

M-Switch MIXER Evaluation Guide

Configuring R19.2 core release of Isode's MIXER Gateway server on Windows and Linux platforms for use as a Gateway between SMTP and X.400 Messaging Systems that could be used in both EDI and other solutions.

Contents

Contents	2
Introduction.....	3
Objectives	3
Using Isode Support.....	5
Preparing the Server Environment	6
Naming the Server	6
Install the Isode Software	6
Activating the Isode Products.....	7
Creating the Messaging Configuration.....	8
Running the MConsole Configuration Wizard.....	8
Starting the Services	16
Configure the Switch Operations View.....	18
Creating Security Database	20
Configure the Routing Tree	20
Adding the External MTAs	23
Testing the routing and MIXER mappings	33
Testing the X.400 MTA Authentication	34
Configuring the Audit Database and Testing.....	35
Configuring the Audit Database	35
Testing	39
Using Strong Authentication With M-Switch	42
Create an Isode PKI.....	42
Configure the Security Database	45
Create Certificate for P1	51
Enable strong authentication for the local mta	55
Enable strong authentication for the external mta.....	56
Test X400p1 Strong Auth connection.....	57
What Next?.....	59
Whitepapers	59
Copyright	60

Introduction

This guide is intended to give the reader basic information on how to configure the Isode M-Switch and M-Vault server products. These Products combine to create a Mixer Messaging Solution.

More information on these products can be found at the URLs below.

<https://www.isode.com/product/x-400-message-switch/>

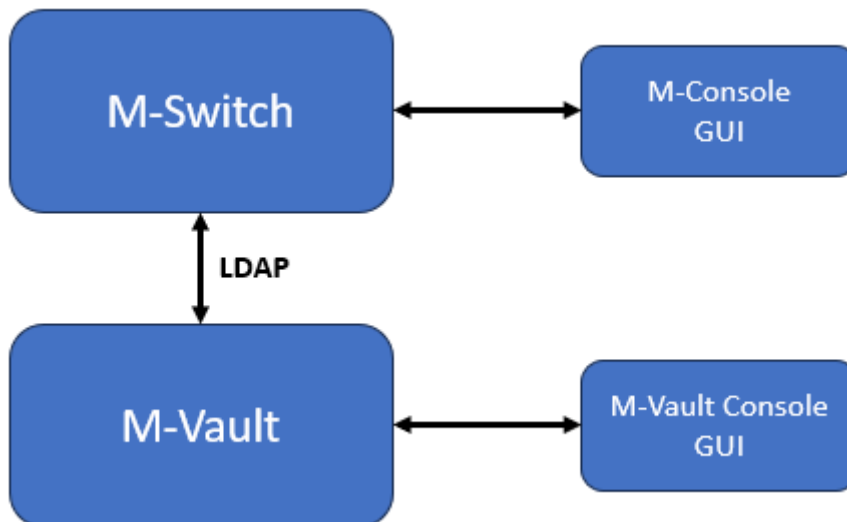
www.isode.com/product/ldap-x-500-directory/

Objectives

In this guide you will be shown how to configure the X.400 PRMD “/P=MIXER/A=ISODE/C=GB/, the internet domain mixer.net and to configure connections to other X.400 and SMTP MTAs.

The diagram below gives an overview of this setup.

System Overview

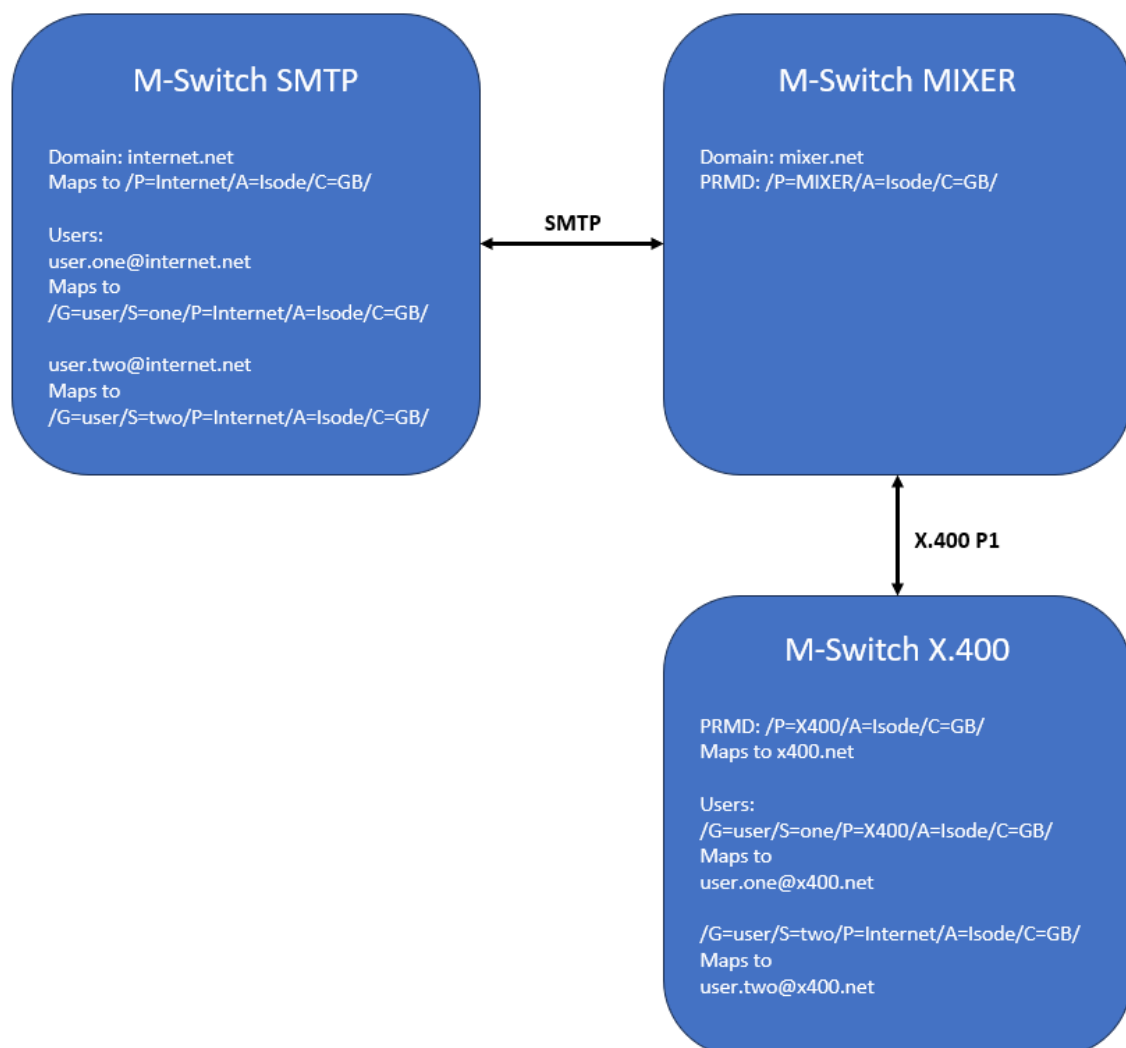


By the end of this guide, you will have:

1. Installed the M-Switch and M-Vault products.
2. Configured M-Switch and M-Vault using MConsole.
3. Configured a Connection to an external SMTP Server (M-Switch SMTP).
4. Created a connection to an external X.400 MTA server (M-Switch X.400)
5. Transferred a message between the systems in each direction.
6. Viewed the conversion using M-Console Message Tracking in the Audit Database.

This guide is part of a set of three Guides; M-Switch SMTP, M-Switch MIXER and M-Switch X.400 and they connect to each other as below.

M-Switch SMTP, M-Switch MIXER & M-Switch X.400



Using Isode Support

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

Preparing the Server Environment

You should visit <https://www.isode.com/support/platform-support/> to discover which operating systems are supported for Isode evaluations.

Naming the Server

Make the machine name: ISODE-MIXER-EVL

Make the primary dns suffix for the server MIXER.NET

Alternatively, you may use your own names or add dns entries in a dns server or hosts file.

Install the Isode Software

Follow the instructions in the release notes for the appropriate platform for the products. For this guide, the following products were used:

M-Vault 19.2v2 Core

M-Switch 19.2v2 Core

MAS 1.1V3

On Windows, select the default install options when executing the installer for the Isode Products.

Remember to install an appropriate java runtime engine (refer to product release notes) and in a Windows environment the visual c++ redistributable package.

On linux, before installation, create the user “pp” which will be used by the installation.

```
# sudo useradd pp
```

On Linux, install all the RPMs with the command:

```
# sudo rpm -i ISD*.rpm
```

The appropriate list of rpm files is :

```
ISDbase-core-19.2v2-0.x86_64.rpm
```

```
ISDdsa-core-19.2v2-0.x86_64.rpm
```

```
ISDdsaman-core-19.2v2-0.x86_64.rpm
```

```
ISDpp-core-19.2v2-0.x86_64.rpm
```

```
ISDppX-core-19.2v2-0.x86_64.rpm
```

```
ISDsodium-core-19.2v2-0.x86_64.rpm
```

ISDtps-core-19.2v2-0.x86_64.rpm

ISDx400-core-19.2v2-0.x86_64.rpm

Please use a supported web browser as documented in the product release notes.

Activating the Isode Products

The Isode Products are Activated using the Isode Messaging Activation Server (MAS). You should refer to the MAS Evaluation Guide for how to activate the products. When requesting the activation from Isode Support, ask for M-Vault Core and M-Switch Mixer Core for a “R19.2 Core M-Switch Mixer Evaluation”. If evaluating P3/P7 Strong Authentication, please make this clear.

Creating the Messaging Configuration

Running the MConsole Configuration Wizard

In this chapter we will create the Messaging Configuration using the Mconsole administration tool. The configuration is stored in the M-Vault DSA, which we will also create as part of this process.

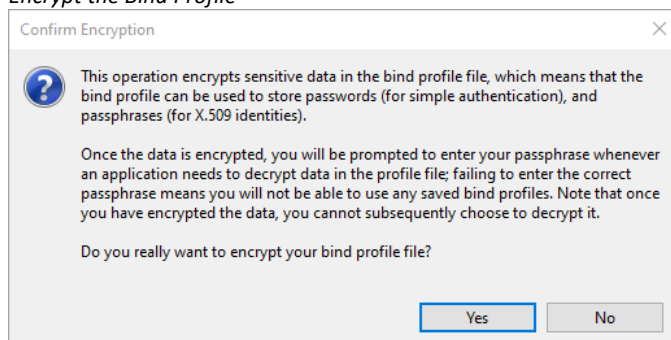
On Windows, start MConsole from the Windows Start Menu.

On Linux type the command:

```
# /opt/isode/bin/mconsole
```

You will see the following prompt:

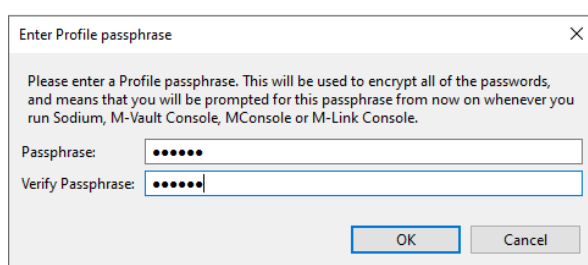
Encrypt the Bind Profile



Click “Yes”

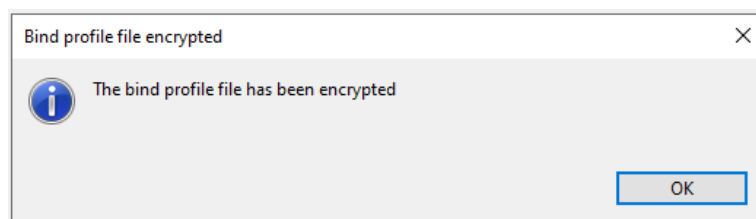
Enter and verify the password “Secret1+”

Provide the Bind Profile Passphrase



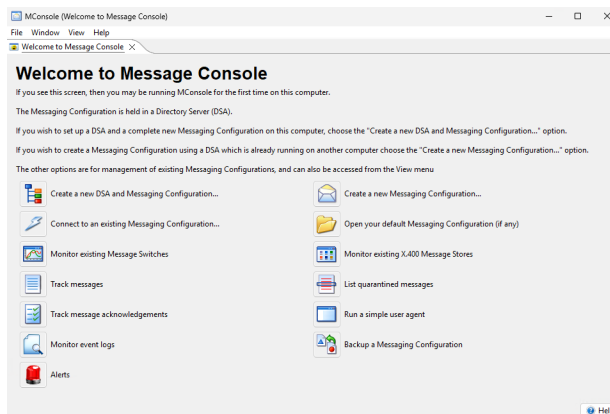
Click “OK”

Bind Profile Encrypted



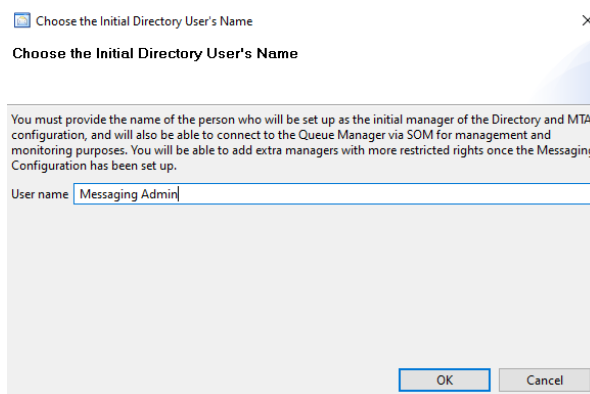
Click “OK”

MConsole Welcome Screen



Select “Create a new DSA and Messaging Configuration ...”.

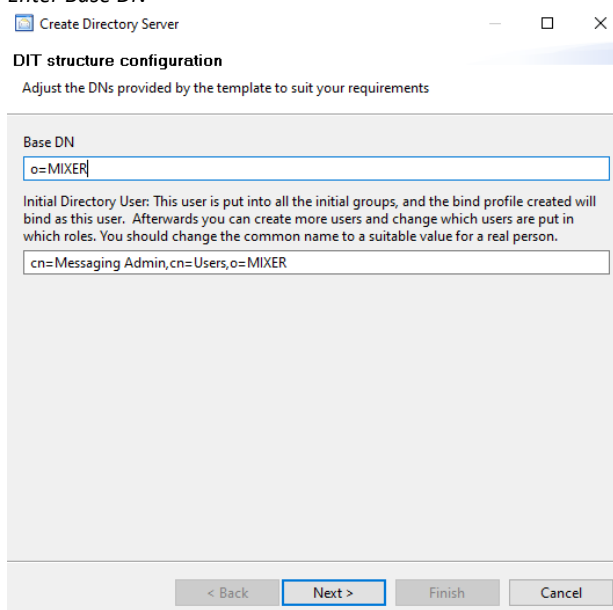
Enter User Name



Typically, we use “Messaging Admin” here, but you can choose your own if you wish.

Enter your User name and Click “OK”.

Enter Base DN



Enter the Base Distinguished Name (DN) for your directory server. You can use the default or choose one of your own.

In this guide we have changed the Base DN to “o=MIXER”.

Click “Next >”

Enter Password

Create Directory Server

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

Initial Directory User: cn=Messaging Admin,cn=Users,o=MIXER

Password: Secret1+ ☒ Show

☐ Record user authentication times (authTimestamps)

Password Hashing
Hashed passwords are more secure, but are not compatible with password-based SASL mechanisms other than PLAIN, LOGIN and SCRAM-SHA-1, SCRAM-SHA-256, SCRAM-SHA-512.
Note that while non-hashed passwords may be recovered from the DSA database, hashed passwords are NOT recoverable.

Password hashing:
SCRAM-SHA-1

The GUI will auto-create a password for the initial directory user – but you can change this to one of your own. In this guide we will use “Secret1+”.

Click “Next >”

Bind Profile Summary

Create Directory Server

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

Management bind profile name: Used to manage the DSA in M-Vault Console
cn=dsa,o=MIXER / Messaging Admin

The folder which will contain the directory server's database and configuration (this folder will be created in order to initialize the DSA):
C:\isode\d3-db

Click “Next >”

Directory Server Summary

Create Directory Server

Address Configuration

Enter the server hostname / IP address and ports to listen on

Hostname:

Enable:

☒ LDAP ☒ DAP

Port numbers:

☐ Standards, no messaging: 389 / 102

☐ Standards with messaging: 389 / 19999

☒ Isode default: 19389 / 19999

☐ Alternate 2: 29389 / 29999

☐ Alternate 3: 39389 / 39999

☐ Alternate 4: 49389 / 49999

☐ Alternate 5: 59389 / 59999

Change the “Hostname” to “ISODE-MIXER-EVL.MIXER.NET”

Click “Next >”

Directory Server Configuration Confirmation

Create Directory Server

Confirm Details

Check the details below before creating the DSA

DSA creation template:
Simple DSA setup for Messaging Evaluations

DSA address:
Host ISODE-MIXER-EVL.MIXER.NET, X.500 on port 19999, LDAP on port 19389

DSA name:
cn=dsa,o=MIXER

Bind profile name:
cn=dsa,o=MIXER / Messaging Admin

Password hashing:
SCRAM-SHA-1

Click “Finish”

You may see the following – wait.

Directory Server Creation and Starting

Background Task Progress

Creating and starting DSA ...

You will then see the following screen.

Product Activation Summary

Product Activation

The Product Activation information on this system is shown here.

Product Activation information: M-Switch is activated, Product is "M-Switch MIXER"

Activated subfeatures are: TLS, x400, smtp, p3p7strong-auth

The remainder of this Messaging Configuration wizard will create a configuration appropriate for M-Switch MIXER

If this is incorrect, contact support@isode.com for a suitable Product Activation Key

< Back **Next >** Finish Cancel

Click "Next >"

Set the Messaging Configuration Base DN

Set the Messaging Configuration Base DN

Select the entry under which a Messaging Configuration entry will be created

> o=MIXER

If you provide an organization name, an entry for the organization name provided will be created automatically under the entry you select.

☐ Create organization name

Messaging configuration name
Messaging Configuration

Base DN: o=MIXER
MHS DN: cn=Messaging Configuration,o=MIXER

< Back **Next >** Finish Cancel

Select the top entry, o=MIXER.

Click "Next >"

Set the Hostname

Hostname

The hostname will be used, among other things, to set the network addresses

Hostname
Enter the fully qualified host name of the machine that will be running this server. For example, mail.isode.com. If not possible, then use the host name.

ISODE-MIXER-EVL.MIXER.NET

< Back **Next >** Finish Cancel

Change the “Hostname” to “ISODE-MIXER-EVL.MIXER.NET”

Click “Next >”

Provide passwords

The screenshot shows the 'Provide passwords' window titled 'Create a new MHS configuration'. It contains the following text and fields:

Password and Security
The SASL Password is used by M-Switch when it connects to M-Vault in order to access its configuration

The SASL Password is used by M-Switch to connect to M-Vault. The SASL Password will be encrypted using the service passphrase

SASL Password: Secret1+ [Hide]

The service passphrase, which will be used to encrypt the SASL password

Passphrase for M-Switch Service: Secret1+Secret1+ [Hide]

At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted.

Provide SASL and passphrase encryption passwords

Click “Next >”

Create Initial Security Database

The screenshot shows the 'Create Initial Security Database' window titled 'Create a new MHS configuration'. It contains the following text and fields:

Create Initial Security Database
Set up a Security Database including a self-signed certificate

Security database file name: switch\mta.secdm

Passphrase: Secret1+ [Hide]

At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted.

Provide the “Security Database Password”

Click “Next >”

SMTP Channel Settings

The screenshot shows the 'SMTP Channel Settings' window titled 'Create a new MHS configuration'. It contains the following text and fields:

SMTP channel specific settings and routing policy
Enter the internet domain regarded as local to this MTA.

The email address domain this MTA is responsible for, e.g isode.com

Email address domain: mixer.net

☐ Create an Internet Message Store for local POP3 or IMAP users

☐ Use DNS

☐ Use MX records

☒ Don't use DNS

At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted.

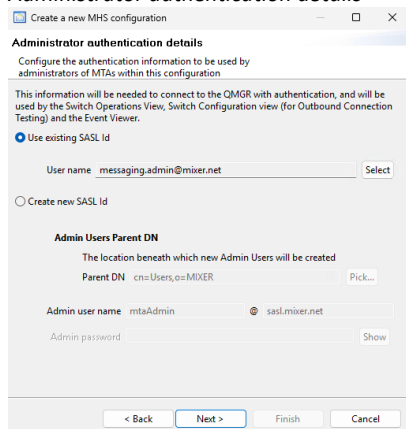
Enter the mixer internet mail domain, we will use “mixer.net”

Uncheck “Create an Internet Message Store...”

Check “Don’t use DNS”.

Click “Next >”

Administrator authentication details



Create a new MHS configuration

Administrator authentication details
Configure the authentication information to be used by administrators of MTAs within this configuration.

This information will be needed to connect to the QMGR with authentication, and will be used by the Switch Operations View, Switch Configuration view (for Outbound Connection Testing) and the Event Viewer.

☒ Use existing SASL id

User name: messaging.admin@mixer.net Select

☐ Create new SASL id

Admin Users Parent DN
The location beneath which new Admin Users will be created

Parent DN: cn=Users,ou=MIXER Pick...

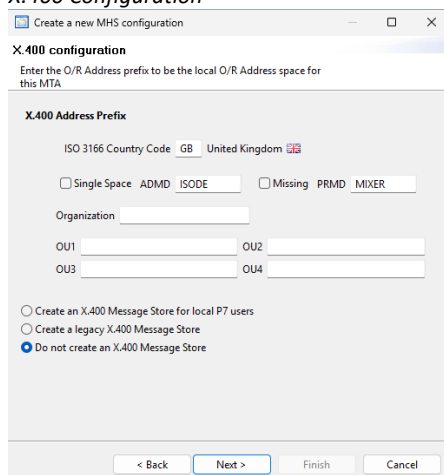
Admin user name: mtaAdmin Ⓢ sasl.mixer.net

Admin password Show

< Back **Next >** Finish Cancel

Click “Next >”

X.400 Configuration



Create a new MHS configuration

X.400 configuration
Enter the O/R Address prefix to be the local O/R Address space for this MTA

X.400 Address Prefix

ISO 3166 Country Code: GB United Kingdom 🇬🇧

☐ Single Space ADMD ISODE ☐ Missing PRMD MIXER

Organization:

OU1: OU2:

OU3: OU4:

☐ Create an X.400 Message Store for local P7 users

☐ Create a legacy X.400 Message Store

☒ Do not create an X.400 Message Store

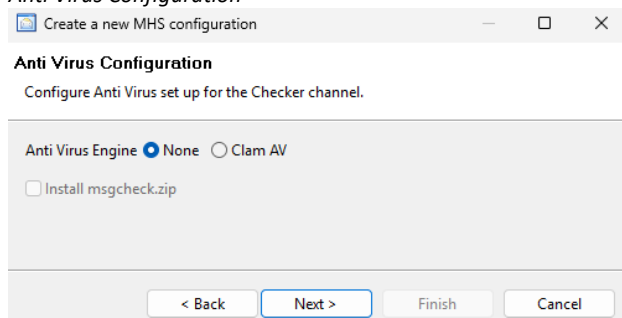
< Back **Next >** Finish Cancel

Provide the X400 Address Prefix for the node : /C=GB/ADMD=ISODE/PRMD=MIXER/

Check “Do not create an X.400 Message Store”

Click “Next >”

Anti Virus Configuration



Create a new MHS configuration

Anti Virus Configuration
Configure Anti Virus set up for the Checker channel.

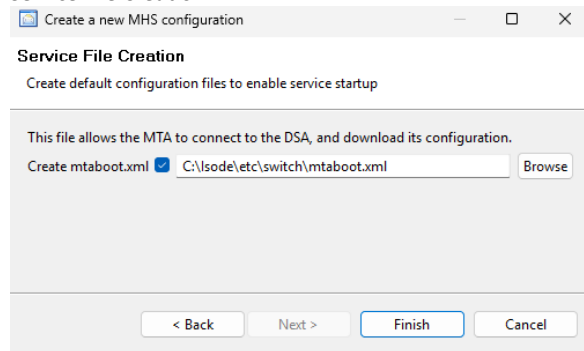
Anti Virus Engine ☒ None ☐ Clam AV

☐ Install msgcheck.zip

< Back **Next >** Finish Cancel

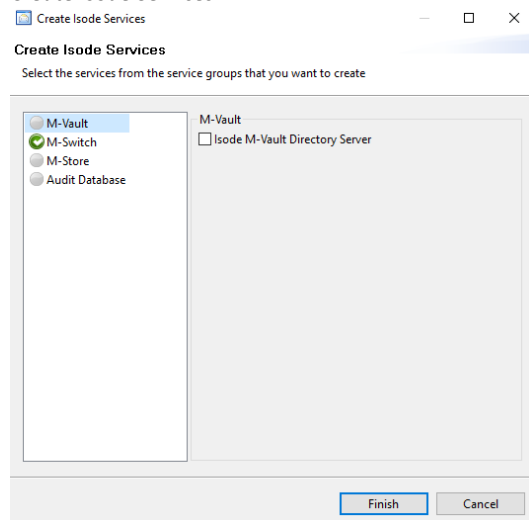
Click “Next >”

Service File Creation



Click “Finish”

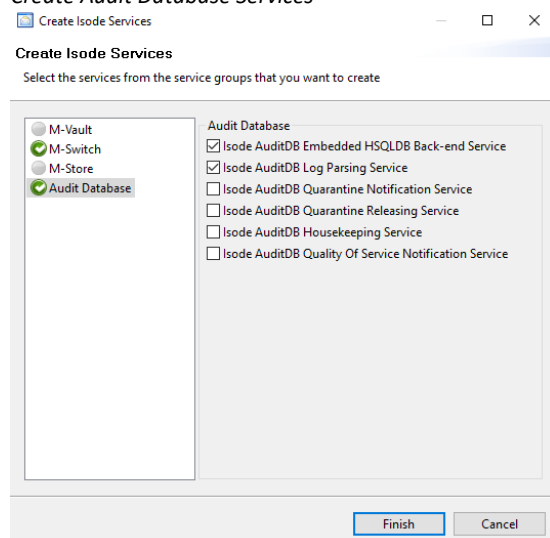
Create Isode Services



The above dialog only appears on Windows.

In this guide we will show you how to configure the Audit Database on Windows. Select “Audit Database” in the left-hand pane.

Create Audit Database Services

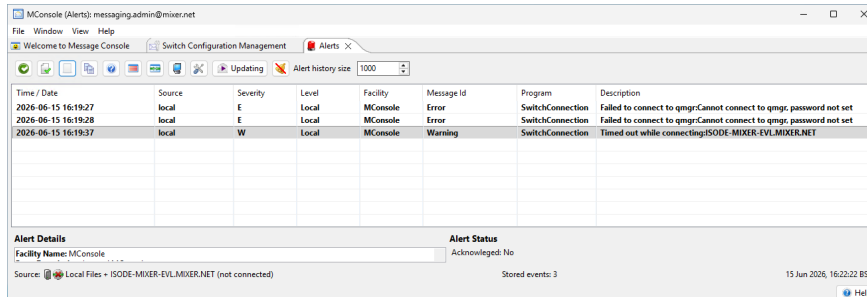


Check “Isode AuditDB Embedded HSQLDB Back-end Service” and “Isode AuditDB Log Parsing Service”

Click “Finish”

Note that the following connection alerts are expected at this stage of configuration

Connection Timeout Alerts



The screenshot shows the MConsole Alerts tab with a table of alerts. The table has columns: Time / Date, Source, Severity, Level, Facility, Message Id, Program, and Description. There are three alerts listed, all from 'local' source, with 'Warning' severity and 'MConsole' level. The descriptions indicate connection failures to 'qmqr' and 'ISODE-MIXER-EVL.MIXER.NET'.

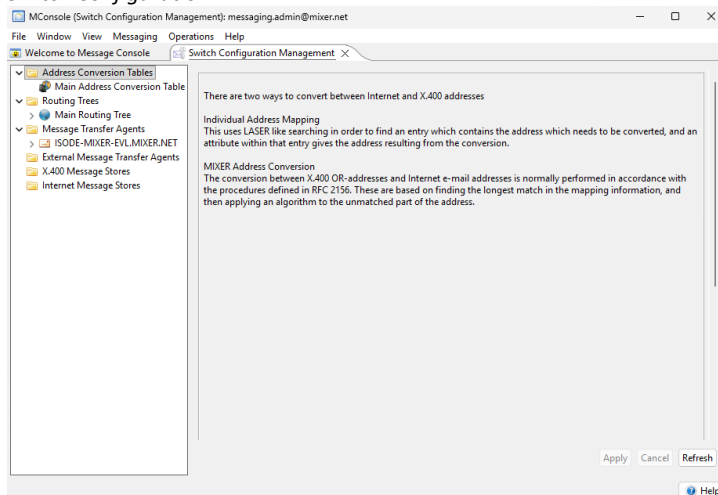
Time / Date	Source	Severity	Level	Facility	Message Id	Program	Description
2026-06-15 16:19:27	local	E	Local	MConsole	Error	SwitchConnection	Failed to connect to qmqr:Cannot connect to qmqr: password not set
2026-06-15 16:19:28	local	E	Local	MConsole	Error	SwitchConnection	Failed to connect to qmqr:Cannot connect to qmqr: password not set
2026-06-15 16:19:37	local	W	Local	MConsole	Warning	SwitchConnection	Timed out while connecting ISODE-MIXER-EVL.MIXER.NET

Below the table, the 'Alert Details' section shows 'Facility Name: MConsole' and 'Source: Local Files + ISODE-MIXER-EVL.MIXER.NET (not connected)'. The 'Alert Status' section shows 'Acknowledged: No' and 'Stored events: 3'.

The alerts tab can be safely closed.

The following screen is displayed.

Switch Configuration



You have now completed the initial configuration of M-Switch MIXER. We now need to start the services.

Starting the Services

On Linux use the following commands to start the services:

```
systemctl start isode-dsa@d3-db
```

```
systemctl start pp
```

In order to ensure that the services start when the machine boots, use the following commands:

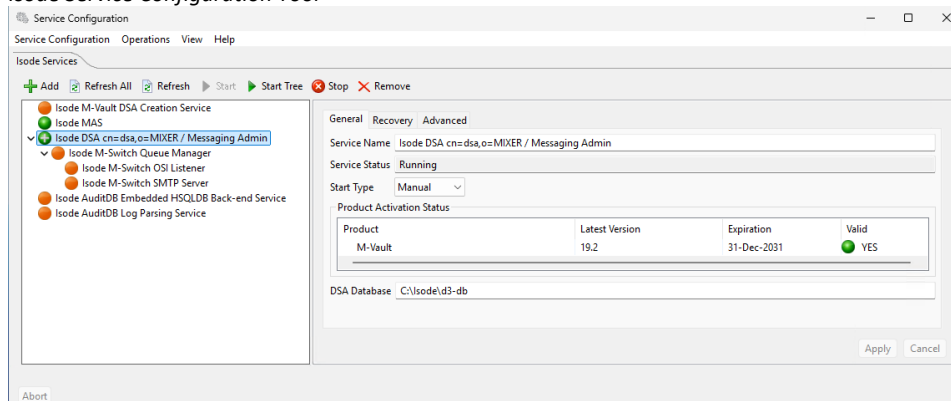
```
systemctl enable isode-dsa@d3-db
```

```
systemctl enable pp
```

On Windows, open “Isode Service Configuration” From the Windows Start Menu

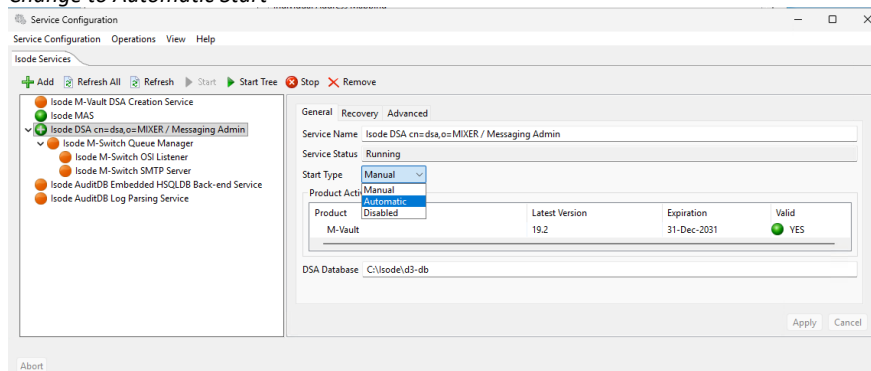
The following screen is displayed :

Isode Service Configuration Tool



Select the Isode DSA service

Change to Automatic Start



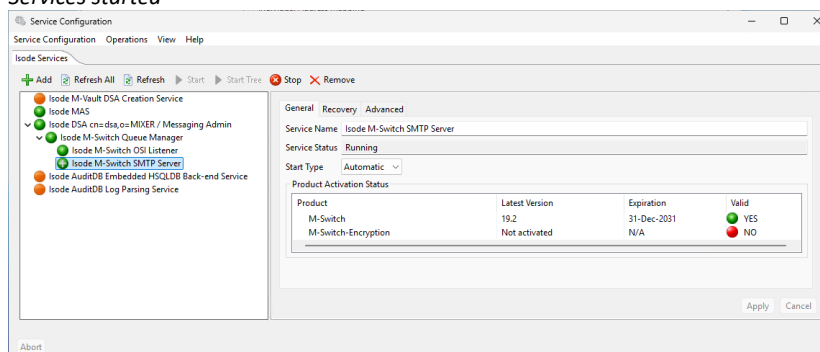
Change the “Start Type” from “Manual” to “Automatic” using the dropdown.

Click “Apply”

Repeat this for the “Isode AuditDB Embedded HSQLDB Back End Service”, “Isode AuditDB Log Parsing Service”, “Isode M-Switch Queue Manager”, “Isode M-Switch OSI Listener” and “Isode M-Switch SMTP Server”.

Start the “Isode M-Switch Queue Manager”, “Isode M-Switch OSI Listener” and “Isode M-Switch SMTP Server” Services.

Services started



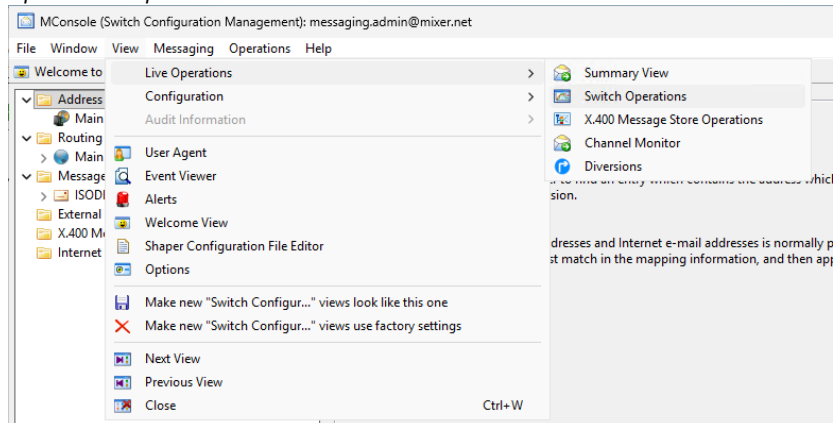
Return to MConsole

Configure the Switch Operations View

The switch operations view communicates with the Switch queue manager using the SOM protocol. We need to configure that connection in order to manage message queues and ensure that most configuration changes in MConsole are implemented immediately.

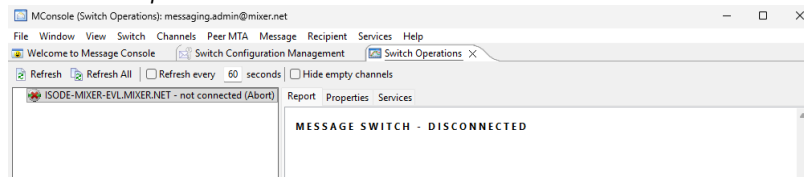
From the MConsole top menu select View→Live Operations→Switch Operations

Open switch operations view



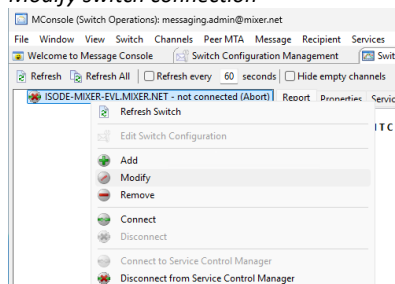
The following error is expected :

Initial Switch operations view



Right Click on the switch displayed and select “Modify”

Modify switch connection



Enter the password you entered when creating the “Initial Directory User”

Provide Connection Password

Edit Message Switch

Friendly Name: ISODE-MIXER-EVL.MIXER.NET

Host: ISODE-MIXER-EVL.MIXER.NET

Userid: messaging.admin@mixer.net

Password: Secret1+ Hide

Authentication Mechanism: SCRAM-SHA-1

Use TLS for SOM protocol: ☐

MTA: ACPI27 Monitoring

Port: ACPI27 OTAM

MTA: ISODE-MIXER-EVL.MIXER.NET

Port ☐ Override port

No services ☐

Host Aliases

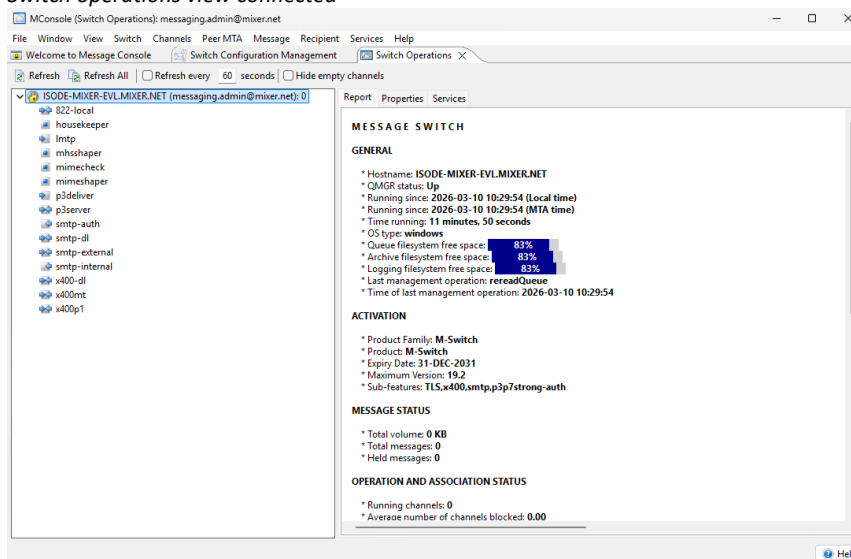
The hostname is required to be set, either as the host or an alias to allow MConsole to connect to the window service controller.

OK Cancel

Click “OK”.

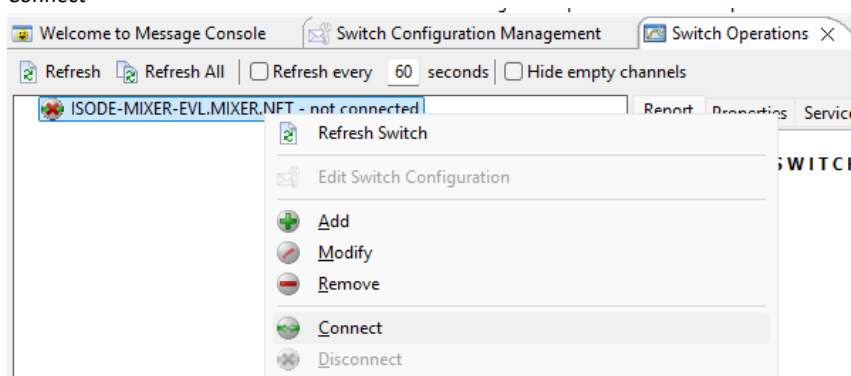
The following screen should be displayed :

Switch operations view connected



If not, try right clicking on the switch and choosing “Connect”

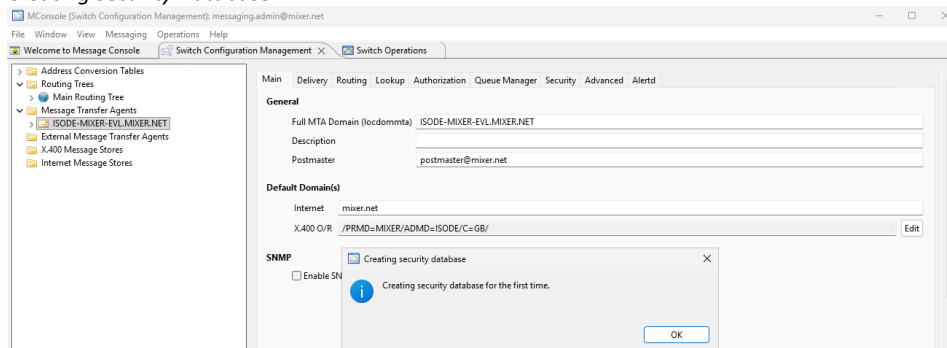
Connect



Creating Security Database

In the Switch Configuration Management view, select the switch object.

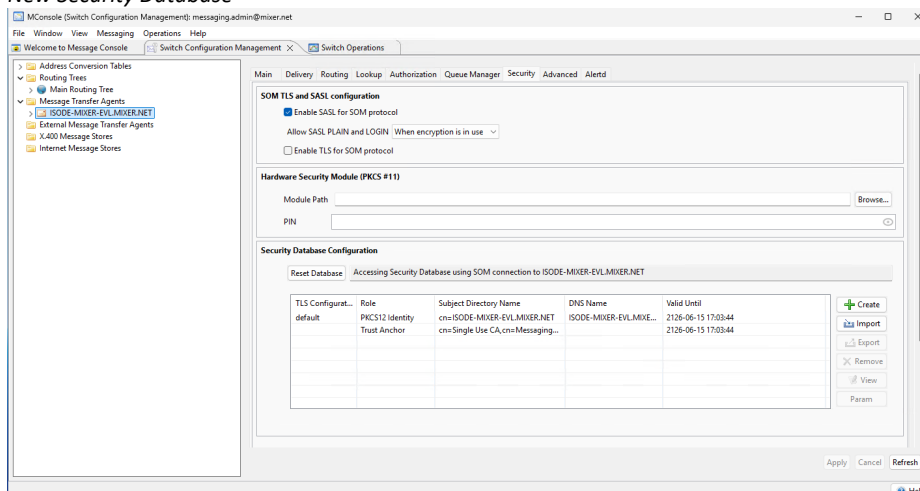
Creating Security Database



On the “Creating Security Database” warning click on “OK”

Select the “Security” tab.

New Security Database

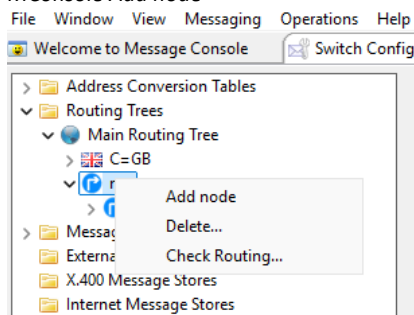


Note that a database has been created with a single use CA trust anchor and a self-signed certificate.

Configure the Routing Tree

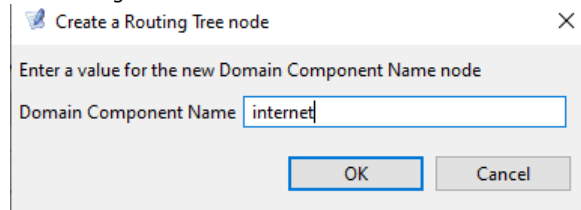
Expand the smtp Routing tree to the node “net” and right-click on it

MConsole Add node



Select “Add node”

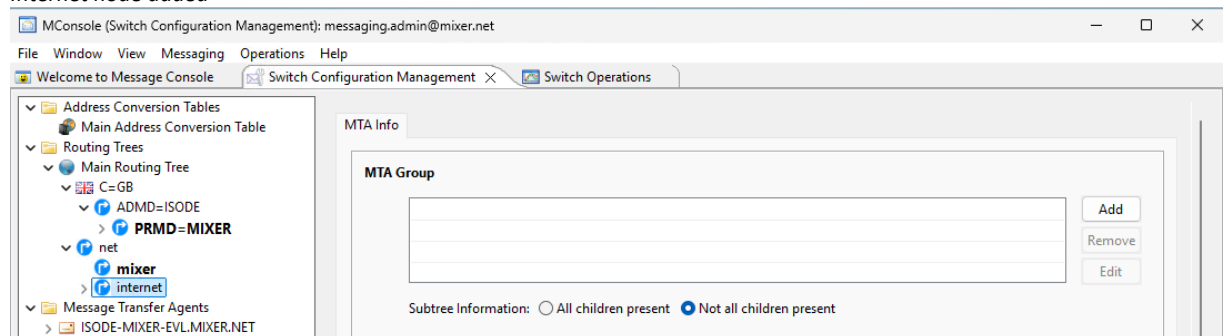
Add routing tree node



Type “internet”

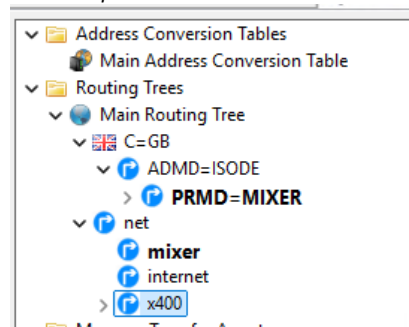
Click “OK”

Internet node added



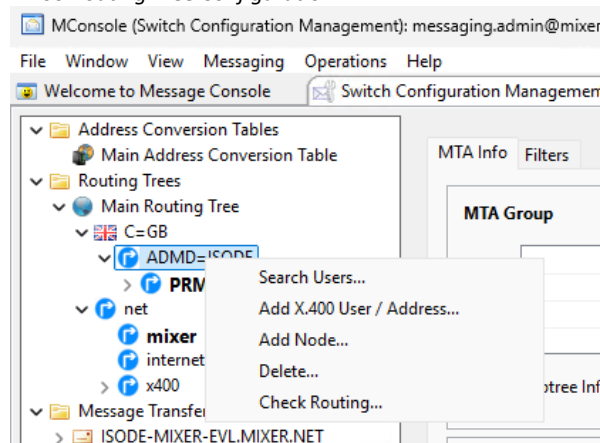
Repeat the above to add the smtp node “x400”

X400 smtp node added



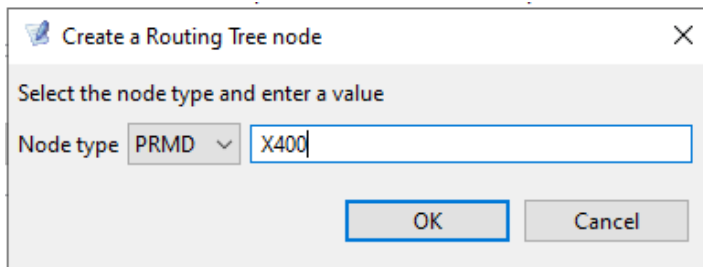
Expand the X400 routing tree and right-click on the Node “ADMD=ISODE”

X.400 Routing Tree Configuration



Select “Add Node...”

Add PRMD X400 to X400 tree



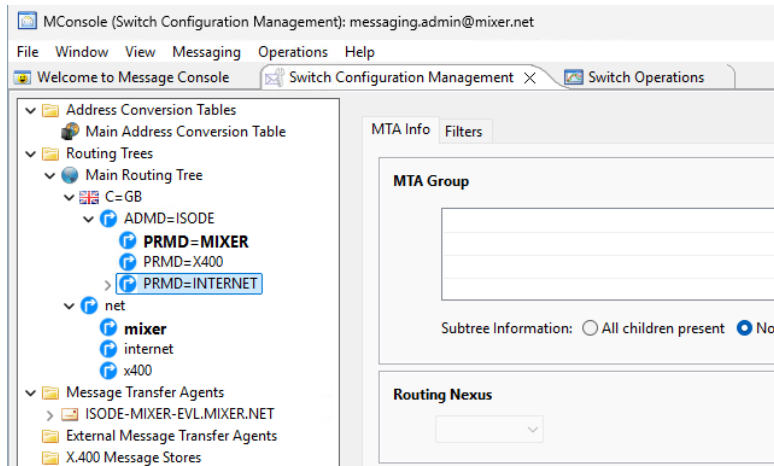
A dialog box titled "Create a Routing Tree node" with a close button (X) in the top right corner. The main instruction is "Select the node type and enter a value". Below this, there is a "Node type" dropdown menu set to "PRMD" and a text input field containing "X400". At the bottom, there are "OK" and "Cancel" buttons.

Type "X400"

Click "OK"

Repeat the above to add node "PRMD=INTERNET" under the node "ADMD=ISODE"

Additional PRMD nodes added



We will return to the routing tree configuration later.

Adding the External MTAs

Before connecting to an External MTA, you will need to exchange information with the owner of the MTA as follows:

MTA :

Your MTA Name:

Your MTA Password:

Your Hostname/IP Address:

Their MTA Name:

Their MTA Password:

Their Hostname/IP Address:

In this guide we will be connecting to the M-Switch X400 MTA described in the M-Switch X400 Evaluation Guide and the M-Switch SMTP MTA described in the M-Switch SMTP Evaluation guide. We will use the following information.

SMTP MTA :

Your Hostname/IP Address: ISODE-MIXER-EVL.MIXER.NET

Their Hostname/IP Address: ISODE-SMTP-EVAL.INTERNET.NET

X400 MTA :

Your MTA Name: ISODE-MIXER-EVL.MIXER.NET

Your MTA Password: Secret1+

Your Hostname/IP Address: ISODE-MIXER-EVL.MIXER.NET

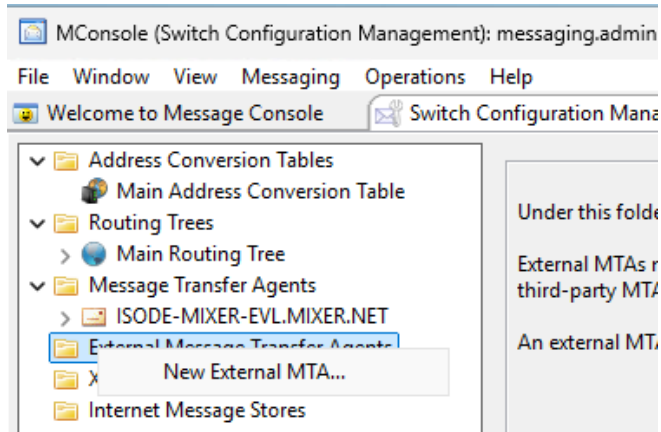
Their MTA Name: ISODE-X400-EVAL.X400.NET

Their MTA Password: Secret1+

Their Hostname/IP Address: ISODE-X400-EVAL.X400.NET

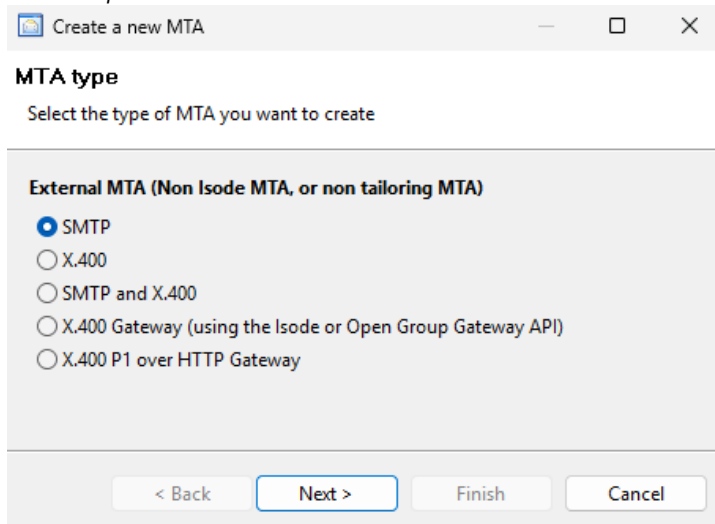
From MConsole Right Click on “External Message Transfer Agents”

New External MTA



Select “New External MTA...”

Select smtp External MTA



Select “SMTP”

Click “Next >”

Add External SMTP MTA

MTA Naming

An External Internet MTA can be given an arbitrary name in your Messaging Configuration

The local name for the external MTA in this configuration

Directory Name

The mail domain or host name to which messages queued to this MTA will be transferred. It is also possible to specify an IP address, but that will require the use of an SMTP channel which has the "nomx" flag set to communicate with this MTA

Destination

Optional local description for the new MTA

Description

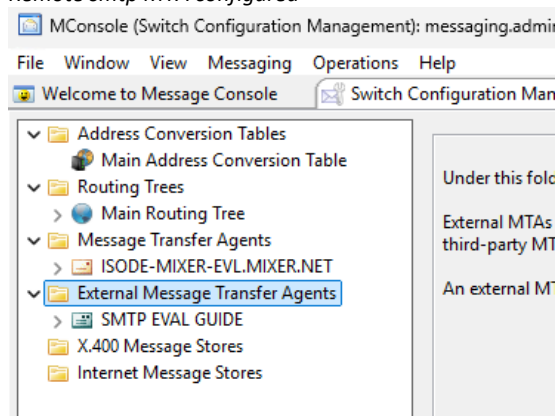
< Back Next > Finish Cancel

The “Directory Name” is free text and should be something to help you identify it.

In the “Destination” type “ISODE-SMTP-EVAL.INTERNET.NET”

Click “Finish”

Remote smtp MTA configured



We follow a similar process for the External X.400 MTA, again Right Click on “External Message Transfer Agents” and select “New External MTA...”.

Add X400 External MTA

MTA type

Select the type of MTA you want to create

External MTA (Non Isode MTA, or non tailoring MTA)

☐ SMTP

☒ X.400

☐ SMTP and X.400

☐ X.400 Gateway (using the Isode or Open Group Gateway API)

☐ X.400 P1 over HTTP Gateway

< Back Next > Finish Cancel

Select “X.400”

Click “Next >”

External X400 MTA parameters

MTA Naming

MTAs can be named in a number of different ways, depending on the context.

The MTA Name, to be used in protocols (like X.400 P1 binds)

MTA name in protocol ISODE-X400-EVAL.X400.NET

The host name or IP address of the system on which the MTA will run

Fully Qualified Hostname isode-x400-eval.x400.net

The local Directory Name in this configuration (defaults to MTA Name)

Directory Name X.400 EVAL GUIDE

Optional local description for the new MTA

Description

< Back Next > Finish Cancel

Provide the “MTA Name” to be used in the X.400 bind, the fully qualified hostname or IP address of the remote MTA and a helpful description for the connection.

Click “Next >”

Select location in routing tree

Default Routing Tree for this MTA

Routing will be setup for the O/R Address Prefix selected, and the default Internet domain selected earlier.

Choose a Routing Tree or Address Conversion Table. Use the tree navigation tool to select a partial or complete O/R address, and then modify this value if necessary via the Edit button.

cn=Main Routing Tree,cn=Messaging Configuration,o=MIXER

- Main Routing Tree
 - C=GB
 - ADMD=ISODE
 - PRMD=INTERNET
 - PRMD=MIXER
 - PRMD=X400

> net

Selected O/R Address

O/R Address /PRMD=X400/ADMD=ISODE/C=GB/ Edit

< Back Next > Finish Cancel

Expand the “Main Routing Tree” and select the node “PRMD=X400”

Click “Next >”

Provide remote mta password

Remote X.400 MTA authentication details

Configure the authentication information to be used to connect to this External X.400 MTA

Remote MTA Name to use in the bind ISODE-X400-EVAL.X400.NET

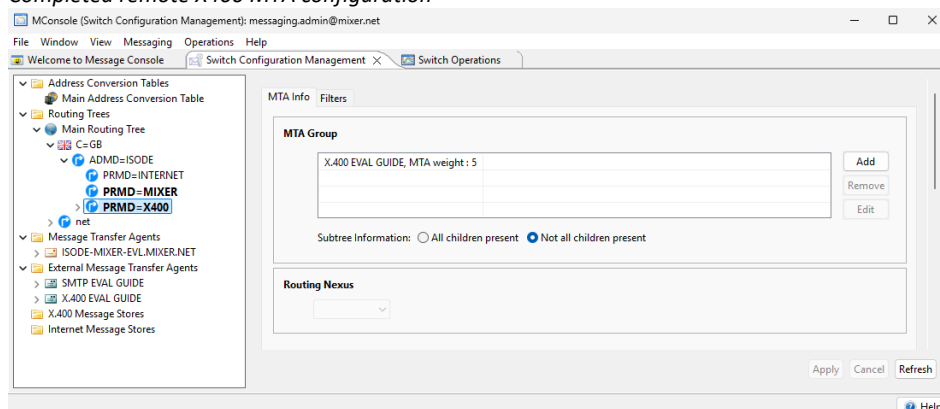
Remote MTA password to use in the bind Secret1+ Hide

< Back Next > Finish Cancel

Provide the “Remote MTA password” to use in the bind from the earlier table.

Click “Finish”.

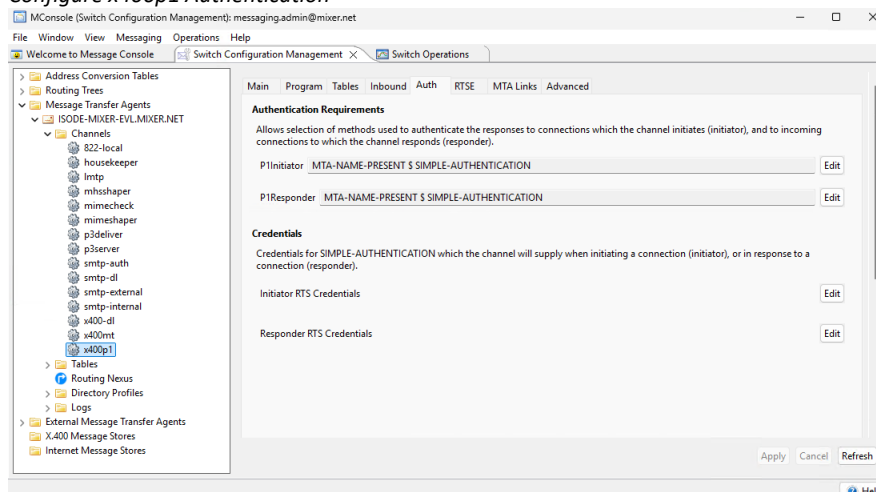
Completed remote X400 MTA configuration



We now need to configure the Authentication details for our local MTA.

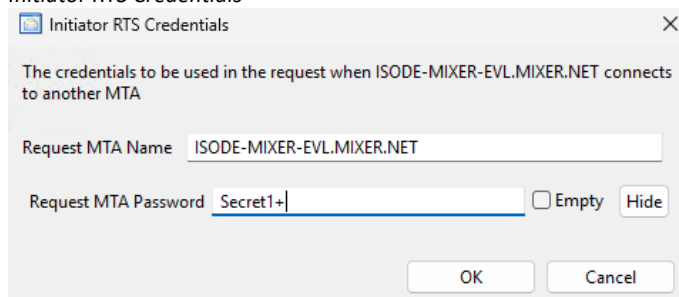
Expand the MTA and channels then select the “x400p1” channel and select the “Auth” tab

Configure x400p1 Authentication



Click “Edit” on the “Initiator RTS Credentials”

Initiator RTS Credentials

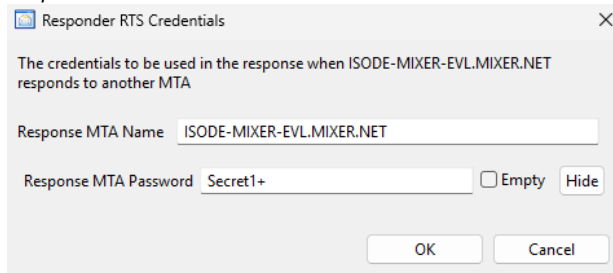


Change the “Request MTA Password” to “Secret1+”

Click “OK”

Do the same for the “Responder RTS Credentials”

Responder RTS Credentials



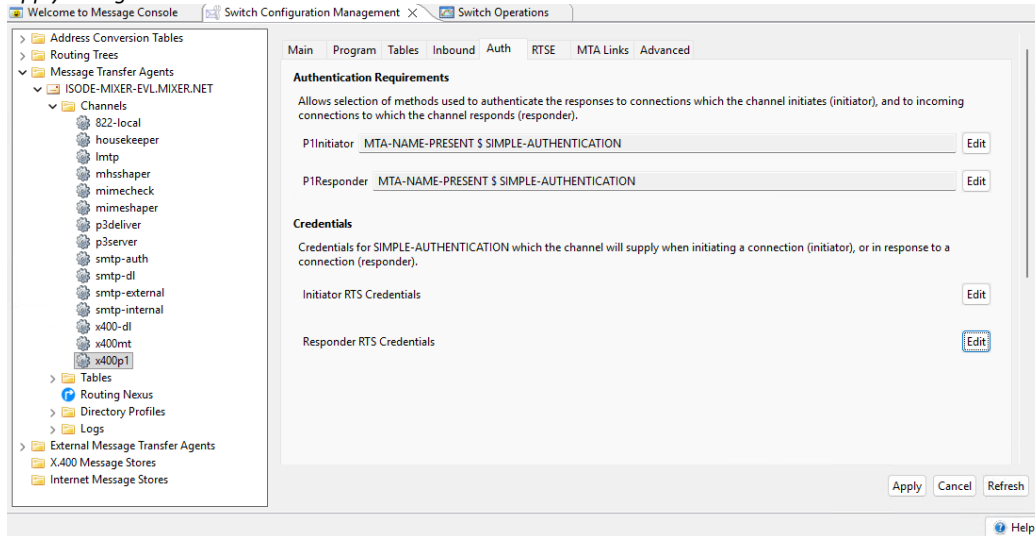
The credentials to be used in the response when ISODE-MIXER-EVL.MIXER.NET responds to another MTA

Response MTA Name

Response MTA Password ☐ Empty

Click “OK”

Apply changes



Welcome to Message Console | Switch Configuration Management | Switch Operations

Main | Program | Tables | Inbound | Auth | RTSE | MTA Links | Advanced

Authentication Requirements
Allows selection of methods used to authenticate the responses to connections which the channel initiates (initiator), and to incoming connections to which the channel responds (responder).

P1Initiator

P1Responder

Credentials
Credentials for SIMPLE-AUTHENTICATION which the channel will supply when initiating a connection (initiator), or in response to a connection (responder).

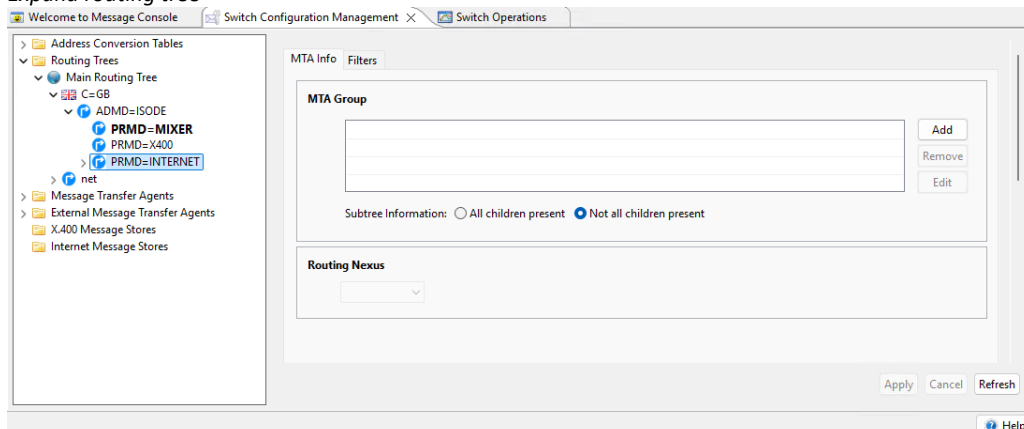
Initiator RTS Credentials

Responder RTS Credentials

Click “Apply”

We now need to configure the routing, Expand the X400 Routing Tree

Expand routing tree



Welcome to Message Console | Switch Configuration Management | Switch Operations

MTA Info | Filters

MTA Group

Subtree Information: ☐ All children present ☒ Not all children present

Routing Nexus

Select “PRMD=Internet” and Click “Add”.

Configure routing to internet

By editing the MTA information for this routing tree node, you can set the routing for the selected O/R hierarchy. The DN configured in the MTAInfo is the DN of an MTA.

Routing for this node

Select the MTA that is going to handle this node

cn=ISODE-MIXER-EVL.MIXER.NET
cn=ISODE-MIXER-EVL.MIXER.NET
cn=SMTP EVAL GUIDE
cn=X.400 EVAL GUIDE

Dealing

MTA weights affect the routing algorithm: if multiple MTAs are present in a node, lower weighted MTAs are preferred.

MTA weight 5

Channel Information

In case that it's possible to contact the remote MTA using more than one channel, you can select the first one to be used by adding it to the table with a lower weight

AE title	Weight

+ Add
X Remove
Edit

OK Cancel

Select “SMTP EVAL GUIDE” from the drop down

Click “OK”

Apply internet mta

Welcome to Message Console | Switch Configuration Management | Switch Operations

Address Conversion Tables
Routing Trees
Main Routing Tree
C=GB
net
PRMD=MIXER
PRMD=X400
PRMD=INTERNET

MTA Info Filters

MTA Group

SMTP EVAL GUIDE, MTA weight: 5

Add
Remove
Edit

Subtree Information: ☐ All children present ☒ Not all children present

Routing Nexus

Apply Cancel Refresh

Help

Click “Apply”

Now navigate to the “internet” node in the smtp routing tree

Configure internet node

Welcome to Message Console | Switch Configuration Management | Switch Operations

Address Conversion Tables
Routing Trees
Main Routing Tree
C=GB
net
internet
mixer
v400

MTA Info Filters

MTA Group

Subtree Information: ☐ All children present ☒ Not all children present

Routing Nexus

Domain Synonyms

Non-wildcard synonym
Wildcard synonym

☒ Discard unmatched components on wildcard match ☐ Retain unmatched components on wildcard match

Apply Cancel Refresh

Help

Click “Add”

MConsole Configure Routing

Edit MTA Info

By editing the MTA information for this routing tree node, you can set the routing for the selected O/R hierarchy
The DN configured in the MTAInfo is the DN of an MTA

Routing for this node

Select the MTA that is going handle this node

cn=ISODE-MIXER-EVL.MIXER.NET
cn=ISODE-MIXER-EVL.MIXER.NET
cn=SMTP EVAL GUIDE
cn=X.400 EVAL GUIDE

Dealing

MTA Weights affect the routing algorithm: if multiple MTAs are present in a node, lower weighted MTAs are preferred.

MTA weight

Channel Information

In case that it's possible to contact the remote MTA using more than one channel, you can select the first one to be used by adding it to the table with a lower weight

AE title	Weight

Select “SMTP EVAL GUIDE” from the drop down.

Click “OK”

Apply smtp routing

Welcome to Message Console | Switch Configuration Management | Switch Operations

Address Conversion Tables

- Routing Trees
 - Main Routing Tree
 - Cs=GB
 - ADMD=ISODE
 - PRMD=MIXER**
 - PRMD=X400
 - PRMD=INTERNET

MTA Info Filters

MTA Group

SMTP EVAL GUIDE, MTA weight : 5

Subtree Information: ☐ All children present ☒ Not all children present

Routing Nexus

Click “Apply”

Repeat the above process to configure the “x400” internet routing node to route to the “X.400 EVAL GUIDE” MTA.

Configure x400 smtp node routing

Welcome to Message Console | Switch Configuration Management | Switch Operations

Address Conversion Tables

- Routing Trees
 - Main Routing Tree
 - Cs=GB
 - ADMD=ISODE
 - PRMD=MIXER
 - PRMD=X400
 - PRMD=INTERNET**

MTA Info

MTA Group

X.400 EVAL GUIDE, MTA weight : 5

Subtree Information: ☐ All children present ☒ Not all children present

Routing Nexus

Domain Synonyms

Non-wildcard synonym

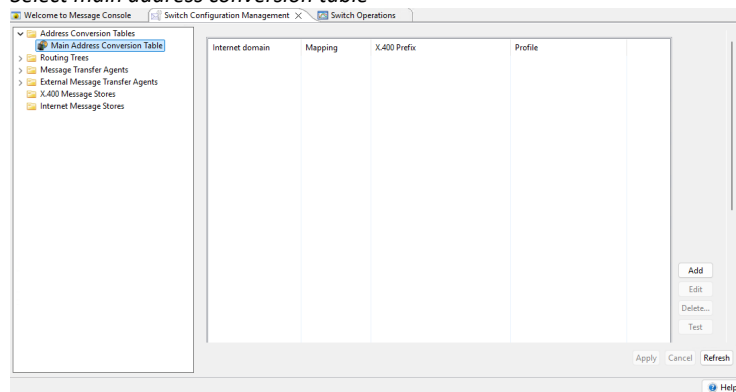
Wildcard synonym

☒ Discard unmatched components on wildcard match ☐ Retain unmatched components on wildcard match

That is the routing configuration complete, we now need to configure the MIXER Mappings.

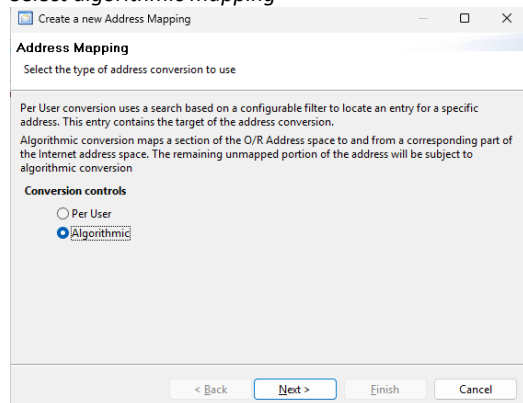
Select the “Main Address Conversion Table”

Select main address conversion table



Click “Add”

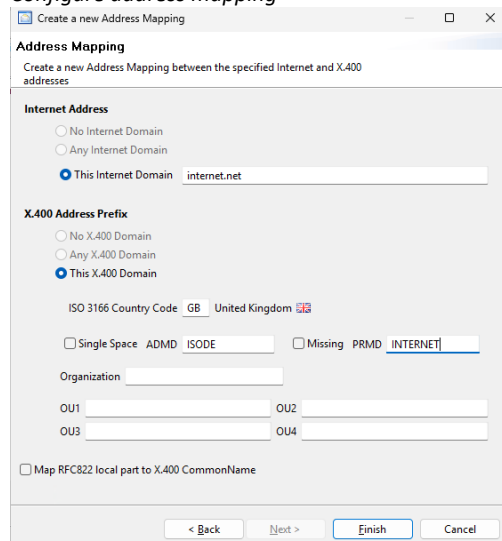
Select algorithmic mapping



Select “Algorithmic”

Click “Next >”

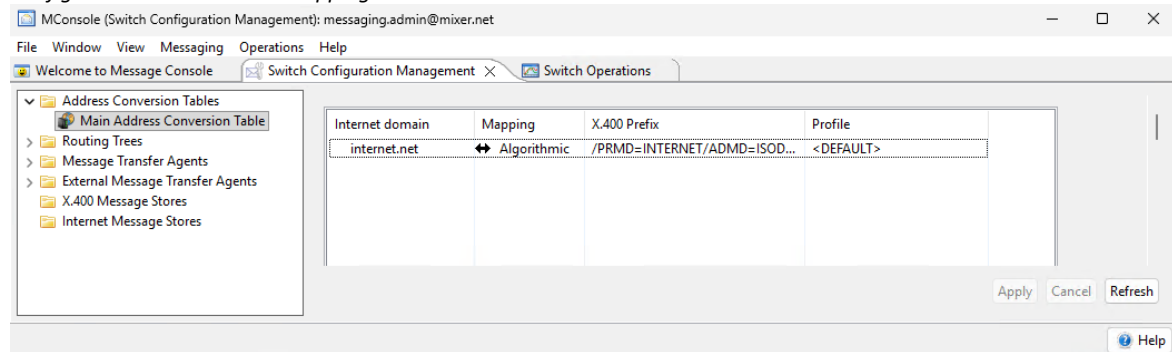
Configure address mapping



Type “internet.net” in “This Internet Domain” and enter the X.400 mapping as shown above.

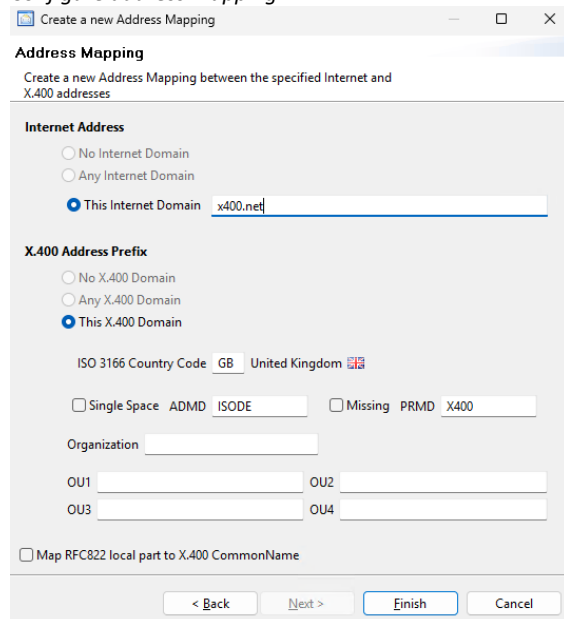
Click “Finish”

Configured internet domain mapping



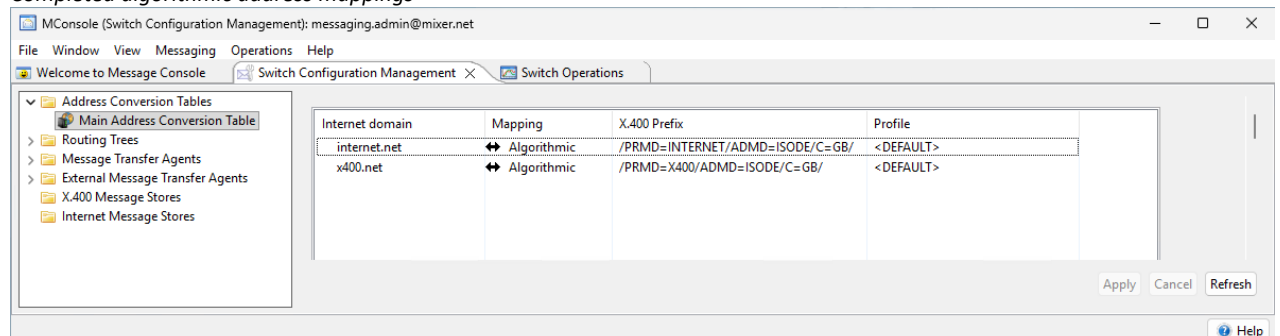
Repeat the above process for the “x400.net” internet domain

Configure address mapping



Click “Finish”

Completed algorithmic address mappings



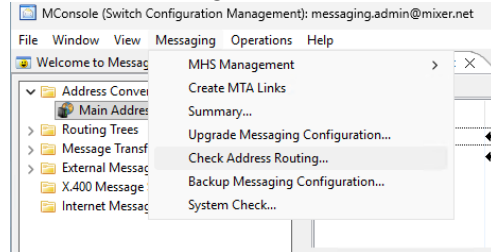
This completes the configuration of the MIXER Mappings.

We now need to test the Routing and MIXER Mappings.

Testing the routing and MIXER mappings

From the Mconsole “Switch Configuration View” menu, select “Messaging”

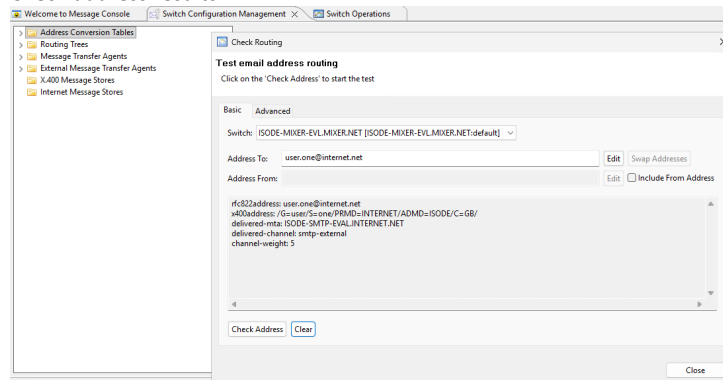
Check address routing



Select “Check Address Routing...”

In “Address To:” type “user.one@internet.net”

Check address results

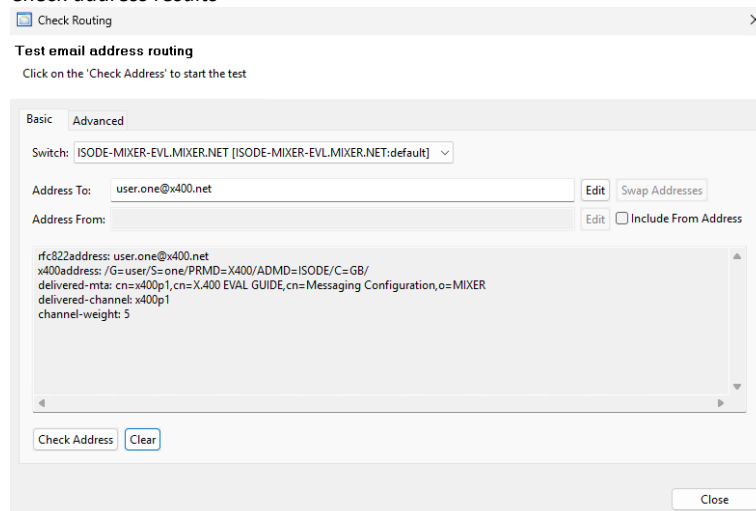


Click “Check Address”

You should see the above address mapping and that the routing is to the “smtp-external” channel.

Repeat the above process for user.one@x400.net.

Check address results



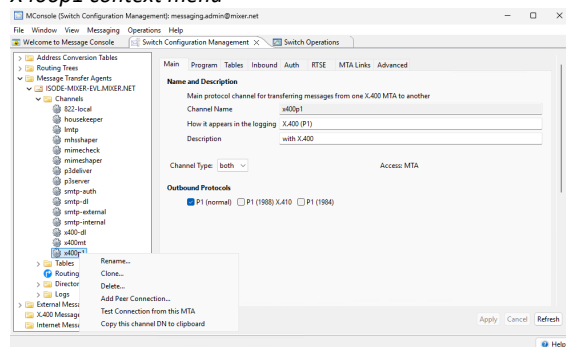
This address is routed via the x400p1 channel

Click “Close”

Testing the X.400 MTA Authentication

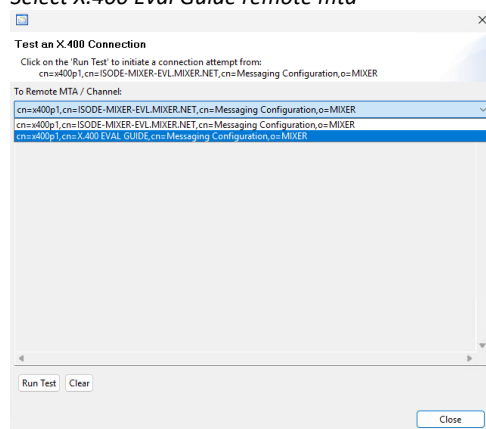
We should also check that the X.400 P1 Authentication works. From the Switch Configuration View select the x400p1 Channel and Right-Click.

X400p1 context menu



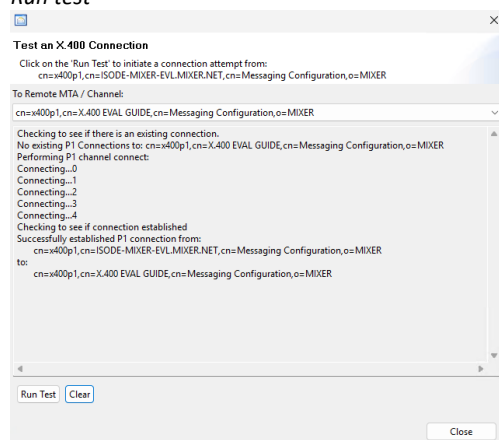
Select “Test Connection from this MTA”.

Select X.400 Eval Guide remote mta



Select the “X.400 EVAL Guide MTA” from the drop down

Run test



Click “Run Test”

You should see something like the above.

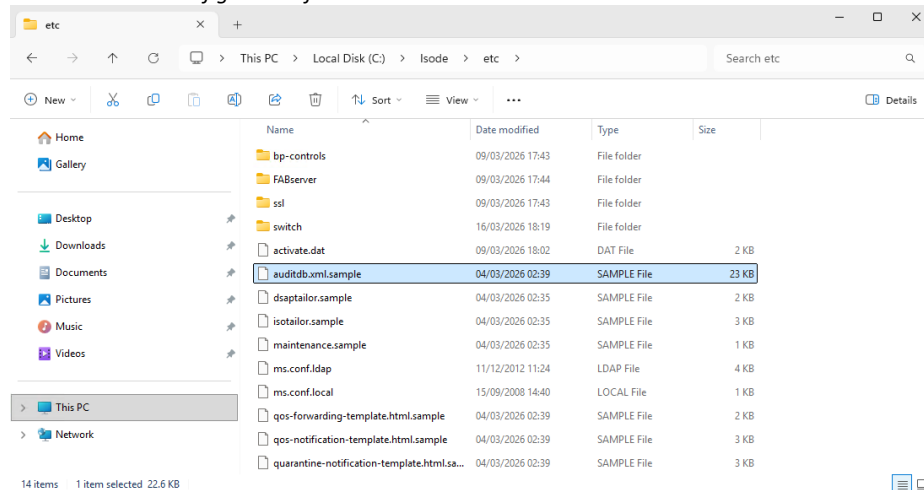
You are now ready to send messages through the MIXER Gateway. We will use the SMTP Eval Guide and X.400 Eval Guide Servers to do this.

Configuring the Audit Database and Testing

Configuring the Audit Database

In the “\Isode\etc” folder there is a file “auditdb.xml.sample”.

Audit Database Configuration file



Make a copy of this file and rename it to “auditdb.xml”, then edit that file and make the following changes.

Change :

```
<!-- Default HSQLDB server connection (evaluation only) -->

<database type="$(default)" name="$(default)"
host="$(default)" port="$(default)" driver="$(default)">

<user>$(default)</user>

<password servpass:encrypt="true">$(default)</password>

<connectingTimeout>$(default)</connectingTimeout>

<probePeriod>$(default)</probePeriod>

<probeTimeout>$(default)</probeTimeout>

</database>

<!-- HSQLDB server connection (evaluation only) -->

<!-- <database type="hsqldb" name="auditdb" host="localhost"
port="9001" driver="">

<user>SA</user>
```

```

    <password servpass:encrypt="true"></password>

    <connectingTimeOut>120</connectingTimeOut>

    <probePeriod>300</probePeriod>

    <probeTimeOut>10</probeTimeOut>

</database> -->

```

To this :

```

<!-- Default HSQLDB server connection (evaluation only) -->

<!-- <database type="$ (default) " name="$ (default) "
host="$ (default) " port="$ (default) " driver="$ (default) ">

    <user>$ (default)</user>

    <password servpass:encrypt="true">$ (default)</password>

    <connectingTimeOut>$ (default)</connectingTimeOut>

    <probePeriod>$ (default)</probePeriod>

    <probeTimeOut>$ (default)</probeTimeOut>

</database> -->

<!-- HSQLDB server connection (evaluation only) -->

    <database type="hsqldb" name="auditdb" host="localhost"
port="9001" driver="">

    <user>SA</user>

    <password servpass:encrypt="true"></password>

    <connectingTimeOut>120</connectingTimeOut>

    <probePeriod>300</probePeriod>

    <probeTimeOut>10</probeTimeOut>

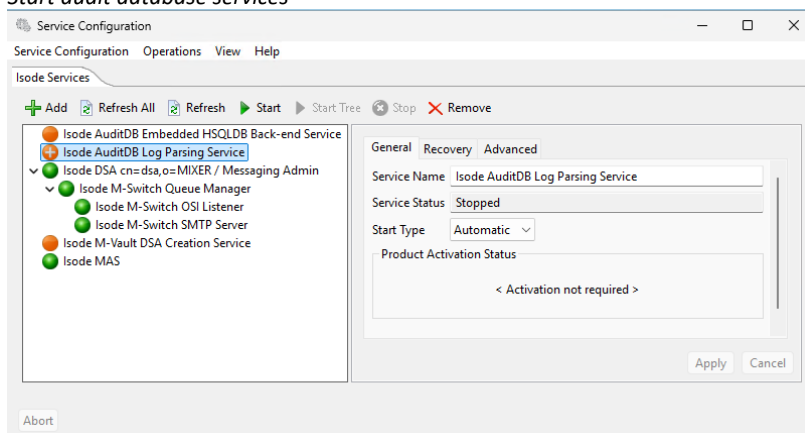
</database>

```

Save the file.

Now you need to start the Audit Database Services. On Windows use the Isode Service Configuration Tool.

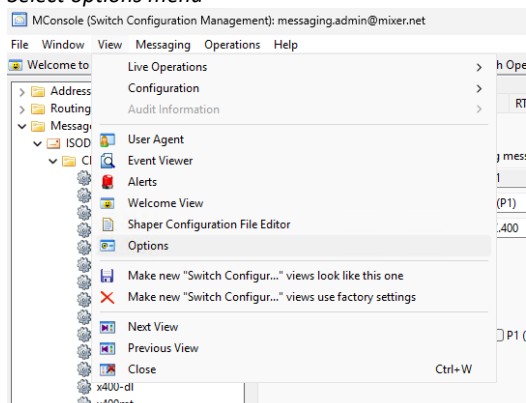
Start audit database services



Start the two “AuditDB” services.

Then from MConsole Select “View” from the top menu.

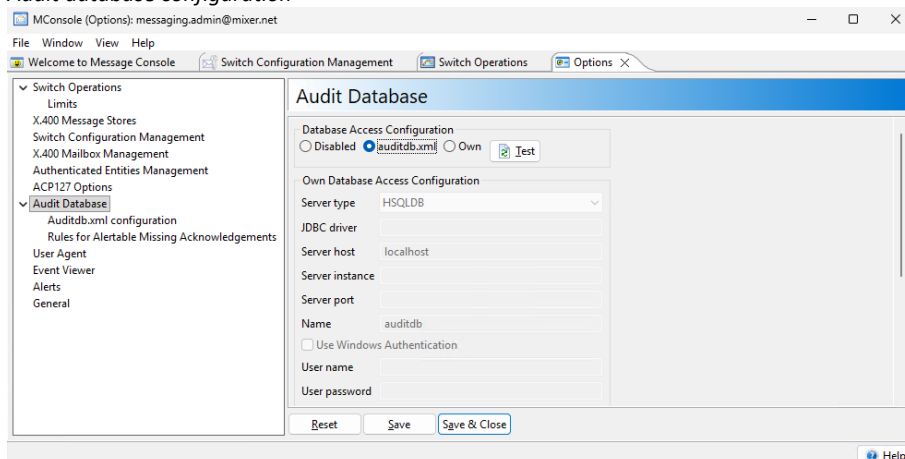
Select options menu



Select “Options”

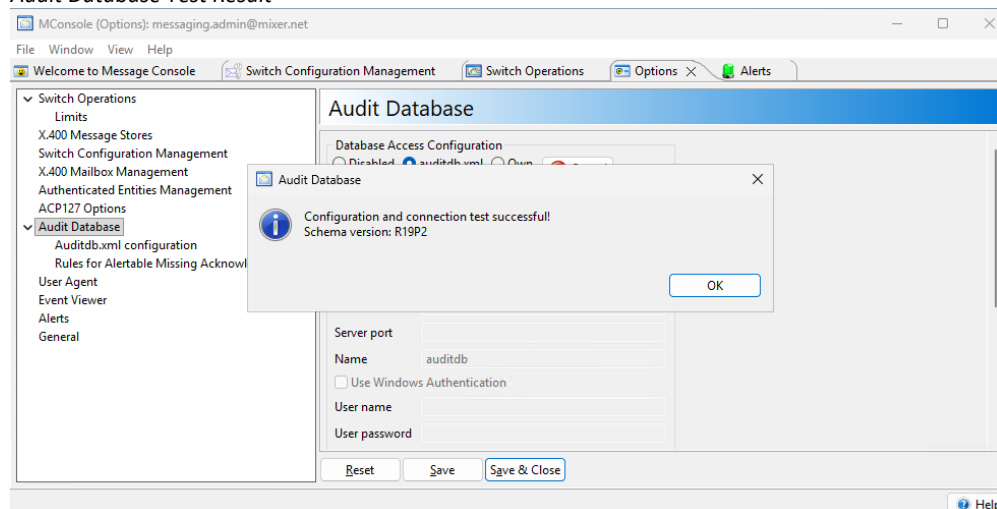
Select “Audit Database”.

Audit database configuration



Select “auditdb.xml” and click “Test”.

Audit Database Test Result

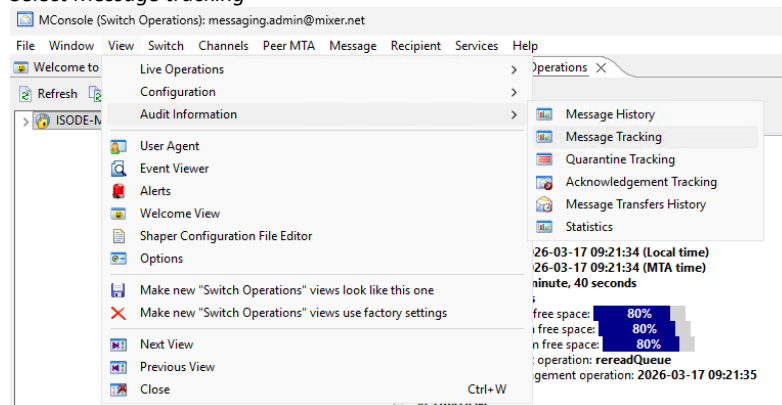


You should see the above.

Click “OK” and “Save & Close”.

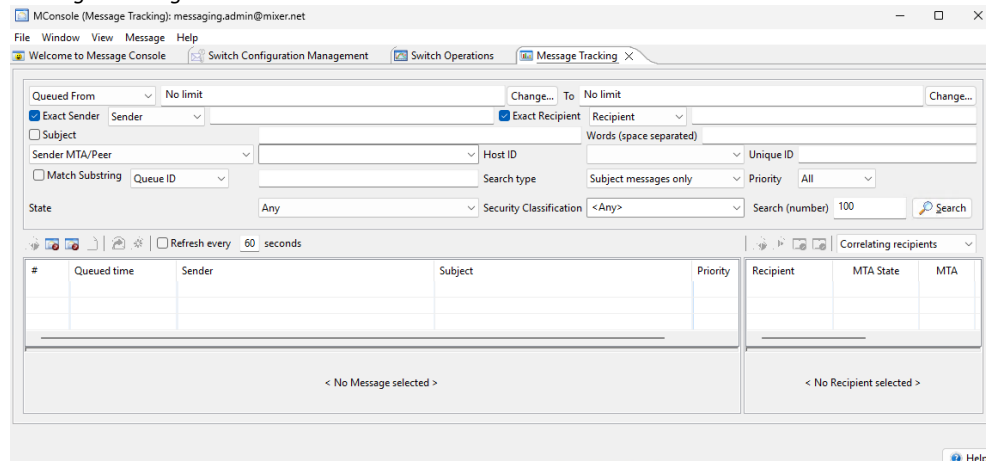
From the top menu select “View→Audit Information”.

Select Message tracking



Select “Message Tracking”.

Message tracking view



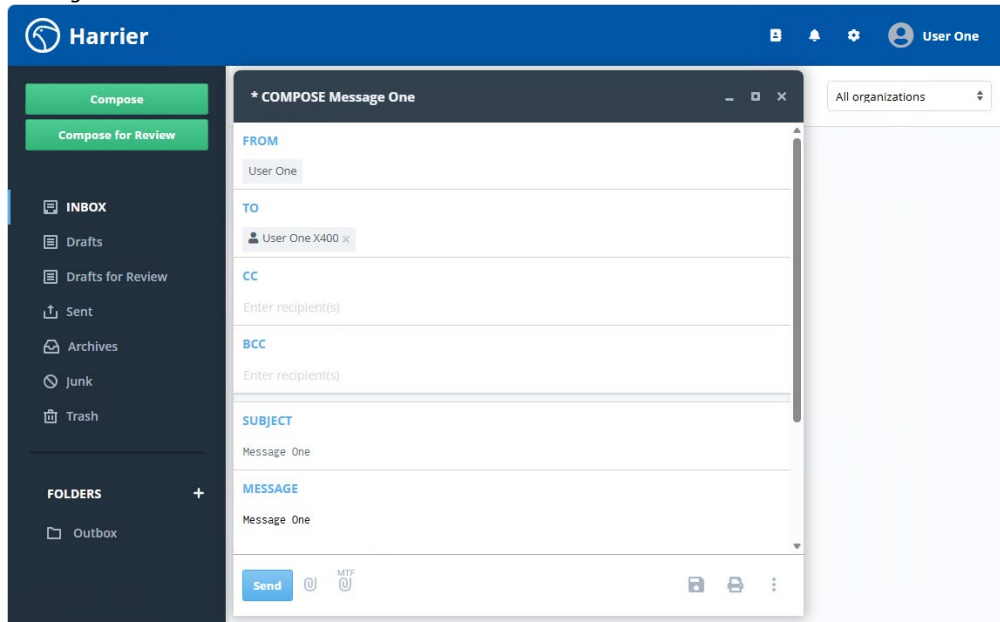
Testing

We will use the server in the M-Switch SMTP Eval Guide to send a message

From: user.one@internet.net

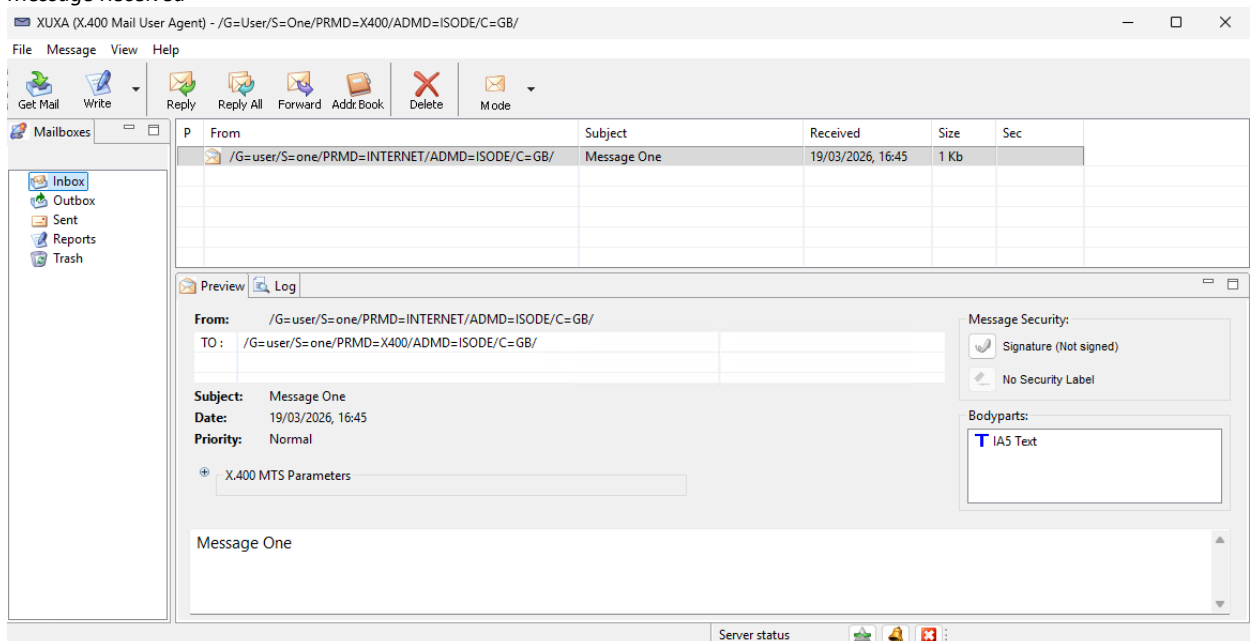
To: user.one@x400.net

Message From Internet to X.400



This is successfully received at the X.400 Eval Guide

Message Received



Then from the X.400 side we will send a message

From: /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/

To: /G=User/S=One/PRMD=Internet/ADMD=ISODE/C=GB/

Message From X.400 To Internet

Message Two

File Help

Send Attach

From: /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/

To: /G=User/S=One/PRMD=Internet/ADMD=ISODE/C=GB/ Per Recip

Subject: Message Two

X.400 MTS Parameters

Message Two

Message Security: Don't sign message No Security Label

Priority: Normal

Bodyparts:

Message Two received at internet.net

Harrier

Compose Compose for Review

INBOX Drafts Drafts for Review Sent Archives Junk Trash

FOLDERS Outbox

Receipt requested: Decline Return receipt

User One

From: User.One@x400.net
Sender: <User.One@x400.net>
Sent: 19-Mar-2026 16:51

Message Two

To: User.One@internet.net

Message Two

If you Click the “Return receipt” the following is what the X.400 user sees.

Receipt notification at X.400

File Message View Help

Get Mail Write Reply Reply All Forward Addr Book Delete Mode

Mailboxes

From	Subject	Received	Size	Sec
/G=user/S=one/PRMD=INTERNET/ADMD=ISODE/C=GB/	Message One	19/03/2026, 16:45	1 Kb	
/S=postmaster/PRMD=INTERNET/ADMD=ISODE/C=GB/	Delivery report (success) for /G=...		1 Kb	
/G=user/S=one/PRMD=INTERNET/ADMD=ISODE/C=GB/	IPN	19/03/2026, 17:08	1 Kb	

Preview Log

From: /G=user/S=one/PRMD=INTERNET/ADMD=ISODE/C=GB/

To: /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/

Subject: IPN

Date: 19/03/2026, 17:08

Priority: Normal

X.400 MTS Parameters

Message Security: Signature (Not signed) No Security Label

Bodyparts:

Receipt Notification for your message with
Subject IPN: 1 260319165123Z/G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/
Your message was read at 260319170824Z

Listed 6 messages in the Sent folder Server status

Then return to MConsole Message Tracking

Change “Search Type” to “All Messages”

Press “Search”

Message Tracking

Welcome to Message Console

Switch Configuration Management

Switch Operations

Message Tracking

Queued From

No limit

Change...

To

No limit

Change...

☒ Exact Sender

Sender

☐ Subject

☒ Exact Recipient

Recipient

Words (space separated)

Sender MTA/Peer

Host ID

Unique ID

☐ Match Substring

Queue ID

Search type

All messages

Priority

All

State

Any

Security Classification

<Any>

Search (number)

100

Search

Refresh every 60 seconds

Correlating recipients

#	Queued time	Sender	Subject	Priority	Size	Recipient	MTA State	MTA	Char
1	2026-03-19 16:51:24	/G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/	Message Two	Normal	198				
2	2026-03-19 16:45:10	/G=user/S=one/PRMD=INTERNET/ADMD=ISODE/C...	Message One	Normal	966				
3	2026-03-19 17:08:24	/G=user/S=one/PRMD=INTERNET/ADMD=ISODE/C...	Return Receipt (displayed) - Message Two	Normal	3151				
4	2026-03-19 17:05:53	<>	Delivery report (success) for /G=User/S=One/PRMD...	Normal	1636				
5	2026-03-19 17:05:53	<>	Delivery report (success) for /G=User/S=One/PRMD...	Urgent	1041				

< No Message selected >

< No Recipient selected >

Help

Using Strong Authentication With M-Switch

It is possible to bind using strong authentication in the M-Switch product set. Strong Authentication is possible within the P1, P7 and P3 protocols. The following sections describe how to implement Strong Authentication in the P1 protocol. Please refer to the M-Switch Core X.400 Evaluation guide to see configuration of Strong Authentication for the P3 and P7 protocols. Strong Authentication is not subject to export control. P7 and P3 authentication requires an additional activation component.

Create an Isode PKI

Isode provides a CA for test purposes. It isn't supported in a production environment. These steps explain how to create an Isode PKI to generate certificates.

You may skip this step if you already possess a PKI infrastructure.

Create the directory "C:\IsodeCerts"

On Linux create the directory "/root/IsodeCerts"

Open "Sodium CA" from the Windows start menu

On Linux run :

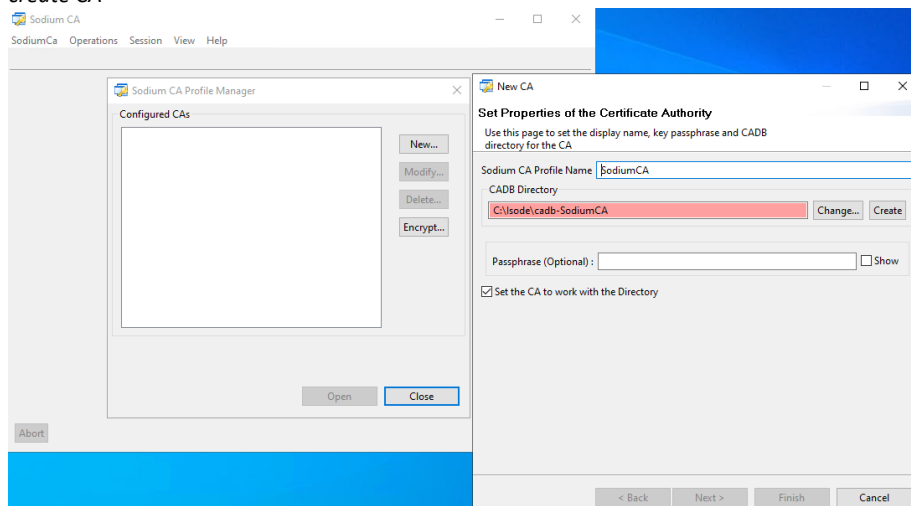
```
/opt/isode/sbin/sodiumca
```

Click "New"

On "Set Properties of the Certificate Authority" leave defaults

Click "Create"

create CA



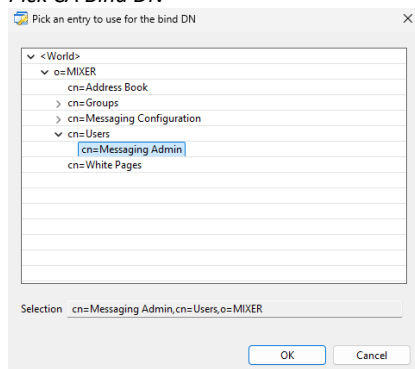
Click "Next >"

In "Hostname" type the fully qualified host name ("ISODE-MIXER-EVL.MIXER.NET")

Click "Pick"

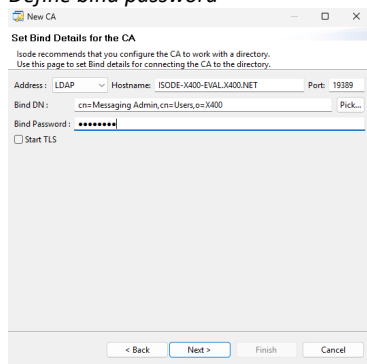
Browse to "cn=Messaging Admin,cn=Users,o=MIXER"

Pick CA Bind DN



Click “OK”

Define bind password



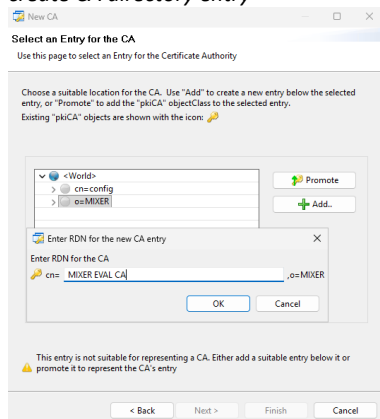
In “Bind Password” type “Secret1+”

Click “Next >”

On “Select an Entry for the CA” browse to and select “o=MIXER”

Click “Add ..”

create CA directory entry



On “Enter RDN for the new CA” type “MIXER EVAL CA”

Click “OK”

Click “Next >”

On “Set Key Type, Subject and Subject Alternative Names” leave default options

Click “Next >”

On “Certificate Status Sharing” leave Defaults

Click “Next >”

On “Set the CRL Distribution Point for the CA” leave defaults

Click “Next >”

On “Set the Access Description List for the CA” leave defaults

Click “Next >”

On “Set Basic Constraints and KeyUsage Extension” leave defaults

Click “Next >”

On “Generate Self Signed Certificate or CSR” select “Generate a Self Signed Root Certificate

generate self signed CA certificate

Leave the defaults.

Click “Next >”

On “Root CA Certificate” leave Defaults

Click “Next >”

On “Finish CA Configuration” press “Finish”

On “Sodium CA Profile Manager” select “SodiumCA”

Click “Open”

open configured CA

In “Enter Bind Password” type “Secret1+”

Click “OK”

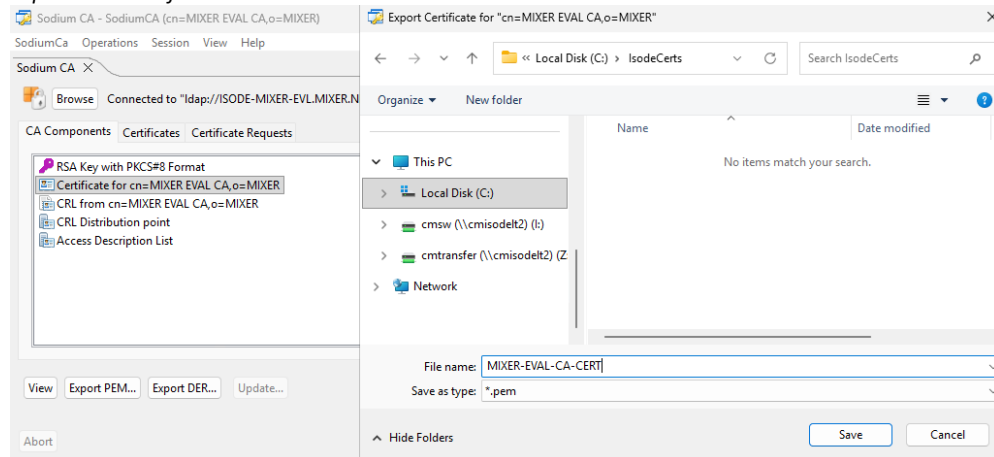
Select “Certificate for cn=MIXER EVAL CA, o=MIXER”

Press “Export PEM ..”

On “Export Certificate for “cn=MIXER EVAL CA, o=MIXER”, browse to “C:\IsodeCerts” (Linux : “/root/IsodeCerts)

Change Filename to “MIXER-EVAL-CA-CERT.pem”

export root certificate

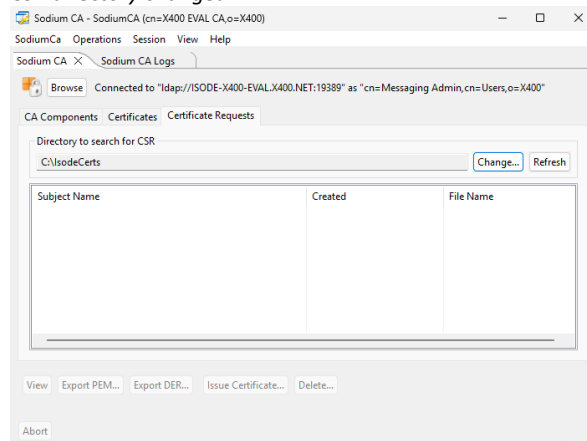


Press “Save”

On “Certificate for cn=MIXER EVAL CA, o=MIXER” exported Click “OK”

Change to “Certificate Requests” tab

CSR directory changed



Change “Directory to Search for CSR” to “C:\IsodeCerts” (Linux : “/root/IsodeCerts)

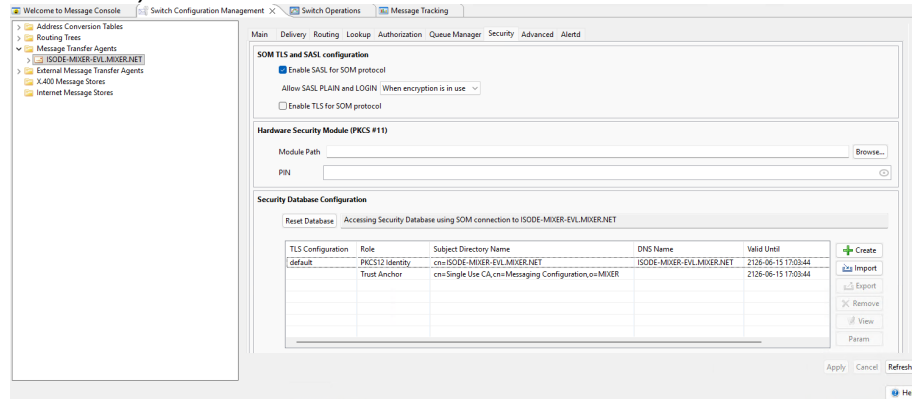
Configure the Security Database

Open Mconsole

Select the “Message transfer Agent” “ISODE-MIXER-EVL.MIXER.NET”

Select the “Security” tab

Initial Security Tab

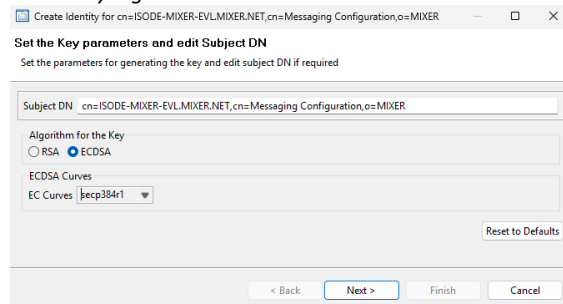


Note – the server has it's own self-signed certificate.

We will create a new certificate for the server from the local CA.

Press “Create”

Select Key algorithm



For “Algorithm for the Key” select “ECDSA”

For “EC Curves” select “secp384r1”

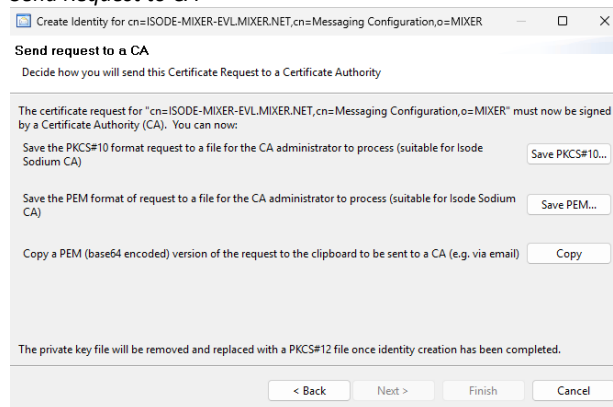
Press “Next >”

On “Set the Key parameters and edit Subject DN” press “Next >”

On “Select and add Subject Alternative Names and Clearance” press “Next >”

On “Certificate Request Contents” type Click “Next >”

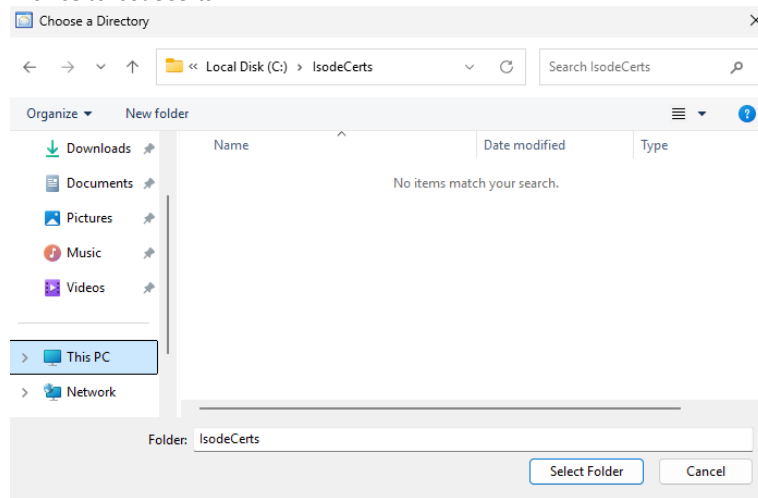
Send Request to CA



Press “Save PEM ...”

Browse to “C:\IsodeCerts” (Linux : “/root/IsodeCerts”)

Browse to IsodeCerts



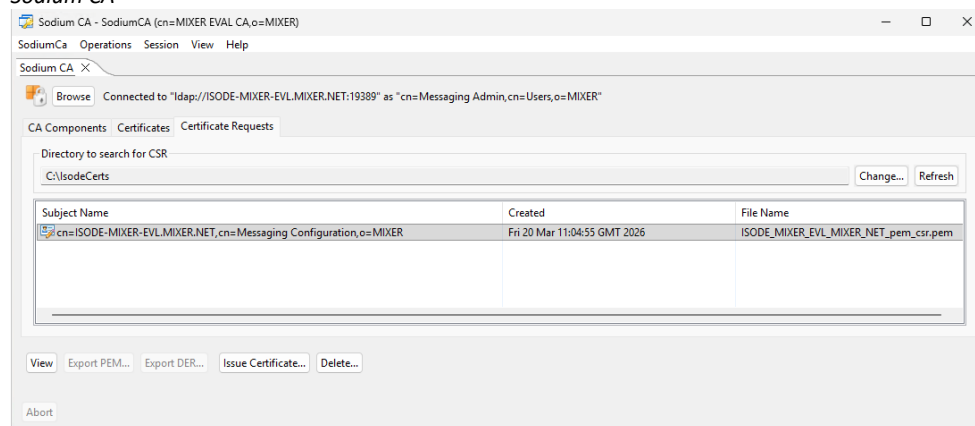
Press “Select Folder”

Open Sodium CA:

Change to “Certificate Requests” tab

Press “Refresh”

Sodium CA



Ensure that the Certificate request is selected

Click “Issue Certificate...”

On “Certificate Signing Request” leave defaults

Click “Next >”

On “Select and add Subject Alternative Names” leave defaults

Press “Next >”

On “Select and Create X.509 Extensions” leave defaults

Press “Next >”

Set Signature Algorithm

In the “Signature Algorithm” dropdown select “SHA384WITHRSA”

Click “Next >”

Generated Certificate

In the “Export to Disk” dropdown, select “Write Certificate Chain in PEM Format”

Press “Finish”

On “CSR Signed” Click “OK”.

Return to “Mconsole”

On “Send Request to CA” press “Next >”

On “Continue or defer identity creation” Select “The CA has provided a certificate”

Press “Next >”

On “User Certificate” press “Next >”

Other Certificates

Press “Next >”

On “Save Identity information” Press “Finish”

Press “Apply”

New Certificate Created

Security Database Configuration

TLS Configur...	Role	Subject Directory Name	DNS Name	Valid Until	
default	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET	ISODE-MIXER-EVL.MIXE...	2126-03-20 10:59:58	+ Create Import Export Remove View Param
	Trust Anchor	cn=Single Use CA, cn=Messaging...	ISODE-MIXER-EVL.MIXE...	2126-03-20 10:59:58	
	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET	ISODE-MIXER-EVL.MIXE...	2035-03-20 11:06:22	
	Certificate Authori...	cn=MIXER EVAL CA, o=MIXER		2036-03-17 18:06:07	

Note the additional PKCS12 Identity and Certificate Authority.

Note that the “default” certificate is the one marked “default” in the left-hand column.

Select the new certificate below that.

Certificate context menu

Security Database Configuration

Reset Database Accessing Security Database using SOM connection to ISODE-MIXER-EVL.MIXER.NET

TLS Configuration	Role	Subject Directory Name	DNS Name	Valid Until	
default	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET	ISODE-MIXER-EVL.MIXER.NET	2126-06-15 17:03:44	+ Create Import Export Remove View Param
	Trust Anchor	cn=Single Use CA, cn=Messaging Configuration, o=MIXER		2126-06-15 17:03:44	
	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET	MIXER-EVL.MIXER.NET; /C=GB/ADMD=ISODE/PRMD=MIXER/IS...	2035-06-22 13:43:35	
	Certificate Authority	cn=MIXER EVAL CA, o=MIXER		2036-06-22 13:18:42	

Copy URI
Assign or update TLS Configuration

Apply Cancel Refresh

Right click

From the menu, choose “Assign or update TLS configuration”

Change default certificate

Security Database Configuration

TLS Configurat...	Role	Subject Directory Name	DNS Name	Valid Until	
default	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET	ISODE-MIXER-EVL.MIXE...	2126-03-20 10:59:58	+ Create Import Export Remove View Param
	Trust Anchor	cn=Single Use CA, cn=Messaging...		2126-03-20 10:59:58	
	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET	ISODE-MIXER-EVL.MIXE...	2035-03-20 11:06:22	
	Certificate Authority	cn=MIXER EVAL CA, o=MIXER		2036-03-17 18:06:07	

Copy URI
Assign or update TLS Configuration

In “TLS Configuration Name” type “default”

Press “OK”

Default pending

Security Database Configuration

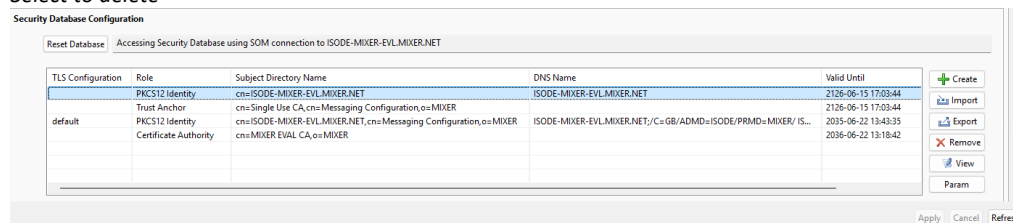
Reset Database Accessing Security Database using SOM connection to ISODE-MIXER-EVL.MIXER.NET

TLS Configuration	Role	Subject Directory Name	DNS Name	Valid Until	
default	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET	ISODE-MIXER-EVL.MIXER.NET	2126-06-15 17:03:44	+ Create Import Export Remove View Param
	Trust Anchor	cn=Single Use CA, cn=Messaging Configuration, o=MIXER		2126-06-15 17:03:44	
	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET, cn=Messaging Configuration, o=MIXER	ISODE-MIXER-EVL.MIXER.NET; /C=GB/ADMD=ISODE/PRMD=MIXER/IS...	2035-06-22 13:43:35	
	Certificate Authority	cn=MIXER EVAL CA, o=MIXER		2036-06-22 13:18:42	

Apply Cancel Refresh

Press “Apply”

Select to delete



Select the previously “default” certificate.

Press “Remove”

Press “Apply”

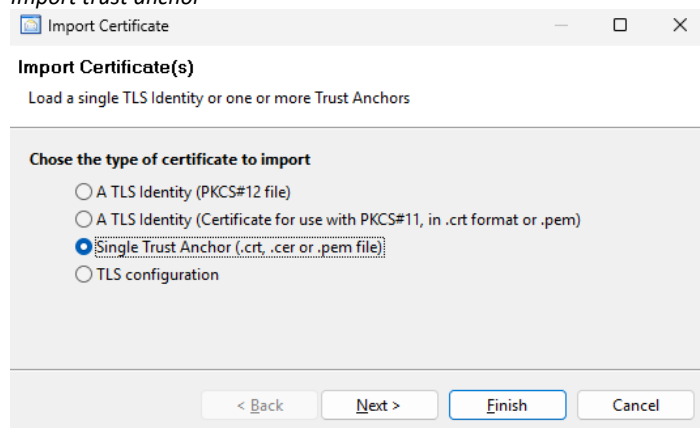
Select the “Single use CA” trust anchor.

Press “Remove”

Press “Apply”

Press “Import”

Import trust anchor

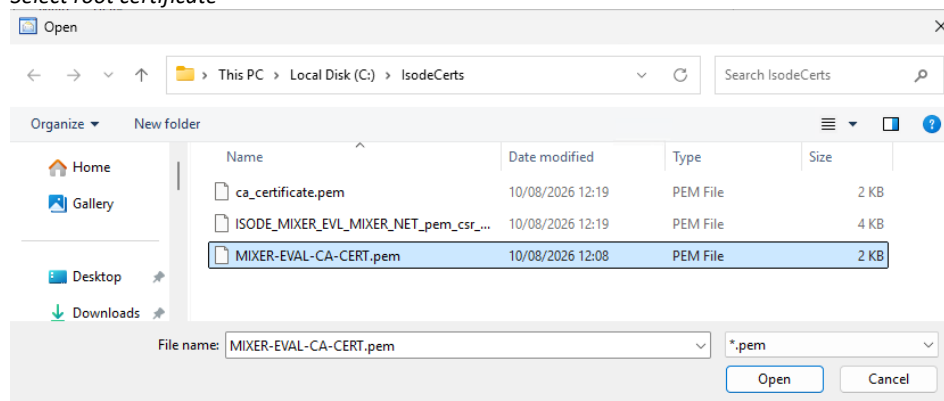


Select “Single Trust Anchor”

Press “Next >”

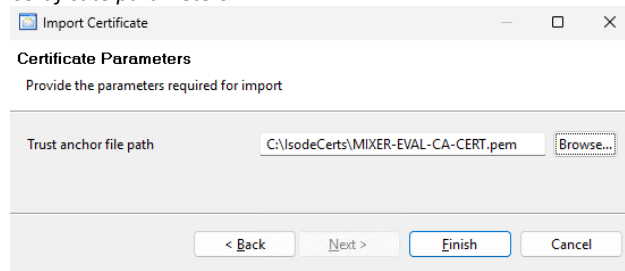
Browse to “C:\IsodeCerts” (Linux : “/root/IsodeCerts”)

Select root certificate



Select the file “MIXER-EVAL-CA-CERT.PEM”

Certificate parameters



Import Certificate

Certificate Parameters
Provide the parameters required for import

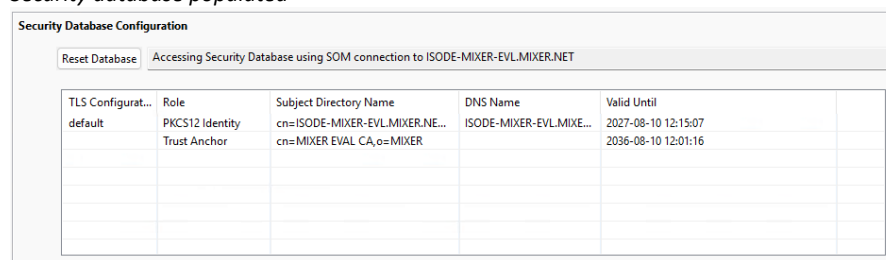
Trust anchor file path: C:\IsodeCerts\MIXER-EVAL-CA-CERT.pem Browse...

< Back Next > Finish Cancel

Press “Finish”

Press “Apply”

Security database populated



Reset Database Accessing Security Database using SOM connection to ISODE-MIXER-EVL.MIXER.NET

TLS Configur...	Role	Subject Directory Name	DNS Name	Valid Until
default	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NE...	ISODE-MIXER-EVL.MIXE...	2027-08-10 12:15:07
	Trust Anchor	cn=MIXER EVAL CA,o=MIXER		2036-08-10 12:01:16

Create a Certificate for P1

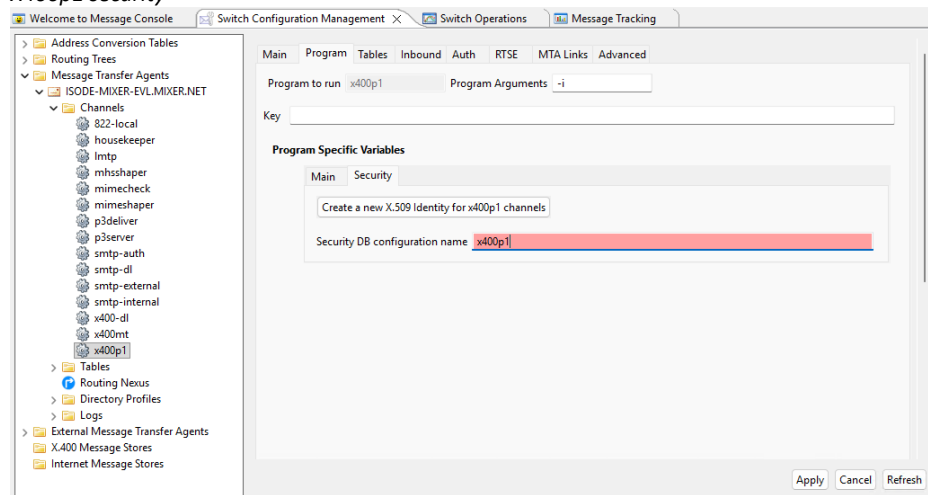
Expand channels in the left-hand pane and select “X400p1”

Select the “Program” tab

Below that, select the “Security” tab

In “Security DB configuration name” type “x400p1”

X400p1 security



Welcome to Message Console | Switch Configuration Management | Switch Operations | Message Tracking

Main Program Tables Inbound Auth RTSE MTA Links Advanced

Program to run: x400p1 Program Arguments: -i

Key:

Program Specific Variables

Main Security

Create a new X.509 Identity for x400p1 channels

Security DB configuration name: x400p1

Apply Cancel Refresh

Press “Apply”

Press “Create a new X.509 Identity for x400p1 channels”

Select key algorithm

For “Algorithm for the Key” select “ECDSA”

For “EC Curves” select “secp384r1”

Press “Next >”

On “Select and add Subject Alternative Names and Clearance” press “Next >”

On “Certificate Request Contents” press “Next >”

On “Send request to CA” press “Save PEM ...” and save the CSR in the folder “C:\IsodeCerts” (Linux : “/root/IsodeCerts”)

Press “Next >”

Return to Sodium CA:

Change to “Certificate Requests” tab

Press “Refresh”

Ensure that the Certificate request is selected

Click “Issue Certificate...”

On “Certificate Signing Request” leave defaults

Click “Next >”

On “Select and add Subject Alternative Names” leave defaults

Press “Next >”

On “Select and Create X.509 Extensions” leave defaults

Press “Next >”

Set Signature Algorithm

In the “Signature Algorithm” dropdown select “SHA384WITHRSA”

Click “Next >”

Generated Certificate

Generated Certificate
The following certificate will be generated.

Subject	cn=ISODE-MIXER-EVL.MIXER.NET,cn=Messaging Configuration,o=MIXER
Issuer	cn=MIXER EVAL CA,o=MIXER
Valid from	Mon Aug 10 12:35:13 BST 2026
Valid to	Tue Aug 10 12:35:13 BST 2027
Serial	5F:6E:D0:DD:CA:93:FE:CD:28:EF
PublicKeyInfo	Algorithm: ECDSA, KeySize: 384
SignatureAlgorithm	SHA384WITHRSA
CertificateType	Version v3 (Not a CA Certificate)

Display Detailed Information

Export to disk: Write certificate chain in PEM format

You can also load this certificate into the directory by checking the box below:
☒ Load this certificate into the directory entry

< Back Next > Finish Cancel

In the “Export to Disk” dropdown, select “Write Certificate Chain in PEM Format”

Press “Finish”

On “CSR Signed” Click “OK”.

Return to “Mconsole”

On “Continue or defer identity creation” Select “The CA has provided a certificate”

Press “Next ...”

On “User Certificate” press “Next >”

On “Other Certificates” press “Next >”

On “Save Identity information” Press “Finish”

Press “Apply”

New x400p1 Certificate

Security Database Configuration

Security Database Certificates

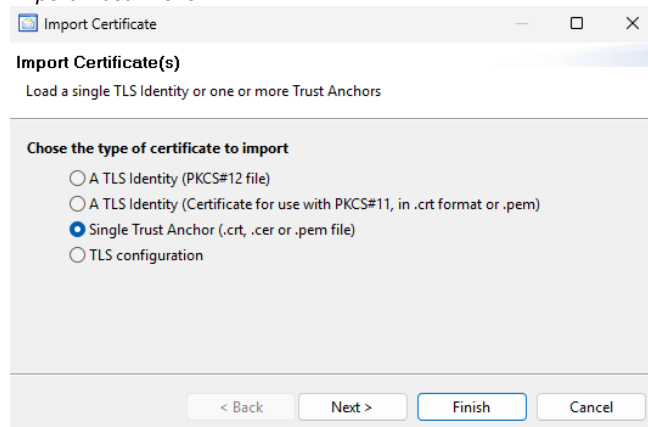
TLS Configurat...	Role	Subject Directory Name	DNS Name	Valid Until
default	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET,cn=Messaging Configuration...	ISODE-MIXER-EVL.MIXER.NET;/C=GB/ADMD=IS...	2035-03-20 11:06:22
	Certificate Authority	cn=MIXER EVAL CA,o=MIXER		2036-03-17 18:06:07
x400p1	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NET,cn=Messaging Configuration...	ISODE-MIXER-EVL.MIXER.NET;/C=GB/ADMD=IS...	2035-03-20 11:19:53

Create Import Export Remove View Param

Note that in the Security database, a new certificate marked “x400p1” has been created.

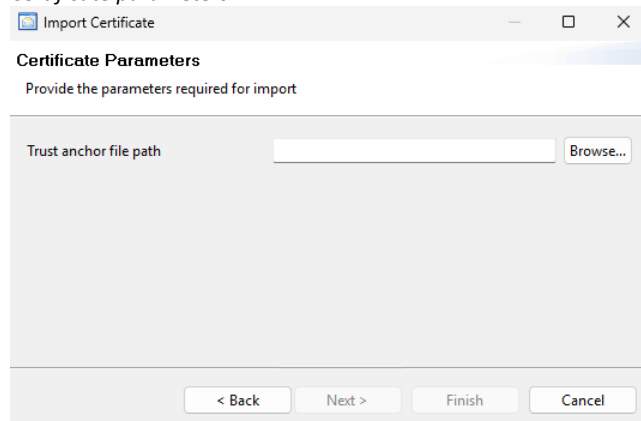
On the X400 Eval guide server, copy the file “X400-EVAL-CA-CERT.pem” from the C:\IsodeCerts (Linux : “/root/IsodeCerts”) folder to the same folder on the Mixer server.

Click on “Import”

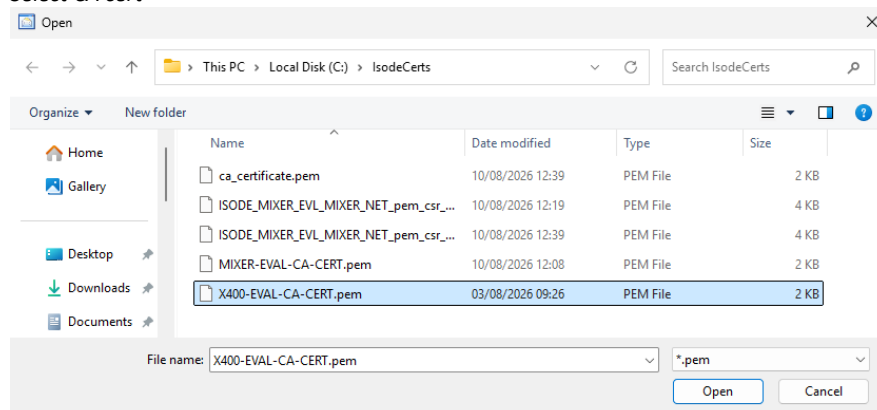
Import Trust Anchor

Select “Single Trust Anchor”

Press “Next >”

Certificate parameters

Press “Browse ..”

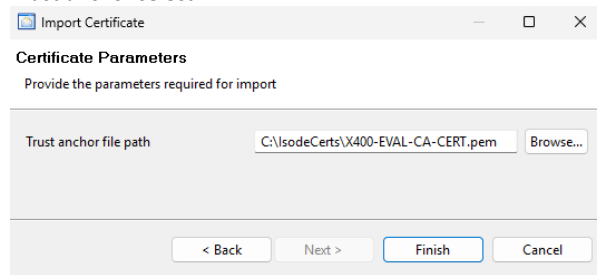
Select CA cert

Navigate to the folder “C:\IsodeCerts” (Linux : “/root/IsodeCerts”)

In the file extension dropdown, select “*.pem”

Select the file “X400-EVAL-CA-CERT.pem”

Click “Open”

Trust anchor select


Import Certificate

Certificate Parameters
Provide the parameters required for import

Trust anchor file path:

Press “Finish”

Press “Apply”

Trust anchors Added

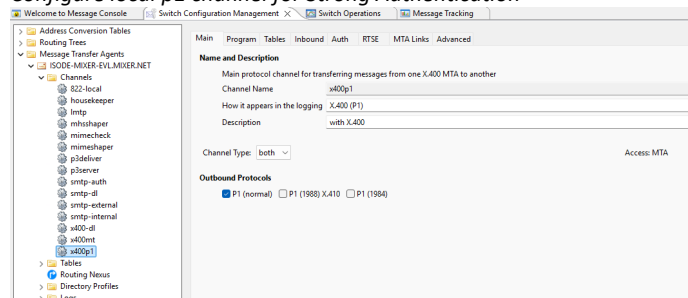
Security Database Configuration

Accessing Security Database using SOM connection to ISODE-MIXER-EVL.MIXER.NET

TLS Configur...	Role	Subject Directory Name	DNS Name	Valid Until	
default	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NE...	ISODE-MIXER-EVL.MIXE...	2027-08-10 12:15:07	
	Trust Anchor	cn=MIXER EVAL CA,o=MIXER		2036-08-10 12:01:16	
x400p1	PKCS12 Identity	cn=ISODE-MIXER-EVL.MIXER.NE...	ISODE-MIXER-EVL.MIXE...	2027-08-10 12:35:13	
	Trust Anchor	cn=X400 EVAL CA,o=X400		2036-08-03 09:18:39	

Enable strong authentication for the local mta

Select the local x400p1 channel

Configure local p1 channel for Strong Authentication


Welcome to Message Console | Switch Configuration Management | Switch Operations | Message Tracking

Main | Program | Tables | Inbound | Auth | RTSE | MTA Links | Advanced

Name and Description
Main protocol channel for transferring messages from one X.400 MTA to another

Channel Name:

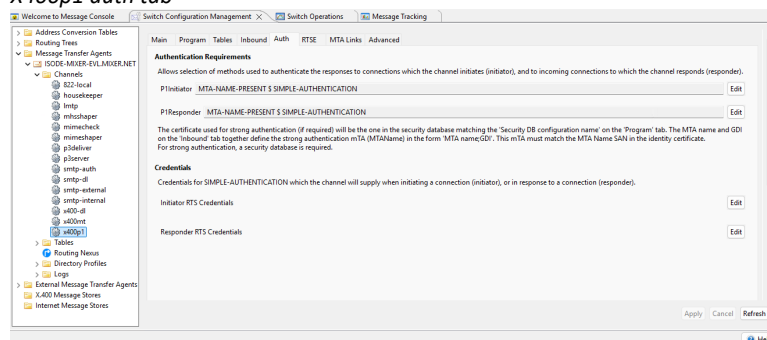
How it appears in the logging:

Description:

Channel Type: Access: MTA

Outbound Protocols
☒ P1 (normal)
 ☐ P1 (1988) X.410
 ☐ P1 (1984)

Select the “Auth” tab

X400p1 auth tab


Welcome to Message Console | Switch Configuration Management | Switch Operations | Message Tracking

Main | Program | Tables | Inbound | Auth | RTSE | MTA Links | Advanced

Authentication Requirements
Allows selection of methods used to authenticate the responses to connections which the channel initiates (initiator), and to incoming connections to which the channel responds (responder).

P1 Initiator:

P1 Responder:

The certificate used for strong authentication (if required) will be the one in the security database matching the 'Security DB configuration name' on the 'Program' tab. The MTA name and GDI on the 'Inbound' tab together define the strong authentication mTA (MTAName) in the form 'MTA name:GDI'. This mTA must match the MTA Name SAN in the identity certificate. For strong authentication, a security database is required.

Credentials
Credentials for SIMPLE-AUTHENTICATION which the channel will supply when initiating a connection (initiator), or in response to a connection (responder).

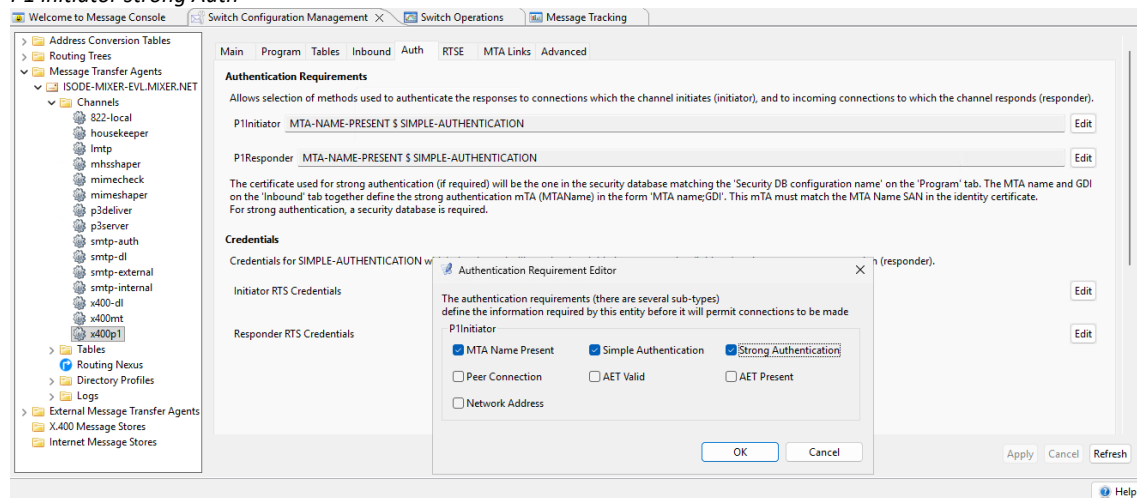
Initiator RTS Credentials:

Responder RTS Credentials:

To the right of “p1 Initiator” press “Edit”

Select “Strong Authentication”

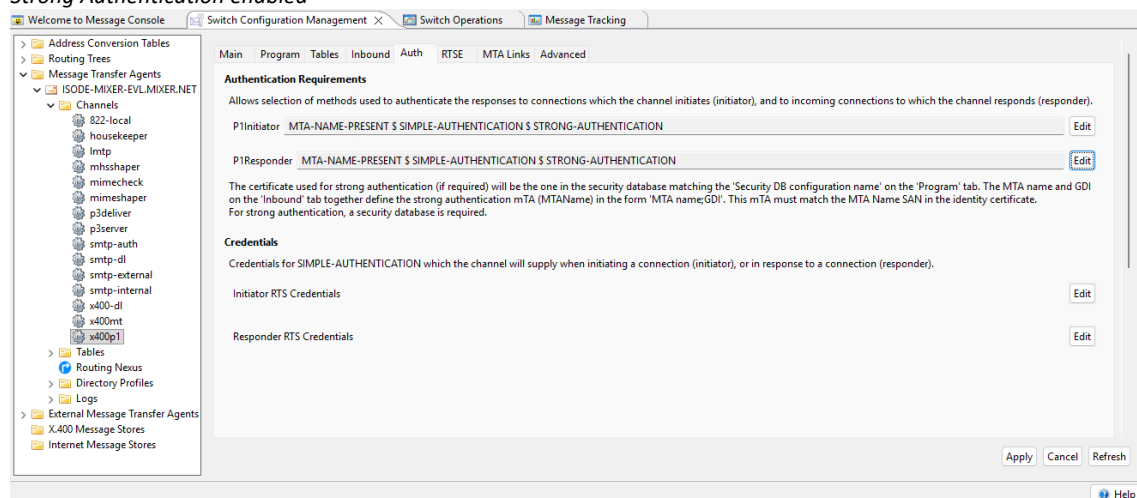
P1 initiator strong Auth



Press “OK”

Repeat the above steps to enable Strong Authentication for the “P1 Responder”

Strong Authentication enabled



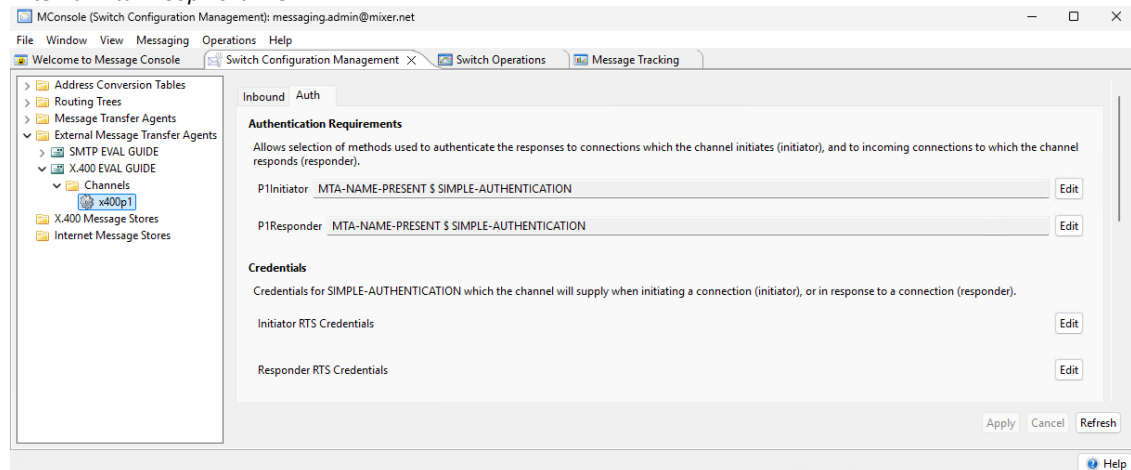
Press “Apply”

Enable strong authentication for the external mta

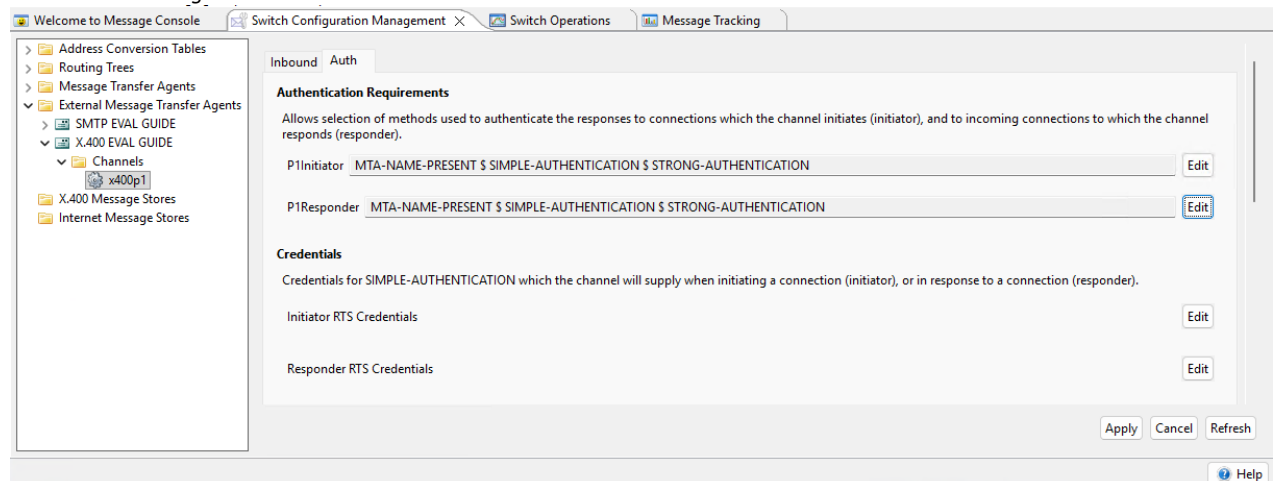
Expand the left-hand pane to the “External Message Transfer Agent” “X.400 EVAL GUIDE”

Select “x400p1”

Change to the “Auth” tab

External mta x400p1 channel

Repeat the previous steps to enable Strong Authentication for the P1initiator and the P1Responder.

External mta strong auth enabled

Press “Apply”

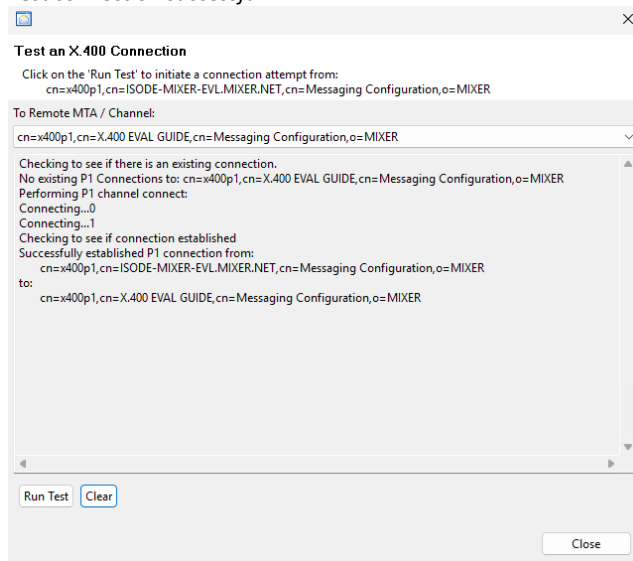
Test X400p1 Strong Auth connection

Ensure that the steps for configuring strong authentication have been followed in the X400 Evaluation guide.

Select the local x400p1 channel and using the context menu, select “Test Connection from this MTA”

Select the remote mta “X.400 EVAL GUIDE”

Press “Run Test”

Test connection successful

It can be verified that strong authentication takes place by examining the mta-audit log :

```
2026-08-10 12:53:05 x400p1 06108 (#0 ) P1InitConnOK
chan:x400p1 theirmtaname:ISODE-X400-EVAL.X400.NET
theirpa:"\"591\"/URI+0000+URL+itot://isode-x400-eval.x400.net"
ourmtaname:ISODE-MIXER-EVL.MIXER.NET rtse_type:normal appcon:3
recov:false dialogmode:mono auth_req:31 our_auth_req:31 rtsid:3
ckpoint:63 window:3 actno:0 rts_flags:c15 bindtype:strong
oursubject:"cn=ISODE-MIXER-EVL.MIXER.NET,cn=Messaging
Configuration,o=MIXER" ourissuer:"cn=MIXER EVAL CA,o=MIXER"
ourserial_num:15DC1AB2157406B3F15A theirissuer:"cn=X400 EVAL
CA,o=X400" theirssubject:"cn=ISODE-X400-EVAL.X400.NET,cn=Messaging
Configuration,o=X400" theirserial_num:090EE952E69FE7D43D6A
oursangdi:/C=GB/ADMD=ISODE/PRMD=MIXER/ oursanmta:ISODE-MIXER-
EVL.MIXER.NET theirsangdi:/C=GB/ADMD=ISODE/PRMD=X400/
theirsanmta:ISODE-X400-EVAL.X400.NET tokenmta:ISODE-MIXER-
EVL.MIXER.NET
```

Note the “**bindtype:strong**” for the transaction.

What Next?

More information on M-Switch MIXER can be found on the Isode website at <https://www.isode.com/product/smtp-x-400-gateway>

Whitepapers

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

Copyright

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

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

Isode software is © copyright Isode Limited 2002-2026, All rights reserved.

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

This manual is © copyright Isode Limited 2026.