, the first instance forwards `MEDEVAC 9-Line` forms from the *`fdpdomain.wonderland.lit`* domain to *`march.hare@rabbit.hole`*. The second instance forwards the same forms to *`alice@wonderland.lit`*. In each case, the M-Link FDP Gateway is connecting to the same server (*`wonderland.lit`*) and so they both can use the same `certs-file` file.

11.8.1 Multiple M-Link FDP Gateway instances with Command Line Arguments

Multiple copies of the M-Link FDP Gateway can be run from the command-line, or in the background, using command line parameters, as separate processes. For example (lines split for readability):

```
% /opt/isode/bin/fdpgateway
 --login-jid mad.hatter@wonderland.lit
 --login-password secret
 --fdp-domain fdpdomain.wonderland.lit
 --fdp-topic "MEDEVAC 9-Line"
 --target-jid march.hare@rabbit.hole
 --serialize-mode SERIALIZE
 --data-directory /home/user/documents/fdpGateway/march-hare
 --certs-file /home/users/fdpgateway/servercert.pem
```

and

```
% /opt/isode/bin/fdpgateway
 --login-jid mad.hatter@wonderland.lit
 --login-password secret
 --fdp-domain fdpdomain.wonderland.lit
 --fdp-topic "MEDEVAC 9-Line"
 --target-jid alice@wonderland.lit
 --serialize-mode SERIALIZE
 --data-directory /home/user/documents/fdpGateway/alice
 --certs-file /home/user/fdpgateway/servercert.pem
```

11.8.2 Multiple M-Link FDP Gateway instances with XML Files

Alternatively the parameters for both configuration could be included in an XML file with separate instances of M-Link FDP Gateway being launched for each profile. For example:

```
<gateway_configuration version="1">

<profile id="Profile 1">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password>secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>march.hare@rabbit.hole</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<data-directory>/home/user/documents/march-hare</data-directory>
<get-items-threshold>25</get-items-threshold>
<certs-file>/home/user/fdpgateway/servercert.pem</certs-file>
</profile>

<profile id="Profile 2">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password>secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>alice@wonderland.lit</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<data-directory>/home/user/documents/march-alice</data-directory>
<get-items-threshold>25</get-items-threshold>
<certs-file>/home/user/fdpgateway/servercert.pem</certs-file>
</profile>

</gateway_configuration>
```

On a Unix based system if this is saved to *`/home/user/documents/gateway-parms.xml`* then gateways for these profiles can be launched using the commands:

```
% /opt/isode/bin/fdpgateway
 --xml-file /home/user/documents/gateway-parms.xml
 --profile "Profile 1"
```

and

```
% /opt/isode/bin/fdpgateway
 --xml-file /home/user/documents/gateway-parms.xml
 --profile "Profile 2"
```

11.8.3 Multiple M-Link FDP Gateway instances with Windows services

Section 11.4.5, “Running the gateway as a Windows service.” describes the use of the file *`(ETCDIR)/fdpgateway-params.xml`* to configure a single Windows service which will run the M-Link FDP Gateway. Deploying multiple services with different configuration requires that:

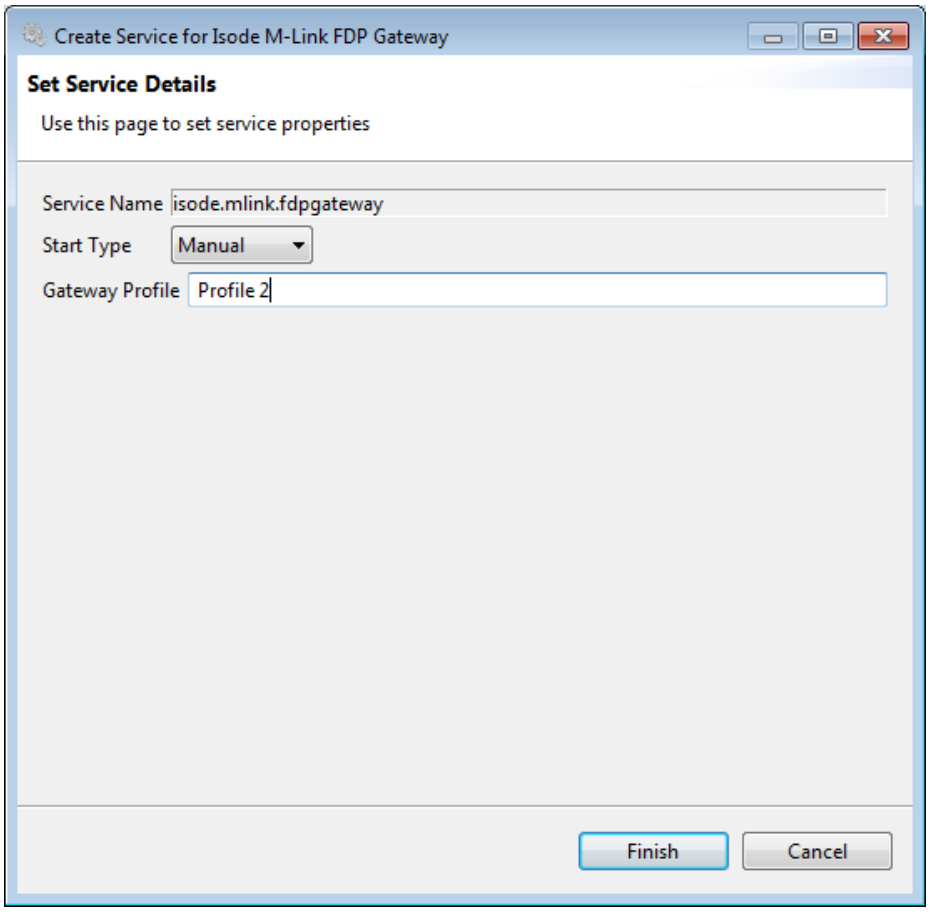
1. A profile for each required Windows service is created in *`(ETCDIR)/fdpgateway-params.xml`*. Here is an example:

```
<gateway_configuration version="1">

<profile id="Profile 1">
```

```
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password>secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>march.hare@rabbit.hole</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<data-directory>C:\\fdpgateway\\hare-data>
<get-items-threshold>25</get-items-threshold>
<certs-file>C:\\fdpgateway\\servercert.pem</certs-file>
</profile>

<profile id="Profile 2">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password>secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>alice@wonderland.lit</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<data-directory>C:\\fdpgateway\\alice-data>
<get-items-threshold>25</get-items-threshold>
<certs-file>C:\\fdpgateway\\servercert.pem</certs-file>
</profile>

</gateway_configuration>
```

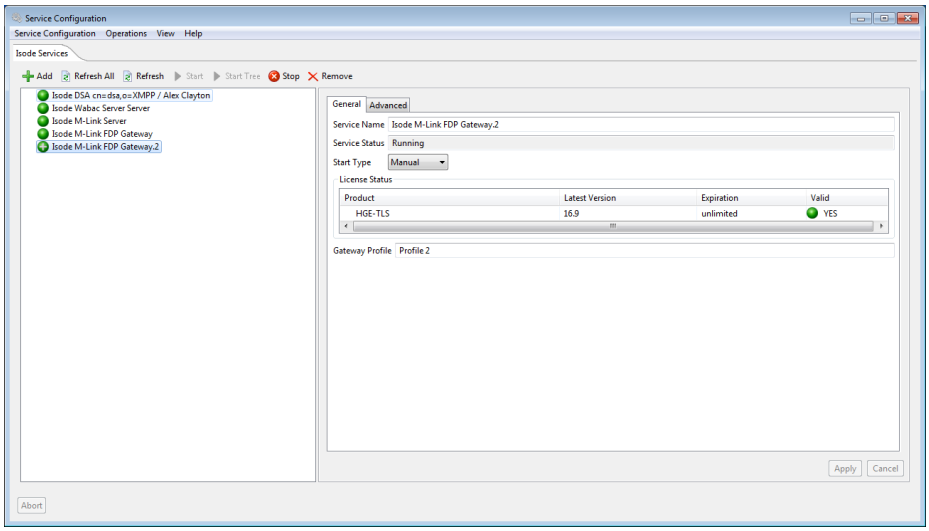
2. For each profile you wish to run an M-Link FDP Gateway create a new service as detailed in Section 11.4.5, “Running the gateway as a Windows service.” setting the *Gateway Profile* value to the profile name.

Figure 11.6. Creating a service for an addditonal M-Link FDP Gateway



3. The new services can then be started as required.

Figure 11.7. Running the additional service



11.9 Encrypting sensitive information in XML files using servpass

By default the fields in the XML configuration file used by M-Link FDP Gateway are stored in plain text. This may not desirable for certain sensitive information, such as passwords. The Isode servpass command line tools can be used to hide the information, encrypting it into a format that only M-Link FDP Gateway can decrypt.

To encrypt sensitive fields the following steps must be followed:

1. (This step only needs to be peformed once.) Before being able to encrypt parameters in an M-Link FDP Gateway configuration file, a service key must be created for the M-Link FDP Gateway service. The service key only needs to be created once: having created a service key, you can use it to encrypt any number of parameter files for the M-Link FDP Gateway.

   To create the service key, use the **spassmgt** tool on the same machine as the M-Link FDP Gateway will be run.

   spassmgt can be found in *(SBINDIR)*. To create the required key the following command should be run:

```
(SBINDIR)/spassmgt set "isode.fdpgateway"
```

   Example use is shown below:

   Unix

```
# /opt/isode/sbin/spassmgt set "isode.fdpgateway"
```

Windows

```
C:\>"C:\Program Files\Isode\bin\spassmgt" set "isode.fdpgateway"
```

When run this command will require a passphrase. This should be at least 16 characters long and should include at least 3 of the character groups: upper case alphabetic, lower case alphabetic, decimal digit, non-alphanumeric.

2. (This and the following steps should be performed for any file that needs to be encrypted.) The XML Configuration file should be prepared to specify which service it should be encrypted for and which fields should be encrypted. To do so the following changes should be made:
   - The `<gateway_configuration>` element should have the attributes "`xmlns:servpass='http://www.isode.com/servpass'`" and "`updater='isode.fdpgateway'`" added to it.
   - There should be a `<servpass:info service='isode.fdpgateway'/>` element added to the `<gateway_configuration>`, at the top above the `<profile>` elements.
   - The field that require encryption should have the attribute "`servpass:encrypt='true'`" added to it.

   Here is an example of a XML configuration form, prepared so that the `login-password` parameter is encrypted:

```
<gateway_configuration version="1"
 xmlns:servpass='http://www.isode.com/servpass'
 updater='isode.fdpgateway'>

<servpass:info service='isode.fdpgateway'>

<profile id="Profile 1">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password servpass:encrypt='true' >secret</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>march.hare@rabbit.hole</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<log-file>C:\\fdpgateway\\fdpgateway-hare.log</log-file>
<data-directory>C:\\fdpgateway\\hare-data>
<get-items-threshold>25</get-items-threshold>
<certs-file>C:\\fdpgateway\\servercert.pem</certs-file>
</profile>

</gateway_configuration>
```

3. The spasscrypt should be run on the XML file to encrypt the tagged fields. spasscrypt can be found in the (SBINDIR). To encrypt the file the following command should be run:

```
(SBINDIR)/spasscrypt -e -s 'isode.fdpgateway' -x (pathToXMLFile)
```

Where `(pathTOXMLFile)` is the path to the XML configuration file. Example use is shown below (split over multiple lines for readability, should be run on one line):

Unix

```
# /opt/isode/sbin/spasscrypt -e -s 'isode.fdpgateway'
 -x /home/user/documents/gateway-parms.xml
```

Windows

```
C:\>"C:\Program Files\Isode\bin\spasscrypt" -e
 -s 'isode.fdpgateway' -x (ETCDIR)/fdpgateway-params.xml
```

When run this will encrypt the contents of the fields tagged with `servpass:encrypt='true'` the resulting XML file will look something like this:

```
<gateway_configuration version="1"
 xmlns:servpass='http://www.isode.com/servpass'
 updater='isode.fdpgateway'>

<servpass:info service='isode.fdpgateway'>

<profile id="Profile 1">
<login-jid>mad.hatter@wonderland.lit</login-jid>
<login-password servpass:encrypt='true' >
{spcrypt2}2lj/o2FmhvvKgP+U2mv8/4KXGqWL</login-password>
<fdp-domain>fdpdomain.wonderland.lit</fdp-domain>
<fdp-topic>MEDEVAC 9-Line</fdp-topic>
<target-jid>march.hare@rabbit.hole</target-jid>
<serialize-mode>SERIALIZE</serialize-mode>
<log-file>C:\\fdpgateway\\fdpgateway-hare.log</log-file>
<data-directory>C:\\fdpgateway\\hare-data>
<get-items-threshold>25</get-items-threshold>
<certs-file>C:\\fdpgateway\\servercert.pem</certs-file>
</profile>

</gateway_configuration>
```

When **spasscrypt** encrypts the file it will created a backup of the original file in the same location. This will have the same name as the original file but with the extension '*.bak*'. This can and should be deleted if the encrypted data should not be stored to the file system as plain text.

4. The M-Link FDP Gateway instance(s) can now be (re)started. They should automatically detect that the field has been encrypted and decrypt it.

If in the future the XML configuration file is update, or a new file is created, then the fields in it can be encrypted by repeating the above from step 2 onwards.

Chapter 12 XMPP over BOSH

This chapter discusses configuration of XMPP over BOSH.

12.1 Overview

Bidirectional-streams Over Synchronous HTTP (BOSH) is a transport protocol that emulates the semantics of a long-lived, bidirectional *TCP* connection between two entities (such as a client and a server) by efficiently using multiple synchronous *HTTP* request/response pairs without requiring the use of frequent polling or chunked responses. XMPP over BOSH provides an alternative to traditional XMPP Client-to-Server (C2S) service. In this guide and within M-Link Server and M-Link Console, the term BOSH often refers to the XMPP over BOSH.

12.2 Using M-Link Console to manage BOSH configuration

M-Link Console allows you to manage BOSH configuration using a customised editor which appears in the *General* editor of *XMPP Service* view under the *BOSH* tab. The editor will only appear for *Server* administrators. Note that M-Link Server allows for both cluster-wide as well as node-specific BOSH configuration (i.e., you can have different values for BOSH configuration parameters on separate nodes in the same cluster). Isode recommends you to set the majority of BOSH configuration for all nodes of the cluster and therefore on the service-wide **BOSH Editor** of the *XMPP Service* view. You should only set specific values that need to be overwritten for a particular server node on the node's **BOSH Configuration** editor. The 'BOSH Listener Host' should only be set only in node-specific configuration.

Select *BOSH* tab of the *General* editor to see or modify information about current BOSH configuration. For a cluster with multiple nodes, expand and select the *Node* view under the *General* editor to see and override node-specific BOSH configuration values.

12.2.1 Configuring BOSH

A basic configuration of BOSH can be setup using the BOSH Configuration editor in M-Link Console. Only one option must be set to enable BOSH service, the 'BOSH Path' option which names the resource which clients obtain BOSH service at. If this option is set to `/bosh` on a particular node, the BOSH service would be available at the URL `http://node.example.com:5280/bosh` where `node.example.com` is domain name resolving to one or more of that node's IP addresses. Note that this domain name is independent of any of the IM domains serviced by the node. Note as well that this URL is specific to a particular node. Node-independent URLs are discussed below.

It is generally recommended that service be offered using HTTP over TLS instead of HTTP. Setting 'Enable BOSH TLS (https://)' will cause the server to require use of HTTP over TLS (`https://`) instead of HTTP (`http://`). In this case, the BOSH service would be available at `https://node.example.com:5280/bosh`. The server must be configured to support TLS before enabling this option.

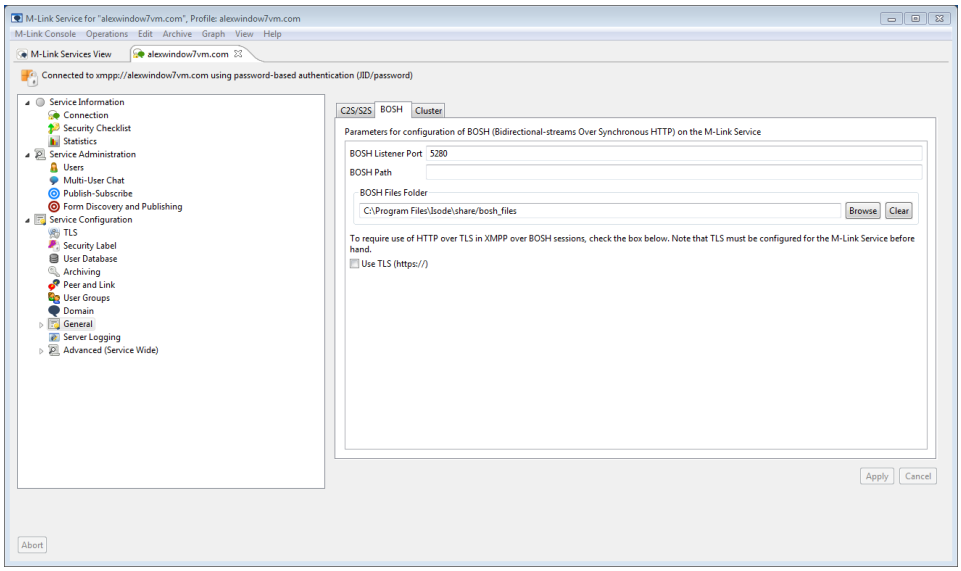
The port to provide BOSH on may be changed using the 'BOSH Listener Port' option.

By default, the M-Link Server will listen for connections on IP addresses of all interfaces. By setting 'BOSH Listener Host', listeners can be restricted to particular IP addresses.

BOSH clients are typically configured by specification of a `http://` or `https://` URL. It is desirable for this URL to be node independent such that clients can use any node providing BOSH service. For example, `https://xmpp.example.com:5280/bosh` where `xmpp.example.com` resolves to the set of IP addresses the cluster is providing service. This requires options impacting URL to be provided to users for client configuration, namely 'BOSH Path', 'BOSH TLS', and 'BOSH Listener Port' to be consistently set across the cluster.

See Section 2.9.5, “DNS Configuration” for information about how to configure DNS to support BOSH clients.

Figure 12.1. BOSH Configuration editor



The description for the configuration parameters for BOSH can be found in the appendix starting from Section H.1.30, “BOSH Path”.

Chapter 13 Filtering using Schematron

This chapter describes how stanzas can be filtered using schematron, and how M-Link Console can be used to configure certain types of filters.

13.1 Using M-Link Console to configure schematron for stanza filtering

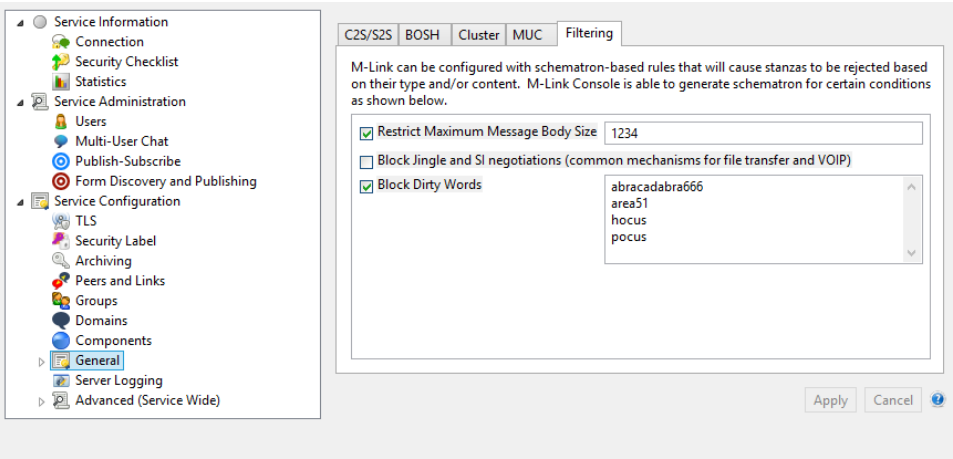
Schematron provides a way to specify a set of rules about which types of stanza should be rejected by the M-Link service. The M-Link server stores schematron in XML format, and M-Link Console is able to generate schematron that represents rules for certain common cases.

M-Link Console allows you to manage schematron configuration using a customised editor which appears in the *General* editor of *XMPP Service* view under the *Filtering* tab. The editor will only appear for *Server* administrators. Note that M-Link Server allows for both cluster-wide as well as node-specific schematron configuration (i.e., you can have different values for schematron configuration parameters on separate nodes in the same cluster). Isode recommends you to set schematron configuration for all nodes of the cluster and therefore on the service-wide **Filtering Editor** of the *XMPP Service* view. You should only set specific values that need to be overwritten for a particular server node on the node's **Filtering Configuration** editor.

Select *Filtering* tab of the *General* editor to see or modify information about current schematron filtering configuration. For a cluster with multiple nodes, expand and select the *Node* view under the *General* editor to see and override node-specific schematron filtering configuration values.

13.1.1 Configuring Schematron

Figure 13.1. Filtering Configuration editor



M-Link Console provides editors that can generate schematron to represent three different types of filter (to view or modify the schematron directly you can use the Advanced editor):

- *Restrict Maximum Message Body Size* allows you to specify that the M-Link Server should reject messages whose body exceeds a certain number of characters. For example, setting this value to 10 would block a message saying "Hello everyone!" but would allow a message saying "Hello all!"

- *Block Jingle and SI negotiations (common mechanisms for file transfer and VOIP)* can be used to block file transfer negotiation for clients using the standard Jingle and Session Initiation file transfer mechanisms.
- *Block Dirty Words* allows you to specify a list of text patterns (containing letters and/or digits) which will be disallowed in the body of any message stanza. Letters 'a'..'z' are not case-sensitive: in other words, if you include "Area51" as a pattern to be blocked, then this will also block "AREA51", "area51" and "ArEa51" etc.. Note that the blocking does not take account of word breaks, so a pattern of "help", will block "help" and "helpful" and "whelp", etc..

The **Advanced** editor (see Section F.1, “Advanced Configuration using MLC”) is able to display and modify the XML schematron, although any changes made to the schematron specification in that editor are likely to mean that M-Link Console will be unable to decode the updated value.

Chapter 14 Clustering

This chapter explains M-Link clustering, and how M-Link Console can be used to configure it.

14.1 Background

An M-Link service which consists of two or more M-Link Server instances co-operating to provide a single XMPP service is called a *cluster*. Each of the M-Link Server instances is a *cluster node* or *node*. This chapter explains how clusters are managed using M-Link Console. If you are not interested in cluster configurations, you can skip this chapter.

Some of the reasons for using a cluster, rather than a standalone M-Link service, include:

- To provide redundancy: if one system fails, then the XMPP service will continue to be provided by other systems that are part of the same cluster. Additionally, single systems may be removed and re-added to the cluster in a controlled manner (for example, when upgrading software) without the service having to be completely shut down.
- To spread load: as workload increases, it may be more effective to add extra servers that act as cluster members, rather than upgrade the hardware of a single system.
- To reduce network latency: if clients of the service are distributed over a wide geographical area, then having all of them depending on a server in a single location may be less efficient than providing servers at locations which are close to the users.

Reasons that you might *not* want to use a clustered configuration would include:

- Cost: for every member of the cluster that is added, extra hardware and product licenses are required.
- Management complexity: while clustering is relatively straightforward, it does require extra configuration.
- Clustering overhead: nodes of an M-Link cluster communicate with one another to share state, and so enabling clustering entails some level of extra load on the network and systems.

14.2 How nodes are added to a cluster

A single-node M-Link service becomes a cluster when you create a new M-Link Server that is part of the existing service. The two nodes co-operate to ensure that the service configuration is consistent between them (see Section 2.1, “About M-Link Server and M-Link Console”).

Once a two-node cluster has been created, further nodes can be added simply by creating another M-Link Server with reference to any of the existing nodes. The initial node retains no special status; all members of a cluster are equal peers.

Creating a cluster, or adding subsequent nodes to an existing cluster, requires that you provide the M-Link Server passphrase (see Figure 2.21, “M-Link Server passphrase”).

When creating a new cluster node, you can either create

- a new *Local* node, by invoking M-Link Console on the system where you want to create the new cluster member
- a new *remote* node, by invoking M-Link Console on any other system (including one where an existing server is running).

The description below focuses on the process of creating a new *Local* node.

14.3 Creating a new Local Cluster Node with M-Link Console

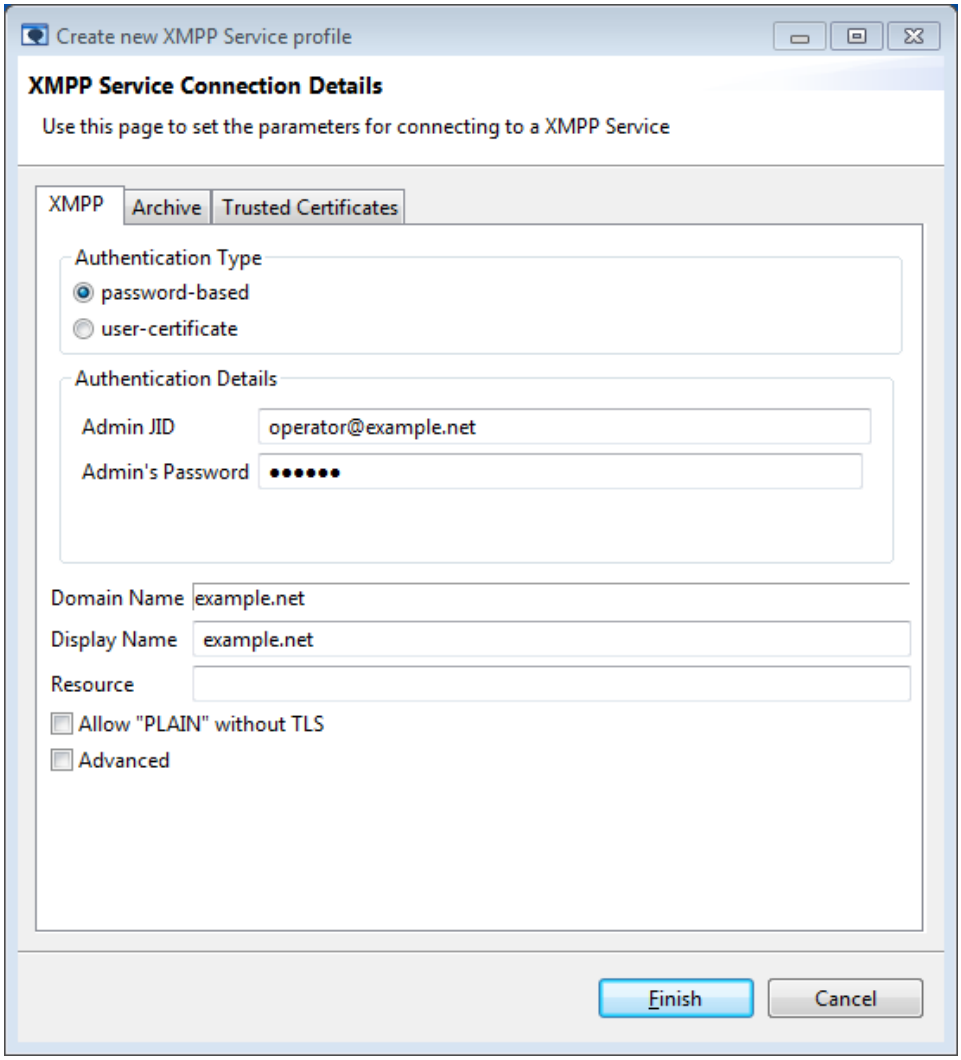
This section will show how a cluster is created for the M-Link service `example.net`, using M-Link Console. The process involves the following steps, each of which will be described below:

- Run M-Link Console on the system where you want to create the new cluster member.
- Add a profile for the M-Link service which is to be promoted to a cluster (see Section 14.4, “Add a profile for the existing M-Link service”).
- Make sure that you can establish a management connection to the existing service (see Section 14.5, “Verify that the existing service can be managed”).
- Ask M-Link Console to create a new cluster member (see Section 14.6, “Using the wizard to create a new cluster node”).

14.4 Add a profile for the existing M-Link service

M-Link Console needs to be able to connect to the existing service, and so the first step is to create a profile for it. Use the **M-Link Console → Create Profile for existing XMPP Service...**, and fill in the details required. Note that appropriate credentials (such as the *Admin JID* and *XMPP Service Admin's Password*, in the case of simple authentication) are required in order to be able to establish a connection with administrator rights.

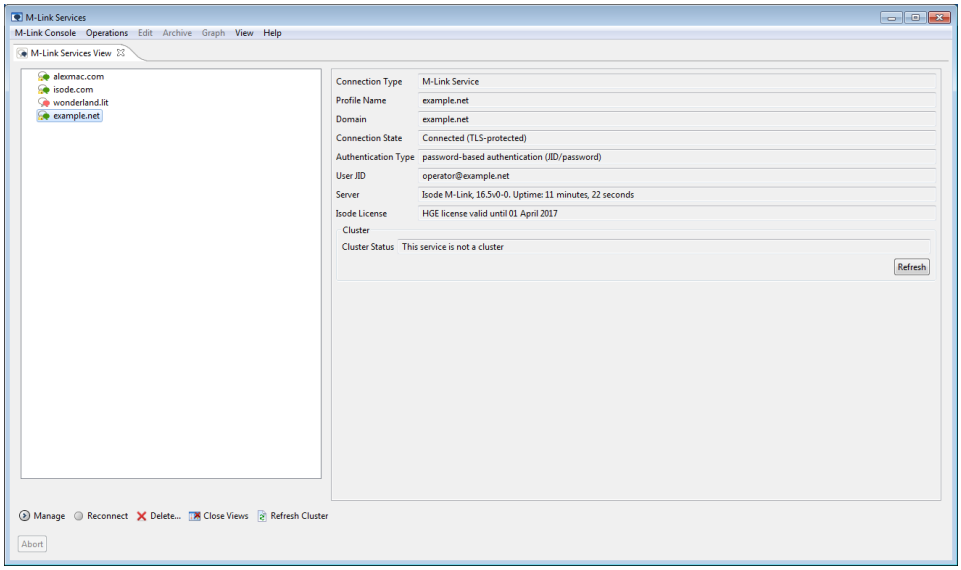
Figure 14.1. Adding a profile for example.net



14.5 Verify that the existing service can be managed

When M-Link Console knows about the existing service, it will attempt to connect to it, using the JID and password you provided. Select the service in the left-hand pane of the Services view and make sure that you have a connection. If you do not have administrator access, M-Link Console will display the *Cluster Status* as not available. Otherwise, M-Link Console will indicate that you have a connection but that the service is not (yet) clustered.

Figure 14.2. Verify the connection to example.net

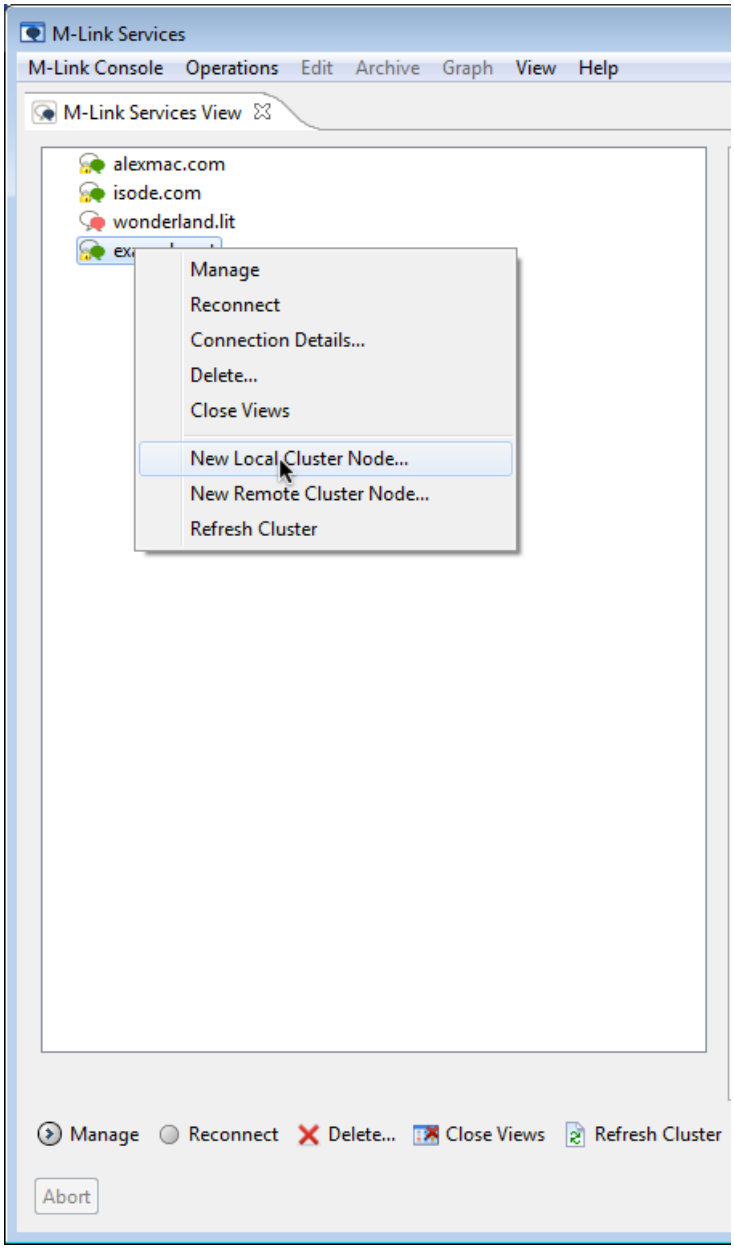


To create the new cluster node, M-Link Console needs similar information to that used when creating a new M-Link Server (see Section 2.7, “Create an M-Link Server”), and so it uses a version of the same wizard. M-Link Console can obtain service configuration for the new node from an existing node, but the node-specific configuration and some passwords must be provided, as detailed in the following section.

14.6 Using the wizard to create a new cluster node

Select the service in the services view, and use either **Operations** → **New Local Cluster Node...**, or *right-click* to expose the menu that provides options to create a new cluster node.

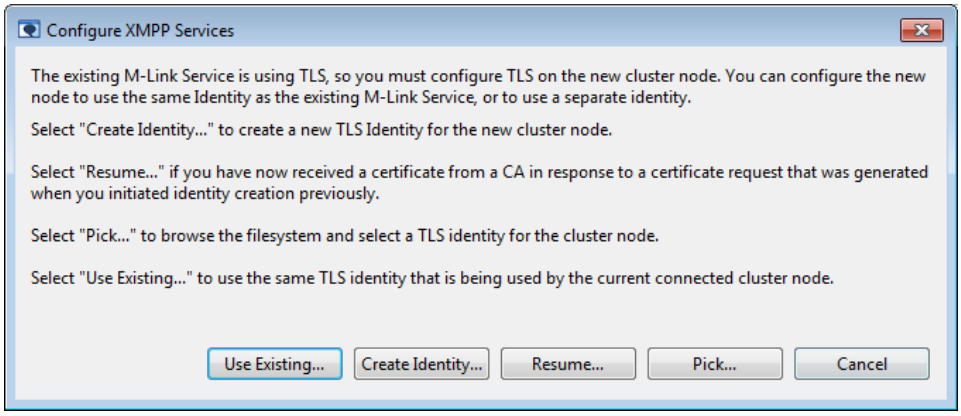
Figure 14.3. Menu to create new cluster node



When adding a new cluster node, one of the first things that M-Link Console checks is whether the existing service is using TLS. If it is, then you will be required to specify an identity for the new server.

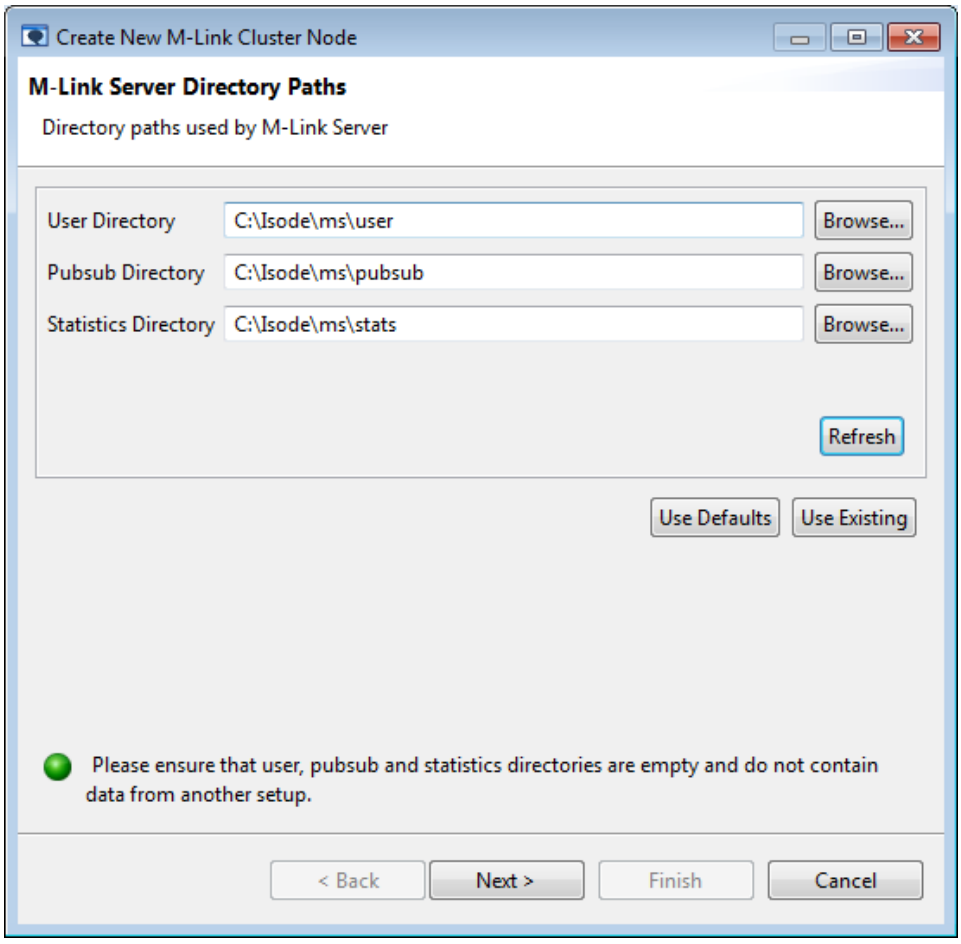
While it is possible to use different identities on different servers in a cluster, it is usually appropriate to have the same identity on each server. The **Use Existing...** button can be used in this case (Should you wish to create a separate identity, the process is described Section 5.3, “Creating a new identity for the M-Link Server”):

Figure 14.4. TLS configuration required when joining a cluster



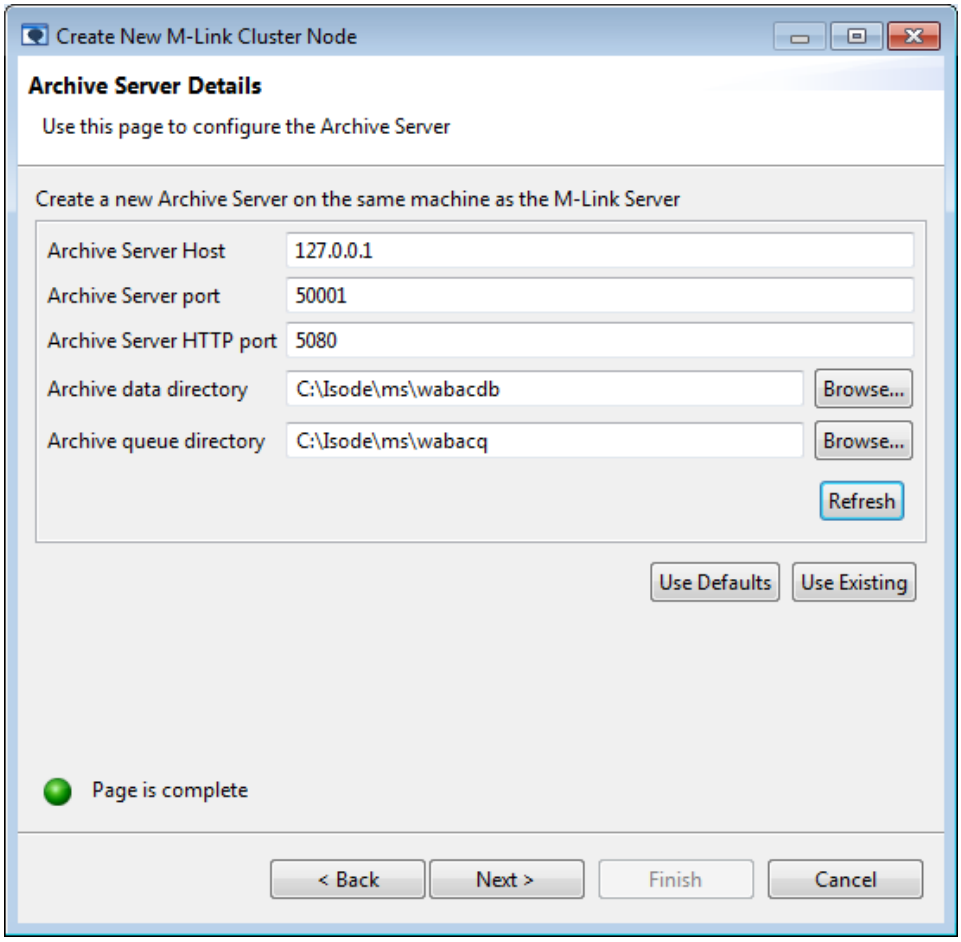
The new node will be using directories on the local filesystem, and so the wizard will require you to provide names of the relevant directories (defaults are suggested):

Figure 14.5. Local directory paths



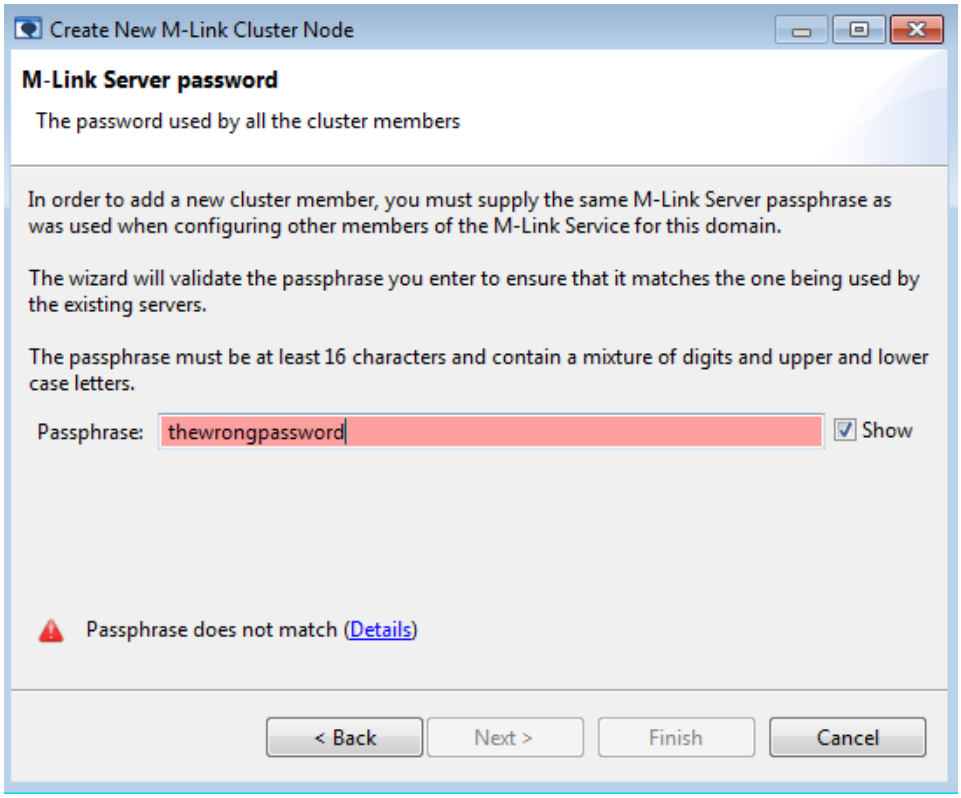
On pressing next, you will be prompted to provide the configuration details of the archive server also called M-Link Archive Server (see Chapter 15, *Archive Management*). The description for the configuration parameters for M-Link Archive Server can be found in the appendix starting from Section H.1.135, "Archive Server Host". The wizard will suggest suitable defaults which can be modified on this page.

Figure 14.6. Archive Server Database Details



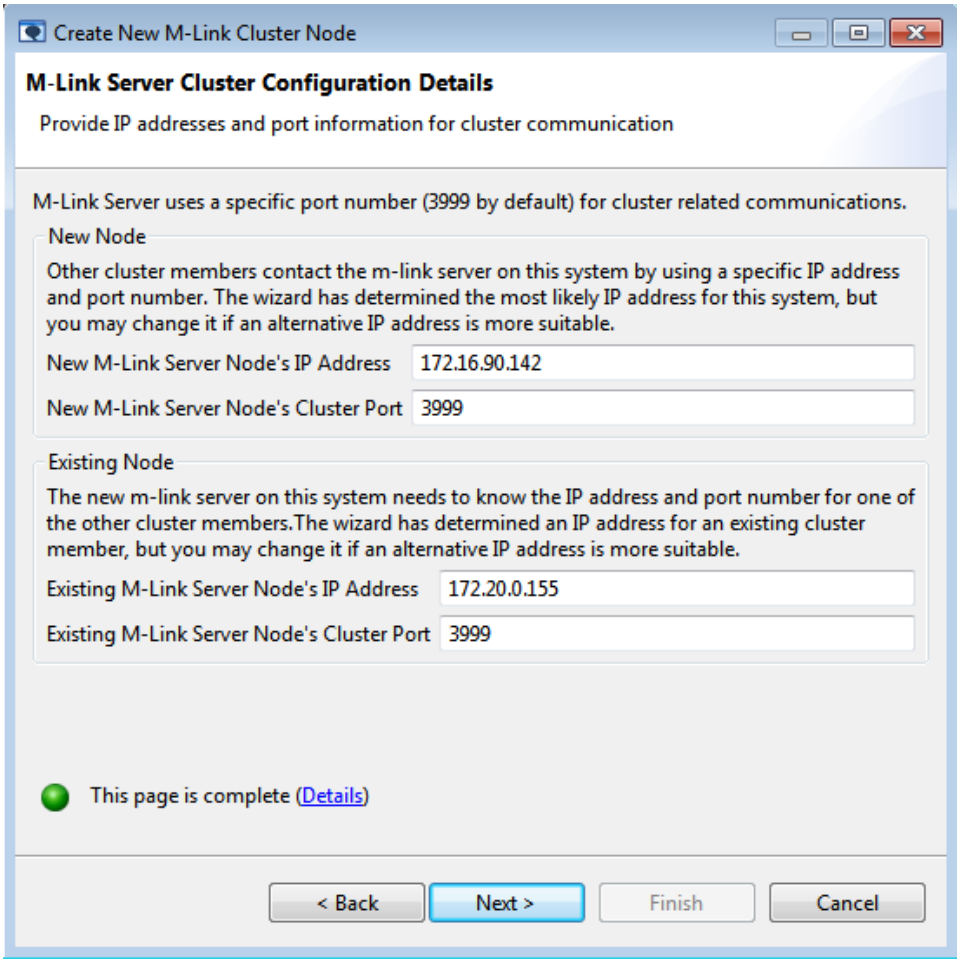
Next, you need to enter the M-Link service passphrase. This is the same passphrase that you specified when the initial M-Link Server was created (see Figure 2.21, “M-Link Server passphrase”). The wizard will not let you proceed until you have entered the correct passphrase.

Figure 14.7. M-Link Service password



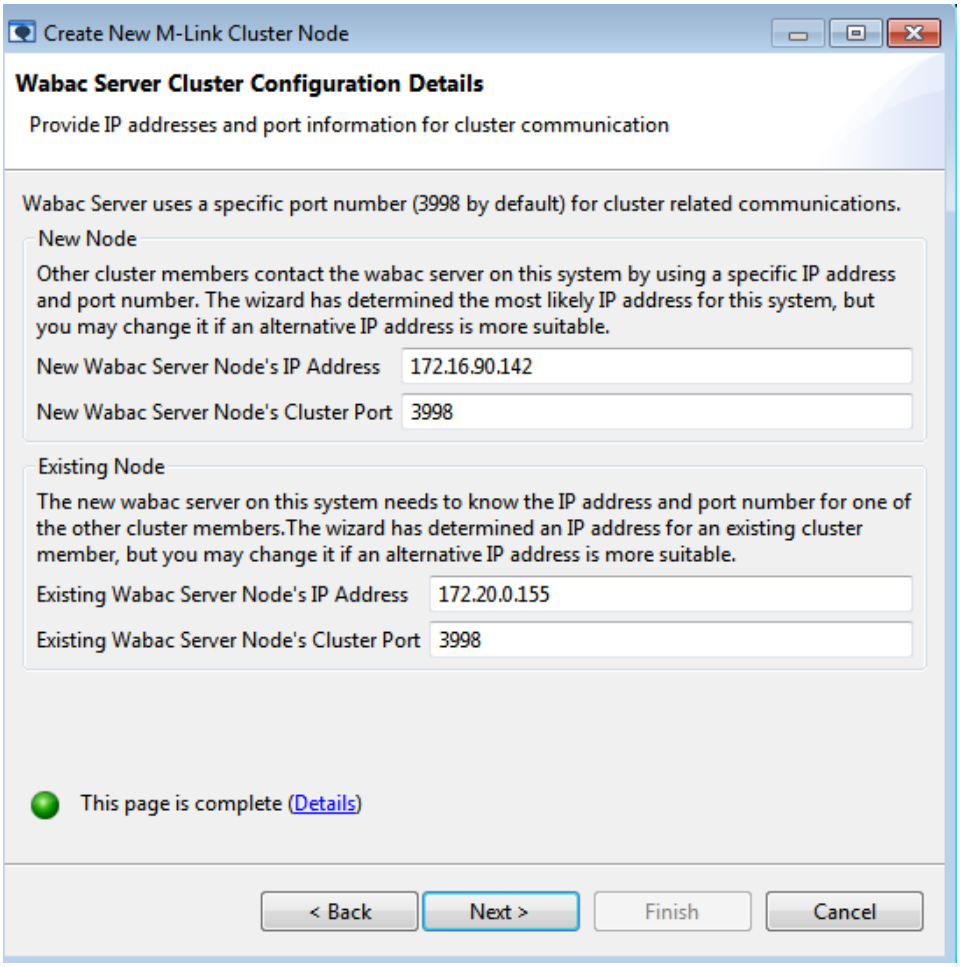
The last thing to be considered is the IP address and port numbers that are used for intra-cluster communication. The wizard will fill in values for you based on what configuration it detects, and in most cases these will be suitable. For systems where you have multiple IP addresses defined, or when you have other applications using specific port numbers, you can override the values suggested by the wizard.

Figure 14.8. Cluster IP address and port numbers



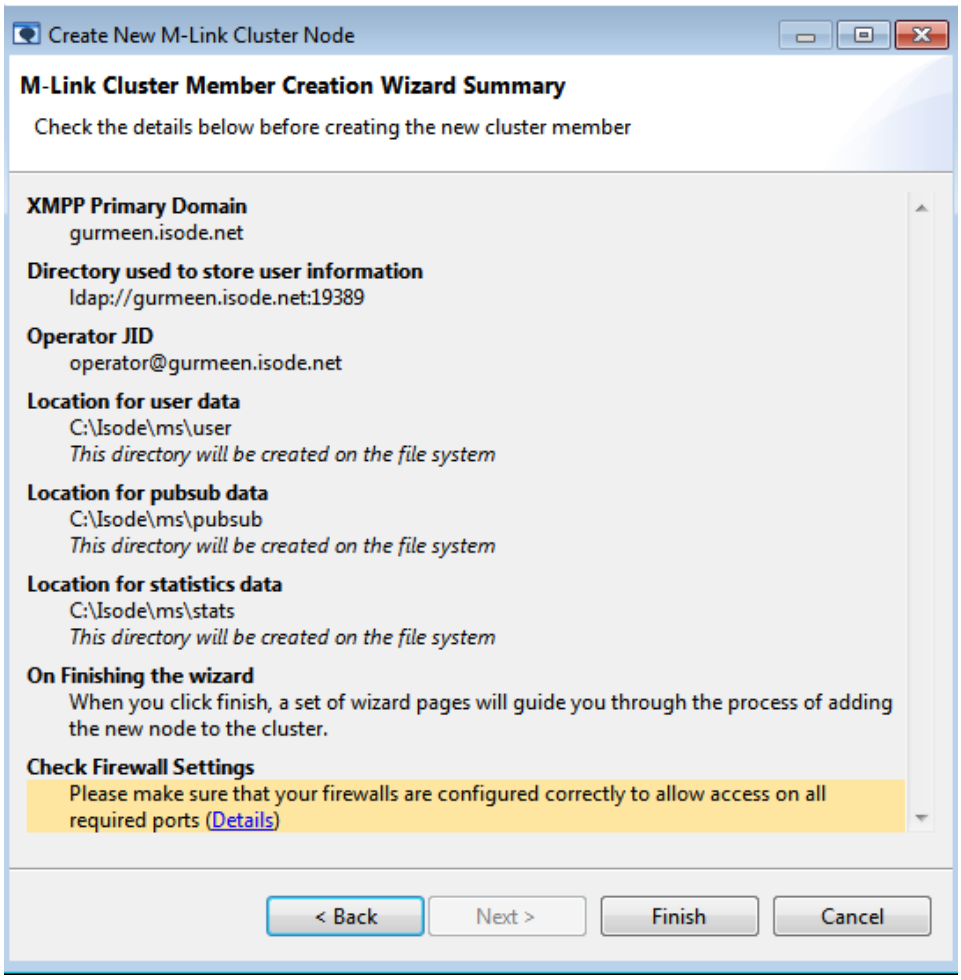
On pressing **Next** a similar page will appear for providing the IP addresses and port numbers of the Archive cluster as shown below:

Figure 14.9. Wabac IP address and port numbers



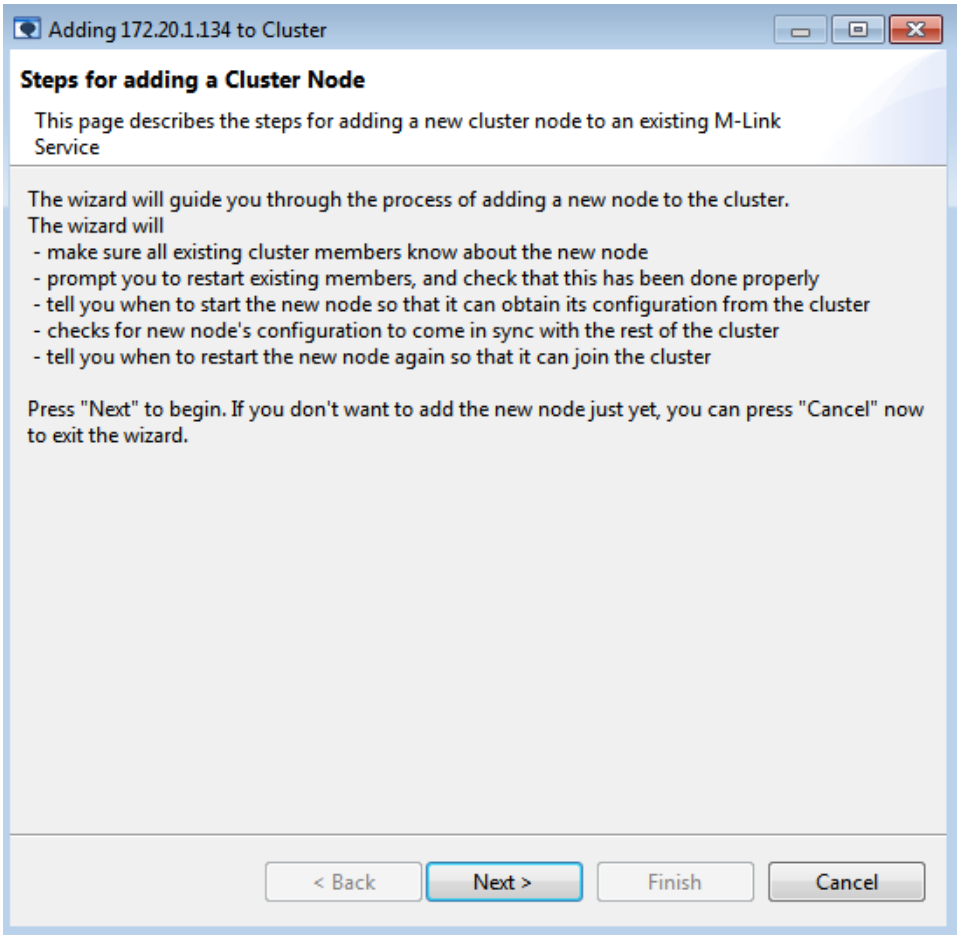
Finally, the wizard displays a summary page confirming the information you have provided that will be used to create the configuration for the new cluster member.

Figure 14.10. Cluster creation summary



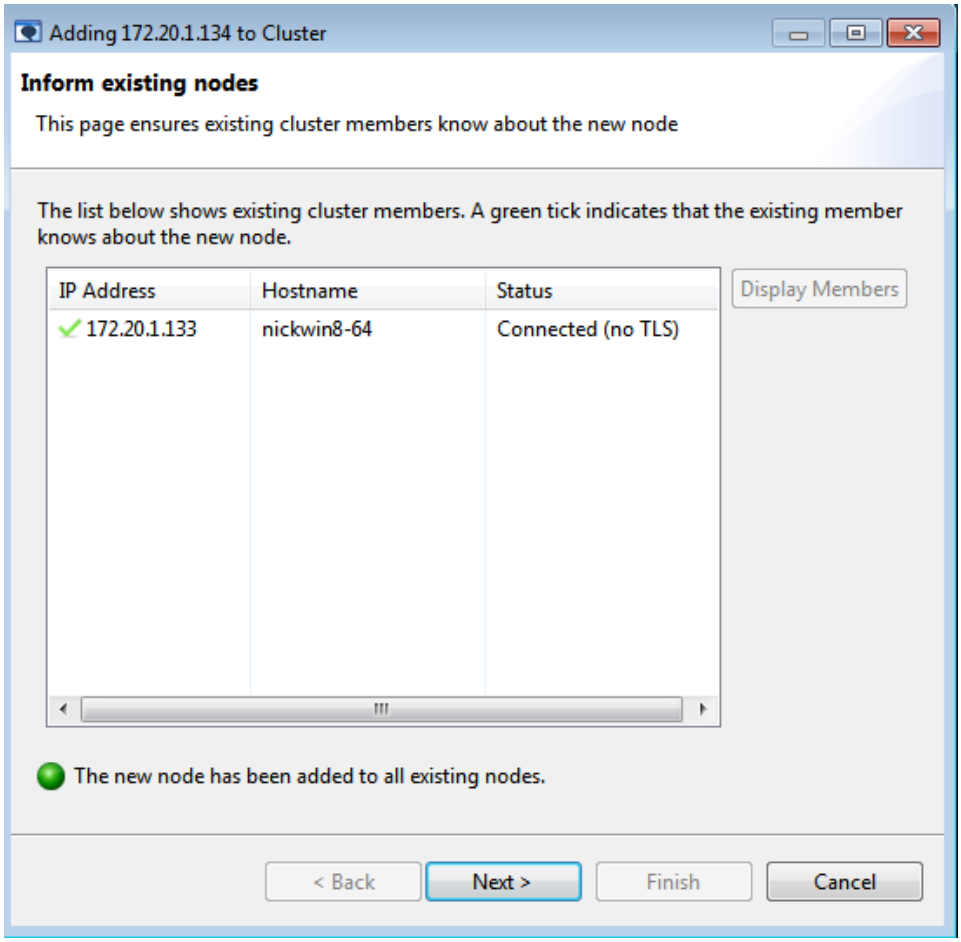
For the newly configured server to become a cluster member, the other cluster members have to be restarted. A follow-on wizard is used to guide you through the steps involved:

Figure 14.11. Steps to add a new node to a cluster



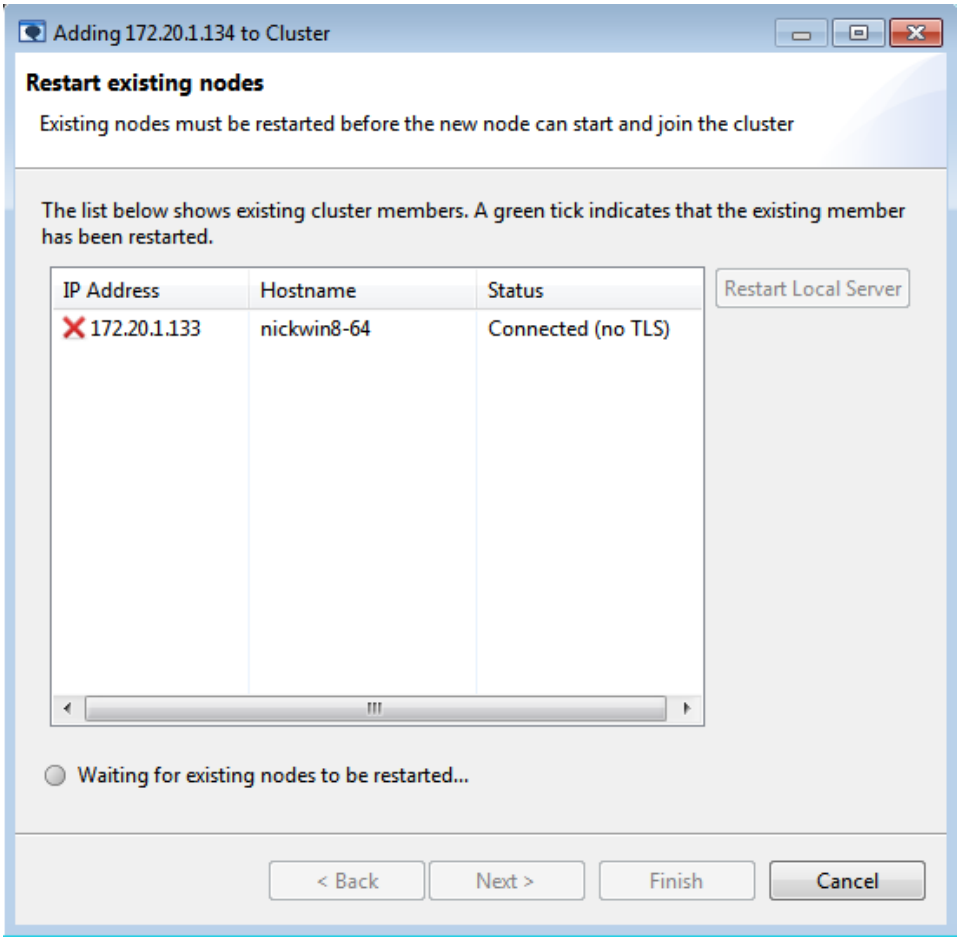
The first stage is for M-Link Console to tell all the existing cluster members about the new node. The wizard will wait until the other member have been updated, and so you must ensure that all other cluster member(s) are online and accessible:

Figure 14.12. Informing existing nodes of a new cluster member



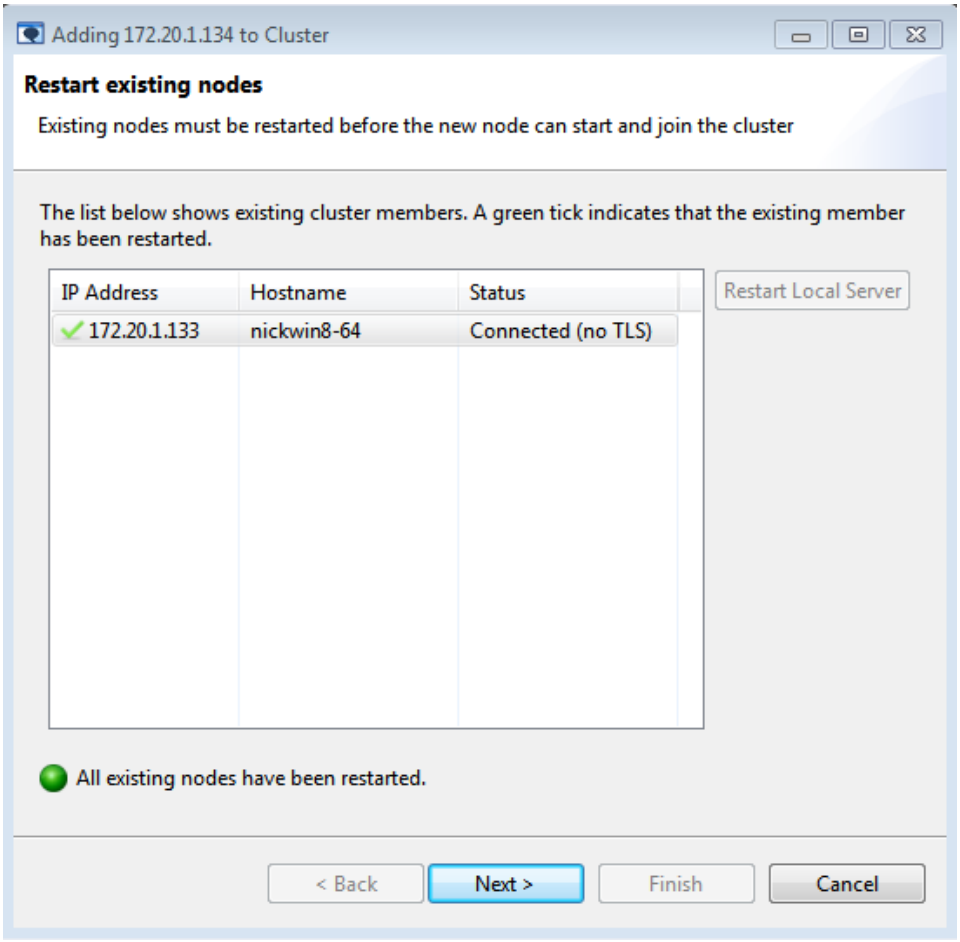
Once existing cluster members have been informed about the new cluster member, they must be restarted. M-Link Console cannot remotely restart them, and so waits for the administrator to perform this action:

Figure 14.13. Waiting for cluster members to restart



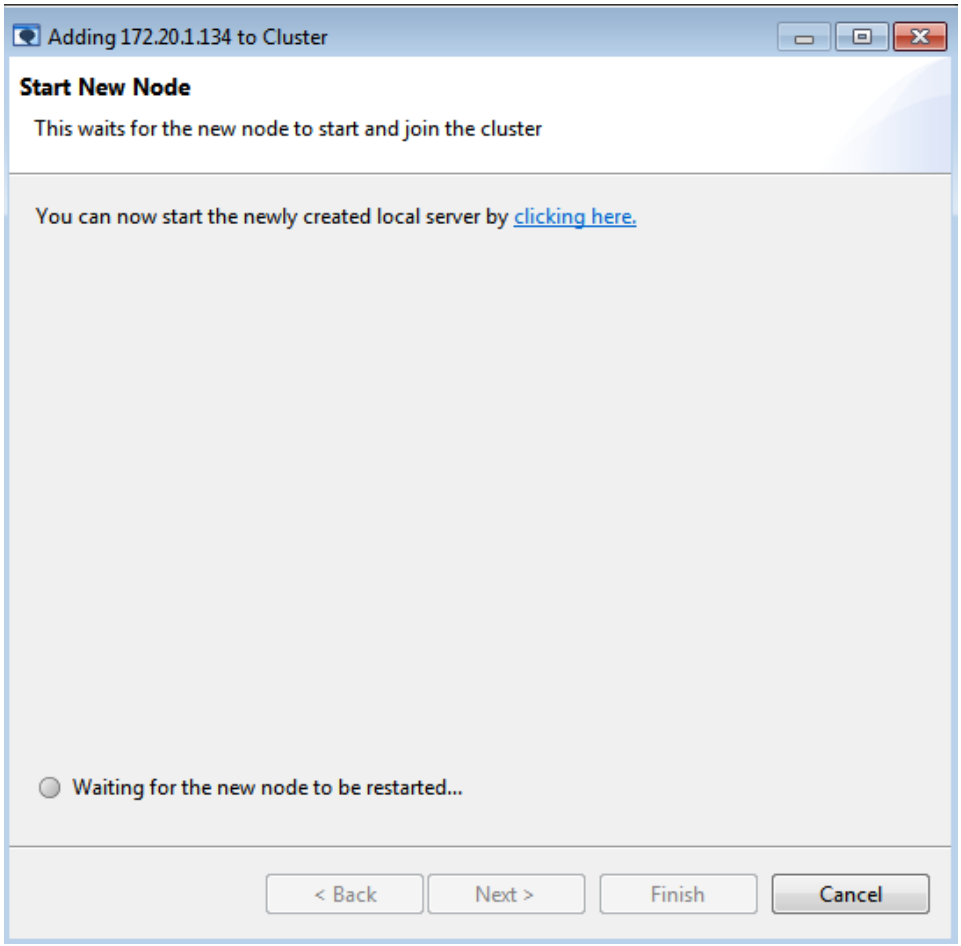
M-Link Console will indicate when the other members have been restarted:

Figure 14.14. Existing cluster members restarted



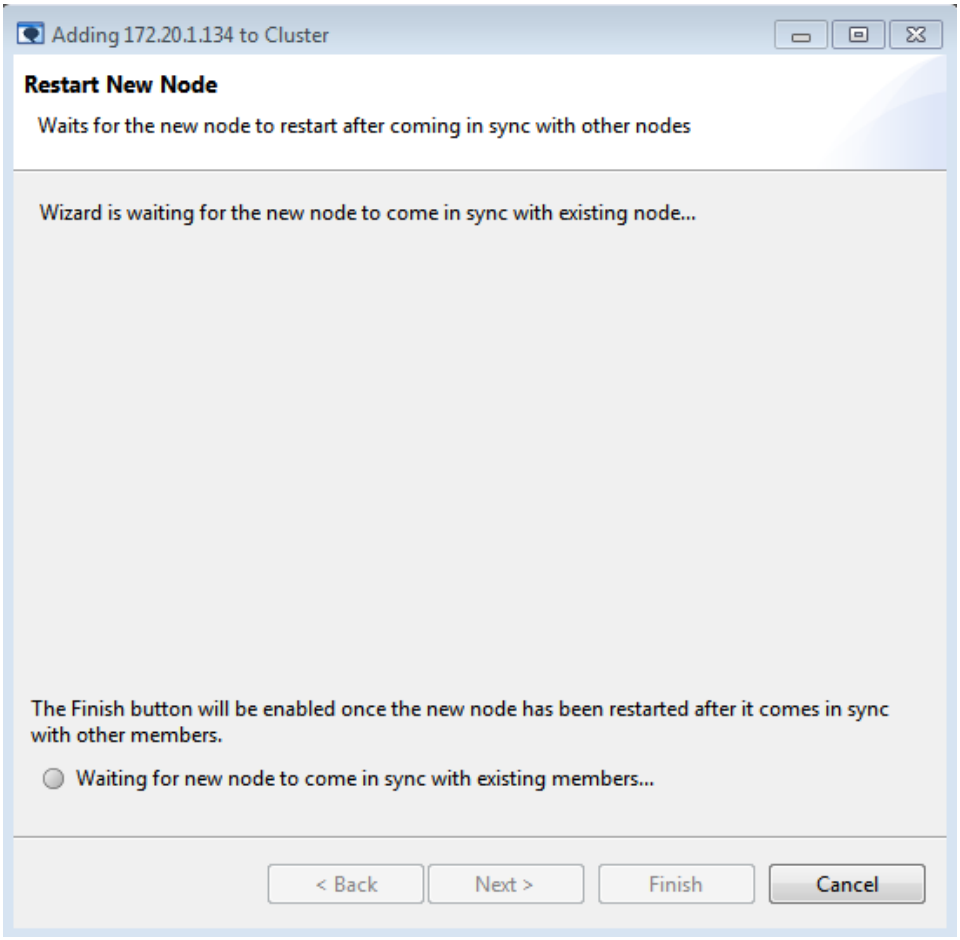
The next step is to start the new node so that it can update its configuration from the cluster:

Figure 14.15. Ready to start new node to update configuration



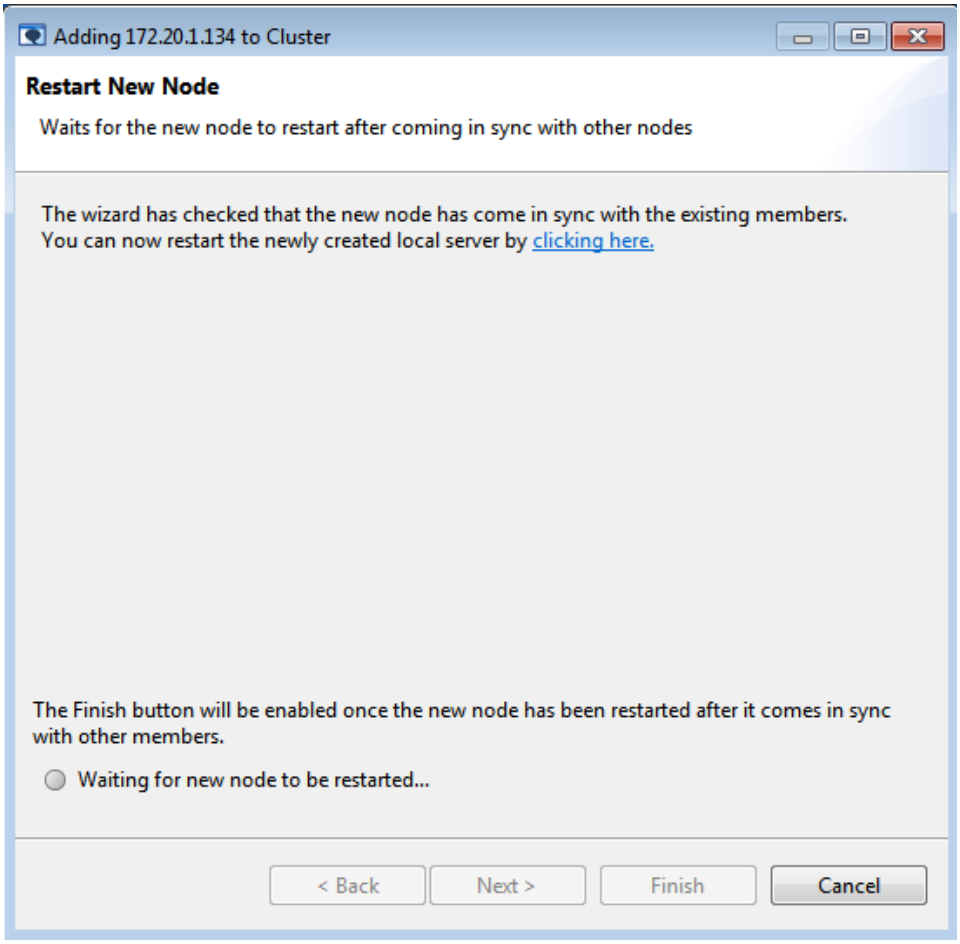
The wizard will check for the new node's configuration to come in sync with the rest of the cluster after it has been started:

Figure 14.16. Check new node's configuration to come in sync



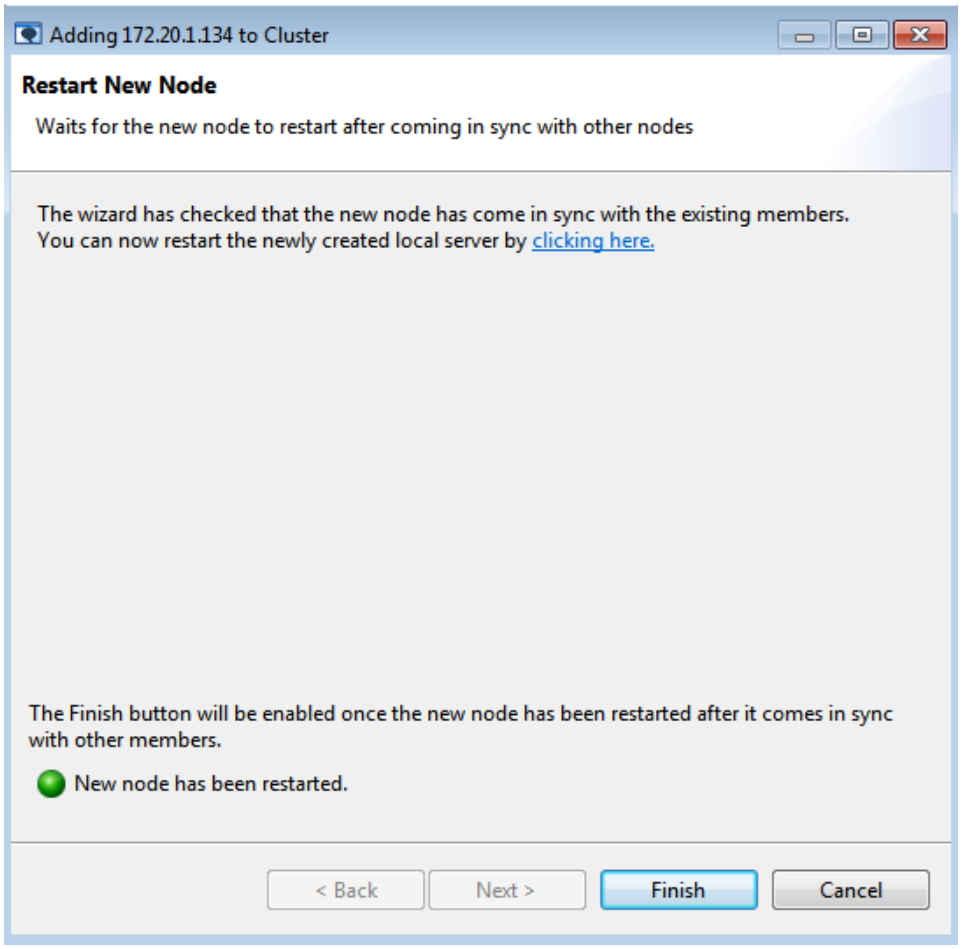
Once the new node comes in sync with the rest of the cluster, it needs to to be restarted for the configuration to take effect:

Figure 14.17.



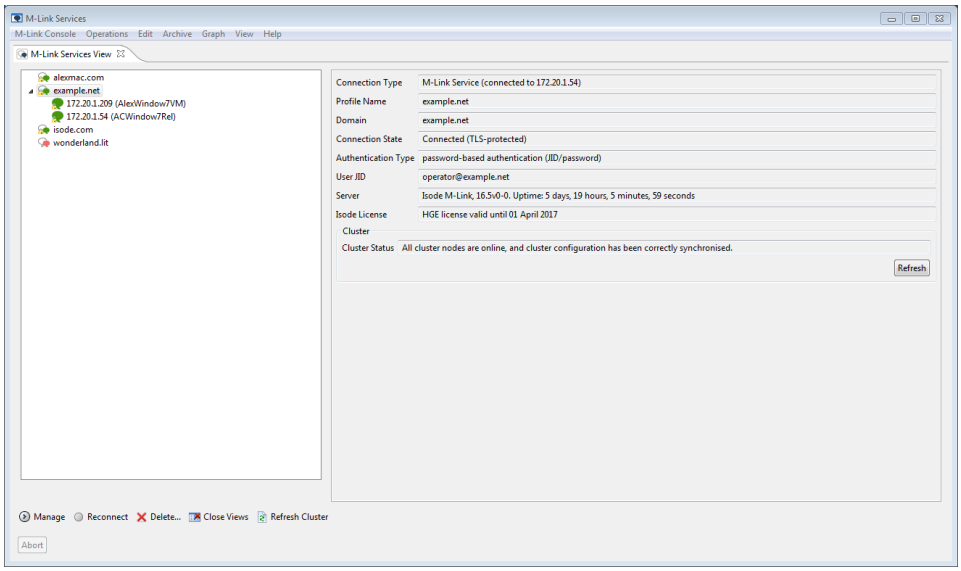
The restarting of the new node is the final step which leads to finishing of the wizard:

Figure 14.18.



The newly started node will appear in the Services view, with a "green" status (along with a padlock, if the connection is using TLS):

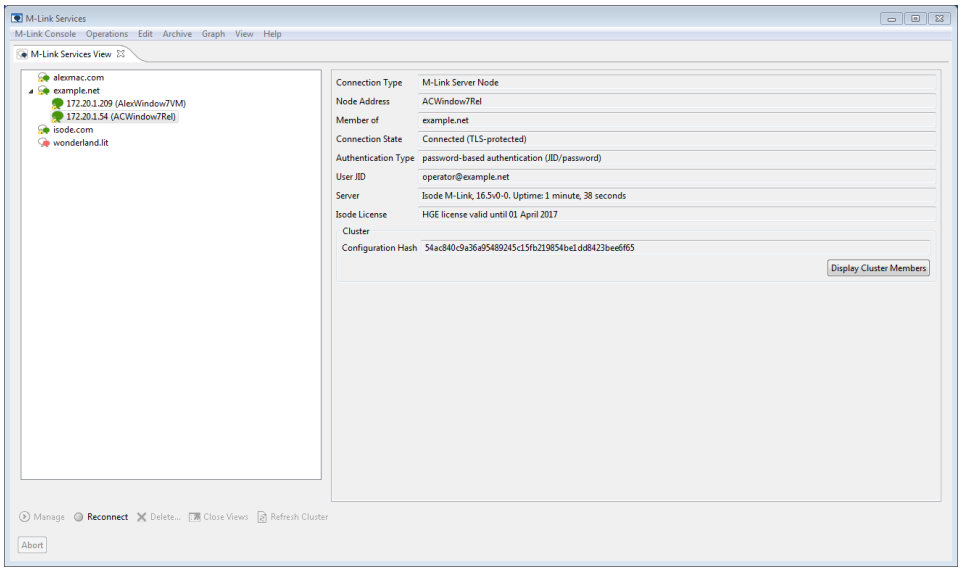
Figure 14.19. New cluster node added



When the cluster is operating, member nodes will synchronize service configuration. When it is correctly synchronized, the *configuration hash* value (obtained using see Section G.52, "Get Hash (Node)") will be the same on each node of the cluster. M-Link Console uses this value to check whether there is a possible synchronization issue, and displays the result of its check in the *Cluster Status* field in the services view (see the previous screenshots).

If there is a problem with cluster synchronization, you can look at individual nodes in a cluster to determine the exact value of their configuration hash, which is visible in the services view when you select a particular node:

Figure 14.20. Cluster member configuration hash

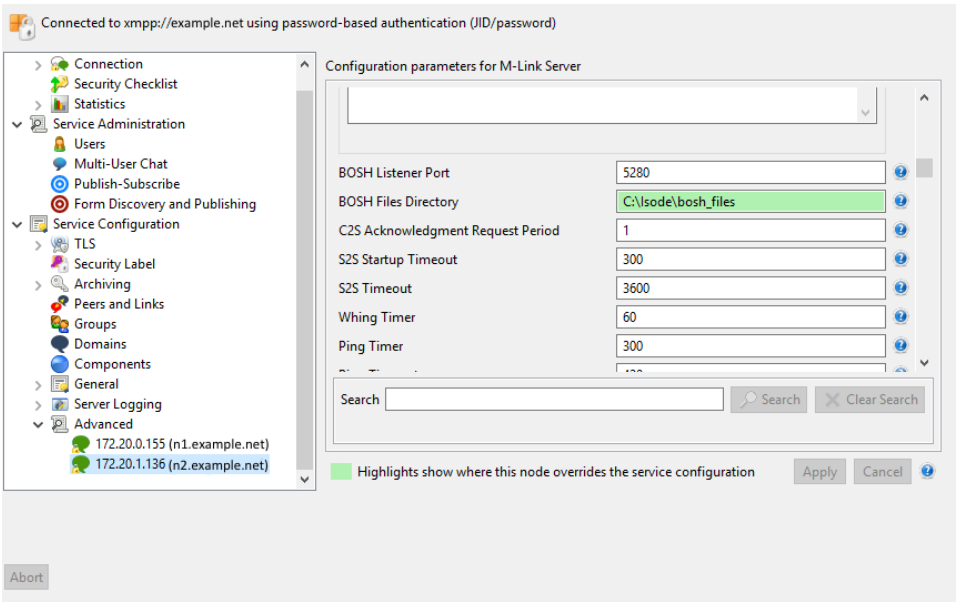


One time when it may be useful to note the configuration hash values is if a cluster of more than two servers is failing to synchronize, in which case it may be possible to ascertain which of the servers has a problem (if it reports a hash value different from all the other cluster members).

14.7 Specifying node-specific configuration

When you open the *Service View* to manage a clustered service, some of the configuration elements will appear as expandable items, to reflect the fact that certain service-wide configuration can be overridden on a per-node basis. For example, configuration parameters that contain filenames may well be different on each node of the cluster. To view node-specific configuration, select the item in the left hand pane corresponding to a node. The right hand pane will show the configuration for that node: where the configuration for a node is *different* to the service-wide configuration, the value will be highlighted:

Figure 14.21. Node-specific overriding of configuration



In the screenshot above, the node *n2.example.net* is configured to serve bosh files using a locally configured directory path. Because this value differs from the shared configuration that would otherwise be used, the editor highlights (in green) the node setting. A tooltip will show the service configuration for the parameter concerned.

If you make a change in the node-specific configuration editor, then the editor will highlight the value in this way, unless you happen to make a change which results in the node-specific value being the same as the service-wide configuration (in which case the value will appear *without* a green highlight).

Chapter 15 Archive Management

This chapter describes the M-Link archiving capabilities.

15.1 M-Link Archive Server

The M-Link Archive Server is used to archive the XMPP traffic on behalf of M-Link Server. Communication between the M-Link Archive Server and the M-Link Server uses a high performance protocol.

Most stanzas that pass through the M-Link Server using XMPP, covering all types of traffic, are sent to the configured M-Link Archive Server. Key state changes are also sent. The archiving mechanism is asynchronous, and so normal processing of XMPP traffic is not affected by database writes (or reads). The M-Link Server writes queued archive data to disk until they have been transferred to the M-Link Archive Server and acknowledged. This makes archiving resilient to outages and restarts of both M-Link Archive Server and M-Link Server processes.

The M-Link Archive Server normally shares configuration settings with the M-Link Server running on the host system. When M-Link Server configuration is reloaded, it signals the M-Link Archive Server to reload its configuration.

15.2 User Access to Archives

End user access to the archives is provided using the XMPP extension protocol called Message Archive Management (MAM). XMPP clients that implement MAM issue queries to the M-Link Server which in turn queries the M-Link Archive Server. Standard XMPP authentication and access control applies, so users can only see traffic that they were party to or could have been party to. This includes security label checks (Chapter 7, *Security Labels in XMPP*).

Isode provides the Message Archive Browser, a XMPP over BOSH client that uses MAM to provide user access to the archives.

15.3 Administrator Access to Archives

M-Link Console connects directly to the M-Link Archive Server to provide administrator access to the archive as described in Section 15.7.2, “Using Archive Services in M-Link Console”. A command-line interface is also provided as described in Section A.8, “M-Link Console Archive commands”.

These tools utilize a HTTP based protocol to communicate with the M-Link Archive Server. This Isode internal protocol makes use of JavaScript Object Notation (JSON) objects to communicate information. To allow for customer-developed administrative access tools, this protocol is described in Appendix E, *Administrator Archive Access Protocol*.

Direct access is available only to Section 2.5, “M-Link Server Administrators” and gives them privileged access to all data. Access is authenticated, to ensure that only authorized users access the data, and will generally be TLS protected through the use of HTTPS (`https://`).

15.4 Archive Data and Configuration

M-Link Console allows you to configure archiving for a domain as described in Section 3.2, “Using M-Link Console to manage domain configuration”.

The following data can be archived:

- 1:1 user chat message

  Archiving is done if the option Section H.3.1.31, “Archiving” is set to `all` for the IM domain of the local user(s) in the 1:1 chat. If the service has multiple IM domains, and both users belong to different local domains, then archiving will be done if this option is set for either of the two local domains.

  All children of the <message/> stanza are stored in the archive except Chat State Notifications [*XEP-0085*].

  Such a message is returned in a MAM query on the user's archive if the option Section H.3.1.32, “Enable XEP-0313 Archives Access (MAM)” is set to `true` for the IM domain of the user.

  Free text search can be done on the text contained in the <body/> element of the <message/> stanza.
- *Multi-User Chat* (MUC) groupchat message

  Archiving is done if the option Section H.3.2.11, “Archiving” is set to `all` for the MUC domain of the room.

  All children of the <message/> stanza are stored in the archive.

  Such a message is returned in a MAM query on the room's archive if the option Section H.3.2.12, “Enable XEP-0313 Archives Access (MAM)” is set to `true` for the MUC domain of the room.

  Free text search can be done on the text contained in the <body/> element of the <message/> stanza.
- MUC private message

  Archiving of a private message sent to or received by a local user in a local room is done if the option Section H.3.1.31, “Archiving” is set to `all` for the the IM domain of the user.

  All children of the <message/> stanza are stored in the archive.

  Such a message is returned in a MAM query on the user's archive if the option Section H.3.1.32, “Enable XEP-0313 Archives Access (MAM)” is set to `true` for the IM domain of the user.

  Free text search can be done on the text contained in the <body/> element of the <message/> stanza.
- MUC subject

Archiving is done if the option Section H.3.2.11, “Archiving” is set to `all` or `events-only` for the MUC domain.

All children of the <message/> stanza are stored in the archive.

The subject is returned in a MAM query on the room's archive if the option Section H.3.2.12, “Enable XEP-0313 Archives Access (MAM)” is set to `true` for the MUC domain of the room.

Free text search can be done on the text contained in the <subject/> element of the <message/> stanza.

- MUC events

  Archiving is done if the option Section H.3.2.11, “Archiving” is set to `all` or `events-only` for the MUC domain.

  Only the relevant information in the stanza is stored in the archive.

  Free text search can not be done.

  The following events are archived:

  - Room creation
  - Room destruction
  - Room configuration change
  - User joining the room
  - Occupant nickname change
  - Occupant availability status change
  - Kicking an occupant
  - Occupant leaving the room
- *Publish-Subscribe* (PubSub) data

  Archiving of a node item created by a local user is done if the option Section H.3.3.12, “Archiving” is set to `all` for the PubSub domain of the node.

  The node items are returned in a MAM query on the PubSub archive if the option Section H.3.3.13, “Enable XEP-0313 Archives Access (MAM)” is set to `true` for the PubSub domain of the node.

  Free text search can be done on the text contained in the node items.
- PubSub events

  Archiving is done if the option Section H.3.3.12, “Archiving” is set to `all` or `events-only` for the PubSub domain.

  Only the relevant information in the stanza is stored in the archive.

  Free text search can not be done.

  The following events are archived:

  - Node creation
  - Node deletion
  - Publishing an item
- Statistics

  This is a type of PubSub data. The statistics domain is a PubSub domain and behaves like any PubSub domain with respect to archiving. Each node of the PubSub corresponds to a type of statistic that the M-Link Server generates. The list of supported statistic

nodes can be obtained by sending a Service Discovery Items request to the statistics PubSub domain.

More details are given in Section 17.3, “Live Statistics”.

- Form Discovery and Publishing (FDP) [*XEP-0346*] templates and published forms

  This is a type of PubSub data. The FDP domain is a PubSub domain and behaves like any PubSub domain with respect to archiving. The list of nodes can be obtained by sending a Service Discovery Items request to the FDP domain.

  More details are given in Section 10.5, “ Using M-Link Console to manage Form Discovery and Publishing”.

- *Personal Eventing Protocol* (PEP) [*XEP-0163*] data

  This is treated as *Publish-Subscribe* (PubSub) data. The list of supported PEP nodes can be obtained by sending a Service Discovery Items request to the user JID.

  Archiving of PEP data is done if the option Section H.3.1.31, “Archiving” is set to `all` for the IM domain of the local user.

  PEP data is returned in a PubSub-like MAM query on the user's archive if the option Section H.3.1.32, “Enable XEP-0313 Archives Access (MAM)” is set to `true` for the IM domain of the user.

- Component traffic

  Archiving of traffic to and from the component (for example, 1-1 messages) is done if the option *archiving* is set to `all` for the component.

  MAM queries can not be done to components.

15.5 Clustering and Archiving

The clustering of the M-Link Server is described in Chapter 14, *Clustering*.

In a clustered configuration, Isode recommends running an M-Link Archive Server on each cluster node. There is an archive clustering protocol that connects the M-Link Archive Servers on each node, so that each M-Link Archive Server holds information from all cluster nodes. This results in each M-Link Archive Server holding the archived data of the entire cluster, so that searches on any M-Link Archive Server will return results for the whole cluster.

Alternative configurations could be used. For example, a single M-Link Archive Server could be run co-located with one M-Link Server while a second M-Link Server on another node could also connect to it directly. Or neither of the M-Link Servers could have a co-located M-Link Archive Server and could connect to the M-Link Archive Server running standalone on a separate machine. These configurations mean that archive access has a single point of failure.

15.6 Archive Configuration Options

The following options can be used to configure archiving:

- Section H.1.135, “Archive Server Host”
- Section H.1.136, “Archive Server Port”
- Section H.1.143, “Timeout for Archive Operations”
- Section H.1.137, “Archive Database Directory”
- Section H.1.138, “Archive Queue Directory”
- Section H.1.139, “Archive HTTP Server Host”
- Section H.1.140, “Archive HTTP Server Port”
- Section H.1.141, “Enable Archive HTTP TLS”
- Section H.1.144, “Archive Database Journal Mode”
- Section H.1.145, “Archive Include Remote MUCs in User Results”
- Section H.1.142, “XMPP Server shares Archive Server Config”

15.7 Archive Service Management in M-Link Console

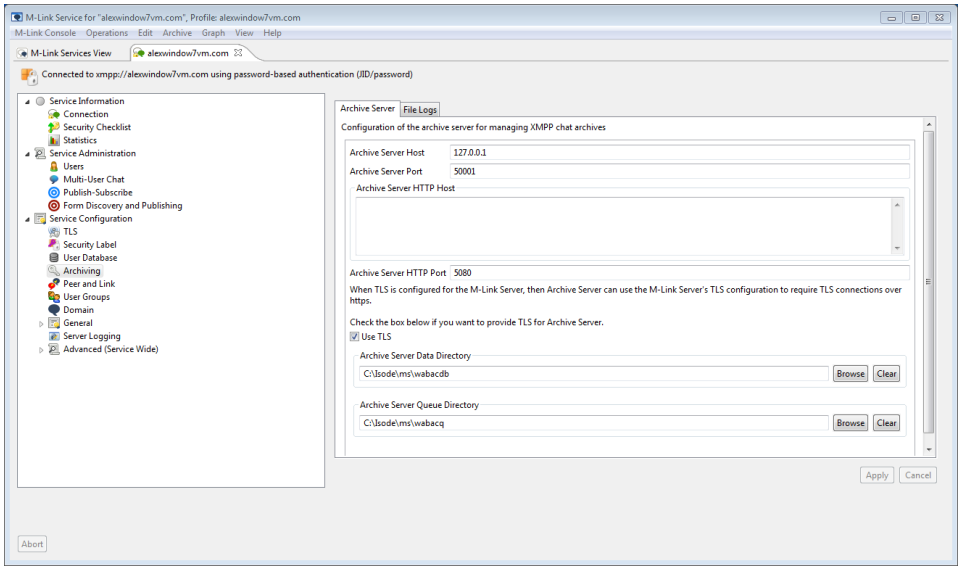
For Section 2.5, “M-Link Server Administrators”, it is possible to query and manage Archive services for a single-node or cluster-node M-Link Server configuration.

15.7.1 Archive Service Configuration in M-Link Console

M-Link Console allows you to manage M-Link Archive Server configuration using a customised editor which appears in the **XMPP Service** view. Note that Isode recommends using node-specific configuration for Archive Service options (i.e. configuration for Archive Services should not be cluster-wide), and so no equivalent editor appears for the cluster-wide M-Link Archive Server Configuration

Select the *Archiving* editor in the service view to see or modify information about current M-Link Archive Server configuration. For a cluster with multiple nodes, expand and select the *node* view to see and modify the configuration.

Figure 15.1. Archive Server Configuration Editor



The description for the configuration parameters for the Archive Service can be found in the appendix starting from Section H.1.135, “Archive Server Host”.

Note that TLS should be enabled on the M-Link Archive Server if M-Link service has been configured to provide TLS and vice versa, as otherwise you will not be able to use Archive Services using M-Link Console

15.7.2 Using Archive Services in M-Link Console

For a profile connected as a *Server* administrator, it is possible to query and manage the Archive service for a single-node or cluster-node M-Link Server configuration. M-Link Server provides both graphical and command line tools for importing and exporting data from the Archive database, as well as an interface to search archive data. The following section details the usage of these tools.

15.7.2.1 Searching the Archives

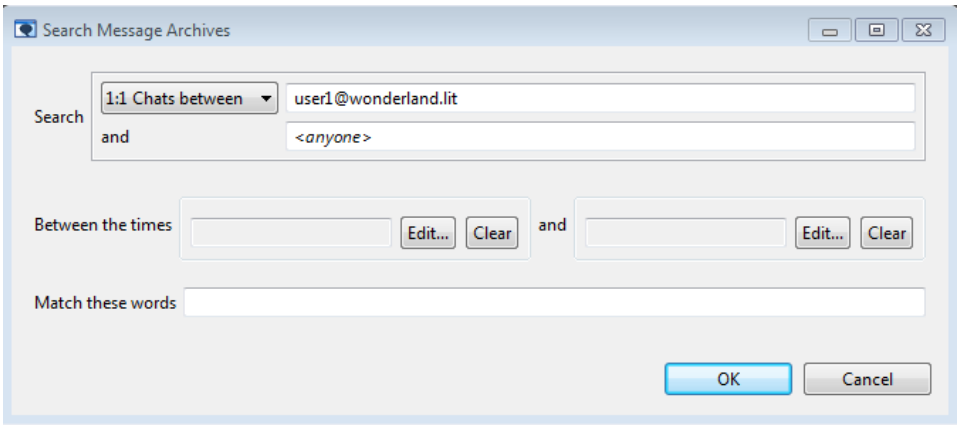
M-Link Server provides an interface to perform search queries on the archives. This enables a *Server* administrator to search for MUC and user chat history, with the option to redact selected messages, perform zoom operations on a selection of messages, or export the current page of results to a file in *PDF/A* format. It is also possible to search the database to see information about submitted FDP forms.

To perform a search, select the **Search...** option from the **Archive** menu. This will display a dialog, allowing you to specify the search parameters. By searching for 1:1 chats, results will include only messages that have been sent to or from a specific person (JID). A search of 1:1 chats will match all messages that are sent to or from the specified JID. If you want to limit these results, you can specify a second JID in the **Chats with**: in this case, only messages exchanged between those to users will be returned.

Select the **Chatroom** option to search for messages that appeared in a specific chatroom (MUC). The dialog will pre-fill the chatroom field with a list of current chatrooms, which means you can select a room from a drop-down list. You can also enter a specific chatroom name, which may be useful if the drop-down list is very large, or if you want to see history for a chatroom that no longer exists.

Select the **FDP Topic** option to search for submitted forms related to a specific FDP topic. The dialog will pre-fill the topic field with a list of current FDP topics, which means you can select a topic from a drop-down list. You can also enter a specific topic, which may be useful if the drop-down list is very large, or if you want to see history for a topic that no longer exists. FDP topics exist in the context of a domain: to specify a topic, use the topic name and domain name separated by an `@` sign, for example `MEDEVAC 9-Line@fdpdomain.wonderland.lit`.

Figure 15.2. Archive Search Tool



In addition, it is also possible to specify a date-time range, limiting the results to messages sent between the specified times. These are optional and one or both date-time parameters may be omitted from a search query, in which case the maximum available time range is returned.

The final parameter is an optional text filter, allowing you to specify a string of text that must be present in the results. Any results that do not contain the specified string will not be displayed. Text searching is not applicable in the case of FDP searches.

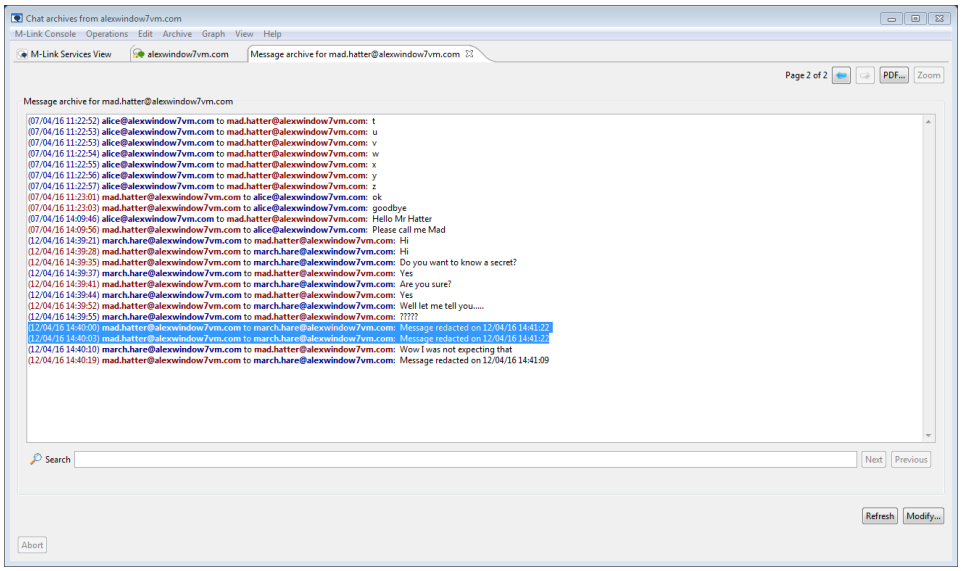
When a search is performed, M-Link Console will query the Archive database, and present the results in a message viewer. This will display the timestamp for the message, the message sender, message recipient, and the message content. If there are redacted messages in the results, these will display the date they were redacted on.

15.7.2.1.1 Message redaction

Redaction is a process whereby content is adapted into a form suitable for publication. Within the context of M-Link Console, redaction of messages refers to the removal of selected message content, preventing the message content from appearing in subsequent search results. This is useful in cases where it may not be possible or desirable to disclose the content of specific search results in search history or exported data. By redacting a message, the content of the message is removed and the message is marked as redacted. Any subsequent searches returning redacted messages will only display the details of the message, excluding the message body. When displaying a redacted message in M-Link Console, text will be displayed in the body of the message indicating that the message has been redacted, specifying the time at which the redaction occurred.

In order to redact one or more messages, select the messages you want to redact with the cursor, and then select **Redact Selected Messages...** from the **Archive** menu. This will prompt you to make sure that you intend to redact the selection.

Figure 15.3. Archive viewer showing a redacted selection



Note that it is not possible to undo a redact operation. Applying the redaction will remove the content of the selected messages. While the contents of a redacted message are permanently removed from the archive, the message header containing the time stamp and sender/recipient address is retained. If a time-based search returns redacted messages, they will be shown in the results view, with a message indicating that they have been redacted. It is also worth noting that some IM clients maintain local chat history, and any such history will be unaffected by a redaction operation.

15.7.2.1.2 Zoom function

The zoom function in M-Link Console is provided to display a selected message from a Archive search query in context, with the immediately chronologically preceding and proceeding messages. Note, this option is only enabled when search results have been filtered according to a specified search term using the '**Match these words**' field in the search dialog, or when a search query has been made within a specified time period, and a result is selected.

When enabled, the **Zoom** button will become enabled on the search results page. The zoom function can also be accessed by navigating to the **Archive** menu.

Zoom will display messages immediately surrounding the selected message, and continue to zoom out with subsequent zoom operations, increasing the number of visible search results surrounding the selected message. This is useful in situations where a message from a search query needs to be viewed in context. The results of the zoom operation result are displayed in a new tab.

Where a search term has been provided in a search query, only results containing that term will be displayed. This means that the chronologically preceding and proceeding messages are not necessarily visible, depending on whether they contain the search term or not. By selecting a message from the search results, and selecting the **Zoom** button, chronologically preceding and proceeding results will be displayed regardless of whether they contain the search term.

Where a time period has been specified, results will only be displayed if the time-stamp for each message falls within this period. This may exclude immediately surrounding messages, depending on the time-stamp of each message. In this context, the **Zoom** button will display chronologically preceding and proceeding messages regardless of their time-stamp.

15.7.2.2 Expiring Data

Expiring data is a way to remove data from the Archive database. This can be useful in situations where data can only be retained for a specified time period. M-Link Console provides a *command-line interface* (CLI) and a *graphical user interface* (GUI) for expiring data before a specified date and time.

When performing an expire operation, an expire request is sent to the M-Link Archive Server, which removes all of the data before a specified date and time. Depending on the size of the database, this may take some time to complete, and the operation can not be undone. Both the CLI and the GUI require a mandatory date-time parameter to be specified.

Note that once you have expired any data from the Archive database, you must not subsequently import data to that database if that data contains information which precedes the expiry date.

15.7.2.2.1 Expiring data using the command line interface

The basic syntax required in order to expire data using the CLI is as follows:

```
expire --user (ADMINISTRATOR_JID) --pwd (PASSWORD)
 --expdate (EXPIRY_DATE)
```

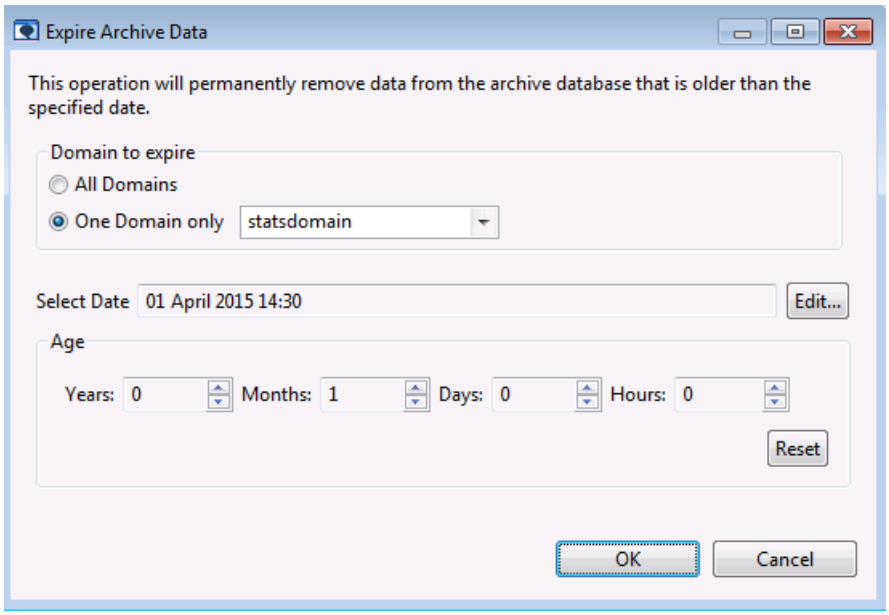
Running the expire command will prompt you to confirm that you want to remove all data before the specified date-time. Proceeding will remove the archive data and return a completion message when the operation has finished.

A summary of the expire command and any optional parameters can be found in Section A.8.4, “Expire parameters”.

15.7.2.2.2 Expiring data using the graphical user interface

In order to expire data using M-Link Console, select the **Expire...** option from the **Archive** menu. It is possible to expire data on a single domain, or for all domains. The **Expire Archive Data** dialog allows you to specify the date-time before which all messages will be expired: either by selecting a specific date, or by specifying a time period relative to the current date-time. A confirmation dialog will be shown before the expiration is carried out. Note that expired data cannot be recovered from the archive, so it may be appropriate to back up the archive before performing an expire operation.

Figure 15.4. M-Link Archive Expire Tool



15.7.2.3 Archive Backup

The backup operation is used to create a backup of the M-Link Archive Server database, in a database file format (*.db*). Backups are stored in a *backups* directory in the path specified by Section H.1.137, “Archive Database Directory”, and are named chronologically using the time-stamp. The backup operation differs from an export operation in several ways:

- Unlike an export operation where data is converted into XML or PDF/A, the format of the data does not need to be changed for backup. This means that in many cases a backup operation will execute significantly faster than an export operation.
- Archive data can be cloned into a new M-Link Server installation without having to import the data. To do this, the backup database can be cloned into the Section H.1.137, “Archive Database Directory” directory. More details can be found in Section B.2, “Restore”.

A summary of the backup operation can be found in Section A.8.5, “Backup parameters”.

15.7.2.3.1 Creating backups using the command line interface

M-Link Console facilitates backup of the M-Link Archive Server database through a CLI. This can be scheduled to run on a regular basis for automated backups. The syntax for a backup command is as follows:

```
backup --user (ADMINISTRATOR_JID) --pwd (PASSWORD)
```

15.7.2.4 Importing Data

The M-Link Server enables loading data from an XML file to the archive.

When performing an import operation, the M-Link Archive Server will attempt to validate the provided file(s). On the basis that the provided files are valid archive XML files, M-Link Console will upload the data to the server. In cases where multiple files are being imported, M-Link Console will attempt to upload each file in turn. Any files that can not be imported will be displayed in an error message or dialog.

Note that once you have expired any data from the Archive database, you must not subsequently import data to that database if that data contains information which precedes the expiry date. For more information on data expiry, see Section 15.7.2.2, “Expiring Data”.

M-Link Console provides two methods for importing data, via a CLI or via a GUI.

The XML format of the import is given in Appendix C, *Message Archive Format*.

15.7.2.4.1 Importing data using the CLI

The command line tool can be used to import both single files and directories into the Archive database. Files should contain valid archive XML data, as defined in the schema

The basic syntax required for a single-file import is as follows:

```
import --user (ADMINISTRATOR_JID) --pwd (PASSWORD) --impfn (FILE_PATH)
```

There is also a command to import a directory of archive data from a file based archive. The file-based archive format is discussed in Section 15.8, “File based *auditing* archive”. This can be achieved by using the command:

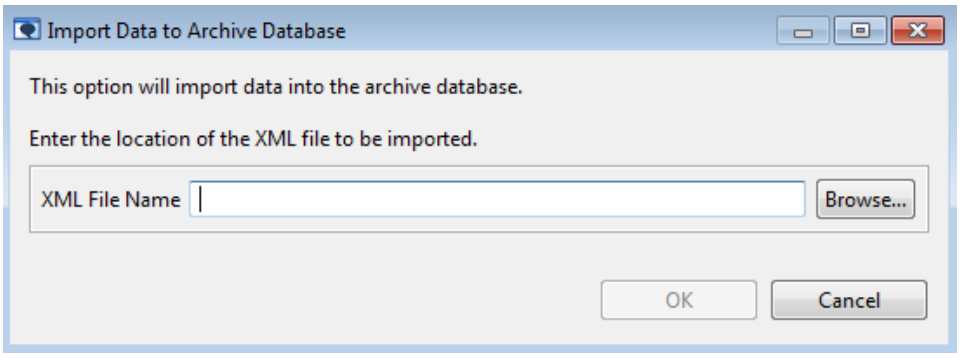
```
importFolder --user (ADMINISTRATOR_JID) --pwd (PASSWORD) --impdn
(DIRECTORY_PATH)
```

A summary of the import command and any optional parameters can be found in Section A.8.1, “Import parameters” and Section A.8.2, “Import folder parameters”.

15.7.2.4.2 Importing data using the GUI

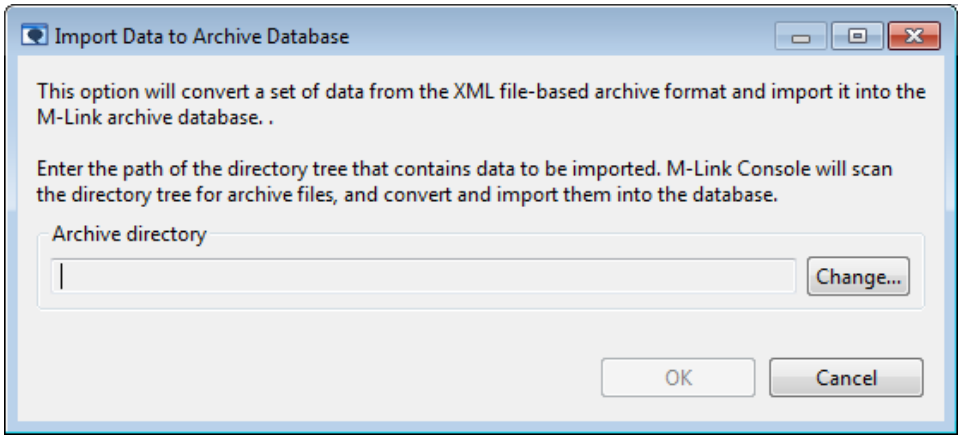
In addition to the command line tool, it is also possible to import data using the M-Link Console import file and import archive options. These are available from the **Archive** menu, under the option **Import**. **Import archive...** can be used to import a single XML file into the Archive database. **Convert and import file-base archive...** can be used to import multiple XML files from a file-based archive format (as described in Section 15.8, “File based *auditing* archive”) into the Archive database.

Figure 15.5. M-Link Archive Import XML Tool



The **Import archive...** option presents a dialog allowing you to select an XML file to import into the Archive database. Once a valid selection has been made, M-Link Console will attempt to upload and import the specified file. If the file can not be validated, or an error occurs during import, M-Link Console will present an error message and any temporary resources created during the import operation will be removed.

Figure 15.6. M-Link Archive Convert and Import Tool



The **Convert and import file-based archive...** option presents a dialog allowing you to import multiple XML files from a file-based archive format (as described in Section 15.8, "File based *auditing* archive") into the Archive database. Upon selecting a parent directory, M-Link Console will scan the directory and any sub-directories for XML files. When the directory scan has completed, any XML files found below the parent directory will be presented in a list where you will have the option to specify which files to import.

15.7.2.5 Exporting Data

The M-Link Server enables exporting archive data to an XML file. It is possible to export data for a specific domain, or for all domains, and to specify what time period the export should include.

The export functionality of M-Link Console can be used to export data from the Archive database to an XML or PDF/A file. This is useful in situations where automated long-term archiving is required as it is possible to schedule an export script or command to execute. For these requirements, PDF/A is a good choice as it provides excellent long term compatibility, the main advantage being that all resources required to reliably render the document are packaged with the PDF/A file. XML export is useful in situations where a backup of archive data is required. This is because it can be imported into a Archive server in the event of a loss of data, loss of hardware or corruption.

When performing an export, M-Link Console sends a request to the server for the archive data. This is then returned as XML data, where it is exported to an XML file, or converted into PDF/A format before being exported to a PDF/A file. M-Link Console provides command line interface tools, and graphical user interface tools for exporting data.

The XML format of the export is given in Appendix C, *Message Archive Format*.

15.7.2.5.1 Exporting data using the command line interface

The basic syntax required to export from the Archive database is as follows:

```
export -user (ADMINISTRATOR_JID) -pwd (PASSWORD) --expfn (FILE_PATH)
-sdate(START_DATE) -edate (END_DATE)
```

The start date (sdate) and end date(edate) are optional time parameters for specifying the time period to export. The "xml" option specifies XML as the output format, if omitted

the output format is PDF by default. When an export operation is in progress, M-Link Console will provide status messages indicating the progress. Depending on the amount of data being exported, and whether conversion to PDF is required, this may take some time to complete. If an error is encountered, the operation will terminate and an error message will be output to the command line.

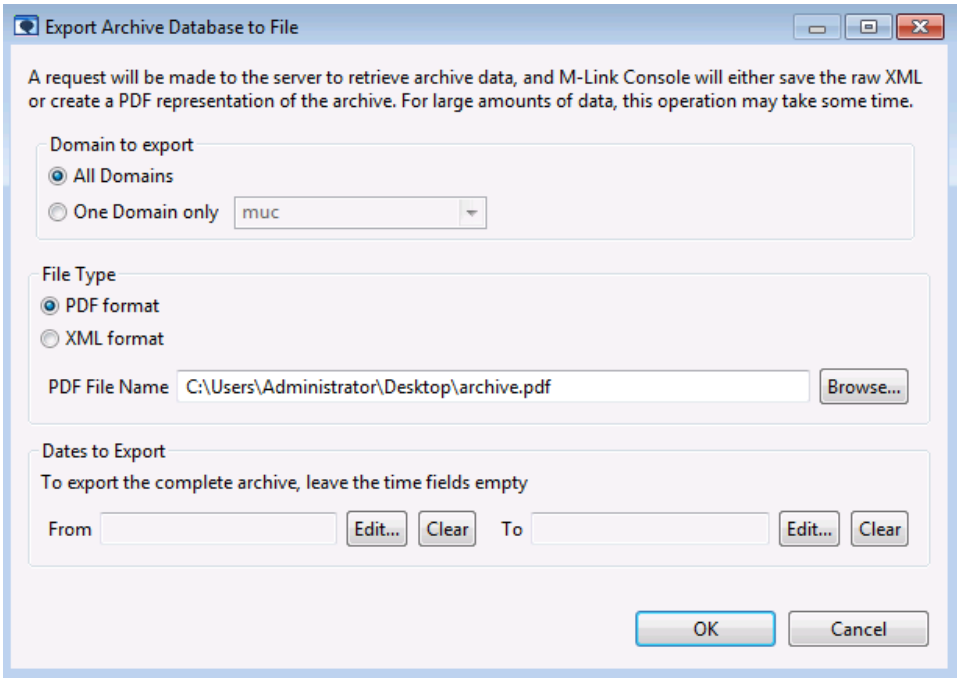
A summary of the export command and any optional parameters can be found in Section A.8.3, “Export parameters”

15.7.2.5.2 Exporting data using the graphical user interface

M-Link Console has an **Export...** option in the **Archive** menu for exporting data from the Archive database. Selecting this option will present a dialog where you will be able to specify the domain to export (if applicable), the file type, either PDF/A or XML, the time period to export, and the output directory. It is possible to exclude one of the time fields, in which case data before/after the specified time will be exported. If no times are specified, the complete archive (for the selected domains) will be exported.

Selecting **OK** will send an export request to the Archive server, which will return the results to M-Link Console. These results are then written to a file. Depending on the size of the database, this may take some time. The progress dialog will display the current stage of the operation and a success or failure dialog will be presented when the operation completes, detailing any errors if applicable.

Figure 15.7. M-Link Archive Export Tool



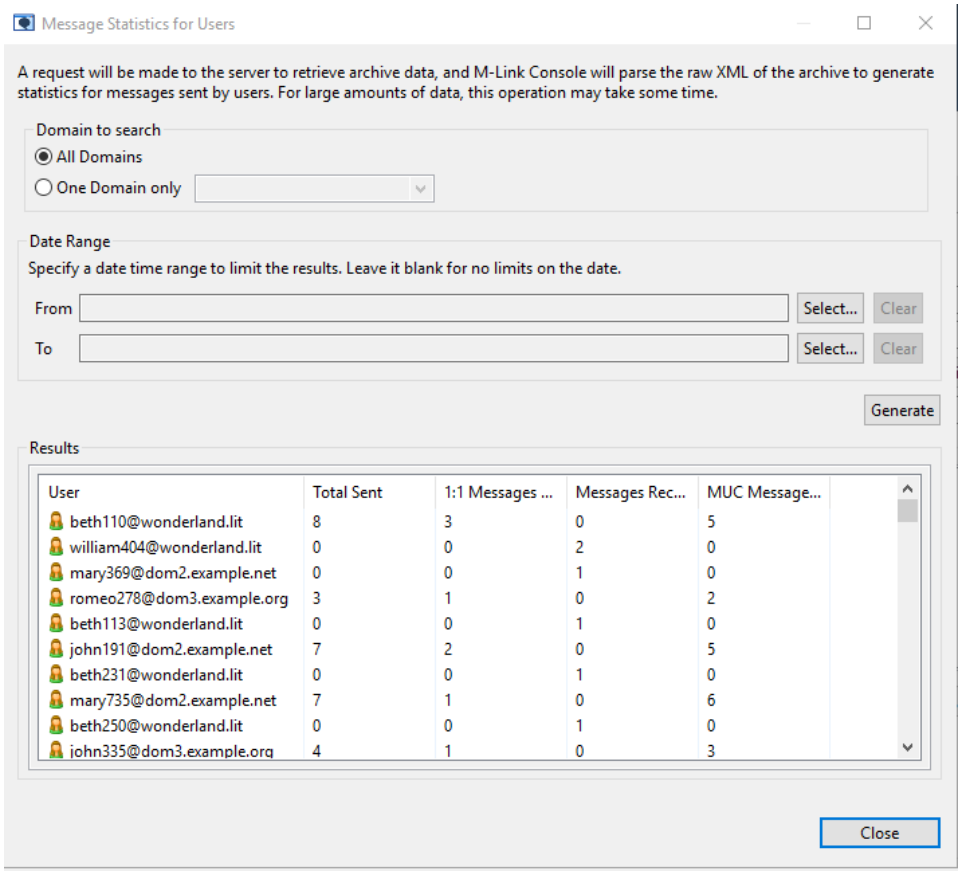
15.7.2.6 Message Statistics

M-Link Console has a **Message Statistics...** option in the **Archive** menu for generating statistics for messages sent and received by the users. A resquest is made to the Archive database to get the XML which is then parsed to generate statistics for each user that appears in the archive XML.

The statistics can be generated either for users of all domains or a selected domain by selecting the option in the **Domains to search** panel. The **Date Range** can be used to limit the results based on a time interval. Press the **Generate** button to generate the statistics.

The results will be displayed in the form of a table containing rows per user. The columns will represent types of message numbers for each user.

Figure 15.8. M-Link Archive Message Statistics



15.8 File based *auditing* archive

> **Note:** This feature is deprecated in favor of using M-Link Archive Server based archiving. M-Link Archive Server provides a superset of the capabilities of file-based *auditing* archives.

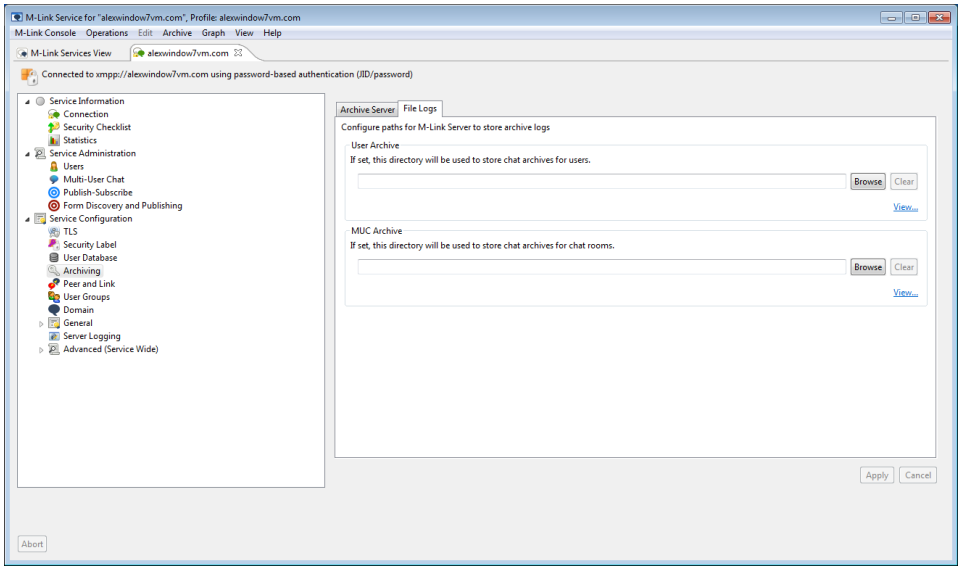
M-Link Server can be configured to provide a file based *auditing* archive, which can be configured to audit all messages sent either by user, by MUC room, or both. This auditing archive is stored in a set of XML files in a filesystem, and a viewer is provided in M-Link Console.

15.8.1 Configuring auditing

The User and MUC audit archive can be enabled by specifying a directory in which to archive in the M-Link Server configuration - see Section H.1.114, “User Audit Archive Directory” and Section H.1.113, “MUC Audit Archive Directory” respectively.

You can use M-Link Console to specify the location of these directories. Since the names of the directories used for log files are likely to be system-specific, M-Link Console recommends setting these paths on the *Node specific* editors, that appear on expanding the **XMPP Logging Configuration** tree item in a clustered configuration. For a single node service, M-Link Console displays a single editor for the service to configure paths on the local node.

Figure 15.9. XMPP Logging Configuration

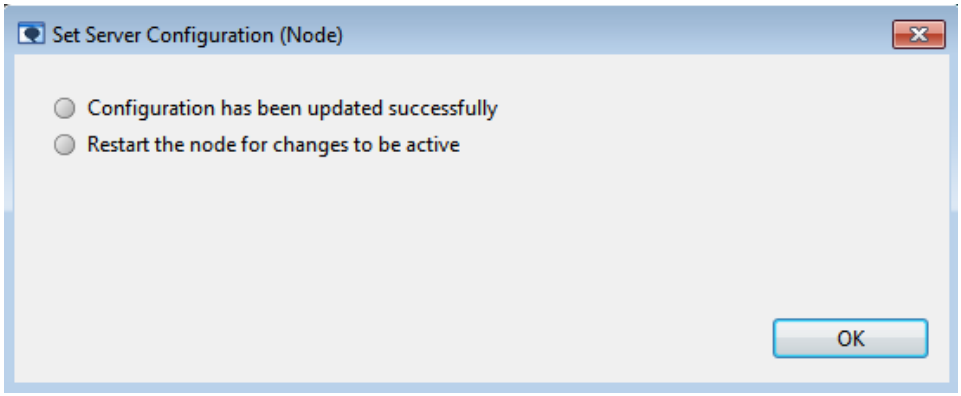


The editor shows the location of the directories for User and MUC audit archives. The following sections describe how to view the User and MUC archive logs

15.8.2 MUC Archives

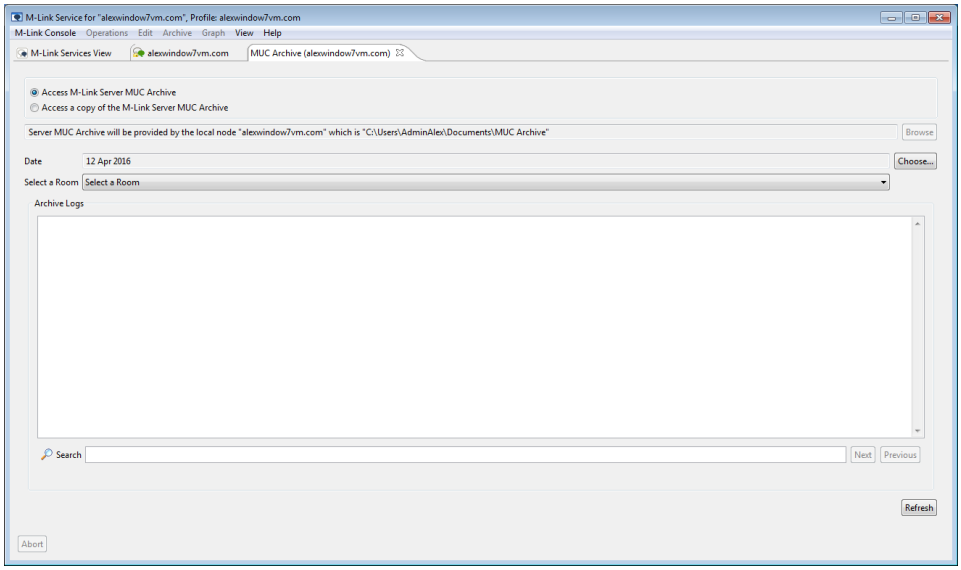
To enable MUC archiving, ensure that a valid directory path is specified (the editor will indicate if you have chosen a path name which does not exist), and press **Apply**. Note that if you set, or change the value of the MUC archive directory, the change will not take effect until the server has been restarted.

Figure 15.10. Restart Server Node



Once a suitable directory has been configured, and the server restarted, you can view MUC archives by selecting the *View...* link on the *MUC Archive* group. For a clustered service, the *View...* link only appears on the Node specific editor and not on the shared cluster-wide editor.

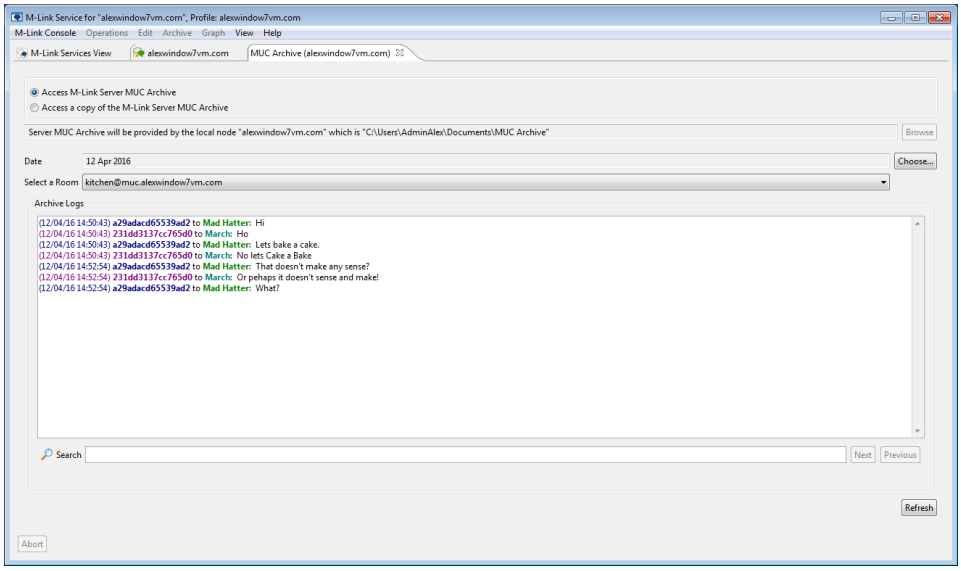
Figure 15.11. Browsing MUC Archives



By default, the editor will assume that you want to read MUC archives directly from the local system (on the assumption that M-Link Console knows where these files are, and has sufficient rights to read them). In some cases though, it may be that M-Link Console does not have direct access to the MUC archives, in which case you can still use its browsing functionality to view the archives, provided you have copied them to a location which M-Link Console *can* read: in this case, select the **Access a copy of the M-Link Server MUC archive** option, and enter the name of a directory where the original MUC archives have been copied to.

Archive log files roll over each day, and so you need to specify which date you are interested in looking at, as well as the room name. Once you have selected a date (using the **Choose...** button) for which logs exist, M-Link Console will display a list of rooms that have archive data for that date in the *Select a Room* combo-box. Select the room whose archive is to be viewed, and the *Archive Logs* dialog will display the appropriate transcript:

Figure 15.12. Browsing MUC Archives

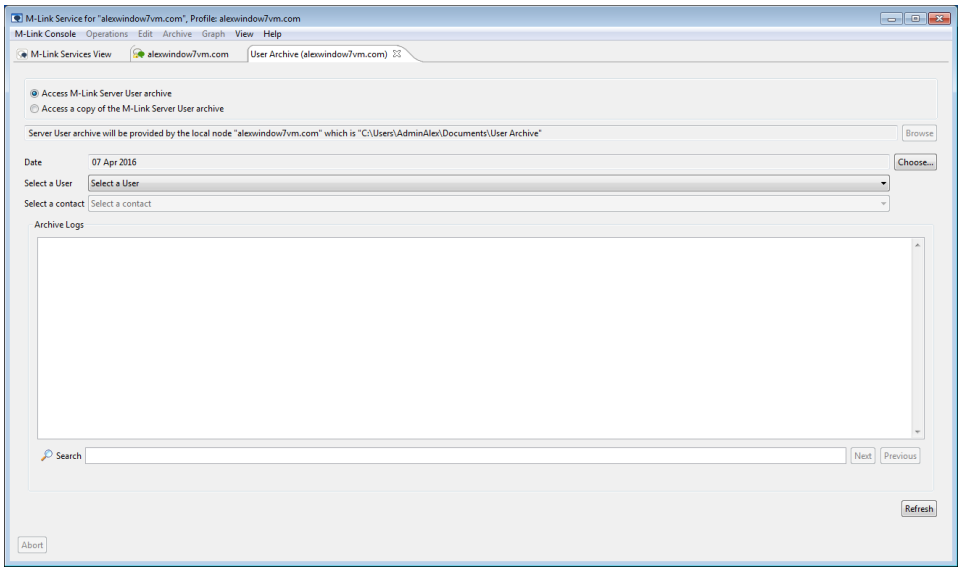


15.8.3 User Archives

You can look at the chat history of specific users if you have configured a suitable user archive directory. Select the **View...** link on the **User Archive** group on **XMPP Logging**

Configuration editor (expand and select the node for a clustered service) on the XMPP service view:

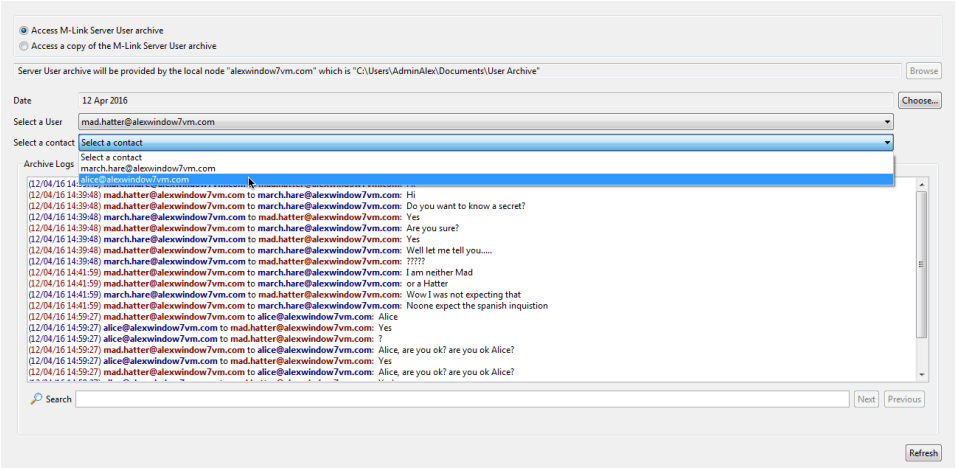
Figure 15.13. Browsing User Archives



By default, the editor will assume that you want to read MUC archives directly from the local system (on the assumption that M-Link Console knows where these files are, and has sufficient rights to read them). In some cases though, it may be that M-Link Console does not have direct access to the user archives, in which case you can still use its browsing functionality to view the archives, provided you have copied them to a location which M-Link Console *can* read: in this case, select the **Access a copy of the M-Link Server user archive** option, and enter the name of a directory where the original user archives have been copied to.

User archive files roll over each day, and so you need to specify which date you are interested in looking at, as well as the user name. Once you have selected a date (using the **Choose...** button) for which logs exist, M-Link Console will display a list of users that have data for that date in the *Select a User* combo-box. Select the user whose archive is to be viewed, and then, optionally, the contact (in *Select a contact* to focus on) will display the appropriate transcript in the *Archives* dialog:

Figure 15.14. Browsing User Archives



Chapter 16 Troubleshooting

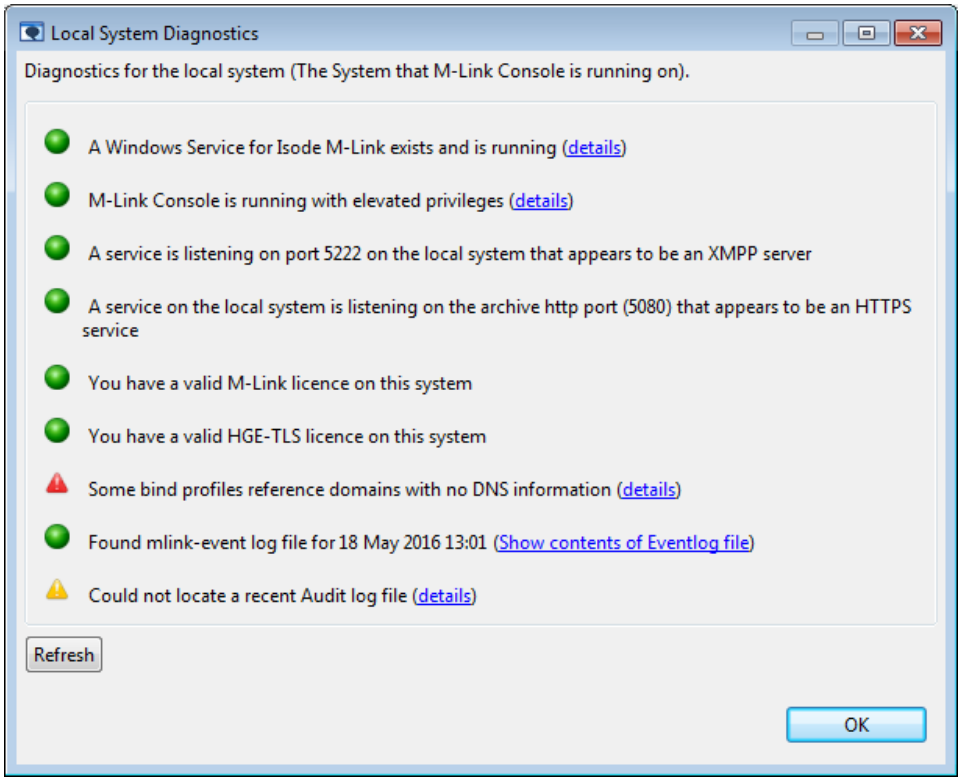
This chapter discusses troubleshooting.

16.1 Local System Diagnostics using M-Link Console

M-Link Console can perform some diagnostic tests on the local system which may provide information that is useful when things do not appear to be working properly, especially if it is running on the same system as the M-Link Server. Some of the tests may reveal simple configuration problems which can be resolved straight away. It will also be useful to include any test results when contacting Isode support.

You can invoke the **Local System Diagnostics** window by using **Help->Local System Diagnostics...**. The window will display the results of a series of tests, as shown below. Note that depending on your system configuration, the set of tests run may be different from that shown.

Figure 16.1. System Diagnostics



For each of the tests, a green icon is used to indicate that the test was successful, a red icon indicates a situation which is likely to mean that functionality is in some way broken or limited, and a yellow icon indicates a potential problem which may or may not impact the service functionality.

Some of the tests performed are described below:

- On Windows, M-Link Server runs as a Windows service. A diagnostic test will report whether a local Windows service for M-Link Server is configured and running.

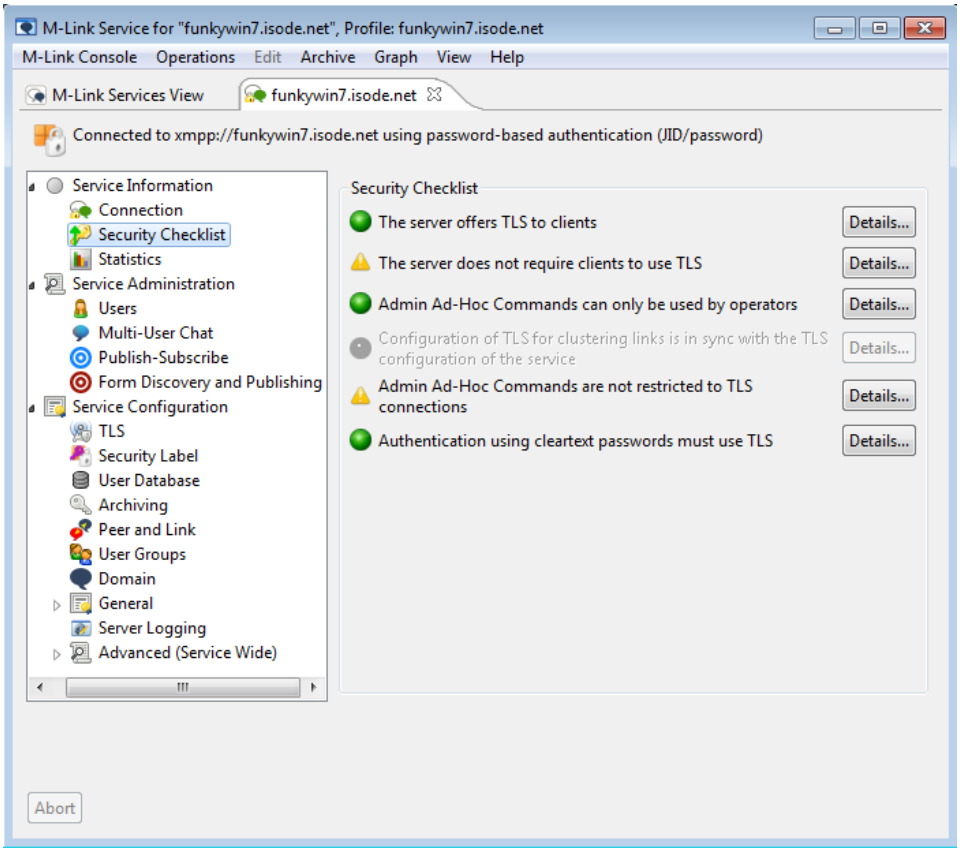
- On Windows, M-Link Console needs to run with elevated privileges (*Run as Administrator*) in order to be able to start and stop M-Link Server, and so a diagnostic will report whether M-Link Console has been invoked in this way.
- Port 5222 is the default port used by an XMPP server which is accepting client connections. A diagnostic test will report whether this port is in use on the local system, and if so whether the server using it appears to be an XMPP server.
- XMPP clients (and other XMPP servers) wanting to connect to an M-Link service commonly use DNS SRV resource records to locate it. Alternatively, clients may use other DNS resource records, such as A and AAAA resource records for the domain. A diagnostic test will check whether any locally configured M-Link Server instances can be located using standard DNS discovery methods.
- The M-Link Server will write to a log file, and so one of the diagnostic tests will verify the existence of a log file in the default location and allow you to view the current log contents. Note that if you have configured the server so that it is logging somewhere other than the default location (see Chapter 18, *Monitoring the M-Link Server*), then the diagnostic may not show any logs.

16.2 Security Checklist

M-Link Console performs some checks on the configured M-Link service and its nodes to check the security aspects of the XMPP service.

The checks are displayed on the **Security checklist** editor of the XMPP service view.

Figure 16.2. Security Checklist



For each of the checks, a green icon is used to indicate that the service is secure, with respect to, the security aspect being tested, a red icon indicates that the configuration may cause a security threat, and a yellow icon indicates a security warning. The details for each check will be displayed by clicking the **Details...** button for the check.

Some of the checks that are performed by M-Link Console are described below:

- An M-Link service can offer *Transport Layer Security* (TLS) to its clients. A check will report whether the service offers TLS to its clients.
- There are checks for the availability of administrative Ad-Hoc Commands based on the group of the connected user and type of XMPP connection.
- Depending on your environment, it may be acceptable for passwords to be transmitted without being encrypted, but in case you are using networks which may not be secure, one of the tests will warn if you are not requiring that cleartext authentication use TLS.

Chapter 17 Statistics

This chapter discusses collection and viewing of M-Link Server statistics.

17.1 M-Link Server Statistics

The M-Link Server is capable of reporting various information about its configuration and status. Two types of statistical information are available:

- *on-demand* statistics, which are returned in response to a request from a client. These statistics are always available to a suitably privileged client (such as M-Link Console, when connected as a *Server* administrator). In some cases, a non-trivial amount of work is required to compute these values, and so the M-Link Server will only compute them in response to a request from a client. For this reason, it is generally not a good idea to poll the server for these statistics.
- *live* statistics, which are published by the server to a special pubsub domain, and which will be seen by any client which has an appropriate pubsub subscription. The server regards the publishing of this data to be a relatively low-priority task, so while some of the statistics may be refreshed every minute or so, the period between updates is not guaranteed to be regular.

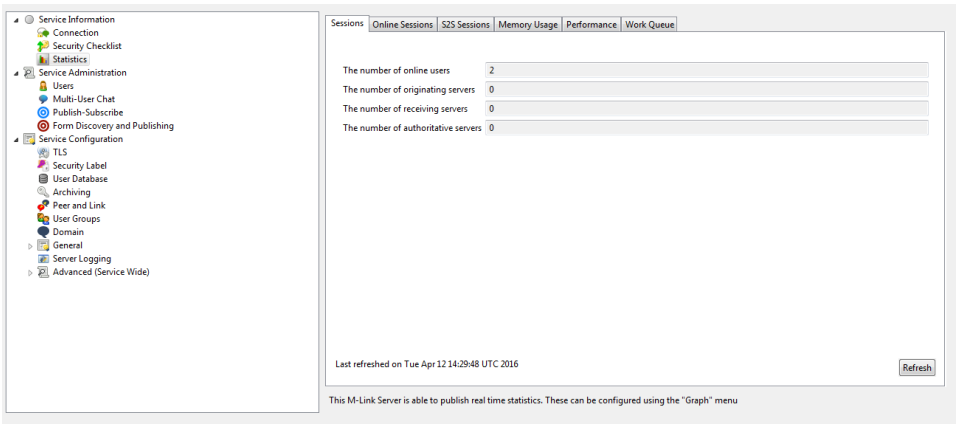
  Since live statistics are associated with a pubsub domain, it is possible to capture live statistics in the archive, which allows a historical record of "live" statistics. This can provide a useful way to assess the behaviour and load experienced by an M-Link Server over a relatively long period of time.

M-Link Console can be used to view both types of statistic, as described in the sections below.

17.2 On Demand Statistics

An M-Link server provides a range of on demand statistics. These statistics are available from the server on a request basis, i.e. the values must be explicitly requested from the server. M-Link Console provides a number of customized views for these statistics, accessed via the statistics editor.

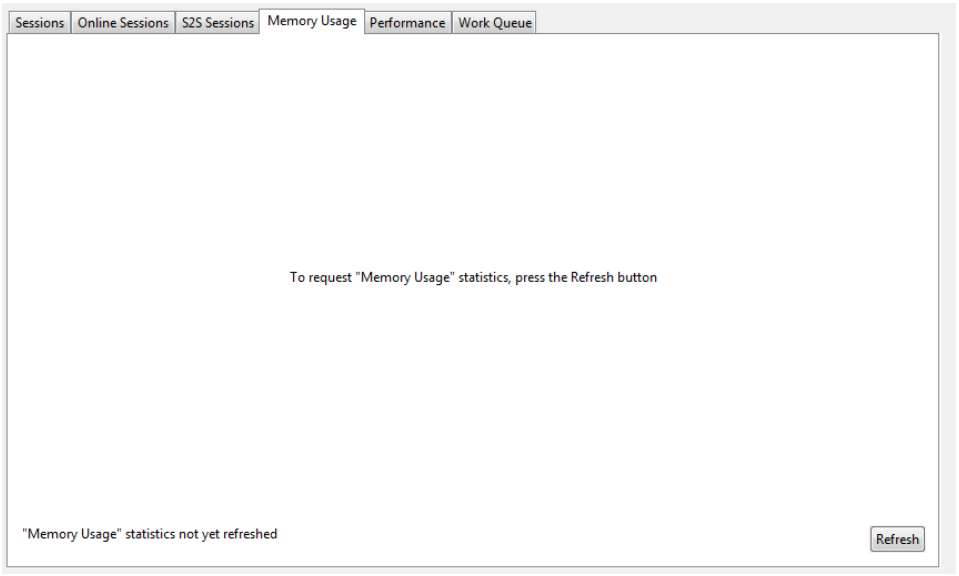
Figure 17.1. Example of the On Demand Statistics



The On Demand statistics are spread over a number of tabs, each one representing a collection of related statistics.

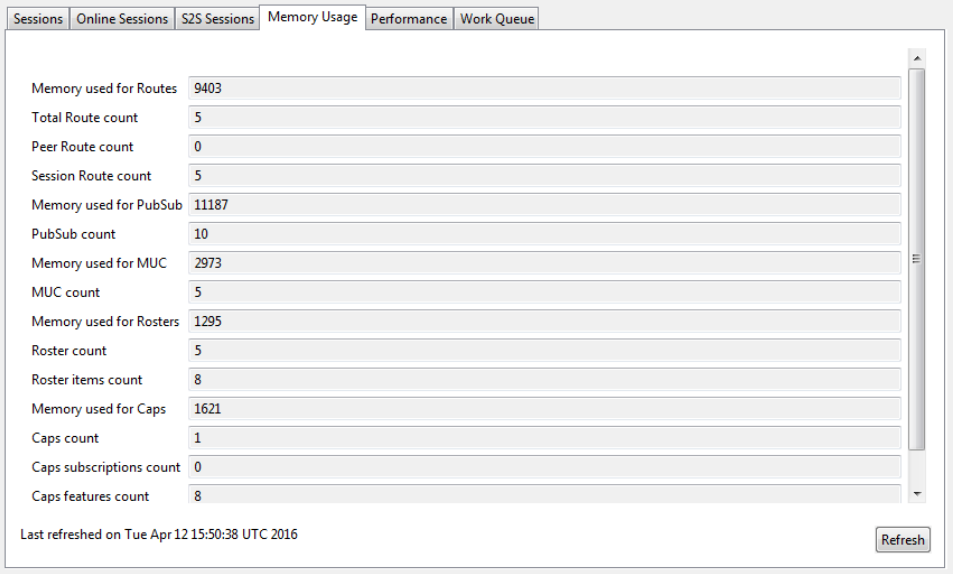
The tabs are not automatically updated. To get the latest values the **Refresh** button should be pressed. Some of the tabs will be automatically filled in with initial values when M-Link Console loads. Others represent statistics that may take a non-trivial amount of work to compute. These will have to be explicitly requested from the server. Initially the editor will display a message in the tab explaining that a refresh is needed to load the statistics.

Figure 17.2. A refresh is needed to load the statistics



To request the data the **Refresh** buttons should be pressed. The server will calculate the current values for the associated statistics and they will then be displayed.

Figure 17.3. The Tab after the statistics have been loaded



17.3 Live Statistics

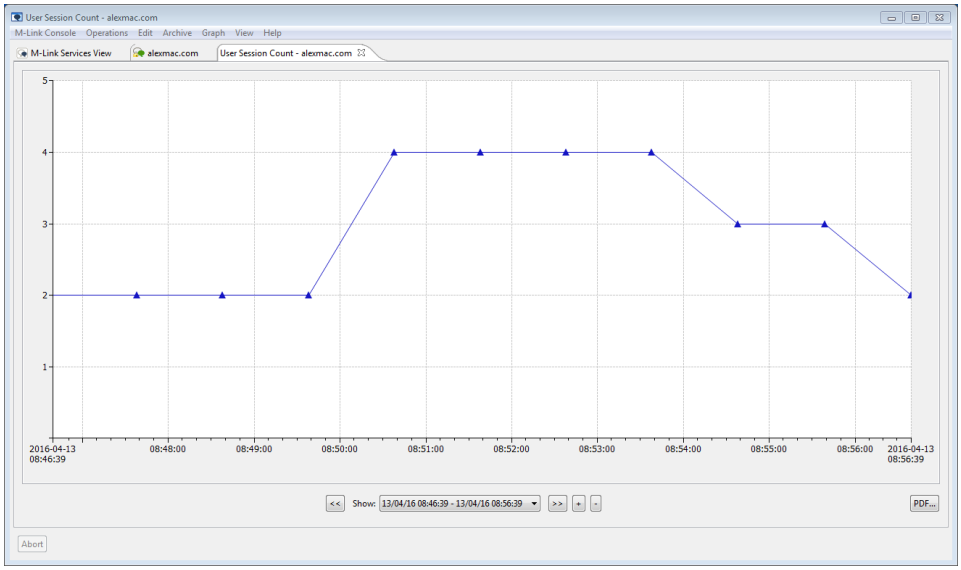
An *M-Link service* can be configured to provide Live Statistics. This is a publish subscribe service that provides real time statistic information for the service.

M-Link Console can then display these statistics, in a graphical format, as part of the *Live Statistics* view.

Enabling live statistics on an *M-Link service* can be used via the *Configure Live Statistics* tool in the *Graph* menu in *M-Link Console*

Optionally, if the archive database is configured on the service, (see Section 15.7, “ Archive Service Management in M-Link Console”) then it can be configured to archive the statistic. If this is done, then *M-Link Console* will allow browsing of the historical statistic data for the service.

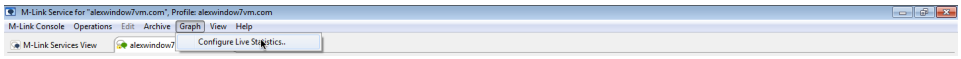
Figure 17.4. An example of the live statistics for an M-Link Server



17.3.1 Enabling live statistics

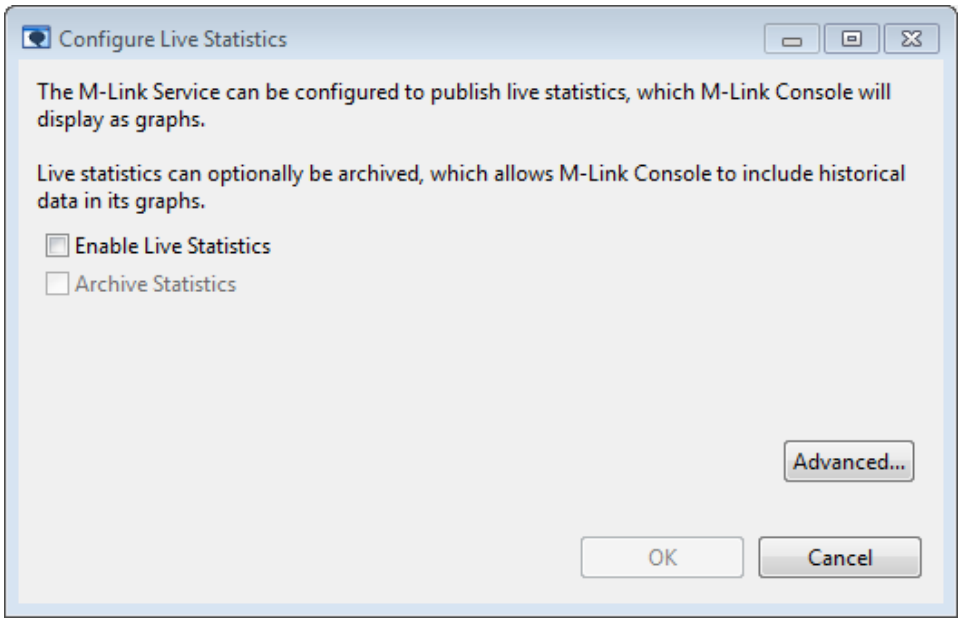
Live statistics can be enabled via the *Configure Live Statistics* tool found in *M-Link Console*'s *Graph* menu

Figure 17.5. Launching the Configure Live Statistics tool



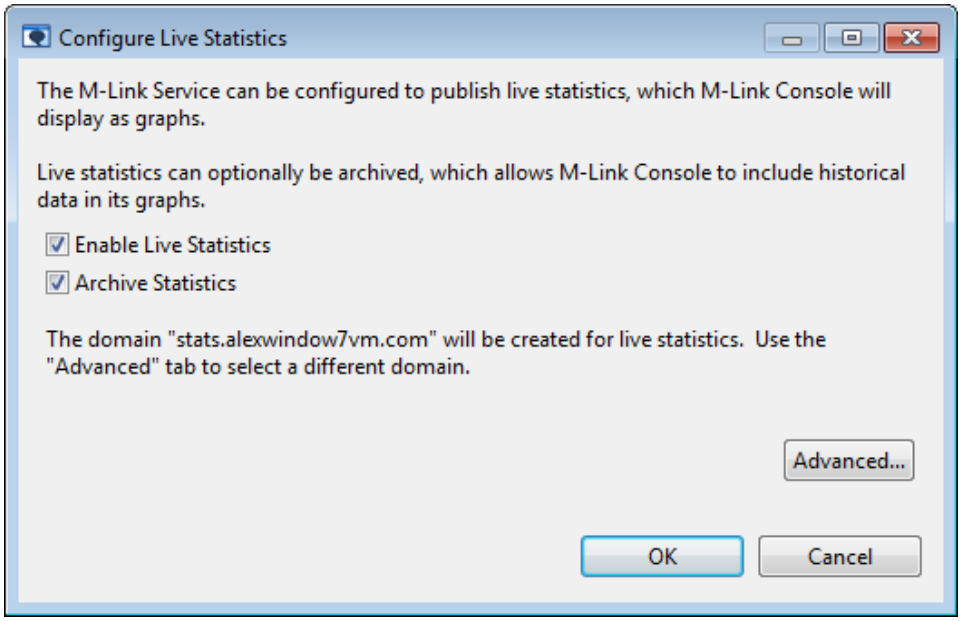
When launched the tool will display whether *Live Statistics* are enabled on the service and provide check boxes for enabling *Live Statistics* and *Live Statistic Archiving*.

Figure 17.6. Configure Live Statistics



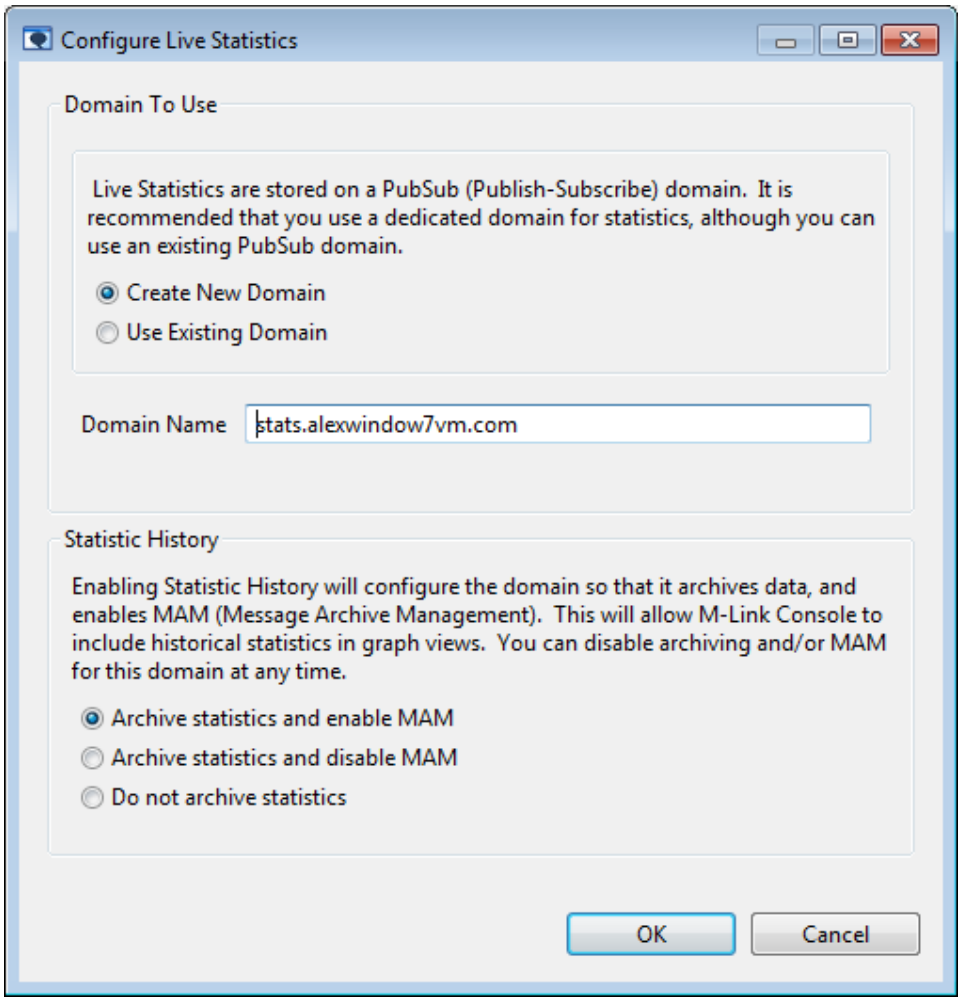
Checking the *Enable Live Statistics* checkbox will enable live statistics on the service. Doing so will also cause the *Archive Statistics* button to be enabled and checked. If the archive database is configured on the server this will mean that the *Live Statistics* will be archived, allowing *M-Link Console* to provide historical data about statistics. To disable *Live Statistic Archiving* uncheck the *Archive Statistics*.

Figure 17.7. Service with Live Statistics and Archiving enabled



By default when configuring *Live Statistics M-Link Console* will create a new publish subscribe domain with the name *stats.<servername>* on the service and configure the *M-Link service* to push the live statistics data to that domain. For advanced configuration options select the *Advanced...* button.

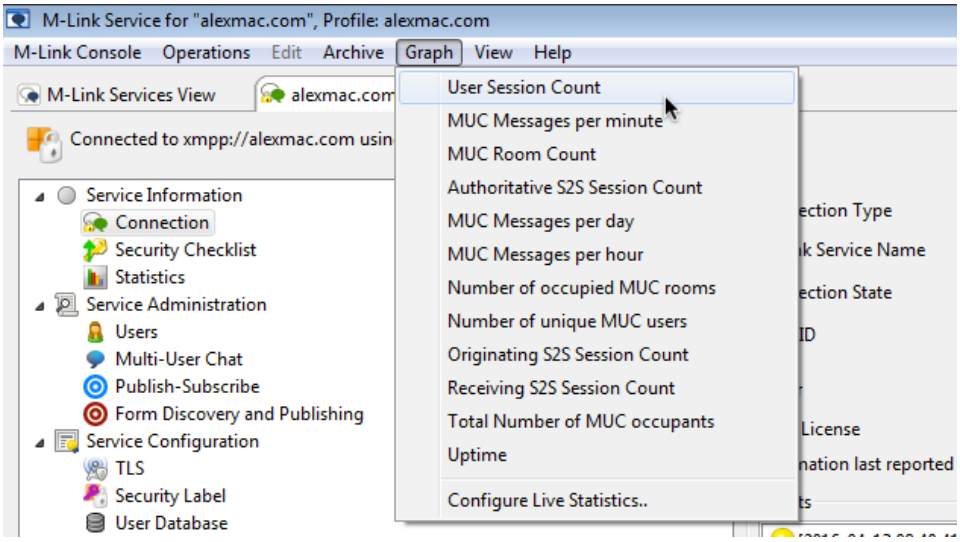
Figure 17.8. Advanced Live Statistics Configuration



17.3.2 Viewing Live Statistics

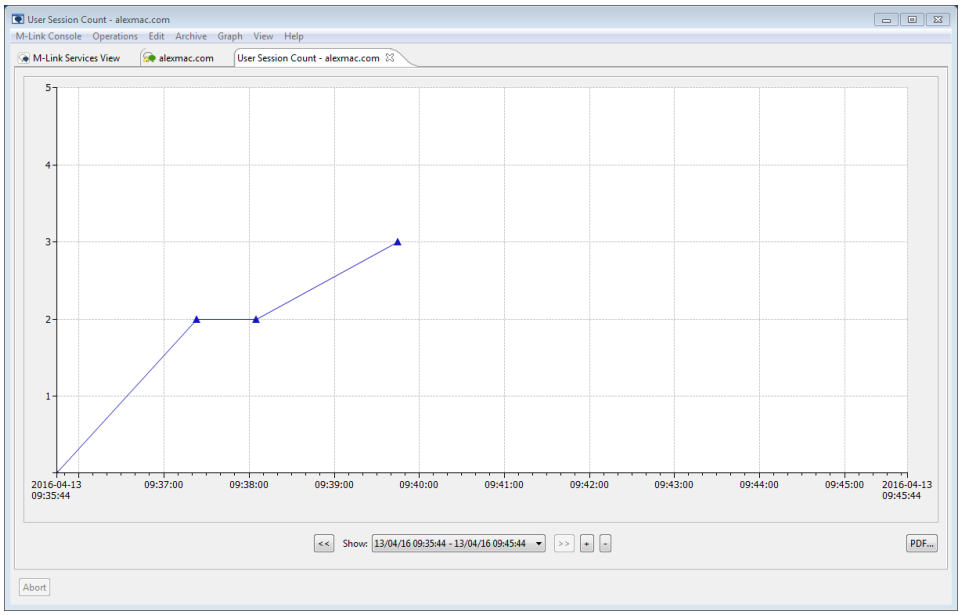
Once enabled on the *M-Link service*, live statistics will be visible in Graph menu; which will contain a list of live statistics available on the service

Figure 17.9. Graph Menu



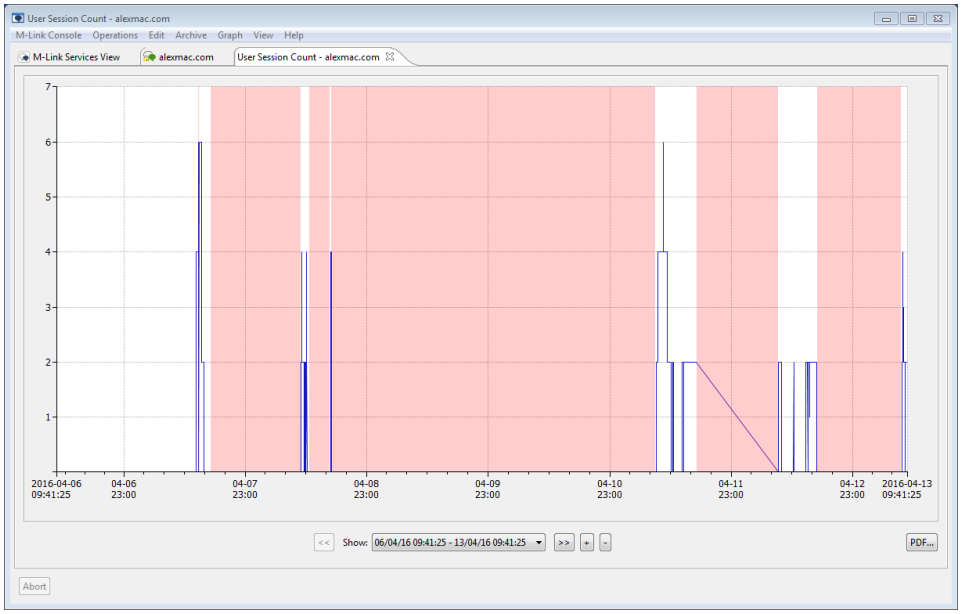
Selecting a statistic will display it as a graph in a *Live Statistics View*. The graph will be a line graph plotting value of the statistic against time. If archiving of the statistics domain is enabled, then the graph will include historical data (including data before M-Link console was started). If no archiving has been enabled, then the graph will only show data that has been published since M-Link Console connected to the service.

Figure 17.10. Live Statistics View



Red lines or regions on the graph indicate when the M-Link Server's **Uptime** statistic indicates that the server was not running.

Figure 17.11. Red lines or regions indicate when the server is down



The server publishes a variety of live statistics; M-Link Console allows you to select which statistic is being shown.

The control bar at the bottom of the view allows navigation through the historic values for the statistic. If statistic archiving is not enabled on the server, then you will not be able to scroll to a time earlier than when M-Link Console connected to the service. The controls allow you to:

- scroll backwards and forwards in time
- zoom the scale of the horizontal axis, to show larger periods of time, or focus on a shorter period
- snap the horizontal axis to a predefined time period, such as the last hour, day, week, etc.
- export a copy of the currently displayed graph to a PDF file.

Chapter 18 Monitoring the M-Link Server

M-Link Server's logging configuration provides a way for the server to log events in various ways.

18.1 Logging

This section begins with the use of M-Link Console to configure logging. This is followed by an overview of the general structure of the Isode logging subsystem.

Note: Since in most cases you will be using M-Link Console to view and update logging configuration, it is not necessary to be familiar with the details of the logging implementation, but it may be useful to have an understanding of some of the concepts involved.

18.1.1 How logging works

This section contains information to help you understand the content and configuration of log files in more detail.

18.1.1.1 Record types

All Isode applications generate two types of log records during normal execution: audit records and event records.

- Audit records are used to record 'auditable events' – configuration change, for example. They do not have a severity level associated with them, and have a well defined format, so that they can be easily parsed.
- Event records are used to record errors, normal program operation, or to provide debugging information. They are associated with a particular severity level, and contain free-form text with substituted data items. The free-form text is contained in a separate dynamically-loaded library (on Windows) or a message catalog (on Unix), which makes it possible to replace the standard set of English messages with equivalent text in other languages simply by substituting a suitable message file.

No output mechanism is directly associated with log records. When an event or audit record is generated by an application, then whether or not it is logged, where it is logged to, and what the output of the log looks like, depends on what output streams have been configured.

18.1.1.2 Output streams

An output stream is a description of how a particular set of event and audit records should be recorded or displayed. Multiple output streams may be configured for an application, and whenever an event or audit record is generated, the logging subsystem checks to see which, if any, of the available output streams is eligible to process it.

As well as defining which records are eligible to be logged, the configuration of an output stream also determines the format of the messages that are produced by the stream.

This means that a single event or audit record may be processed by one or more separate streams (or by no stream at all), and that, in the case of multiple streams, the messages output by the streams may be of differing formats, containing more or less detail. For example, it would be possible to configure one output stream to generate a brief message

about all 'warning' level events, and another to generate a detailed message about a specific 'warning' event which is of particular interest.

Stream types that are currently available:

- the `file` type, where the records are output to a file
- the `mpp` type, which sends logging over the network to Isode's server watch daemon, which enables further processing and/or consolidation.
- the `snmp` type, which sends events to an SNMP agent. See Section 18.2, “High-priority event monitoring using SNMP” for more details.
- the `system` type, where the records are passed to the system event log (**syslog** on Unix systems and the **Application Event Log** on Windows)
- the `tty` type, which is identical to file type, except that the records are written to either `stdout` or `stderr`

M-Link will be configured with a default *file* stream to record log events.

18.1.1.3 Format of messages in output streams

When a given audit or event is generated, then for each output stream that is configured to process records of that type, the settings for the output stream determine the format of the message that is output. In the case of `file` and `tty` streams, the stream may be configured to contain any combination (including none) of the following fields:

- **date and time**: the format of date and time is configurable on a per-stream basis.
- **program name**: the name of the program generating the message. Any `isode` prefix will have been removed, and the program name will be truncated to 8 characters.
- **process id**
- **thread id**: this field may be useful to distinguish separate threads in the same process.
- **username**: the username of the process which generated the record. This field is only meaningful on Unix systems. If the username cannot be established, then a numeric UID is logged.
- **severity**: audit records have no associated severity, but event records always have a severity, which, if displayed, is represented using one of the following single letters, as follows:

`I` – Information	`N` – Notice	`S` – Success	`D` – Detail
`W` – Warning	`E` – Error	`F` – Fatal	`C` – Critical
`L` – AuthOK	`A` – Authfail	`X` – Debug	`P` – PDU

- **facility code**: the name of the facility which generated the message. Audit records are not associated with a particular facility.
- **message identifier**: an identifier representing the event. Audit records do not have a message identifier.
- **text**: the formatted text describing this event. Audit records do not have a text field.
- **supplementary audit record parameters**

  For certain types of audit records, extra information may be associated with the record, and if the stream is suitably configured, this will be included as a sequence of *key-value* pairs on the end of the message.

As an example of an audit record, consider that the node configuration has been modified by the *Server* administrator. Assuming an audit stream has been created to capture such records, and that the stream is configured to display all possible fields, then the resultant message from the audit output stream will look like this:

```
2015-02-13 14:20:27 xmppd    04932 (root    )
MLink_AdHoc-Server_Configuration session:SID-2
jid:william.brown@funkywin7.isode.net
operation:"http://isode.com/xmpp/config#set_config_node"
```

As an example of an event record, consider that the M-Link Server is shut down. Assuming an event stream has been created to capture such records, and that the stream is configured to display all possible fields, then the resultant message from the event output stream will look like this:

```
2015-02-13 15:20:27 xmppd    04932 (root    ) N-MLink-Notice
PROCESS: exited(0) shutting down
```

In both cases, the date, program name (`xmppd`) and process id (`04932`) and username (`root`) are included.

The event record contains severity (`N`, for Notice), facility (`MLink`) and identifier (`Notice`) of the event, as well as the text field giving more details.

The audit record is identified by the fixed string `MLink_AdHoc-Server_Configuration`. This type of audit record contains supplementary information which (assuming the stream is configured to display them) is shown in the log as a sequence of *`key:value`* pairs. In this case, the `MLink_AdHoc-Server_Configuration` operation is logged with three supplementary parameters, `session`, `jid` and `operation`.

18.1.1.4 Logging configuration

Information about logging stream configuration is stored as XML data.

An application loads its logging stream configuration generally from an XML file. For Isode DUAs (such as M-Link Console and Sodium, this is contained in the *dualogging.xml* file, located in either *`(ETCDIR)`* or *`(SHAREDIR)`*. In the case of M-Link Server, the corresponding *mlinklogging.xml* file contains configuration used by the M-Link Server.

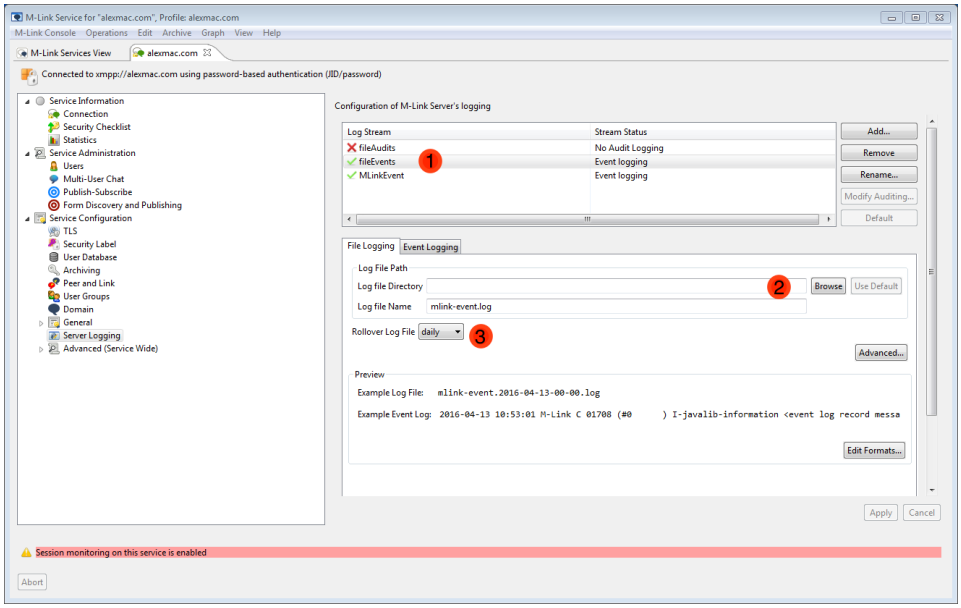
M-Link Server provides a customised editor (see Section 18.1.2, “ Changing M-Link Server logging using M-Link Console”) for modifying the logging configuration via the Ad-Hoc Command described in Section G.54, “Set Logging Settings (Node)”. This GUI is also available as a standalone tool (in the case of individual XML files, see Section 18.1.3, “Using the standalone logconfig tool”) which can be used for managing any Isode product's (including M-Link Console) logging configuration XML file.

18.1.2 Changing M-Link Server logging using M-Link Console

You can use M-Link Console to configure logging for your M-Link Server.

M-Link Console allows you to manage log configuration using the *Server Logging* editor which appears in the *XMPP Service* view for *Server* administrators. Note that M-Link does not allow for cluster-wide common logging configuration (i.e., logging configuration is *node-specific*), and so no equivalent editor appears for the cluster-wide logging.

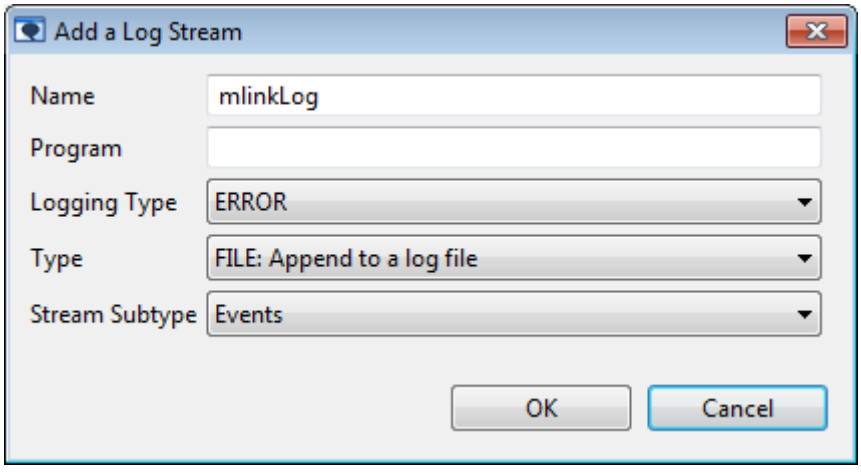
Figure 18.1. Configuring logging using M-Link Console



1. Two different record types (see Section 18.1.4, “What is written to the log files?”) are shown (**Audit** and **MLinkEvent**):
   - If you select **Audit** (as shown above), the information below relates to the audit record type.
   - If you select **MLinkEvent**, the information relates to the event record type.

   Existing log streams can be renamed, removed or modified. It is also possible to add one or more log streams to the logging configuration using the **Add** button.

Figure 18.2. Add a Log Stream

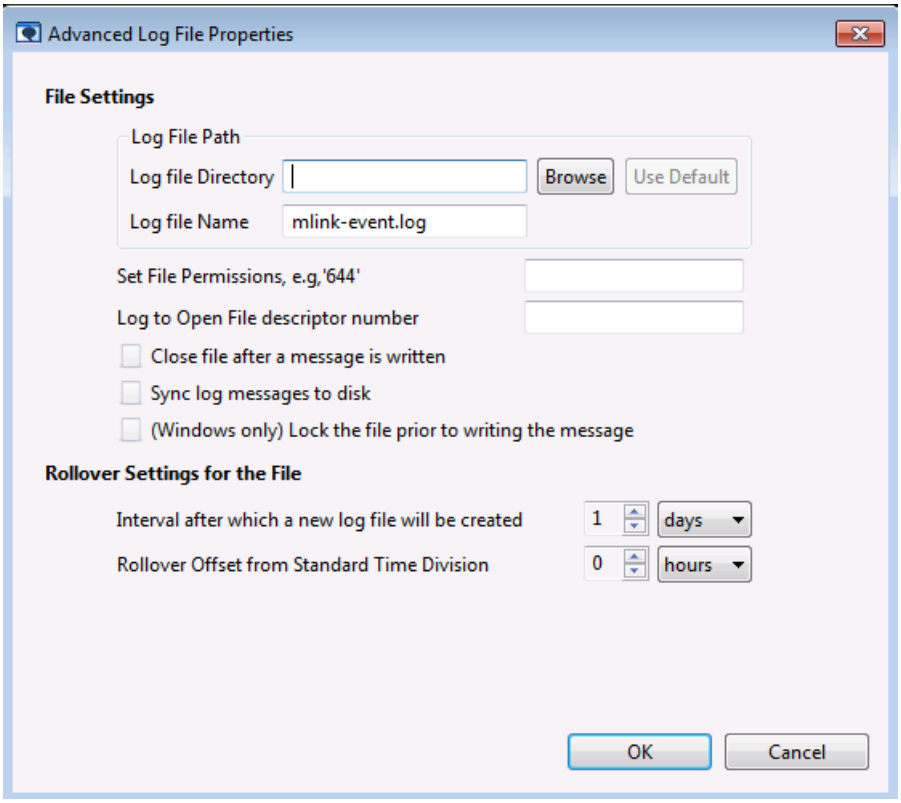


2. Either **Browse** to find a suitable directory in which to store the log files, or click **Use Default**.

   The **Log file Name** is shown by default. For the **Audit** log it is *mlink-audit.log* and for the **MLinkEvent** log it is *mlink-event.log*.
3. You can choose to create a new log file at regular intervals. The default is for a new file to be created daily, but you can change this to hourly or weekly if you prefer. The name of the log file contains the date and time at which it was created; for example, *mlink-event.2012-08-27-00-00.log*

   Click **Advanced** to specify more details.

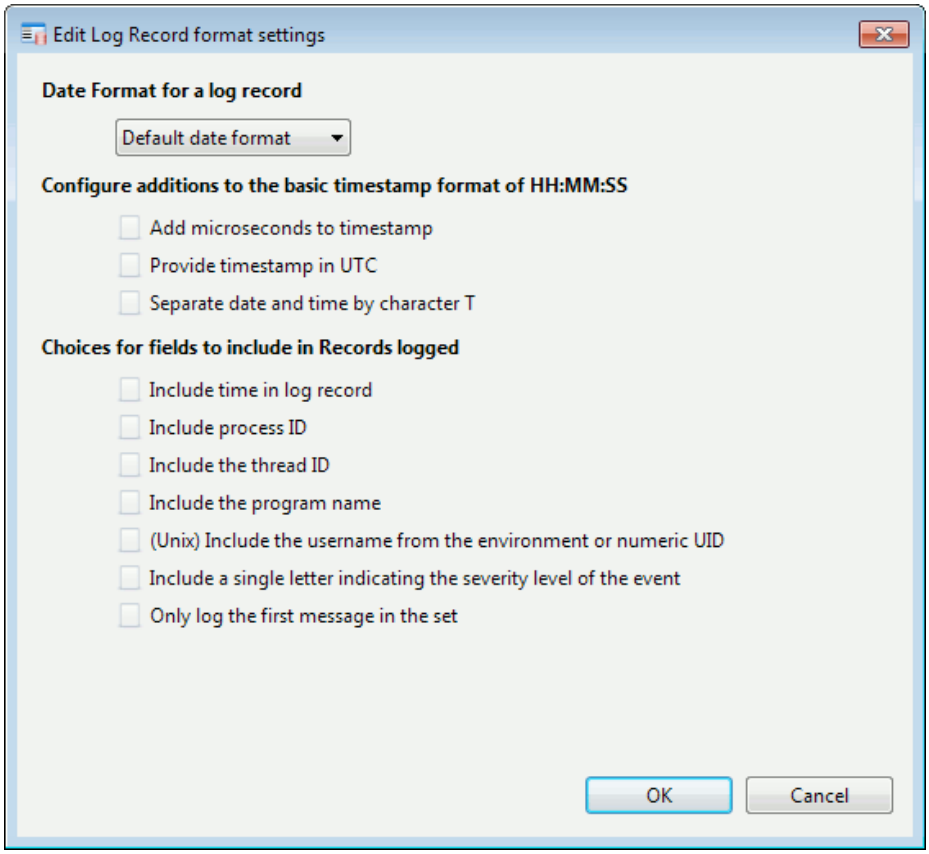
Figure 18.3. Advanced Setting for File Stream



- **Log File Path** - information is as on the basic page.
- **Set File Permissions** - You can set read, write and execute file permissions.
- **Log to Open File descriptor number** - Enter the integer that identifies the file.
- **Close file after a message is written** - The file is opened to write the message and closed again immediately afterwards. This helps to ensure security of the data but there is a significant performance overhead.
- **Sync log messages to disk** - asks the operating system to ensure that messages are written to disk. The helps to ensure security of the data but there is a significant performance overhead.
- **(Windows only) Lock the file prior to writing the message** - ensures that if multiple processes are logging to the same file, the messages are not mixed.
- **Rollover Settings for the File** - sets a rollover interval for the file and enables you to specify an offset from the default start point of the specified period. For example, the default start time for a daily roll-over is midnight, and the default start point for a weekly roll-over is 00:00 hours on a Sunday.

4. Click **Edit Formats** to change the content of the log file. Examples are shown of the current format in the **Preview** area – you may need to enlarge the window to see them.

Figure 18.4. Logging Formats

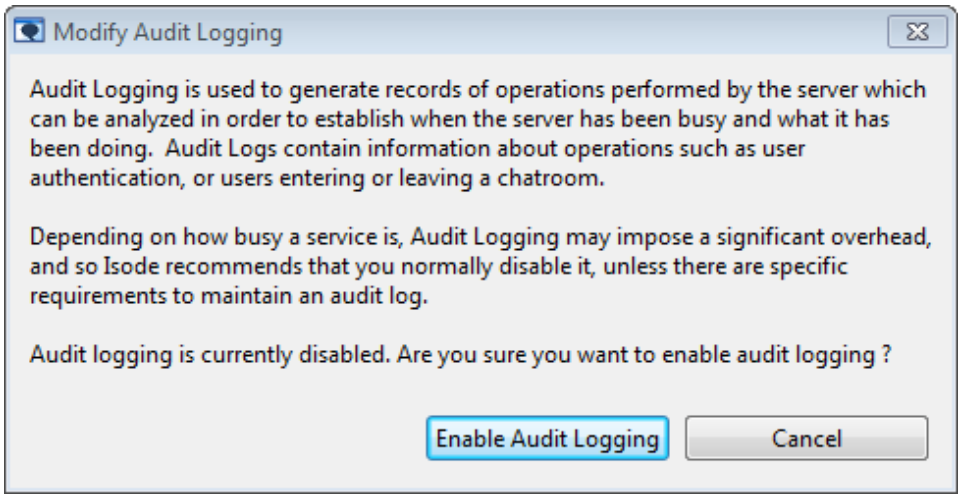


- Select your preferred date format from the options available. The default is `YYYY-MM-DD HH:MM:SS`.
- Select any additions you want to make to the timestamp.
- Select any fields you want to be included or excluded from the records. This option is: a green tick specifies that a field will be included, a red cross specifies that it will not. Leave the option blank for it to take a default value.

18.1.2.1 Audit logging

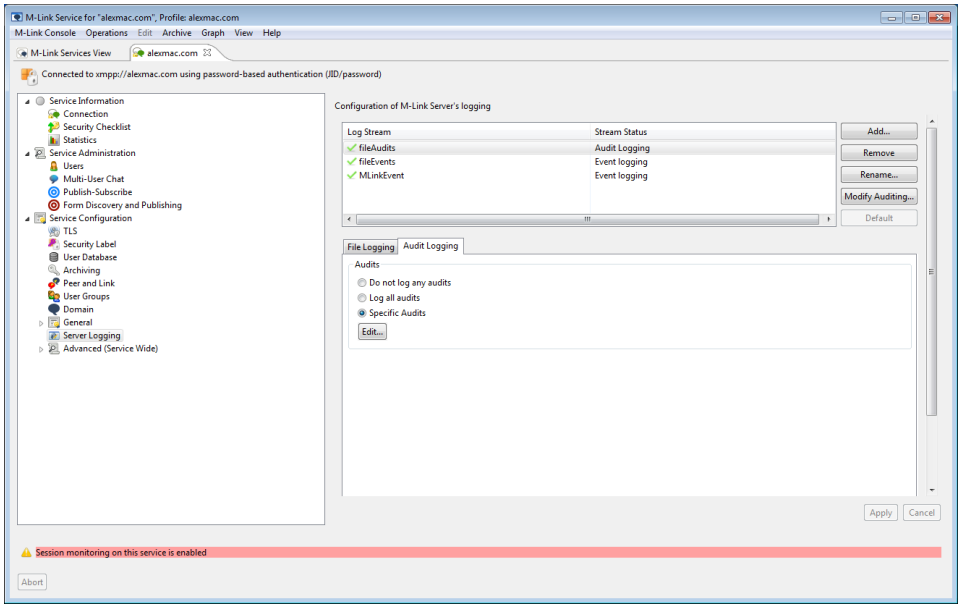
Audit logging can be switched on and off as desired. By default it is off and no audit logs will be created. To switch it on or off, use the **Modify Auditing...** button to open the Modify Auditing Dialog

Figure 18.5. Modify Auditing Dialog



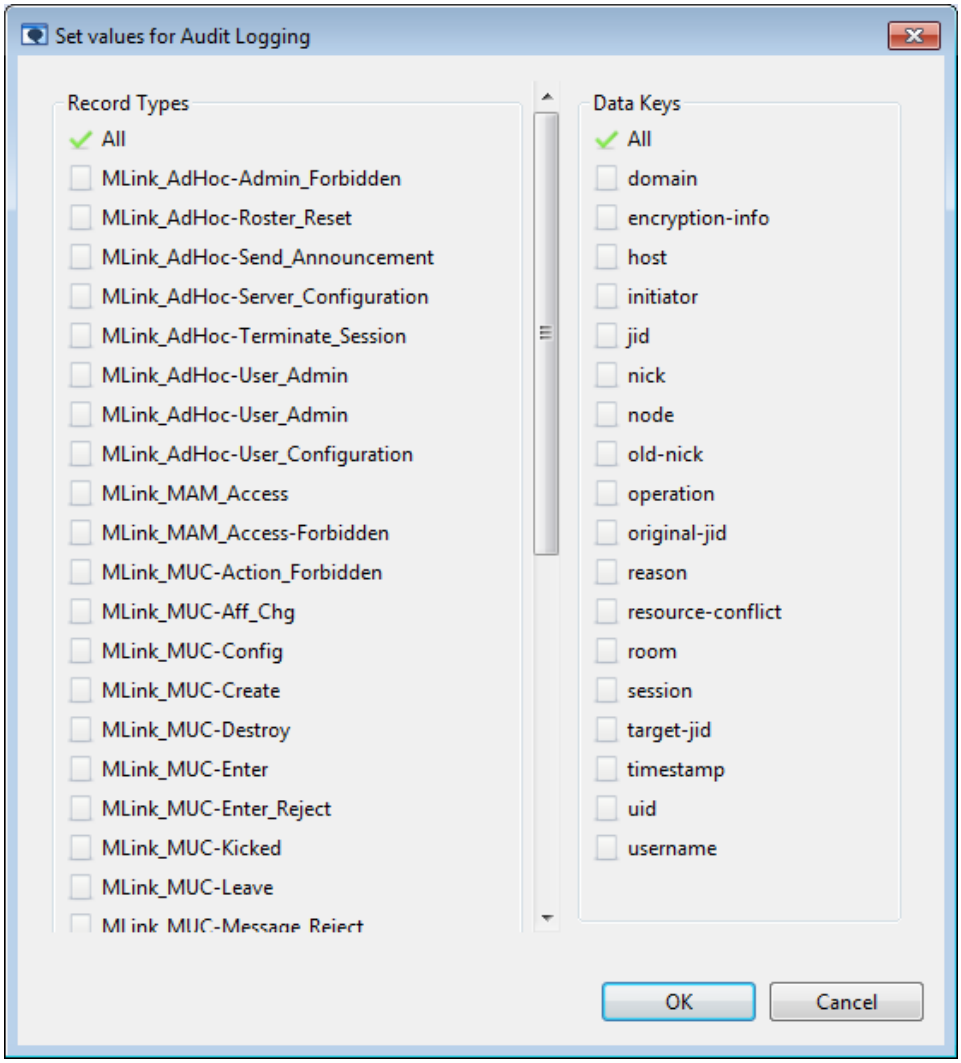
By default enabling auditing will cause all audits to be logged. To log only specific audits open the *Audit Logging* tab and select the *Specific Audits* radio button.

Figure 18.6. Select Specific Audits



To specify which audits are logged click the *Edit* button to bring up the Specific Audits Dialog.

Figure 18.7. Specific Audits Dialog



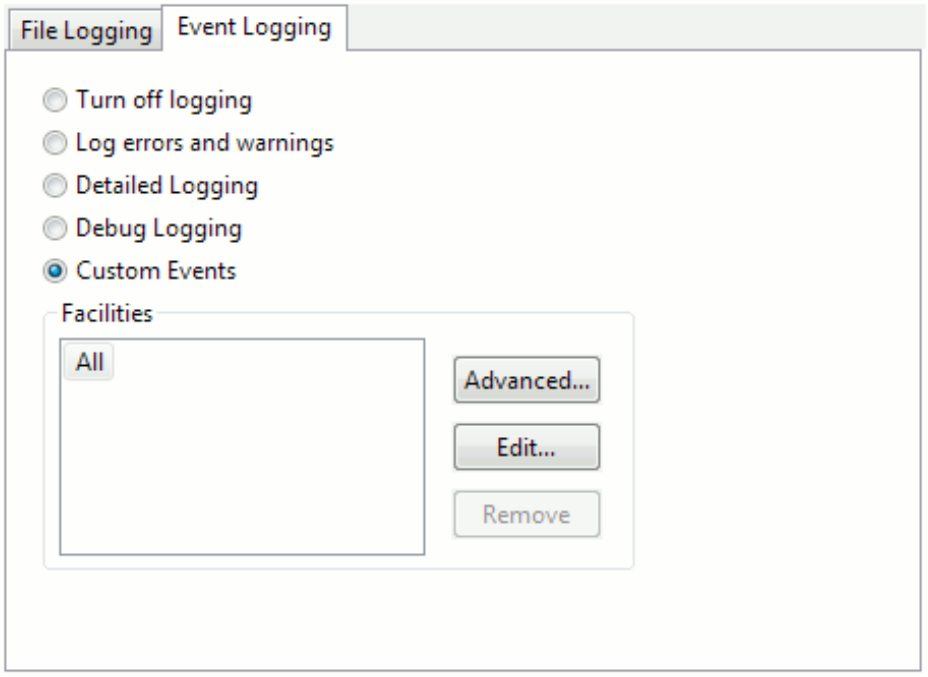
The example above shows that all **Record Types** and all **Data Keys** will be included.

- Click an item to include it.
- Click a included item to exclude it.

18.1.2.2 Event logging

First choose the level of event logging you want to include in the log files.

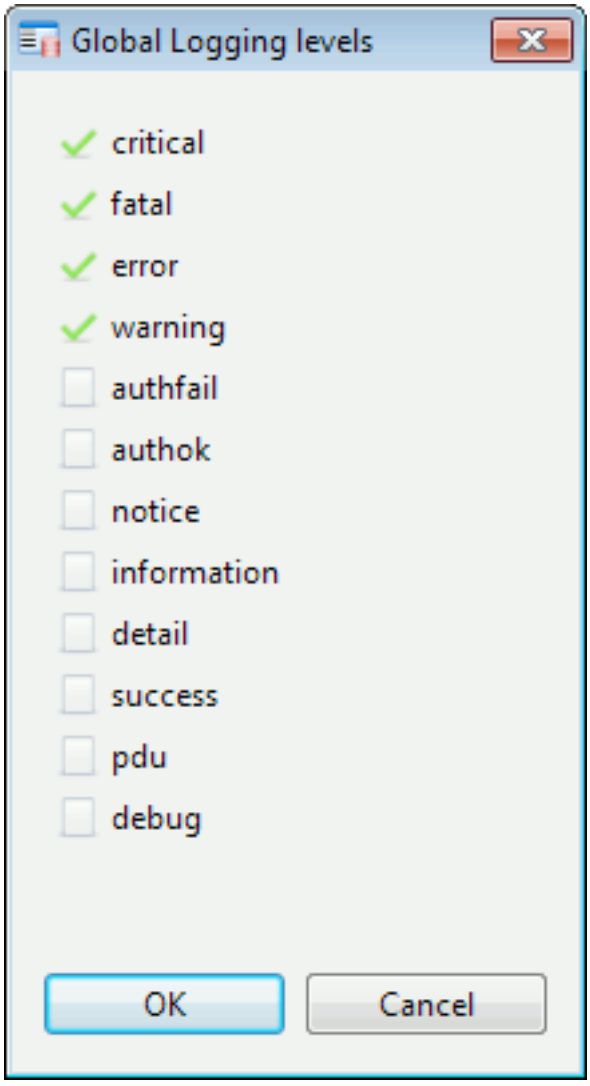
Figure 18.8. Event Logging



You can choose **Custom Events** if you want to specify the logging levels not offered by the other radio buttons.

Note: To see what is included and excluded at each level, select the level and click **Edit...**. The example below shows what is included when **Log errors and warnings** is selected.

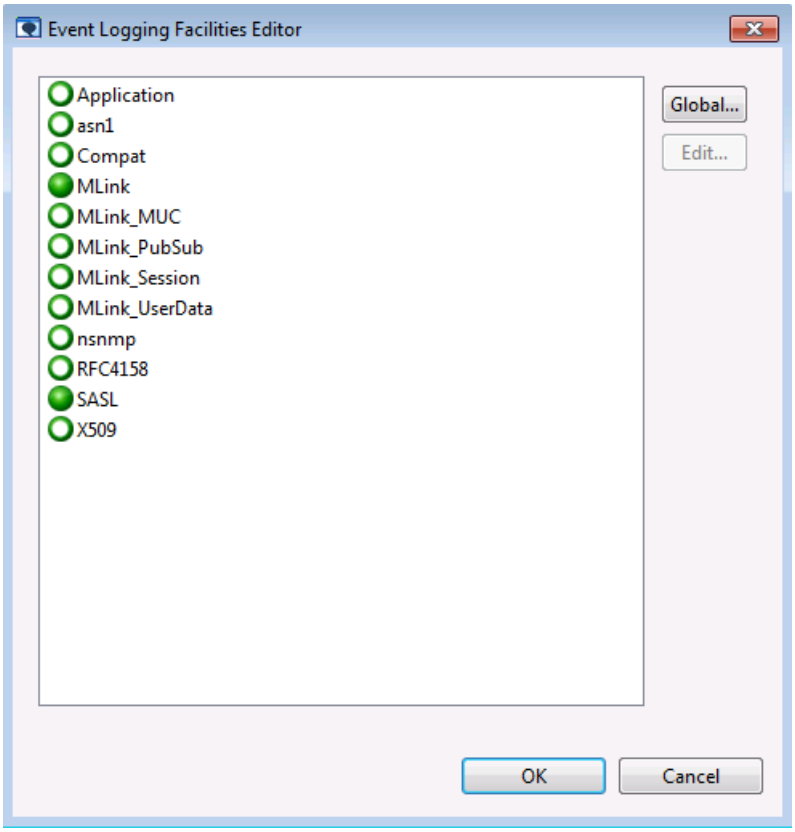
Figure 18.9. Logging Levels



Click **Advanced...** to specify in more detail exactly what you want to log. This also allows you to set logging levels for facilities offered by the server.

Facilities are used by the M-Link Server to group logging for similar events, in order to simplify event log analysis. For example, all X.509 related logging is done using the `X509` facility. In order to debug X.509 related problems, specific events and levels can be enabled for the `X509` facility.

Figure 18.10. Advanced Logging Levels

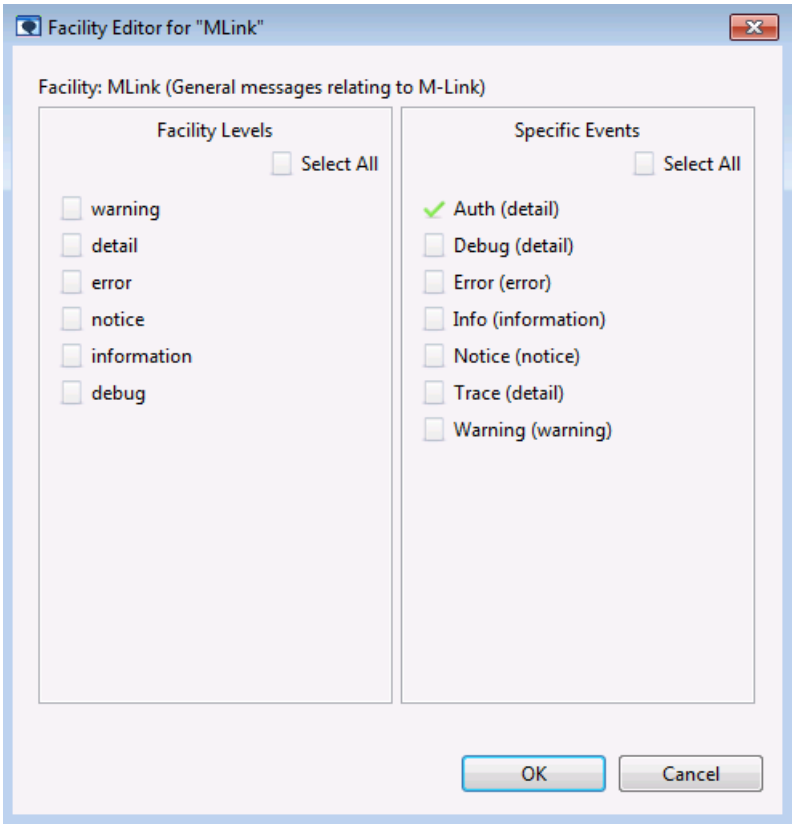


The facility which has logging levels set to a value other than default will be shown by solid green icon, while the others would be shown by an empty green icon.

Note: A tool tip is displayed if you hover your mouse over an entry giving details of the type of event referenced by that entry. For example, **X.509** displays **X.509 System**.

- **Global...** takes you to the **Global Logging Levels** window (above). These levels apply to the default logging levels for the server which can be overridden for certain facilities and events if required.
- To specify more details about a particular event type, select it and click **Edit...**.

Figure 18.11. Facility Logging Levels and Events



18.1.2.3 Creating a new logging stream

You can create a new logging stream for information of a particular type or from a specific tool or program. To create the new log stream:

Click **Add** on the tool bar and select **Log Stream** from the options displayed. Follow the instructions given in Section 18.1.3, “Using the standalone logconfig tool”, except that you will not need to specify the **Application Type**.

18.1.3 Using the standalone logconfig tool

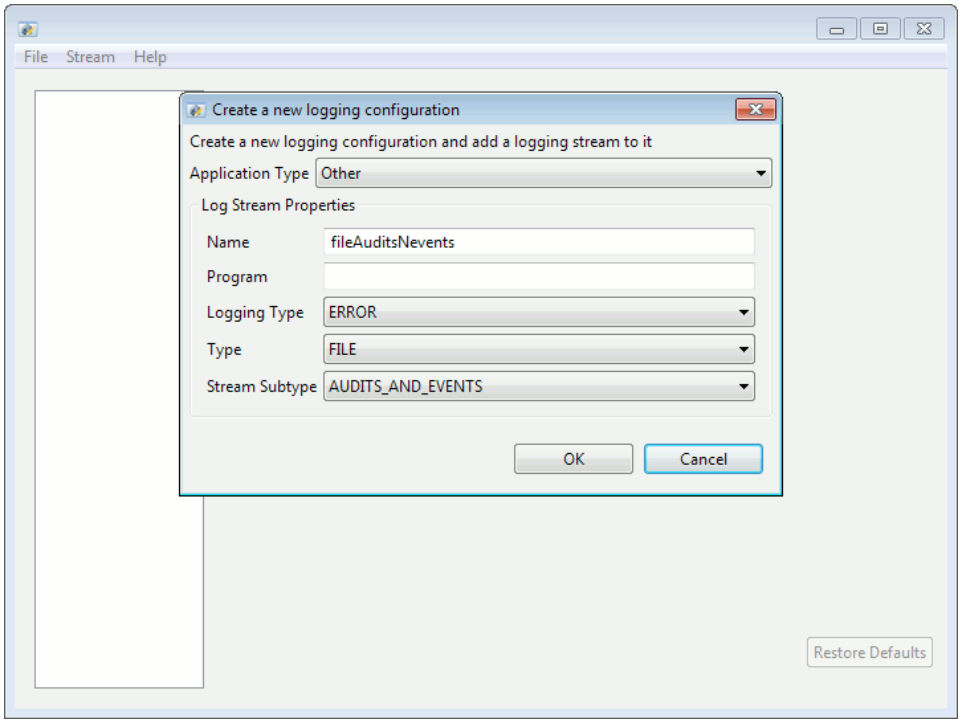
This section describes the use of the standalone logconfig tool, and shows how you can create new log streams in any Isode product's logging configuration.

On Unix systems, run */opt/isode/sbin/logconfig*

On Windows, a shortcut to the **Log Configuration Tool** will have been set up in the **Isode** folder on your **Start** menu.

If no logs have been configured, the tool opens displaying a window ready to create a new logging configuration.

Figure 18.12. Create Log Stream

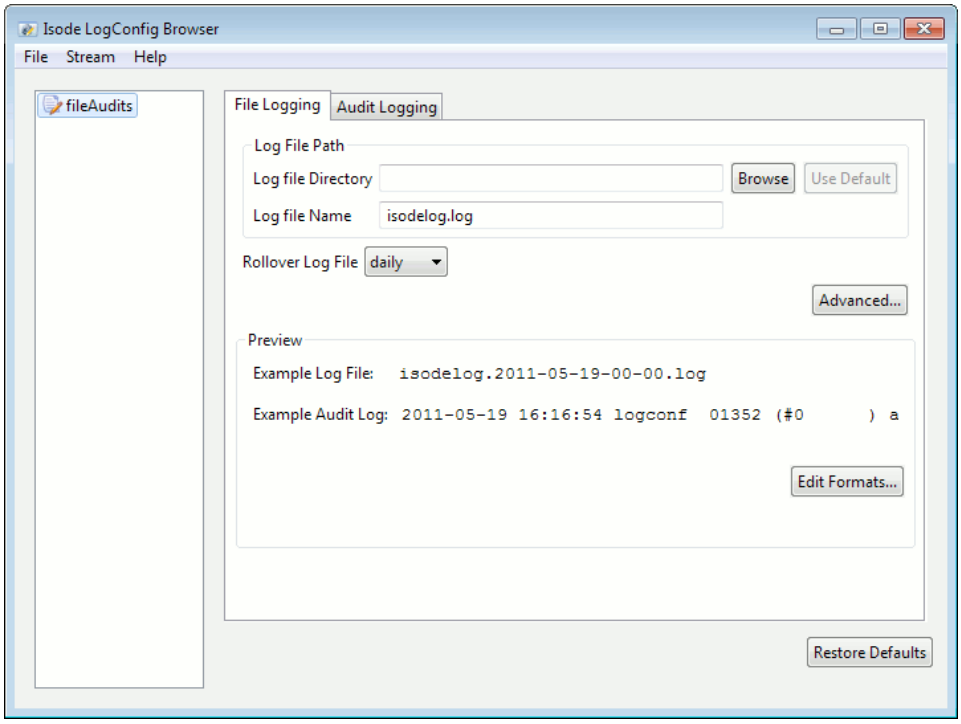


1. Select **M-Link XMPP Server** from the list in **Application Type** (assuming you are creating a configuration for the M-Link Server).
2. The default **Name** will change to a new name if you change the **Type** or **Stream Subtype** (final options).
3. If you want to associate this particular logging stream with a program or utility, type its name in **Program**. If you do not specify anything here, this stream will be used for all programs and utilities.
4. Select the **Logging Type**: **ALL**, **DETAIL**, **ERROR**, **NONE** or **WARNING**.
5. Select the **Type** of output (see Section 18.1.1.2, “Output streams” for an explanation of the options available).
6. Select the **Stream Subtype**. This option is only available if **FILE** or **TTY** was selected in **Type**. You can choose from **AUDITS**, **EVENTS** or **AUDITS_AND_EVENTS**.

Once the stream has been created, it should be set to output to a suitable log file. The stream may be configured using the various available tabs.

You may wish to create several logging streams in order to configure different types of logging. To create a new stream, select **Stream** → **Add** from the menu.

Figure 18.13. Log Config Browser



All of the other configuration options available in the standalone logconfig tool are identical to those within M-Link Console and are described in Section 18.1.2, “ Changing M-Link Server logging using M-Link Console”.

18.1.4 What is written to the log files?

The default configuration for an M-Link Server provides two file output streams:

- The **Events** stream captures all event records with severity of Notice (`N`), Warning (`W`), Error (`E`), Fatal (`F`), Critical (`C`), or Information (`I`). It will capture messages for the facilities *MLink* and *SASL*. These are output to *mlink-event_<date>.log* in *`(LOGDIR)`*.

  If you are reporting a potential bug to support@isode.com, then it may be useful to configure the **Events** stream (or to create another output stream), so that while reproducing the problem, all levels of event records are logged. The resulting output should then be included in your report.

  > **Note:** Production M-Link Server instances should not be run with full logging, as this can significantly impact performance and use up large amounts of disk space.

- The **Audit** stream captures all audit records, with the exception of those relating to “internal” events, and outputs them to the *mlink-audit_<date>.log* in *`(LOGDIR)`*.

The following sections describe logging behaviour when these default settings are in effect. However, since the streams are fully configurable, and streams may be added or removed, it may be that the filenames and file contents will be different on a given system.

18.1.4.1 Events stream

A new record is appended to it whenever the M-Link Server generates an event with a severity level of `N`, `W`, `E`, `F`, `C` or `I` (see Section 18.1.1.3, “Format of messages in output streams”). Problems that prevent the M-Link server from operating correctly have a severity level of `E`, `F` or `C`. Possible problems that may be worthy of investigation have `N`, `W`, `E`, `F` or `C` severity codes.

For an example of what the contents of *mlink-event.log* look like, see Section 18.1.1.3, “Format of messages in output streams”.

18.1.4.2 Audit stream

A new record is appended to this file whenever an auditable event, such as configuration update, is generated by the M-Link Server.

Each audit record may include supplementary information which is shown as a sequence of *`key:value`* pairs. The types of audit records that may be logged, with their corresponding supplementary parameters, are described in the following sections. Bear in mind that it is possible to configure a stream so that audit message parameters are omitted from the log file.

18.2 High-priority event monitoring using SNMP

Production systems may require that certain high-priority events, such as 'server has stopped' are not simply logged to a file, but instead cause SNMP traps to be sent to interested SNMP management tools. Isode's Server Watch Daemon (if available) enables this.

The daemon is configured by the *`(ETCDIR)`/ms.conf* file. The XML file needs to contain at least the following two elements:

`mlogd_host`
: On Unix systems this is the name of a UNIX-domain socket if the value starts with a `/`. Otherwise it is the hostname or IP address to listen on.

`mlogd_port`
: If `mlogd_host` contains a domain name or IP address, `mlogd_port` identifies the TCP port number that should be listened on.

Any mpp log streams should be configured to log to this daemon. Once enabled, Server Watch Daemon (if available) can be configured to act as an AgentX sub-agent by adding the following element to *`(ETCDIR)`/ms.conf*:

`agentx_slave`
: This element is empty.

To enable SNMP traps to be issued, the *etc/snmp/snmpd.conf* file (on Windows) or */etc/snmp/snmpd.conf* file (on Unix) needs to be edited to contain the line:

```
trap2sink hostname public
```

Chapter 19 Session Monitoring

This chapter discusses monitoring of sessions.

19.1 Background

It is sometimes useful to be able to monitor traffic sent to and from a specific client or peer. The M-Link Server allows monitoring of this traffic in real-time using special-purpose chat rooms, in which will appear copies of the stanzas sent to and from clients and other servers, as well as state changes.

M-Link Console can be used to configure session monitoring, and to monitor the contents of the associated chatrooms, providing a "live view" of session traffic. Two important factors should be noted:

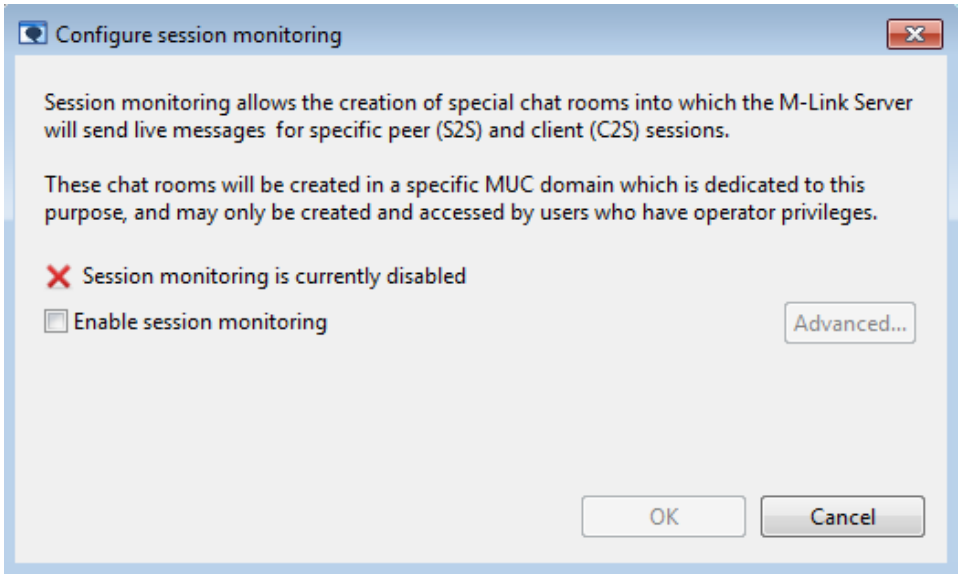
- Any data shown in the session monitor will be uncompressed and unencrypted. There is no mechanism to hide or obfuscate any sensitive data, *including passwords* in the session logs.
- Enabling session monitoring may impose a performance overhead on the server

For these reasons, session monitoring is disabled by default, and, when enabled, can only be accessed by *Server* administrators (see Section 2.5, “M-Link Server Administrators”). Isode recommends that session monitoring only be used to diagnose problems, and only after appropriate consideration of the ramifications.

19.2 Configuring Session Monitoring

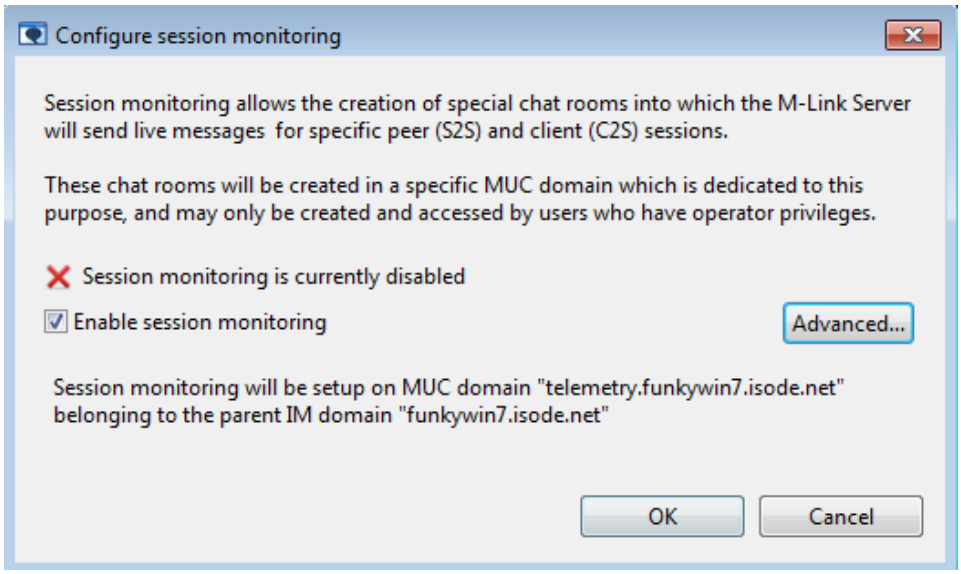
In order to be able to monitor traffic for a specific session, the server must first be configured to enable the session monitoring feature. To do this, use the **Session Monitor...** → **Configure...** from the **Operations** menu. M-Link Console displays a window which shows you whether session monitoring is enabled, and lets you change the server setting:

Figure 19.1. Enabling Session Monitoring



You can use the **Enable session monitoring** checkbox to enable session monitoring; in this case, M-Link Console will configure a new MUC domain:

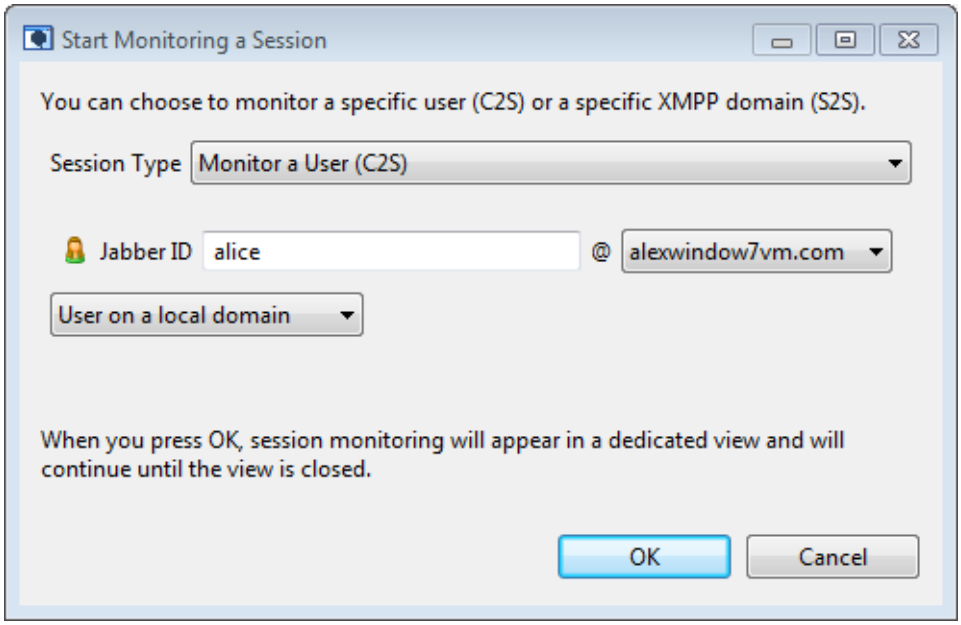
Figure 19.2. Enabling Session Monitoring



Note: If session monitoring is enabled, then M-Link Console will display a warning message whenever a connection is made to the service; the warning is intended to help avoid a situation where session monitoring is left enabled after it is no longer required.

When session monitoring is enabled, you can monitor user sessions (*C2S*), or server traffic (*S2S*) by using the **Session Monitor...** → **Monitor...** from the **Operations** menu:

Figure 19.3. Choosing a session to monitor



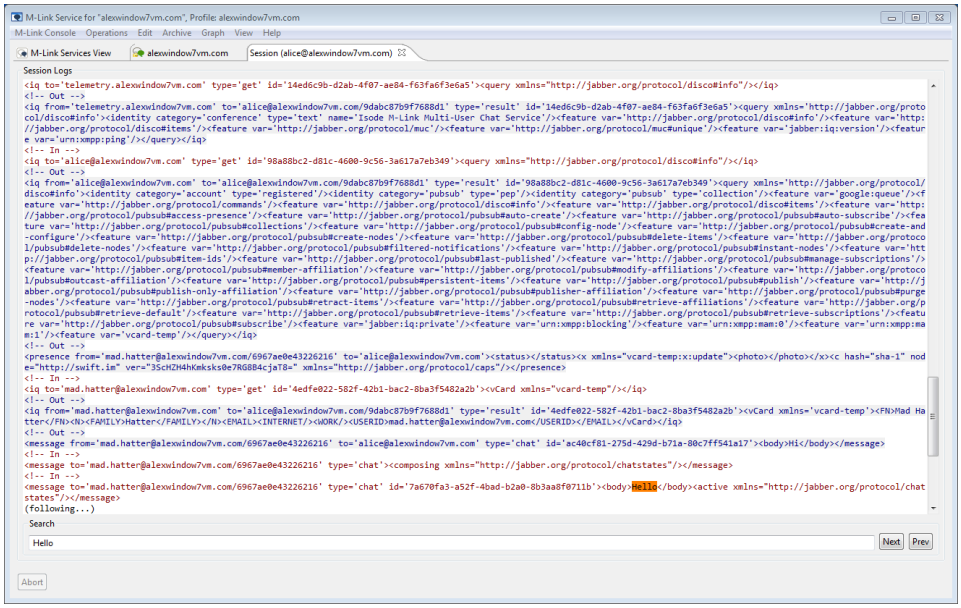
S2S monitoring cannot be used to capture traffic for *X2X* (XEP-0361/XEP-0365) connections, but it is possible to use *C2S* monitoring to view *X2X* traffic for specific users on a server which is configured for *XEP-0361/XEP-0365*: in this case, use the **User on a remote domain** option and provide the appropriate remote user ID and domain.

Note: You cannot monitor yourself (because anything you monitor would need to be reported back to you, generating more traffic that needs to be reported back to you, resulting in an infinite loop).

A new window will be displayed that contains any data for the nominated user (C2S) or server (S2S). You can monitor multiple sessions at the same time; a separate window will be created for each session being monitored.

The monitoring window displays stanzas sent from and to the client (or server) being monitored. Messages are colored and prefixed by <*!-- In --* > and <*!-- Out --* > to help distinguish which direction they are going. The window will update in real-time, and you can use the **Search** box to search for specific strings inside the log:

Figure 19.4. Viewing live C2S session data



Session monitoring will continue until the window is closed.

Chapter 20 M-Link Web Application

This chapter discusses deployment, configuration and use of the M-Link Web Application

20.1 Overview

The M-Link Web Application provides monitoring and management capabilities for an M-Link Server through a *web browser*. This can be useful when multiple clients need access to specific functionality on the M-Link Server from a range of devices. In this context, it is often impossible to ensure each client has access to M-Link Console, as in many cases clients may not support desktop applications. Even if each client has the capability to support an M-Link Console installation, it is often undesirable to expose all of the functionality provided by M-Link Console. The M-Link Web Application addresses these issues by providing access to management capabilities through a web browser. This enables hosts to configure the modules available to clients, and the only requirement for clients is access to a web browser.

The M-Link Web Application is implemented using JavaScript A modern *web browser* is required and browser support for JavaScript applications must be enabled. For instance, Internet Explorer versions prior to version 10 are *not supported*.

The M-Link Web Application utilizes M-Link Server's XMPP over BOSH service.

20.2 Deployment

The M-Link Web Application can be deployed in two ways: self hosted or deployment as part of an existing WWW service.

Both methods are dependent on having the XMPP over BOSH service enabled. Configuring BOSH is discussed in detail in Chapter 12, *XMPP over BOSH*.

20.2.1 Self-Hosted deployment

M-Link, by default, provides self-hosting of the M-Link Web Application simply by having the 'BOSH File Folder' configuration option having the default value when configuring BOSH.

If the BOSH URL is `http://node.example.com:5280/bosh`, simply browse to `http://node.example.com:5280` to begin.

20.2.2 WWW Integration

To deploy the M-Link Web Application using an existing WWW service the content of the *`(SHAREDIR)`/webapps/mlink/webmlink.zip* package must be extracted into the appropriate directory on for serving by an existing web browser. The default location of this directory will vary depending on the server used to host the applications. After configuring the web browser to serve the content, it is often desirable to configure the M-Link Web Application as described below.

20.2.2.1 Apache HTTP Server configuration

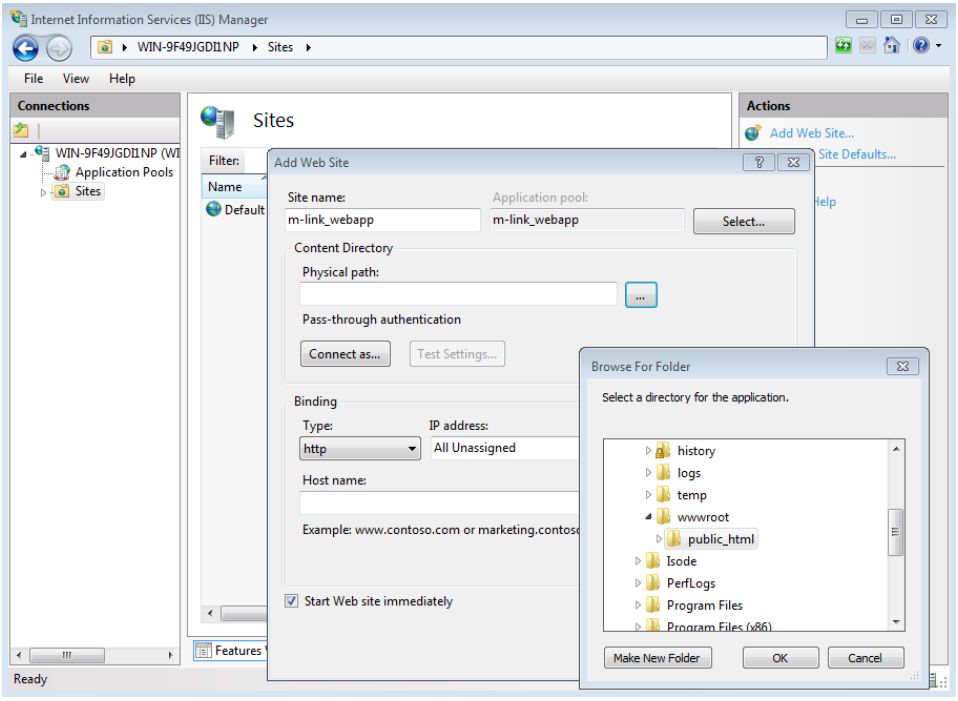
On Apache HTTP Server, default content directories are typically:

- Linux systems: */var/www*
- Unix systems: *(HOME_DIR)/Sites*
- Windows systems: *(LOCAL_DRIVE):\(APACHE_INSTALLDIR)\www*

To install the M-Link Web Application into an Apache HTTP Server content directory, the *public_html* folder must be extracted into the *www* folder on the server. Optionally, you may choose to rename the *public_html* folder.

20.2.2.2 Microsoft IIS configuration

Figure 20.1. Configuring the M-Link Web Application on Microsoft Internet Information Services Manager



For deployment on a Microsoft Internet Information Services (IIS) managed server, the default directory for content is *(LOCAL_DRIVE):\inetpub\wwwroot*. The applications can be extracted into this folder; alternatively it is possible to deploy the M-Link Web Application using the Internet Information Services manager interface. To do this, open the Internet Information Services Manager and select the Sites node from the Connections tree. Next, select **Add Web Site...** and specify the path for the *public_html* folder extracted from the M-Link Web Application package.

After extracting and deploying the M-Link Web Application, the application can be accessed with the relevant URL. Assuming default names, the URL is constructed as follows: *http://(SERVER-ADDRESS)/public_html/index.html*.

20.3 Configuration

20.3.1 The configuration file

A configuration file (*config.js*) is provided with the M-Link Web Application, enabling administrators to configure application parameters. This can be used, for instance, to select which authentication mechanisms the M-Link Web Application should use when connecting to M-Link Server. Assuming default folder names, the configuration file can be found in the *(SHAREDIR)/public_html* folder, a sample configuration (*config_sample.json*) has also been provided for reference. To add a new configuration, copy the sample configuration file and modify the parameters as required. To enable the configuration, replace the existing *config.js* with the new configuration. The configurable options include:

- `transports` -- This specifies the transport protocol used by the application, this should be specified as `bosh`.
- `boshURL` -- This is the URL used to connect to the M-Link Server using XMPP over BOSH. Its formed as described in Chapter 12, *XMPP over BOSH*.
- `hideLoginURLs` -- This specifies whether the BOSH URL field is visible on the login page. Set to `true` to hide, set to `false` for BOSH URL field to be visible.
- `login` -- This option should be set to the empty string.
- `pwd` -- This option should be set to the empty string.
- `sasl` -- The methods available to authenticate the user. This option does not generally need to be altered.
- `modules` -- This option specifies the modules enabled on the application. The available modules are:
  - `fdp` -- Provides form discovery and publishing capabilities, allowing users to publish and subscribe to available FDP nodes.
  - `mam` -- Provides Message Archive Management (MAM) capabilities.
  - `stats` -- Provides statistics monitoring capabilities for the M-Link Server.

  By default all modules are enabled and will be accessible from the menu in the M-Link Web Application. It is possible to disable modules by changing the value from true to false.

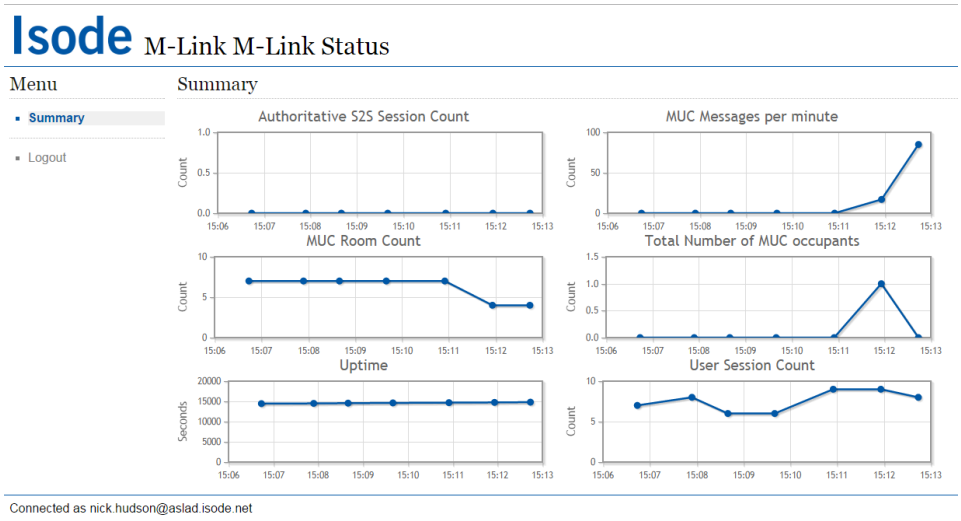
> **Note:** The contents of this file are readable by anyone able to access the M-Link Web Application files, including all M-Link Web Application users, and hence should be free of sensitive information.

20.4 Usage

The M-Link Web Application requires administrative rights on the server in order to access certain features. This can be configured using M-Link Console by navigating to **User Group Configuration** and adding members to the relevant groups. Group configuration is covered in detail in Chapter 4, *Configuring Groups*. Provided a user has the required privileges to access the M-Link Web Application, they will be able to login and use the available modules listed in the application menu.

20.4.1 Statistics

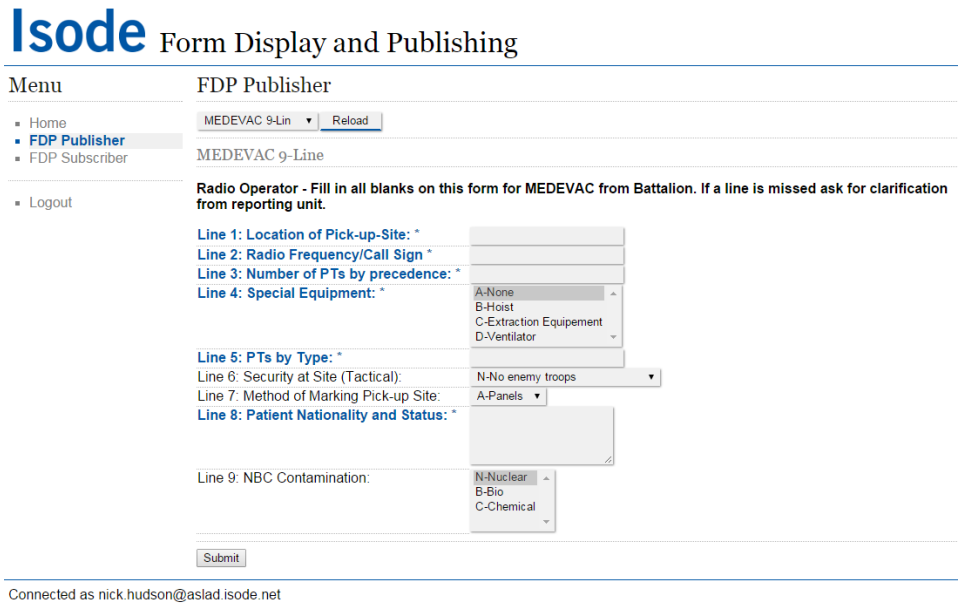
Figure 20.2. M-Link Web Application - Statistics



The Statistics module provides an overview of some key statistics for the M-Link Server, displaying a graph for each statistic and a summary of the current values in a table. These include the authoritative server-to-server (S2S) session count, MUC messages per hour, MUC room count, total number of MUC occupants, server uptime and user session count. The charts are updated automatically, at a regular time interval determined by the M-Link Server.

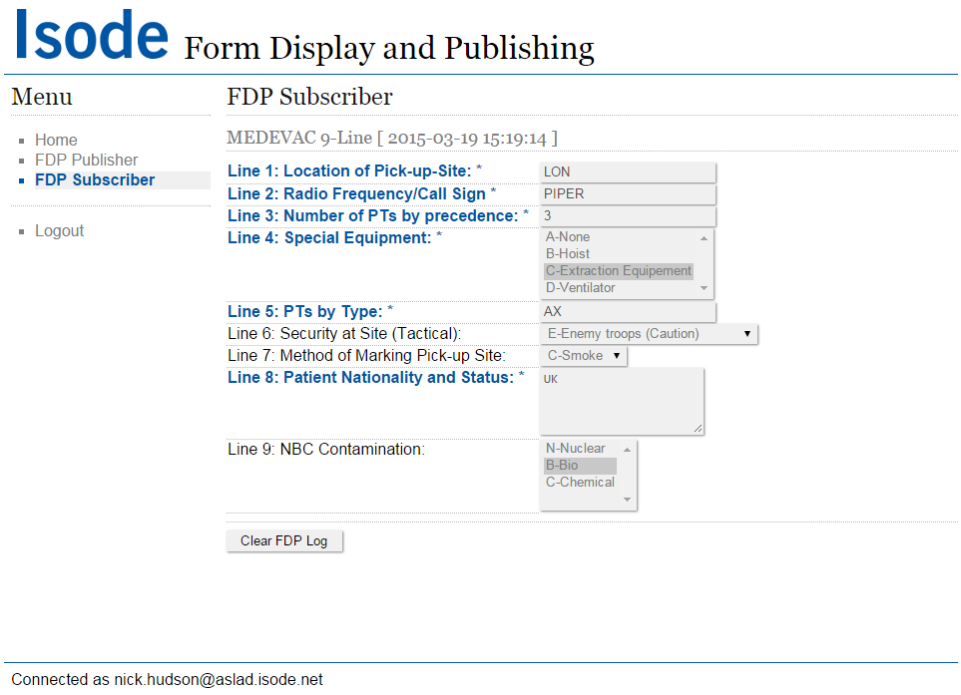
20.4.2 Form Discovery and Publishing

Figure 20.3. M-Link Web Application - FDP Publisher



The FDP Publisher module provides capabilities to view and submit FDP forms. The FDP Publisher module lets users fill in and submit FDP forms. It contains a selection box, where available FDP templates on the M-Link Server will be listed. Choosing a template and selecting **Reload** will display the selected template on the page. The template can then be filled in, when the **Submit** button is selected the form will be published on the M-Link Server. The mobile version provides the same functionality, but with a layout more suited to mobile devices.

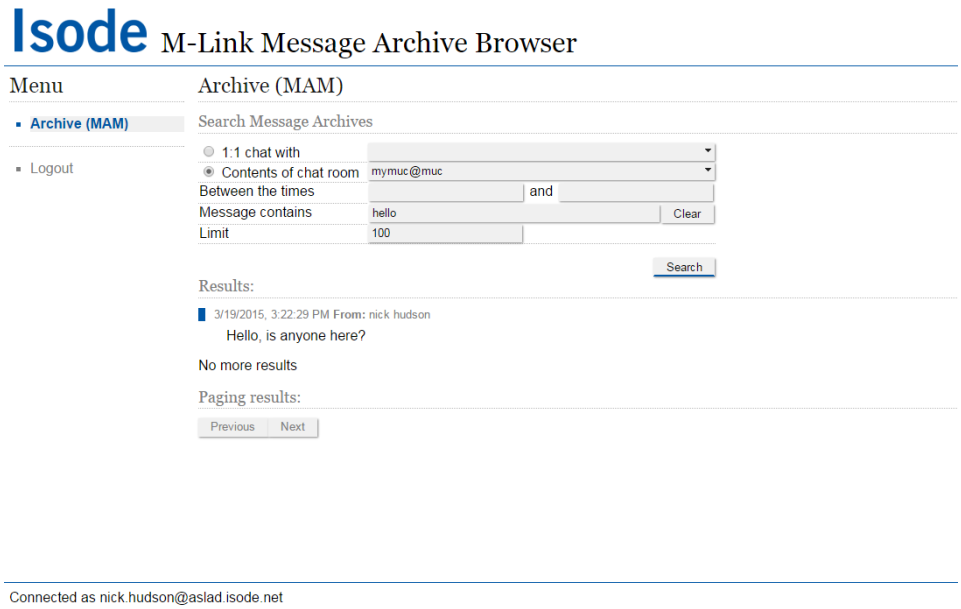
Figure 20.4. M-Link Web Application - FDP Subscriber



The FDP Subscriber module displays a log of any published FDP forms from subscribed FDP topics. The log contains the form title, time-stamp and form content. The log is updated when the server publishes a new form. To reset the FDP log, select the **Clear FDP Log** button.

20.4.3 M-Link Web Application - Message Archive Browser

Figure 20.5. Message Archive Browser



The Message Archive Browser module provides access to MAM-based message archives, allowing administrators to view chat history for Multi-User Chat rooms and chat history between specific users. The page displays several filters allowing you to configure the search query. Once the search has been configured, you can select the **Search** button to display a log of the chat history.

Chapter 21 SPIF Editor

This chapter describes the SPIF Editor application and explains how to use it to create, edit and view a SPIF (Security Policy Information File) and various utility functions.

The term SPIF referes to Security Policy Information File. A Security Policy is represented as an SDN.801c SPIF in the Open XML SPIF format. A SPIF is structured data which defines for a given policy ID the valid classifications and security categories. It also can define strings to be associated with labels, which are used for mark-up of data for human reading. It can define equivalent policies, which enables labels defined by a different authority to be associated with labels defined in this SPIF. It also defines how the ‘Access Control Decision Function' (ACDF) is to be applied.

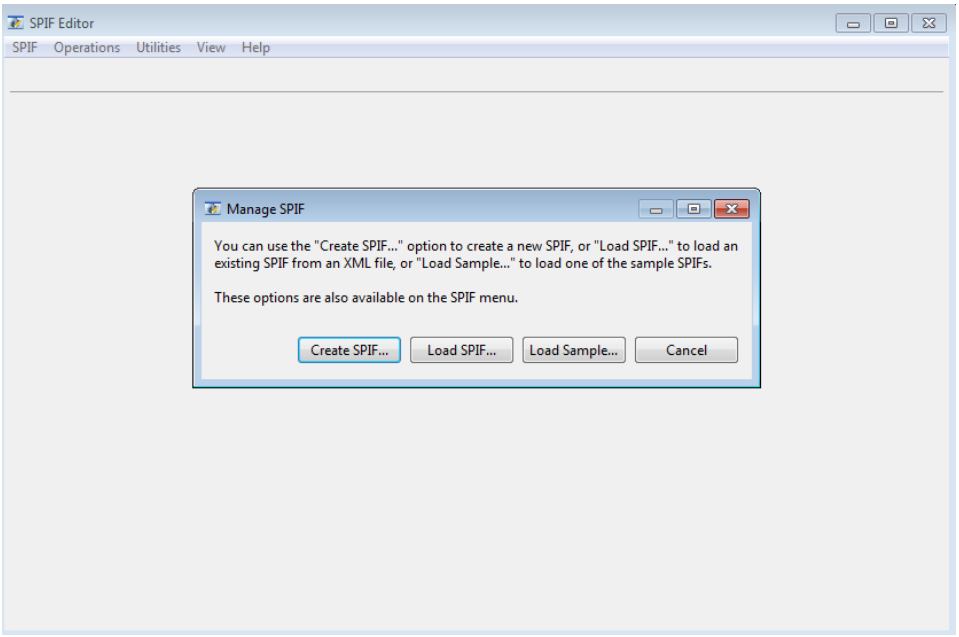
21.1 SPIF Editor Overview

SPIF Editor is a GUI that allows you to create, edit and view SPIFs. The primary purpose of the editor is to make it easy to create and manage security labeling for Isode servers and clients. It is not necessary to use the SPIF Editor in order to use security labeling in Isode products, but in many cases it may prove to be the simplest means of doing so.

21.1.1 Getting started

On launching the SPIF editor, a dialog will appear that provides options to create a new SPIF, load an existing SPIF XML file or load one of the samples provided as part of its installation.

Figure 21.1. SPIF Editor Launch Screen

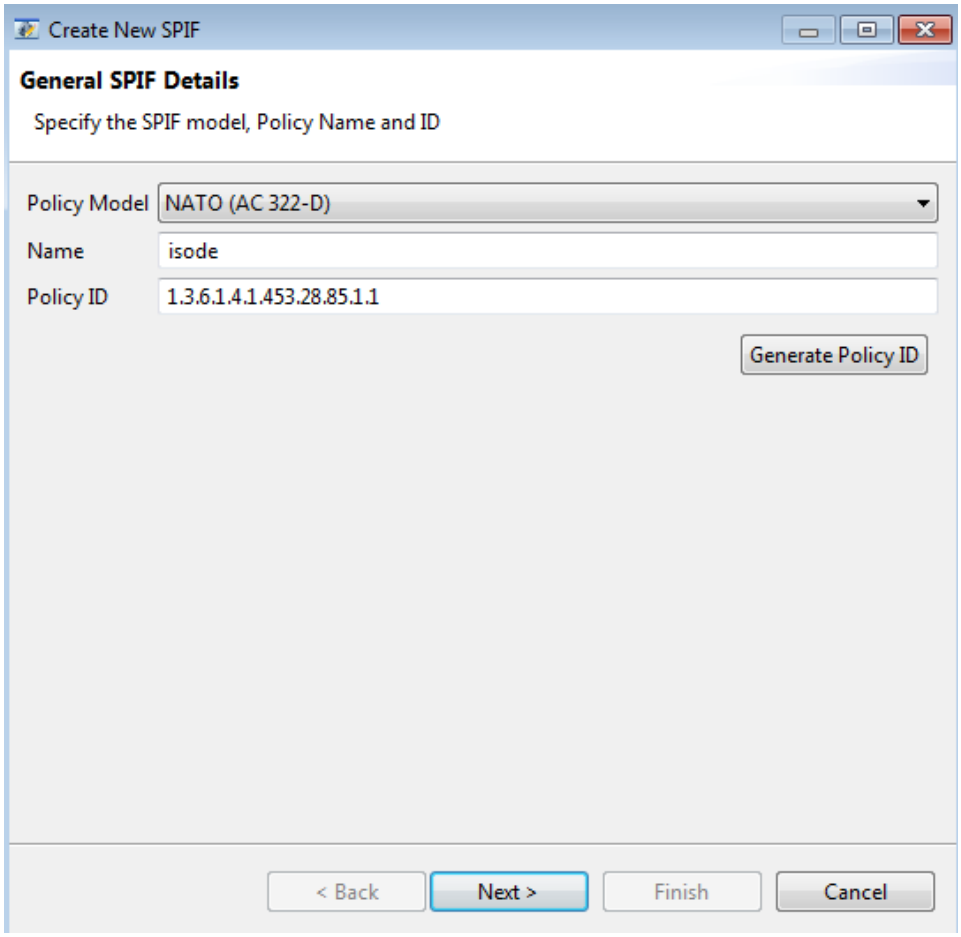


21.2 Creating New SPIF

A new SPIF can be created by choosing the **"Create SPIF..."** button on the launch dialog. The option is also available on the **SPIF** → **Create...** menu. The wizard for creating a new SPIF is shown in the figure below.

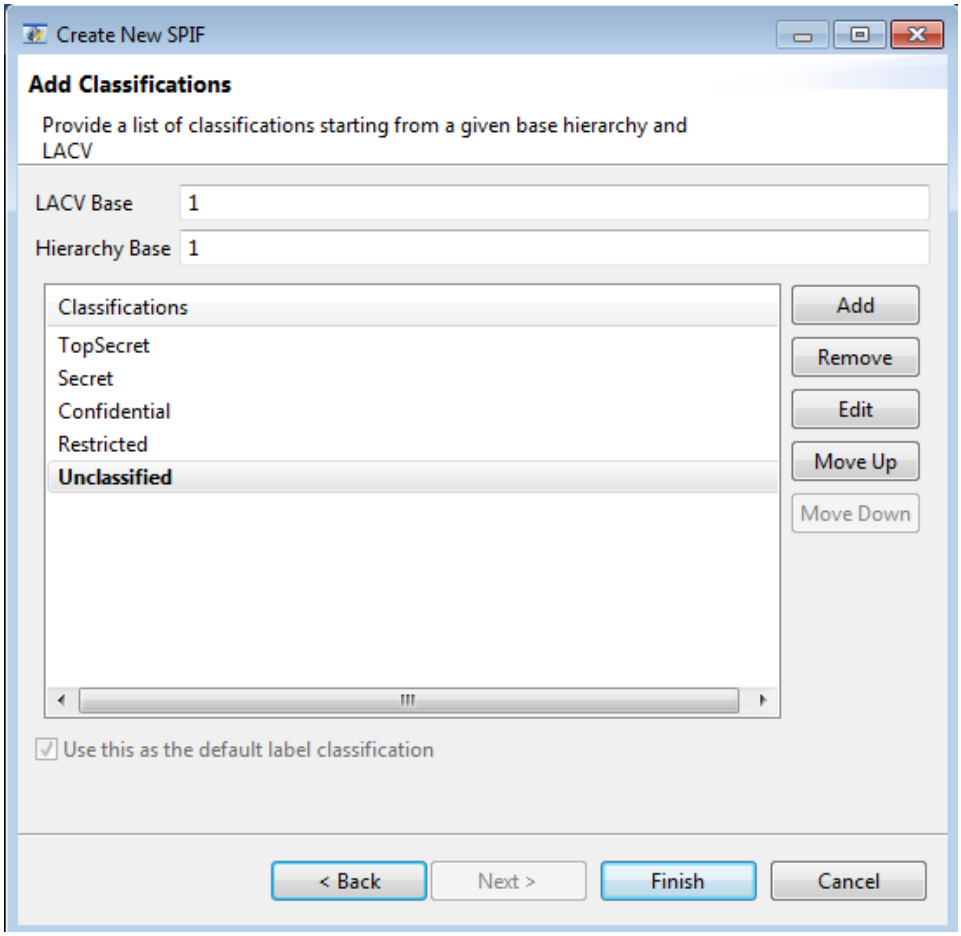
Provide the policy model, name and ID for the SPIF on the first page.

Figure 21.2. Create SPIF



On pressing **Next** button, list of standard classifications will be offered as a default.

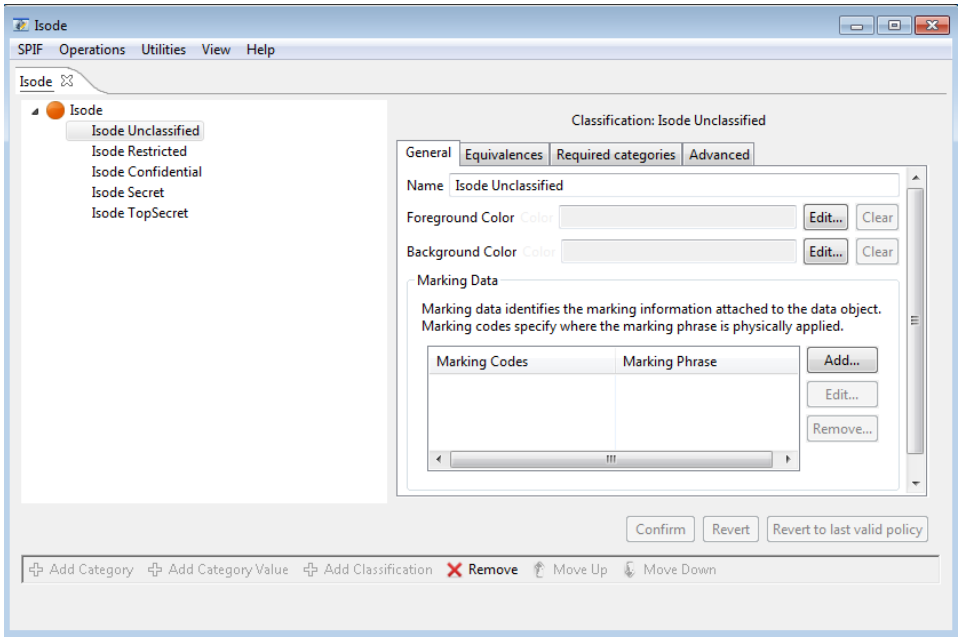
Figure 21.3. Create SPIF Classifications



The list can be modified to add or remove classifications. The name of the classifications can be modified using **Edit...** button. The LACV value stands for the classification value whereas the hierarchy governs the ordering of the classifications in the SPIF.

On pressing **Finish**, the SPIF will appear on the SPIF editor as shown below.

Figure 21.4. Created SPIF



21.3 Managing Existing SPIF

An existing SPIF XML file can be loaded in a SPIF editor using the **SPIF → Load...** menu.

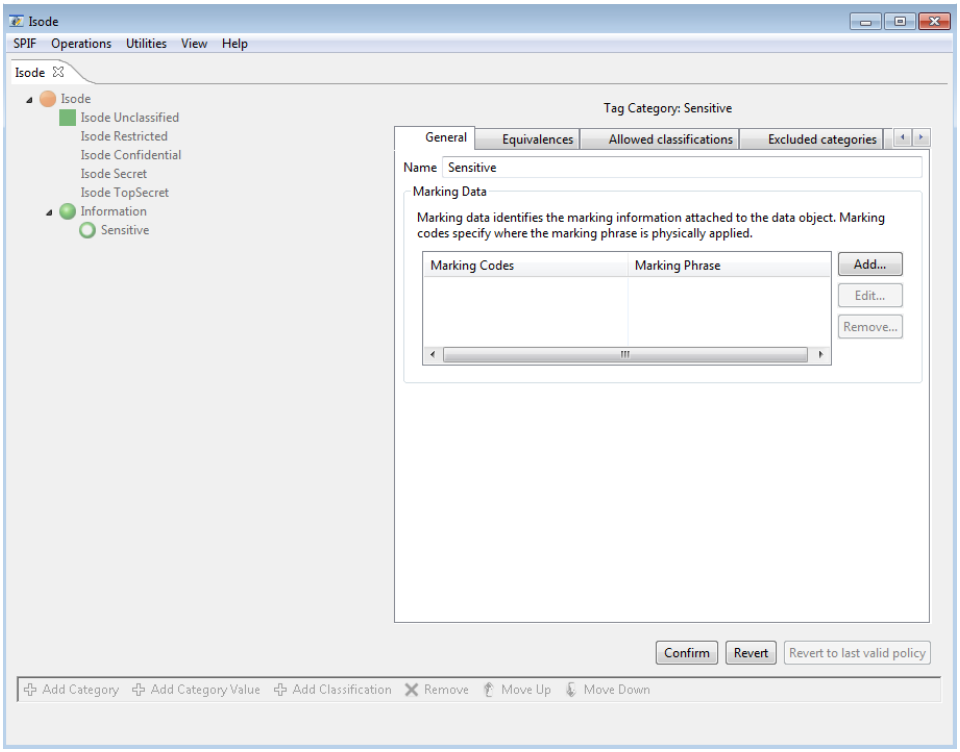
Once a SPIF has been created or loaded from an XML file, it can be viewed or edited using the SPIF editor. The left hand side presents the classifications and categories of the SPIF in a tree format. The classifications are listed on top of the tree followed by categories.

Classifications are displayed using their background color icon and categories are displayed using green circle icons. Note that categories are optional and may not exist in most SPIFs.

On selecting a classification or a category, the right hand side pane will display the details of selected classification or category.

When the selected classification or category is edited, the **Confirm** and **Revert** buttons will get enabled to let you apply the current set of changes or cancel them. Note that the **Confirm** button will not get enabled until the current set of changes made are complete and valid.

Figure 21.5. Category Edit



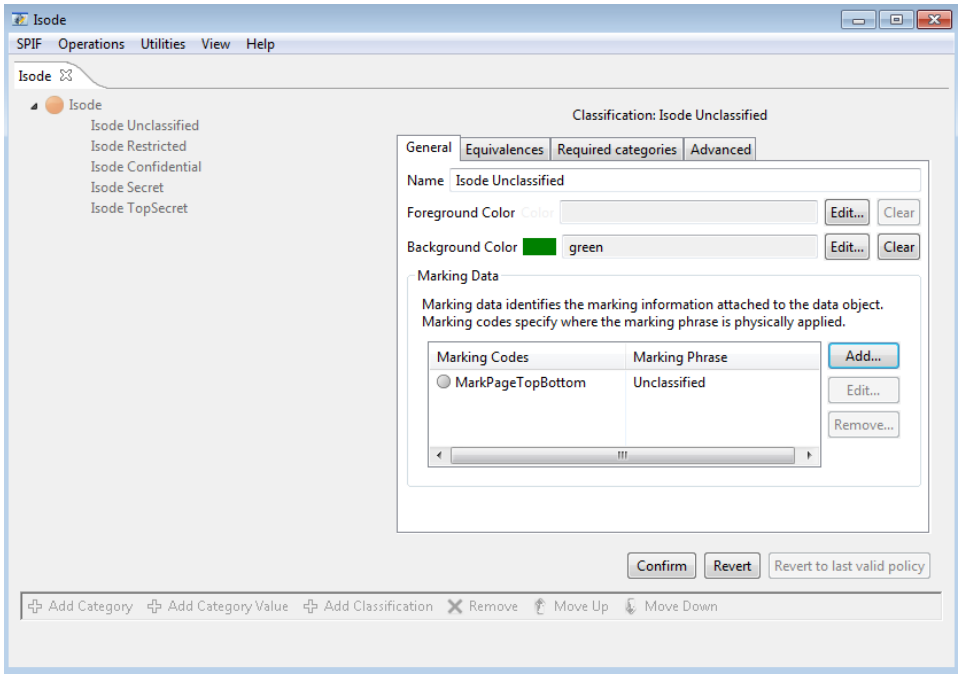
The editor allows you to modify only one classification or category in one operation. For complex policies, a change in more than one classification or category may be required to create a valid policy. If an edit makes the policy invalid **Revert to last valid policy** will get enabled to allow you to revert to last valid state to undo the changes that lead to the invalid policy.

21.4 SPIF Classifications

Select a classification on the left hand side side in order to edit it. After making the required changes, click the **Confirm** button.

The following figure displays the SPIF after adding a marking code and changing the background color of the classification.

Figure 21.6. Classification Edit

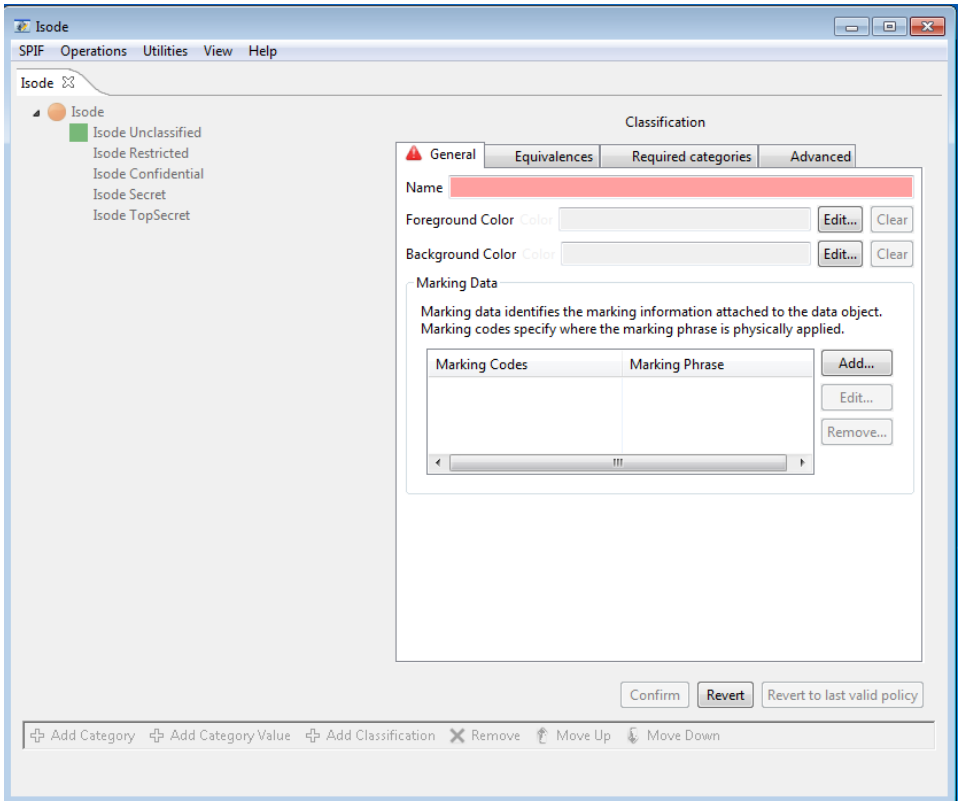


The **General** tab lists the most commonly used attributes. Rest of the tabs define advanced parameters that are required for complex SPIFs.

21.4.1 Adding Classifications

Select the topmost tree item for the policy and click **Add Classification** button to add a new classification. Provide the details of the new classification to be added on the right hand side pane. The tabs that require mandatory parameters for completing classification creation will display a red icon on the top.

Figure 21.7. Add Classification



Once the details of the new classification have been provided, press the **Confirm** button to create the new classification. By default, the editor will fill in default values and in simple cases you will only need to provide the classification name. Colors and markings can be added to suit the requirements.

21.4.2 Removing Classifications

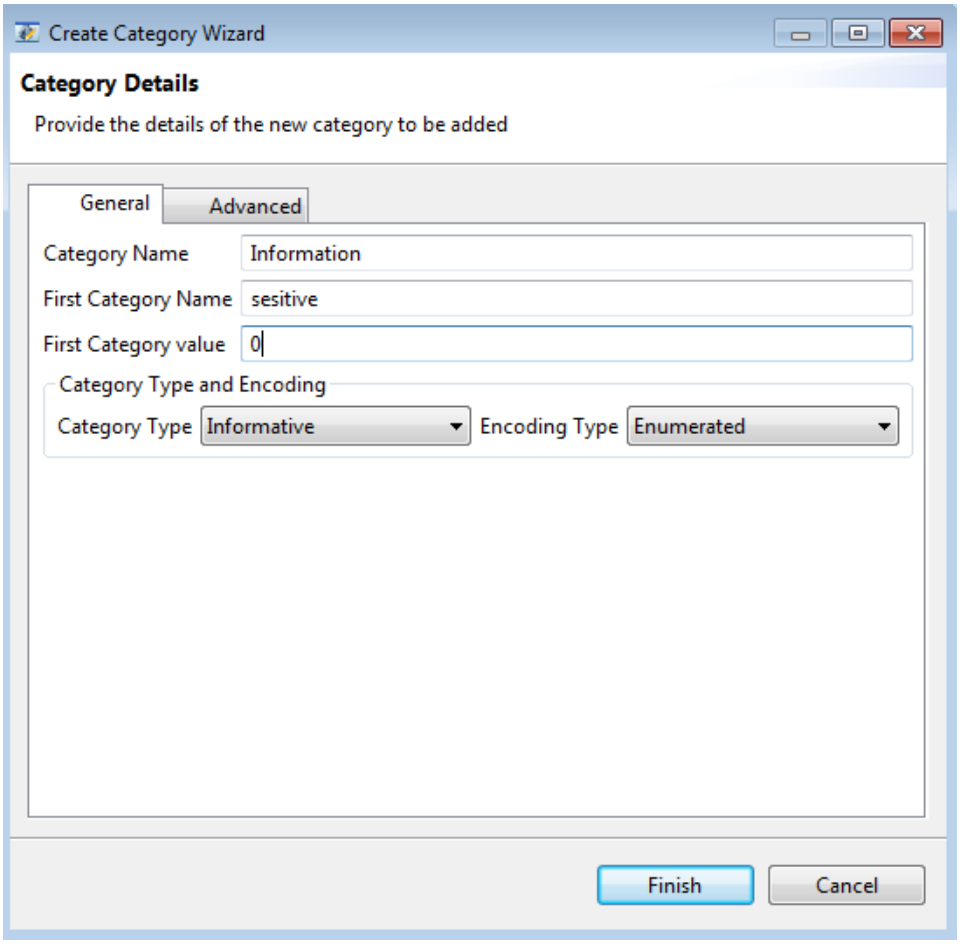
Select a classification and click **Remove** button and confirm to remove the selected classification from the policy. Errors will be reported if removal of a classification invalidates the security policy.

21.5 SPIF Categories

21.5.1 Adding Category

In order to add a new category group, select the topmost tree item for the policy and click **Add Category** button. A wizard to add a new category will be displayed.

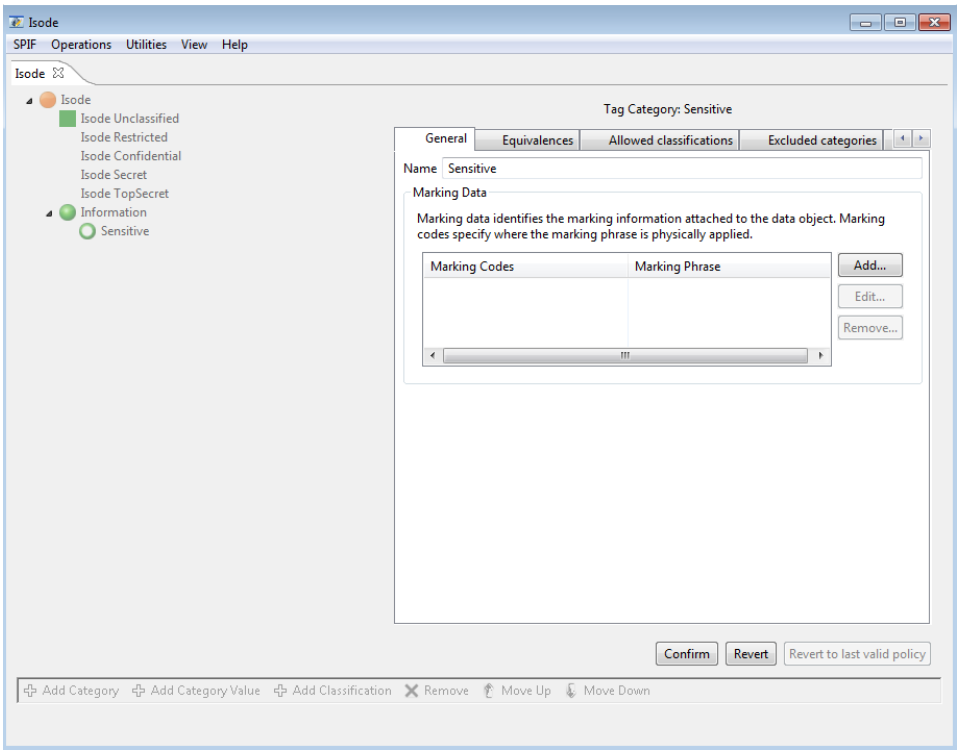
Figure 21.8. Adding Category



The wizard page will ask you to provide the details of the new category group and first value in the group. For simple case, category name and type will have to be provided. See the tooltips on the widgets for more information on the parameters.

On pressing the **Finish** button the editor will display the category to be added on the editor. You can make further changes to the values for this category. Press **Confirm** button to add the category to the SPIF.

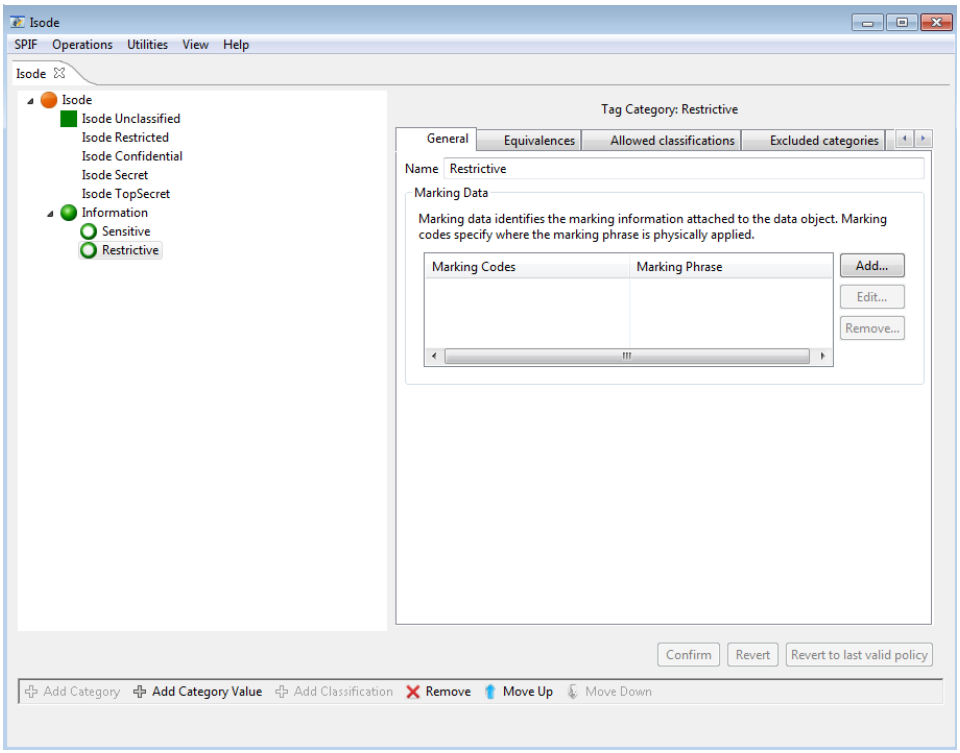
Figure 21.9. New Category



21.5.2 Adding Category Value

To add a new category value to an existing category group, select the category group and click the **Add Category Value** button. The right hand side pane will change to a mode for adding a new category. Provide the name of the category value and other details if required and press the **Confirm** button. The new value will be added to the SPIF as shown below.

Figure 21.10. Adding Category Value



21.5.3 Removing Category

Select the category value and click **Remove** button to confirm removal of the category value. Similarly, select a category group and click **Remove** button to remove the selected category group and all its values from the policy. Errors will be reported if removal of a category invalidates the security policy.

21.5.4 Moving Categories

Select a category group or value and click on **Move Up** or **Move Down** button to move it up or down the hierarchy. Press **Confirm** to apply the changes to the SPIF.

21.6 SPIF Utilities

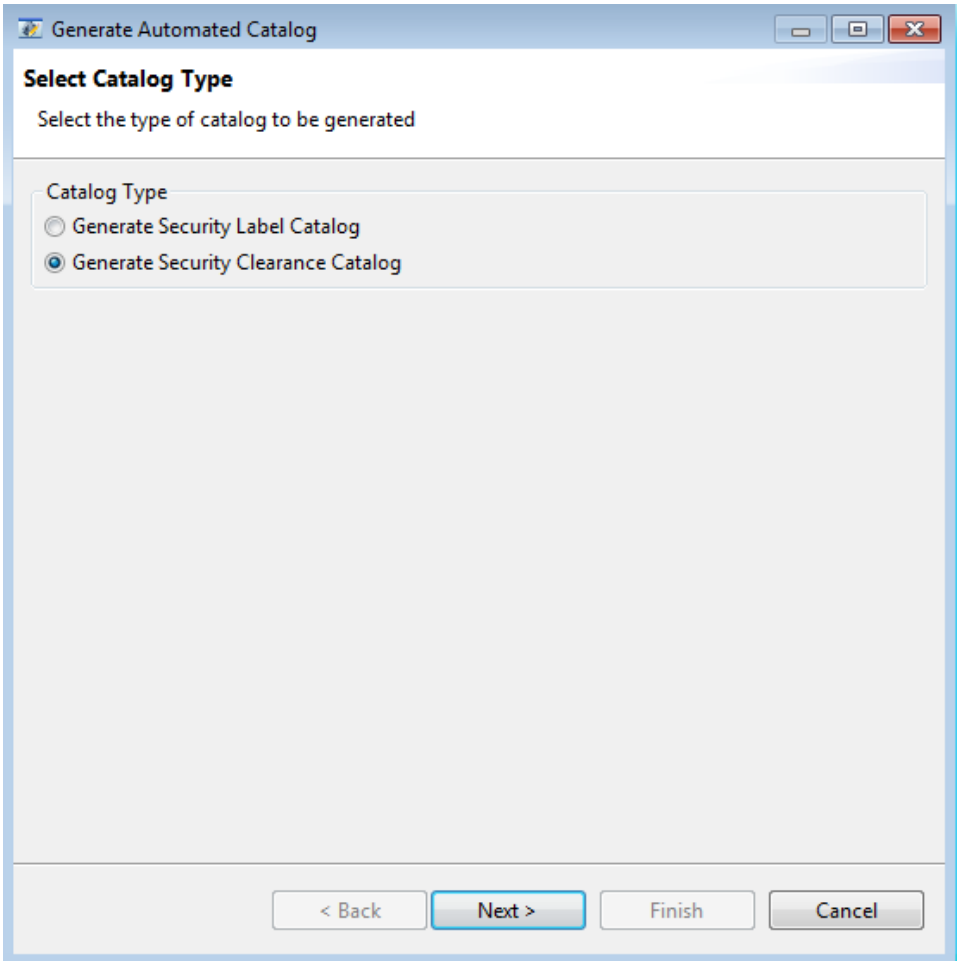
The SPIF editor provides commonly used functions that are available via the **Utilities** menu.

21.6.1 Generate Catalog

Security label and clearance catalogs are collections of security labels and clearances. Click the **Utilities** → **Generate Catalog...** menu to launch a wizard to auto generate label and clearance catalogs.

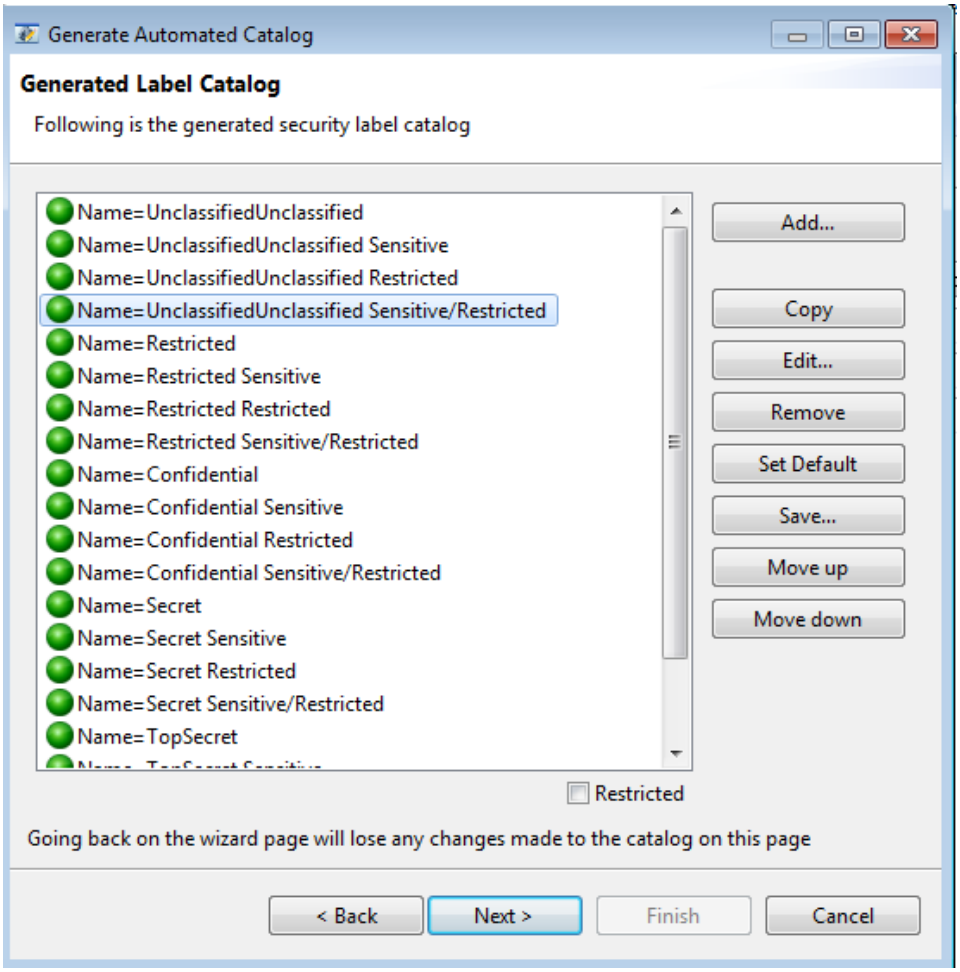
First select the type of catalog to be generated.

Figure 21.11. Select Catalog Type



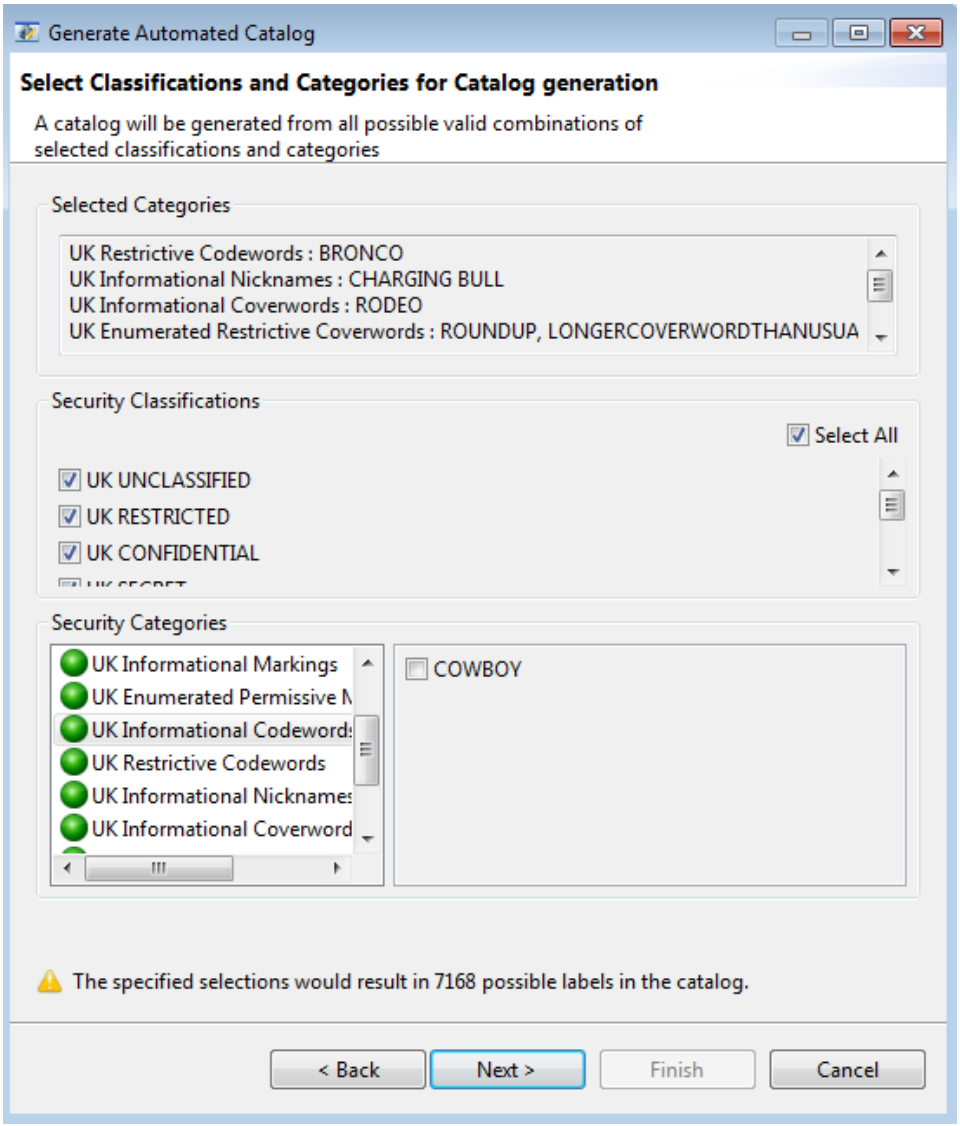
If the policy is simple with few classifications and categories (optional), the wizard will generate a catalog with all possible combinations of classifications and categories. The generated catalog will appear as shown in the figure below that displays a sample auto generated label catalog.

Figure 21.12. Label Catalog



However, for a policy which has large number of classifications and categories, the wizard will present a page to choose a set of classifications and categories to be included in the catalog.

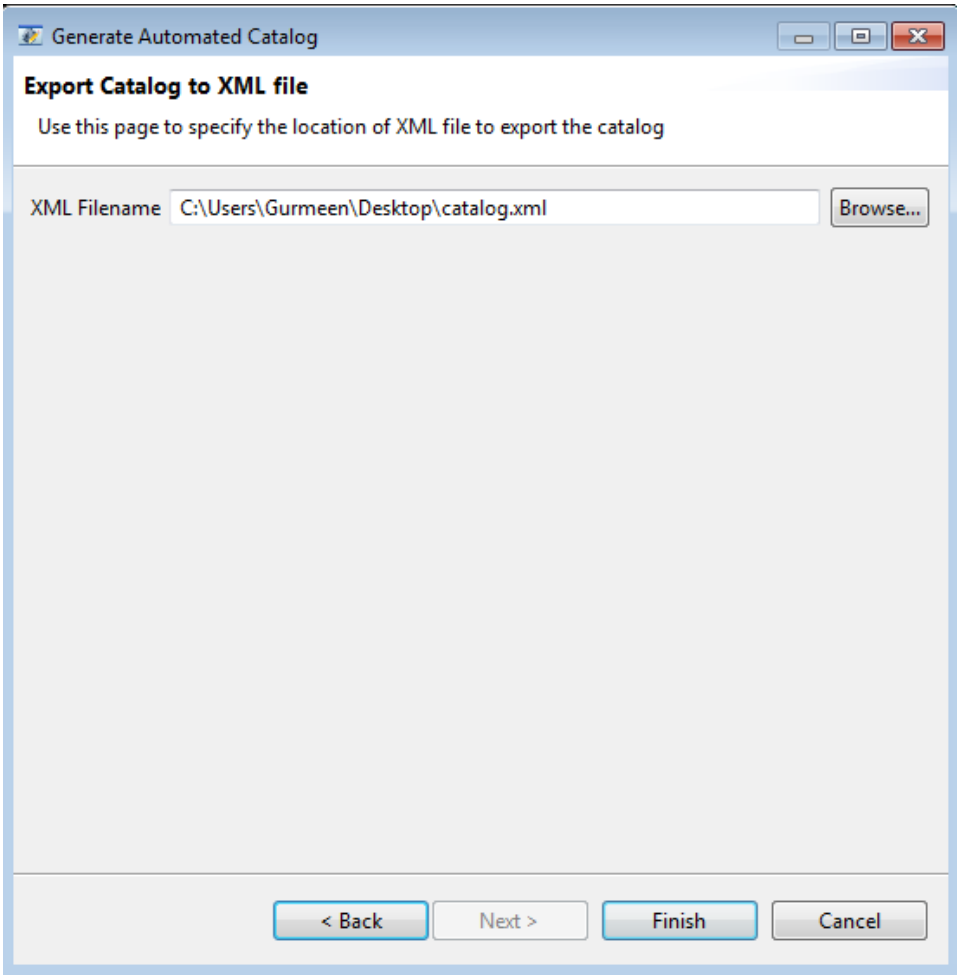
Figure 21.13. Selected Classifications and Categories



The wizard will attempt to generate a catalog from all possible combinations of selected classifications and categories. A warning will be displayed on the bottom of wizard page if the number of possible combinations is high (in terms of hundreds) and an error will be displayed if the number of combinations is very high (in terms of thousands).

Once a label or clearance catalog has been generated, it can be edited if required on the wizard page that displays the genererated list as shown in figure Figure 21.12, “Label Catalog”. On pressing the **Next** button, the page will prompt you to select an XML file location to save the catalog.

Figure 21.14. Export Catalog

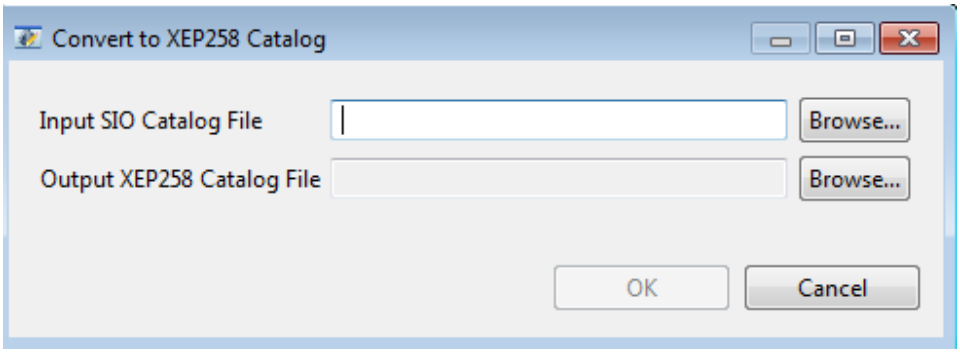


Press **Finish** to complete the catalog generation.

21.6.2 Converting Label Catalog to XEP-258 Format

The **Utilities** → **Convert to XEP258 Catalog...** can be used to convert a label catalog to a format that conforms to the XEP 258 format of the XMPP standards.

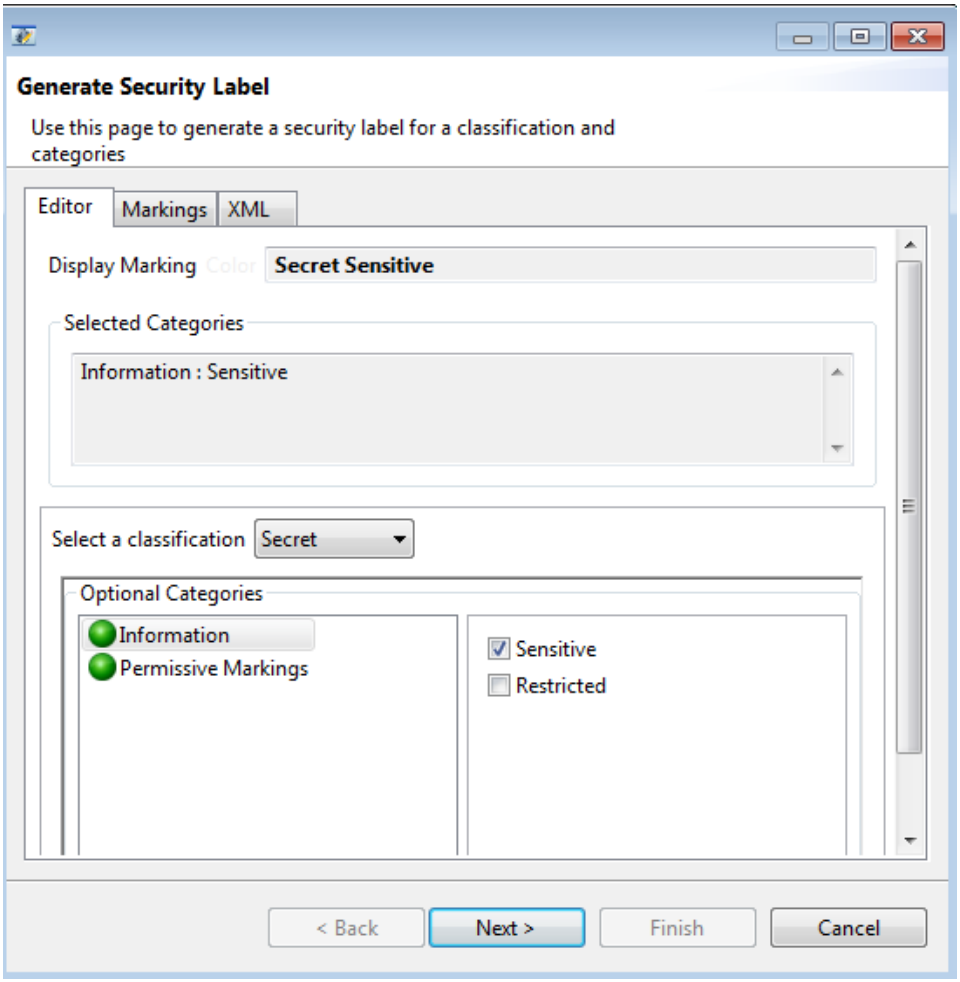
Figure 21.15. Convert to XEP258 Catalog



21.6.3 Generate Label

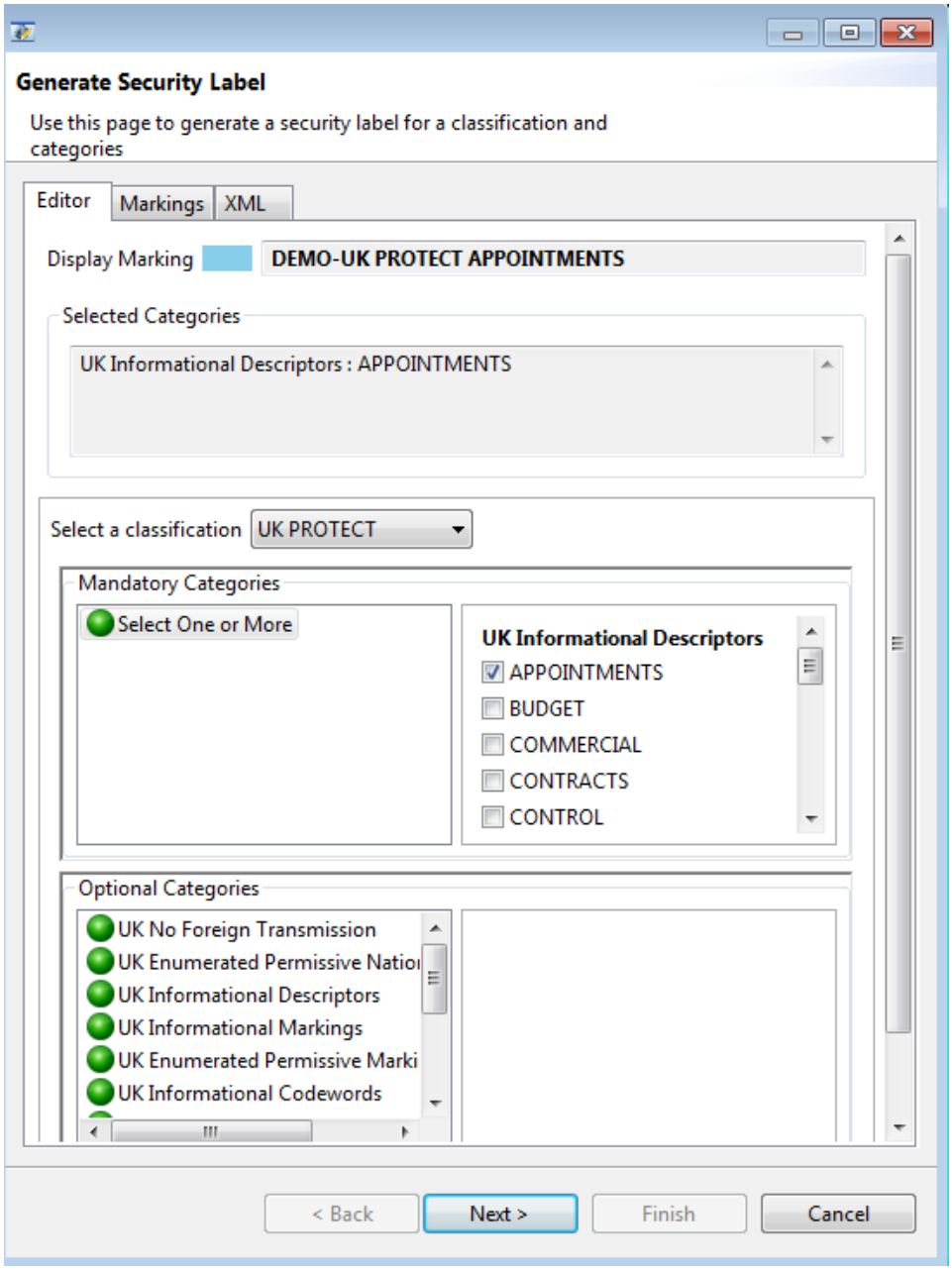
For simple policies, select a classification and one or more categories to generate a label.

Figure 21.16. Generate Label for Simple Policy



Label generation for complex policies is described below.

Figure 21.17. Generate Label for Complex Policy



First select a classification from the drop-down list. Selecting a classification may or may not require inclusion of certain categories. The required categories if any will be displayed as a list in the **Required Categories** pane. The **Optional Categories** pane lists all the categories in the configured policy from which the user can select certain categories to be added to the label. The categories which are disallowed based on the selection of a certain category or the classification will be disabled automatically on the editor. The obsolete categories will be allowed for editing based on whether **Edit obsolete elements** is selected or not.

Selection rules of a category group determine whether it allows selection of single or multiple categories in the group. For single category selection, the categories are displayed using radio buttons and for multiple category selection they are displayed as check-boxes.

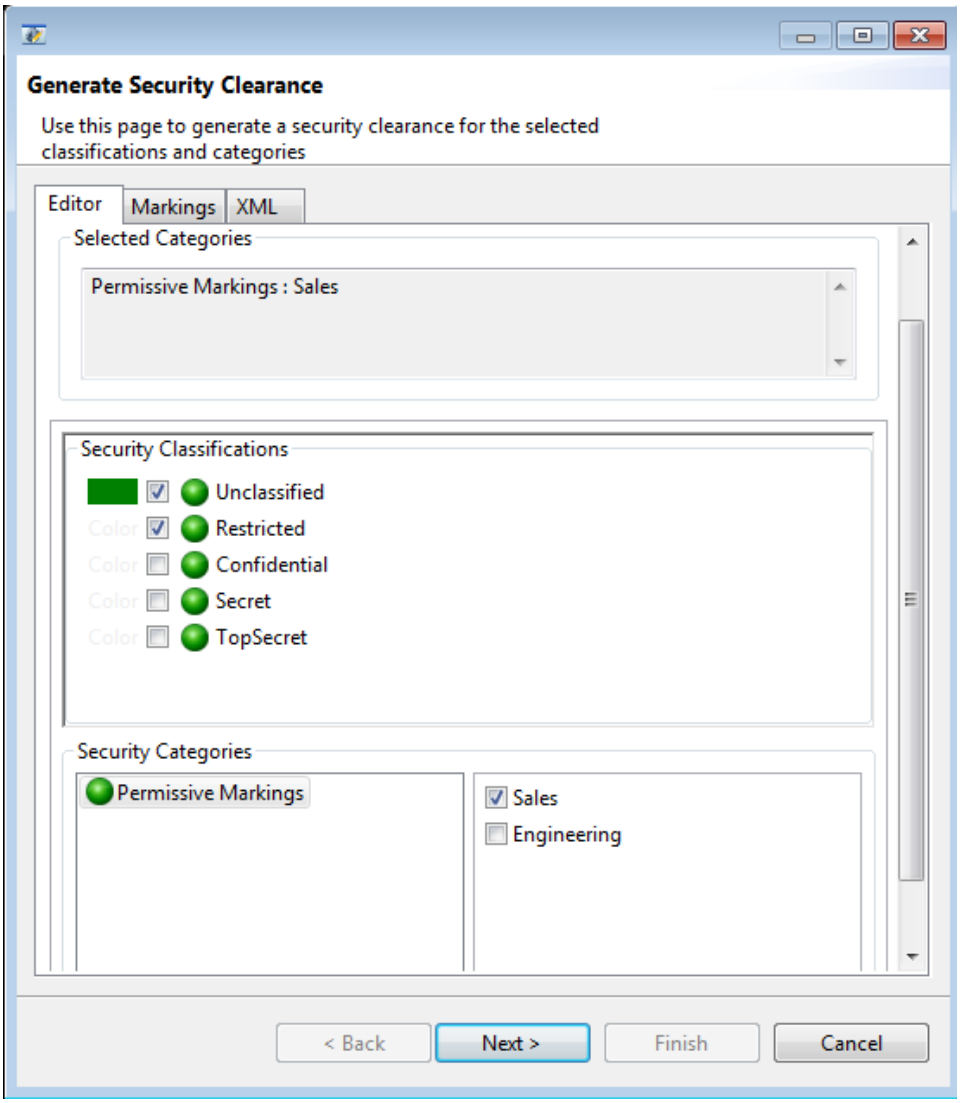
The markings get updated on the **Markings** tab when a valid combination of categories has been selected.

> **Note:** Rules for label editing are based on SDN.801c and are configured in the security policy.

21.6.4 Generate Clearance

The **Utilities** -> **Generate Clearance...** can be used to generate a security clearance using the selected policy. The following wizard will be presented for clearance generation.

Figure 21.18. Generate Clearance

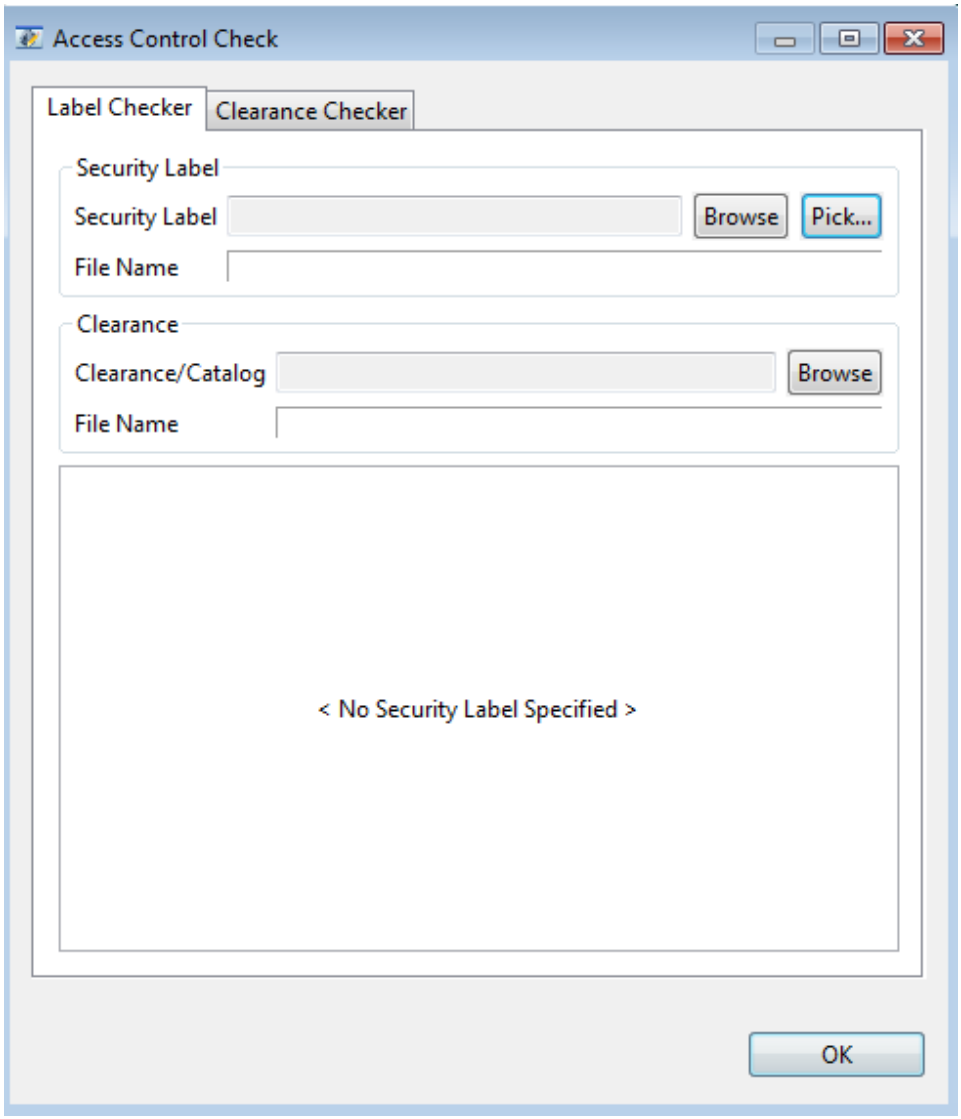


One or more classifications can be selected from the **Security Classifications** pane to be added to the clearance. The **Security Categories** pane lists all the categories in the configured policy from which the user can select certain categories to be added to the clearance. The markings get updated on the **Markings** tab as and when the clearance is edited.

21.6.5 Access Control Checks

SPIF editor can be used to verify a security label against a security clearance and vice versa. To check access controls, select **Utilities** -> **Access control checks...**. menu. A dialog for performing these checks will be presented.

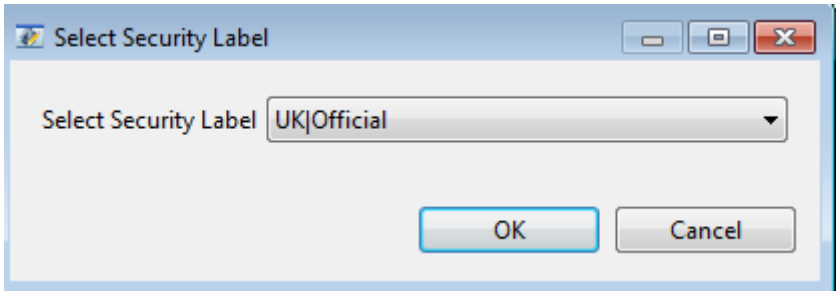
Figure 21.19. Access Control Checks



Select **Label Checker** to check access control of a label against a clearance or a catalog of clearances. Select **Clearance Checker** to check access control of a clearance against a label or a catalog of labels.

The label can be selected from an XML file by browsing the file system using the **Browse** button or picked up from a label calaog using the **Pick...** button. The **Pick...** button will offer the labels in the catalog in the form of a dropdown list as shown below.

Figure 21.20. Pick Label from Catalog



The label can be checked against a clearance or a clearance catalog that can be selected from the file system using the **Browse** button.

Once a label and clearance/catalog has been selected, the result of access control checks will be displayed in the bottom pane.

Figure 21.21. Access Control Check of Label with Clearance Catalog

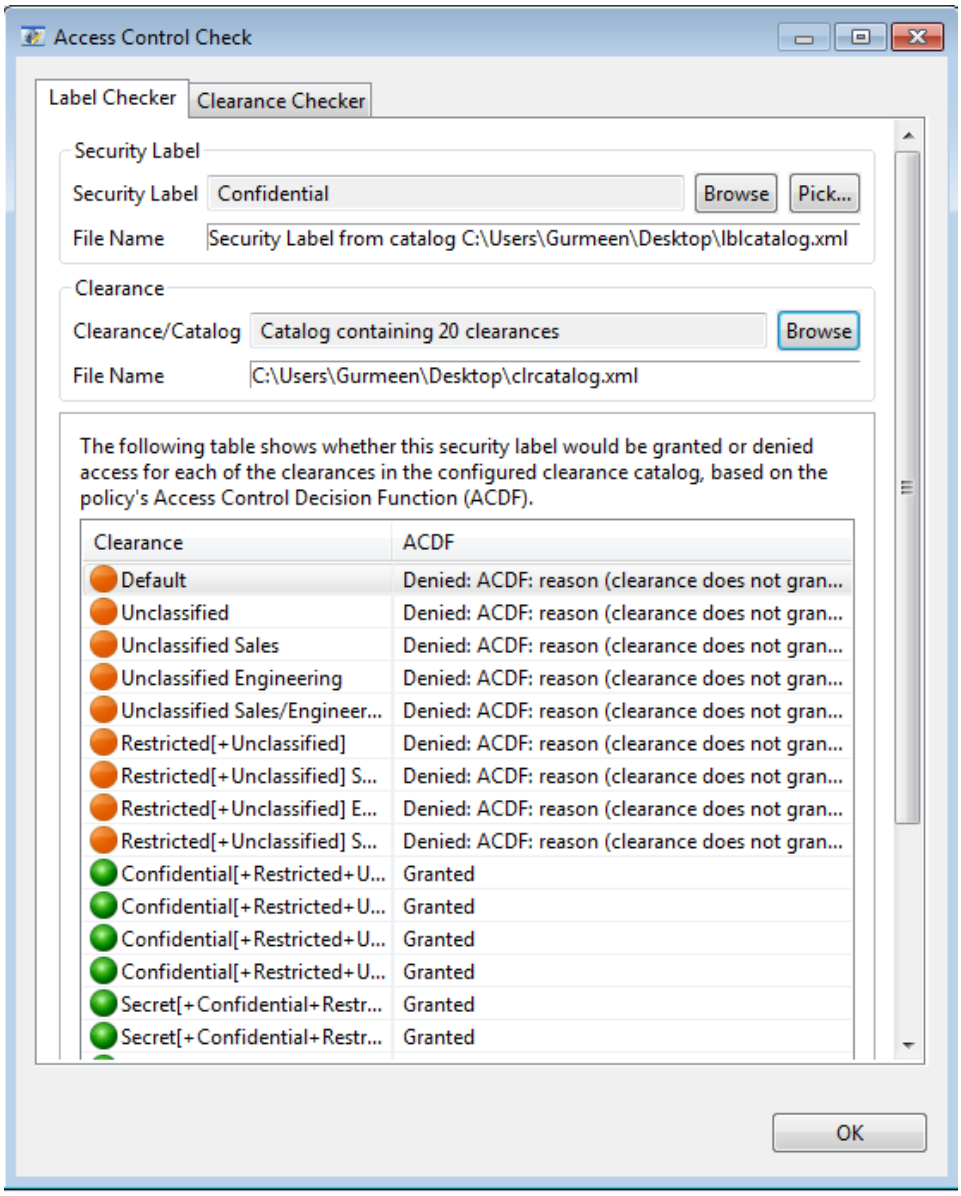


Figure 21.22. Access Control Check of Label - Acess Granted

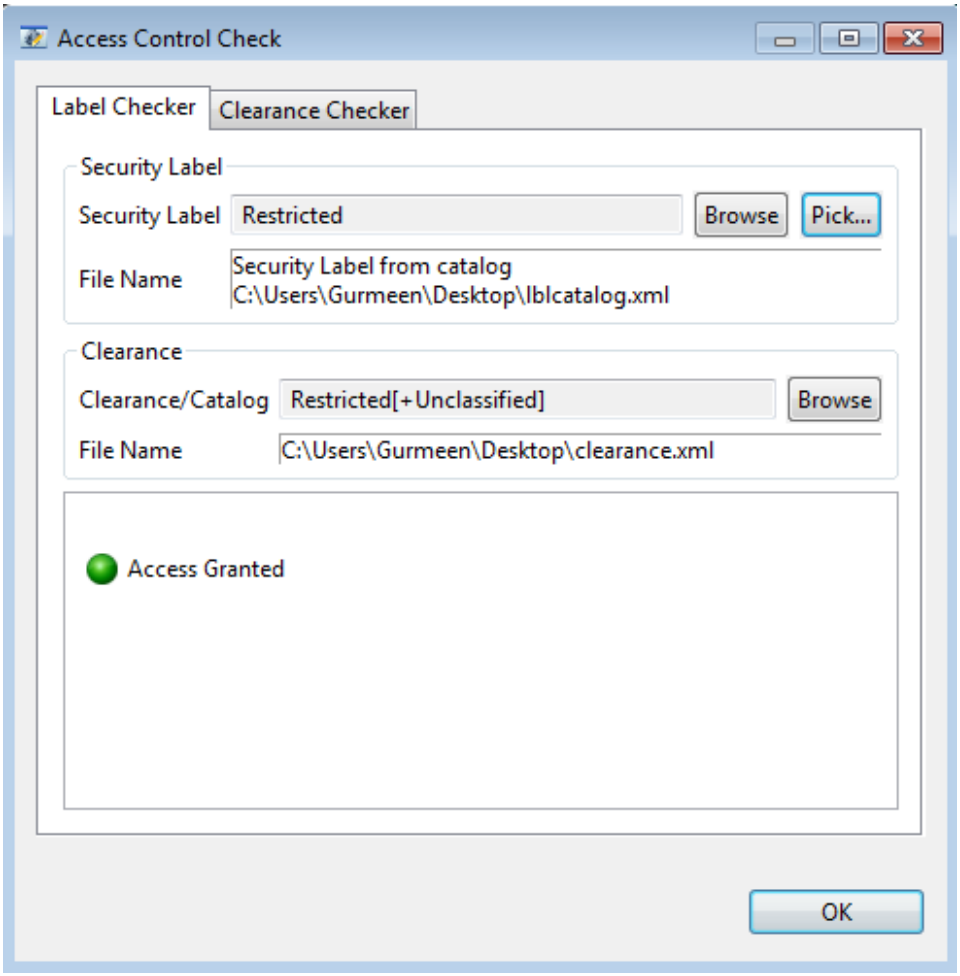
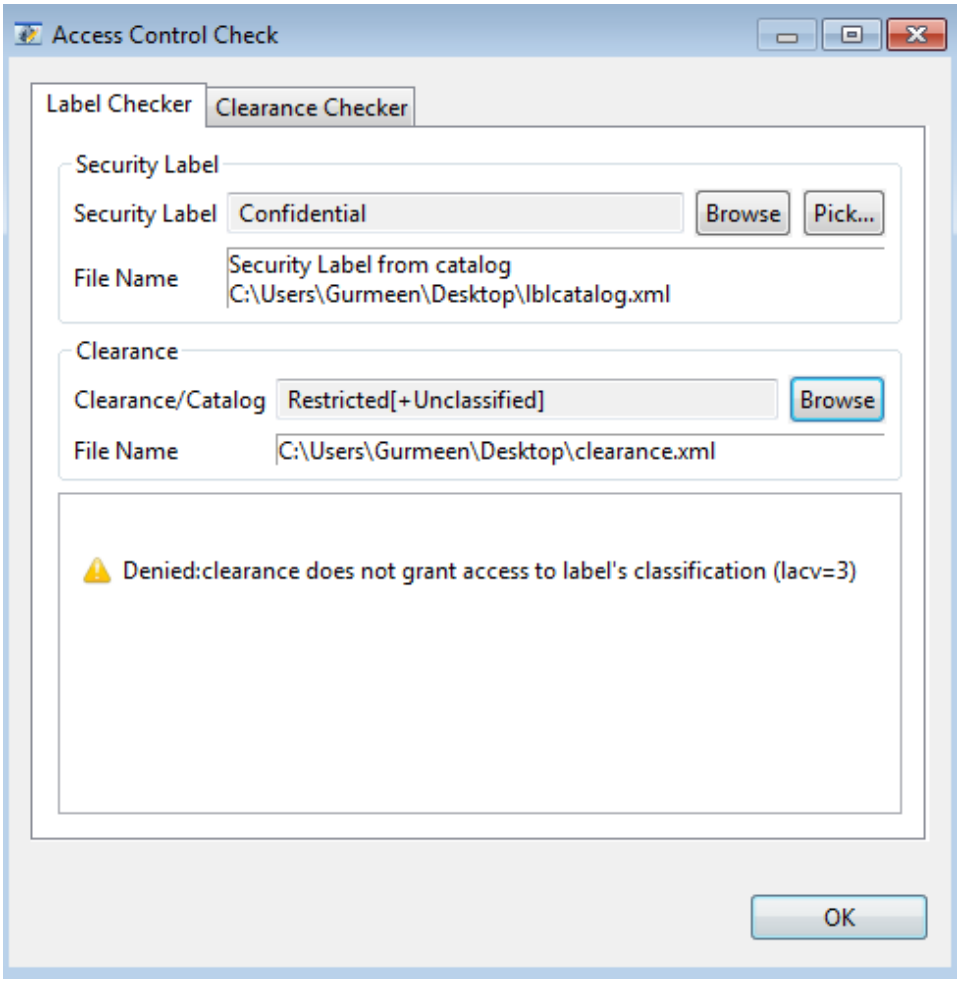


Figure 21.23. Access Control Check of Label - Access Denied



Follow the above steps in a similar way to check a clearance against a label or a catalog of labels by selecting the **Clearance Checker** tab.

Appendix A Command Line Operations

This chapter explains the command-line operations to manage the M-Link.

A.1 Running as Operating System Service

This section describes how to setup M-Link Server as an operating system service. This setup differs depending on the host operating system.

A.1.1 Linux

On Linux the M-Link Server can be identified by the process `isode.xmppd` and M-Link Archive Server by the process `isode.wabacd`.

An example startup/shutdown script, */opt/isode/sbin/mlink.sh*, is included in the M-Link package.

The script can start, stop and query the M-Link Server as well as M-Link Archive Server. A symbolic link *mlink* to the script is created in the *rc* directory specific to the platform. For example, on Red Hat Enterprise Linux 3.0 this will be */etc/init.d/mlink*.

In order to start M-Link Server and M-Link Archive Server; run:

```
# /etc/init.d/mlink start
```

In order to stop it run:

```
# /etc/init.d/mlink stop
```

To check if the M-Link Server is running:

```
# /etc/init.d/mlink status
```

To allow core files to be created (or to override the system-wide setting), set the `DAEMON_COREFILE_LIMIT` parameter in */etc/isode/mlink.rc* to the value `unlimited`. A restart of the server using the startup script is required for any changes to come into effect.

```
DAEMON_COREFILE_LIMIT=unlimited
```

A.1.2 Windows

When M-Link Console is used to create M-Link Server instance, it will setup M-Link Server and M-Link Archive Server to run as Windows services and can be used to start and stop these services as needed. However, at times, it may be desirable to start and stop using other service management tools, such as Services Microsoft Management Console (MMC).

While you may use such tools to start and stop the M-Link Windows services, it is recommended you do not use these to add or remove these services or modify their run time parameters. Instead the M-Link Console or, where needed, the Isode Service Configuration tool should be used. Isode Service Configuration tool is documented in the *M-Vault Administration Guide*

The M-Link Server and M-Link Archive Server can be identified by the Windows service services `isode.mlink.xmppd` and `isode.mlink.wabacd`, respectively.

You may use **mlink.exe** to uninstall, install, stop and start M-Link Server in cases where M-Link Console is not available (such as when Java is not installed). **mlink.exe** will need to be run with Administrator privileges or a user with the relevant permissions to manage these Windows services. Each of the following commands must be run from the command prompt as Administrator.

A.1.2.1 Deleting a service

```
C:\>"C:\Program Files\Isode\bin\mlink.exe"  uninstall
```

A.1.2.2 Adding a service

```
C:\>"C:\Program Files\Isode\bin\mlink.exe"  install
```

A.1.2.3 Starting and stopping a service

```
C:\>"C:\Program Files\Isode\bin\mlink.exe" start
```

```
C:\>"C:\Program Files\Isode\bin\mlink.exe"  stop
```

A.2 Start the server (debug mode)

The M-Link Server and M-Link Archive Server can be started on the command-line. This will usually be required when debugging the server. Otherwise M-Link should be run as a service. See Section A.1, “Running as Operating System Service”

The command name for M-Link Server is **isode.xmppd**.The command name for M-Link Archive Server is **isode.wabacd**.

The set of command line parameters used when starting either server are described below.

-d
: Run the server in debug mode. When running from the command line, this parameter should be specified. On Unix, the server will not detach and does not become a daemon. On Windows, the server is not started as a Windows service service.

-c configuration-file
: Specifies the name of the configuration file. If this parameter is not specified, then the server will look for the default configuration file *(ETCDIR)/mlink.conf*. If that is not found, then it will look for the default configuration file of versions before 15.2, namely *(ETCDIR)/ms.conf*. If that is also not found, then the server will use hardcoded defaults.

-l log-path
: Specifies the directory where the server will create its log files. If this parameter is not specified, then *(LOGDIR)*.

-s label
: Specifies the logging label that is going to be used to identify this instance of the server. For the M-Link Server, it must start with `xmppd`, for e.g. *xmppd-01*. If this parameter is not specified, then the default service name `xmppd` is used. Similarly for M-Link Archive Server, it must start with `wabacd` which is also the default.

Example use is shown below:

Unix

```
# /opt/isode/sbin/isode.wabacd -d -c /etc/isode/mlink.conf
  -l /var/isode/log
# /opt/isode/sbin/isode.xmppd -d -c /etc/isode/mlink.conf
  -l /var/isode/log
```

Windows

```
C:\>"C:\Program Files\Isode\bin\isode.wabacd.exe" -d
 -c C:\Isode\etc\mlink.conf -l C:\Isode\log
C:\>"C:\Program Files\Isode\bin\isode.xmppd.exe" -d
 -c C:\Isode\etc\mlink.conf -l C:\Isode\log
```

As each of these commands will run until it is interrupted, each must be run in a different command shell.

A.3 Reload configuration

This can be done to load the configuration on a node (say if the configuration files are hand-edited) or reload the groups on the node from the directory. If the *service* configuration file on the node has changed, the reload will trigger the configuration to be passed on to all the nodes of the cluster.

Example use is shown below:

Unix

```
# /etc/init.d/mlink reload
```

Windows

```
C:\>"C:\Program Files\Isode\bin\mlink.exe" reload
```

A.4 mlinkadm utility

The **mlinkadm** utility is used for certain administrative tasks like resetting the passphrase of the server or creating or updating the server. The various tasks will be described in later sections.

The set of command line parameters used when starting **mlinkadm** are described below.

-c configuration-file
: Refer to Section A.2, “Start the server (debug mode)”.

-l log-path
: Refer to Section A.2, “Start the server (debug mode)”.

-v
: Report version of software.

-s
: Use secure mode in the **mlinkadm** prompt which does not store the history of commands. This is especially useful if passwords are set. The secure mode has no effect on Windows.

Examples of **mlinkadm** below.

Unix

```
# /opt/isode/sbin/mlinkadm -s
mlinkadm:>
```

Windows

```
 C:\>"C:\Program Files\Isode\bin\mlinkadm.exe"
mlinkadm:>
```

A.5 Reset server passphrase

Passwords in the configuration files are stored in an encrypted form. A server passphrase is required by the mechanism used to encrypt these. You will be required to choose this server passphrase when you create the first node of the cluster. When creating any subsequent nodes, you will need to provide the same passphrase as the passwords encrypted on one node will need to be decrypted on another. The passphrase can be reset if desired, but it will have to be done on all nodes. This will usually be required when a new node is being added and you have forgotten the original server passphrase.

The passphrase must contain at least 16 characters and have characters from at least three of the following groups:

- Uppercase letters
- Lowercase letters
- Digits
- Everything else

Start the **mlinkadm** utility as described in Section A.4, “mlinkadm utility”.

The set of command line parameters used on the **mlinkadm** prompt when resetting the passphrase are described below.

-c configuration-file
: Refer to Section A.2, “Start the server (debug mode)”.

-p passphrase
: Passphrase to use for encrypting passwords (must be the same on all cluster nodes).

The M-Link Server on the node needs to be stopped before resetting the passphrase.

Example use is shown below:

Unix

```
# Stop-the-server
# /opt/isode/sbin/mlinkadm -s
mlinkadm:> configure -c /etc/isode/mlink.conf
           -p Secret0123456789
1:configure succeeded
mlinkadm:> quit
# Start-the-server
```

Windows

```
# Stop-the-server
 :\>"C:\Program Files\Isode\bin\mlinkadm.exe"
mlinkadm:> configure -c C:\Isode\etc\mlink.conf
           -p Secret0123456789
1:configure succeeded
mlinkadm:> quit
# Start-the-server
```

A.6 Create or update server configuration

M-Link stores its configuration in files *(ETCDIR)/mlink.conf* and *(ETCDIR)/mlink.conf.node*. This section describes the commands to create simple configuration files or make simple updates to them. For advanced configuration, Ad-Hoc Commands commands described in Section 1.1.6, “Management through Ad-Hoc Commands” need to be used.

Start the **mlinkadm** utility as described in Section A.4, “mlinkadm utility”.

The set of command line parameters used on the **mlinkadm** prompt are described below.

-c configuration-file
: Specifies the path and name of the service configuration file. If this parameter is not specified, then the service configuration file is assumed to be *(ETCDIR)/mlink.conf* and the corresponding node configuration file *(ETCDIR)/mlink.conf.node*.

-p passphrase
: Passphrase to use for encrypting passwords as described in Section A.5, “Reset server passphrase”.

-w
: This is specified to create a new configuration. It ignores and overwrites any existing configuration files of the same name and generates new ones from scratch. If this is not specified, then any existing configuration files of the same name will be read first and then updated, and configuration options that were not updated will remain.

-r
: This should be used if the configuration is being generated for a remote system.

-m name=value
: The `name` can be the `Config file XML Option` value of any configuration option in Section H.1, “Global Options”. The `value` is the value to be assigned to this configuration option. These configuration options are for the service configuration file.

-n name=value
: The `name` can be the `Config file XML Option` value of any configuration option in Section H.1, “Global Options”. The `value` is the value to be assigned to this configuration option. These configuration options are for the node configuration file.

-o server-admin
: The JID of the initial server administrator. If the configuration option Section H.1.50, “Server Administrators” is supplied using '-m' above, then a local group of the name corresponding to the option value will be created in the primary IM domain. The JID indicated here will be set as the member of that group.

-b backend
: This specifies the primary Instant Messaging domain's authentication backend. The possible values are anonymous, xmldb, ldap, authp.

-a name=value
: The `name` can be the `Config file XML Option` value of any primary Instant Messaging domain authentication option. The `value` is the value to be assigned to this configuration option. These configuration options are for the service configuration file. Plese contact support@isode.com for details of these options.

A.6.1 Local configuration

Example use to create the configuration if the M-Link Server is on the local system is shown below. This will also do other initialization required for the M-Link Server on the local system.

On Unix, please ensure that you execute the command as 'root' or Section H.1.16, “Runtime User ID”. The user running the command should have the correct ownership and permissions of the *(ETCDIR)/servpass* folder if it exists and if not, then the user should have the correct permissions to create it.

Windows

```
 C:\>"C:\Program Files\Isode\bin\mlinkadm.exe"
mlinkadm:> configure -w -p "Secret0123456789"
 -o "john.doe@example.net"
 -m "server_admins=example.net/group;local;name:admins"
 -m "domain=example.net"
```

```
 -b ldap
 -a "password=secret"
 -a "authcid=cn=M-Link server,cn=Users,o=example"
 -a "user_base=cn=Users,o=example"
 -a "uri=ldap://ldap.example.net:29389"
 -n "service_group=isode.mlink"
 -a "group_base=cn=Groups,o=example"
1:configure succeeded
mlinkadm:> quit
```

A.6.2 Remote configuration

Example use to create the configuration for a remote system is shown below.

Windows

```
 C:\>"C:\Program Files\Isode\bin\mlinkadm.exe"
mlinkadm:> configure -r -w -p "Secret0123456789"
 -o "john.doe@example.net"
 -m "server_admins=example.net/group;local;name:admins"
 -c C:\mlink.conf
 -m "domain=example.net"
 -b ldap
 -a "password=secret"
 -a "authcid=cn=M-Link server,cn=Users,o=example"
 -a "user_base=cn=Users,o=example"
 -a "uri=ldap://ldap.example.net:29389"
 -n "service_group=isode.mlink"
 -a "group_base=cn=Groups,o=example"
1:configure succeeded
mlinkadm:> quit
```

Before copying the above files to the remote system, some initialization needs to be done on the remote system. An example on how to do this on the remote system is shown below. The passphrase specified in this command should be the same as that specified when creating the configuration above.

On Unix, please ensure that you execute the command as 'root' or Section H.1.16, “Runtime User ID”. The user running the command should have the correct ownership and permissions of the *(ETCDIR)/servpass* folder if it exists and if not, then the user should have the correct permissions to create it.

Windows

```
 C:\>"C:\Program Files\Isode\bin\mlinkadm.exe"
mlinkadm:> configure -w -p "Secret0123456789"
1:configure succeeded
mlinkadm:> quit
```

The configuration files generated before can now be copied over to the *(ETCDIR)* folder of the remote system.

A.6.3 Resulting configuration

The above example will produce configuration files similar to below:

(ETCDIR)/mlink.conf

```
<ms_options xmlns:servpass='http://www.isode.com/servpass'
  updater='xmppd'>
 <servpass:info service='xmppd' verifier='AbeFP'/>
 <domain>example.net</domain>
 <server_admins>example.net/group;local;name:admins</server_admins>
 <multidomain>
  <domain name='example.net'>
   <auth>
    <ldap>
     <uri>ldap://ldap.example.net:29389</uri>
     <authcid>cn=M-Link server,cn=Users,o=example</authcid>
     <password servpass:encrypt='true'>{spcrypt2}xxx</password>
     <user_base>cn=Users,o=example</user_base>
     <group_base>cn=Groups,o=example</group_base>
    </ldap>
    <local_groups>
     <group name='admins'>
      <member id='john.doe@example.net'/>
     </group>
    </local_groups>
   </auth>
  </domain>
 </multidomain>
 <peering>
 </peering>
</ms_options>
```

(ETCDIR)/mlink.conf.node

```
<ms_options xmlns:servpass='http://www.isode.com/servpass'
  updater='xmppd'>
 <servpass:info service='xmppd' verifier='AbeFP'/>
 <service_group>isode.mlink</service_group>
 <peering>
 </peering>
</ms_options>
```

It is advised that you use M-Link Console to create a test M-Link Server with the features you require and use the options in generated configuration files to construct the correct command line arguments.

A.7 Import and export of user data

This can be used to export user data from the M-Link Server or import user data into the M-Link Server according to XEP-0227.

Example use is shown below:

Unix
: Help

```
# /opt/isode/sbin/xep227 -h
Usage: /opt/isode/sbin/xep227 -v | -h | [-qndea] [-c config]
```

```
  [-l log path] filename

-v : version - display version message, and exit.
-h : help    - display this message, and exit.

-q : quit    - at first error.
-n : dry run - do not write anything.
-d : debug   - produce verbose messages.
-c : config  - select alternate config file.
-l : log path  - select alternate log file.
-e : export  - exports users.
-a : all  - exports all users even ones already exported.
```

Export to directory /tmp/export-2015-03-14

```
# /opt/isode/sbin/xep227 -e /tmp/export-2015-03-14
Finding users
Exporting users

Exporting domains

Number of users exported: 300
```

Import the data exported above

```
# /opt/isode/sbin/xep227 /tmp/export-2015-03-14/xep227.xml

Number of users imported: 300
```

Windows

Export shown here, the rest are similar to Unix examples

```
C:\>"C:\Program Files\Isode\bin\xep227.exe" -e C:\export
Finding users
Exporting users

Exporting domains

Number of users exported: 300
```

A.8 M-Link Console Archive commands

M-Link Console provides a command-line interface with which you can perform certain operations on the Archive Server for an M-Link Service. The four available commands are:

- export - exports the data from the Archive server to a file in XML or PDF/A format
- expire - removes data from the Archive server database prior to a specified date

- backup - creates a backup of the Archive SQLite3 database in a database format
- import - imports an XML file that was previously exported from a Archive server
- importFolder - converts and imports a set of XML archive data (see Chapter 15, *Archive Management*)

Commands for Archive operations are structured as follows:

Unix:

```
% (BINDIR)/mlc (MANDATORY_PARAMETERS) (COMMAND) (COMMAND_PARAMETERS)
```

Windows (note: a default path for the Java 8 JRE is assumed in this example):

```
C:\> cd $bindir;
C:\Program Files\Isode\bin>"C:\Program Files\Java\jre8\bin\java.exe"
-jar java\classes\isode-mlc.jar (MANDATORY_PARAMETERS)
(COMMAND) (COMMAND_PARAMETERS)
```

Every Archive command requires two common, mandatory parameters; a user JID and corresponding password. These parameters are defined below:

-u / --user JID
: The JID of a user with the required privileges to perform the Archive command.

-p / --pwd password
: The password corresponding to the specified JID.

In addition to operation specific optional parameters, there are several optional parameters that are applicable to all Archive commands:

-s / --silent
: Run the command in silent mode. This will disable any output logged to the command line.

-h / --host
: The HTTP hostname to use for the command.

-port / --port
: The HTTP port number to use for the command.

-tls / --tls
: Specifies TLS encryption, using the HTTPS protocol.

-cf / --certfile
: Specifies a certificate file that contains one or more pinned certificates in PEM format to use for verifying server certificate.

-tf / --tafile
: tafile Specifies one or more trust anchors (root CA certificates) in PEM format to use for verifying server certificate.

A.8.1 Import parameters

The Archive import command can be used to import data into the Archive database from a Archive XML file-based format.

-if / --impfn
: [mandatory] The input file to use. This should be an XML file containing valid Archive archive data.

An example of an import command is included below:

Unix:

```
% $(BINDIR)/mlc import -u admin@wonderland.lit -p secret
-if archive.xml
```

Windows:

```
C:\>cd (BINDIR)
C:\Program Files\Isode\bin>"C:\Program Files\Java\jre8\bin\java.exe"
-jar java\classes\isode-mlc.jar import -u admin@wonderland.lit
-p secret -if archive.xml
```

A.8.2 Import folder parameters

The Archive import archive command is used to import file-based XML archives, as described in Chapter 15, *Archive Management*.

-id / --impdn
: [mandatory] The input directory to use. This should be the path of a directory tree containing XML file-based archives.

An example of an import folder command is included below:

Unix:

```
% $(BINDIR)/mlc importFolder -u admin@wonderland.lit -p secret
-id archive_folder
```

Windows:

```
C:\>cd (BINDIR)
C:\Program Files\Isode\bin>"C:\Program Files\Java\jre8\bin\java.exe"
-jar java\classes\isode-mlc.jar importFolder
-u admin@wonderland.lit -p secret -id archive_folder
```

A.8.3 Export parameters

The Archive export command can be used to export archive data to XML or PDF/A file format.

-dom / --domain
: The domain to which this operation applies

-sdate / --startdate
: The date-time after which all archive data will be exported. This should be in the form dd/MM/yyyy'T'HH:mm:ss, e.g. 03/09/2014T12:35:00

-edate / --enddate
: The date-time before which all archive data will be exported. This should be in the form dd/MM/yyyy'T'HH:mm:ss, e.g. 03/09/2014T12:35:00

-xml / --isXML
: Specifies the file type to export, either XML or PDF/A.

-ef / --expfn
: [mandatory] The path and name for the output file, e.g. /home/user/output.xml. The path prefix should be a valid directory on the file system.

An example of an export command is included below:

Unix:

```
% $(BINDIR)/mlc export -u admin@wonderland.lit -p secret
-ef archive.pdf
```

Windows:

```
C:\>cd (BINDIR)
C:\Program Files\Isode\bin>"C:\Program Files\Java\jre8\bin\java.exe"
-jar java\classes\isode-mlc.jar export -u admin@wonderland.lit
-p secret -ef archive.pdf
```

A.8.4 Expire parameters

The expire command is used to remove data before a specified date-time. Note that this operation can not be reversed.

-dom / --domain
: The domain to which this operation applies

-exdate / --expdate
: [mandatory] The expiry date before which all messages will be removed. This should be in the form dd/MM/yyyy'T'HH:mm:ss, e.g. 03/09/2014T12:35:00

An example of the expire command is included below:

Unix:

```
% $(BINDIR)/mlc expire -u admin@wonderland.lit -p secret
-exdate 03/09/2014T12:35:00
```

Windows:

```
C:\>cd (BINDIR)
C:\Program Files\Isode\bin>"C:\Program Files\Java\jre8\bin\java.exe"
-jar java\classes\isode-mlc.jar expire -u admin@wonderland.lit
-p secret -exdate 03/09/2014T12:35:00
```

A.8.5 Backup parameters

The Archive backup command can be used to create a backup of the Archive SQLite3 database, as a database file (.db). There are no optional parameters for the backup command, except the standard optional parameters defined in Section A.8, “M-Link Console Archive commands”.

Running a Archive backup operation will construct a copy of the database with the current time-stamp as the file name, and place this into the *backups* directory within the path specified by Section H.1.137, “Archive Database Directory”.

An example of a backup command is included below:

Unix:

```
% $(BINDIR)/mlc backup -u admin@wonderland.lit -p secret
```

Windows:

```
C:\>cd (BINDIR)
C:\Program Files\Isode\bin>"C:\Program Files\Java\jre8\bin\java.exe"
-jar java\classes\isode-mlc.jar backup -u admin@wonderland.lit
-p secret
```

Appendix B Backing up M-Link

This appendix explains how to take a backup of the M-Link system and restore it with the backup.

B.1 Backup

Before taking the backup, create the the M-Link Archive Server backup as described in Section 15.7.2.3, “Archive Backup”. This will create *YYYY-MM-DD-HH-MM-SS.db*.

Taking a backup of the M-Link system data means backing up the following directories:

- *(ETCDIR)*
- *(MSDIR)*
- Directory specified by Section H.1.1, “Users Root Directory” if not part of *(MSDIR)*
- Directory specified by Section H.1.137, “Archive Database Directory” if not part of *(MSDIR)*
- Directory specified by Section H.1.138, “Archive Queue Directory” if not part of *(MSDIR)*
- Directory specified by Section H.1.111, “Queues Statistics Directory” if not part of *(MSDIR)*
- Directory specified by Section H.1.112, “Publish-Subcribe Directory” if not part of *(MSDIR)*
- *(LOGDIR)* or the non-default log-path as specified in Section A.2, “Start the server (debug mode)”

B.2 Restore

Stop the M-Link Server and the M-Link Archive Server before restoring it from a backup.

Restore the backed up copies of the above directories to their original locations.

In the path specified by Section H.1.137, “Archive Database Directory”, delete *archive.db*, *archive.db-shm* and *archive.db-wal*. Rename the backup of the Archive Server *YYYY-MM-DD-HH-MM-SS.db* to *archive.db* in the path specified by Section H.1.137, “Archive Database Directory”.

Start the M-Link Server and the M-Link Archive Server.

Appendix C Message Archive Format

This chapter provides an example of the format of an import or export of the message archive.

XML Comments are included in the below example as documentation of the format. These are not generated by M-Link during export and will be ignored during import. An ellipsis (...) is sometimes used to elide uninteresting content of stanzas.

```
<!-- v1.1 -->
<archives xmlns="http://isode.com/xmpp/archiving" name="example"
          start="2013-07-21T02:58:15.000Z"
          end="2014-07-21T02:58:15.000Z">
  <!-- Archives might also have a domain attribute if this file was
       generated as an export operation for a single domain -->
  <users>
    <user jid="localuser1@example.com">
      <!-- all archived stanzas in order, one per item element -->
      <item uid="a" timestamp="2014-07-21T02:56:15.000Z"
            order="0">
        <!-- The stanza is embedded here unmodified other than
             injecting the correct namespace -->
        <message to="localuser1@example.com/etuhet"
                 from="remoteuser1@example.org" type="normal"
                 id="maybe" xmlns="jabber:client" lang="en">
          <!-- stanza payloads remain here-->
          <body>Hi Kev</body>
          <xhtml-im xmlns="..."><b>
            Hi user
          </b></xhtml-im>
        </message>
      </item>

      <item uid="b" timestamp="2014-07-21T02:58:15.000Z">
        <message from="localuser1@example.com/etuhet"
                 to="remoteuser1@example.org" type="normal"
                 id="maybe2" xmlns="jabber:client">
          <body>Hi back</body>
        </message>
      </item>
    </user>
  </users>
  <pubsub>
    <!-- Publish-Subscribe history is split per service (including
         PEP services) and per node -->
    <service jid="localuser1@example.com">
      <node node="http://jabber.org/protocol/geoloc">
        <!-- Node creations are logged with the user responsible
             and timestamp -->
        <item publisher="localuser1@example.com/bou.adg2d98213"
              timestamp="1979-07-21T02:55:15.000Z" uid="b"
              order="0">
          <create></create>
        </item>

        <!-- Item publication wraps the payload in an
             <item><publish>... format -->
        <item publisher="localuser1@example.com/bou.adg2d98213"
              id="uteutudaos"
              timestamp="1979-07-21T02:56:15.000Z"
              uid="c" order="0">
          <publish>
            <!--payload here-->
            <geoloc
```

```
              xmlns='http://jabber.org/protocol/geoloc'
              xml:lang='en'>
            <accuracy>20</accuracy>
            <country>Italy</country>
            <lat>45.44</lat>
            <locality>Venice</locality>
            <lon>12.33</lon>
          </geoloc>
        </publish>
      </item>

      <!-- Node deletions are logged with the user responsible
           and timestamp -->
      <item publisher="localuser1@example.com/bou.adg2d98213"
            timestamp="1979-07-21T02:57:15.000Z" uid="d"
            order="0">
        <destroy></destroy>
      </item>
    </node>
  </service>
  <service jid="pubsub.isode.com">
    <!-- Where an item is published and replaced by another with
         the same pubsub id, both publishes are archived -->
    <node node="notes/for/user2">
      <item publisher="localuser2@example.com/etuhoe"
            id="euth.tu" timestamp="1979-07-21T02:56:15.000Z">
        <publish>
          <note>this is note 1</note>
        </publish>
      </item>

      <item publisher="localuser3@example.com/Psi" uid="e"
            id="euth.tu" timestamp="1989-07-21T02:57:15.000Z">
        <publish>
          <note>this is note 2</note>
        </publish>
      </item>
    </node>
  </service>
</pubsub>
<mucs>
  <!-- MUC history is stored sequentially per room -->
  <room jid="room1@talk.example.com">
    <item uid="f" publisher="localuser1@example.com/etuhet"
          timestamp="2014-07-21T02:56:15.000Z" order="0"
          nick="User 1">
      <message from="localuser1@example.com/etuhet"
               to="room1@talk.example.com" type="groupchat"
               id="maybe" xmlns="jabber:client">
        <!-- payloads here-->
        <body>Hi Everyone</body>
      </message>
    </item>

    <item uid="g" publisher="localuser1@example.com/etuhet"
          timestamp="2014-07-21T02:56:15.000Z" nick="User 1">
      <presence></presence>
    </item>

    <item uid="h" publisher="localuser5@example.com/oued"
          timestamp="2014-07-21T02:56:16.000Z" nick="User5">
      <subject>Changing the subject</subject>
    </item>

    <item uid="i" publisher="localuser5@example.com/oued"
          timestamp="2014-07-21T02:56:17.000Z" nick="User5" >
```

```
        <nick>Old Nick</nick>
      </item>

      <item uid="j" publisher="localuser5@example.com/oued"
            timestamp="2014-07-21T02:56:16.000Z" nick="User5">
        <!-- the new config is stored when it changes -->
        <config>...</config>
      </item>

      <item uid="k" publisher="localuser5@example.com/oued"
            timestamp="2014-07-21T02:56:16.000Z" nick="User5">
        <kicked>Go away</kicked>
      </item>

      <item uid="l" publisher="localuser5@example.com/oued"
            timestamp="2014-07-21T02:56:16.000Z" nick="User5">
        <leave>I'm going home</leave>
      </item>

      <item uid="m" publisher="localuser5@example.com/oued"
            timestamp="2014-07-21T02:56:16.000Z" nick="User5">
        <join>status</join>
      </item>

      <item uid="n" publisher="localuser5@example.com/oued"
            timestamp="2014-07-21T02:56:16.000Z" nick="User5">
        <destroy>reason</destroy>
      </item>

      <item uid="o" publisher="localuser5@example.com/oued"
            timestamp="2014-07-21T02:56:16.000Z" nick="User5">
        <create>reason</create>
      </item>
    </room>
  </mucs>
</archives>
```

Appendix D Customizing Archive PDF/A Files

This appendix discusses customization of the Archive PDF/A files.

Archive PDF/A files generated using M-Link Console for exporting archives can be customized using the property files. Sample property files are installed in *(SHAREDIR)*. Local copies in *(ETCDIR)* can override the files in *(SHAREDIR)*.

D.1 Property Files

M-Link Console generates PDF/A files for three different purposes. Each PDF/A file can be customised using a corresponding property file.

- The file *search.props* in *(ETCDIR)* can be used to customise PDF/A files generated from Archive search results (see Section 15.7.2.1, “Searching the Archives”).
- The file *stats.props* in *(ETCDIR)* can can be used to customise PDF/A files generated from the statistics graphs (see Section 17.3.2, “Viewing Live Statistics”)
- The file *export.props* in *(ETCDIR)* can be used to customise PDF/A files generated from exported archive data see(Section 15.7.2.5, “Exporting Data”)

D.2 Customisation

D.2.1 Metadata

The PDF metadata is used to provide additional information about the PDF file. This data can be modified using the properties for the keys starting with *META_* in the corresponding property file. The properties allow you to provide the title, author, subject and keywords metadata for the PDF.

As an example the following line in the property file sets the title metadata to “XMPP Archives.”

```
META_TITLE=XMPP Archives
```

D.2.2 Cover Page

It is also possible to customise the cover page and security label on the header and footer of pages on the export and search query PDFs. Note that this customisation is not supported for the statistics graph PDF.

In order to modify the image logo on the cover page, provide the absolute path of the image file for the *IMAGE_LOGO* key using the format as specified in the example below.

Unix example:

```
IMAGE_LOGO=file:///home/user/logo.svg
```

Windows example:

```
IMAGE_LOGO=file:///C:/Isode/etc/image/logo.svg
```

The value of the *TITLE* key provides the title on the cover page.

The label that appears on the header and footer is derived from the value of the *LABEL* key. This should be left blank if no label is to be displayed on the PDF.

The cover page displays a table that lists information about the archive. If required, more rows can be added to this table using the property file. All properties starting with *TABLE_* will appear as additional rows on the cover page table.

The following is a sample property to add a row with columns “Point Of Contact” as “Henry Brown” to the table.

```
TABLE_Point Of Contact=Henry Brown
```

Appendix E Administrator Archive Access Protocol

This chapter provides the protocol for administrator access to message archives.

The administrator access is an HTTP based protocol using JavaScript Object Notation (JSON)

E.1 Request

```
{
    "type": "jsonwsp/request",
    "version": "1.0",
    "methodname": <method-name>,
    "args": { ( <key>: <value>, )* }
}
```

E.2 Response

```
{
    "type": "jsonwsp/response",
    "version": "1.0",
    "methodname": <method-name>,
    "result": <value>
}
```

E.3 Fault

```
{
    "type": "jsonwsp/fault",
    "version": "1.0",
    "fault": {
        "methodname": <method-name>,
        "code": <fault-code>,
        "string": <fault-string>
    }
}
```

E.4 Description

```
{
    "type": "jsonwsp/description",
    "version": "1.0",
    "types": {
        "message": {
            "uid": "string",
            "to": "string",
            "from": "string",
            "timestamp": "number"(,
            "id": "string")?(,
            "node": "string")?(,
            "item_id": "string")?(,
            "stanza_type": "string")?(,
            "payload": "string")?
        },
        "response": {
            "success": "boolean"
        }
        "port_state": {
            "uploaded": "boolean",
            "downloaded": "boolean",
            "imported": "boolean",
            "exported": "boolean",
            "valid": "boolean",
            "invalid": "boolean"
        },
        "port": {
            "url": "string",
            ("name": "string",)?
            ("domain": "string",)?
            "start": "number",
            "end": "number",
            "recCnt": "number",
            "state": "port_state"
        },
        "op_history": {
            "operation": ( "backup" | "import" | "export" |
                           "upload" | "delete" | "download" |
                           "unknown" ),
            "successful": "boolean",
            "run_time": "float"(,
            ("name": "string")?
        },
        "active_op": {
            "methodname": ( "export" | "import" | "backup" |
                            "none" ),
            "percentCompleted": "number"
        },
        "list_response": {
            "files": [ "port" ],
            "operation_history": [ "op_history" ](,
            ("activeOperation": "active_op")?
        }
    },
    "methods": {
        "query": {
            "doc_lines": ["Query an archive to find messages which
```

```
                    match a given filter"],
            "params": {
                "archive": {
                    "doc_lines": ["JID of archive to query"],
                    "type": "string",
                    "optional": false
                },
                "with": {
                    "doc_lines": ["Matching JID"],
                    "type": "string",
                    "optional": true
                },
                "start": {
                    "doc_lines": ["Start timestamp"],
                    "type": "number",
                    "optional": true
                },
                "end": {
                    "doc_lines": ["End timestamp"],
                    "type": "number",
                    "optional": true
                },
                "text": {
                    "doc_lines": ["Text string to match the body
                                   on"],
                    "type": "string",
                    "optional": true
                },
                "before": {
                    "doc_lines": ["Return messages sent before this
                                   UID, or from the end of the
                                   archive in case of null"],
                    "type": ["string", "null"],
                    "optional": true
                },
                "after": {
                    "doc_lines": ["Return messages sent after this
                                   UID"],
                    "type": "string",
                    "optional": true
                },
                "max": {
                    "doc_lines": ["Maximum number of messages to
                                   return"],
                    "type": "number",
                    "optional": true
                },
                "count": {
                    "doc_lines": ["Return the number of messages
                                   instead of the messages
                                   themselves"],
                    "type": "boolean",
                    "optional": true
                },
                "node": {
                    "doc_lines": ["PubSub node to query"],
                    "type": "string",
                    "optional": true
                }
                "real_jids": {
                    "doc_lines": ["Determines wether to return
                                   real jids or occupant jids
                                   in results for MUC rooms"],
                    "type": "boolean",
                    "optional": true
                }
```

```
            },
            "ret_info": {
                "doc_lines": ["List of messages, or number of
                               messages if count is requested"],
                "type": ( "number" | [ ( "message" )* ] )
            }
        },
        "expire": {
            "doc_lines": ["Expire messages sent before the
                           specified end timestamp"],
            "params": {
                "end": {
                    "doc_lines": ["End timestamp"],
                    "type": "number",
                    "optional": true
                }
                "domain": {
                    "doc_lines": ["If specified, only expire data
                                   from jids in this domain"],
                    "type": "string",
                    "optional": false
                },
            },
            "ret_info": {
                "doc_lines": ["Result of the expire"],
                "type": ["response"]
            }
        },
        "redact": {
            "doc_lines": ["Redact a message in the archives"],
            "params": {
                "uid": {
                    "doc_lines": ["Unique ID of the message"],
                    "type": "string",
                    "optional": false
                },
            },
            "ret_info": {
                "doc_lines": ["Result of the redact"],
                "type": ["response"]
            }
        }
        "export": {
            "doc_lines": ["Export archive to an XML file"],
            "params": {
                "name": {
                    "doc_lines": ["Resource of data to export"],
                    "type": "string",
                    "optional": false
                },
                "start": {
                    "doc_lines": ["Start timestamp"],
                    "type": "number",
                    "optional": true
                },
                "end": {
                    "doc_lines": ["End timestamp"],
                    "type": "number",
                    "optional": true
                }
                "domain": {
                    "doc_lines": ["If specified, only export data
                                   associated with this domain"],
                    "type": "string",
                    "optional": false
                },
```

```
            },
            "ret_info": {
                "doc_lines": ["Result of the export"],
                "type": ["response"]
            }
        }
        "import": {
            "doc_lines": ["Import data from an XML file into the
                           archive"],
            "params": {
                "name": {
                    "doc_lines": ["Resource of data to import"],
                    "type": "string",
                    "optional": false
                },
            },
            "ret_info": {
                "doc_lines": ["Result of the import"],
                "type": ["response"]
            }
        }
        "list": {
            "doc_lines": ["List of import / export files"],
            "ret_info": {
                "doc_lines": ["List of files"],
                "type": ["list_response"]
            }
        }
        "backup": {
            "doc_lines": ["Backup of archive"],
            "ret_info": {
                "doc_lines": ["Result of the backup"],
                "type": ["response"]
            }
        }
    }
}
```

Appendix F Advanced Configuration

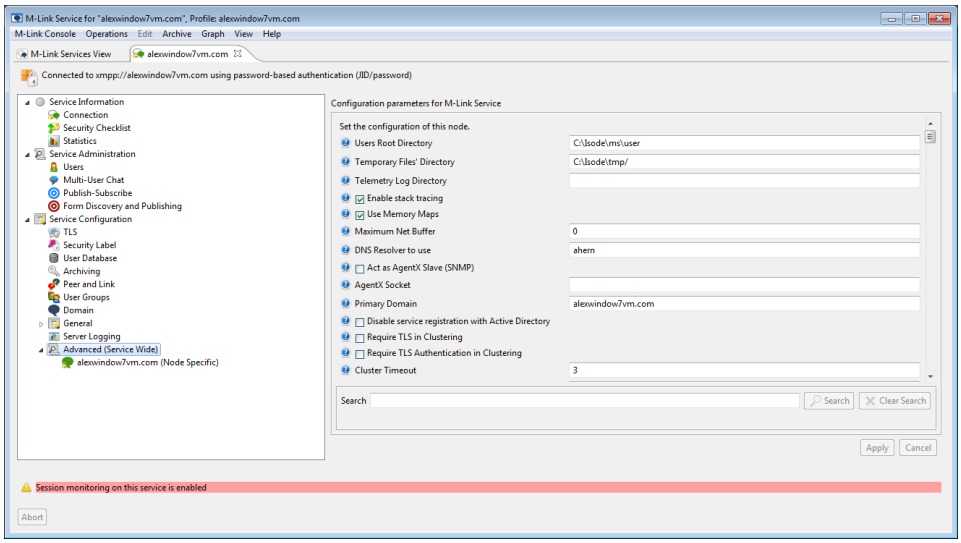
This appendix explains how to do advanced configuration.

F.1 Advanced Configuration using MLC

M-Link Console attempts to provide a reasonably friendly interface to allow you to access the most common configuration options, and separates service and node options to reduce the chance of misconfiguration. However, there may be cases where you want to view or modify a parameter which is not catered in the standard views, or where you want to set a parameter at the node or service level regardless of whether M-Link Console thinks that this is a good idea.

The XMPP Service view contains an *Advanced* item, which provides a way to read and/or modify any of the values that the M-Link Server exposes using its Ad-Hoc Commands Section G.24, “Set Server Configuration (Shared)” for service and Section G.25, “Set Server Configuration (Node)” and for node configuration respectively. For example, within the *General Configuration (Node specific)* editor, you can update node-specific configuration for any parameter, including those which M-Link Console would normally restrict to only being visible in an editor for the cluster-wide service.

Figure F.1. Advanced General Configuration



Note that the configuration options which appear under the *Advanced* item comprise a superset of the ad-Hoc based configuration which M-Link Console presents elsewhere. For example, all of the configuration available in the *XMPP Log Configuration* editor could be modified by changing the appropriate values in the *General Configuration (Node Specific)* editor (although without any of the checking that M-Link Console might otherwise be carrying out on the validity of any changes you make).

Appendix G Ad-Hoc Command Reference

This appendix lists the Ad-Hoc Commands offered by the M-Link Server.

G.1 Send announcement

Description:
Enter the message below to send to all online users.

Ad-Hoc Command:
http://jabber.org/protocol/admin#announce

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.2 End user session

Description:
Enter the Jabber ID(s) to be disconnected.

Ad-Hoc Command:
http://jabber.org/protocol/admin#end-user-session

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
yes

Available to users:
no

G.3 Get number of online sessions

Description:
-None-

Ad-Hoc Command:
http://jabber.org/protocol/admin#get-online-users-num

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.4 Get a list of online sessions

Description:
Enter the max number of users to be listed

Ad-Hoc Command:
http://jabber.org/protocol/admin#get-online-users-list

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.5 Get User Statistics

Description:
Fill out this form to gather user statistics.

Ad-Hoc Command:
http://jabber.org/protocol/admin#user-stats

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
yes

Available to users:
no

G.6 Get information about a server

Description:
-None-

Ad-Hoc Command:
http://isode.com/protocol/admin#server-info

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.7 Get a list of S2S sessions

Description:
Enter the max number of sessions to be listed

Ad-Hoc Command:
http://isode.com/protocol/admin#get-s2s-list

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.8 Get Domain S2S Statistics

Description:
Fill out this form to gather domain S2S statistics.

Ad-Hoc Command:
http://isode.com/protocol/admin#domain-stats

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.9 Get information about a cluster

Description:
-None-

Ad-Hoc Command:
http://isode.com/protocol/admin#cluster-info

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.10 Dump the router table to disk

Description:
The file xmpp_state.txt containing the router dump of the node will be created in the 'Queues Statistics Directory' if it exists. If a file already exists, it will be overwritten. This feature is used for debugging only.

Ad-Hoc Command:
http://isode.com/protocol/admin#router-table-dump

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.11 Get work-queue statistics

Description:
-None-

Ad-Hoc Command:
http://isode.com/protocol/admin#workqueue-stats

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.12 Get performance statistics

Description:
-None-

Ad-Hoc Command:
http://isode.com/protocol/admin#performance-stats

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.13 Get memory usage statistics

Description:
-None-

Ad-Hoc Command:
http://isode.com/protocol/admin#memusage-stats

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.14 Reset a user's roster

Description:
Fill out this form to reset a user's roster

Ad-Hoc Command:
http://isode.com/protocol/admin#roster-reset

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.15 No-Op

Description:
-None-

Ad-Hoc Command:
http://isode.com/xmpp/commands#test

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.16 User Configuration

Description:
Complete the form below to configure personal preferences.

Ad-Hoc Command:
http://isode.com/xmpp/commands#user_config

Applicable to user account:
yes

Available to Server Admins:
no

Available to IM Domain Admins:
no

Available to users:
yes

G.17 List blocked users

Description:
Lists all users that're being blocked.

Ad-Hoc Command:
http://isode.com/xmpp/commands#list_blocks

Applicable to user account:
yes

Available to Server Admins:
no

Available to IM Domain Admins:
no

Available to users:
yes

G.18 Block User

Description:
Add a user to your block list.

Ad-Hoc Command:
http://isode.com/xmpp/commands#add_block

Applicable to user account:
yes

Available to Server Admins:
no

Available to IM Domain Admins:
no

Available to users:
yes

G.19 Unblock User

Description:
Remove a user from your block list.

Ad-Hoc Command:
http://isode.com/xmpp/commands#remove_block

Applicable to user account:
yes

Available to Server Admins:
no

Available to IM Domain Admins:
no

Available to users:
yes

G.20 Reload Server Data

Description:
Reload data like configuration file, user groups and TLS context.

Ad-Hoc Command:
http://isode.com/protocol/admin#reload_data

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.21 List Residual Users (Node)

Description:
Traverse the on-disk user data and report an overview of users that no longer exist

Ad-Hoc Command:
http://isode.com/protocol/admin#list_residual_users

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.22 Remove Residual User Data (Node)

Description:
Remove on-disk data belonging to the specified users. Only data that can no longer be correlated to existing users may be removed. A list of residual users can be obtained using the 'List Residual Users' command.

Ad-Hoc Command:
http://isode.com/protocol/admin#remove_residual_user_data

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.23 Scrub User References

Description:
Remove references to a user from PubSub and MUC affiliations, rosters and blocklists

Ad-Hoc Command:
http://isode.com/protocol/admin#scrub_user_references

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.24 Set Server Configuration (Shared)

Description:
Set the configuration of the server shared by all nodes. Note that any of the configuration values may have been overridden on either or all of the nodes.

Ad-Hoc Command:
http://isode.com/xmpp/config#set_config

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.25 Set Server Configuration (Node)

Description:
Set the configuration of this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#set_config_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.26 Set SIO Configuration (Shared)

Description:
Set the Security Information Objects configuration of the server shared by all nodes. Note that any of the configuration values may have been overridden on either or all of the nodes.

Ad-Hoc Command:
http://isode.com/xmpp/config#set_config_sio

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.27 Set SIO Configuration (Node)

Description:
Set the Security Information Objects configuration of this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#set_config_sio_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.28 Set Filter Configuration (Shared)

Description:
Set the filter configuration of the server shared by all nodes. Note that any of the configuration values may have been overridden on either or all of the nodes.

Ad-Hoc Command:
http://isode.com/xmpp/config#set_config_filter

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.29 Set Filter Configuration (Node)

Description:
Set the filter configuration of this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#set_config_filter_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.30 Get Domain Configuration

Description:
Get the configuration of a domain.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_domain

Applicable to IM Domain:
yes

Applicable to MUC Domain:
yes

Applicable to PubSub Domain:
yes

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.31 Add Domain Configuration

Description:
Add the configuration of a domain.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_config_domain

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.32 Modify Domain Configuration

Description:
Modify the configuration of a domain.

Ad-Hoc Command:
http://isode.com/xmpp/config#mod_config_domain

Applicable to IM Domain:
yes

Applicable to MUC Domain:
yes

Applicable to PubSub Domain:
yes

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.33 Delete Domain Configuration

Description:
Delete the configuration of a domain.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_config_domain

Applicable to IM Domain:
yes

Applicable to MUC Domain:
yes

Applicable to PubSub Domain:
yes

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.34 Get Component Configuration

Description:
Get the configuration of a component.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_component

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.35 Add Component Configuration

Description:
Add the configuration of a component.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_config_component

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.36 Modify Component Configuration

Description:
Modify the configuration of a component.

Ad-Hoc Command:
http://isode.com/xmpp/config#mod_config_component

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.37 Delete Component Configuration

Description:
Delete the configuration of a component.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_config_component

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.38 Get Peer Configuration

Description:
Get the configuration of a peer.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_peer

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.39 Add Peer Configuration

Description:
Add the configuration of a peer.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_config_peer

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.40 Modify Peer Configuration

Description:
Modify the configuration of a peer.

Ad-Hoc Command:
http://isode.com/xmpp/config#mod_config_peer

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.41 Delete Peer Configuration

Description:
Delete the configuration of a peer.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_config_peer

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.42 Get Link Configuration

Description:
Get the configuration of a link.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_link

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.43 Add Link Configuration

Description:
Add the configuration of a link.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_config_link

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.44 Modify Link Configuration

Description:
Modify the configuration of a link.

Ad-Hoc Command:
http://isode.com/xmpp/config#mod_config_link

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.45 Delete Link Configuration

Description:
Delete the configuration of a link.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_config_link

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.46 Add Local Group Configuration

Description:
Add the configuration of a local group.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_config_group

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.47 Modify Local Group Configuration

Description:
Modify the configuration of a local group.

Ad-Hoc Command:
http://isode.com/xmpp/config#mod_config_group

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.48 Delete Local Group Configuration

Description:
Delete the configuration of a local group.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_config_group

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.49 Get Cluster List (Node)

Description:
Get the list of cluster nodes configured on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_list_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.50 Add Node to Cluster (Node)

Description:
Add a cluster node to the list configured on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_config_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.51 Delete Node from Cluster (Node)

Description:
Delete a cluster node from the list configured on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_config_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.52 Get Hash (Node)

Description:
Get the hash of the shared config on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_hash_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.53 Get Host (Node)

Description:
Get the host name of this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_host_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.54 Set Logging Settings (Node)

Description:
Set the logging settings of this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#set_config_log_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.55 Get Passphrase Info (Node)

Description:
Get the servpass service and verifier used on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_servpass_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.56 Get Archive Cluster List (Node)

Description:
Get the list of Archive cluster nodes configured on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_config_wabac_list_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.57 Add Archive Node to Cluster (Node)

Description:
Add a Archive cluster node to the list configured on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_config_wabac_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.58 Delete Archive Node from Cluster (Node)

Description:
Delete a Archive cluster node from the list configured on this node.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_config_wabac_node

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.59 Get Roster Groups

Description:
Get the roster groups configured on a domain.

Ad-Hoc Command:
http://isode.com/xmpp/config#get_roster_groups

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.60 Add Roster Group

Description:
Add a roster group to a domain.

Ad-Hoc Command:
http://isode.com/xmpp/config#add_roster_group

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

G.61 Delete Roster Group

Description:
Delete a roster group from a domain.

Ad-Hoc Command:
http://isode.com/xmpp/config#del_roster_group

Applicable to IM Domain:
yes

Applicable to MUC Domain:
no

Applicable to PubSub Domain:
no

Available to Server Admins:
yes

Available to IM Domain Admins:
no

Available to users:
no

Appendix H Configuration Option Reference

This appendix describes each M-Link Server configuration option.

H.1 Global Options

This section describes each global configuration option.

Ad-Hoc Commands:

- See Section G.24, “Set Server Configuration (Shared)”.
- See Section G.25, “Set Server Configuration (Node)”.

The parent XML element in the configuration file is `<ms_options>`.

H.1.1 Users Root Directory

Description:
This specifies the default location for user data. Each user's data will be located in a subdirectory of this directory, named after the user.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that if the directory exists then it has correct ownership and permissions and if it does not exist then the 'Runtime User ID' has the correct permissions to create it.

Syntax:
String (Mandatory)

Default Value:
/var/isode/ms/user

Example:
C:\JabberStore\users\

Config file XML Option:
userdir

Other Info:
Update requires server restart.

H.1.2 User Directory Hash Format

Description:
This specifies the user hash format, which is used in constructing the user's data directory path. The default simply uses a hash of the username, and is suitable for

almost every system. This should not be changed on a running system. Please contact Isode support before changing.

Syntax:
String (Mandatory)

Default Value:
${hash}

Example:
${hash}

Config file XML Option:
user_hash

Other Info:
Update requires server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.3 Temporary Files' Directory

Description:
This directory is used by the system for temporary files, particularly cache files.

Syntax:
String (Mandatory)

Default Value:
/tmp

Example:
C:\Isode\tmp

Config file XML Option:
cache_tmpdir

Other Info:
Update requires server restart.

H.1.4 Runtime Directory

Description:
This specifies the runtime directory for the server on Unix. This is the current directory for a server before it switches to the daemon mode and where it saves the pid file.

All files in this directory are created as the user that starts the daemon so it should be ensured that the directory has correct ownership and permissions.

Syntax:
String (Mandatory)

Default Value:
/var/run

Example:
/var/isode/ms/run

Config file XML Option:
run_dir

Other Info:
Update requires server restart. Unix only option.

H.1.5 Telemetry Log Directory

Description:
This specifies the top level directory for telemetry logging. This directory must exist for telemetry logs to be generated.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that the directory has correct ownership and permissions.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/var/telemetry

Config file XML Option:
telemetry_log

Other Info:
Update does not require server restart.

H.1.6 Automatically create Telemetry user directories

Description:
If set to true, and telemetry_log is set, telemetry directories for entities are automatically created

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
telemetry_auto_create

Other Info:
Update does not require server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.7 Enable stack tracing

Description:
If enabled, when a crash occurs, a file containing the back trace is created in the same directory that logs are generated in. The same file is also used to log the stack trace of the running process using a pre-defined signal.

This option is not supported on Solaris.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
stack_tracing

Other Info:
Update requires server restart.

H.1.8 Minimum Number of Worker Threads

Description:
This option specifies the minimum number of worker threads that will be created for any work queue. This value can not be less than 1.

The exact number of worker threads depends on the number of CPU cores and the value of the 'Maximum Number of Worker Threads' option.

If the number of CPU cores is less than or equal to the value of this option, then the number of threads created will be the value of this option.

If the number of CPU cores is greater than or equal to the value of the 'Maximum Number of Worker Threads', then the number of threads created will be the value of the 'Maximum Number of Worker Threads' option.

Otherwise the number of threads is equal to the number of CPU cores.

Syntax:
Numeric (Mandatory)

Default Value:
1

Example:
4

Config file XML Option:
thread_pool_min

Other Info:
Update requires server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.9 Maximum Number of Worker Threads

Description:
This option specifies the maximum number of worker threads that will be created for any work queue.

See 'Minimum Number of Worker Threads' for details.

Syntax:
Numeric (Mandatory)

Default Value:
8

Example:
16

Config file XML Option:
thread_pool_max

Other Info:
Update requires server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.10 Use Memory Maps

Description:
If set to false, various operations typically using memory-mapped files will instead use simple file reads.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
use_mmap

Other Info:
Update does not require server restart.

H.1.11 Maximum Net Buffer

Description:
If any session has more than this number of bytes outstanding after a write attempt, the session is considered choked and will be dropped to avoid a sizable buffer build-up. Low bandwidth connections using high traffic are particularly likely to fall foul of this, as are the presence of large avatar images on the network. High bandwdith connections can also run afoul of this, especially when traffic is amplified. This option should only be used in cases where the memory use is so large that it hinders proper operation of the service.

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
1073741824

Config file XML Option:
max_net_buffer

Other Info:
Update does not require server restart.

H.1.12 DNS Resolver to use

Description:
This option specifies which DNS Resolver to use, ahern (the default) or c-ares (deprecated).

Syntax:
String (Mandatory)

Default Value:
ahern

Example:
c-ares

Config file XML Option:
resolver

Other Info:
Update requires server restart.

H.1.13 Act as AgentX Slave (SNMP)

Description:
If set, the system connects to an SNMP master agent via AgentX and exports statistical data over SNMP.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
agentx_slave

Other Info:
Update requires server restart.

H.1.14 AgentX Socket

Description:
This can be used to override the standard AgentX socket address.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/var/run/agentx/socket

Config file XML Option:
agentx_socket

Other Info:
Update requires server restart.

H.1.15 Primary Domain

Description:
This specifies the domain name to use if an unqualified userid is received.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
example.com

Config file XML Option:
domain

Other Info:
Update requires server restart. Shared only option.

H.1.16 Runtime User ID

Description:
This specifies the runtime Unix user.

If the server is started as 'root' it will then drop privileges to run as this user. All files in the 'Users Root Directory', 'PubSub Directory', 'Queues Statistics Directory', 'MUC Audit Archive Directory', 'User Audit Archive Directory' and 'Telemetry Log Directory' are created as this user so it should be ensured that the directories have correct ownership and permissions.

Syntax:
String (Mandatory)

Default Value:
mbox

Example:
xmppsrv

Config file XML Option:
ms_user

Other Info:
Update requires server restart. Unix only option.

H.1.17 Process Manager is used

Description:
This specifies if the services are to be managed internally. When managed internally, each process forks a child process that would perform the actual work, while the parent process keeps monitoring the child and will restart the child if it terminates abnormally. Set this to 'false' if the services are to be managed by an external manager such as daemontools or Solaris SMF.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
managed_services

Other Info:
Update requires server restart. Unix only option.

H.1.18 Windows Service Group Name

Description:
This allows multiple copies of the server to run. Typically this is not required.

Syntax:
String (Optional)

Default Value:
isode.mbox-17.0

Example:
isode.mlink-15.2

Config file XML Option:
service_group

Other Info:
Update requires server restart. Windows only option. Advanced option - not available in Ad-Hoc Commands.

H.1.19 Require TLS in Clustering

Description:
If this is set to 'true' then TLS is required over clustering links.

Otherwise TLS will be used optimistically.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
cell_tls

Other Info:
Update requires server restart.

H.1.20 Require TLS Authentication in Clustering

Description:
If this option is set to 'true', then the cluster node will authenticate other cluster nodes by 'self' certificate checks.

This option implicitly requires TLS.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
false

Config file XML Option:
cell_tls_auth

Other Info:
Update requires server restart.

H.1.21 Cluster Timeout

Description:
This specifies how long a M-Link node has to send a heartbeat before it is declared unreachable. The value is in seconds and the minumum value is 1.

Syntax:
Numeric (Mandatory)

Default Value:
6

Example:
10

Config file XML Option:
cluster_timeout

Other Info:
Update does not require server restart.

H.1.22 Dcons Port

Description:
This provides access, via localhost, to a realtime debugging log, accessing via TELNET. Customers will be advised on occasion to use this by Isode support.

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
4000

Config file XML Option:
dcons_port

Other Info:
Update requires server restart.

H.1.23 XMPP S2S Listener Host

Description:
This restricts the system to binding to a specific address for XMPP S2S (server-to-server). If unspecified, the system listens on all addresses.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
127.0.0.1

Config file XML Option:
xmpp_server_host

Other Info:
Update requires server restart. Node only option.

H.1.24 XMPP S2S Listener Port

Description:
This is the port listened to for incoming XMPP S2S sessions.

Syntax:
Numeric (Mandatory)

Default Value:
5269

Example:
15269

Config file XML Option:
xmpp_server_port

Other Info:
Update requires server restart.

H.1.25 XMPP C2S Listener Host

Description:
This restricts the system to binding to a specific address for XMPP C2S (client-to-server). If unspecified, the system listens on all addresses.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
127.0.0.1

Config file XML Option:
xmpp_client_host

Other Info:
Update requires server restart. Node only option.

H.1.26 XMPP C2S Listener Port

Description:
This is the port listened to for XMPP C2S sessions.

Syntax:
Numeric (Mandatory)

Default Value:
5222

Example:
15222

Config file XML Option:
xmpp_client_port

Other Info:
Update requires server restart.

H.1.27 Enable XMPPS (deprecated)

Description:
Enable XMPPS C2S service. This service is deprecated in favor of the C2S service and its standard facility for using TLS in XMPP.

Enabling XMPPS C2S is not generally advised or needed.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
enable_xmpps

Other Info:
Update requires server restart.

H.1.28 XMPPS C2S Listener Host

Description:
This restricts the system to binding to a specific address for XMPPS C2S (client-to-server). If unspecified, the system listens on all addresses.

This option is only relevant when 'XMPPS C2S (deprecated)' has been enabled.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
192.168.0.1

Config file XML Option:
xmpps_client_host

Other Info:
Update requires server restart. Node only option.

H.1.29 XMPPS C2S Listener Port

Description:
This is the port listened to for XMPPS C2S sessions.

This option is only relevant when 'XMPPS C2S (deprecated)' has been enabled.

Syntax:
Numeric (Mandatory)

Default Value:
5223

Example:
5229

Config file XML Option:
xmpps_client_port

Other Info:
Update requires server restart.

H.1.30 BOSH Path

Description:
This option specifies the path for BOSH clients to access the XMPP over BOSH (client-to-server) service. When set, the XMPP over BOSH service is enabled.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/bosh

Config file XML Option:
bosh_uri

Other Info:
Update does not require server restart.

H.1.31 Enable BOSH TLS (https://)

Description:
When true, use of the HTTP over TLS (i.e.: https://) is expected in XMPP over BOSH sessions instead of HTTP (i.e., http://).

This option is only relevant when 'BOSH Path' has been set.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
bosh_tls

Other Info:
Update requires server restart.

H.1.32 BOSH Listener Host

Description:
This restricts the server to binding to a specific address for XMPP over BOSH. If unspecified, the server listens on all addresses.

This option is only relevant when 'BOSH Path' has been set.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
example.com

Config file XML Option:
bosh_host

Other Info:
Update requires server restart. Node only option.

H.1.33 BOSH Listener Port

Description:
This is the port listened to for XMPP over BOSH sessions.

This option is only relevant when 'BOSH Path' has been set.

Syntax:
Numeric (Mandatory)

Default Value:
5280

Example:
5289

Config file XML Option:
bosh_port

Other Info:
Update requires server restart.

H.1.34 BOSH Files Directory

Description:
Files within this directory will be read in (once, at startup) and served on demand over the BOSH HTTP or HTTPS service.

The directory set by default contains M-Link Webapps.

This option is only relevant when 'BOSH Path' has been set.

Syntax:
String (Mandatory)

Default Value:
/opt/isode/share/bosh_files

Example:
C:\Isode\ms\bosh_files

Config file XML Option:
bosh_files

Other Info:
Update requires server restart.

H.1.35 C2S Acknowledgment Request Period

Description:
By default, M-Link's XEP-0198 implementation will request an acknowledgement after every stanza. For sessions with XMPP clients, this can be send after every N stanzas by setting a value here. This may be used to tune network traffic patterns.

Syntax:
Numeric (Mandatory)

Default Value:
1

Example:
10

Config file XML Option:
xmpp_c2s_ack_request_period

Other Info:
Update does not require server restart.

H.1.36 S2S Startup Timeout

Description:
XMPP Server-to-Server (S2S) sessions which never start to send or receive stanzas will be terminated after this amount of time.

Syntax:
Numeric (Mandatory)

Default Value:
300

Example:
900

Config file XML Option:
xmpp_s2s_startup_timeout

Other Info:
Update does not require server restart.

H.1.37 S2S Timeout

Description:
XMPP Server-to-Server (S2S) sessions which stop sending or receiving stanzas for this amount of time will be terminated.

Syntax:
Numeric (Mandatory)

Default Value:
3600

Example:
7200

Config file XML Option:
xmpp_s2s_timeout

Other Info:
Update does not require server restart.

H.1.38 Transfer Pending X2X Stanzas

Description:
If this option is set to 'true', pending stanzas on a not-yet-established connection are delivered via the new connection whenever a new incoming X2X connection is established.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
xmpp_x2x_transfer_pending

Other Info:
Update does not require server restart. Shared only option.

H.1.39 Whing Timer

Description:
This provides the timer used to send inactive sessions a space character, or 'Whitespace Ping', designed to maintain the TCP session. It also acts as the timer to trigger XMPP Ping and XMPP Ping Timeout checks.

Syntax:
Numeric (Mandatory)

Default Value:
60

Example:
120

Config file XML Option:
xmpp_whing

Other Info:
Update does not require server restart.

H.1.40 Ping Timer

Description:
This provides the time a client or server session can be inactive before a ping request (described in XEP-0199) will be sent, designed to elicit a response from an inactive session. The value will be effectively rounded up to the nearest multiple of the 'Whing Timer'.

Syntax:
Numeric (Mandatory)

Default Value:
300

Example:
600

Config file XML Option:
xmpp_ping

Other Info:
Update does not require server restart.

H.1.41 Ping Timeout

Description:
This provides the longest period a client session may be silent before being terminated. Note that the 'Ping Timer' will force the client into a response, so this value should be set to a higher value, and the difference between the two acts as a timeout for the ping (described in XEP-0199). The value will be effectively rounded up to the nearest multiple of the 'Whing Timer'.

Syntax:
Numeric (Mandatory)

Default Value:
420

Example:
840

Config file XML Option:
xmpp_ping_timeout

Other Info:
Update does not require server restart.

H.1.42 Probe Timeout

Description:
When this option is non-zero, then the results of previous presence probes will be checked for timeouts periodically, causing removal of the contacts from the cache if no response has been seen for N seconds (specified here) after the last probe was sent.

The trigger for this timeout being checked is typically further presence being sent, so this timeout value represents a minimum timeout rather than an exact one.

Syntax:
Numeric (Mandatory)

Default Value:
60

Example:
0

Config file XML Option:
xmpp_probe_timeout

Other Info:
Update does not require server restart.

H.1.43 Reprobe Time

Description:
When this option is non-zero, then probes will be emitted for online sessions periodically.

The trigger for this time being checked is typically further presence being sent, so this time value represents a minimum time between probes rather than an exact one.

Syntax:
Numeric (Mandatory)

Default Value:
3600

Example:
0

Config file XML Option:
xmpp_reprobe_time

Other Info:
Update does not require server restart.

H.1.44 Return Probe from Local Cache

Description:
If this option is set to 'true', then the initial probe emitted on behalf of a client when it sends its initial presence will be satisfied from the cache if possible. The probes are still sent, so updated presence information may arrive later (as per normal).

If 'Probe Timeout' is 0, then this option will be ignored.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
xmpp_probe_cache

Other Info:
Update does not require server restart.

H.1.45 Suppress Duplicate Presence

Description:
When this option is set to 'true', duplicate presence from contacts will be suppressed, and not passed through to the client. M-Link has a very conservative view of what constitutes a duplicate presence, so setting this option is typically safe, but semantically duplicate presence will pass through on occasion.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
xmpp_probe_supress_dup

Other Info:
Update does not require server restart.

H.1.46 Enable Bidirectional XMPP S2S

Description:
If set to true, M-Link will use XEP-0288 bidirectional sessions between servers when possible.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
bidi

Other Info:
Update does not require server restart.

H.1.47 Dialback Secret

Description:
All nodes within the cluster should share a common dialback secret. It is recommended that a randomly generated character sequence be used.

Syntax:
String (Optional)

Default Value:
-None-

Example:
d14lb4ck-s3cr3t

Config file XML Option:
xmpp_db_secret

Other Info:
Update requires server restart. Shared only option.

H.1.48 Enable XEP-0138 compression

Description:
If set to true, M-Link will negotiate XEP-0138 compression where offered by a peer server, and will offer XEP-0138 compression to clients and peer servers.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
xep_138

Other Info:
Update requires server restart.

H.1.49 Maximum Decompression Buffer Size

Description:
If set to a non-zero number, M-Link will drop any connection that has XEP-0138 or TLS compression enabled and has a backlog of more than this amount of bytes after decompression.

Syntax:
Numeric (Mandatory)

Default Value:
10485760

Example:
10485760

Config file XML Option:
max_decompression_size

Other Info:
Update does not require server restart.

H.1.50 Server Administrators

Description:
The users of the group configured here will have special admin privileges over the entire server.

Syntax:
String (Optional)

Default Value:
-None-

Example:
example.com/group;local;name:admins

Config file XML Option:
server_admins

Other Info:
Update does not require server restart.

H.1.51 Admin Ad-Hoc Commands Checks

Description:
Administrative Ad-Hoc Commands will be offered to a user if all checks required by this field pass. The checks are space separated. Supported checks are 'operator' (require the user to be a member of the server administrators group) and 'secure' (require TLS protection)

Syntax:
String (Optional)

Default Value:
operator

Example:
operator secure

Config file XML Option:
admin_adhoc_checks

Other Info:
Update does not require server restart.

H.1.52 FIPS-140 Mode

Description:
The 140 series of Federal Information Processing Standards (FIPS) are U.S. government computer security standards that specify requirements for cryptography modules. When this option is set to true, it enables FIPS-140 compliance mode, which will restrict which hash and encryption algorithms are allowed in TLS and SASL. FIPS-140 mode is not available in this version of M-Link.

Syntax:
String (Optional)

Options:
true - Enable

false - Disable

os_default - Set Operating System Default

Default Value:
os_default

Example:
true

Config file XML Option:
fips140_mode

Other Info:
Update requires server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.53 TLS Cipher List

Description:
List of space (or colon) separated TLS ciphers the server is allowed to use, in the format recognized by the "openssl ciphers" command.

Syntax:
String (Mandatory)

Default Value:
DEFAULT

Example:
DHE-RSA-AES256-SHA DHE-DSS-AES256-SHA AES256-SHA

Config file XML Option:
tls_cipher_list

Other Info:
Update requires server restart.

H.1.54 TLS security level

Description:
TLS security level controls which ciphersuites, RSA and EC key sizes and hash functions can be used.

Syntax:
Numeric (Mandatory)

Default Value:
1

Example:
4

Config file XML Option:
tls_security_level

Other Info:
Update requires server restart.

H.1.55 Trust Anchors

Description:
This option's value contains the PEM representation of one or more CA certificates, each of which will be regarded as a Trust Anchor for the purpose of peer server authentication.

If this option is unset, and the option 'Trust Anchors File' is not set, or refers to an empty file, then authentication of clients and peer servers will not be possible, although TLS may still be used for encryption.

This option is ignored if the option 'Trust Anchors File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIBvDCCASWgAwIBAgIKIBN/w92XqfsbQTANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjMxNDU2MzdaFw0yMjEwMjMxNDU2MzdaMA0xCzAJBgNV

BAoTAkNBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCYDSLD9nMBzbwHTwWo

RK9O9+qR6Ymj7bamtbY2duO2aCvkiaMwsGBMb+nTRa/vMmoX5fRq9LFg3DPp/Sg7

0q+hvOM4XwI+8Sla7YD0FMlJOf195ou5GVfNVuKbDZGLFbIDL8UgRRVgGLJBlvYe

dC1IDET234WqU5ierKeH1ynYYQIDAQABoyMwITAOBgNVHQ8BAf8EBAMCAQYwDwYD

VR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQAkHKkRKa7KLgpvxujYkAao

Fg2AUdocY9zsjlm3w9hH47ZjP9cTb+oI6B0G2/FGdLcoq7Cq5AW+lv8zWlKf+Ja0

prXPUjynNMpyRP9DE8xFOy8HzBwYC2WRtCjx6MYwIaLKCxE8OfcVoc7zbPdqYVND

4AJTbHhgdOrokMnoFfBROA==

-----END CERTIFICATE-----

Config file XML Option:
tls_ca_certs

Other Info:
Update requires server restart.

H.1.56 Trust Anchors File

Description:
This specifies the name to a PEM file ('.pem' extension) corresponding to the option 'Trust Anchors'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/server-tls/trust-anchors.pem

Config file XML Option:
tls_ca_file

Other Info:
Update requires server restart.

H.1.57 TLS Certificate

Description:
This specifies the server's own certificate and corresponding certificate chain. These certificates will be sent by the server to any client that wishes to confirm the server's identity when negotiating secure communication.

The format is PEM ('.pem' extension).

Without the server certificate specified, TLS services will only be offered using anonymous cipher suites, which are disabled by default. Anonymous cipher suites are typically unsupported by client software, and therefore should be used with care.

It is ignored if the option 'TLS Certificate File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIICxDCCAi2gAwIBAgIKZ1d0o6sV47g1DjANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjMxNDU3NTlaFw0xMzEwMjMxNDU3NTlaMBsxGTAXBgNV

BAMTEGxvbmRvbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB

ANcBnOkOtwvGM7orZkwhUUxXQbG1UjxMBYz8ptAnfnwJSr2zYjWzPGjo9DPFSHQw

/virwx6nRIWP78NSa5TC1/TNPJBAeKLj3Ps76JiR7NbbBQN6TFWY/qJ+ykKiiGDG

W6lZuaVhTOxFgkLLH6LfThVwCRo00oW0UPZt+DAh0AK5AgMBAAGjggEbMIIBFzCB

lwYDVR0RBIGPMIGMghBsb25kb24uaXNvZGUubmV0oCsGCCsGAQUFBwgHoB8WHV94

bXBwLXNlcnZlci5sb25kb24uaXNvZGUubmV0oCsGCCsGAQUFBwgHoB8WHV94bXBw

LWNsaWVudC5sb25kb24uaXNvZGUubmV0oB4GCCsGAQUFBwgFoBIMEGxvbmRvbi5p

c29kZS5uZXQwDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYE

FMVIpnvX6WN+BVS7FuT7rCrlnh57MD4GA1UdIwQ3MDWAFCKcUg/+XPHfYvZ2Osxq

0LSnDg68oRGkDzANMQswCQYDVQQKEwJDQYIKIBN/w92XqfsbQTANBgkqhkiG9w0B

AQUFAAOBgQBkFQDMGYoGMpvg5qSQ3BGgdxxK0CVDEvfgPwDhKROZUIIbhz/S8wkh

+pg3nD3ZGbFnyIHV+eGFBnxauiYfqYpmRmQ59R/KCfjYY9/USXgEOEdlxT8N85op

th6aH/7K6uP5PNF/6VXDYWk4zZCLI6L2ErBRdgI5VjN6anqyjnElHg==

-----END CERTIFICATE-----

Config file XML Option:
tls_cert

Other Info:
Update requires server restart.

H.1.58 TLS Certificate File

Description:
This specifies the full path to a file corresponding to the option 'TLS Certificate'.

The certificate format can be either PEM ('.pem') or PKCS#12 ('.p12').

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/server-tls/server_certificate.pem

Config file XML Option:
tls_cert_file

Other Info:
Update requires server restart.

H.1.59 TLS Key

Description:
This specifies the private key belonging to the server certificate.

The key format is PEM. If encrypted, 'TLS Key Password' must be set.

If this option and the option 'TLS Key File' are not set, the value of the 'TLS Certificate' or 'TLS Certificate File' is used.

This option and 'TLS Key File' are not used when 'TLS Certificate File' has PKCS#12 format.

This option is ignored if the option 'TLS Key File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,33EA8F3A016EC013

QvrosxH8Ai1vxxyEHSUk+j5KHqN/z/1U/l2TokGfCpfDrar9NO7pPIvxEKZYgrCa

L5/13DUBdffvwl2SgNlYMf1UoKORV/3EgzUXSP+Yghgad+/ogJY9g/vDrixu8xtv

ToRRVukS8PxR3V3EaHh29H77sGTi4e2U/fanISY7foy6ihTa5hrTvMyMnjH0VlKE

xHxLvA0xAPAdNcl6T/HXev/OG8RkmkRIVXeh96AJCM3axdJO8WjE0iSrvxtCUwjI

y2HKkUT1+/g7nuu5cKy0hAvkUYbLZ+tywtgEKjz7XZhnSdQts4rqkOeW8rc1QB9m

aDxR5wC2lkzwm6Yn+pG8jjRPtbQlCNQvA4DyIbaSpeHX0zmlMov9NtcK7gYyrqa7

V7Z/7Op2nmE4Mps5ZX0lUbmS6yqwYiuK1b9M61ZufBVHeevfO4P4Gq7Mkmkr20CX

kL6rY9Wm2F2gqxATKtStqyKn2xalzCOCe03UiEIC5acc7Fk+Tdd5DeyZXHwCCgix

ZzZQjXQL6uWDSntb4ADV+olLs5HKHRrHup/oGOX8xs40S4tX6Abvy+L0YUJzF9o/

QFVsvmDe/Nd5wukMu5Ibmyrp1RyV0QCTzB6I2iutE0oASHOezz6F2C0shdqYdOex

BfhQV5MqbUwH4Pq53Df+9gUx8OdPkUSTJgpDZbiKdliDu7X2oPXgzvz0HDzGpT/K

Rp90qEXx+6UB2q81D3CO+IElpEwuSWWIoADKGxP5dpqKaqqhVUi5CDPwbIRxosui

cbT+Z/v3SAKdBDD+kAS3s8brv+/nh03UrFPVcobsgr8ttSysvJu2TQ==

-----END RSA PRIVATE KEY-----

Config file XML Option:
tls_key

Other Info:
Update requires server restart.

H.1.60 TLS Key File

Description:
This specifies the full path to a PEM file corresponding to the option 'TLS Key'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/server-tls/server-key.pem

Config file XML Option:
tls_key_file

Other Info:
Update requires server restart.

H.1.61 TLS Key Password

Description:
This specifies the password used to decrypt the server's private key. When empty (the default), the private key must not be not encrypted

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
SuperS0cret-Password

Config file XML Option:
tls_key_password

Other Info:
Update requires server restart.

H.1.62 Self Certificates

Description:
This option's value contains the PEM representation of one or more certificates, each of which will be regarded as trusted for the purpose of self authentication such as in intra-clustering communications.

If this option is unset, and the option 'Self Certificates File (PEM)' is not set, or refers to an empty file, only nodes sharing the same server certificate will be authenticated.

This option is ignored if the option 'Self Certificate File (PEM)' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIBvDCCASWgAwIBAgIKIBN/w92XqfsbQTANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjMxNDU2MzdaFw0yMjEwMjMxNDU2MzdaMA0xCzAJBgNV

BAoTAkNBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCYDSLD9nMBzbwHTwWo

RK9O9+qR6Ymj7bamtbY2duO2aCvkiaMwsGBMb+nTRa/vMmoX5fRq9LFg3DPp/Sg7

0q+hvOM4XwI+8Sla7YD0FMlJOf195ou5GVfNVuKbDZGLFbIDL8UgRRVgGLJBlvYe

dC1IDET234WqU5ierKeH1ynYYQIDAQABoyMwITAOBgNVHQ8BAf8EBAMCAQYwDwYD

VR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQAkHKkRKa7KLgpvxujYkAao

Fg2AUdocY9zsjlm3w9hH47ZjP9cTb+oI6B0G2/FGdLcoq7Cq5AW+lv8zWlKf+Ja0

prXPUjynNMpyRP9DE8xFOy8HzBwYC2WRtCjx6MYwIaLKCxE8OfcVoc7zbPdqYVND

4AJTbHhgdOrokMnoFfBROA==

-----END CERTIFICATE-----

Config file XML Option:
tls_self_certs

Other Info:
Update requires server restart.

H.1.63 Self Certificates File

Description:
This specifies the path to a PEM file ('.pem' extension) corresponding to the option 'Self Certificates'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/server-tls/self.pem

Config file XML Option:
tls_self_certs_file

Other Info:
Update requires server restart.

H.1.64 TLS Compression

Description:
If disabled, TLS compression will not be used. This may be useful on sites with particularly high connection levels.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_compression

Other Info:
Update requires server restart.

H.1.65 Verify Depth

Description:
This specifies the maximum depth of a certificate verification chain.

Syntax:
Numeric (Mandatory)

Default Value:
5

Example:
7

Config file XML Option:
tls_verify_depth

Other Info:
Update requires server restart.

H.1.66 Verify Timeout

Description:
This specifies the certificate verification time out.

Syntax:
Numeric (Mandatory)

Default Value:
10

Example:
30

Config file XML Option:
tls_verify_timeout

Other Info:
Update requires server restart.

H.1.67 LDAP Directory Host for CRL Retrieval

Description:
This provides an LDAP directory hostname for CRL lookups.

Note that the LDAP server is accessed using an anonymous bind (no user authentication).

Syntax:
String (Optional)

Default Value:
-None-

Example:
localhost

Config file XML Option:
tls_ldap_server

Other Info:
Update requires server restart.

H.1.68 LDAP Directory Port for CRL Retrieval

Description:
This provides the LDAP directory port number for CRL lookups.

Note that the LDAP server is accessed using an anonymous bind (no user authentication).

Syntax:
Numeric (Mandatory)

Default Value:
19389

Example:
389

Config file XML Option:
tls_ldap_port

Other Info:
Update requires server restart.

H.1.69 Check revocation

Description:
This controls whether revocation status should be checked for certificates. If this is true, then certificates will only be trusted if the revocation status can be checked, and is found to be satisfactory.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_check_crls

Other Info:
Update requires server restart.

H.1.70 Check revocation on end-entity certificates

Description:
This controls whether revocation status should be checked for just end-entity certificates. If this is true, then end-entity certificates will only be trusted if the revocation status can be checked, and is found to be satisfactory. This has no effect if all certificates are being checked in 'Check Revocation'.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_check_leaf

Other Info:
Update requires server restart.

H.1.71 Use nonce in OCSP

Description:
This controls whether the nonce extension will be added to OCSP requests. This has no effect if revocation checking is not being performed.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_ocsp_nonce

Other Info:
Update requires server restart.

H.1.72 URI for OCSP

Description:
This sets a URI to be used for OCSP queries, ordinarily a local OCSP responder (one that caches CRLs or proxies OCSP). For each certificate, if the specified URI does not produce a response then if the certificate contains a URI for OCSP then that will also be queried.

Syntax:
String (Optional)

Default Value:
-None-

Example:
http://ocsp.example.com

Config file XML Option:
tls_ocsp_uri

Other Info:
Update requires server restart.

H.1.73 OCSP Responder Certificate

Description:
This is a PEM-format certificate that will be accepted as a signer of OCSP responses (ordinarily this would be used in conjunction with 'URI for OCSP').

This option is ignored if the option 'OCSP Responder Certificate File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIC0zCCAjygAwIBAgIKY9jxz11/UjFYZDANBgkqhkiG9w0BAQUFADASMRAwDgYD

VQQKEwdndXJtZWVuMB4XDTEyMTAxMTE1Mjc0NFoXDTEzMTAxMTE1Mjc0NFowHDEa

MBgGA1UEAxMRZ3VybWVlbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0A

MIGJAoGBAIN45yMMt/eiM3hmSOOAoV/NCM80B4Fuu7HnUSCaNWJT+HvUf+YIWzEh

c8KaBvOvY6scl5euqXZKCiGfBUuf7b8mo16M0D6JhTw5mHYjU+H7bxEQNX9OcweS

7ZiNB1cBl3LUc/e31LVlaG4z52MJefnF8fzF4C3vr+mCBsE+vqUFAgMBAAGjggEk

MIIBIDCBmwYDVR0RBIGTMIGQghFndXJtZWVuLmlzb2RlLm5ldKAsBggrBgEFBQcI

B6AgFh5feG1wcC1zZXJ2ZXIuZ3VybWVlbi5pc29kZS5uZXSgLAYIKwYBBQUHCAeg

IBYeX3htcHAtY2xpZW50Lmd1cm1lZW4uaXNvZGUubmV0oB8GCCsGAQUFBwgFoBMM

EWd1cm1lZW4uaXNvZGUubmV0MA4GA1UdDwEB/wQEAwIF4DAMBgNVHRMBAf8EAjAA

MB0GA1UdDgQWBBTWgBSrTYUQwALHa8GxT/W4BKm0LzBDBgNVHSMEPDA6gBTtI+61

Mbuq3UaCXAm7PC1PvM25nqEWpBQwEjEQMA4GA1UEChMHZ3VybWVlboIKTXeI0/b+

70cwWzANBgkqhkiG9w0BAQUFAAOBgQAxVfzDpfplNRJRXw6+5fkINS+S78rkgSsw

I2MrTKoZ5JS2X08/jiqWdpFAjmkypoVjlZb4nU/8vsvxBzYSIiAYo6+jmTLqGaQ4

3rtj4JdGeN25ht5D2+j8Vzp98LO7ohUCY7JBrTL1/+JQQUT35/du1LY0nwZY+Guf

vwJsG6BSkQ==

-----END CERTIFICATE-----

Config file XML Option:
tls_ocsp_responder_cert

Other Info:
Update requires server restart.

H.1.74 OCSP Responder Certificate File

Description:
This specifies the full path to a PEM file ('.pem' extension) corresponding to the option 'OCSP Responder Certificate'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/certificates/oscp-responder.pem

Config file XML Option:
tls_ocsp_responder

Other Info:
Update requires server restart.

H.1.75 Don't use configured OCSP URI

Description:
This disables use of the configured OCSP URI.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_ocsp_configured

Other Info:
Update requires server restart.

H.1.76 Don't use OCSP URIs from certificate extensions

Description:
If set to 'true', this disables use of OCSP URI from authorityInfoAccess extensions.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_ocsp_uri

Other Info:
Update requires server restart.

H.1.77 Don't get CRLs from configured LDAP server

Description:
This disables use of the configured LDAP server to retrieve CRLs.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_crl_configured

Other Info:
Update requires server restart.

H.1.78 Don't get certs from configured LDAP server

Description:
This mostly disables use of the configured LDAP server to retrieve certificates. (If an entry is being read to retrieve CRLs, then certificates will also be read.)

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_cert_configured

Other Info:
Update requires server restart.

H.1.79 Don't use URIs from extensions to look up CRLs

Description:
This disables use of CRL DP, ARL DP, freshestCRL extensions.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_crl_uri

Other Info:
Update requires server restart.

H.1.80 Don't use URIs from extensions to look up certificates

Description:
If set to 'true', this disables following authorityInfoAccess extensions to find certificates.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_cert_uri

Other Info:
Update requires server restart.

H.1.81 Ignore freshestCRL extensions

Description:
This disables use of freshestCRL extensions in certificates and CRLs.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_freshestcrl

Other Info:
Update requires server restart.

H.1.82 Always use HTTP POST for OCSP requests

Description:
This disables use of HTTP GET for OCSP requests (by default, encoded requests smaller than 255 bytes will be made using HTTP GET).

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_lookup_avoid_ocsp_httpget

Other Info:
Update requires server restart.

H.1.83 User Certificate Trust Anchors

Description:
This option's value contains the PEM representation of one or more CA certificates, each of which will be regarded as a Trust Anchor for the purpose of user authentication.

If this option is unset, and the option 'User Certificate Trust Anchors File' is not set, or refers to an empty file, then certificate-based authentication of user will not be possible, although TLS may still be used for encryption and other authentication methods will remain available.

This option is ignored if the option 'Trust Anchors File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIBvDCCASWgAwIBAgIKIBN/w92XqfsbQTANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjMxNDU2MzdaFw0yMjEwMjMxNDU2MzdaMA0xCzAJBgNV

BAoTAkNBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCYDSLD9nMBzbwHTwWo

RK9O9+qR6Ymj7bamtbY2duO2aCvkiaMwsGBMb+nTRa/vMmoX5fRq9LFg3DPp/Sg7

0q+hvOM4XwI+8Sla7YD0FMlJOf195ou5GVfNVuKbDZGLFbIDL8UgRRVgGLJBlvYe

dC1IDET234WqU5ierKeH1ynYYQIDAQABoyMwITAOBgNVHQ8BAf8EBAMCAQYwDwYD

VR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQAkHKkRKa7KLgpvxujYkAao

Fg2AUdocY9zsjlm3w9hH47ZjP9cTb+oI6B0G2/FGdLcoq7Cq5AW+lv8zWlKf+Ja0

prXPUjynNMpyRP9DE8xFOy8HzBwYC2WRtCjx6MYwIaLKCxE8OfcVoc7zbPdqYVND

4AJTbHhgdOrokMnoFfBROA==

-----END CERTIFICATE-----

Config file XML Option:
tls_user_ca_certs

Other Info:
Update requires server restart.

H.1.84 User Certificate Trust Anchors File

Description:
This specifies the name to a PEM file ('.pem' extension) corresponding to the option 'User Certificate Trust Anchors'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/server-tls/user_ca.pem

Config file XML Option:
tls_user_ca_file

Other Info:
Update requires server restart.

H.1.85 Check user certificate revocation

Description:
This controls whether revocation status should be checked for user certificates and their issuers' certificates. If this is true, then user certificates will only be trusted if the revocation status can be checked, and is found to be satisfactory.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_user_check_crls

Other Info:
Update requires server restart.

H.1.86 Check user end-entity certificate revocation

Description:
This controls whether revocation status should be checked for just user certificates. If this is true, then user end-entity certificates will only be trusted if the revocation status can be checked, and is found to be satisfactory. This option has no effect if 'Check User Certificate Revocation' is set to 'true'.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_user_check_leaf

Other Info:
Update requires server restart.

H.1.87 Alternative domain for user certificates

Description:
Match user identities only after replacement of domain with specified alternative.

Syntax:
String (Optional)

Default Value:
-None-

Example:
identity-authoritity.mil

Config file XML Option:
tls_user_domain

Other Info:
Update does not require server restart.

H.1.88 Match user to SAN email address

Description:
Match user identity against SAN email address.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
tls_user_match_email

Other Info:
Update does not require server restart.

H.1.89 Match user to SAN XMPPAddress (JID)

Description:
Match user identity against SAN XMMPAddress (JID).

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
tls_user_match_jid

Other Info:
Update does not require server restart.

H.1.90 Match user to SAN User Principal Name (UPN)

Description:
Match user identity against SAN User Principal Name (UPN).

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_user_match_upn

Other Info:
Update does not require server restart.

H.1.91 Match user to Subject Common Name (CN)

Description:
Match user identity against Common Name (CN) attribute in Subject DN.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_user_match_subject_cn

Other Info:
Update does not require server restart.

H.1.92 Match user to Subject Email

Description:
Match user identity against E-mail (email) attribute in Subject DN.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tls_user_match_subject_email

Other Info:
Update does not require server restart.

H.1.93 Require TLS

Description:
This option, when true, requires XMPP clients to use TLS.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
require_tls

Other Info:
Update does not require server restart.

H.1.94 Maximum Number of Authentication Failures

Description:
When set to a non-zero number, each session will be limited to that number of authentication failures, beyond which they will be disconnected by the server. This means that an attacker must reconnect frequently in order to attempt brute force password attacks.

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
1

Config file XML Option:
max_auth_failures

Other Info:
Update does not require server restart.

H.1.95 XMPP Message of the Day

Description:
This option may be used to provide a message or service warning displayed to users as they become available. The message is sent as plain text only.

Syntax:
String (Optional)

Default Value:
-None-

Example:
Welcome to the XMPP Service

Config file XML Option:
xmpp_motd

Other Info:
Update does not require server restart.

H.1.96 Enable last login reporting

Description:
When set, this will record the last successful login, and a number of failed logins, and send messages describing them to clients on their next successful login.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
last_login

Other Info:
Update does not require server restart. Shared only option.

H.1.97 Maximum auth_fail reports

Description:
If last login reporting is enabled, this option is used to control the maximum number of authentication failures kept and shown to users. If the option is set to 0, then no limit will be applied; this will result in a possible denial of service attack.

Syntax:
Numeric (Mandatory)

Default Value:
5

Example:
-1

Config file XML Option:
last_login_fail_max

Other Info:
Update requires server restart. Shared only option.

H.1.98 Per-user session limit

Description:
If set to a non-zero value, then each user may only connect that many times. Further connections will be rejected after authentication.

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
3

Config file XML Option:
xmpp_session_limit

Other Info:
Update does not require server restart.

H.1.99 Non-exists Cache Period

Description:
M-Link keeps a cache of users known not to exist; this is the time-to-live for this negative cache.

Syntax:
Numeric (Mandatory)

Default Value:
10

Example:
60

Config file XML Option:
nonexists_cache_period

Other Info:
Update does not require server restart.

H.1.100 Auto-accept Local Default

Description:
If this setting is set, the default behaviour when a user received a subscription request from a local domain will be for the server to automatically accept it without user confirmation.

This can be overridden by the user.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
autoaccept_local_default

Other Info:
Update does not require server restart. Shared only option.

H.1.101 Auto-subscribe Local Default

Description:
If this option is set, then when a user receives a subscription request, the server will, by default, send a subscription request in return. This can be overridden by the user, and is independent of Auto Accept options including 'Auto-accept Local Default'.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
autosubscribe_local_default

Other Info:
Update does not require server restart. Shared only option.

H.1.102 Enable XMPP Roster Groups

Description:
If this is turned off, roster groups will no longer be added to rosters. This is generally only useful as a fault isolation option.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
xmpp_process_roster_groups

Other Info:
Update does not require server restart. Shared only option.

H.1.103 Groups Discovery

Description:
This setting may be 'true', to have groups visible in service discovery to all; or 'false'. Server administrators will always be able to do groups discovery and so will IM domain administrators on IM domains they administer.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
groups_discovery

Other Info:
Update does not require server restart. Shared only option.

H.1.104 XEP-0055 Search Default

Description:
This setting may be 'never', to have users never visible in searches; 'always', to have user always visible in searches; and 'local', to allow users to find each other, but hide users from remote searches.

Syntax:
String (Mandatory)

Default Value:
never

Example:
always

Config file XML Option:
xep55_search_default

Other Info:
Update does not require server restart. Shared only option.

H.1.105 Offline Message Default

Description:
This option defines the default for a user's offline messaging behaviour. It can be overridden by user settings.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
true

Config file XML Option:
offline_messaging_default

Other Info:
Update does not require server restart. Shared only option.

H.1.106 Offline Messaging

Description:
When this option is set to 'true', offline messaging is enabled across the server. Whether a message to an individual user who is offline will be held until the user is online depends on several settings:

1. This setting must be on.

2. The user must have offline messaging enabled, either by the default, or by a user specific setting.

3. The user's offline messaging store must contain fewer than the maximum number of offline messages.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
true

Config file XML Option:
offline_messaging

Other Info:
Update does not require server restart. Shared only option.

H.1.107 Offline Message Limit

Description:
This option defines the maximum number of offline messages the server will store for a user.

Syntax:
Numeric (Mandatory)

Default Value:
100

Example:
2500

Config file XML Option:
offline_message_max

Other Info:
Update does not require server restart. Shared only option.

H.1.108 Offline Message Size

Description:
This option defines the maximum size a message in the offline store. The actual maximum is calculated by multiplying this value by the 'Offline Message Limit'.

Syntax:
Numeric (Mandatory)

Default Value:
256

Example:
100

Config file XML Option:
offline_message_size

Other Info:
Update does not require server restart. Shared only option.

H.1.109 XMPP MUC Domain

Description:
This option is deprecated; please see the multidomain configuration.

Syntax:
String (Optional)

Default Value:
-None-

Example:
talk.example.com

Config file XML Option:
xmpp_muc_domain

Other Info:
Update requires server restart. Shared only option. Advanced option - not available in Ad-Hoc Commands.

H.1.110 Statistics Domain

Description:
If set, this option specifies the Publish-Subscribe domain that will serve server statistics. This domain must already exist as a standard pubsub domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
pubsub.example.com

Config file XML Option:
stats_domain

Other Info:
Update requires server restart. Shared only option.

H.1.111 Queues Statistics Directory

Description:
If it exists, this directory is populated with router dumps and memory-mapped files which maintain a live view of internal work queue data. This provides important debugging information.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that if the directory exists then it has correct ownership and permissions and if it does not exist then the 'Runtime User ID' has the correct permissions to create it.

Syntax:
String (Optional)

Default Value:
-None-

Example:
C:\Isode\ms\stats

Config file XML Option:
stats_dir

Other Info:
Update requires server restart.

H.1.112 Publish-Subcribe Directory

Description:
This specifies the directory used for persistent Multi-User Chat and Publish-Subscribe services.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that if the directory exists then it has correct ownership and permissions and if it does not exist then the 'Runtime User ID' has the correct permissions to create it.

Syntax:
String (Mandatory)

Default Value:
/var/isode/ms/pubsub

Example:
C:\Isode\ms\pubsub

Config file XML Option:
pubsub_dir

Other Info:
Update requires server restart.

H.1.113 MUC Audit Archive Directory

Description:
This enables audit archiving for MUC rooms and specifies the directory used to store them.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that if the directory exists then it has correct ownership and permissions and if it does not exist then the 'Runtime User ID' has the correct permissions to create it.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/work/ms/muc

Config file XML Option:
muc_archive_dir

Other Info:
Update requires server restart.

H.1.114 User Audit Archive Directory

Description:
This enables audit archiving for user accounts and specifies the directory used to store them.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that if the directory exists then it has correct ownership and permissions and if it does not exist then the 'Runtime User ID' has the correct permissions to create it.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/work/ms/archive

Config file XML Option:
user_archive_dir

Other Info:
Update requires server restart.

H.1.115 Cache XMPP Service Discovery Information

Description:
This option caches local clients' XEP-0115/XEP-0030 responses, and serves these in response to subsequent requests. This reduces bandwidth to clients.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
xmpp_disco_cache

Other Info:
Update does not require server restart. Shared only option.

H.1.116 XMPP Maximum MUC History Limit

Description:
This provides an absolute upper limit to the number of messages which may be held in a chatroom's history backlog.

Syntax:
Numeric (Mandatory)

Default Value:
200

Example:
1000

Config file XML Option:
xmpp_max_muc_history_limit

Other Info:
Update does not require server restart. Shared only option.

H.1.117 Delay the flush so items writes can be batched together

Description:
This option specifies the delay before an item is flushed to disk so items can be batch togther. 0 is no delay and a maximum of 5 seconds delay.

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
2

Config file XML Option:
pubsub_flush_delay

Other Info:
Update does not require server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.118 Timeout in seconds for userdb syncing

Description:
The timeout can be disabled by setting it to value less than 1.

Syntax:
Numeric (Mandatory)

Default Value:
2

Example:
-1

Config file XML Option:
userdb_timeout

Other Info:
Update does not require server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.119 Enable TCS Compatibility Mode

Description:
If set to true, M-Link will act more like Tactical Chat Server (TCS) would. Useful when clients specifically designed for TCS must be supported.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
tcs_compat

Other Info:
Update does not require server restart. Shared only option.

H.1.120 Send Multiple MUC Status Codes

Description:
If set to true, both a 201 and a 110 statuc code will be sent upon MUC room creation, as required by XEP-0045. If set to false, M-Link only a 201 reply will be sent to increase compatibility with some old clients.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
send_multiple_muc_status_codes

Other Info:
Update does not require server restart. Shared only option.

H.1.121 Enable XEP-0289 FMUC

Description:
This enables XEP-0289 Federated Multiuser Chat.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
fmuc

Other Info:
Update requires server restart.

H.1.122 FMUC Rejoin Frequency

Description:
After an FMUC federation has been broken for fmuc_rejoin_frequency seconds, a rejoin will be attempted. Set to 0 to disable automatic rejoining (in which case rejoin will only be triggered by activity in the room).

Syntax:
Numeric (Mandatory)

Default Value:
30

Example:
60

Config file XML Option:
fmuc_rejoin_frequency

Other Info:
Update does not require server restart.

H.1.123 Enable IRC Gateway

Description:
This enables IRC Gateway support for MUC rooms.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
irc

Other Info:
Update requires server restart.

H.1.124 Propagate IRC channel joining error to MUC room

Description:
If set to true, and the IRC server forbids the user joining the channel, then the user is kicked out of the MUC room in order to preserve consistency between participants in the MUC room and in the IRC channel.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
irc_kick_on_error

Other Info:
Update does not require server restart. Shared only option.

H.1.125 Maximum IRC Prefix Length

Description:
This value specifies a maximum number of characters allocated for the IRC prefix. This can be increased in case sent messages are being truncated.

Syntax:
Numeric (Mandatory)

Default Value:
200

Example:
250

Config file XML Option:
irc_prefix_size

Other Info:
Update does not require server restart. Shared only option. Advanced option - not available in Ad-Hoc Commands.

H.1.126 IRC Outgoing Nickname Prefix

Description:
If specified, all XMPP users in gatewayed rooms will have this prefix in the IRC channel. The prefix itself must be a valid IRC nickname. Setting this option does not modify what users look like in the MUC room.

Syntax:
String (Optional)

Default Value:
-None-

Example:
XMPP-

Config file XML Option:
irc_outgoing_nick_prefix

Other Info:
Update does not require server restart. Shared only option.

H.1.127 Enable Audit Module

Description:
This enables or disables the user audit logging. It produces a number of audit logging messages which may be directed to files via the logging configuration.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
audit

Other Info:
Update requires server restart.

H.1.128 AMP HTTP Host

Description:
This specifies a specific IP address to listen to for the HTTP API. If not specified, then the service is available on all interfaces.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
192.168.0.1

Config file XML Option:
amp_http_host

Other Info:
Update requires server restart. Node only option.

H.1.129 HTTP API Port

Description:
If specified, this will enable the HTTP API module, and listen on this port for requests.

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
8080

Config file XML Option:
amp_http_port

Other Info:
Update requires server restart.

H.1.130 Enable HTTP API TLS

Description:
If set to true, the HTTP API will use 'https' rather than 'http'.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
amp_http_tls

Other Info:
Update requires server restart.

H.1.131 HTTP API support files path

Description:
The HTTP API uses various images and other support files in some cases. Currently, this is limited to PNG images corresponding to the standard XMPP 'show' states, plus 'available' and 'offline'. These are loaded at startup from this directory.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/var/isode/ms/images/

Config file XML Option:
amp_http_files

Other Info:
Update requires server restart.

H.1.132 Enable XEP-0060 presence processing for local users

Description:
If enabled, Pubsub (XEP-0060) services will track presence of local users and react accordingly, including the pseudo-presence of connected components.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
amp_pubsub_presence

Other Info:
Update requires server restart. Shared only option.

H.1.133 Enable monitor MUC domain

Description:
This can be set to an existing, local Multi-User Chat domain. Once this is done, e.g. on the domain 'monitor-muc.local.domain', then administrators can monitor all C2S and S2S traffic using MUC rooms in this domain.

S2S traffic between any local domain and the remote domain 'any.remote.domain' can be monitored in the room 'any.remote.domain@monitor-muc.local.domain'. C2S traffic of a user 'user@any.local.domain' can be monitored in the room 'user\40any.local.domain@monitor-muc.local.domain'.

Please note that chat rooms on this MUC domain can only be used by administrators and for live protocol monitoring.

Syntax:
String (Optional)

Default Value:
-None-

Example:
monitor-muc.local.domain

Config file XML Option:
amp_monitor_muc

Other Info:
Update requires server restart. Shared only option.

H.1.134 Timeout for delegated user IQs

Description:
This specifies how long M-Link will wait for a response from the component for delegated user IQs. If the component fails to answer within this timeframe, M-Link will generate an error response.

Syntax:
Numeric (Mandatory)

Default Value:
60

Example:
60

Config file XML Option:
amp_iq_delegation_timeout

Other Info:
Update does not require server restart.

H.1.135 Archive Server Host

Description:
For the Archive Server, this restricts the system to binding to a specific address for communications with the XMPP Server. If unspecified, the system listens on all addresses.

For the XMPP Server, this is the host to connect to for communications with the Archive Server.

On Unix, when 'Archive Server Host' is configured as a Unix pipe, the value of 'Archive Server Port' will be ignored.

Syntax:
String (Mandatory)

Default Value:
/var/run/wabac

Example:
127.0.0.1

Config file XML Option:
wabac_host

Other Info:
Update requires server restart.

H.1.136 Archive Server Port

Description:
For the Archive Server, the port on which it will listen for connections on.

For the XMPP Server, and port that it will connect to the Archive Server on.

On Unix, when 'Archive Server Host' is configured as a Unix pipe, the value of this option will be ignored.

Syntax:
Numeric (Mandatory)

Default Value:
50001

Example:
-None-

Config file XML Option:
wabac_port

Other Info:
Update requires server restart.

H.1.137 Archive Database Directory

Description:
Specifies the directory used by the Archive Server for storing its data.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that if the directory exists then it has correct ownership and permissions and if it does not exist then the 'Runtime User ID' has the correct permissions to create it.

Syntax:
String (Mandatory)

Default Value:
/var/isode/ms/wabacdb

Example:
C:\Isode\ms\wabacdb

Config file XML Option:
wabac_data_dir

Other Info:
Update requires server restart.

H.1.138 Archive Queue Directory

Description:
Specifies the directory used by XMPP Server for storing messages not yet acknowledged to have been archived by the Archive Server.

On Unix, all files in this directory are created as the user specified in the option 'Runtime User ID' so it should be ensured that if the directory exists then it has correct ownership and permissions and if it does not exist then the 'Runtime User ID' has the correct permissions to create it.

Syntax:
String (Mandatory)

Default Value:
/var/isode/ms/wabacq

Example:
C:\Isode\ms\wabacq

Config file XML Option:
wabac_queue_dir

Other Info:
Update requires server restart.

H.1.139 Archive HTTP Server Host

Description:
'Archive HTTP Server Host' and 'Archive HTTP Server Port' are the host and port on which the Archive Server will listen for HTTP connections. If the 'Archive HTTP Server Host' is not specified, then INADDR_ANY is assumed, hence listening on all interfaces.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
127.0.0.1

Config file XML Option:
wabac_http_host

Other Info:
Update requires server restart. Shared only option.

H.1.140 Archive HTTP Server Port

Description:
See 'Archive HTTP Server Host' for details.

Syntax:
Numeric (Mandatory)

Default Value:
5080

Example:
-None-

Config file XML Option:
wabac_http_port

Other Info:
Update requires server restart.

H.1.141 Enable Archive HTTP TLS

Description:
If set to 'true', the Archive Server will use 'https' rather than 'http' on the HTTP interface.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
wabac_http_tls

Other Info:
Update requires server restart.

H.1.142 XMPP Server shares Archive Server Config

Description:
This should be enabled if the XMPP Server shares its config file with the Archive Server it connects to using 'Archive Server Host' and 'Archive Server Port'. This is only possible if it is on the same host. In such a case, the XMPP Server will forward any trigger to reload the configuration to the Archive Server too.

Note that there should always be an XMPP Server running on the same host as the Archive Server, even if its function is just to configure the local Archive Server.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
wabac_config_share

Other Info:
Update does not require server restart.

H.1.143 Timeout for Archive Operations

Description:
This specifies how long the XMPP Server will wait for a response from the Archive Server for operations.

Syntax:
Numeric (Mandatory)

Default Value:
30

Example:
60

Config file XML Option:
wabac_timeout

Other Info:
Update does not require server restart.

H.1.144 Archive Database Journal Mode

Description:
This specifies the journal mode as used by the database backend of the Archive Server. Selecting 'Rollback Journal' mode will increase data resiliance, but will decrease performance.

Syntax:
String (Mandatory)

Options:
wal - Write-Ahead Logging

journal - Rollback Journal

Default Value:
wal

Example:
journal

Config file XML Option:
wabac_journal_mode

Other Info:
Update requires server restart.

H.1.145 Archive Include Remote MUCs in User Results

Description:
If enabled, return group chat messages for remote MUC rooms when querying a user archive.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
wabac_include_remote_mucs_in_user_results

Other Info:
Update does not require server restart. Shared only option.

H.1.146 Archive Server database memory limit

Description:
Soft limit on the amount of heap memory allocated by the Archive Server database backend

Syntax:
Numeric (Mandatory)

Default Value:
268435456

Example:
536870912

Config file XML Option:
wabac_sqlite_heap_limit

Other Info:
Update requires server restart.

H.1.147 Maximum number of MAM results per request

Description:
This option specifies the maximum number of items returned per MAM query.

Syntax:
Numeric (Mandatory)

Default Value:
100

Example:
10

Config file XML Option:
max_mam_items

Other Info:
Update does not require server restart.

H.1.148 Enable XEP-0280 Message Carbons

Description:
If set to true, M-Link will allow clients to use XEP-0280 Message Carbons.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
carbons

Other Info:
Update requires server restart. Shared only option. Advanced option - not available in Ad-Hoc Commands.

H.1.149 Schematron Rules

Description:
A Schematron format rule-set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
Escaped XML

Config file XML Option:
schematron

Other Info:
Update requires server restart.

H.1.150 XEP-0258 Security Label Format

Description:
This option specifies the default encoding to use when generating security labels (as described in XEP-0258).

Syntax:
String (Mandatory)

Options:
xep258ess - XEP 258 ESS

isode - Isode

nato-xcl - NXL (Experimental)

x400 - X.400/X.500 (Experimental)

Default Value:
xep258ess

Example:
isode

Config file XML Option:
xep258_format

Other Info:
Update does not require server restart. Shared only option.

H.1.151 CDCIE CCP Enabled

Description:
This option enables/disables transparent support for locally connected CDCIE CCP clients such as 'TransVerse'.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
cdcie_ccp

Other Info:
Update does not require server restart. Shared only option.

H.1.152 Inject FLOT for labels

Description:
This option enables/disables First-Line-Of-Text (FLOT) injection in stanzas sent to clients which do not advertise support for security labels (as described in XEP-0258) or CDCIE CCP.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
flot

Other Info:
Update does not require server restart. Shared only option.

H.1.153 Inject FLOT for default labels

Description:
This option, when false, disables injection of a FLOT when stanza label is the default label.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
flot_default

Other Info:
Update does not require server restart. Shared only option.

H.1.154 Provide default labels

Description:
This option, when false, disables inclusion of a stanza label when it is the default label.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
provide_default

Other Info:
Update does not require server restart. Shared only option.

H.1.155 Deny unrecognized XEP 258 labels

Description:
When true (default), access to stanzas with unrecognized XEP 258 labels will be denied. When false, unrecognized XEP 258 labels will be treated as equivalent to the security policy's default label.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
sio_deny_unrecognized_labels

Other Info:
Update does not require server restart. Shared only option.

H.1.156 Deny unrecognized CDCIE CCP labels

Description:
When true (default), access to stanzas with unrecognized CDCIE CCP labels will be denied. When false, unrecognized CDCIE CCP labels will be treated as equivalent to the security policy's default label.

Syntax:
Boolean (Mandatory)

Default Value:
true

Example:
false

Config file XML Option:
sio_deny_unrecognized_cdcie_ccp_labels

Other Info:
Update does not require server restart. Shared only option.

H.1.157 Interval between AuthDB refreshes

Description:
Interval in seconds between refreshes of AuthDB provider data.

Syntax:
Numeric (Mandatory)

Default Value:
60

Example:
120

Config file XML Option:
authdb_refresh

Other Info:
Update does not require server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.158 Excluded LDAP attributes

Description:
List of LDAP attributes M-Link will not fetch from the LDAP server. Excluding attributes may have operational implications for the server.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
jpegPhoto

Config file XML Option:
authdb_excluded_ldap_attribute

Other Info:
Update does not require server restart. Advanced option - not available in Ad-Hoc Commands.

H.1.159 AuthDB timestamp window

Description:
When refreshing LDAP entries, AuthDB will try to find users modified since this many seconds before the newest object it already knows about.

Syntax:
Numeric (Mandatory)

Default Value:
10

Example:
20

Config file XML Option:
authdb_ldap_timestamp_window

Other Info:
Update does not require server restart. Advanced option - not available in Ad-Hoc Commands.

H.2 SIO Options

This section describes each SIO configuration option.

Ad-Hoc Commands:

- See Section G.26, “Set SIO Configuration (Shared)”.
- See Section G.27, “Set SIO Configuration (Node)”.

The parent XML element in the configuration file is `<ms_options>`.

H.2.1 Security Policy (SPIF) File

Description:
This option specifies the security (label) policy of the server or peer for which it is defined. The server's security policy option enables and generally governs security label processing. It is generally a pre-requisite for all other security label options.

A peer control may optionally have a relabel out policy, which if set is used instead of the server policy in generating markings and equivalent labels in that peer's relabel out functions.

The contents are in the Open XML Security Policy Information File (SPIF) format.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/policy.xml

Config file XML Option:
sio_policy_file

Other Info:
Update requires server restart.

H.2.2 XEP-0258 Security Label Catalog File

Description:
This option specifies a catalog of security labels for this server.

This catalog is used to generate catalogs of labels returned to clients. Generated catalogs are filtered by applicable clearances.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

This option is an alternative to the 'Security Label Catalog File' option and trumps it if both are specified.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/xep258_label_catalog.xml

Config file XML Option:
xep258_label_catalog_file

Other Info:
Update does not require server restart.

H.2.3 Security Label Catalog File

Description:
This option specifies a catalog of security labels for this server.

This catalog is used to generate catalogs of labels returned to clients.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

This option is an alternative to the 'XEP-0258 Security Label Catalog File' option and is trumped by it if both are specified.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/label_catalog.xml

Config file XML Option:
sio_label_catalog_file

Other Info:
Update does not require server restart.

H.2.4 Clearance Catalog File

Description:
This option specifies the clearance catalog of this server.

This catalog is used to generate catalogs of clearances returned to clients.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/clearance_catalog.xml

Config file XML Option:
sio_clearance_catalog_file

Other Info:
Update does not require server restart.

H.2.5 Security Label File

Description:
This option specifies the security label of the server or domain for which it is defined. This restricts access to the entity to only those users and peers with sufficient clearance.

If the label has not been specified for the server, server access is restricted by the policy default label. If the label is not specified for the domain, access will be governed solely by the server's label.

When specified for a peer, it indicates to relabel to the specified label using the relabel out 'Security Policy (SPIF) XML' option, if set, else the server's 'Security Policy (SPIF) XML' option.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lConfidential.xml

Config file XML Option:
sio_label_file

Other Info:
Update requires server restart.

H.2.6 Clearance File

Description:
This option specifies the security clearance of the server, domain or peer for which it is defined, controlling which labeled contents may be handled by that entity. For instance, any message that has a label denying access to the peer clearance will not be sent to the peer and rejected if received from the peer.

If the clearance has not been specified for the server, no server-wide traffic restrictions exist. If the clearance has not been specified for an XMPP domain, then it inherits the restrictions of the server.

If the clearance has not been specified for the peer, then traffic is restricted by the default clearance specified in the server's security policy. The peer's clearance is also used in authorization decisions in accesses by the peer's users.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cRestricted.xml

Config file XML Option:
sio_clearance_file

Other Info:
Update does not require server restart.

H.2.7 Default Stanza Security Label File

Description:
This option specifies the security label to be applied to any unlabeled stanza sent to or from the server, domain or peer for which it is defined.

If the default label has not been specified for the server, the policy default label applies. If the default label is not specified for the domain, the domain will inherit the default label of the server.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lRestricted.xml

Config file XML Option:
sio_default_label_file

Other Info:
Update does not require server restart.

H.2.8 Default User Clearance File

Description:
This option specifies the security clearance to be applied to an authenticated user that has no otherwise specified applicable clearance. It is used instead of the default clearance specified in the policy.

It is used in deployments where all authenticated local users of a server have at minimum a clearance different from the policy default clearance, allowing the deployment to only maintain per-user clearance attributes for users which exceed this minumum.

It applies to all authenticated local users of the server for which it is defined.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cSecret.xml

Config file XML Option:
sio_default_clearance_file

Other Info:
Update requires server restart.

H.3 Domains Options

This section describes each domain configuration option.

Ad-Hoc Commands:

- See Section G.30, “Get Domain Configuration”.
- See Section G.31, “Add Domain Configuration”.
- See Section G.32, “Modify Domain Configuration”.
- See Section G.33, “Delete Domain Configuration”.

H.3.1 Instant Messaging Domain

The parent XML element in the configuration file is `<ms_options><multidomain><domain>`.

H.3.1.1 Domain Name

Description:
This specifies the name of the domain.

In XMPP, domains are used to identify both instant messaging services, such as 'example.com' in 'joe@example.com', and other services, such as Multi-User Chat.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
test.example.com

Config file XML Option:
Attribute 'name' of parent element

Other Info:
Update does not require server restart. Shared only option.

H.3.1.2 Domain Type

Description:
This specifies the type of the domain.

Syntax:
String (Mandatory)

Options:
IM - Instant Messaging Domain

MUC - Multi-User Chat Domain

PubSub - Publish-Subscribe Domain

Default Value:
-None-

Example:
IM

Config file XML Option:
Parent element 'domain', 'muc_domain', or 'pubsub_domain', depending on the type of domain

Other Info:
Update does not require server restart. Shared only option.

H.3.1.3 Child MUC Domains

Description:
This specifies the list of child Multi-User Chat (MUC) domains held under this domain.

Each instant messaging domain typically has at least one Multi-User Chat which is considered local to, or subordinate to, that service, and clients may discover this hierarchy by querying the server using Service Discovery or 'Disco' service (XEP-0030).

M-Link’s implementation supports multiple MUC domains per IM domain.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
muc.example.com

Config file XML Option:
Attribute 'name' of each element 'muc_domain'

Other Info:
Update does not require server restart. Shared only option.

H.3.1.4 Child PubSub Domains

Description:
This specifies the list of child Publish-Subscribe (PubSub) domains held under this domain.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
pubsub.example.com

Config file XML Option:
Attribute 'name' of each element 'pubsub_domain'

Other Info:
Update does not require server restart. Shared only option.

H.3.1.5 Child Component Domains

Description:
This specifies the list of child component domains (described in XEP-0114) held under this domain.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
component.example.com

Config file XML Option:
Attribute 'name' of each element 'component'

Other Info:
Update does not require server restart. Shared only option.

H.3.1.6 Service Name

Description:
This is the friendly name of the domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
XMPP Service

Config file XML Option:
name

Other Info:
Update does not require server restart. Shared only option.

H.3.1.7 Authentication Backend

Description:
This specifies the type of the authentication backend.

Syntax:
String (Mandatory)

Options:
anonymous - anonymous

XMLDB - XMLDB

LDAP - LDAP

AUTHP - AUTHP

Default Value:
-None-

Example:
LDAP

Config file XML Option:
auth_backend

Other Info:
Update does not require server restart. Shared only option.

H.3.1.8 XMLDB User File

Description:
This option specifies a path to the XMLDB file which may be used as a lightweight authentication database for small, constrained, deployments. This option is only used when the 'Authentication Backend' is 'XMLDB'. Please contact Isode support for further information.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/xmldb.xml

Config file XML Option:
auth_xml

Other Info:
Update does not require server restart. Shared only option.

H.3.1.9 LDAP Server URL

Description:
This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
ldaps://secure.example.com

Config file XML Option:
auth_ldap_uri

Other Info:
Update does not require server restart. Shared only option.

H.3.1.10 LDAP TLS Certificate

Description:
This specifies the domain's LDAP certificate.

The certificate format is PEM ('.pem' extension).

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIC0zCCAjygAwIBAgIKem7/6HDBqxaYpjANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjUxMjM0NDRaFw0xMzEwMjUxMjM0NDRaMB4xHDAaBgNV

BAMTE2ltLmxvbmRvbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ

AoGBAK8zoVsFcX1/mYJDMb0gfdjQ2w8l0JFOKy1VpkIT+p7oYm3EDj530zxv7JVV

4gflkOhyfz7eIP6/CFRo0iuGDQsudM+5FyS3tBCCcSbyiIH+jiJFhyp3ciozwN2h

pWQLeRV1XcCqychzVZHKtNhMk0FOweA7257mYDxHsvuCDShvAgMBAAGjggEnMIIB

IzCBowYDVR0RBIGbMIGYghNpbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLXNlcnZlci5pbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLWNsaWVudC5pbS5sb25kb24uaXNvZGUubmV0oCEGCCsGAQUFBwgF

oBUME2ltLmxvbmRvbi5pc29kZS5uZXQwDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB

/wQCMAAwHQYDVR0OBBYEFKIbfUlRLeHoAfFarJOtWkYDY6JmMD4GA1UdIwQ3MDWA

FCKcUg/+XPHfYvZ2Osxq0LSnDg68oRGkDzANMQswCQYDVQQKEwJDQYIKIBN/w92X

qfsbQTANBgkqhkiG9w0BAQUFAAOBgQBvNPjGelpVYMauqMfmXUCrSc4x2ymzTdUv

IbF+1Bg5NoJqTZCnH4R19VSpv1gNyuunOjDXT89c5SM3GSK4XWC439RU7W9Tdxqy

Si8jKRP2pLia27lAdQGR7X8aTThaifLXv02PcxMozkvYrt782XSrSix6vV9L/N/C

uJvEEz/fxQ==

-----END CERTIFICATE-----

Config file XML Option:
authldap_tls_cert

Other Info:
Update does not require server restart. Shared only option.

H.3.1.11 LDAP TLS Key

Description:
This specifies the private key belonging to the LDAP TLS certificate, if any, for the domain.

The key format is PEM.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,19B5B03D190DDF64

eyYMX7We12IjbROImeu4KSPzT2ARJjmRAJwlx/Y+Xut12OGmrwaCWc8CIlJvqnik

FGrJT5npbLQI+pXPNi7Xypj7LCyCR9xZNd1X7ST9/1ScAuLiPKzo3toIkZN2s2FQ

PSwuBVuXAevFUsfPN9jpaN9eatH6lV48SMInb+WAqi5xlb1EpZmXy86JI9GDnZay

Q5a8Do4JJ4vYKXKjPdG6T4rEcLB3+Hp4MmwMI0Rhkx+9ppNSpSB+9cgzIlz/qtTB

NsauhqwlhUKBZ2eC6kmj9J7ky7N0aePw4o93K1PuHBcBBiFaJpojwg1P9MbzTF4S

9HJW5+56e2qkE0bTZKQz005NBDCbN1pH+B40rMgPQjs2EWSQa3Z1QHgdjFpQa7xg

Xqfb0A2G0fkFN5ROULOvAJhLFLJkOSd0mS7e+olDE+mjbqXD5LNUsRWxAlFXpbOA

zRbSRdlwl4F0Grga4CKJr8Nkog8Aj5W45QiKCHee1woZbi/p5Y3dHOnw4I7DxHLH

y5HGxf2+h+upii/CIZ7EaisdazZwnOdM/rdl7jJ50mWkgg+WDR9DxghJBmop41KP

Zh6C5hXScCg4UIMUYSZG3SXJPsXeWmMwDQiTN5Wo9Bg+GBlcP7TyjSJtCEHOf2hs

Fk7QyyIcjWdkLYwtIB2nTLg6lLlVh85Sivgn4HYVXY1S3ZxUwgnGAXjY0uop+ekM

9GTdODRv0FK2CDjmPVVLHUctKqmj64RntMFObCebV2H5TswALTwOOIK5LEW6vitn

JZOhCZtiqXx8u2O7fWsHAfP/FJ631O+sj193h1o9hnt6xpa2vcLg6w==

-----END RSA PRIVATE KEY-----

Config file XML Option:
authldap_tls_key

Other Info:
Update does not require server restart. Shared only option.

H.3.1.12 LDAP TLS Key Password

Description:
This specifies the password used to decrypt the LDAP private key.

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
s3cret!

Config file XML Option:
authldap_tls_key_password

Other Info:
Update does not require server restart. Shared only option.

H.3.1.13 LDAP Authentication Identity

Description:
It is the DN (or DN equivalent) for LDAP Simple authentication. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
cn=Manager,o=Corp,c=US

Config file XML Option:
auth_ldap_authcid

Other Info:
Update does not require server restart. Shared only option.

H.3.1.14 LDAP Password

Description:
Password for use in LDAP Simple authentication. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
supersecret

Config file XML Option:
auth_ldap_password

Other Info:
Update does not require server restart. Shared only option.

H.3.1.15 LDAP Users Base

Description:
This option specifies the search base DN for users in the LDAP server. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
cn=Users,o=XMPP

Config file XML Option:
auth_ldap_user_base

Other Info:
Update does not require server restart. Shared only option.

H.3.1.16 LDAP User Attribute

Description:
This option specifies the attribute used to match the JID. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
mail

Example:
mail

Config file XML Option:
auth_ldap_user_attr

Other Info:
Update does not require server restart. Shared only option.

H.3.1.17 LDAP Users Scope

Description:
This option specifies the search scope for user objects in the LDAP server. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Options:
subtree - Subtree

onelevel - Onelevel

base - Base

Default Value:
onelevel

Example:
subtree

Config file XML Option:
auth_ldap_user_scope

Other Info:
Update does not require server restart. Shared only option.

H.3.1.18 LDAP Users Filter

Description:
This option specifies an additional LDAP search filter used in the selection of user entries in the LDAP server. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
(objectclass=user)

Config file XML Option:
auth_ldap_user_filter

Other Info:
Update does not require server restart. Shared only option.

H.3.1.19 LDAP User ID Rules

Description:
This is an XML blob constructed from an ordered set of rules. Each rule looks like <rule><match>match-value</match><replace>replacement-value</replace></rule>. All rules are enclosed in the <userid_rules>..</userid_rules> element.

This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
<userid_rules>

<rule><match>+</match><replace>.</replace></rule>

<rule><match>(@.*)</match><replace>@</replace></rule>

<rule><match>@$</match><replace>@example.com</replace></rule>

</userid_rules>

Config file XML Option:
auth_ldap_userid_rules

Other Info:
Update does not require server restart. Shared only option.

H.3.1.20 LDAP Groups Base

Description:
This option specifies the search base DN for groups in the LDAP server. All groups within the group search scope matching the optional filter will automatically be added to the system. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
cn=Groups,o=XMPP

Config file XML Option:
auth_ldap_group_base

Other Info:
Update does not require server restart. Shared only option.

H.3.1.21 LDAP Groups Scope

Description:
This option specifies the search scope for groups in the LDAP server. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Options:
subtree - Subtree

onelevel - Onelevel

base - Base

Default Value:
onelevel

Example:
subtree

Config file XML Option:
auth_ldap_group_scope

Other Info:
Update does not require server restart. Shared only option.

H.3.1.22 LDAP Groups Filter

Description:
This option specifies an addtional LDAP search filter used in the selection of group entries in the LDAP server. This option is only used when the 'Authentication Backend' is 'LDAP'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
(objectclass=group)

Config file XML Option:
auth_ldap_group_filter

Other Info:
Update does not require server restart. Shared only option.

H.3.1.23 Domain Administrators

Description:
The users of the group configured here will have special admin privileges over the domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
example.com/group;local;name:admins

Config file XML Option:
domain_admins

Other Info:
Update does not require server restart. Shared only option.

H.3.1.24 TLS Certificate

Description:
This specifies the domain's certificate. If this option and the option 'TLS Certificate File' is not specified, the TLS certificate of the parent domain will be used (if a parent domain exists), or else the server's TLS certificate will be used.

The certificate format is PEM ('.pem' extension).

TLS must be available for the server before it is configured for a domain.

This option is ignored if the option 'TLS Certificate File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIC0zCCAjygAwIBAgIKem7/6HDBqxaYpjANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjUxMjM0NDRaFw0xMzEwMjUxMjM0NDRaMB4xHDAaBgNV

BAMTE2ltLmxvbmRvbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ

AoGBAK8zoVsFcX1/mYJDMb0gfdjQ2w8l0JFOKy1VpkIT+p7oYm3EDj530zxv7JVV

4gflkOhyfz7eIP6/CFRo0iuGDQsudM+5FyS3tBCCcSbyiIH+jiJFhyp3ciozwN2h

pWQLeRV1XcCqychzVZHKtNhMk0FOweA7257mYDxHsvuCDShvAgMBAAGjggEnMIIB

IzCBowYDVR0RBIGbMIGYghNpbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLXNlcnZlci5pbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLWNsaWVudC5pbS5sb25kb24uaXNvZGUubmV0oCEGCCsGAQUFBwgF

oBUME2ltLmxvbmRvbi5pc29kZS5uZXQwDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB

/wQCMAAwHQYDVR0OBBYEFKIbfUlRLeHoAfFarJOtWkYDY6JmMD4GA1UdIwQ3MDWA

FCKcUg/+XPHfYvZ2Osxq0LSnDg68oRGkDzANMQswCQYDVQQKEwJDQYIKIBN/w92X

qfsbQTANBgkqhkiG9w0BAQUFAAOBgQBvNPjGelpVYMauqMfmXUCrSc4x2ymzTdUv

IbF+1Bg5NoJqTZCnH4R19VSpv1gNyuunOjDXT89c5SM3GSK4XWC439RU7W9Tdxqy

Si8jKRP2pLia27lAdQGR7X8aTThaifLXv02PcxMozkvYrt782XSrSix6vV9L/N/C

uJvEEz/fxQ==

-----END CERTIFICATE-----

Config file XML Option:
tls_cert

Other Info:
Update requires server restart.

H.3.1.25 TLS Certificate File

Description:
This specifies the full path to a file corresponding to the option 'TLS Certificate'.

The certificate format can be either PEM ('.pem') or PKCS#12 ('.p12').

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.p12

Config file XML Option:
tls_cert_file

Other Info:
Update requires server restart.

H.3.1.26 TLS Key

Description:
This specifies the private key belonging to the domain certificate, if any.

The key format is PEM.

If this option and the option 'TLS Key File' are not set, the value of the 'TLS Certificate' or 'TLS Certificate File' is used.

This option and 'TLS Key File' are not used when 'TLS Certificate File' has PKCS#12 format.

This option is ignored if the option 'TLS Key File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,19B5B03D190DDF64

eyYMX7We12IjbROImeu4KSPzT2ARJjmRAJwlx/Y+Xut12OGmrwaCWc8CIlJvqnik

FGrJT5npbLQI+pXPNi7Xypj7LCyCR9xZNd1X7ST9/1ScAuLiPKzo3toIkZN2s2FQ

PSwuBVuXAevFUsfPN9jpaN9eatH6lV48SMInb+WAqi5xlb1EpZmXy86JI9GDnZay

Q5a8Do4JJ4vYKXKjPdG6T4rEcLB3+Hp4MmwMI0Rhkx+9ppNSpSB+9cgzIlz/qtTB

NsauhqwlhUKBZ2eC6kmj9J7ky7N0aePw4o93K1PuHBcBBiFaJpojwg1P9MbzTF4S

9HJW5+56e2qkE0bTZKQz005NBDCbN1pH+B40rMgPQjs2EWSQa3Z1QHgdjFpQa7xg

Xqfb0A2G0fkFN5ROULOvAJhLFLJkOSd0mS7e+olDE+mjbqXD5LNUsRWxAlFXpbOA

zRbSRdlwl4F0Grga4CKJr8Nkog8Aj5W45QiKCHee1woZbi/p5Y3dHOnw4I7DxHLH

y5HGxf2+h+upii/CIZ7EaisdazZwnOdM/rdl7jJ50mWkgg+WDR9DxghJBmop41KP

Zh6C5hXScCg4UIMUYSZG3SXJPsXeWmMwDQiTN5Wo9Bg+GBlcP7TyjSJtCEHOf2hs

Fk7QyyIcjWdkLYwtIB2nTLg6lLlVh85Sivgn4HYVXY1S3ZxUwgnGAXjY0uop+ekM

9GTdODRv0FK2CDjmPVVLHUctKqmj64RntMFObCebV2H5TswALTwOOIK5LEW6vitn

JZOhCZtiqXx8u2O7fWsHAfP/FJ631O+sj193h1o9hnt6xpa2vcLg6w==

-----END RSA PRIVATE KEY-----

Config file XML Option:
tls_key

Other Info:
Update requires server restart.

H.3.1.27 TLS Key File

Description:
This specifies the full path to a PEM file ('.pem' extension) corresponding to the option 'TLS Key'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.key

Config file XML Option:
tls_key_file

Other Info:
Update requires server restart.

H.3.1.28 TLS Key Password

Description:
This specifies the password used to decrypt the domain's private key.

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
s3cret!

Config file XML Option:
tls_key_password

Other Info:
Update requires server restart.

H.3.1.29 Allow Non-SASL Authentication

Description:
If this is set to 'true', then Non-SASL authentication as defined in XEP-0078 is allowed on this domain.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
xep_78

Other Info:
Update does not require server restart. Shared only option.

H.3.1.30 Allow Anonymous Sessions

Description:
If this is set to 'true', then the domain will only allow SASL ANONYMOUS mechanism for client authentication, as specified in XEP-0175.

A change to this option will only affect new sessions.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
anonymous

Other Info:
Update does not require server restart. Shared only option.

H.3.1.31 Archiving

Description:
This option specifies what will be archived.

Syntax:
String (Mandatory)

Options:
none - Do not archive

events-only - Archive events only

all - Archive messages and events

Default Value:
none

Example:
none

Config file XML Option:
archive

Other Info:
Update does not require server restart. Shared only option.

H.3.1.32 Enable XEP-0313 Archives Access (MAM)

Description:
Allow XMPP Message Archive Management (XEP-0313) queries on this domain. MAM will only be advertised to clients when this option is enabled. This option can only be effective when archiving is active.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
mam

Other Info:
Update does not require server restart. Shared only option.

H.3.1.33 Fallback to Default User Clearance for authorization

Description:
If set, the Default User Clearance will be used to determine whether a user is authorized to log in when a domain or the M-Link service is configured with a Security Label, and the LDAP server does not return a clearance for the user.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
authz_fallback_to_default_clearance

Other Info:
Update does not require server restart. Shared only option.

H.3.1.34 Security Label File

Description:
This option specifies the security label of the server or domain for which it is defined. This restricts access to the entity to only those users and peers with sufficient clearance.

If the label has not been specified for the server, server access is restricted by the policy default label. If the label is not specified for the domain, access will be governed solely by the server's label.

When specified for a peer, it indicates to relabel to the specified label using the relabel out 'Security Policy (SPIF) XML' option, if set, else the server's 'Security Policy (SPIF) XML' option.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lConfidential.xml

Config file XML Option:
sio_label_file

Other Info:
Update requires server restart.

H.3.1.35 Clearance File

Description:
This option specifies the security clearance of the server, domain or peer for which it is defined, controlling which labeled contents may be handled by that entity. For instance, any message that has a label denying access to the peer clearance will not be sent to the peer and rejected if received from the peer.

If the clearance has not been specified for the server, no server-wide traffic restrictions exist. If the clearance has not been specified for an XMPP domain, then it inherits the restrictions of the server.

If the clearance has not been specified for the peer, then traffic is restricted by the default clearance specified in the server's security policy. The peer's clearance is also used in authorization decisions in accesses by the peer's users.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cRestricted.xml

Config file XML Option:
sio_clearance_file

Other Info:
Update does not require server restart.

H.3.1.36 Default Stanza Security Label File

Description:
This option specifies the security label to be applied to any unlabeled stanza sent to or from the server, domain or peer for which it is defined.

If the default label has not been specified for the server, the policy default label applies. If the default label is not specified for the domain, the domain will inherit the default label of the server.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lRestricted.xml

Config file XML Option:
sio_default_label_file

Other Info:
Update does not require server restart.

H.3.1.37 Default User Clearance File

Description:
This option specifies the security clearance to be applied to an authenticated user that has no otherwise specified applicable clearance. It is used instead of the default clearance specified in the policy.

It is used in deployments where all authenticated local users of a server have at minimum a clearance different from the policy default clearance, allowing the deployment to only maintain per-user clearance attributes for users which exceed this minumum.

It applies to all authenticated local users of the server for which it is defined.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cSecret.xml

Config file XML Option:
sio_default_clearance_file

Other Info:
Update requires server restart.

H.3.1.38 JID Filter Mode

Description:
This applies to stanzas according to the JID filter match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'jid_filter'

Other Info:
Update does not require server restart. Shared only option.

H.3.1.39 JID Filter Match Rules Set

Description:
This is the set of rules to be used for JID filtering. Each entry should be set to the recipient (which will be matched with the 'to' attribute of the stanza), followed by a space, and then followed by the sender (which will be matched with the 'from' attribute of the stanza).

The recipient and sender can be specified in any of the following ways:

1) any JID - indicated by specifying '@'

2) any JID at a specified domain - indicated by specifying '@' followed by the domain name, for example, '@example.net'

3) the specified bare JID - for example, fred@example.net

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
@ @example.net

Config file XML Option:
Attribute 'to' of child element 'match' of 'jid_filter' set to the recipient and attribute 'from' of child element 'match' of 'jid_filter' set to the sender

Other Info:
Update does not require server restart. Shared only option.

H.3.1.40 IQ Filter 'From' Mode

Description:
This applies to IQ stanzas from the peer, domain, etc. for which this filter is created, according to the IQ filter 'from' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'from')

Other Info:
Update does not require server restart. Shared only option.

H.3.1.41 IQ Filter 'From' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas from the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.3.1.42 IQ Filter 'To' Mode

Description:
This applies to IQ stanzas directed to the peer, domain, etc. for which this filter is created, according to the IQ filter 'to' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'to')

Other Info:
Update does not require server restart. Shared only option.

H.3.1.43 IQ Filter 'To' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas directed to the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.3.2 Multi-User Chat Domain

The parent XML element in the configuration file is `<ms_options><multidomain><domain><muc_domain>`.

H.3.2.1 Domain Name

Description:
This specifies the name of the domain.

In XMPP, domains are used to identify both instant messaging services, such as 'example.com' in 'joe@example.com', and other services, such as Multi-User Chat.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
test.example.com

Config file XML Option:
Attribute 'name' of parent element

Other Info:
Update does not require server restart. Shared only option.

H.3.2.2 Domain Type

Description:
This specifies the type of the domain.

Syntax:
String (Mandatory)

Options:
IM - Instant Messaging Domain

MUC - Multi-User Chat Domain

PubSub - Publish-Subscribe Domain

Default Value:
-None-

Example:
IM

Config file XML Option:
Parent element 'domain', 'muc_domain', or 'pubsub_domain', depending on the type of domain

Other Info:
Update does not require server restart. Shared only option.

H.3.2.3 Parent Domain Name

Description:
This specifies the parent Instant Messaging domain under which this domain is held.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
example.com

Config file XML Option:
Attribute 'name' of grandparent element 'domain'

Other Info:
Update does not require server restart. Shared only option.

H.3.2.4 Service Name

Description:
This is the friendly name of the domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
XMPP Service

Config file XML Option:
name

Other Info:
Update does not require server restart. Shared only option.

H.3.2.5 Domain Administrators

Description:
The users of the group configured here will have special admin privileges over the domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
example.com/group;local;name:admins

Config file XML Option:
domain_admins

Other Info:
Update does not require server restart. Shared only option.

H.3.2.6 TLS Certificate

Description:
This specifies the domain's certificate. If this option and the option 'TLS Certificate File' is not specified, the TLS certificate of the parent domain will be used (if a parent domain exists), or else the server's TLS certificate will be used.

The certificate format is PEM ('.pem' extension).

TLS must be available for the server before it is configured for a domain.

This option is ignored if the option 'TLS Certificate File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIC0zCCAjygAwIBAgIKem7/6HDBqxaYpjANBgkqhkiG9w0BAQUFADANMQswCQYD
VQQKEwJDQTAeFw0xMjEwMjUxMjM0NDRaFw0xMzEwMjUxMjM0NDRaMB4xHDAaBgNV
BAMTE2ltLmxvbmRvbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAK8zoVsFcX1/mYJDMb0gfdjQ2w8l0JFOKy1VpkIT+p7oYm3EDj530zxv7JVV
4gflkOhyfz7eIP6/CFRo0iuGDQsudM+5FyS3tBCCcSbyiIH+jiJFhyp3ciozwN2h
pWQLeRV1XcCqychzVZHKtNhMk0FOweA7257mYDxHsvuCDShvAgMBAAGjggEnMIIB
IzCBowYDVR0RBIGbMIGYghNpbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH
oCIWIF94bXBwLXNlcnZlci5pbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH
oCIWIF94bXBwLWNsaWVudC5pbS5sb25kb24uaXNvZGUubmV0oCEGCCsGAQUFBwgF
oBUME2ltLmxvbmRvbi5pc29kZS5uZXQwDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB
/wQCMAAwHQYDVR0OBBYEFKIbfUlRLeHoAfFarJOtWkYDY6JmMD4GA1UdIwQ3MDWA
FCKcUg/+XPHfYvZ2Osxq0LSnDg68oRGkDzANMQswCQYDVQQKEwJDQYIKIBN/w92X
qfsbQTANBgkqhkiG9w0BAQUFAAOBgQBvNPjGelpVYMauqMfmXUCrSc4x2ymzTdUv
IbF+1Bg5NoJqTZCnH4R19VSpv1gNyuunOjDXT89c5SM3GSK4XWC439RU7W9Tdxqy
Si8jKRP2pLia27lAdQGR7X8aTThaifLXv02PcxMozkvYrt782XSrSix6vV9L/N/C
uJvEEz/fxQ==

-----END CERTIFICATE-----

Config file XML Option:
tls_cert

Other Info:
Update requires server restart.

H.3.2.7 TLS Certificate File

Description:
This specifies the full path to a file corresponding to the option 'TLS Certificate'.

The certificate format can be either PEM ('.pem') or PKCS#12 ('.p12').

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.p12

Config file XML Option:
tls_cert_file

Other Info:
Update requires server restart.

H.3.2.8 TLS Key

Description:
This specifies the private key belonging to the domain certificate, if any.

The key format is PEM.

If this option and the option 'TLS Key File' are not set, the value of the 'TLS Certificate' or 'TLS Certificate File' is used.

This option and 'TLS Key File' are not used when 'TLS Certificate File' has PKCS#12 format.

This option is ignored if the option 'TLS Key File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,19B5B03D190DDF64

eyYMX7We12IjbROImeu4KSPzT2ARJjmRAJwlx/Y+Xut12OGmrwaCWc8CIlJvqnik

FGrJT5npbLQI+pXPNi7Xypj7LCyCR9xZNd1X7ST9/1ScAuLiPKzo3toIkZN2s2FQ

PSwuBVuXAevFUsfPN9jpaN9eatH6lV48SMInb+WAqi5xlb1EpZmXy86JI9GDnZay

Q5a8Do4JJ4vYKXKjPdG6T4rEcLB3+Hp4MmwMI0Rhkx+9ppNSpSB+9cgzIlz/qtTB

NsauhqwlhUKBZ2eC6kmj9J7ky7N0aePw4o93K1PuHBcBBiFaJpojwg1P9MbzTF4S

9HJW5+56e2qkE0bTZKQz005NBDCbN1pH+B40rMgPQjs2EWSQa3Z1QHgdjFpQa7xg

Xqfb0A2G0fkFN5ROULOvAJhLFLJkOSd0mS7e+olDE+mjbqXD5LNUsRWxAlFXpbOA

zRbSRdlwl4F0Grga4CKJr8Nkog8Aj5W45QiKCHee1woZbi/p5Y3dHOnw4I7DxHLH

y5HGxf2+h+upii/CIZ7EaisdazZwnOdM/rdl7jJ50mWkgg+WDR9DxghJBmop41KP

Zh6C5hXScCg4UIMUYSZG3SXJPsXeWmMwDQiTN5Wo9Bg+GBlcP7TyjSJtCEHOf2hs

Fk7QyyIcjWdkLYwtIB2nTLg6lLlVh85Sivgn4HYVXY1S3ZxUwgnGAXjY0uop+ekM

9GTdODRv0FK2CDjmPVVLHUctKqmj64RntMFObCebV2H5TswALTwOOIK5LEW6vitn

JZOhCZtiqXx8u2O7fWsHAfP/FJ631O+sj193h1o9hnt6xpa2vcLg6w==

-----END RSA PRIVATE KEY-----

Config file XML Option:
tls_key

Other Info:
Update requires server restart.

H.3.2.9 TLS Key File

Description:
This specifies the full path to a PEM file ('.pem' extension) corresponding to the option 'TLS Key'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.key

Config file XML Option:
tls_key_file

Other Info:
Update requires server restart.

H.3.2.10 TLS Key Password

Description:
This specifies the password used to decrypt the domain's private key.

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
s3cret!

Config file XML Option:
tls_key_password

Other Info:
Update requires server restart.

H.3.2.11 Archiving

Description:
This option specifies what will be archived.

Syntax:
String (Mandatory)

Options:
none - Do not archive

events-only - Archive events only

all - Archive messages and events

Default Value:
none

Example:
none

Config file XML Option:
archive

Other Info:
Update does not require server restart. Shared only option.

H.3.2.12 Enable XEP-0313 Archives Access (MAM)

Description:
Allow XMPP Message Archive Management (XEP-0313) queries on this domain. MAM will only be advertised to clients when this option is enabled. This option can only be effective when archiving is active.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
mam

Other Info:
Update does not require server restart. Shared only option.

H.3.2.13 Security Label File

Description:
This option specifies the security label of the server or domain for which it is defined. This restricts access to the entity to only those users and peers with sufficient clearance.

If the label has not been specified for the server, server access is restricted by the policy default label. If the label is not specified for the domain, access will be governed solely by the server's label.

When specified for a peer, it indicates to relabel to the specified label using the relabel out 'Security Policy (SPIF) XML' option, if set, else the server's 'Security Policy (SPIF) XML' option.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lConfidential.xml

Config file XML Option:
sio_label_file

Other Info:
Update requires server restart.

H.3.2.14 Clearance File

Description:
This option specifies the security clearance of the server, domain or peer for which it is defined, controlling which labeled contents may be handled by that entity. For instance, any message that has a label denying access to the peer clearance will not be sent to the peer and rejected if received from the peer.

If the clearance has not been specified for the server, no server-wide traffic restrictions exist. If the clearance has not been specified for an XMPP domain, then it inherits the restrictions of the server.

If the clearance has not been specified for the peer, then traffic is restricted by the default clearance specified in the server's security policy. The peer's clearance is also used in authorization decisions in accesses by the peer's users.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cRestricted.xml

Config file XML Option:
sio_clearance_file

Other Info:
Update does not require server restart.

H.3.2.15 Default Stanza Security Label File

Description:
This option specifies the security label to be applied to any unlabeled stanza sent to or from the server, domain or peer for which it is defined.

If the default label has not been specified for the server, the policy default label applies. If the default label is not specified for the domain, the domain will inherit the default label of the server.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lRestricted.xml

Config file XML Option:
sio_default_label_file

Other Info:
Update does not require server restart.

H.3.2.16 Default User Clearance File

Description:
This option specifies the security clearance to be applied to an authenticated user that has no otherwise specified applicable clearance. It is used instead of the default clearance specified in the policy.

It is used in deployments where all authenticated local users of a server have at minimum a clearance different from the policy default clearance, allowing the deployment to only maintain per-user clearance attributes for users which exceed this minumum.

It applies to all authenticated local users of the server for which it is defined.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cSecret.xml

Config file XML Option:
sio_default_clearance_file

Other Info:
Update requires server restart.

H.3.2.17 JID Filter Mode

Description:
This applies to stanzas according to the JID filter match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'jid_filter'

Other Info:
Update does not require server restart. Shared only option.

H.3.2.18 JID Filter Match Rules Set

Description:
This is the set of rules to be used for JID filtering. Each entry should be set to the recipient (which will be matched with the 'to' attribute of the stanza), followed by a space, and then followed by the sender (which will be matched with the 'from' attribute of the stanza).

The recipient and sender can be specified in any of the following ways:

1) any JID - indicated by specifying '@'

2) any JID at a specified domain - indicated by specifying '@' followed by the domain name, for example, '@example.net'

3) the specified bare JID - for example, fred@example.net

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
@ @example.net

Config file XML Option:
Attribute 'to' of child element 'match' of 'jid_filter' set to the recipient and attribute 'from' of child element 'match' of 'jid_filter' set to the sender

Other Info:
Update does not require server restart. Shared only option.

H.3.2.19 IQ Filter 'From' Mode

Description:
This applies to IQ stanzas from the peer, domain, etc. for which this filter is created, according to the IQ filter 'from' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'from')

Other Info:
Update does not require server restart. Shared only option.

H.3.2.20 IQ Filter 'From' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas from the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.3.2.21 IQ Filter 'To' Mode

Description:
This applies to IQ stanzas directed to the peer, domain, etc. for which this filter is created, according to the IQ filter 'to' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'to')

Other Info:
Update does not require server restart. Shared only option.

H.3.2.22 IQ Filter 'To' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas directed to the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.3.3 Publish-Subscribe Domain

The parent XML element in the configuration file is `<ms_options><multidomain><domain><pubsub_domain>`.

H.3.3.1 Domain Name

Description:
This specifies the name of the domain.

In XMPP, domains are used to identify both instant messaging services, such as 'example.com' in 'joe@example.com', and other services, such as Multi-User Chat.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
test.example.com

Config file XML Option:
Attribute 'name' of parent element

Other Info:
Update does not require server restart. Shared only option.

H.3.3.2 Domain Type

Description:
This specifies the type of the domain.

Syntax:
String (Mandatory)

Options:
IM - Instant Messaging Domain

MUC - Multi-User Chat Domain

PubSub - Publish-Subscribe Domain

Default Value:
-None-

Example:
IM

Config file XML Option:
Parent element 'domain', 'muc_domain', or 'pubsub_domain', depending on the type of domain

Other Info:
Update does not require server restart. Shared only option.

H.3.3.3 Parent Domain Name

Description:
This specifies the parent Instant Messaging domain under which this domain is held.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
example.com

Config file XML Option:
Attribute 'name' of grandparent element 'domain'

Other Info:
Update does not require server restart. Shared only option.

H.3.3.4 Service Name

Description:
This is the friendly name of the domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
XMPP Service

Config file XML Option:
name

Other Info:
Update does not require server restart. Shared only option.

H.3.3.5 Domain Administrators

Description:
The users of the group configured here will have special admin privileges over the domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
example.com/group;local;name:admins

Config file XML Option:
domain_admins

Other Info:
Update does not require server restart. Shared only option.

H.3.3.6 TLS Certificate

Description:
This specifies the domain's certificate. If this option and the option 'TLS Certificate File' is not specified, the TLS certificate of the parent domain will be used (if a parent domain exists), or else the server's TLS certificate will be used.

The certificate format is PEM ('.pem' extension).

TLS must be available for the server before it is configured for a domain.

This option is ignored if the option 'TLS Certificate File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIC0zCCAjygAwIBAgIKem7/6HDBqxaYpjANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjUxMjM0NDRaFw0xMzEwMjUxMjM0NDRaMB4xHDAaBgNV

BAMTE2ltLmxvbmRvbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ

AoGBAK8zoVsFcX1/mYJDMb0gfdjQ2w8l0JFOKy1VpkIT+p7oYm3EDj530zxv7JVV

4gflkOhyfz7eIP6/CFRo0iuGDQsudM+5FyS3tBCCcSbyiIH+jiJFhyp3ciozwN2h

pWQLeRV1XcCqychzVZHKtNhMk0FOweA7257mYDxHsvuCDShvAgMBAAGjggEnMIIB

IzCBowYDVR0RBIGbMIGYghNpbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLXNlcnZlci5pbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLWNsaWVudC5pbS5sb25kb24uaXNvZGUubmV0oCEGCCsGAQUFBwgF

oBUME2ltLmxvbmRvbi5pc29kZS5uZXQwDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB

/wQCMAAwHQYDVR0OBBYEFKIbfUlRLeHoAfFarJOtWkYDY6JmMD4GA1UdIwQ3MDWA

FCKcUg/+XPHfYvZ2Osxq0LSnDg68oRGkDzANMQswCQYDVQQKEwJDQYIKIBN/w92X

qfsbQTANBgkqhkiG9w0BAQUFAAOBgQBvNPjGelpVYMauqMfmXUCrSc4x2ymzTdUv

IbF+1Bg5NoJqTZCnH4R19VSpv1gNyuunOjDXT89c5SM3GSK4XWC439RU7W9Tdxqy

Si8jKRP2pLia27lAdQGR7X8aTThaifLXv02PcxMozkvYrt782XSrSix6vV9L/N/C

uJvEEz/fxQ==

-----END CERTIFICATE-----

Config file XML Option:
tls_cert

Other Info:
Update requires server restart.

H.3.3.7 TLS Certificate File

Description:
This specifies the full path to a file corresponding to the option 'TLS Certificate'.

The certificate format can be either PEM ('.pem') or PKCS#12 ('.p12').

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.p12

Config file XML Option:
tls_cert_file

Other Info:
Update requires server restart.

H.3.3.8 TLS Key

Description:
This specifies the private key belonging to the domain certificate, if any.

The key format is PEM.

If this option and the option 'TLS Key File' are not set, the value of the 'TLS Certificate' or 'TLS Certificate File' is used.

This option and 'TLS Key File' are not used when 'TLS Certificate File' has PKCS#12 format.

This option is ignored if the option 'TLS Key File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,19B5B03D190DDF64

eyYMX7We12IjbROImeu4KSPzT2ARJjmRAJwlx/Y+Xut12OGmrwaCWc8CIlJvqnik

FGrJT5npbLQI+pXPNi7Xypj7LCyCR9xZNd1X7ST9/1ScAuLiPKzo3toIkZN2s2FQ

PSwuBVuXAevFUsfPN9jpaN9eatH6lV48SMInb+WAqi5xlb1EpZmXy86JI9GDnZay

Q5a8Do4JJ4vYKXKjPdG6T4rEcLB3+Hp4MmwMI0Rhkx+9ppNSpSB+9cgzIlz/qtTB

NsauhqwlhUKBZ2eC6kmj9J7ky7N0aePw4o93K1PuHBcBBiFaJpojwg1P9MbzTF4S

9HJW5+56e2qkE0bTZKQz005NBDCbN1pH+B40rMgPQjs2EWSQa3Z1QHgdjFpQa7xg

Xqfb0A2G0fkFN5ROULOvAJhLFLJkOSd0mS7e+olDE+mjbqXD5LNUsRWxAlFXpbOA

zRbSRdlwl4F0Grga4CKJr8Nkog8Aj5W45QiKCHee1woZbi/p5Y3dHOnw4I7DxHLH

y5HGxf2+h+upii/CIZ7EaisdazZwnOdM/rdl7jJ50mWkgg+WDR9DxghJBmop41KP

Zh6C5hXScCg4UIMUYSZG3SXJPsXeWmMwDQiTN5Wo9Bg+GBlcP7TyjSJtCEHOf2hs

Fk7QyyIcjWdkLYwtIB2nTLg6lLlVh85Sivgn4HYVXY1S3ZxUwgnGAXjY0uop+ekM

9GTdODRv0FK2CDjmPVVLHUctKqmj64RntMFObCebV2H5TswALTwOOIK5LEW6vitn

JZOhCZtiqXx8u2O7fWsHAfP/FJ631O+sj193h1o9hnt6xpa2vcLg6w==

-----END RSA PRIVATE KEY-----

Config file XML Option:
tls_key

Other Info:
Update requires server restart.

H.3.3.9 TLS Key File

Description:
This specifies the full path to a PEM file ('.pem' extension) corresponding to the option 'TLS Key'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.key

Config file XML Option:
tls_key_file

Other Info:
Update requires server restart.

H.3.3.10 TLS Key Password

Description:
This specifies the password used to decrypt the domain's private key.

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
s3cret!

Config file XML Option:
tls_key_password

Other Info:
Update requires server restart.

H.3.3.11 Additional Identity Type

Description:
If set, an additional identity element with this type will be returned for disco#info queries to this domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
urn:xmpp:fdp:0

Config file XML Option:
identity_type

Other Info:
Update does not require server restart. Shared only option.

H.3.3.12 Archiving

Description:
This option specifies what will be archived.

Syntax:
String (Mandatory)

Options:
none - Do not archive

events-only - Archive events only

all - Archive messages and events

Default Value:
none

Example:
none

Config file XML Option:
archive

Other Info:
Update does not require server restart. Shared only option.

H.3.3.13 Enable XEP-0313 Archives Access (MAM)

Description:
Allow XMPP Message Archive Management (XEP-0313) queries on this domain. MAM will only be advertised to clients when this option is enabled. This option can only be effective when archiving is active.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
mam

Other Info:
Update does not require server restart. Shared only option.

H.3.3.14 Security Label File

Description:
This option specifies the security label of the server or domain for which it is defined. This restricts access to the entity to only those users and peers with sufficient clearance.

If the label has not been specified for the server, server access is restricted by the policy default label. If the label is not specified for the domain, access will be governed solely by the server's label.

When specified for a peer, it indicates to relabel to the specified label using the relabel out 'Security Policy (SPIF) XML' option, if set, else the server's 'Security Policy (SPIF) XML' option.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lConfidential.xml

Config file XML Option:
sio_label_file

Other Info:
Update requires server restart.

H.3.3.15 Clearance File

Description:
This option specifies the security clearance of the server, domain or peer for which it is defined, controlling which labeled contents may be handled by that entity. For instance, any message that has a label denying access to the peer clearance will not be sent to the peer and rejected if received from the peer.

If the clearance has not been specified for the server, no server-wide traffic restrictions exist. If the clearance has not been specified for an XMPP domain, then it inherits the restrictions of the server.

If the clearance has not been specified for the peer, then traffic is restricted by the default clearance specified in the server's security policy. The peer's clearance is also used in authorization decisions in accesses by the peer's users.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cRestricted.xml

Config file XML Option:
sio_clearance_file

Other Info:
Update does not require server restart.

H.3.3.16 Default Stanza Security Label File

Description:
This option specifies the security label to be applied to any unlabeled stanza sent to or from the server, domain or peer for which it is defined.

If the default label has not been specified for the server, the policy default label applies. If the default label is not specified for the domain, the domain will inherit the default label of the server.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lRestricted.xml

Config file XML Option:
sio_default_label_file

Other Info:
Update does not require server restart.

H.3.3.17 Default User Clearance File

Description:
This option specifies the security clearance to be applied to an authenticated user that has no otherwise specified applicable clearance. It is used instead of the default clearance specified in the policy.

It is used in deployments where all authenticated local users of a server have at minimum a clearance different from the policy default clearance, allowing the deployment to only maintain per-user clearance attributes for users which exceed this minumum.

It applies to all authenticated local users of the server for which it is defined.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cSecret.xml

Config file XML Option:
sio_default_clearance_file

Other Info:
Update requires server restart.

H.3.3.18 JID Filter Mode

Description:
This applies to stanzas according to the JID filter match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'jid_filter'

Other Info:
Update does not require server restart. Shared only option.

H.3.3.19 JID Filter Match Rules Set

Description:
This is the set of rules to be used for JID filtering. Each entry should be set to the recipient (which will be matched with the 'to' attribute of the stanza), followed by a space, and then followed by the sender (which will be matched with the 'from' attribute of the stanza).

The recipient and sender can be specified in any of the following ways:

1) any JID - indicated by specifying '@'

2) any JID at a specified domain - indicated by specifying '@' followed by the domain name, for example, '@example.net'

3) the specified bare JID - for example, fred@example.net

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
@ @example.net

Config file XML Option:
Attribute 'to' of child element 'match' of 'jid_filter' set to the recipient and attribute 'from' of child element 'match' of 'jid_filter' set to the sender

Other Info:
Update does not require server restart. Shared only option.

H.3.3.20 IQ Filter 'From' Mode

Description:
This applies to IQ stanzas from the peer, domain, etc. for which this filter is created, according to the IQ filter 'from' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'from')

Other Info:
Update does not require server restart. Shared only option.

H.3.3.21 IQ Filter 'From' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas from the peer, domain, etc. for which this filter is created. Each entry should be set to the name of

the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.3.3.22 IQ Filter 'To' Mode

Description:
This applies to IQ stanzas directed to the peer, domain, etc. for which this filter is created, according to the IQ filter 'to' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'to')

Other Info:
Update does not require server restart. Shared only option.

H.3.3.23 IQ Filter 'To' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas directed to the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.4 Components Options

This section describes each component configuration option.

Ad-Hoc Commands:

- See Section G.34, “Get Component Configuration”.
- See Section G.35, “Add Component Configuration”.
- See Section G.36, “Modify Component Configuration”.
- See Section G.37, “Delete Component Configuration”.

H.4.1 Component Domain

The parent XML element in the configuration file is `<ms_options><multidomain><domain><component>`.

H.4.1.1 Domain Name

Description:
This specifies the name of the domain.

In XMPP, domains are used to identify both instant messaging services, such as 'example.com' in 'joe@example.com', and other services, such as Multi-User Chat.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
test.example.com

Config file XML Option:
Attribute 'name' of parent element

Other Info:
Update does not require server restart. Shared only option.

H.4.1.2 Parent Domain Name

Description:
This specifies the parent Instant Messaging domain under which this domain is held.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
example.com

Config file XML Option:
Attribute 'name' of grandparent element 'domain'

Other Info:
Update does not require server restart. Shared only option.

H.4.1.3 Service Name

Description:
This is the friendly name of the domain.

Syntax:
String (Optional)

Default Value:
-None-

Example:
XMPP Service

Config file XML Option:
name

Other Info:
Update does not require server restart. Shared only option.

H.4.1.4 TLS Certificate

Description:
This specifies the domain's certificate. If this option and the option 'TLS Certificate File' is not specified, the TLS certificate of the parent domain will be used (if a parent domain exists), or else the server's TLS certificate will be used.

The certificate format is PEM ('.pem' extension).

TLS must be available for the server before it is configured for a domain.

This option is ignored if the option 'TLS Certificate File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIC0zCCAjygAwIBAgIKem7/6HDBqxaYpjANBgkqhkiG9w0BAQUFADANMQswCQYD

VQQKEwJDQTAeFw0xMjEwMjUxMjM0NDRaFw0xMzEwMjUxMjM0NDRaMB4xHDAaBgNV

BAMTE2ltLmxvbmRvbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ

AoGBAK8zoVsFcX1/mYJDMb0gfdjQ2w8l0JFOKy1VpkIT+p7oYm3EDj530zxv7JVV

4gflkOhyfz7eIP6/CFRo0iuGDQsudM+5FyS3tBCCcSbyiIH+jiJFhyp3ciozwN2h

pWQLeRV1XcCqychzVZHKtNhMk0FOweA7257mYDxHsvuCDShvAgMBAAGjggEnMIIB

IzCBowYDVR0RBIGbMIGYghNpbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLXNlcnZlci5pbS5sb25kb24uaXNvZGUubmV0oC4GCCsGAQUFBwgH

oCIWIF94bXBwLWNsaWVudC5pbS5sb25kb24uaXNvZGUubmV0oCEGCCsGAQUFBwgF

oBUME2ltLmxvbmRvbi5pc29kZS5uZXQwDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB

/wQCMAAwHQYDVR0OBBYEFKIbfUlRLeHoAfFarJOtWkYDY6JmMD4GA1UdIwQ3MDWA

FCKcUg/+XPHfYvZ2Osxq0LSnDg68oRGkDzANMQswCQYDVQQKEwJDQYIKIBN/w92X

qfsbQTANBgkqhkiG9w0BAQUFAAOBgQBvNPjGelpVYMauqMfmXUCrSc4x2ymzTdUv

IbF+1Bg5NoJqTZCnH4R19VSpv1gNyuunOjDXT89c5SM3GSK4XWC439RU7W9Tdxqy

Si8jKRP2pLia27lAdQGR7X8aTThaifLXv02PcxMozkvYrt782XSrSix6vV9L/N/C

uJvEEz/fxQ==

-----END CERTIFICATE-----

Config file XML Option:
tls_cert

Other Info:
Update requires server restart.

H.4.1.5 TLS Certificate File

Description:
This specifies the full path to a file corresponding to the option 'TLS Certificate'.

The certificate format can be either PEM ('.pem') or PKCS#12 ('.p12').

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.p12

Config file XML Option:
tls_cert_file

Other Info:
Update requires server restart.

H.4.1.6 TLS Key

Description:
This specifies the private key belonging to the domain certificate, if any.

The key format is PEM.

If this option and the option 'TLS Key File' are not set, the value of the 'TLS Certificate' or 'TLS Certificate File' is used.

This option and 'TLS Key File' are not used when 'TLS Certificate File' has PKCS#12 format.

This option is ignored if the option 'TLS Key File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,19B5B03D190DDF64

eyYMX7We12IjbROImeu4KSPzT2ARJjmRAJwlx/Y+Xut12OGmrwaCWc8CIlJvqnik

FGrJT5npbLQI+pXPNi7Xypj7LCyCR9xZNd1X7ST9/1ScAuLiPKzo3toIkZN2s2FQ

PSwuBVuXAevFUsfPN9jpaN9eatH6lV48SMInb+WAqi5xlb1EpZmXy86JI9GDnZay

Q5a8Do4JJ4vYKXKjPdG6T4rEcLB3+Hp4MmwMI0Rhkx+9ppNSpSB+9cgzIlz/qtTB

NsauhqwlhUKBZ2eC6kmj9J7ky7N0aePw4o93K1PuHBcBBiFaJpojwg1P9MbzTF4S

9HJW5+56e2qkE0bTZKQz005NBDCbN1pH+B40rMgPQjs2EWSQa3Z1QHgdjFpQa7xg

Xqfb0A2G0fkFN5ROULOvAJhLFLJkOSd0mS7e+olDE+mjbqXD5LNUsRWxAlFXpbOA

zRbSRdlwl4F0Grga4CKJr8Nkog8Aj5W45QiKCHee1woZbi/p5Y3dHOnw4I7DxHLH

y5HGxf2+h+upii/CIZ7EaisdazZwnOdM/rdl7jJ50mWkgg+WDR9DxghJBmop41KP

Zh6C5hXScCg4UIMUYSZG3SXJPsXeWmMwDQiTN5Wo9Bg+GBlcP7TyjSJtCEHOf2hs

Fk7QyyIcjWdkLYwtIB2nTLg6lLlVh85Sivgn4HYVXY1S3ZxUwgnGAXjY0uop+ekM

9GTdODRv0FK2CDjmPVVLHUctKqmj64RntMFObCebV2H5TswALTwOOIK5LEW6vitn

JZOhCZtiqXx8u2O7fWsHAfP/FJ631O+sj193h1o9hnt6xpa2vcLg6w==

-----END RSA PRIVATE KEY-----

Config file XML Option:
tls_key

Other Info:
Update requires server restart.

H.4.1.7 TLS Key File

Description:
This specifies the full path to a PEM file ('.pem' extension) corresponding to the option 'TLS Key'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/extra-domain.key

Config file XML Option:
tls_key_file

Other Info:
Update requires server restart.

H.4.1.8 TLS Key Password

Description:
This specifies the password used to decrypt the domain's private key.

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
s3cret!

Config file XML Option:
tls_key_password

Other Info:
Update requires server restart.

H.4.1.9 Component Key

Description:
This specifies the component password or key for authentication during Jabber component protocol access.

Syntax:
Encrypted String (Optional)

Default Value:
-None-

Example:
s3cret!

Config file XML Option:
component_key

Other Info:
Update does not require server restart. Shared only option.

H.4.1.10 Component Rights

Description:
Access rights for the component

Syntax:
Multi-Valued String (Optional)

Options:
route - Route lookup

roster - Access rosters

subscribe - Subscription access

muc - MUC access

blocklist - Blocklist access

account - Generic account access

admin_server - Administer server

pubsub - PubSub access

all_domains - Allow sending on behalf of all local domains

mam - MAM access

Default Value:
-None-

Example:
-None-

Config file XML Option:
Values of 'acl' children of 'rights' element

Other Info:
Update does not require server restart. Shared only option.

H.4.1.11 Archiving

Description:
This option specifies what will be archived.

Syntax:
String (Mandatory)

Options:
none - Do not archive

all - Archive messages

Default Value:
none

Example:
none

Config file XML Option:
archive

Other Info:
Update does not require server restart. Shared only option.

H.4.1.12 Delegated user IQ XML namespaces

Description:
All IQs sent to bare JIDs of local users with these XML namespaces will be forwarded to the component

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
http://example.com/xmlns

Config file XML Option:
handle_user_iqs

Other Info:
Update does not require server restart. Shared only option.

H.4.1.13 Security Label File

Description:
This option specifies the security label of the server or domain for which it is defined. This restricts access to the entity to only those users and peers with sufficient clearance.

If the label has not been specified for the server, server access is restricted by the policy default label. If the label is not specified for the domain, access will be governed solely by the server's label.

When specified for a peer, it indicates to relabel to the specified label using the relabel out 'Security Policy (SPIF) XML' option, if set, else the server's 'Security Policy (SPIF) XML' option.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lConfidential.xml

Config file XML Option:
sio_label_file

Other Info:
Update requires server restart.

H.4.1.14 Clearance File

Description:
This option specifies the security clearance of the server, domain or peer for which it is defined, controlling which labeled contents may be handled by that entity. For instance, any message that has a label denying access to the peer clearance will not be sent to the peer and rejected if received from the peer.

If the clearance has not been specified for the server, no server-wide traffic restrictions exist. If the clearance has not been specified for an XMPP domain, then it inherits the restrictions of the server.

If the clearance has not been specified for the peer, then traffic is restricted by the default clearance specified in the server's security policy. The peer's clearance is also used in authorization decisions in accesses by the peer's users.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cRestricted.xml

Config file XML Option:
sio_clearance_file

Other Info:
Update does not require server restart.

H.4.1.15 Default Stanza Security Label File

Description:
This option specifies the security label to be applied to any unlabeled stanza sent to or from the server, domain or peer for which it is defined.

If the default label has not been specified for the server, the policy default label applies. If the default label is not specified for the domain, the domain will inherit the default label of the server.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lRestricted.xml

Config file XML Option:
sio_default_label_file

Other Info:
Update does not require server restart.

H.4.1.16 Default User Clearance File

Description:
This option specifies the security clearance to be applied to an authenticated user that has no otherwise specified applicable clearance. It is used instead of the default clearance specified in the policy.

It is used in deployments where all authenticated local users of a server have at minimum a clearance different from the policy default clearance, allowing the deployment to only maintain per-user clearance attributes for users which exceed this minumum.

It applies to all authenticated local users of the server for which it is defined.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cSecret.xml

Config file XML Option:
sio_default_clearance_file

Other Info:
Update requires server restart.

H.4.1.17 JID Filter Mode

Description:
This applies to stanzas according to the JID filter match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'jid_filter'

Other Info:
Update does not require server restart. Shared only option.

H.4.1.18 JID Filter Match Rules Set

Description:
This is the set of rules to be used for JID filtering. Each entry should be set to the recipient (which will be matched with the 'to' attribute of the stanza), followed by a space, and then followed by the sender (which will be matched with the 'from' attribute of the stanza).

The recipient and sender can be specified in any of the following ways:

1) any JID - indicated by specifying '@'

2) any JID at a specified domain - indicated by specifying '@' followed by the domain name, for example, '@example.net'

3) the specified bare JID - for example, fred@example.net

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
@ @example.net

Config file XML Option:
Attribute 'to' of child element 'match' of 'jid_filter' set to the recipient and attribute 'from' of child element 'match' of 'jid_filter' set to the sender

Other Info:
Update does not require server restart. Shared only option.

H.4.1.19 IQ Filter 'From' Mode

Description:
This applies to IQ stanzas from the peer, domain, etc. for which this filter is created, according to the IQ filter 'from' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'from')

Other Info:
Update does not require server restart. Shared only option.

H.4.1.20 IQ Filter 'From' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas from the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.4.1.21 IQ Filter 'To' Mode

Description:
This applies to IQ stanzas directed to the peer, domain, etc. for which this filter is created, according to the IQ filter 'to' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'to')

Other Info:
Update does not require server restart. Shared only option.

H.4.1.22 IQ Filter 'To' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas directed to the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.5 Groups Options

This section describes each groups configuration option.

Ad-Hoc Commands:

- See Section G.46, “Add Local Group Configuration”.
- See Section G.47, “Modify Local Group Configuration”.
- See Section G.48, “Delete Local Group Configuration”.

The parent XML element in the configuration file is `<ms_options><group>`.

H.5.1 Local Group Name

Description:
This is the name used for presentation and is used to refer to all of the users it contains.

It is also used to construct the local group's JID.

This JID may be used as an entry in the affiliations of a chatroom (or PubSub node), such that all members of that local group will have that affiliation. Note that specific affiliations set for a member will take precedence.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
server-admins

Config file XML Option:
Attribute 'name' of parent element

Other Info:
Update does not require server restart. Shared only option.

H.5.2 Members

Description:
Member JIDs.

Syntax:
Multi-Valued JID (Mandatory)

Default Value:
-None-

Example:
hermann.baumann@example.com

Config file XML Option:
Attribute 'id' of element 'member'

Other Info:
Update does not require server restart. Shared only option.

H.6 Peers Options

This section describes each peer configuration option.

Ad-Hoc Commands:

- See Section G.38, “Get Peer Configuration”.
- See Section G.39, “Add Peer Configuration”.
- See Section G.40, “Modify Peer Configuration”.
- See Section G.41, “Delete Peer Configuration”.

The parent XML element in the configuration file is `<ms_options><peering><peer>`.

H.6.1 Domain

Description:
This is usually set to the domain name. Unless a link is being used to connect to the peer, wildcards can also be used.

The following wildcarding mechanism is used for the domain name - any other wildcards will not match any domain:

1. '*.example.com' applies to all subdomains of 'example.com' but not to 'example.com' itself.

2. '+.example.com' applies to 'example.com' and all of its subdomains.

3. If this option is left empty, then this is assumed to be the default peer control.

Syntax:
String (Optional)

Default Value:
-None-

Example:
+.example.com

Config file XML Option:
Attribute 'domain' of parent element

Other Info:
Update does not require server restart. Shared only option.

H.6.2 Connect To Host

Description:
If specified, traffic for the peer is routed to one of the hosts in this list. Multiple hosts can be specified for failover. Either IP address or hostname can be specified, optionally followed by ':' and a port number. If the port number is absent, it is assumed to be 5269.

This option is ignored if the option 'Connect Link List' is populated.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
edge.example.com:5999

Config file XML Option:
Attribute 'host' of element 'connect'

Other Info:
Update requires server restart. Shared only option.

H.6.3 Connect Link List

Description:
If specified, traffic for the peer is routed to one of the links in this list.

Multiple links can be specified for failover. Note that a link remains in use until it is broken.

Syntax:
Multi-Valued String (Optional)

Options:
-None-

Default Value:
-None-

Example:
links-to-edge

Config file XML Option:
Attribute 'link' of element 'connect'

Other Info:
Update requires server restart.

H.6.4 Deny

Description:
If set to 'true', all XMPP traffic to the peer will be disallowed and connection attempts from the peer will be denied.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'deny' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.5 Require TLS

Description:
If set to 'true', the server requires TLS (possibly unauthenticated) on sessions with the peer.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'require_tls' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.6 Require TLS Authentication

Description:
If set to 'true', the server requires authenticated TLS in sessions it initiates with the peer.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'require_tls_auth' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.7 Require Strong Authentication

Description:
If set to 'true', the server requires peers connecting to it to assert a valid X.509 certificate.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'require_strong_auth' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.8 TLS Certificate(s)

Description:
This specifies PEM-formatted certificates which are sufficient to authenticate the peer.

It is ignored if the option 'TLS Certificate(s) File' is set.

Syntax:
String (Optional)

Default Value:
-None-

Example:
-----BEGIN CERTIFICATE-----

MIIC0zCCAjygAwIBAgIKY9jxz11/UjFYZDANBgkqhkiG9w0BAQUFADASMRAwDgYD

VQQKEwdndXJtZWVuMB4XDTEyMTAxMTE1Mjc0NFoXDTEzMTAxMTE1Mjc0NFowHDEa

MBgGA1UEAxMRZ3VybWVlbi5pc29kZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0A

MIGJAoGBAIN45yMMt/eiM3hmSOOAoV/NCM80B4Fuu7HnUSCaNWJT+HvUf+YIWzEh

c8KaBvOvY6scl5euqXZKCiGfBUuf7b8mo16M0D6JhTw5mHYjU+H7bxEQNX9OcweS

7ZiNB1cBl3LUc/e31LVlaG4z52MJefnF8fzF4C3vr+mCBsE+vqUFAgMBAAGjggEk

MIIBIDCBmwYDVR0RBIGTMIGQghFndXJtZWVuLmlzb2RlLm5ldKAsBggrBgEFBQcI

B6AgFh5feG1wcC1zZXJ2ZXIuZ3VybWVlbi5pc29kZS5uZXSgLAYIKwYBBQUHCAeg

IBYeX3htcHAtY2xpZW50Lmd1cm1lZW4uaXNvZGUubmV0oB8GCCsGAQUFBwgFoBMM

EWd1cm1lZW4uaXNvZGUubmV0MA4GA1UdDwEB/wQEAwIF4DAMBgNVHRMBAf8EAjAA

MB0GA1UdDgQWBBTWgBSrTYUQwALHa8GxT/W4BKm0LzBDBgNVHSMEPDA6gBTtI+61

Mbuq3UaCXAm7PC1PvM25nqEWpBQwEjEQMA4GA1UEChMHZ3VybWVlboIKTXeI0/b+

70cwWzANBgkqhkiG9w0BAQUFAAOBgQAxVfzDpfplNRJRXw6+5fkINS+S78rkgSsw

I2MrTKoZ5JS2X08/jiqWdpFAjmkypoVjlZb4nU/8vsvxBzYSIiAYo6+jmTLqGaQ4

3rtj4JdGeN25ht5D2+j8Vzp98LO7ohUCY7JBrTL1/+JQQUT35/du1LY0nwZY+Guf

vwJsG6BSkQ==

-----END CERTIFICATE-----

Config file XML Option:
tls_cert

Other Info:
Update does not require server restart. Shared only option.

H.6.9 TLS Certificate(s) File

Description:
This specifies the full path to a file containing a PEM ('.pem') certificate(s) corresponding to the option 'TLS Certificate(s)'.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/certs/example.com.pem

Config file XML Option:
tls_cert_file

Other Info:
Update does not require server restart.

H.6.10 Accept Address

Description:
If specified, then S2S connections from the domain will be refused unless made from the specified address.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
10.0.0.1

Config file XML Option:
Attribute 'address' of element 'accept'

Other Info:
Update does not require server restart. Shared only option.

H.6.11 Relay Zone

Description:
This specifies the relay zones for controlling relaying. A stanza will only be forwarded between two remote systems if those two systems are in different zones.

Syntax:
String (Optional)

Default Value:
-None-

Example:
Example-zone

Config file XML Option:
Attribute 'zone' of element 'relay'

Other Info:
Update does not require server restart. Shared only option.

H.6.12 Message Fold Mode

Description:
This applies to message stanzas according to the 'Message Fold Match Rules Set'.

Syntax:
String (Mandatory)

Options:
none - None

keep - The server will pass the matched elements to the peer

strip - The server will not pass the matched elements to the peer

Default Value:
none

Example:
strip

Config file XML Option:
Attribute 'mode' of element 'message_fold'

Other Info:
Update does not require server restart. Shared only option.

H.6.13 Message Fold Require

Description:
If the folded stanza does not contain one of the required elements, the whole stanza will be discarded.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
body

Config file XML Option:
Attribute 'element' of child element 'require' of 'message_fold'

Other Info:
Update does not require server restart. Shared only option.

H.6.14 Message Fold Match Rules Set

Description:
This is the set of rules to be used for message folding for stanzas to the peer. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'message' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
html http://jabber.org/protocol/xhtml-im

Config file XML Option:
Attribute 'element' of child element 'match' of 'message_fold' set to the element and attribute 'ns' of child element 'match' of 'message_fold' set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.6.15 Presence Fold Mode

Description:
This applies to presence stanzas according to the 'Presence Fold Match Rules Set'.

Syntax:
String (Mandatory)

Options:
none - None

keep - The server will pass the matched elements to the peer

strip - The server will not pass the matched elements to the peer

Default Value:
none

Example:
strip

Config file XML Option:
Attribute 'mode' of element 'presence_fold'

Other Info:
Update does not require server restart. Shared only option.

H.6.16 Presence Fold Match Rules Set

Description:
This is the set of rules to be used for presence folding for stanzas to the peer. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'presence' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

If the 'Presence Fold Mode' is to pass the matched elements, and no elements are specified here, then an empty presence stanza will be sent.

If the 'Presence Fold Mode' is to not pass the matched elements, and no elements are specified here, then no presence stanza will be sent at all.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
c http://jabber.org/protocol/caps

Config file XML Option:
Attribute 'element' of child element 'match' of 'presence_fold' set to the element and attribute 'ns' of child element 'match' of 'presence_fold' set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.6.17 Enable SIO Relabel Out

Description:
This enables or disables SIO relabelling controls.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.18 Disable Relabel Out XEP-0258

Description:
If set to 'true', this disables inclusion of security labels (described in XEP-0258) in outbound stanzas.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'no_xep258' of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.19 Inject FLOT for labels

Description:
This option enables/disables First-Line-Of-Text (FLOT) labels to the remote server.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'flot' of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.20 Inject FLOT for default labels

Description:
This controls whether FLOT text markers will be added to messages using the default label.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'flot_default' of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.21 Relabel Out XEP-0131 Classification

Description:
If set to 'true', this enables sending of stanza headers and Internet metadata (described in XEP-0131) Classification elements to the peer.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'xep131_classification' of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.22 Relabel Out Provide Default

Description:
This option enables/disables insertion of a default security label in stanzas which have no security label.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'provide_default' of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.23 Relabel Out Use Equivs

Description:
If set to 'true', this enables replacement of security label based upon security policy equivalences of a default security label in stanzas which have no security label.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'use_equivs' of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.24 Update Markings

Description:
If this is set, display markings on labels received from this peer will not be trusted, and will be rewritten prior to delivery.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'update_markings' of element 'sio_relabel_out' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart. Shared only option.

H.6.25 XEP-0258 Security Label Format

Description:
This option specifies the default encoding to use when generating security labels (as described in XEP-0258).

Syntax:
String (Optional)

Options:
xep258ess - XEP 258 ESS

isode - Isode

nato-xcl - NXL (Experimental)

x400 - X.400/X.500 (Experimental)

Default Value:
-None-

Example:
xep258ess

Config file XML Option:
Element 'xep258_format' of element 'sio_relabel_out'

Other Info:
Update does not require server restart. Shared only option.

H.6.26 Reject if input XEP 258 label does not match the relabel out raw label

Description:
This option enables/disables raw label matching. Requires relabel_out raw_label to be set. Only supports IC-ISM (v1 and v2) XEP-258 labels

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
-None-

Other Info:
Update does not require server restart. Shared only option.

H.6.27 Clearance File

Description:
This option specifies the security clearance of the server, domain or peer for which it is defined, controlling which labeled contents may be handled by that entity. For instance, any message that has a label denying access to the peer clearance will not be sent to the peer and rejected if received from the peer.

If the clearance has not been specified for the server, no server-wide traffic restrictions exist. If the clearance has not been specified for an XMPP domain, then it inherits the restrictions of the server.

If the clearance has not been specified for the peer, then traffic is restricted by the default clearance specified in the server's security policy. The peer's clearance is also used in authorization decisions in accesses by the peer's users.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/cRestricted.xml

Config file XML Option:
sio_clearance_file

Other Info:
Update does not require server restart.

H.6.28 Default Stanza Security Label File

Description:
This option specifies the security label to be applied to any unlabeled stanza sent to or from the server, domain or peer for which it is defined.

If the default label has not been specified for the server, the policy default label applies. If the default label is not specified for the domain, the domain will inherit the default label of the server.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lRestricted.xml

Config file XML Option:
sio_default_label_file

Other Info:
Update does not require server restart.

H.6.29 Security Policy (SPIF) File

Description:
This option specifies the security (label) policy of the server or peer for which it is defined. The server's security policy option enables and generally governs security label processing. It is generally a pre-requisite for all other security label options.

A peer control may optionally have a relabel out policy, which if set is used instead of the server policy in generating markings and equivalent labels in that peer's relabel out functions.

The contents are in the Open XML Security Policy Information File (SPIF) format.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/policy.xml

Config file XML Option:
sio_policy_file

Other Info:
Update requires server restart.

H.6.30 Security Label File

Description:
This option specifies the security label of the server or domain for which it is defined. This restricts access to the entity to only those users and peers with sufficient clearance.

If the label has not been specified for the server, server access is restricted by the policy default label. If the label is not specified for the domain, access will be governed solely by the server's label.

When specified for a peer, it indicates to relabel to the specified label using the relabel out 'Security Policy (SPIF) XML' option, if set, else the server's 'Security Policy (SPIF) XML' option.

The server option 'Security Policy (SPIF) XML' must be set before setting this option.

The contents are in XML.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lConfidential.xml

Config file XML Option:
sio_label_file

Other Info:
Update requires server restart.

H.6.31 Raw Security Label File

Description:
This option specifies a "raw" security label of the peer it is defined. When specified, all labeling will be replaced (where appropriate) with the raw content.

As the content is used verbatim¸ it must be an XML fragment which when injected into an stanza yields valid XMPP.

Syntax:
String (Optional)

Default Value:
-None-

Example:
/etc/isode/sio/lRaw.xml

Config file XML Option:
raw_label_file

Other Info:
Update does not require server restart.

H.6.32 JID Filter Mode

Description:
This applies to stanzas according to the JID filter match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'jid_filter'

Other Info:
Update does not require server restart. Shared only option.

H.6.33 JID Filter Match Rules Set

Description:
This is the set of rules to be used for JID filtering. Each entry should be set to the recipient (which will be matched with the 'to' attribute of the stanza), followed by a space, and then followed by the sender (which will be matched with the 'from' attribute of the stanza).

The recipient and sender can be specified in any of the following ways:

1) any JID - indicated by specifying '@'

2) any JID at a specified domain - indicated by specifying '@' followed by the domain name, for example, '@example.net'

3) the specified bare JID - for example, fred@example.net

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
@ @example.net

Config file XML Option:
Attribute 'to' of child element 'match' of 'jid_filter' set to the recipient and attribute 'from' of child element 'match' of 'jid_filter' set to the sender

Other Info:
Update does not require server restart. Shared only option.

H.6.34 IQ Filter 'From' Mode

Description:
This applies to IQ stanzas from the peer, domain, etc. for which this filter is created, according to the IQ filter 'from' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'from')

Other Info:
Update does not require server restart. Shared only option.

H.6.35 IQ Filter 'From' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas from the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'from') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.6.36 IQ Filter 'To' Mode

Description:
This applies to IQ stanzas directed to the peer, domain, etc. for which this filter is created, according to the IQ filter 'to' match rules set.

Syntax:
String (Mandatory)

Options:
deny - The server will deny an inbound stanza if the stanza matches any of the rules in the filter match rules set

accept - The server will only pass an inbound stanza if the stanza matches a specified rule in the filter match rules set

Default Value:
deny

Example:
accept

Config file XML Option:
Attribute 'mode' of element 'iq_filter' (where attribute 'target' has value 'to')

Other Info:
Update does not require server restart. Shared only option.

H.6.37 IQ Filter 'To' Match Rules Set

Description:
This is the set of rules to be used for inbound IQ filtering for stanzas directed to the peer, domain, etc. for which this filter is created. Each entry should be set to the name of the element (which will be matched with the first level child element of the 'iq' element), followed by a space, and then optionally followed by the namespace of the element name.

The namespace in the rule can be omitted if the element is in the default name space.

Syntax:
Multi-Valued String (Optional)

Default Value:
-None-

Example:
query http://jabber.org/protocol/disco#info

Config file XML Option:
Attribute 'element' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the element and attribute 'ns' of child element 'match' of 'iq_filter' (where attribute 'target' has value 'to') set to the name space

Other Info:
Update does not require server restart. Shared only option.

H.7 Links Options

This section describes each link configuration option.

Ad-Hoc Commands:

- See Section G.42, “Get Link Configuration”.
- See Section G.43, “Add Link Configuration”.
- See Section G.44, “Modify Link Configuration”.
- See Section G.45, “Delete Link Configuration”.

H.7.1 XEP-0361 Zero Handshake Link

The parent XML element in the configuration file is `<ms_options><peering><link>`.

H.7.1.1 Link Name

Description:
This is the unique name to identify the link.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
special

Config file XML Option:
Attribute 'name' of parent element 'link'

Other Info:
Update does not require server restart.

H.7.1.2 Link Type

Description:
This is the type of the link.

'XEP-0361 Zero Handshake Link' is used for SATCOM and similar low-bandwidth IP links. While it may operate over IP/S'5066, performance is better using the 'STANAG 5066 Link (HF Radio)' link type.

Syntax:
String (Mandatory)

Options:
direct_io - XEP-0361 Zero Handshake Link

s5066 - STANAG 5066 Link (HF Radio)

Default Value:
-None-

Example:
direct_io

Config file XML Option:
Attribute 'type' of parent element 'link'

Other Info:
Update does not require server restart.

H.7.1.3 Remote IP

Description:
This specifies the IPv4 or IPv6 address that the remote server listens on.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
172.16.6.7

Config file XML Option:
Attribute 'host' of element 'connect_to'

Other Info:
Update requires server restart.

H.7.1.4 Remote Port

Description:
This specifies the port (0-65535) that the remote server listens on.

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
9999

Config file XML Option:
Attribute 'port' of element 'connect_to'

Other Info:
Update requires server restart.

H.7.1.5 Local IP

Description:
This specifies the IPv4 or IPv6 address that the local server listens on. It can be left empty to imply all interfaces.

Syntax:
String (Optional)

Default Value:
-None-

Example:
172.16.6.8

Config file XML Option:
Attribute 'host' of element 'listen_on'

Other Info:
Update requires server restart.

H.7.1.6 Local Port

Description:
This specifies the port (0-65535) that the local server listens on. Please make sure that it is not a port already in use - for example the XMPP client listener port (usually 5222) or the XMPP server-to-server listener port (usually 5269).

Syntax:
Numeric (Mandatory)

Default Value:
0

Example:
9999

Config file XML Option:
Attribute 'port' of element 'listen_on'

Other Info:
Update requires server restart.

H.7.1.7 Listen Only Link

Description:
If 'true', this flag indicates that this link is only used for listening for connections from the remote peer, not for connecting to it.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'listen_only' indicates 'true', absence indicates 'false'

Other Info:
Update requires server restart.

H.7.1.8 Stream Management

Description:
This enables or disables stream management according to XEP-0198. This needs to be set to the same value on the local and remote end.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'sm' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart.

H.7.1.9 Compress Traffic

Description:
This needs to be set to the same value on the local and remote end.

This flag is ignored when the 'Require TLS' flag is set as TLS implicitly negotiates compression.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'compress' indicates 'true', absence indicates 'false'

Other Info:
Update requires server restart.

H.7.1.10 Encrypt Traffic

Description:
This enables or disables TLS encryption. This needs to be set to the same value on the local and remote ends.

TLS must be available for the server before it is configured for a link.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'tls' indicates 'true', absence indicates 'false'

Other Info:
Update requires server restart.

H.7.2 STANAG 5066 Link (HF Radio)

The parent XML element in the configuration file is `<ms_options><peering><link>`.

H.7.2.1 Link Name

Description:
This is the unique name to identify the link.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
special

Config file XML Option:
Attribute 'name' of parent element 'link'

Other Info:
Update does not require server restart.

H.7.2.2 Link Type

Description:
This is the type of the link.

'XEP-0361 Zero Handshake Link' is used for SATCOM and similar low-bandwidth IP links. While it may operate over IP/S'5066, performance is better using the 'STANAG 5066 Link (HF Radio)' link type.

Syntax:
String (Mandatory)

Options:
direct_io - XEP-0361 Zero Handshake Link

s5066 - STANAG 5066 Link (HF Radio)

Default Value:
-None-

Example:
direct_io

Config file XML Option:
Attribute 'type' of parent element 'link'

Other Info:
Update does not require server restart.

H.7.2.3 STANAG 5066 Server

Description:
This specifies the IPv4 or IPv6 address that the local STANAG 5066 server listens on for the connection from the local M-Link Server.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
172.16.6.9

Config file XML Option:
Attribute 'host' of element 'listen_on'

Other Info:
Update does not require server restart.

H.7.2.4 STANAG 5066 Server Port

Description:
This specifies the port that the local STANAG 5066 server listens on for the connection from the local M-Link Server.

Syntax:
Numeric (Mandatory)

Default Value:
5066

Example:
9999

Config file XML Option:
Attribute 'port' of element 'listen_on'

Other Info:
Update does not require server restart.

H.7.2.5 Remote S5066 Address

Description:
This specifies a valid S5066 address of the remote STANAG 5066 server that the local STANAG 5066 server will connect to.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
10.44.0.1

Config file XML Option:
Attribute 'host' of element 'connect_to'

Other Info:
Update does not require server restart.

H.7.2.6 Local S5066 Address

Description:
This specifies a valid S5066 address of the local STANAG 5066 server. This is to prevent looping on broadcast messages.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
10.44.0.2

Config file XML Option:
Attribute 'hfaddr' of element 'listen_on'

Other Info:
Update does not require server restart.

H.7.2.7 SAP ID

Description:
This specifies the SAP ID which is a value in the range 0-15. This must be the same for the local and remote STANAG 5066 servers.

The following values can interfere with other applications: 0 (Management), 1 (COSS), 2 (M-Switch), 3 (HMTP), 4 (HFPOP), 8 (ETHER), 9 (IP/S'5066), 10/11 (Reserved), 12 (CFTP).

Syntax:
Numeric (Mandatory)

Default Value:
6

Example:
15

Config file XML Option:
Attribute 'port' of element 'connect_to'

Other Info:
Update does not require server restart.

H.7.2.8 Listen Only Link

Description:
If 'true', this flag indicates that this link is only used for listening for connections from the remote peer, not for connecting to it.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'listen_only' indicates 'true', absence indicates 'false'

Other Info:
Update requires server restart.

H.7.2.9 Stream Management

Description:
This enables or disables stream management according to XEP-0198. This needs to be set to the same value on the local and remote end.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'sm' indicates 'true', absence indicates 'false'

Other Info:
Update does not require server restart.

H.7.2.10 Compress Traffic

Description:
This needs to be set to the same value on the local and remote end.

This flag is ignored when the 'Require TLS' flag is set as TLS implicitly negotiates compression.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'compress' indicates 'true', absence indicates 'false'

Other Info:
Update requires server restart.

H.7.2.11 Encrypt Traffic

Description:
This enables or disables TLS encryption. This needs to be set to the same value on the local and remote ends.

TLS must be available for the server before it is configured for a link.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
Presence of empty element 'tls' indicates 'true', absence indicates 'false'

Other Info:
Update requires server restart.

H.8 Clustering Options

This section describes each clustering configuration option.

Ad-Hoc Commands:

- See Section G.49, “Get Cluster List (Node)”.
- See Section G.50, “Add Node to Cluster (Node)”.
- See Section G.51, “Delete Node from Cluster (Node)”.

The parent XML element in the configuration file is `<ms_options>`.

H.8.1 IP address

Description:
This specifies the IP address of the local or peer node.

Multiple M-Link processes can be linked via a mesh networking system to form a cluster, and they will automatically share data inside this network to provide a single service apparently hosted on multiple machines.

Each process within the cluster is known as a 'node'.

Each node is required to be configured with its own location and the location of all peers.

The removal of a single node will leave all M-Link services, and the other nodes, undisturbed.

Syntax:
String (Mandatory)

Default Value:
-None-

Example:
192.168.37.212

Config file XML Option:
See 'Is Local Node'

Other Info:
Update requires server restart.

H.8.2 Port

Description:
This specifies the port that the node listens on for communication from peer nodes of the cluster.

Syntax:
Numeric (Mandatory)

Default Value:
3999

Example:
3998

Config file XML Option:
See 'Is Local Node'

Other Info:
Update requires server restart.

H.8.3 Is Local Node

Description:
This specifies if this is the location of the local node.

Syntax:
Boolean (Mandatory)

Default Value:
false

Example:
true

Config file XML Option:
If local node, then element 'cell_xmpp_uri', otherwise an element 'cell_xmpp' for each peer node, set to the value 'tlvmpp.tcp://ip:port/'

Other Info:
Update requires server restart.

Appendix I MUC Room Settings Reference

This appendix describes each Multi-User Chat room configuration setting.

I.1 Room Title

Configuration Option:
muc#roomconfig_roomname

Description:
The formal name of the room

I.2 Description

Configuration Option:
muc#roomconfig_roomdesc

Description:
The description of the room

I.3 Marking

Configuration Option:
x-isode#roomconfig_marking

Description:
A marking for clients to display

I.4 Marking Foreground Color

Configuration Option:
x-isode#roomconfig_marking_fg_color

Description:
Foreground color for the marking

I.5 Marking Background Color

Configuration Option:
x-isode#roomconfig_marking_bg_color

Description:
Background color for the marking

I.6 Publicly Listed?

Configuration Option:
muc#roomconfig_publicroom

Description:
This controls whether the room is listed in the Service Discovery 'disco#items' listing of the MUC service

I.7 Moderated

Configuration Option:
muc#roomconfig_moderatedroom

Description:
Whether unaffiliated users are initially prevented from sending messages to the room. This option is mutually exclusive with 'Members Only.'

I.8 Members Only

Configuration Option:
muc#roomconfig_membersonly

Description:
If enabled, only JIDs listed with an affiliation of member, moderator or administrator can enter the room. This option is mutually exclusive with 'Moderated.'

I.9 Password

Configuration Option:
muc#roomconfig_roomsecret

Description:
A password that must be provided by users before they can enter the room

I.10 Persistent Room

Configuration Option:
muc#roomconfig_persistentroom

Description:
Persistent rooms exist until they are specifically deleted. Non-persistent rooms disappear as soon as they are empty of occupants.

I.11 Real JIDs visible to

Configuration Option:
muc#roomconfig_whois

Description:
This can be set to various roles to provide a control on what the minimum roles must be to have real JIDs, as well as in-room JIDs, presented to users

I.12 Invitations sent by

Configuration Option:
x-isode#roomconfig_invite

Description:
This sets the minimum role required for a user to have the room issue Multi-User Chat invitations. Invitations sent by a members-only room will cause the invitee to be made a member.

I.13 Private messages sent by

Configuration Option:
x-isode#roomconfig_privmsg

Description:
This sets the minimum role required to send private messages through the MUC system to another occupant

I.14 Allow vCards on anonymous users?

Configuration Option:
x-isode#roomconfig_vcards

Description:
For users whom the requestor can see the real JID, any vCard (XEP-0054) request is redirected to the users' bare JIDs. Where the requestor cannot see the real JID, they will only be redirected if this option is set.

I.15 Allow all users to change subject?

Configuration Option:
muc#roomconfig_changesubject

Description:
This is the minimum role required to change the subject in the room

I.16 History Storage Length

Configuration Option:
x-isode#roomconfig_history_length

Description:
The maximum number of messages stored in the room's history. Older messages are purged as necessary to make room for new messages.

I.17 Default History Served

Configuration Option:
x-isode#roomconfig_default_history

Description:
How many messages from the room's history to be sent to clients entering the room (unless they specifically request a certain amount of history).

I.18 Maximum number of occupants

Configuration Option:
muc#roomconfig_maxusers

Description:
-None-

I.19 Clear History

Configuration Option:
x-isode#roomconfig_history_clear

Description:
Setting this flag will remove the entire room history as soon as the form is submitted. Once history has been removed, the flag is cleared.

I.20 Hide unvoiced occupants

Configuration Option:
x-isode#roomconfig_hide_unvoiced

Description:
If this option is enabled, then presence information will only be sent for occupants who have voice capability

I.21 Accept any message types

Configuration Option:
x-isode#roomconfig_pass_any

Description:
Whether to pass all elements of groupchat messages to occupants. Clearing this flag means that only body, thread and (if XHTML-IM messages are accepted) xhtml elements will be passed.

I.22 Accept XHTML-IM messages

Configuration Option:
x-isode#roomconfig_pass_html

Description:
Whether to pass xhtml elements of groupchat messages to occupants. The setting for this flag is only meaningful if 'Accept any message types' is disabled.

I.23 Creation Policy

Configuration Option:
pubsub#children_association_policy

Description:
Controls who can create new rooms

I.24 Creation Whitelist

Configuration Option:
pubsub#children_association_whitelist

Description:
When 'Creation Policy' is set to 'whitelist', then new rooms may only be created by JIDs specified in this list.

I.25 History requested from FMUC

Configuration Option:
{isode.com}#fmuc_history_len

Description:
How many messages to request from the federated room when joining it (-1 for unlimited).

I.26 Add remote FMUC domain name to nicks

Configuration Option:
{isode.com}#fmuc_add_domain

Description:
Whether the server will add the remote FMUC domain name to the nick of each user from that domain. This will prevent nick conflicts.

I.27 Allow FMUC from arbitrary sources

Configuration Option:
{isode.com}#fmuc_open

Description:
Whether any remote MUC room that tries to federate with this room will be allowed to do so.

I.28 Federated MUC nodes

Configuration Option:
{isode.com}#fmuc_join_nodes

Description:
A list of JIDs representing the rooms that this room will attempt to federate to, and will allow federation from (regardless of the setting for 'Allow FMUC from arbitrary sources')

I.29 IRC Host

Configuration Option:
x-isode#irc_host

Description:
For a room acting as an IRC gateway, this is the host name of the IRC server that this room connects to. If this value is set, then 'IRC Port' and 'IRC Channel' should also be specified

I.30 IRC Port

Configuration Option:
x-isode#irc_port

Description:
For a room acting as an IRC gateway, this is the port number of the IRC server that this room connects to. This value should be specified if 'IRC Host' is set. Common port numbers are 6667 for non-TLS connections and 6697 for TLS connections.

I.31 IRC TLS

Configuration Option:
x-isode#irc_tls

Description:
This controls whether M-Link uses TLS for its connection to the IRC server and so must be set when the specified IRC Port is expecting SSL/TLS connections.

I.32 IRC Channel

Configuration Option:
x-isode#irc_channel

Description:
For a room acting as an IRC gateway, this is the name of the IRC channel that this room is connected to. This value is only used when 'IRC Host' and 'IRC port' are specified. Only one room may act as a gateway for any given IRC channel

I.33 IRC Channel Password

Configuration Option:
x-isode#irc_channel_password

Description:
For a room acting as an IRC gateway, this specifies the password (channel key) to be used when connecting to the IRC. The value is only used when 'IRC Host', 'IRC port' and 'IRC Channel' are specified.

I.34 Nick Regex

Configuration Option:
x-isode#nick_regex

Description:
A regular expression that is used to validate nick names. If a user tries to enter the room and the expression doesn't match, the user will not be able to enter the room

I.35 SIO Label

Configuration Option:
x-isode#sio_label

Description:
The room's security label. Users will be unable to join the room unless they have a clearance which permits access to resources with this label

I.36 SIO Clearance

Configuration Option:
x-isode#sio_clearance

Description:
The room's security clearance. Messages will only appear in this room if their label is appropriate for the room's clearance

I.37 Default SIO Label

Configuration Option:
x-isode#sio_default_label

Description:
A security label that will be applied to all messages which do not have an explicit label

Appendix J TLS Cipher List Format

This chapter describes the TLS cipher list format.

J.1 Overview

TLS ciphers are configured in M-Link Server using textual OpenSSL cipher lists. This appendix describes the format used.

The cipher list consists of one or more cipher strings separated by spaces. Commas or colons are also acceptable separators.

The actual cipher string can take several different forms.

It can consist of a single cipher suite such as `RC4-SHA`.

It can represent a list of cipher suites containing a certain algorithm, or cipher suites of a certain type. For example `SHA1` represents all ciphers suites using the digest algorithm SHA1 and `TLSv1` represents all TLS v1 ciphers.

Lists of cipher suites can be combined in a single cipher string using the + character. This is used as a logical and operation. For example `SHA1+DES` represents all cipher suites containing the SHA1 and the DES algorithms.

Each cipher string can be optionally preceded by the characters `!`, `-` or `+`.

If `!` is used then the ciphers are permanently deleted from the list. The ciphers deleted can never reappear in the list even if they are explicitly stated.

If `-` is used then the ciphers are deleted from the list, but some or all of the ciphers can be added again by later options.

If `+` is used then the ciphers are moved to the end of the list. This option doesn't add any new ciphers it just moves matching existing ones.

If none of these characters is present then the string is just interpreted as a list of ciphers to be appended to the current preference list. If the list includes any ciphers already present they will be ignored: that is they will not moved to the end of the list.

Additionally the cipher string `@STRENGTH` can be used at any point to sort the current cipher list in order of encryption algorithm key length.

Note: M-Link Server modifies the configured cipher list specification to remove unusable ciphers, such as those which are not compatible with the server's configured private key. Additionally, in absence of a HGE-TLS, high grade ciphers will be disabled. Unless low grade ciphers are specifically enabled, no ciphers will be available for M-Link Server to use and TLS use will be disabled. Low grade ciphers are generally inappropriate for use in production environments.

J.2 Cipher strings

The following is a list of all permitted cipher strings and their meanings

`DEFAULT`
: The default cipher list. This is determined at compile time and is normally `ALL:!EXPORT:!DES:!aNULL:!eNULL:!SSLv2`. This must be the first cipher string specified.

`COMPLEMENTOFDEFAULT`
: the ciphers included in `ALL`, but not enabled by default. Currently this is `ADH`. Note that this rule does not cover `eNULL`, which is not included by `ALL` (use `COMPLEMENTOFALL` if necessary).

`ALL`
: all ciphers suites except the `eNULL` ciphers which must be explicitly enabled.

`COMPLEMENTOFALL`
: the cipher suites not enabled by `ALL`, currently being `eNULL`.

`HIGH`
: “high” encryption cipher suites. This currently means those with key lengths larger than 128 bits.

`MEDIUM`
: “medium” encryption cipher suites, currently those using 128 bit encryption.

`LOW`
: “low” encryption cipher suites, currently those using 64 or 56 bit encryption algorithms but excluding export cipher suites.

`EXP`, `EXPORT`
: export encryption algorithms. Including 40 and 56 bits algorithms.

`EXPORT40`
: 40 bit export encryption algorithms

`EXPORT56`
: 56 bit export encryption algorithms.

`eNULL`, `NULL`
: the “NULL” ciphers that is those offering no encryption. Because these offer no encryption at all and are a security risk they are disabled unless explicitly included.

`aNULL`
: the cipher suites offering no authentication. This is currently the anonymous DH algorithms. These cipher suites are vulnerable to a “man in the middle” attack and so their use is normally discouraged.

`kRSA`, `RSA`
: cipher suites using RSA key exchange.

`kEDH`
: cipher suites using ephemeral DH key agreement.

`kDHr`, `kDHd`
: cipher suites using DH key agreement and DH certificates signed by CAs with RSA and DSS keys respectively. Not implemented.

`aRSA`
: cipher suites using RSA authentication, i.e. the certificates carry RSA keys.

`aDSS`, `DSS`
: cipher suites using DSS authentication, i.e. the certificates carry DSS keys.

`aDH`
: cipher suites effectively using DH authentication, i.e. the certificates carry DH keys. Not implemented.

`TLSv1`, `SSLv3`, `SSLv2`
: TLS v1.0, SSL v3.0 or SSL v2.0 cipher suites respectively.

`DH`
: cipher suites using DH, including anonymous DH.

`ADH`
: anonymous DH cipher suites.

`AES`
: cipher suites using AES.

`3DES`
: cipher suites using triple DES.

`DES`
: cipher suites using DES (not triple DES).

`RC4`
: cipher suites using RC4.

`RC2`
: cipher suites using RC2.

`MD5`
: cipher suites using MD5.

`SHA1`, `SHA`
: cipher suites using SHA1.

J.3 Examples

All ciphers including NULL ciphers:

```
ALL:eNULL
```

Include all ciphers except NULL and anonymous DH then sort by strength:

```
ALL:!ADH:@STRENGTH
```

Include only 3DES ciphers and then place RSA ciphers last:

```
3DES:+RSA
```

Include all RC4 ciphers but leave out those without authentication:

```
RC4:!COMPLEMENTOFDEFAULT
```

Include all ciphers with RSA authentication but leave out ciphers without encryption.

```
RSA:!COMPLEMENTOFALL
```

J.4 Cipher suite names

The following lists give the TLS and SSL cipher suites names from the relevant specification and their OpenSSL equivalents. It should be noted that several cipher suite names do not include the authentication used, e.g. `DES-CBC3-SHA`. In these cases, RSA authentication is used.

J.4.1 TLS v1.0 cipher suites

- `TLS_RSA_WITH_NULL_MD5`
- `NULL-MD5`
- `TLS_RSA_WITH_NULL_SHA`
- `NULL-SHA`
- `TLS_RSA_EXPORT_WITH_RC4_40_MD5`
- `EXP-RC4-MD5`
- `TLS_RSA_WITH_RC4_128_MD5`
- `RC4-MD5`
- `TLS_RSA_WITH_RC4_128_SHA`
- `RC4-SHA`
- `TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5`
- `EXP-RC2-CBC-MD5`
- `TLS_RSA_EXPORT_WITH_DES40_CBC_SHA`
- `EXP-DES-CBC-SHA`
- `TLS_RSA_WITH_DES_CBC_SHA`
- `DES-CBC-SHA`
- `TLS_RSA_WITH_3DES_EDE_CBC_SHA`
- `DES-CBC3-SHA`
- `TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA`
- `EXP-EDH-DSS-DES-CBC-SHA`
- `TLS_DHE_DSS_WITH_DES_CBC_SHA`
- `EDH-DSS-CBC-SHA`
- `TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA`
- `EDH-DSS-DES-CBC3-SHA`
- `TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA`
- `EXP-EDH-RSA-DES-CBC-SHA`
- `TLS_DHE_RSA_WITH_DES_CBC_SHA`
- `EDH-RSA-DES-CBC-SHA`
- `TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA`
- `EDH-RSA-DES-CBC3-SHA`
- `TLS_DH_anon_EXPORT_WITH_RC4_40_MD5`
- `EXP-ADH-RC4-MD5`
- `TLS_DH_anon_WITH_RC4_128_MD5`
- `ADH-RC4-MD5`
- `TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA`

- EXP-ADH-DES-CBC-SHA
- TLS_DH_anon_WITH_DES_CBC_SHA
- ADH-DES-CBC-SHA
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
- ADH-DES-CBC3-SHA

J.4.2 AES ciphersuites from RFC3268, extending TLS v1.0

- TLS_RSA_WITH_AES_128_CBC_SHA
- AES128-SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- AES256-SHA
- TLS_DH_DSS_WITH_AES_128_CBC_SHA
- DH-DSS-AES128-SHA
- TLS_DH_DSS_WITH_AES_256_CBC_SHA
- DH-DSS-AES256-SHA
- TLS_DH_RSA_WITH_AES_128_CBC_SHA
- DH-RSA-AES128-SHA
- TLS_DH_RSA_WITH_AES_256_CBC_SHA
- DH-RSA-AES256-SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- DHE-DSS-AES128-SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- DHE-DSS-AES256-SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- DHE-RSA-AES128-SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- DHE-RSA-AES256-SHA
- TLS_DH_anon_WITH_AES_128_CBC_SHA
- ADH-AES128-SHA
- TLS_DH_anon_WITH_AES_256_CBC_SHA
- ADH-AES256-SHA

J.4.3 Additional export 1024 and other cipher suites

Note: these ciphers can also be used in SSL v3.

- TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
- EXP1024-DES-CBC-SHA
- TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
- EXP1024-RC4-SHA
- TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
- EXP1024-DHE-DSS-DES-CBC-SHA
- TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA
- EXP1024-DHE-DSS-RC4-SHA
- TLS_DHE_DSS_WITH_RC4_128_SHA
- DHE-DSS-RC4-SHA

J.4.4 SSL v3.0 cipher suites

- SSL_RSA_WITH_NULL_MD5
- NULL-MD5
- SSL_RSA_WITH_NULL_SHA
- NULL-SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- EXP-RC4-MD5
- SSL_RSA_WITH_RC4_128_MD5
- RC4-MD5
- SSL_RSA_WITH_RC4_128_SHA
- RC4-SHA
- SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- EXP-RC2-CBC-MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- EXP-DES-CBC-SHA
- SSL_RSA_WITH_DES_CBC_SHA
- DES-CBC-SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- DES-CBC3-SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- EXP-EDH-DSS-DES-CBC-SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- EDH-DSS-CBC-SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- EDH-DSS-DES-CBC3-SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- EXP-EDH-RSA-DES-CBC-SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- EDH-RSA-DES-CBC-SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- EDH-RSA-DES-CBC3-SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- EXP-ADH-RC4-MD5
- SSL_DH_anon_WITH_RC4_128_MD5
- ADH-RC4-MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- EXP-ADH-DES-CBC-SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- ADH-DES-CBC-SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- ADH-DES-CBC3-SHA

J.4.5 SSL v2.0 cipher suites

- SSL_CK_RC4_128_WITH_MD5
- RC4-MD5

- SSL_CK_RC4_128_EXPORT40_WITH_MD5
- EXP-RC4-MD5
- SSL_CK_RC2_128_CBC_WITH_MD5
- RC2-MD5
- SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5
- EXP-RC2-MD5
- SSL_CK_DES_64_CBC_WITH_MD5
- DES-CBC-MD5
- SSL_CK_DES_192_EDE3_CBC_WITH_MD5
- DES-CBC3-MD5

J.5 Acknowledgement

This appendix borrows text from OpenSSL ciphers(1) manual page.

Appendix K References

This appendix contains relevant references.

Technical Specifications

Request For Comments (RFCs)

[RFC0793] *Transmission Control Protocol*. J. Postel. RFC 793. September 1981. <*http://www.rfc-editor.org/info/rfc793*>.

[RFC1034] *Domain names - concepts and facilities*. P.V. Mockapetris. RFC 1034. November 1987. <*http://www.rfc-editor.org/info/rfc1034*>.

[RFC1035] *Domain names - implementation and specification*. P.V. Mockapetris. RFC 1035. November 1987. <*http://www.rfc-editor.org/info/rfc1035*>.

[RFC1422] *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*. S. Kent. RFC 1422. February 1993. <*http://www.rfc-editor.org/info/rfc1422*>.

[RFC1964] *The Kerberos Version 5 GSS-API Mechanism*. J. Linn. RFC 1964. June 1996. <*http://www.rfc-editor.org/info/rfc1964*>.

[RFC2068] *Hypertext Transfer Protocol -- HTTP/1.1*. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee. RFC 2068. January 1997. <*http://www.rfc-editor.org/info/rfc2068*>.

[RFC2743] *Generic Security Service Application Program Interface Version 2, Update 1*. J. Linn. RFC 2743. January 2000. <*http://www.rfc-editor.org/info/rfc2743*>.

[RFC2986] *PKCS #10: Certification Request Syntax Specification Version 1.7*. M. Nystrom and B. Kaliski. RFC 2986. November 2000. <*http://www.rfc-editor.org/info/rfc2986*>.

[RFC4120] *The Kerberos Network Authentication Service (V5)*. C. Neuman, T. Yu, S. Hartman, and K. Raeburn. RFC 4120. July 2005. <*http://www.rfc-editor.org/info/rfc4120*>.

[RFC4422] *Simple Authentication and Security Layer (SASL)*. A. Melnikov and K. Zeilenga. RFC 4422. June 2006. <*http://www.rfc-editor.org/info/rfc4422*>.

[RFC4505] *Anonymous Simple Authentication and Security Layer (SASL) Mechanism*. K. Zeilenga. RFC 4505. June 2006. <*http://www.rfc-editor.org/info/rfc4505*>.

[RFC4510] *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*. K. Zeilenga. RFC 4510. June 2006. <*http://www.rfc-editor.org/info/rfc4510*>.

[RFC4512] *Lightweight Directory Access Protocol (LDAP): Directory Information Models*. K. Zeilenga. RFC 4512. June 2006. <*http://www.rfc-editor.org/info/rfc4512*>.

[RFC4514] *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*. K. Zeilenga. RFC 4514. June 2006. <*http://www.rfc-editor.org/info/rfc4514*>.

[RFC4515] *Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters*. M. Smith and T. Howes. RFC 4515. June 2006. <*http://www.rfc-editor.org/info/rfc4515*>.

[RFC4616] *The PLAIN Simple Authentication and Security Layer (SASL) Mechanism*. K. Zeilenga. RFC 4616. August 2006. <*http://www.rfc-editor.org/info/rfc4616*>.

[RFC4752] *The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism*. A. Melnikov. RFC 4752. November 2006. <*http://www.rfc-editor.org/info/rfc4752*>.

[RFC5035] *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility*. J. Schaad. RFC 5035. August 2007. <*http://www.rfc-editor.org/info/rfc5035*>.

[RFC5246] *The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla. RFC 5246. August 2008. <*http://www.rfc-editor.org/info/rfc5246*>.

[RFC5280] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. RFC 5280. May 2008. <*http://www.rfc-editor.org/info/rfc5280*>.

[RFC5802] *Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms*. C. Newman, A. Menon-Sen, A. Melnikov, and N. Williams. RFC 5802. July 2010. <*http://www.rfc-editor.org/info/rfc5802*>.

[RFC6120] *Extensible Messaging and Presence Protocol (XMPP): Core*. P. Saint-Andre. RFC 6120. March 2011. <*http://www.rfc-editor.org/info/rfc6120*>.

[RFC6121] *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*. P. Saint-Andre. RFC 6121. March 2011. <*http://www.rfc-editor.org/info/rfc6121*>.

[RFC6122] *Extensible Messaging and Presence Protocol (XMPP): Address Format*. P. Saint-Andre. RFC 6122. March 2011. <*http://www.rfc-editor.org/info/rfc6122*>.

[RFC7292] *PKCS #12: Personal Information Exchange Syntax v1.1*. K. Moriarty, M. Nystrom, S. Parkinson, A. Rusch, and M. Scott. RFC 7292. July 2014. <*http://www.rfc-editor.org/info/rfc7292*>.

[RFC7590] *Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)*. P. Saint-Andre and T. Alkemade. RFC 7590. June 2015. <*http://www.rfc-editor.org/info/rfc7590*>.

XMPP Extension Protocols (XEPs)

[XEP-0004] *Data Forms*. R. Eatmon, J. Hildebrand, J. Miller, T. Muldowney, and P. Saint-Andre. XSF XEP-0004. August 2007. <*http://xmpp.org/extensions/xep-0004.html*>.

[XEP-0030] *Service Discovery*. J. Hildebrand, P. Millard, R. Eatmon, and P. Saint-Andre. XSF XEP-0030. June 2014. <*http://xmpp.org/extensions/xep-0030.html*>.

[XEP-0045] *Multi-User Chat*. P. Saint-Andre. XSF XEP-0045. February 2012. <*http://xmpp.org/extensions/xep-0045.html*>.

[XEP-0049] *Private XML Storage*. P. Saint-Andre and R. Davis. XSF XEP-0049. March 2004. <*http://xmpp.org/extensions/xep-0049.html*>.

[XEP-0050] *Ad-Hoc Commands*. M. Miller. XSF XEP-0050. June 2005. <*http://xmpp.org/extensions/xep-0050.html*>.

[XEP-0054] *vcard-temp*. P. Saint-Andre. XSF XEP-0054. July 2008. <*http://xmpp.org/extensions/xep-0054.html*>.

[XEP-0059] *Result Set Management*. I. Paterson, P. Saint-Andre, V. Mercier, and J. Seguineau. XSF XEP-0059. September 2006. <*http://xmpp.org/extensions/xep-0059.html*>.

[XEP-0060] *Publish-Subscribe*. P. Millard, P. Saint-Andre, and R. Meijer. XSF XEP-0060. July 2010. <*http://xmpp.org/extensions/xep-0060.html*>.

[XEP-0077] *In-Band Registration*. P. Saint-Andre. XSF XEP-0077. January 2012. <*http://xmpp.org/extensions/xep-0077.html*>.

[XEP-0078] *Non-SASL Authentication*. P. Saint-Andre. XSF XEP-0078. October 2008. <*http://xmpp.org/extensions/xep-0078.html*>.

[XEP-0092] *Software Version*. P. Saint-Andre. XSF XEP-0092. February 2007. <*http://xmpp.org/extensions/xep-0092.html*>.

[XEP-0112] *User Physical Location*. P. Saint-Andre. XSF XEP-0112. October 2004. <*http://xmpp.org/extensions/xep-0112.html*>.

[XEP-0114] *Jabber Component Protocol*. P. Saint-Andre. XSF XEP-0114. January 2012. <*http://xmpp.org/extensions/xep-0114.html*>.

[XEP-0124] *Bidirectional-streams Over Synchronous HTTP (BOSH)*. I. Paterson, D. Smith, P. Saint-Andre, J. Moffitt, L. Stout, and W. Tilanus. XSF XEP-0124. April 2014. <*http://xmpp.org/extensions/xep-0124.html*>.

[XEP-0131] *Stanza Headers and Internet Metadata*. P. Saint-Andre and J. Hildebrand. XSF XEP-0131. July 2006. <*http://xmpp.org/extensions/xep-0131.html*>.

[XEP-0133] *Service Administration*. P. Saint-Andre. XSF XEP-0133. August 2005. <*http://xmpp.org/extensions/xep-0133.html*>.

[XEP-0138] *Stream Compression*. J. Hildebrand and P. Saint-Andre. XSF XEP-0138. May 2009. <*http://xmpp.org/extensions/xep-0138.html*>.

[XEP-0156] *Discovering Alternative XMPP Connection Methods*. J. Hildebrand, P. Saint-Andre, and L. Stout. XSF XEP-0156. January 2014. <*http://xmpp.org/extensions/xep-0156.html*>.

[XEP-0163] *Personal Eventing Protocol*. P. Saint-Andre and K. Smith. XSF XEP-0163. July 2010. <*http://xmpp.org/extensions/xep-0163.html*>.

[XEP-0178] *Best Practices for Use of SASL EXTERNAL with Certificates*. P. Saint-Andre and P. Millard. XSF XEP-0178. May 2011. <*http://xmpp.org/extensions/xep-0178.html*>.

[XEP-0185] *Dialback Key Generation and Validation*. P. Hancke and P. Saint-Andre. XSF XEP-0185. February 2007. <*http://xmpp.org/extensions/xep-0185.html*>.

[XEP-0191] *Blocking Command*. P. Saint-Andre. XSF XEP-0191. July 2012. <*http://xmpp.org/extensions/xep-0191.html*>.

[XEP-0198] *Stream Management*. J. Karneges, P. Saint-Andre, J. Hildebrand, F. Forno, D. Cridland, and M. Wild. XSF XEP-0198. June 2011. <*http://xmpp.org/extensions/xep-0198.html*>.

[XEP-0199] *XMPP Ping*. P. Saint-Andre. XSF XEP-0199. June 2009. <*http://xmpp.org/extensions/xep-0199.html*>.

[XEP-0206] *XMPP Over BOSH*. I. Paterson, P. Saint-Andre, L. Stout, and W. Tilanus. XSF XEP-0206. April 2014. <*http://xmpp.org/extensions/xep-0206.html*>.

[XEP-0220] *Server Dialback*. J. Miller, P. Saint-Andre, and P. Hancke. XSF XEP-0220. August 2014. <*http://xmpp.org/extensions/xep-0220.html*>.

[XEP-0227] *Portable Import/Export Format for XMPP-IM Servers*. M. Henoch and W. Hussain. XSF XEP-0227. March 2010. <*http://xmpp.org/extensions/xep-0227.html*>.

[XEP-0248] *PubSub Collection Nodes*. P. Saint-Andre, R. Meijer, and B. Cully. XSF XEP-0248. September 2010. <*http://xmpp.org/extensions/xep-0248.html*>.

[XEP-0258] *Security Labels in XMPP*. K. Zeilenga. XSF XEP-0258. April 2013. <*http://xmpp.org/extensions/xep-0258.html*>.

[XEP-0289] *Federated MUC for Constrained Environments*. K. Smith. XSF XEP-0289. May 2012. <*http://xmpp.org/extensions/xep-0289.html*>.

[XEP-0297] *Stanza Forwarding*. M. Wild and K. Smith. XSF XEP-0297. October 2013. <*http://xmpp.org/extensions/xep-0297.html*>.

[XEP-0313] *Message Archive Management*. M. Wild and K. Smith. XSF XEP-0313. September 2015. <*http://xmpp.org/extensions/xep-0313.html*>.

[XEP-0324] *Internet of Things - Provisioning*. P. Waher. XSF XEP-0324. May 2014. <*http://xmpp.org/extensions/xep-0324.html*>.

[XEP-0346] *Form Discovery and Publishing*. K. Smith. XSF XEP-0346. April 2014. <*http://xmpp.org/extensions/xep-0346.html*>.

[XEP-0361] *Zero Handshake Server to Server Protocol*. S. Kille. XSF XEP-0361. July 2015. <*http://xmpp.org/extensions/xep-0361.html*>.

[XEP-0365] *Server to Server communication over STANAG 5066 ARQ*. S. Kille. XSF XEP-0365. September 2015. <*http://xmpp.org/extensions/xep-0365.html*>.

Other Documents

[SDN.801] *Access Control Concept and Mechanisms*. National Security Agency, Information Assurance Configuration Management Board. NSA CMB-04.02.029, 0N63616. Revision C. 12 May 1999. *Distribution limited, contact Isode at <mailto:support@isode.com> for availability.*.

[X.500] *Information Technology — Open Systems Interconnection — The Directory: Overview of Concepts, Models, and Services*. ITU-T Rec. X.500(2008). ISO/IEC 9594-1:2008. <*http://www.itu.int*>.

[X.509] *Information Technology — Open Systems Interconnection — The Directory: Authentication Framework*. ITU-T Rec. X.509(2008). ISO/IEC 9594-8:2008. <*http://www.itu.int*>.

Appendix L Glossary

This appendix provides a glossary of terms.

Technical Terms

Abstract Syntax Notation One (ASN.1)
A notation for describing and defining data syntax.
See Also Basic Encoding Rules (BER), Distinguished Encoding Rules (DER).

Active Directory (AD)
A *Directory service* developed by Microsoft for the *Windows* networks. AD is a key component of *Windows Integrated Single Sign-On* solution. AD can act as *LDAP server*.

Application-level Gateway (ALG)
A security component which provides security services specific to an application. In the context of M-Link Server, an instance deployed on the *XMPP* network which provides security services for traffic between two or more XMPP services. An instance operating in this fashion is called an M-Link Edge Server

Authentication
The process of determining the identity of a communications partner.
See Also Authorization.

Authorization
A security service aimed at preventing unauthorized access to a service or capability. Once an identity has been established (see *Authentication*), authorization determines what services, data, and operations may be accessed by that identity.

Basic Encoding Rules (BER)
A standard for representing data described using the *ASN.1*. Unlike *DER*, BER provides many options for representing data. BER is used to in a number of Internet protocols including *LDAP* and *SNMP*.

Bidirectional-streams Over Synchronous HTTP (BOSH)
A transport protocol that emulates the semantics of a long-lived, bidirectional *TCP* connection between two entities (such as a client and a server) by efficiently using multiple synchronous *HTTP* request/response pairs without requiring the use of frequent polling or chunked responses. M-Link supports XMPP over BOSH. See [XEP-0124].

Certificate
A data object providing identity information for a subject entity (e.g., a person or computer system) securely bound to a public key by the certificate issuer, a *certificate authority*. See [X.509] and [RFC5280].

Certificate Authority (CA)
An issuer of *certificates*. Also typically a publisher of certificate revocation information, commonly in the form of *CRL*, for the certificates it have issued. See [X.509] and and [RFC5280]. Sodium CA is a GUI tool for performing CA functions.
See Also Root Certificate Authority (Root CA), Root Certificate Authority (Root CA).

Certificate Chain
A certificate chain is a bundle of *certificates* which consists of an entity's certificate and, if the certificate is not *self-signed*, a sequence of certificates, each the issuer of the previous one, usually finishing at a *root*.

Command-line interface CLI
A man-machine interface where actions are entering lines of text called commands.
See Also Graphical User Interface GUI.

Certificate Revocation List (CSL)
A list of certificates which a *certificate authority* has revoked. See [X.509] and and [RFC5280].

Certificate Signing Request (CSR)
A data object representing an entity's request for a *certificate authority* to issue a *certificate*. See [X.509] and [RFC2986]. Isode provides a number of tools to produce CSRs, such as M-Link Console and Sodium

Clearance
A structured representation of what information sensitivities a person (or other entity) is authorized to access.
See Also Security Label, Security Policy.

Component
A process that acts like a remote domain, but speaks [XEP-0114] instead of S2S

Cross Domain Collaborative Information Environment (CDCIE)
A suite of applications for cross domain collaboration produced by US Department of Defense.

CDCIE Client Chat Protocol (CDCIE-CCP)
The protocol used for *group chat* in the *CDCIE* suite of applications. CDCIE-CCP is derived from *XMPP*.

Distinguished Encoding Rules (DER)
A standard for representing data described using the *ASN.1*. Unlike the *BER*, DER specifies a unique way to encode data. DER is commonly used to encode X.509 *certificates*.

Directory
When referred to as *the Directory*, it is a distributed database built to *X.500* standards [X.509] and, in the context of M-Link Server, accessed using *LDAP*
Alternatively, a container which holds files and other containers in a filesystem. Also referred to as a folder.

Directory Entry
A unit in *the Directory* representing one object and identified by its *Distinguished Name*. See [RFC4512].

Directory Service
The service provided by *the Directory* to its users.

Directory System Agent (DSA)
A server process which maintains and provides access to *the Directory*. In the context of Isode M-Link, a *LDAP Server*.

Directory User Agent (DUA)
A client application which accesses *the Directory*. In the context of Isode M-Link, a *LDAP Client*.

Display Marking
A textual representation of the sensitivity of a piece of information. See [SDN.801].
See Also Security Label.

Distinguished Name (DN)
The name for a *directory entry*. M-Link uses the LDAP DN string format to represent DNs. See [RFC4514].

Domain
See Domain Name.

Domain Name
A name within the *Domain Name System*. See [RFC1035].

Domain Name System (DNS)
A service for providing a mapping between *domain names* (for example, `example.com`) and *IP addresses*. See [RFC1035].

Extensible Messaging and Presence Protocol (XMPP)
A collection of open standards for real-time communication, including those for *instant messaging*, presence, and *multi-user chat*. See [RFC6120].

Extensible Markup Language (XML)
A markup language used to represent structured information which is designed to be readable by both humans and machines.

EXTERNAL
EXTERNAL is a *SASL* authentication mechanism name used by a client to ask the server to utilize identity information established outside of the SASL; exchange for establishing the client's identity. It is typically used to in conjuction with *TLS* user *certificate* authentication. See [RFC4422].

Form Discovery and Publishing (FDP)
A *PubSub* based mechanism that allows the XMPP Server to store a list of form templates that can be enumerated and retrieved by clients. See [XEP-0346].

Federated MUC (FMUC)
An *XMPP* extension for federating *MUC* rooms in constrained network environments. See [XEP-0289].

Fully Qualified Domain Name (FQDN)
A complete *domain name* identifying a host system or other entity on the Internet.
See Also Domain Name System (DNS).

Graphical User Interface GUI
A man-machine interface where actions are performed by manipulating graphical elements.
See Also Command-line interface CLI.

GSSAPI
The *SASL Kerberos V5* authentication mechanism. The mechanism is used in *XMPP* clients and servers for *Windows Integrated Single Sign-On* support. Despite its name, it is not a general purpose *GSS-API* mechanism for use in SASL. It is specifically tied to Kerberos V5. See [RFC4752].

Generic Security Services Application Program Interface (GSS-API)
An application program interface (API) that provides a wide range security functions in a generic fashion. M-Link Server only uses GSS-API to implement the *SASL Kerberos V5* mechanism called *GSSAPI*. See [RFC2743], [RFC4120], [RFC1964]

Hypertext
Text which may contain links to other texts. Some times spelled HyperText.

HyperText Markup Language
A standard markup language. Used to create web pages.

Hypertext Transfer Protocol
A protocol for transferring *hypertext* and other content between a client and a server, possibly via a proxy or gateway. See [RFC2068].

Instant Messaging (IM)
Real-time text-based chatting between two or more people. XMPP IM is described in [RFC6121].

Intermediate Certificate Authority (Intermediate CA)
A *certificate authority* which issues *certificates* on behalf of another CA. An intermediate CA's certificate is, hence, not *self-signed*.

IP address
An address which identifies a host machine on an Internet network. For IPv4, it is 32-bit number commonly written in dotted number notation of the form `192.0.1.100`. For IPv6, it is a 128-bit number commonly written in a notation of the form `2001:db8::100`.

Internet Relay Chat (IRC)
A protocol which supports group communications. IRC can be viewed as an alternative protocol to *XMPP* which supports a small subset of features similar to *MUC*. See [RFC2812].

Jabber
Jabber is the colloquial name for the public *XMPP* network.

JabberId (JID)
See XMPP Address.

Kerberos
An *authentication* protocol which relies on a *trusted third party* to issue *tickets* used to mutually authenticate clients and servers. See [RFC4120]. -->

LDAP Client
A program which accesses *Directory* using *LDAP*. Examples: *Sodium*, *M-Link Server*.

LDAP Server
A server process which provides *LDAP* access to *Directory*. Example: *M-Vault Server*.

Lightweight Directory Access Protocol (LDAP)
An Internet protocol used to provide access to the *Directory*. See [RFC4510].
See Also X.500.

M-Link Console (MLC)
An Isode provided tool for administration of *M-Link Servers*.

M-Link Server
Isode's *XMPP* Server.

M-Vault Console (MVC)
An Isode provided tool for administration of *M-Vault Servers*.

M-Vault Server
Isode's Directory System Agent, a *LDAP server*.

Multi-User Chat (MUC)
An *instant messaging* service allowing multiple users to chat with each other; a group chat service. See [XEP-0045].

Online Certificate Status Protocol (OCSP)
A protocol for checking whether a *certificate* has been revoked without retrieving (and processing) the possibly large *CRL*. See [RFC6960].

PDF/A
A standardized document format suitable for long-term archiving.

PEM
A format for representing *certificates*, keys, and other cryptographic objects. PEM stands for Privacy Enhanced Mail, a defunct standard for securing email. See [RFC1422].
See Also PKCS#12.

Personal Eventing Protocol (PEP)
A generic system for publishing extended user data, such as geolocation and currenty activities, to only those contacts that have an interest in it. See [XEP-0163].

PKCS#12
An archive file format for bundling together a set of *certificates*, keys, and other cryptographic objects. See [RFC7292].
See Also PEM.

PLAIN
A password-based *SASL* authentication mechanism. Using this mechanism, a SASL client simply passes a user name and password to SASL server for the server to verify. The mechanims itself does not ensure integrity or confidentiality of the authentication exchange or any subsequent application protocol data exchange and hence is commonly used only after *TLS* has been establish. The mechanism supports identity assumption. See [RFC4616].
See Also SCRAM.

Port
In the context of networking protocols such as *TCP*, an end-point within a host system.

Presence
Information about availability of an entity. XMPP Presence is described in [RFC6121].

Probe
An electronic message, with an envelope but no content, used to test that messages can be delivered to the intended recipient(s).

Protocol
The set form in which data must be presented to be handled by a particular computer configuration or process.

Public Key Infrastructure (PKI)
A collection of systems which support provisioning and use of *certificates*.

Publish-Subscribe (PubSub)
A scalable method of publishing data and events such that those users or systems interested in these data or events receive them in real-time, without the delays inherent in common *polling systems*. See [XEP-0060].

Request for Comments (RFC)
Internet standard documents defining Internet *protocol*. Relevant RFCs are listed in Appendix K, *References*.

Rich Presence Technology (RPT)
An enhanced form of presence awareness in which participants can determine if other users are online and if so, observe to a limited extent what they are doing.

Root Certificate Authority (Root CA)
A *certificate authority* which utilizes a *self-signed* CA certificate when issuing *certificates*.

SCRAM
A family of secure password-based *SASL* authentication mechanisms. The family includes SCRAM-SHA-1 and SCRAM-SHA-1-PLUS mechanisms, the latter utilizes *TLS* channel bindings. SCRAM is an acronym that stands for Salted Challenge Response Authentication Mechanism. Both SCRAM-SHA-1 and SCRAM-SHA-1-PLUS are mandatory-to-implement authentication mechanismss in *XMPP*. See [RFC5802].
See Also PLAIN.

Security Information Object (SIO)
An object used in making security systems, particularly access control systems. Examples of security information objects include policy, security label, clearance objects. See [SDN.801].
See Also Clearance, Security Label, Security Policy.

Security Label
A structured representation of the sensitivity of a piece of information. A security label is sometimes referred to as a confidentiality label. See [SDN.801].
See Also Clearance, Security Policy.

Security Policy
In the context of M-Link, a policy which governs access control decisions based upon a security label and a clearance. The policy also specifies how produce display markings for security labels. M-Link utilizes expects security policies to be represented in the *XML SPIF* open format. See [SDN.801].
See Also Clearance, Security Label, Security Information Object (SIO).

Security Policy Information File (SPIF)
A file format for representing a security policy. While there exists a number of ASN.1 based SPIF variants, Isode M-Link utilizes the more modern *XML SPIF* open format. See [SDN.801].
See Also Security Policy.

Self-Signed Certificate
A *certificate* which is signed by same entity which the certificate provide identity for.

Service Principal Name (SPN)
A format used to name instances of services in *Windows* systems. A service principal name uniquely identifies an instance of a service in Active Directory.

Simple Authentication and Security Layer (SASL)
A framework which provides authentication and authorization mechanisms to Internet protocols such as *XMPP*. See [RFC4422].

Simple Network Management Protocol (SNMP)
An Internet protocol for managing network devices and services.

Single sign-on (SSO)
Describes an access control system which allows a user, by authenticating to a system, to access multiple independent systems and/or services.
See Also Windows Integrated Single Sign-On (Windows SSO), Smart Card.

Smart Card
Smart cards are credit card sized devices used to provide *single sign-on* authentication services in enterprises. M-Link Server supports smart card authentication of users through use of *TLS* and *Simple Authentication and Security Layer EXTERNAL*.

Sodium
Isode's directory data administration tool, a *LDAP client*. Though always written as "Sodium", Sodium is acronym standing for Secure Open Data, Identity and User Manager. Sodium is used for provisioning of users in *M-Vault Server*. deployments.

Stanza
In *XMPP* one of three types of first-level routable elements of the protocol: message, presence; or info/query (IQ) element. A <message/>, Presence or <iq/> element of either the `jabber:client` or `jabber:server` namespaces at depth of 1 in an XMPP stream. Other first-level elements, termed *nonzas*, the protocol are not routable. See [RFC6120].

Transmission Control Protocol (TCP)
A stream-oriented protocol for providing reliable data communications over the Internet. TCP is the primary transport protocol for *XMPP*. See [RFC0793].

Transport Layer Security (TLS)
A protocol used by application protocols, such as *XMPP*, to provide communications security. It is formally known as Secure Socket Layer (SSL). See [RFC5246].

Trust Anchor (TA)
A certificate of a certificate authority trusted to issue (directly or indirectly) certificates for entities a party wishes to authenticate.

Trusted Third Party
An entity trusted by two parties, such as a client and a server, to facility *authentication* of one of the parties to the other or both parties to each other. In *public key infrastructures*, *certificate authorities*, when trusted, are trusted third parties.

Unix
Any operating system which complies with the *Single UNIX Specification*, such as the Linux and Solaris operating systems.
See Also Windows.

User Principal Name (UPN)
A format used to name user accounts used in *Windows* systems. A user principal name uniquely identifies a user in *Active Directory*.

Windows
A family of operating system produced by Microsoft known as Microsoft Windows or simply Windows.
See Also Unix.

Windows Integrated Single Sign-On (Windows SSO)
Microsoft's *Kerberos* based *single sign-on* solution.

X.500
A set of standards devised for *the Directory*, developed jointly by the ITU-T and ISO/IEC. See [X.500].
See Also Lightweight Directory Access Protocol (LDAP).

XMPP Address
A unique identifier of an entity, such as a user or server, on the *XMPP* network. Commonly called a *JID* (for historical reasons). JID is an acronym standing for *Jabber* ID. See [RFC6122].

XMPP Extension Protocol (XEP)
An Internet standards document pertaining to extensions of the *Extensible Messaging and Presence Protocol* (XMPP). Relevant XEPs are listed in Appendix K, *References*.