

M-Switch X.400 Evaluation Guide

Configuring the R19.2 core release of Isode's X.400 Messaging Servers on Windows and Linux platforms for use as an X.400 Messaging System that could be used in both EDI and Aviation Solutions.

Contents

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	15
Configure the Switch Operations View.....	17
Creating the Security Database	19
Configuring X.400 P7 Users	19
Configuring X.400 P3 Users	23
Testing the System with xuxa	25
P7 mailboxes.....	25
P3 mailboxes.....	32
Adding an External MTA and Address Book entries.....	36
Configuring the External MTA with MConsole	36
Adding Address Book Entries with Sodium	44
Sending a Message to an External X.400 User with XUXA.	48
Prepare for Strong Authentication with M-Switch.....	50
Create an Isode PKI.....	50
Populate the Security Database	53
Configure and Test P1 Strong Authentication.....	61
Create Certificate for P1	61
Enable strong authentication for the local mta	65
Enable strong authentication for the external mta.....	66
Test X400p1 Strong Auth connection.....	67
Enable Mailboxes for Strong Authentication	69
Create User Certificate.....	69
Configure and Test P3 Strong Authentication Between MTA and Message Store	73
Configure and Test Strong Authentication from Xuxa	76
Prepare the system.....	76
Extend the Switch Routing Tree for aviation mailboxes.....	76
Create an aviation P7 mailbox	77
Create an aviation P3 mailbox	79
Create the M-Store Certificates	80
Create the PKCS12 mailbox identities.....	80
Configure and test xuxa P7 Strong Authentication	84
Configure M-Store for Strong P7 Authentication	84
Configure xuxa profile for P7 Strong Authentication.....	85
Configure and test xuxa P3 Strong Authentication	87
Configure the P3 server channel.....	87
Configure xuxa profile for P3 Strong Authentication.....	87
Copyright	90

Introduction

This guide is intended to give the reader basic information on how to configure Isode's M-Switch, M-Vault and M-Store X.400 Server Products. These Products combine to create an X.400 Messaging Solution. You will also use Isode's xuxa X.400 User Agent to test the system.

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

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

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

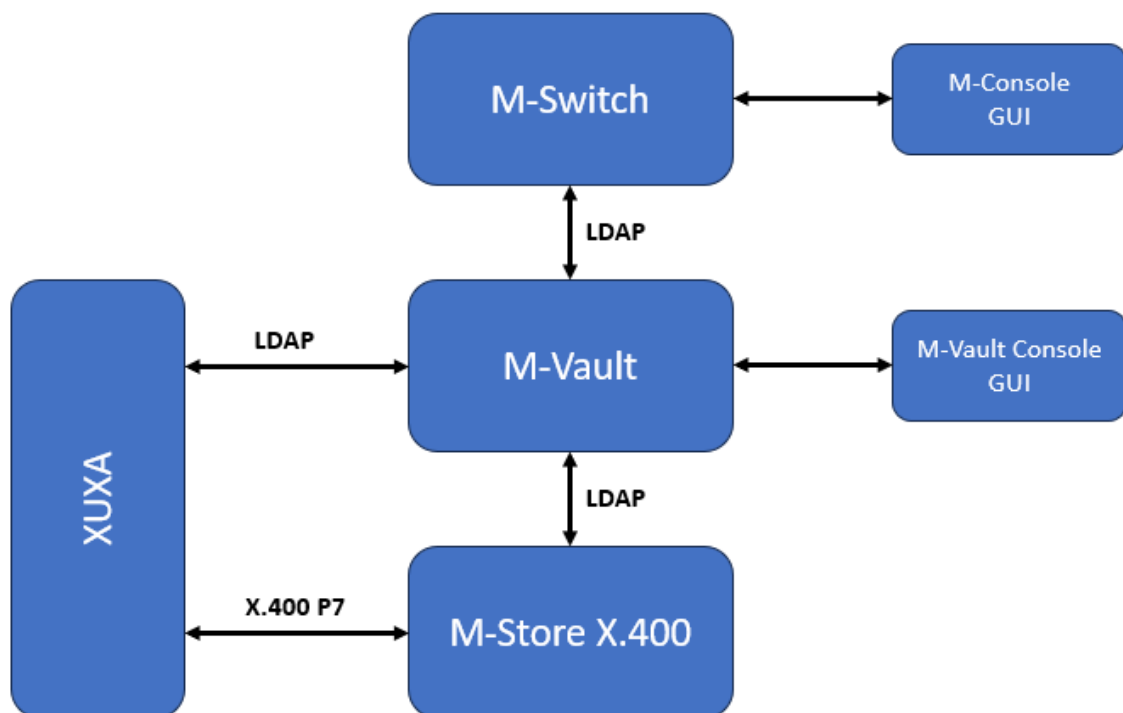
www.isode.com/product/ldap-x-500-directory/

Objectives

In this guide you will be shown how to configure the X.400 PRMD "/P=X400/A=Isode/C=GB/ and to configure connections to other X.400 MTAs.

The diagram below gives an overview of this setup.

System Overview

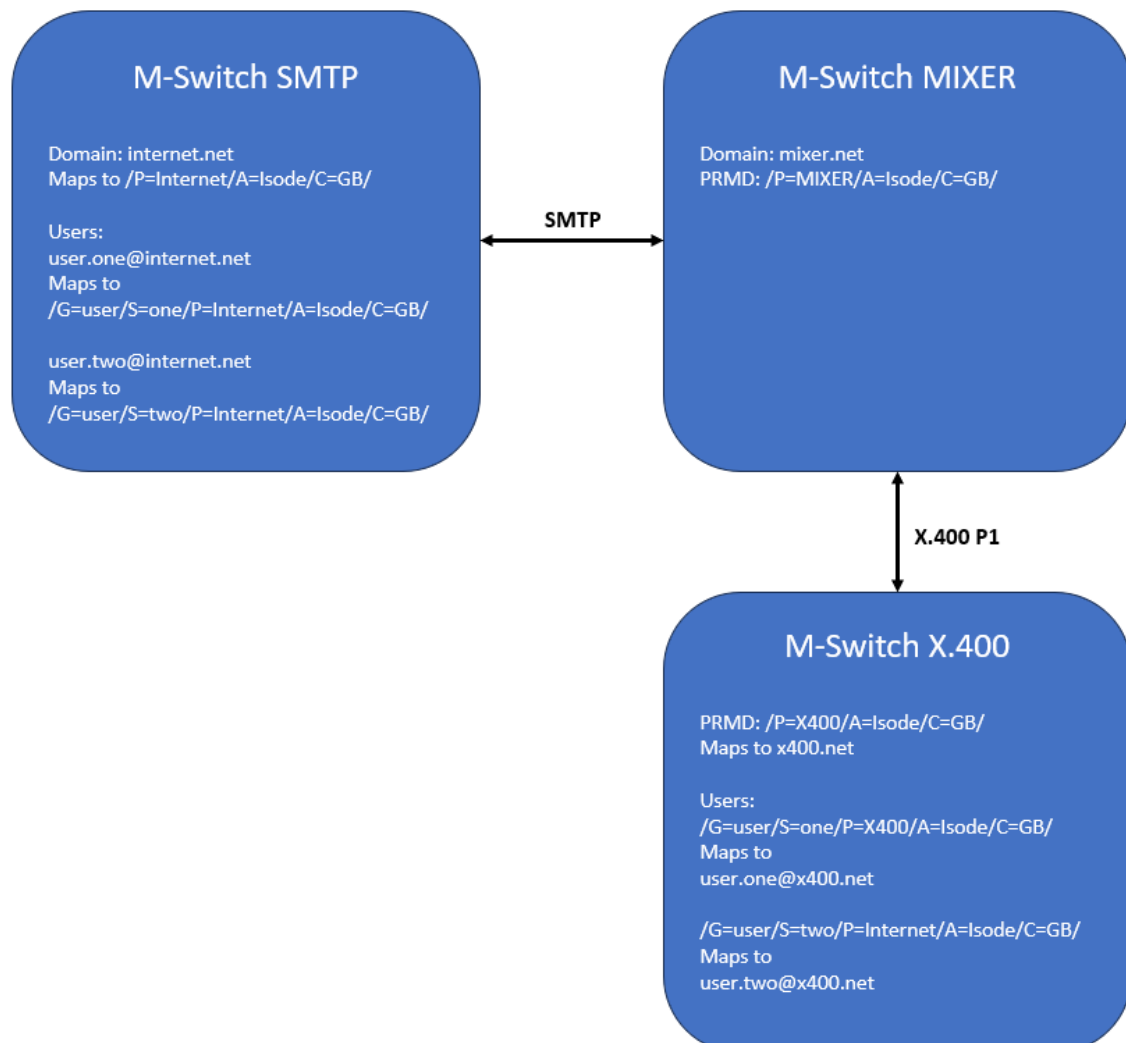


By the end of this guide you will have:

1. Installed the M-Switch, M-Vault, and M-Store X.400 products.
2. Configured M-Switch and M-Vault using MConsole.
3. Provisioned Users using MConsole.
4. Configured XUXA to connect to these Users.
5. Logged in using XUXA and sent Messages between Local X.400 Users
6. Created a connection to an external X.400 MTA server (M-Switch MIXER).
7. Configured all components for strong authentication

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-X400-EVAL

Make the primary dns suffix for the server X400.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 Core 19.2v2

M-Switch Core 19.2v2

M-Store Core 19.2v2

MAS 1.1V3

On Windows, M-Store is part of the M-Switch package.

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
```

On Linux, the following install files were used :

```
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

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

ISDxuxa-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, M-Switch X400 Core and M-Store Core for a “R19.2 Core M-Switch X400 Evaluation”. If evaluating P3/P7 Strong Authentication, please make this clear.

Creating the Messaging Configuration

Running the MConsole Configuration Wizard

In this section 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.

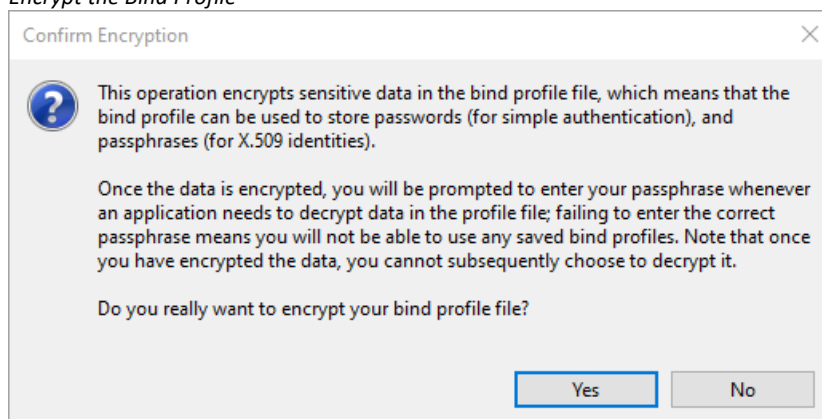
On Windows, start MConsole from the Windows Start Menu.

On Linux type the command:

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

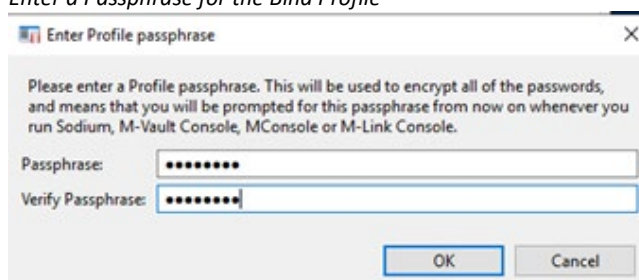
You will see the following prompt:

Encrypt the Bind Profile



Click "Yes"

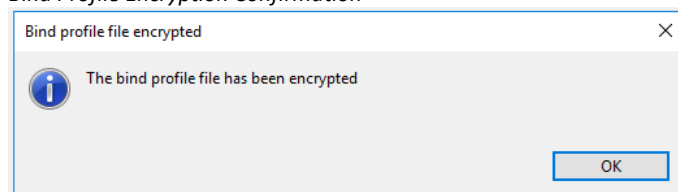
Enter a Passphrase for the Bind Profile



Enter and verify the passphrase "Secret1+"

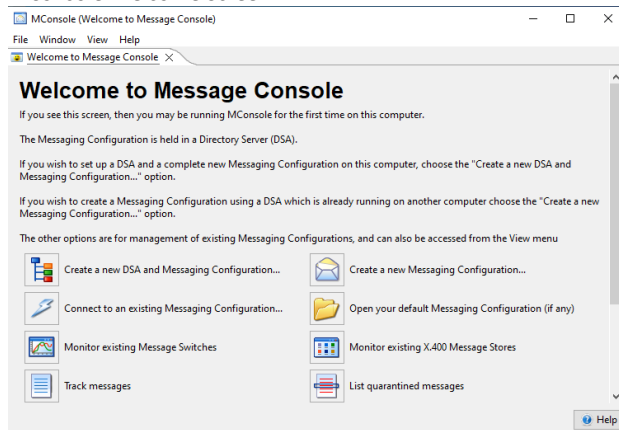
Click "OK"

Bind Profile Encryption Confirmation



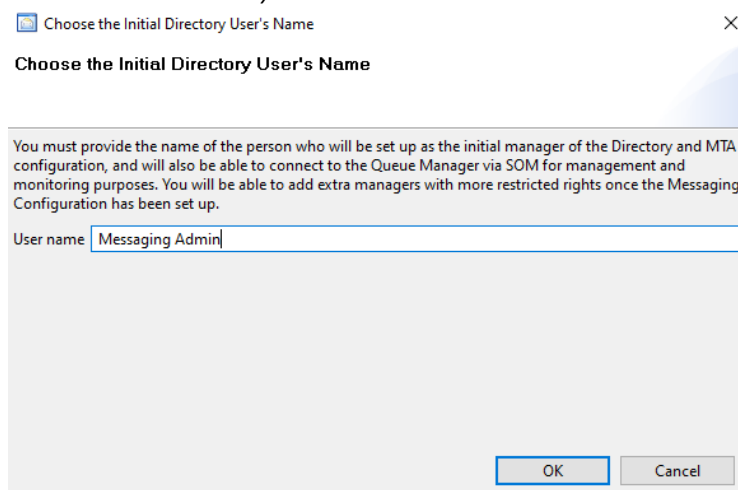
Click "OK"

MConsole Welcome Screen



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

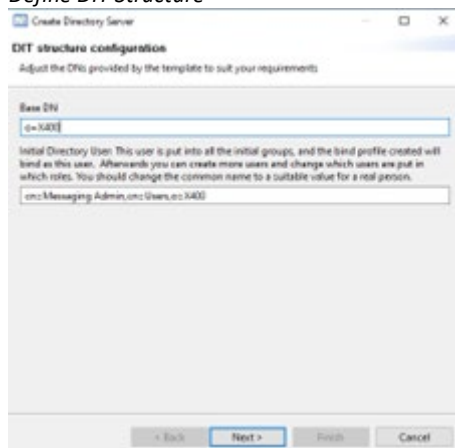
Choose the initial Directory Users name



Enter your User name. This user will be the Master Directory User account and have full access to the Directory Server.

Press “OK”

Define DIT Structure



Enter a “Base DN” of your choice.

In this guide we have changed the Base DN to “o=X400”

Click “Next >”

Provide a password for the Initial Directory user

Provide a password

Press “Next >”

Bind Profile Summary

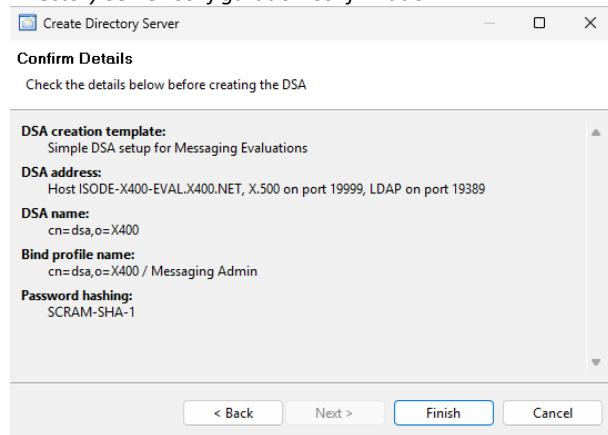
Click “Next >”

Directory Server Summary

Type the hostname “ISODE-X400-EVAL.X400.NET”

Click “Next >”

Directory Server Configuration Confirmation

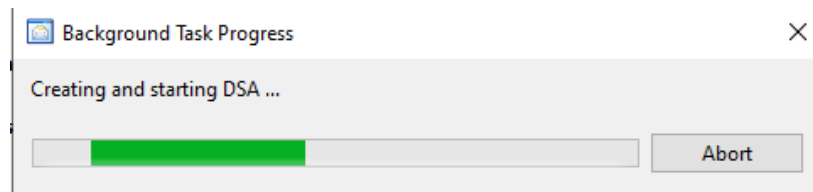


Click “Finish”.

The DSA is created and started.

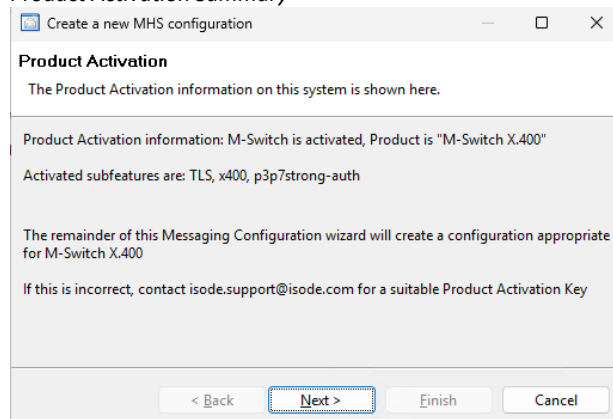
You may see the following – wait.

Directory Server Creation and Starting



You will then see the following screen:

Product Activation Summary



Click “Next >”

Set the Messaging Configuration Base DN

You should select the top entry, o=X400 in this case.

Click “Next >”

Set the Hostname

Type the hostname “ISODE-X400-EVAL.X400.NET”

Click “Next >”

Provide Passwords

Provide the “SASL Password”

Provide the “Passphrase for M-Switch Service”

Click “Next >”

Create Initial Security Database

Create a new MHS configuration

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

Security database file name: switch\mta.secd

Passphrase: Secret1+ Hide

< Back Next > Finish Cancel

Provide the “Security Database Password”

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@ISODE-X400-EVAL.X400.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=X400 Pick...

Admin user name: mtaAdmin sasl.USE-@X400-EVAL.X400.NET

Admin password: Show

< Back Next > Finish Cancel

Click “Next >”

X400 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: X400

Organization:

OU1: OU2:

OU3: OU4:

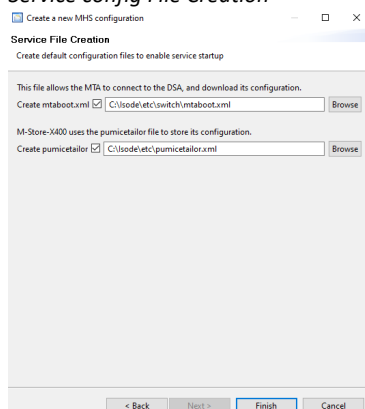
☒ Create an X.400 Message Store for local P7 users
☐ Create a legacy X.400 Message Store
☐ Do not create an X.400 Message Store

< Back Next > Finish Cancel

You now need to set your X.400 Address Space : “/P=X400/A=ISODE/C=GB/” in our example.

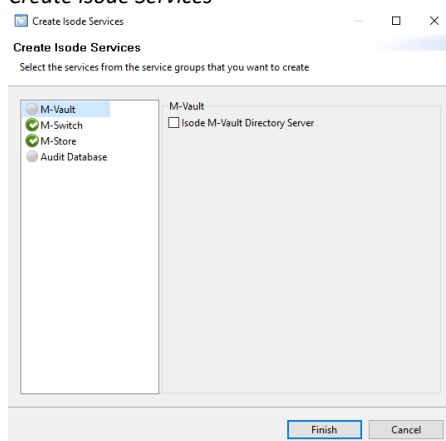
Click “Next >”

Service config File Creation



Click “Finish”.

Create Isode Services

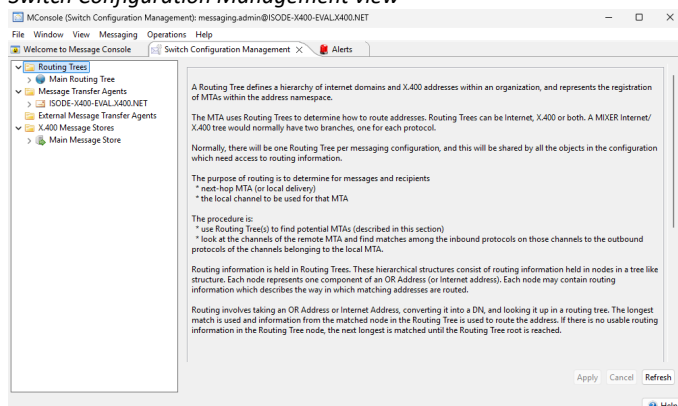


The above install option only appears in a Windows environment.

You can now choose to create any additional Isode Services in addition to defaults. The Audit database is a useful facility for which services may be added here. For further configuration details, please refer to the “M-Switch Core Mixer Evaluation Guide”.

Click “Finish”.

Switch Configuration Management view



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

Connection Timeout Alert

The screenshot shows the MConsole Alerts window. The title bar reads 'MConsole (Alerts): messaging.admin@ISODE-X400-EVALX400.NET'. The menu bar includes 'File', 'Window', 'View', and 'Help'. The toolbar has icons for 'Welcome to Message Console', 'Switch Configuration Management', and 'Alerts'. The 'Alerts' tab is active, showing a table of alerts. The table has columns: Time / Date, Source, Severity, Level, Facility, Message Id, Program, and Description. There are three rows of alerts. The first two rows show errors from 'local' source at '2026-07-31 13:43:58'. The third row shows a warning from 'local' source at '2026-07-31 13:44:08'. Below the table, the 'Alert Details' section shows 'Facility Name: MConsole' and 'Source: Local Files - ISODE-X400-EVALX400.NET (not connected)'. The 'Alert Status' section shows 'Acknowledged: No' and 'Stored events: 3'. The bottom right corner shows the date '31 Jul 2026, 13:45:20 BST' and a 'Help' button.

Time / Date	Source	Severity	Level	Facility	Message Id	Program	Description
2026-07-31 13:43:58	local	E	Local	MConsole	Error	SwitchConnection	Failed to connect to qmgr:Cannot connect to qmgr. password not set
2026-07-31 13:43:58	local	E	Local	MConsole	Error	SwitchConnection	Failed to connect to qmgr:Cannot connect to qmgr. password not set
2026-07-31 13:44:08	local	W	Local	MConsole	Warning	SwitchConnection	Timed out while connecting:ISODE-X400-EVALX400.NET

Alert Details
Facility Name: MConsole
Source: Local Files - ISODE-X400-EVALX400.NET (not connected)

Alert Status
Acknowledged: No
Stored events: 3

31 Jul 2026, 13:45:20 BST

The alerts tab can be safely closed.

You have now created your base M-Switch X.400 Configuration. We now need to start the services.

Starting the Services

Before starting the services on Linux, make the following changes:

```
cd /etc/isode/

cp pp.rc.sample pp.rc
```

Edit the file “pp.rc” to disable any SMTP server daemons:

```
# To disable any SMTP server daemons, define inet_smtp=1

inet_smtp=1
```

On Linux use the following commands to start the services:

```
systemctl start pp

systemctl start pumice
```

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

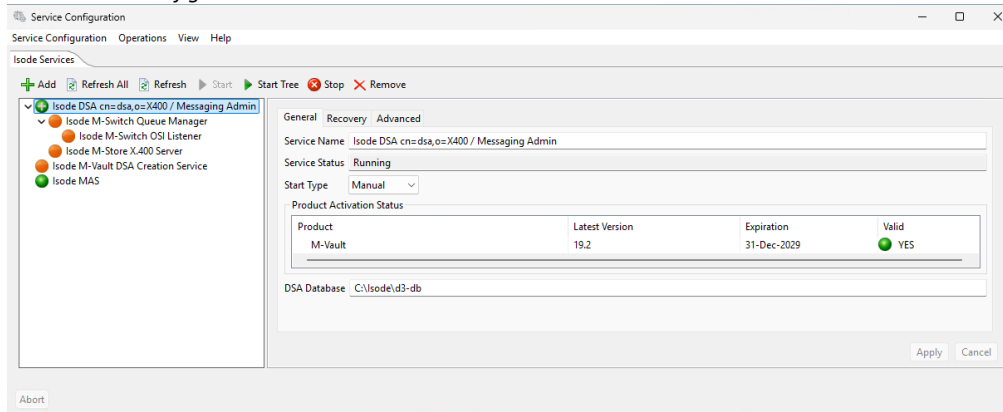
```
systemctl enable isode-dsa@d3-db

systemctl enable pp

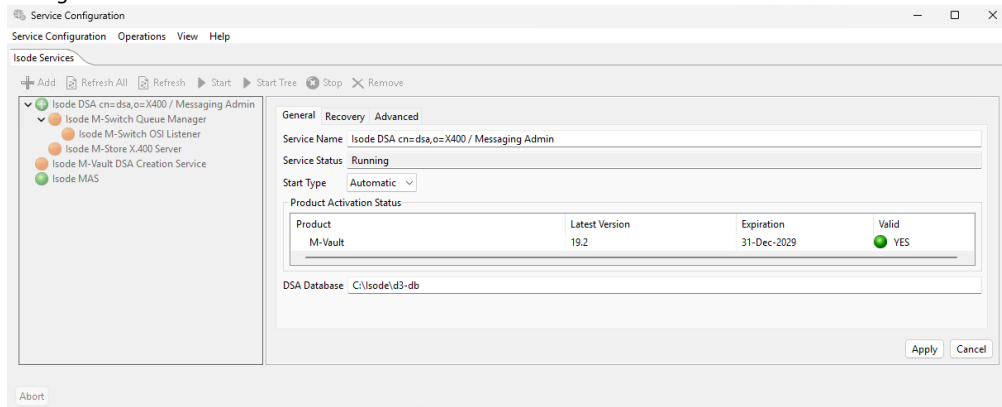
systemctl enable pumice
```

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

The following screen is displayed :

Isode Service Configuration Tool

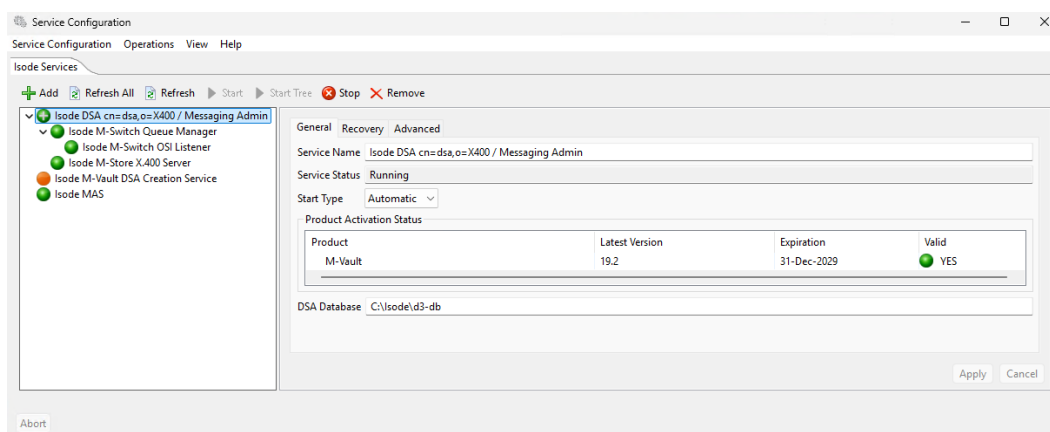
Select the “Isode DSA cn=dsa, o=x400...” Service.

Change to Automatic

Change the “Start Type” from “Manual” to “Automatic” using the Drop Down and Click “Apply”.

Do the same for the “Isode M-Switch Queue Manager”, “Isode M-Switch OSI Listener” and “Isode M-Store X.400 Server”.

Then start the “Isode M-Switch Queue Manager”, “Isode M-Switch OSI Listener” and “Isode M-Store X.400 Server” services.

Isode Services Started

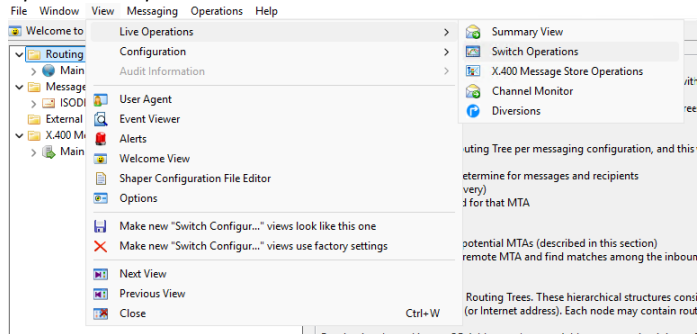
This completes the Windows services configuration. We will now return to MConsole.

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.

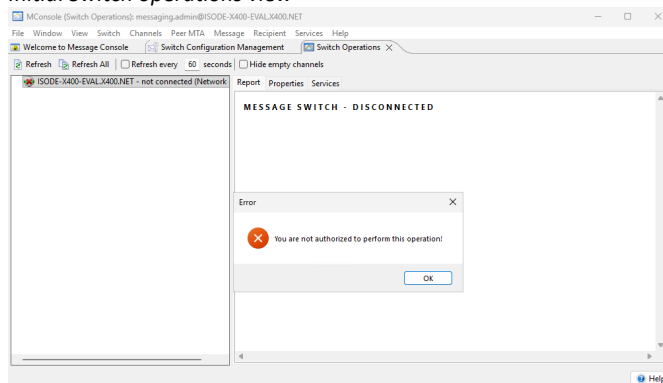
From the MConsole top menu select View→Live Operations→Switch Operations.

Open switch operations view



The following error is expected.

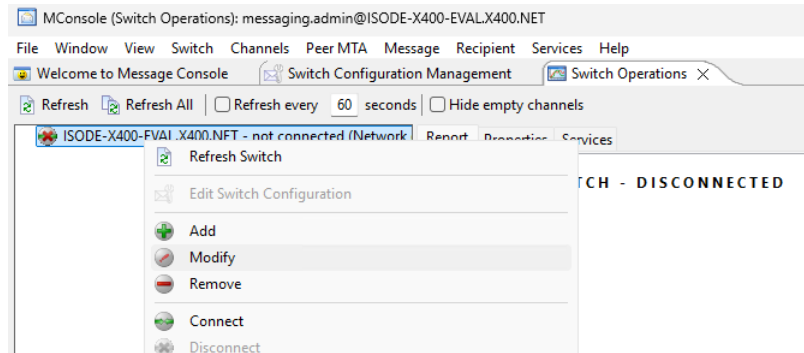
Initial Switch operations view



Click “OK” to clear it.

Right click on the Switch displayed and select “Modify”

Connect to switch



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

Provide Connection Password

Edit Message Switch

Friendly Name

ISODE-X400-EVAL.X400.NET

Host

ISODE-X400-EVAL.X400.NET

Userid

messaging.admin@ISODE-X400-EVAL.X400.NET

Password

Secret1+

Hide

Authentication Mechanism

SCRAM-SHA-1

Use TLS for SOM protocol

MTA

ISODE-X400-EVAL.X400.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.

Add...

Remove

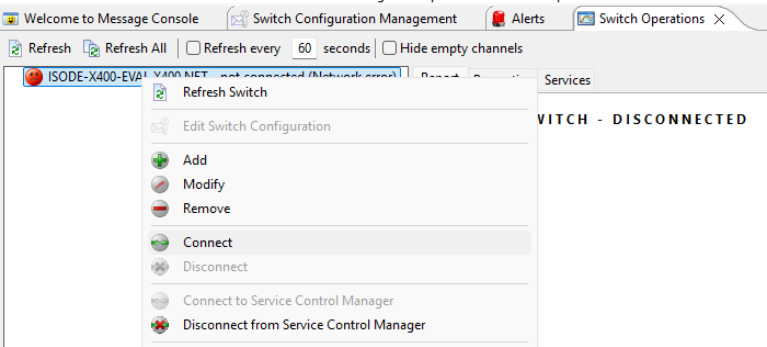
OK

Cancel

Click “OK”.

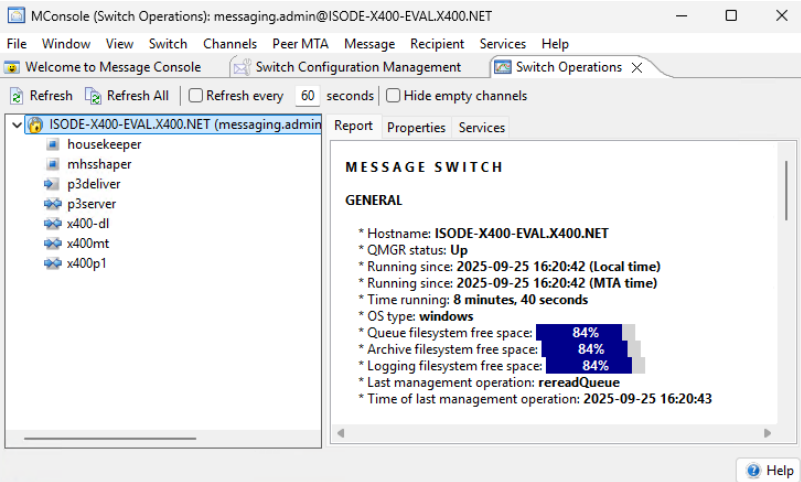
If a connection isn’t automatically made, use the context menu to connect.

Connect context menu option



The following screen will be displayed:

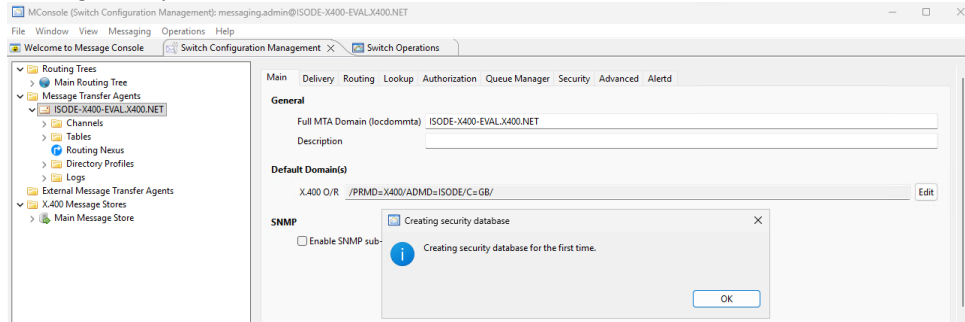
Switch operations view connected



Creating the Security Database

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

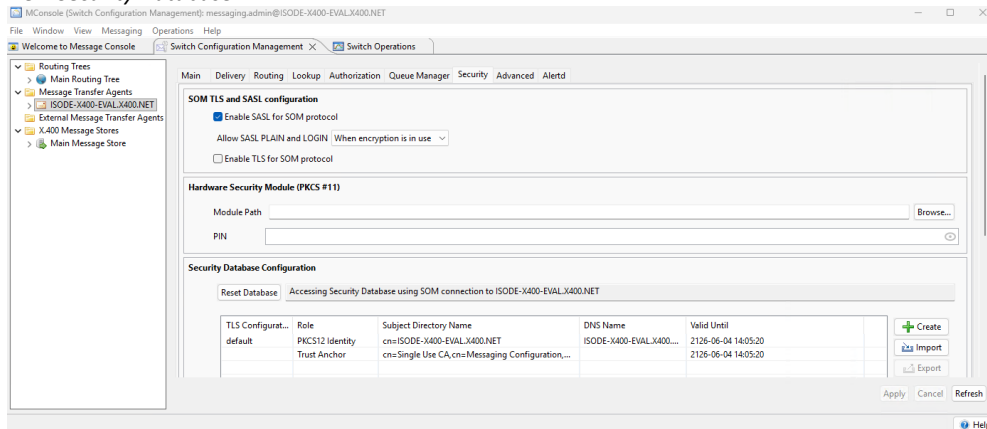
Creating Security Database



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

Select the “Security” tab.

New Security Database

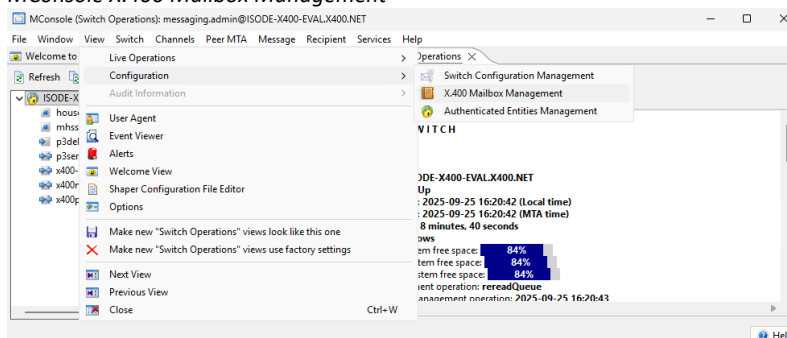


Note that a database has been created with a single use CA trust anchor and a self-signed certificate.

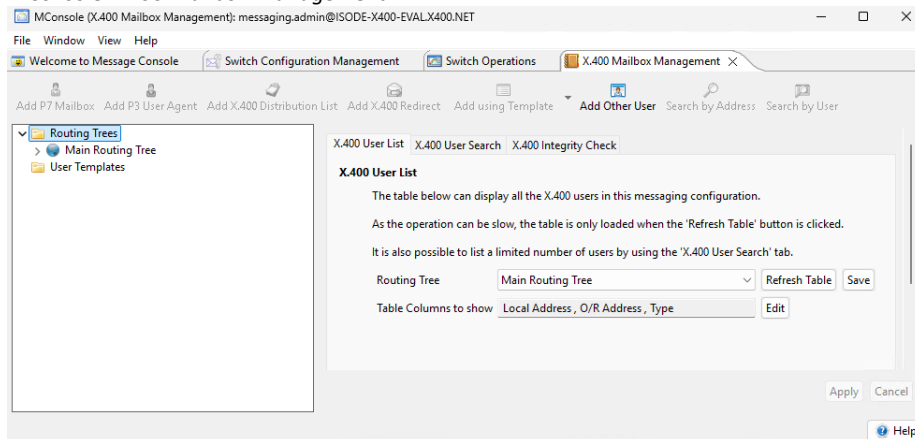
Configuring X.400 P7 Users

From MConsole select View→Configuration→X.400 Mailbox Management.

MConsole X.400 Mailbox Management

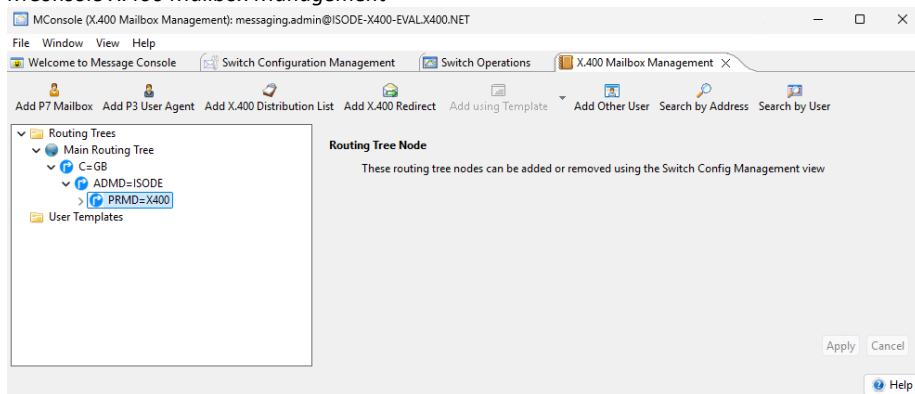


MConsole X.400 Mailbox Management



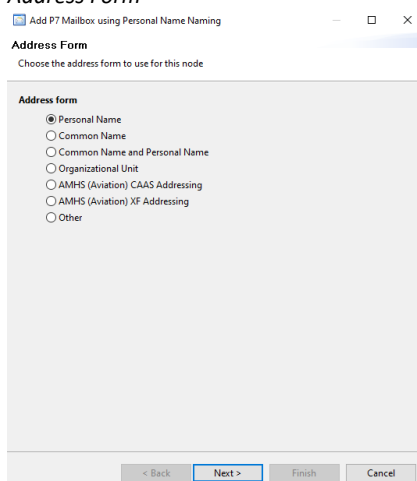
Expand the “Main Routing Tree” on the left until you reach your X.400 Address Space (/PRMD=X400/ADMD=ISODE/C=GB/) in this example and select it.

MConsole X.400 Mailbox Management



Click “Add P7 Mailbox”

Address Form



Select “Personal Name” (or whatever suits your deployment)

Click “Next >”

Add User One mailbox

Add P7 Mailbox using Personal Name Naming

Node name (Personal Name Addressing)
Enter the Personal Name for this node

Surname: One
Given name: User
Initials:
Generation Qualifier:

< Back Next > Finish Cancel

Enter “One” for “Surname” and “User” for “Given name”

Click “Next >”

Confirm O/R address

Add P7 Mailbox using Personal Name Naming

O/R Address
Confirm the chosen O/R Address for this node

O/R Address: /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/ Edit

< Back Next > Finish Cancel

Click “Next >”

Create White pages entry

Add P7 Mailbox using Personal Name Naming

White Pages (Address Book) Entry
Configure a White Pages entry for this address

☐ Do not set up a White Pages entry
☒ Create new White Pages entry

Directory Root
Select where in the DIT the White Pages entry will be created
Directory: cn=White Pages,o=X400 Pick...

Common Name: User One
Initials:
Surname: One
Given name: User

☐ Amend existing White Pages entry

Directory Entry
Select the existing Directory entry to amend
Directory Entry: cn=White Pages,o=X400 Pick...

Advanced White Pages values can be set within the White Pages tab in X.400 Mailbox Management

< Back Next > Finish Cancel

Click “Next >”

MTA and Message Store Details

MTA and Message Store Details
Configure which Message Store, MTA and delivery channel this user will use

Message Store
cn=Main Message Store,cn=Messaging Configuration,o=X400

Supporting MTA
cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration,o=X400

P3 Delivery Channel
p3deliver

< Back Next > Finish Cancel

Click “Next >”

Set P7 password

Passwords
Set the User's P7 and P3 passwords

P7 Message Store Password Secret1+ Hide

P3 Access Password Secret1+ Hide

< Back Next > Finish Cancel

Provide and confirm a message store password.

Click “Finish”

User One mailbox created

MConsole (X.400 Mailbox Management): messaging.admin@ISODE-X400-EVAL.X400.NET

File Window View Help

Welcome to Message Console Switch Configuration Management Switch Operations X.400 Mailbox Management

Add P7 Mailbox Add P3 User Agent Add X.400 Distribution List Add X.400 Redirect Add using Template Add Other User Search by Address Search by User

Routing Trees
Main Routing Tree
C=GB
ADMD=ISODE
PRMD=X400
G=User*S=One

User Templates

Message Store Routed UA Synonyms, Aliases and Redirects White Pages

P7 Message Store Password Enter value to reset password Show

P3 Access Password Enter value to reset password Show

Mailbox Name One0

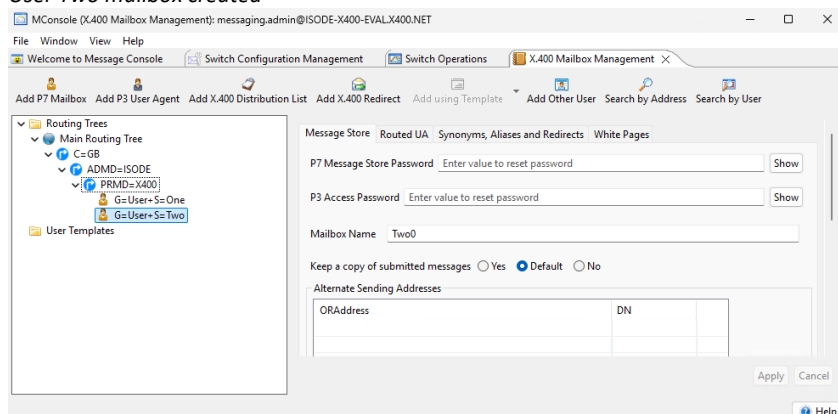
Keep a copy of submitted messages Yes ☒ Default No

Alternate Sending Addresses

ORAddress	DN

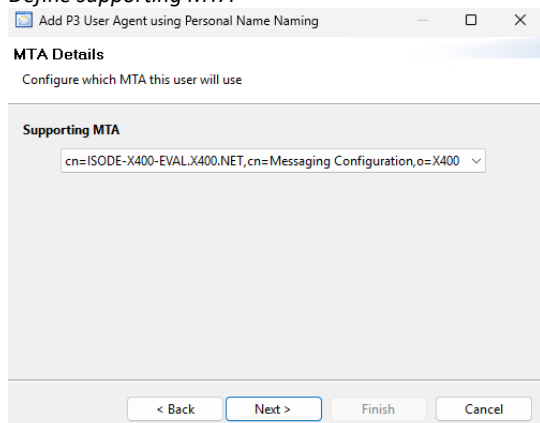
Apply Cancel Help

Repeat the process for “User Two” (/G=User/S=Two/PRMD=X400/ADMD=ISODE/C=GB/)

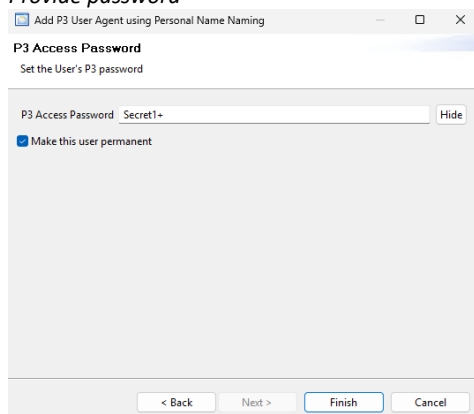
User Two mailbox created**Configuring X.400 P3 Users**

It's also possible but not essential to configure users that might access the switch directly using the P3 protocol. To do that, follow the steps in the previous section but press the button “Add P3 User Agent” instead of the “Add P7 Mailbox”. Add “User Three”.

In this case, only a “Supporting MTA” will be required.

Define supporting MTA

Click “Next >”

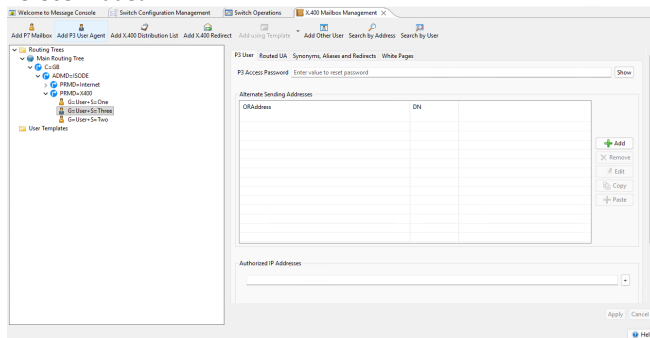
Provide password

Provide a password to authenticate to the P3 channel

Select “Make this User Permanent”

Press “Finish”

P3 User Added



This completes the configuration of the System for Local Users. We will now test the system with xuxa.

Testing the System with xuxa

P7 mailboxes

XUXA is Isode's test UA.

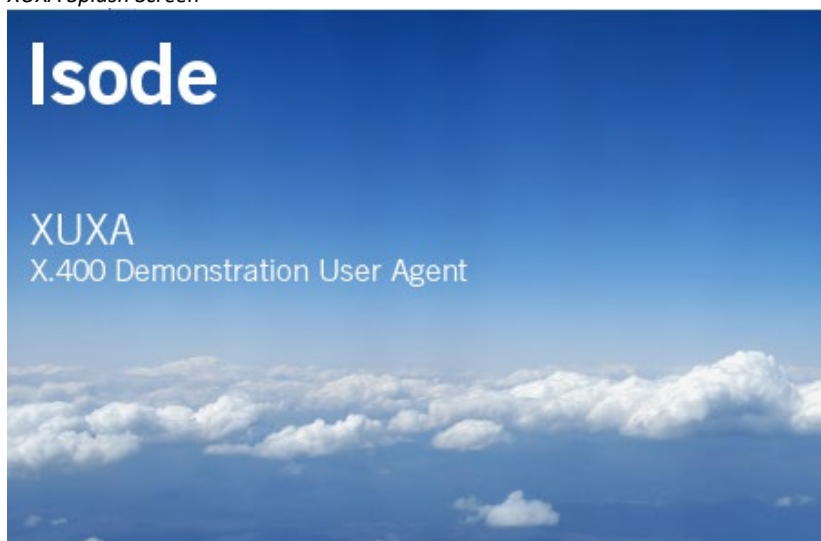
XUXA is started on Linux as below:

```
% /opt/isode/bin/xuxa
```

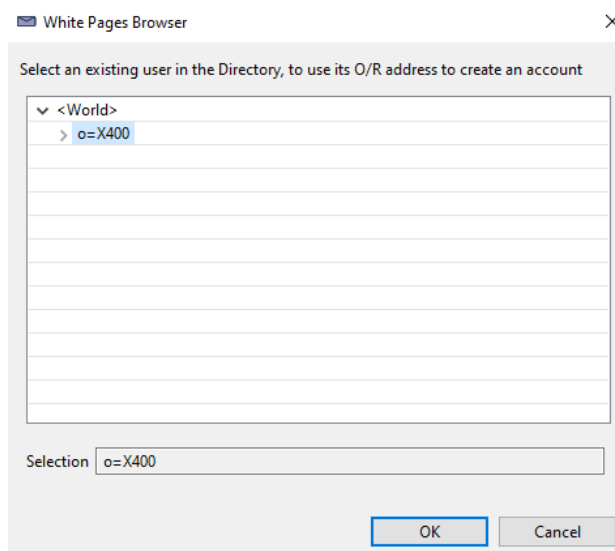
On Windows it can be found on the Windows start menu.

The following splash screen is displayed.

XUXA Splash Screen

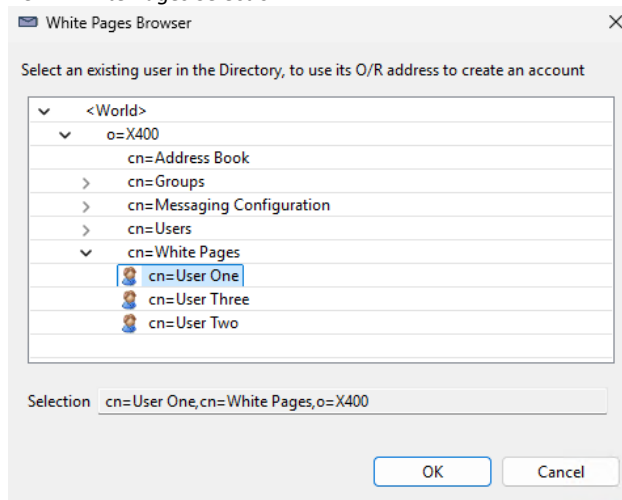


XUXA Initial Screen



Expand o=X400 and cn=White Pages as follows:

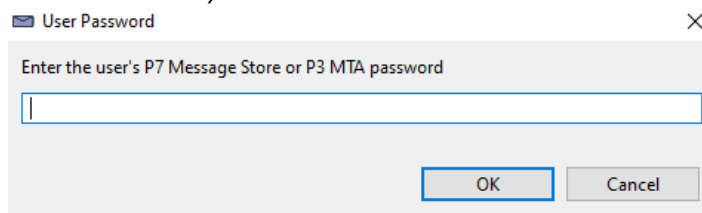
XUXA White Pages Selection



Select “cn=User One”

Click “OK”

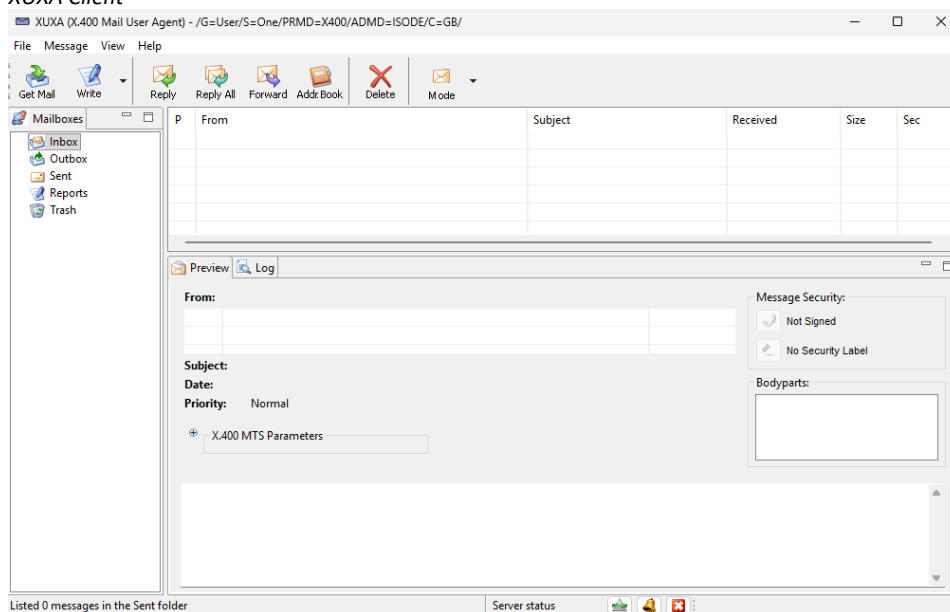
XUXA Password Entry



Enter the mailbox password (“Secret1+”)

Click “OK”

XUXA Client



Click “Write”.

New message

Click the “Address Book” Icon below “**From:**”

Address book

Select User One and User Two in turn and Click “To”

Address message

Click “OK”

Create test message

Enter some text in the Subject and Body then click the “Send” Icon (Top Left).

The following is displayed:

Message submitted

Click “OK”.

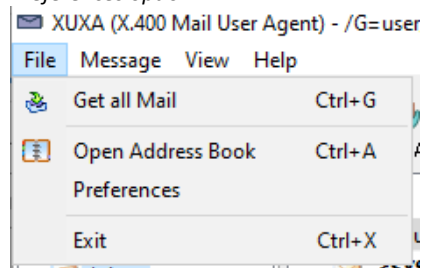
Press “Get Mail”

Message received

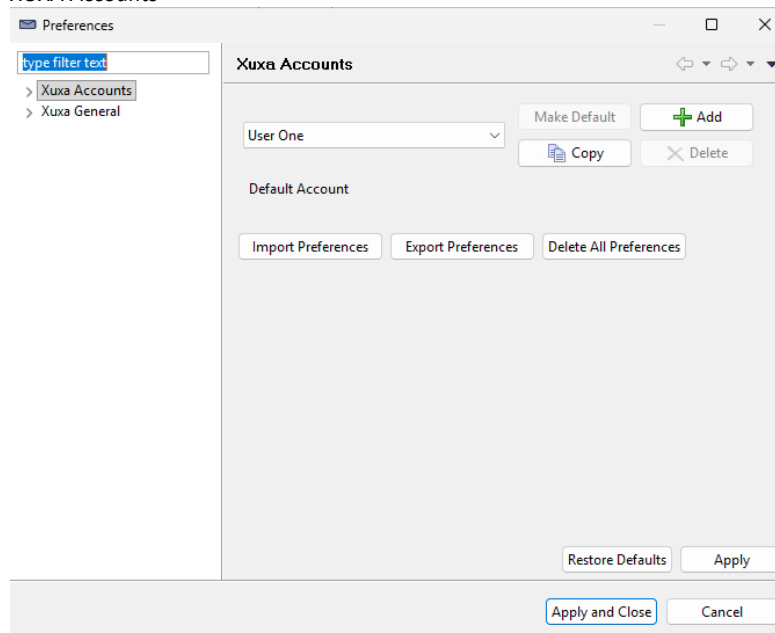
We now need to configure XUXA for User Two.

From the Top Menu Select File→Preferences.

Preferences option

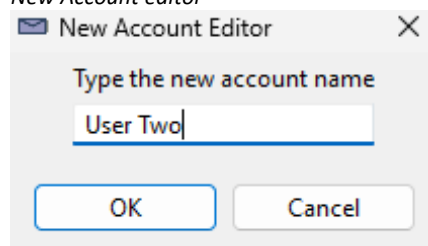


XUXA Accounts



Click “Copy”.

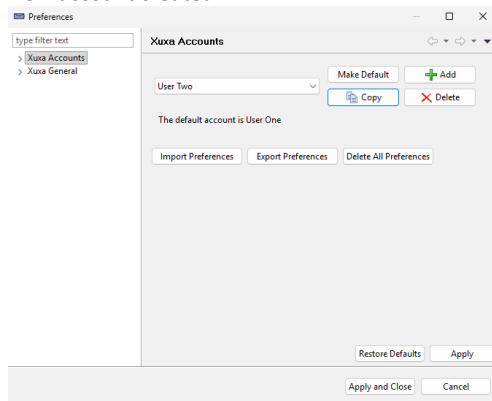
New Account editor



Name the new account

Click “OK”.

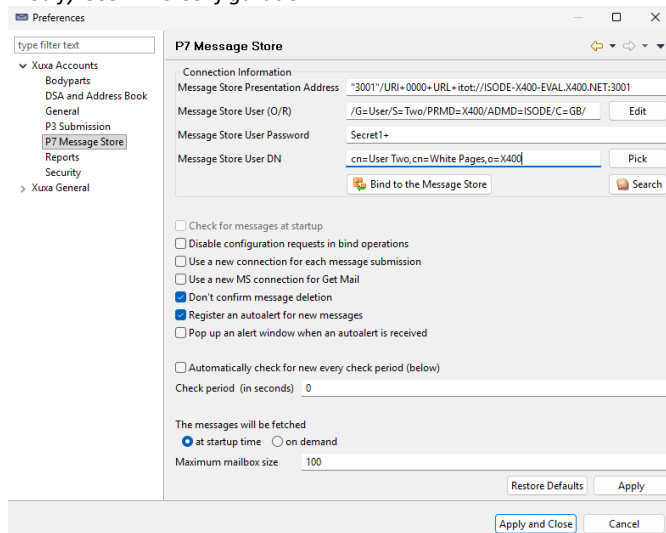
New account created



Expand “Xuxa Accounts” and select “P7 Message Store”.

Change the “Message Store Presentation Address”, “Message Store User (O/R)” and “Message Store User DN” as follows:

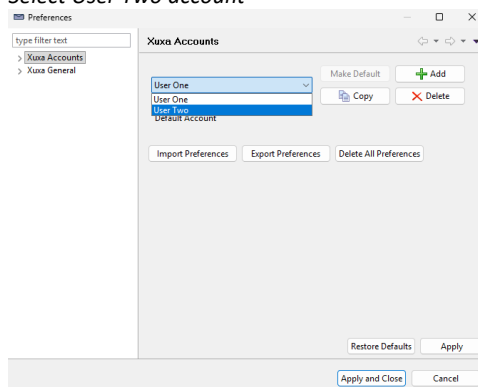
Modify User Two Configuration



Click “Apply and Close”.

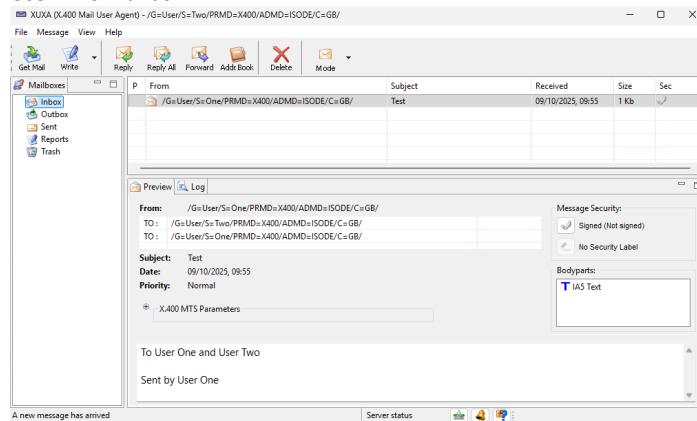
From the Top Menu Select File→Preferences

Select User Two account



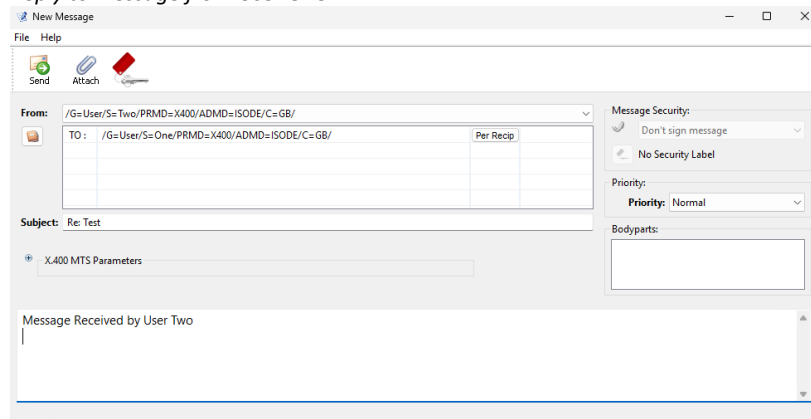
From the dropdown, select the account “User Two”
Press “Apply and Close”

User Two mailbox



You will see the message sent by “User One” – click the “Reply” icon.

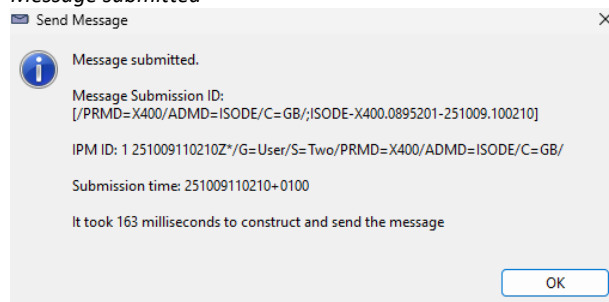
Reply to message from User One



Enter some Body Text.

Click the “Send” Icon.

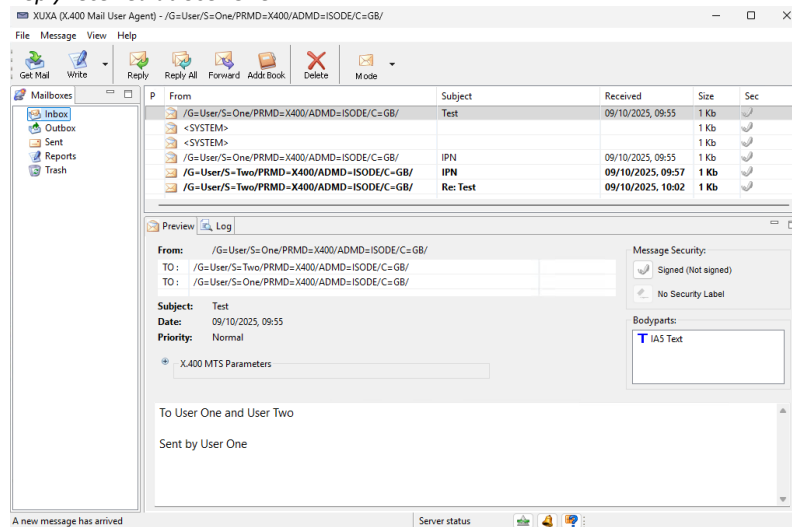
Message submitted



Click “OK”.

Now, using the File→Preferences Switch Back to the User One Account.

Reply received at User One



You can see that the message has been received.

This completes the testing of Local P7 Users.

P3 mailboxes

It's also possible to send and receive messages via p3 using xuxa.

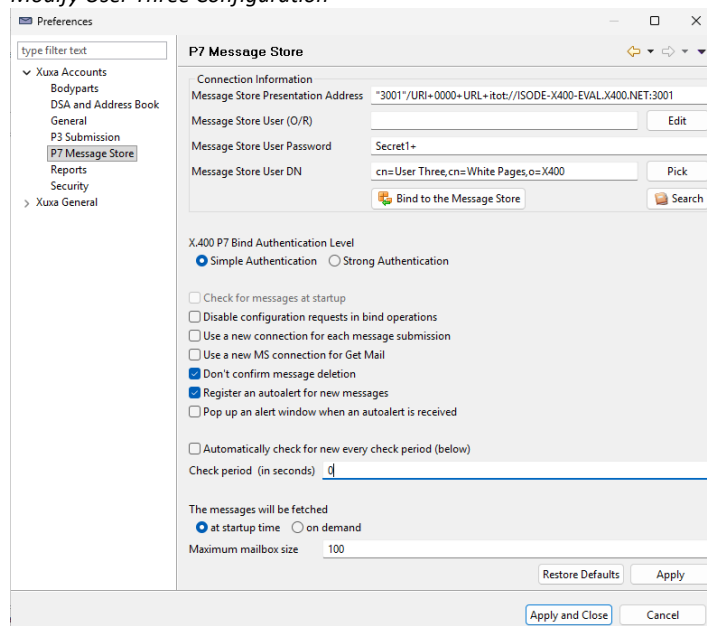
Follow the instructions in the previous section to copy the “User One” account.

Call it “User Three”

Expand “Xuxa Accounts and select “P7 Message Store”.

Change the “Message Store Presentation Address” and “Message Store User DN” and remove the “Message Store User (O/R)” as follows:

Modify User Three Configuration



Select the “P3 submission” tab

Change the “P3 Channel Presentation Address” and “P3 User O/R Address” as follows:

User Three P3 Configuration

P3 Submission

P3 Channel Presentation Address: *593*/URI+0000+URL+itot://ISODE-X400-EVAL.X400.NET

P3 User O/R address: /G=User/S=Three/PRMD=X400/ADMD=ISODE/C=GB/ Edit

P3 User Password: Secret1+ Bind to the P3 Channel Search

X.400 P3 Bind Authentication Level
☒ Simple Authentication ☐ Strong Authentication

☒ Force sending using P3, instead of via the P7 Message Store

P3 Delivery

If you want to read messages queued on the MTA's P3 channel for this user then unset the values in the user parameters in the P7 Message Store tab. If no P7 user values are found, the P3 Submission information will be used instead

NOTE: Receiving messages via P3 (delivery) requires the routing in the MTA to be correctly set, in particular the PP Channel of the user should be p3server, not p3deliver

Restore Defaults Apply

Apply and Close Cancel

Check “Force Sending P3, instead of via the P7 Message Store”

Click “Apply and Close”.

From the Top Menu Select File→Preferences

Select User Three account

Xuxa Accounts

User Three
 User One
 User Two
 User Three

Make Default Add Copy Delete

Import Preferences Export Preferences Delete All Preferences

Restore Defaults Apply

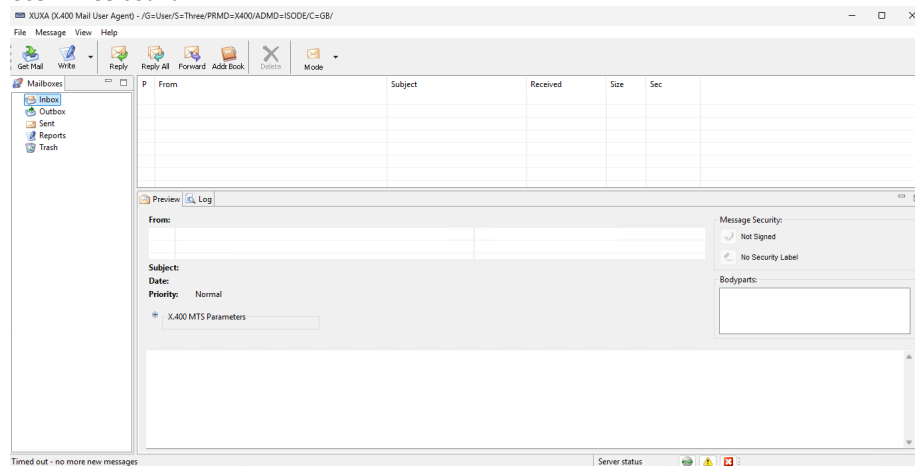
Apply and Close Cancel

From the dropdown, select the account “User Three”

Press “Apply and Close”

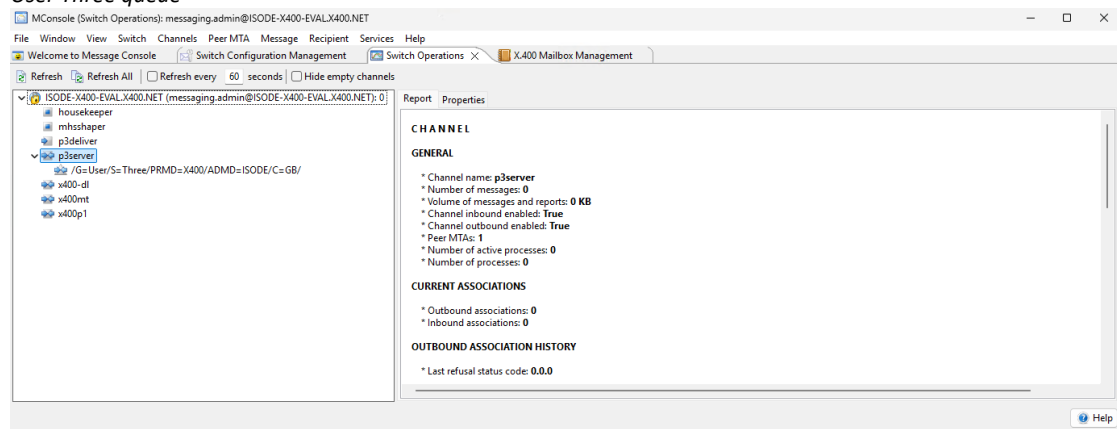
If that doesn’t work, select and apply one of the other profiles first

User Three bound



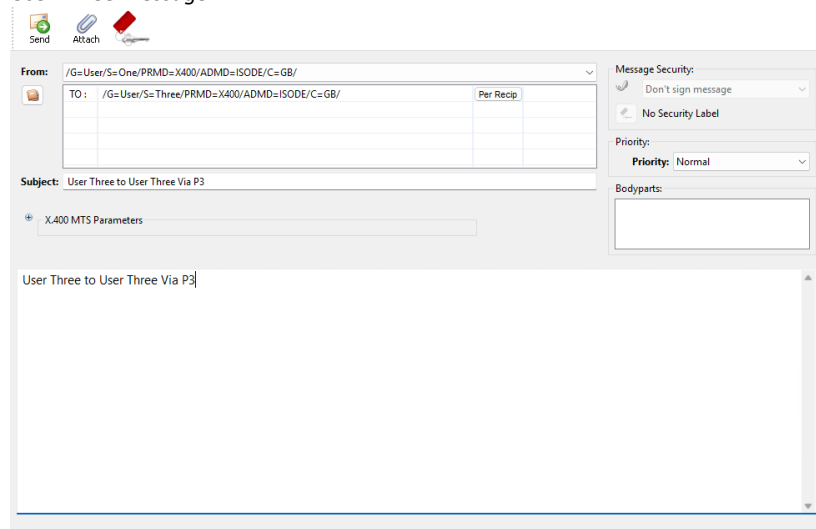
In the operations view in Mconsole, it's possible to see the queue for this connection and the bound UI:

User Three queue



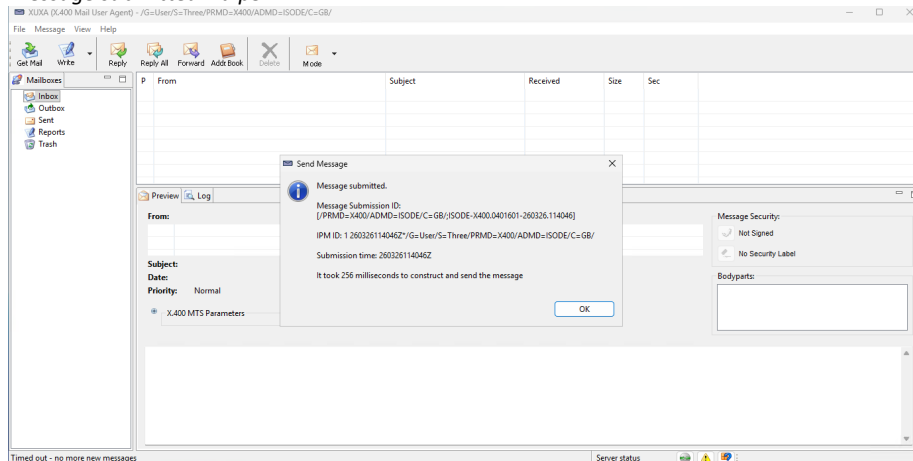
Write a Message from User Three to User Three:

User Three Message



Press "Send"

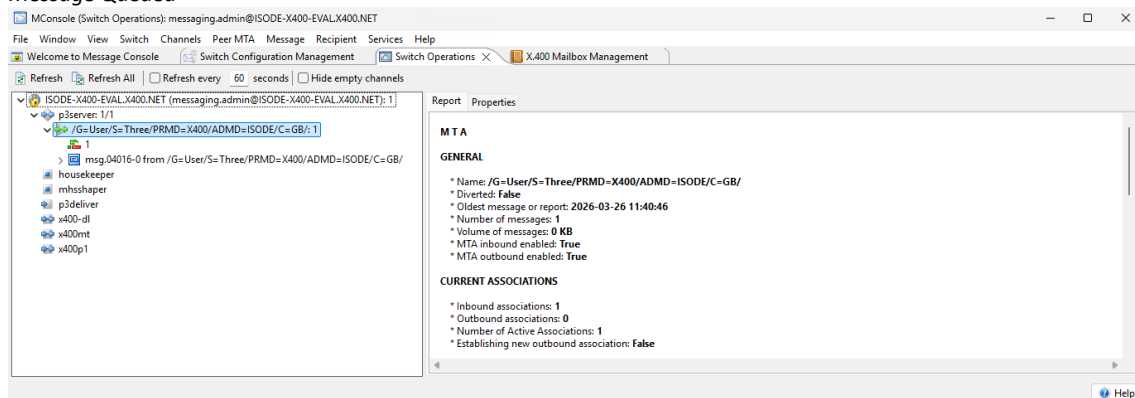
Message submitted via p3



Press “OK”

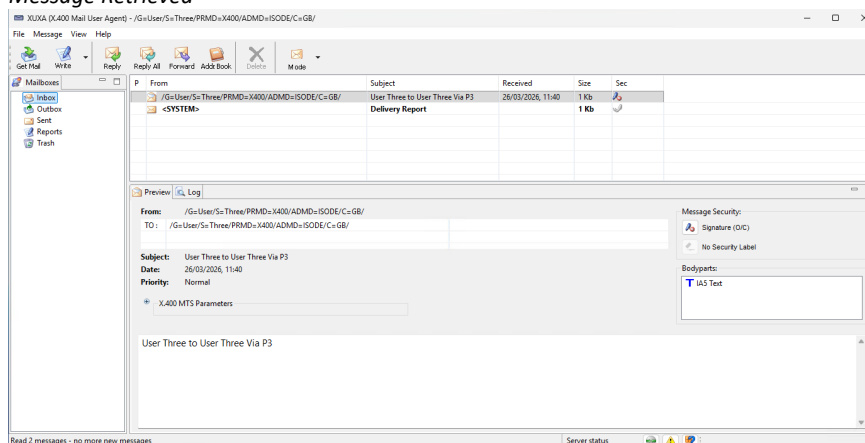
The message is queued:

Message Queued



Press “Get Mail”

Message Retrieved



Because P3 is a delivery mechanism and doesn't involve a message store, it is expected behaviour that if you close and reopen xuxa, the inbox will appear empty.

This completes the testing of Local P3 Users. We now need to configure an External MTA and some Address Book Entries.

Adding an External MTA and Address Book entries

Configuring the External MTA with MConsole

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

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 Core MIXER MTA described in the M-Switch Core MIXER Evaluation Guide and will use the following information.

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

Your MTA Password: Secret1+

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

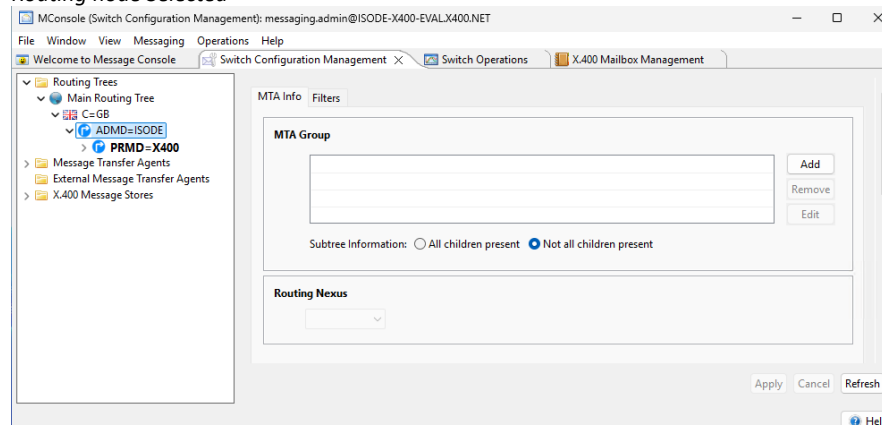
Their MTA Name: ISODE-MIXER-EVL.MIXER.NET

Their MTA Password: Secret1+

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

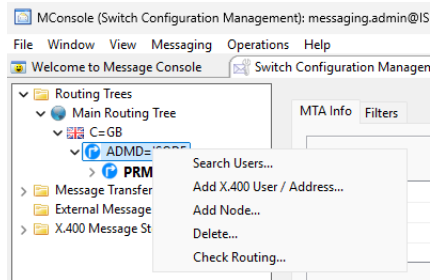
From MConsole expand the Routing Tree to the ADMD “Isode”

Routing node Selected



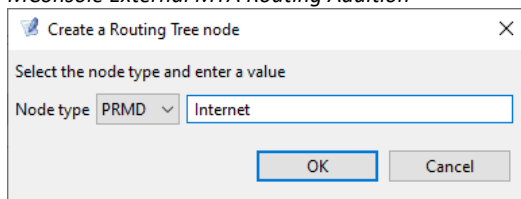
Right Click on “ADMD=Isode”

Context menu with Add Node



Select “Add Node...”.

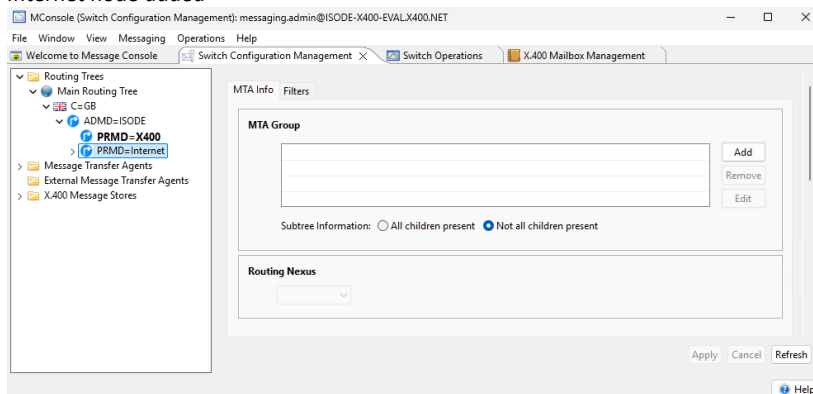
MConsole External MTA Routing Addition



Enter “Internet” for the “PRMD”

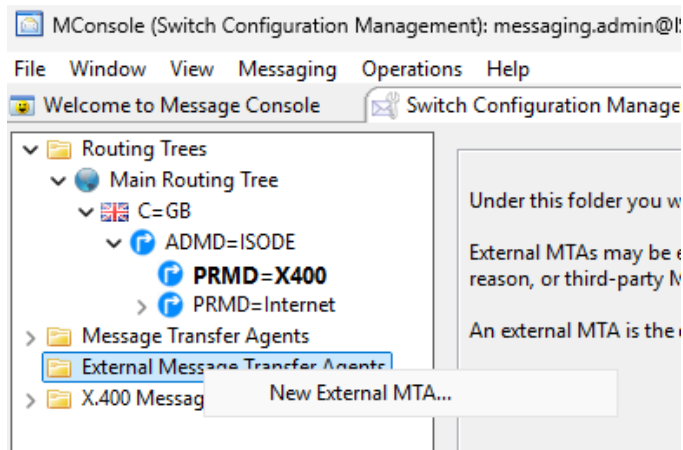
Click “OK”.

Internet node added



Right click on “External Message Transfer Agents”

Create new external MTA



Select “New External MTA...”

Select MTA type

Select “X.400”

Click “Next >”

Name the external MTA

In “MTA name in protocol” type “Their MTA Name”

In “Fully Qualified Hostname” type “Their Hostname/IP Address”

In “Directory Name” type a helpful label

Click “Next >”.

Expand the “Main Routing Tree” until you get to “PRMD=Internet”

Default Routing tree for MTA

Select “PRMD=Internet”

Click “Next >”

Remote X.400 authentication details

Provide the remote MTA password.

Click “Finish”.

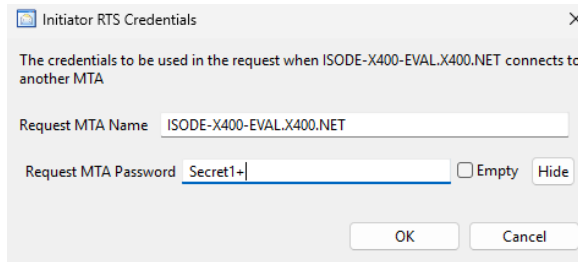
Remote MTA Added

You will see that this new MTA has been added as the MTA for the PRMD=Internet. We now need to configure the password for our x400p1 channel. Expand our MTA and Channels then select the x400p1 channel and select the “Auth” Tab.

MConsole Configure X.400 P1 Channel

Click “Edit” on the “Initiator RTS Credentials”

Initiator RTS Credentials



The credentials to be used in the request when ISODE-X400-EVAL.X400.NET connects to another MTA

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

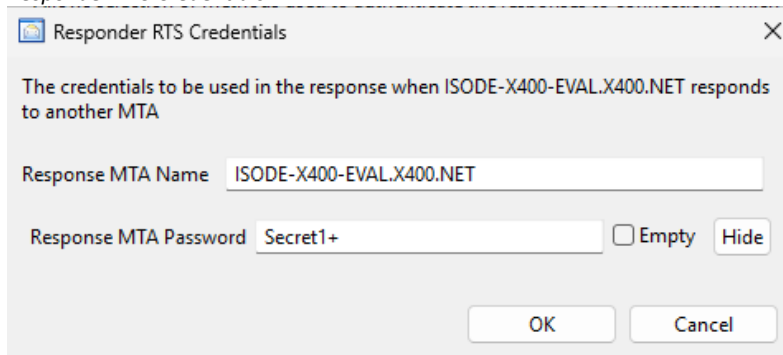
Request MTA Password: Secret1+ ☐ Empty

Change the Password to “Secret1+”

Click “OK”.

Repeat the process for the “Responder RTS Credentials”

Responder RTS Credentials



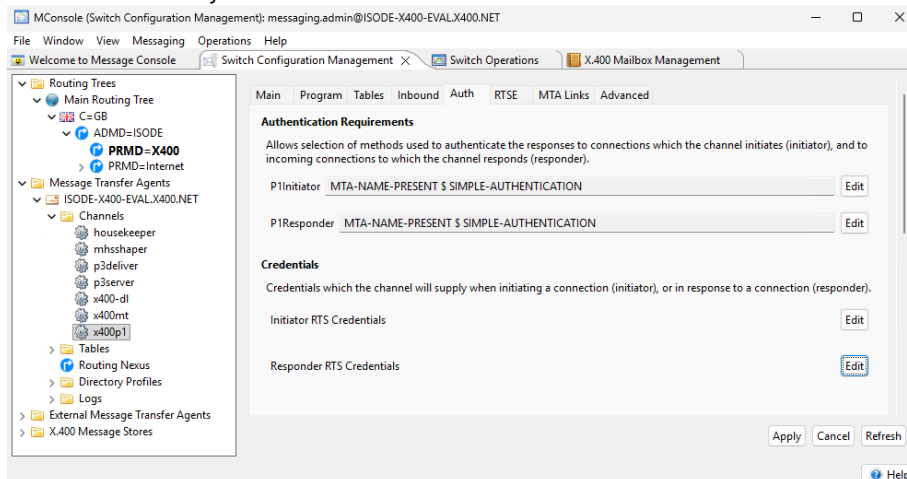
The credentials to be used in the response when ISODE-X400-EVAL.X400.NET responds to another MTA

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

Response MTA Password: Secret1+ ☐ Empty

Click “OK”.

RTS Credentials modified



MConsole (Switch Configuration Management): messaging.admin@ISODE-X400-EVAL.X400.NET

File Window View Messaging Operations Help

Welcome to Message Console | Switch Configuration Management | Switch Operations | X400 Mailbox Management

Routing Trees

- Main Routing Tree
 - C=GB
 - ADMD=ISODE
 - PRMD=X400
 - PRMD=Internet
 - Message Transfer Agents
 - ISODE-X400-EVAL.X400.NET
 - Channels
 - housekeeper
 - mhsstaper
 - p3deliver
 - p3server
 - x400-dl
 - x400mt
 - x400p1
 - Tables
 - Routing Nexus
 - Directory Profiles
 - Logs
 - External Message Transfer Agents
 - X400 Message Stores

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: MTA-NAME-PRESENT \$ SIMPLE-AUTHENTICATION

P1Responder: MTA-NAME-PRESENT \$ SIMPLE-AUTHENTICATION

Credentials

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

Initiator RTS Credentials

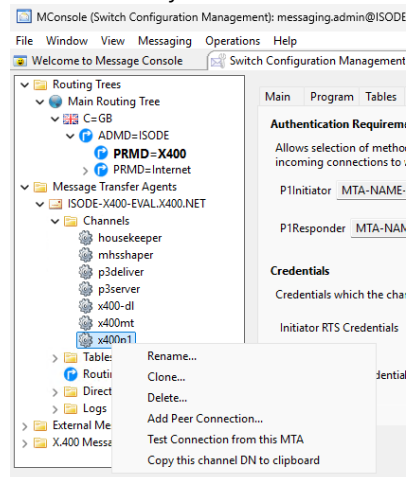
Responder RTS Credentials

Click “Apply”

We now need to test the Connection.

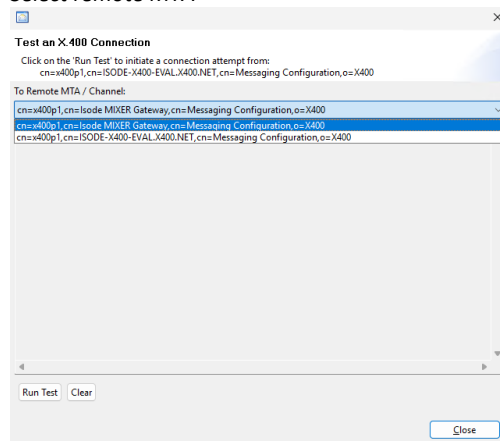
Right Click on the “x400p1” Channel.

Test Connection from this MTA



Select “Test Connection from this MTA”

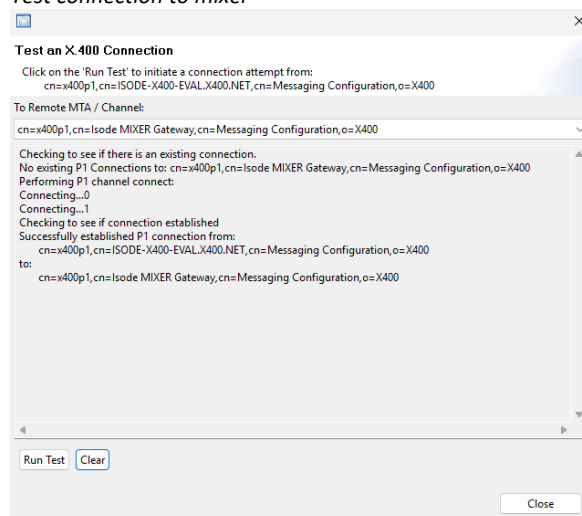
Select remote MTA



Select the remote MTA

Click “Run Test”

Test connection to mixer

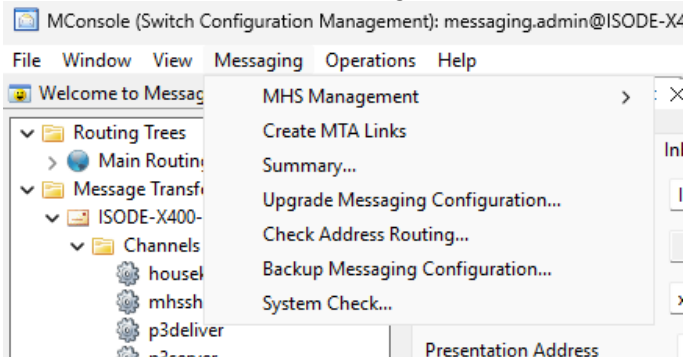


If you do not see a successful connection check Port 102 is open on both machines.

We now need to check the Routing.

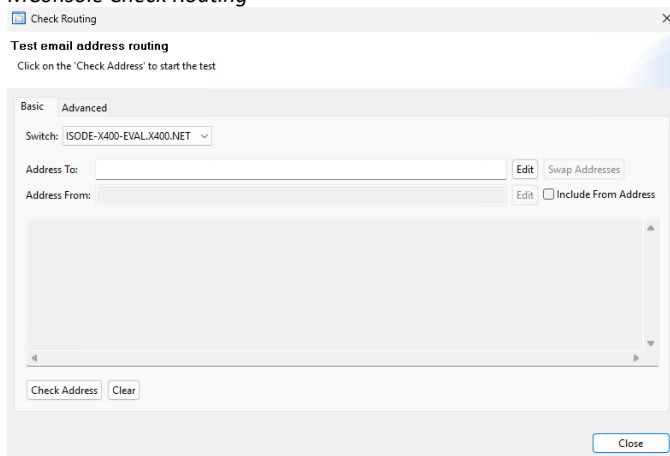
From the “Top Menu” click “Messaging”

Context menu with Check address routing



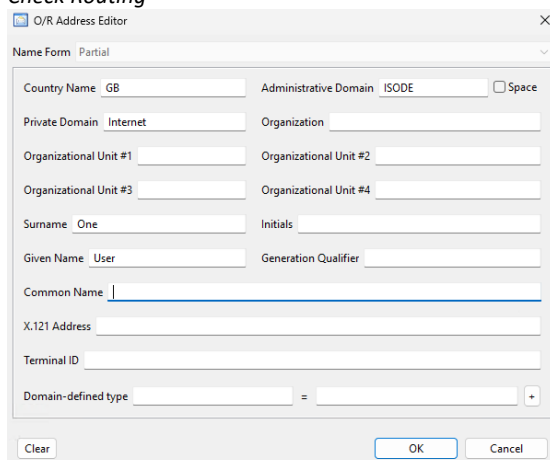
Select “Check Address Routing...”

MConsole Check Routing



Click “Edit” next to “Address To:”

Check Routing



Enter the details for the remote user and click “OK”.

Click “Check Address”

Route check results

Check Routing

Test email address routing
Click on the 'Check Address' to start the test

Basic

Advanced

Switch: ISODE-X400-EVAL.X400.NET

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

Edit

Swap Addresses

Address From:

Edit

☐ Include From Address

```

x400address: /G=User/S=One/PRMD=Internet/ADMD=ISODE/C=GB/
delivered-mta: cn=x400p1,cn=Isode MIXER Gateway,cn=Messaging Configuration,o=X400
delivered-channel: x400p1
channel-weight: 5
        
```

Check Address

Clear

Close

You should see it routing to the new Remote MTA. We now need to Add the Remote Users to the White Pages Address Book for XUXA. We will use an Isode tool called “Sodium” for this.

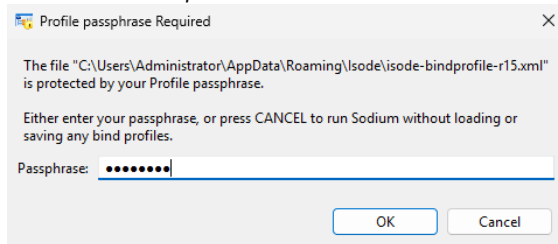
Adding Address Book Entries with Sodium

On Windows, start Sodium from the Windows Start Menu.

On Linux run the following command:

```
/opt/isode/bin/sodium
```

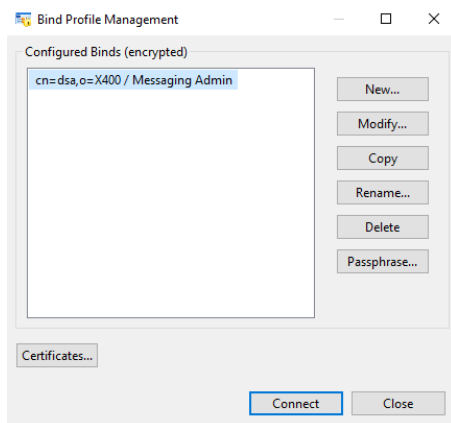
Enter Sodium Passphrase



Enter the Passphrase (same as for MConsole).

Click “OK”

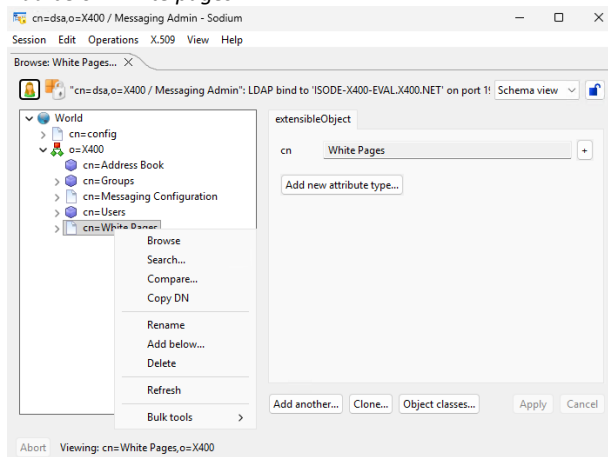
Connect Sodium to dsa



Click “Connect”

Expand the view from “World” until you reach “White Pages”, then right Click on “White Pages”.

Add below white pages



Select “Add below...”

Select person template

Click “Next >”

Select optional parts

Check “Organizational Person”, “Internet Organizational Person” and “X.400 Messaging”

Click “Next >”

Full name

Type “User One Internet”

Click “Finish”

Sodium Add below

cn=dsa,o=X400 / Messaging Admin - Sodium

Session Edit Operations X.509 View Help

Browse: White Pages...

cn=dsa,o=X400 / Messaging Admin: LDAP bind to 'ISODE-X400-EVAL.X400.NET' on port 19389

Template view

World

- cn=config
- o=X400
 - cn=Address Book
 - cn=Groups
 - cn=Messaging Configuration
 - cn=Users
 - cn=White Pages

Personal Group Contact Other Address Photo Employee **Messaging**

Full Name User One Internet

Surname Internet

User Password

Password < No value available > Set...

E-mail

User Certificate

Save... Save as PEM... Remove Load... Request... Import... Verify...

Add another... Clone... Object classes...

Add Cancel

Abort Adding: cn=User One Internet,cn=White Pages,o=X400

Add “Internet” for “Surname”

Select the “Messaging” tab

Messaging tab

cn=dsa,o=X400 / Messaging Admin - Sodium

Session Edit Operations X.509 View Help

Browse: White Pages...

cn=dsa,o=X400 / Messaging Admin: LDAP bind to 'ISODE-X400-EVAL.X400.NET' on port 19389

Template view

World

- cn=config
- o=X400
 - cn=Address Book
 - cn=Groups
 - cn=Messaging Configuration
 - cn=Users
 - cn=White Pages

Personal Group Contact Other Address Photo Employee **Messaging**

OR Addresses

Maximum Content Length

Message Store DN

Deliverable Content Types

Acceptable EITs

Exclusively Acceptable EITs

Unacceptable EITs

O/R Addresses with Capabilities

View Save... Delete...

Add another... Clone... Object classes...

Add Cancel

Abort Adding: cn=User One Internet,cn=White Pages,o=X400

Click “Edit” next to the OR Addresses.

Remote OR address

O/R Address Editor

Name Form Personal Name

Country Name GB Administrative Domain ISODE ☐ Space

Private Domain Internet Organization

Organizational Unit #1 Organizational Unit #2

Organizational Unit #3 Organizational Unit #4

Surname One Initials

Given Name User Generation Qualifier

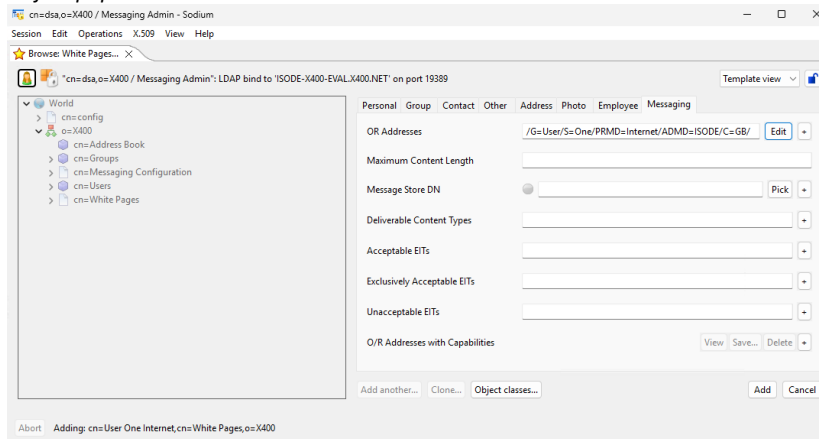
Domain-defined type =

Clear OK Cancel

Provide the remote OR Address

Click “OK”

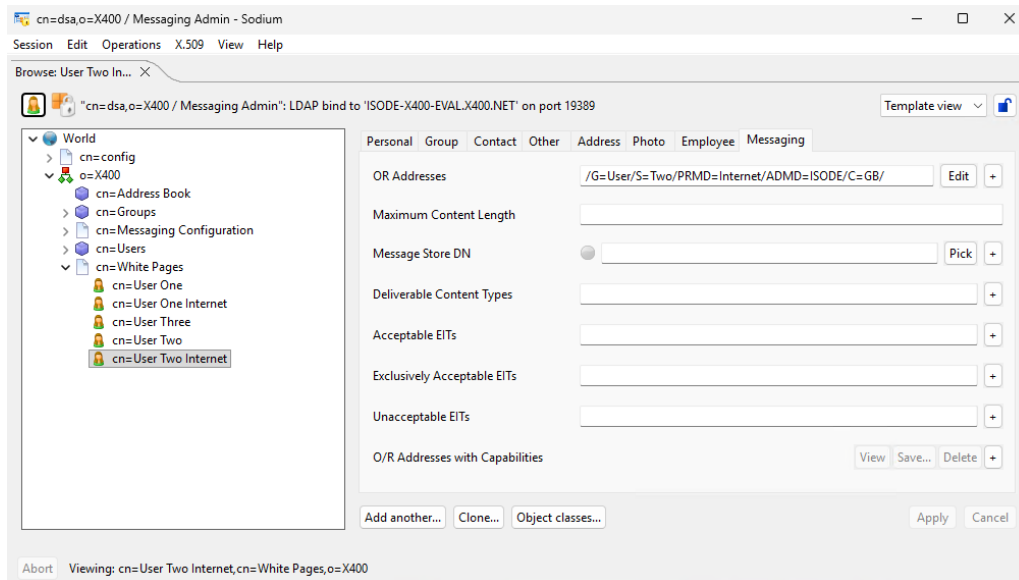
Object populated



Click “Add”

Repeat the process for “User Two Internet”

User Two Internet added



This completes adding the Address Book entries for XUXA.

Sending a Message to an External X.400 User with XUXA.

From XUXA Click the “Write” Icon.

Sending a message to a remote user

Click the “Address Book” Icon

XUXA address book

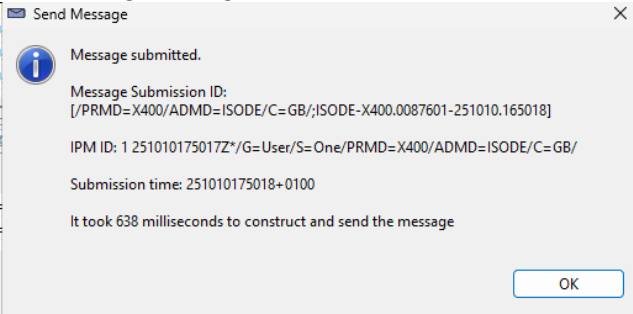
Select /G=User/S=One/PRMD=Internet/ADMD=ISODE/C=GB/

Click “OK”

XUXA populate message

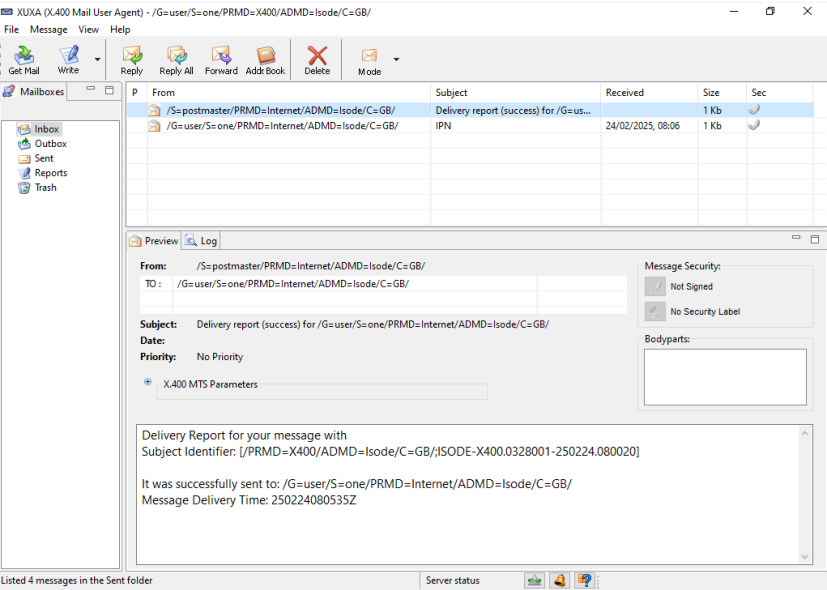
Enter a Subject and some text, then Click the “Send” Icon

XUXA Sending a Message to a Remote User



Click “OK”

XUXA Receive DR



You can see the successful Delivery Report above.

Prepare for 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. Strong authentication is not subject to export control. P7 and P3 strong authentication require 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 :

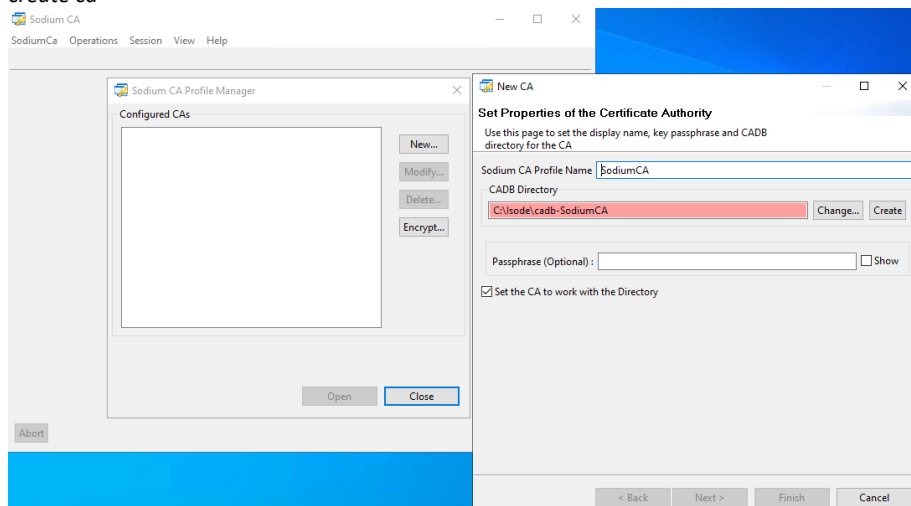
```
/opt/isode/sbin/sodiumca
```

Click "New"

On "Set Properties of the Certificate Authority" leave Defaults

Click "Create"

create ca



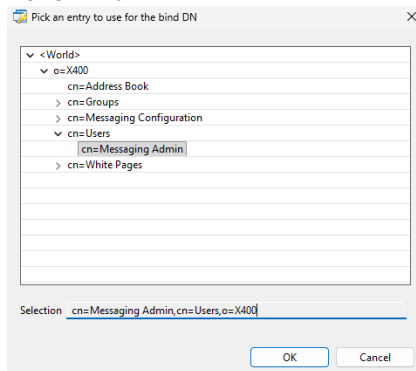
Click "Next >"

In "Hostname" type the fully qualified host name ("ISODE-X400-EVAL.X400.NET")

Click "Pick"

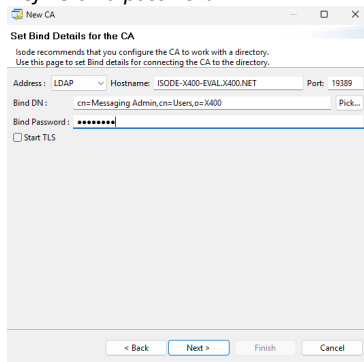
Browse to "cn=Messaging Admin,cn=Users,o=X400"

Pick CA Bind DN



Click “OK”

Define bind password



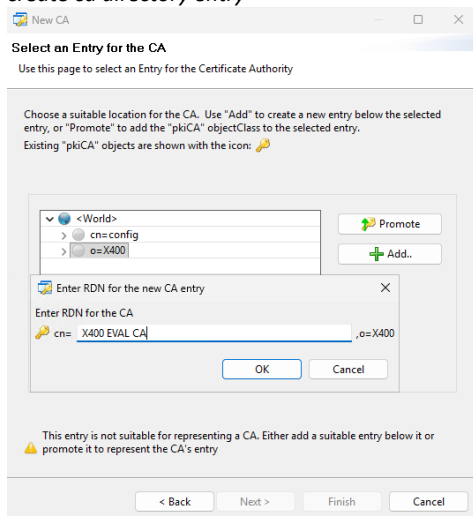
In “Bind Password” type “Secret1+”

Click “Next >”

On “Select an Entry for the CA” browse to and select “o=X400”

Click “Add”

create ca directory entry



On “Enter RDN for the new CA” type “X400 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”

open configured ca

Click “Open”

In “Enter Bind Password” type “Secret1+”

Click “OK”

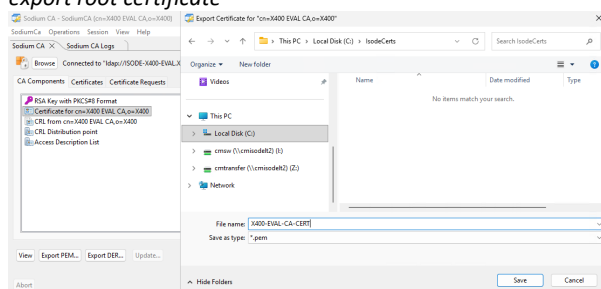
Select “Certificate for cn=X400 EVAL CA, o=X400”

Press “Export PEM ..”

On “Export Certificate for “cn=X400 EVAL CA, o=X400”, browse to “C:\IsodeCerts” (Linux : “/root/IsodeCerts”)

Change Filename to “X400-EVAL-CA-CERT.pem”

export root certificate

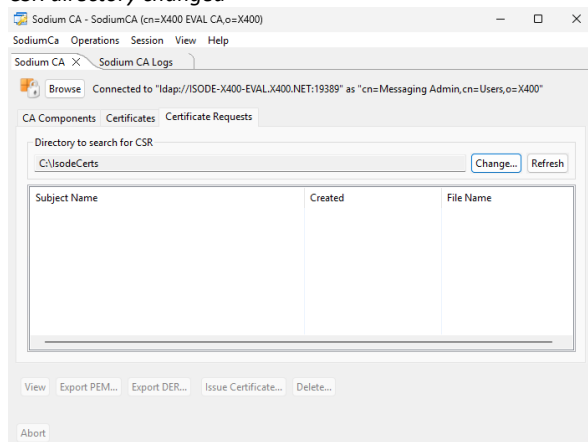


Press “Save”

On “Certificate for cn= X400 EVAL CA, o=X400” exported Click “OK”

Change to “Certificate Requests” tab

CSR directory changed



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

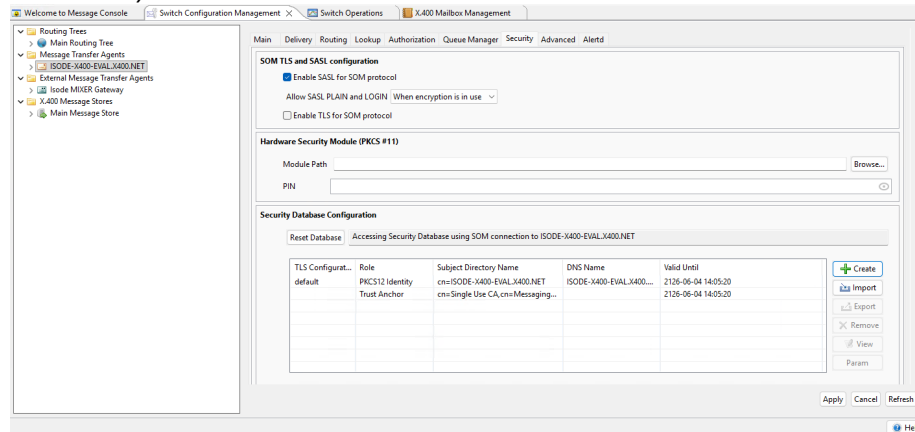
Populate the Security Database

Open Mconsole

Select the “Message transfer Agent” “ISODE-X400-EVAL.X400.NET”

Select the “Security” tab

Initial security database

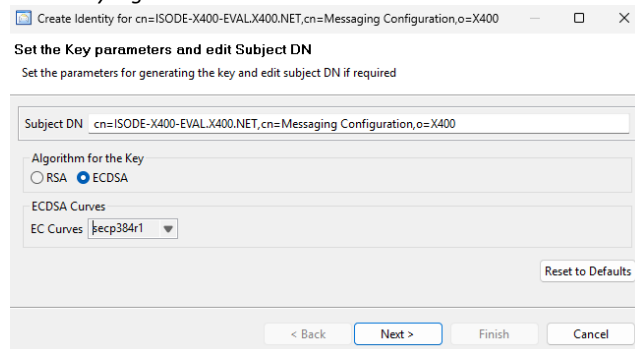


Note – the server has it's own self-signed certificate.

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”

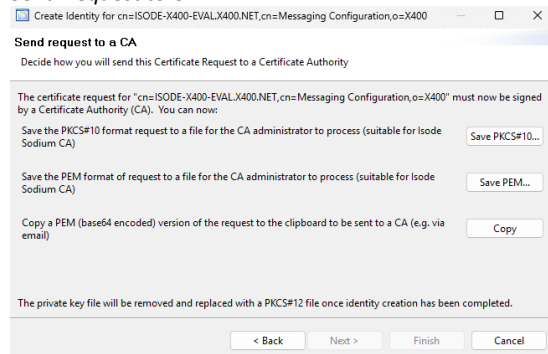
For “EC Curves” select “secp384r1”

Press “Next >”

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

On “Certificate Request Contents” Click “Next >”

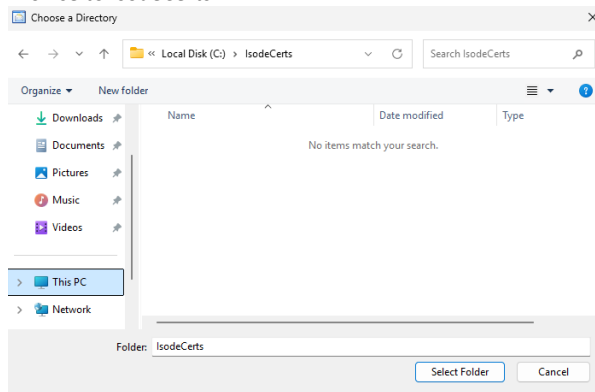
Send Request to CA



Press “Save PEM ...”

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

Browse to IsodeCerts



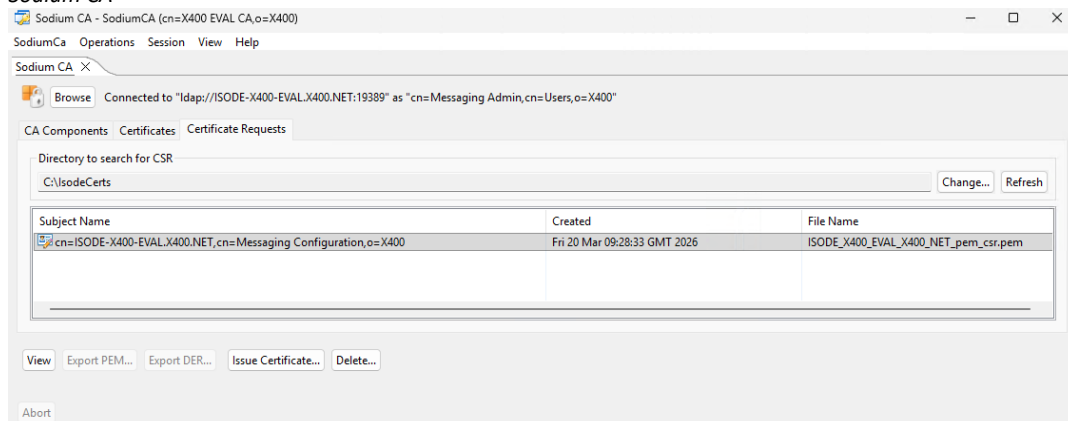
Press “Select Folder”

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

Set Validity and Signature Algorithm for the Certificate
Set the validity and Signature Algorithm for the Certificate and choose to delete the CSR

Valid From: 3 August 2026, 09:36 Edit...
Valid To: 3 August 2027, 09:36 Edit...
Lifetime
Years: 1 Months: 0 Days: 0 Hours: 0 Reset

Signature Algorithm: SHA384WITHRSA

☒ Delete the CSR after the Certificate generation

< Back Next > Finish Cancel

In the “Signature Algorithm” dropdown select “SHA384WITHRSA”

Click “Next >”

Generated Certificate

Generated Certificate
The following certificate will be generated.

| | |
|--------------------|---|
| Subject | cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configur |
| Issuer | cn=X400 EVAL CA,o=X400 |
| Valid from | Mon Aug 03 10:08:01 BST 2026 |
| Valid to | Tue Aug 03 10:08:01 BST 2027 |
| Serial | 41:EB:CD:68:53:5E:3F:B8:F0:1E |
| 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 “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

Create Identity for cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration,o=X400

Other certificates
Specify other certificates to be used for the trust chain

The identity must include a chain of certificates that contains at least one CA certificate. A complete chain includes all certificates from the end entity certificate to a self-signed CA certificate.
The wizard has found a self-signed CA certificate and so has a complete certificate chain for the new identity.

| Type | Certificate | Add certificate... |
|----------------|---|--------------------|
| End entity | cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration,o=X400 | |
| Self Signed CA | cn=X400 EVAL CA,o=X400 | |

Chain status: Certificate chain is complete

< Back Next > Finish Cancel

Press “Next >”

On “Save Identity information” Press “Finish”

Press “Apply”

New Certificate Created

Security Database Configuration

Reset Database Accessing Security Database using SOM connection to ISODE-X400-EVAL.X400.NET

| TLS Configur... | Role | Subject Directory Name | DNS Name | Valid Until | |
|-----------------|-----------------------|---|-------------------------------|---------------------|----------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET | ISODE-X400-EVAL.X400.NET | 2126-06-04 14:05:20 | + Create |
| | Trust Anchor | cn=Single Use CA,cn=Messaging Configuration,o=X400 | | 2126-06-04 14:05:20 | Import |
| | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration,o=X400 | ISODE-X400-EVAL.X400.NET/C... | 2035-06-22 12:48:24 | Export |
| | Certificate Authority | cn=X400 EVAL CA,o=X400 | | 2036-06-22 12:29:12 | Remove |
| | | | | | View |
| | | | | | Param |

Note the additional PKCS12 Identity and Certificate Authority.

Note that the “default” certificate is the one marked “default” in the “TLS Configuration” column.

Select the new certificate below that.

Certificate context menu

Security Database Configuration

Security Database Certificates

| TLS Configur... | Role | Subject Directory Name | DNS Name | Valid Until | |
|-----------------|-----------------|----------------------------------|--------------------------|---------------------|--|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET | ISODE-X400-EVAL.X400.... | 2126-03-20 09:21:54 | |
| | Trust Anchor | cn=Single Use CA,cn=Messaging... | | 2126-03-20 09:21:54 | |
| | PKCS12 Identity | cn=ISODE X400 EVAL X400 NET | ISODE-X400-EVAL.X400.... | 2035-03-20 09:30:19 | |
| | Certifica | | | 2036-03-17 17:20:41 | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Copy URI
Assign or update TLS Configuration

Right click

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

Change default certificate

Security Environment Access Method

Security DB / Legacy (file based): Security Database

Security Database Configuration

Security Database Certificates

| TLS Configurat... | Role | Subject Directory Name | DNS Name | Valid Until |
|-------------------|------------------------|----------------------------------|--------------------------|---------------------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET | ISODE-X400-EVAL.X400.... | 2126-03-20 09:21:54 |
| | Trust Anchor | cn=Single Use CA,cn=Messaging... | | 2126-03-20 09:21:54 |
| | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,c... | ISODE-X400-EVAL.X400.... | 2035-03-20 09:30:19 |
| | Certificate Authori... | cn=X400 EVAL CA,o=X400 | | 2036-03-17 17:20:41 |

TLS Configuration Name

TLS configuration name default

In “TLS Configuration Name” type “default”

Press “OK”

Default pending

Security Environment Access Method

Security DB / Legacy (file based): Security Database

Security Database Configuration

Security Database Certificates

| TLS Configurat... | Role | Subject Directory Name | DNS Name | Valid Until |
|-------------------|------------------------|----------------------------------|--------------------------|---------------------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET | ISODE-X400-EVAL.X400.... | 2126-03-20 09:21:54 |
| | Trust Anchor | cn=Single Use CA,cn=Messaging... | | 2126-03-20 09:21:54 |
| default(pending) | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,c... | ISODE-X400-EVAL.X400.... | 2035-03-20 09:30:19 |
| | Certificate Authori... | cn=X400 EVAL CA,o=X400 | | 2036-03-17 17:20:41 |

Press “Apply”

Select to delete

Security Environment Access Method

Security DB / Legacy (file based): Security Database

Security Database Configuration

Security Database Certificates

| TLS Configurat... | Role | Subject Directory Name | DNS Name | Valid Until |
|-------------------|------------------------|----------------------------------|--------------------------|---------------------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET | ISODE-X400-EVAL.X400.... | 2126-03-20 09:21:54 |
| | Trust Anchor | cn=Single Use CA,cn=Messaging... | | 2126-03-20 09:21:54 |
| | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,c... | ISODE-X400-EVAL.X400.... | 2035-03-20 09:30:19 |
| | Certificate Authori... | cn=X400 EVAL CA,o=X400 | | 2036-03-17 17:20:41 |

Select the previously “default” certificate.

Press “Remove”

Press “Apply”

Select the “Single use CA” trust anchor.

Press “Remove”

Press “Apply”

Self Signed certificates removed

Security Environment Access Method

Security DB / Legacy (file based): Security Database

Security Database Configuration

Security Database Certificates

| TLS Configurat... | Role | Subject Directory Name | DNS Name | Valid Until | |
|-------------------|---|--|--------------------------|--|--|
| default | PKCS12 Identity
Certificate Authori... | cn=ISODE-X400-EVAL-X400.NET,c...
cn=X400 EVAL CA,o=X400 | ISODE-X400-EVAL-X400.... | 2035-03-20 09:30:19
2036-03-17 17:20:41 | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

+ Create
 Import
 Export
 Remove
 View
 Param

Press “Import”

Import trust anchor

Import Certificate

Import Certificate(s)

Load a single TLS Identity or one or more Trust Anchors

Chose the type of certificate to import

☐ A TLS Identity (PKCS#12 file)
☐ A TLS Identity (Certificate for use with PKCS#11, in .crt format or .pem)
☒ Single Trust Anchor (.crt, .cer or .pem file)
☐ TLS configuration

< Back Next > Finish Cancel

Select “Single Trust Anchor”

Press “Next >”

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

Select root certificate

Open

This PC > Local Disk (C:) > IsodeCerts

Search IsodeCerts

| Name | Date modified | Type | Size |
|---|------------------|----------|------|
| ca_certificate.pem | 03/08/2026 09:41 | PEM File | |
| ISODE_X400_EVAL_X400_NET_pem_csr_cert_Chain.... | 03/08/2026 09:41 | PEM File | |
| X400-EVAL-CA-CERT.pem | 03/08/2026 09:26 | PEM File | |

File name: X400-EVAL-CA-CERT.pem *.pem

Open Cancel

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

Certificate parameters

Import Certificate

Certificate Parameters

Provide the parameters required for import

Trust anchor file path

C:\IsodeCerts\X400-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-X400-EVAL.X400.NET

| TLS Configuration | Role | Subject Directory Name | DNS Name | Valid Until |
|-------------------|-----------------|---|-------------------------------------|---------------------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration,o=X400 | ISODE-X400-EVAL.X400.NET/C=GB/AD... | 2027-08-03 09:36:36 |
| | Trust Anchor | cn=X400 EVAL CA,o=X400 | | 2036-08-03 09:18:39 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Configure and Test P1 Strong Authentication

Create Certificate for P1

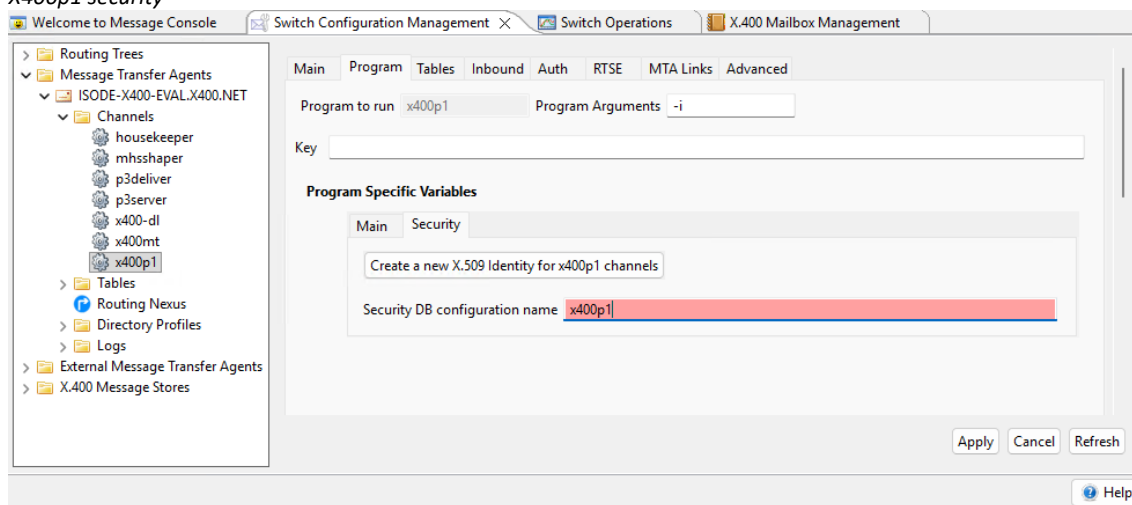
Expand channels in the left-hand pane and select “X4oop1”

Select the “Program” tab

Below that, select the “Security” tab

In “Security DB configuration name” type “x4oop1”

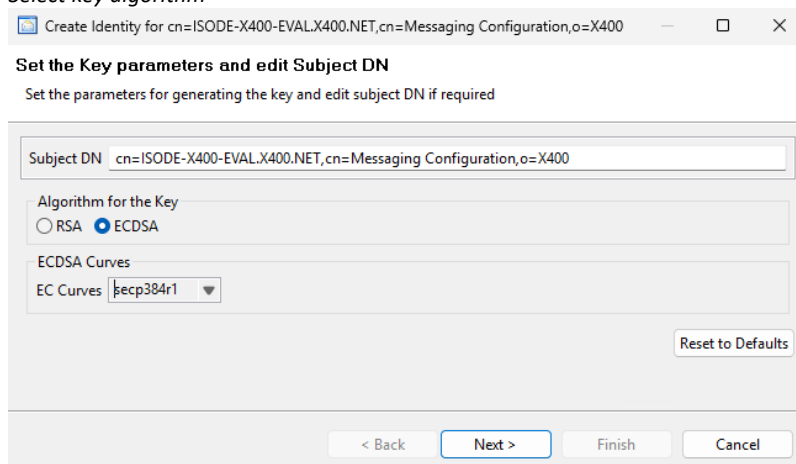
X400p1 security



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

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 ...”

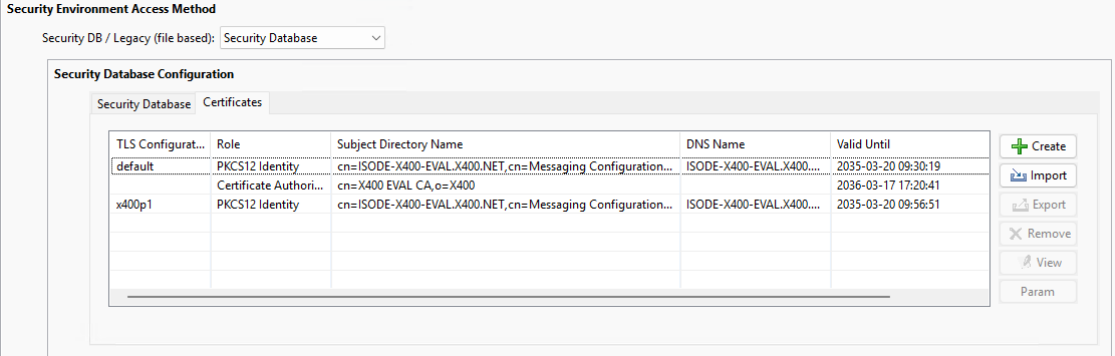
On “User Certificate” press “Next >”

On “Other Certificates” press “Next >”

On “Save Identity information” Press “Finish”

Press “Apply”

New x400p1 Certificate



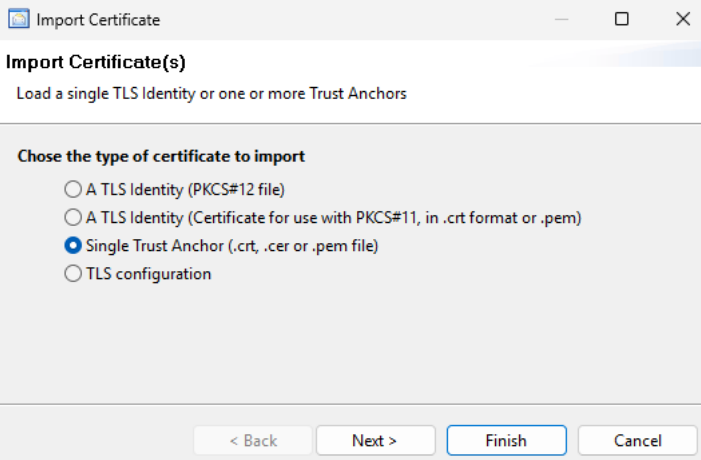
| TLS Configurat... | Role | Subject Directory Name | DNS Name | Valid Until |
|-------------------|------------------------|---|--------------------------|---------------------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration... | ISODE-X400-EVAL.X400.... | 2035-03-20 09:30:19 |
| | Certificate Authori... | cn=X400 EVAL CA,o=X400 | | 2036-03-17 17:20:41 |
| x400p1 | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration... | ISODE-X400-EVAL.X400.... | 2035-03-20 09:56:51 |

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

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

Click on “Import”

Import Trust Anchor



Import Certificate

Import Certificate(s)

Load a single TLS Identity or one or more Trust Anchors

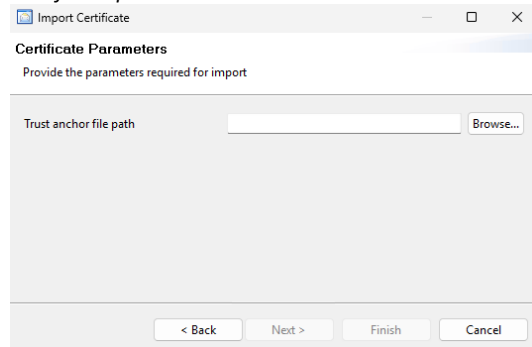
Choose the type of certificate to import

- ☐ A TLS Identity (PKCS#12 file)
- ☐ A TLS Identity (Certificate for use with PKCS#11, in .crt format or .pem)
- ☒ Single Trust Anchor (.crt, .cer or .pem file)
- ☐ TLS configuration

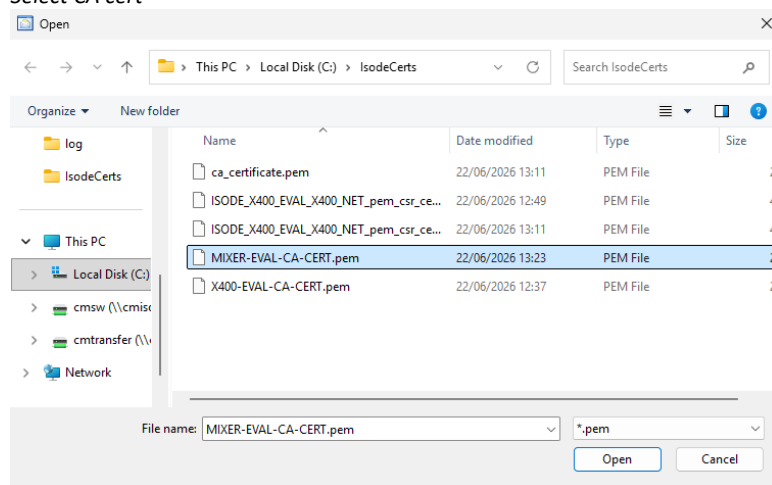
< Back Next > Finish Cancel

Select “Single Trust Anchor”

Press “Next >”

Certificate parameters

Press “Browse ..”

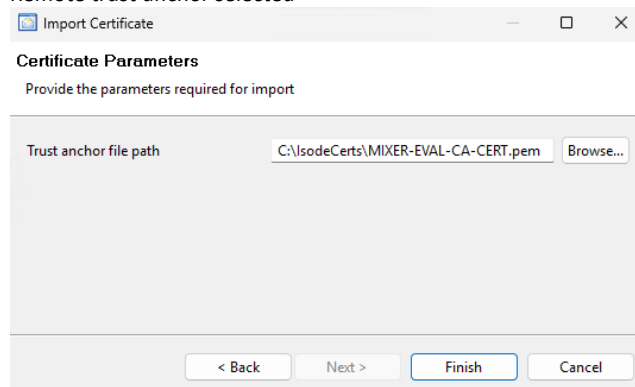
Select CA cert

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

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

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

Click “Open”

Remote trust anchor selected

Press “Finish”

Press “Apply”

Remote trust anchor Added

Security Database Configuration

Reset Database Accessing Security Database using SOM connection to ISODE-X400-EVAL.X400.NET

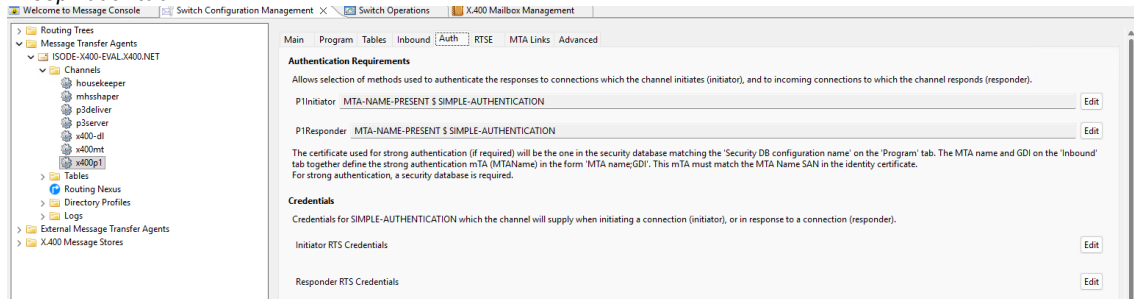
| TLS Configur... | Role | Subject Directory Name | DNS Name | Valid Until |
|-----------------|-----------------|----------------------------------|--------------------------|---------------------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,c... | ISODE-X400-EVAL.X400.... | 2027-08-03 09:36:36 |
| | Trust Anchor | cn=X400 EVAL CA,o=X400 | | 2036-08-03 09:18:39 |
| x400p1 | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,c... | ISODE-X400-EVAL.X400.... | 2027-08-03 10:08:01 |
| | Trust Anchor | cn=MIXER EVAL CA,o=MIXER | | 2036-07-15 15:17:54 |

Enable strong authentication for the local mta

Select the local x400p1 channel

Select the “Auth tab”

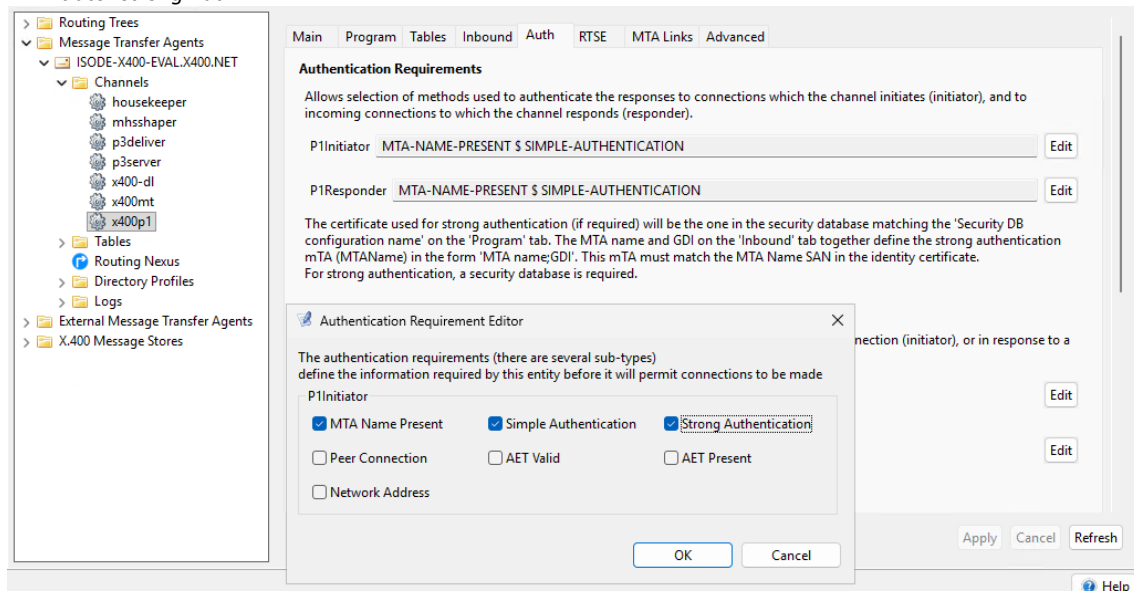
X400p1 auth tab



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

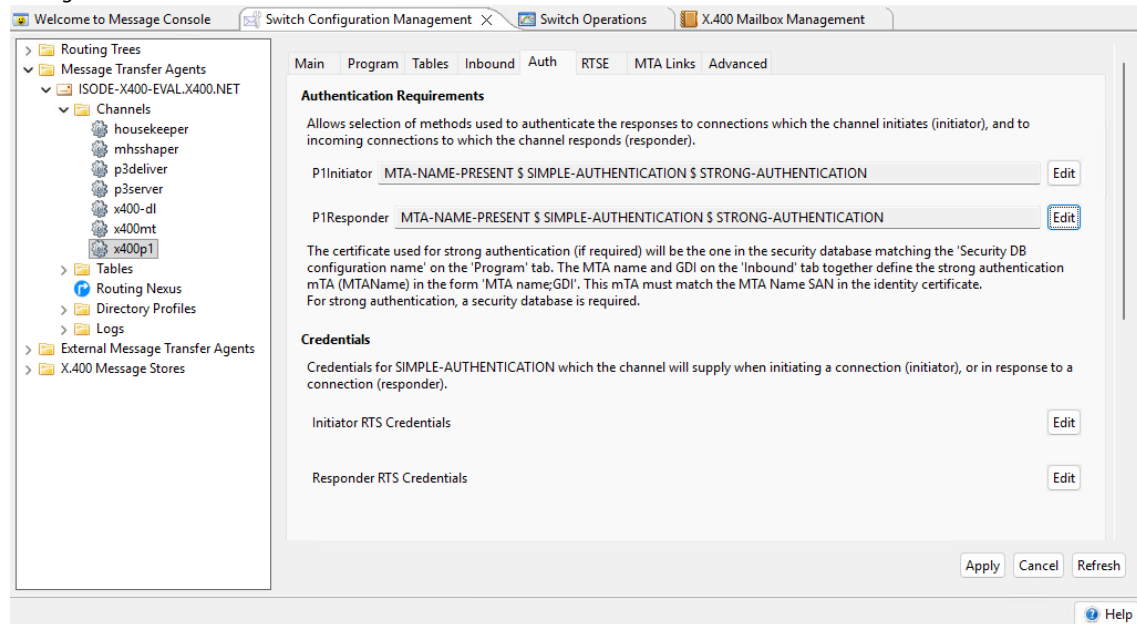
Select “Strong Authentication”

P1 initiator strong Auth



Press “OK”

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

Strong authentication enabled

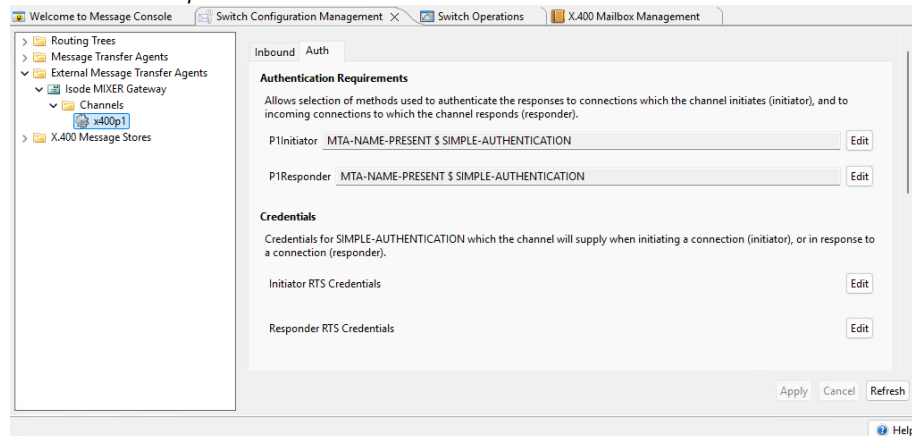
Press “Apply”

Enable strong authentication for the external mta

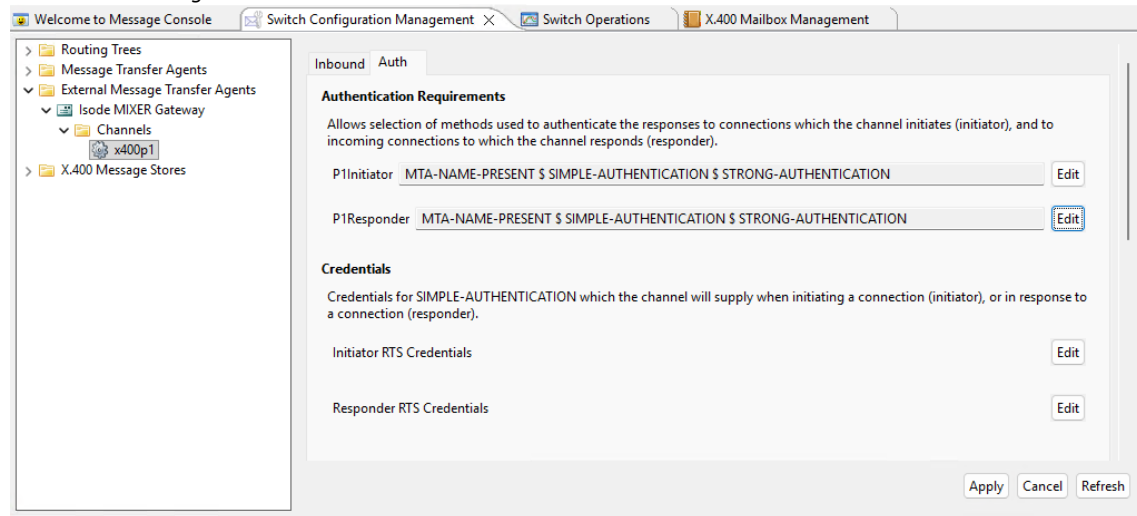
Expand the left-hand pane to the “External Message Transfer Agent” “Isode Mixer Gateway”

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”

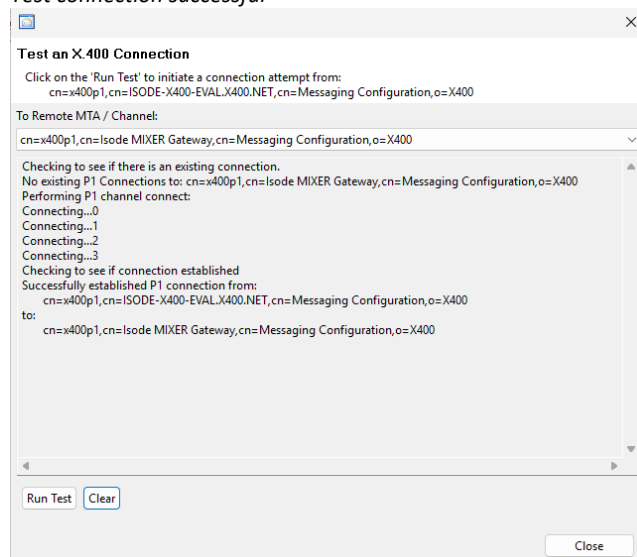
Test X400p1 Strong Auth connection

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

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

Select the remote mta “Isode Mixer Gateway”

Press “Run Test”

Test connection successful

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

```
2026-08-03 10:33:12 x400p1 08308 (#0 ) P1InitConnOK
chan:x400p1 theirmtaname:ISODE-MIXER-EVL.MIXER.NET
theirpa:"\"591\"/URI+0000+URL+itot://ISODE-MIXER-EVL.MIXER.NET"
ourmtaname:ISODE-X400-EVAL.X400.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-X400-EVAL.X400.NET,cn=Messaging
Configuration,o=X400" ourissuer:"cn=X400 EVAL CA,o=X400"
ourserial_num:090EE952E69FE7D43D6A theirissuer:"cn=MIXER EVAL
CA,o=MIXER" theirsubject:"cn=ISODE-MIXER-
EVL.MIXER.NET,cn=Messaging Configuration,o=MIXER"
theirserial_num:34EAF2D472D52E6838E1
oursangdi:/C=GB/ADMD=ISODE/PRMD=X400/ oursanmta:ISODE-X400-
EVAL.X400.NET theirsangdi:/C=GB/ADMD=ISODE/PRMD=MIXER/
theirsanmta:ISODE-MIXER-EVL.MIXER.NET tokenmta:ISODE-X400-
EVAL.X400.NET
```

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

Enable Mailboxes for Strong Authentication

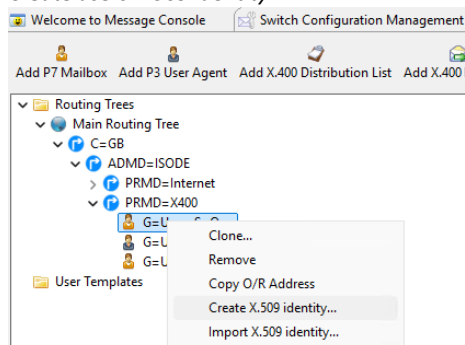
For P3 strong authentication, users must have their own associated certificate generated.

Create User Certificate

In the “X400 Mailbox Management” view, expand the routing tree to “User One”

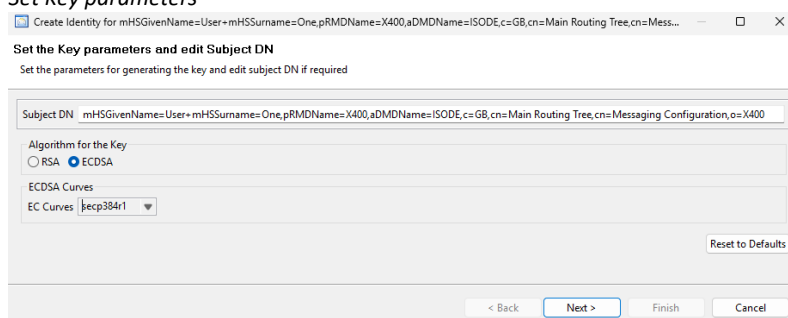
Right Click on User One

Create users X.509 identity



Choose the option “Create X.509 identity ...”

Set Key parameters

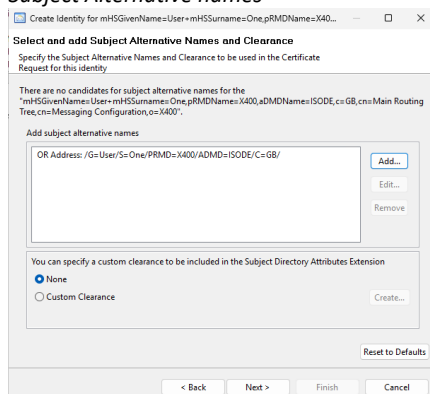


For algorithm select “ECDSA”

For “ECDSA Curves” select “secp384r1”

Click “Next >”

Subject Alternative names



Click “Next >”

Certificate request contents

Certificate Request Contents
Contents of this Certificate Request

The following Certificate Signing Request has been generated. In order to save this to a file or copy its contents, click Next. To change any options, click Back.

Subject: mHSGivenName=User+mHSSurname=One,pRMDName=X400,aDMDName=ISODE,c=GB,cn=Main Routing Tree,cn=Messaging Configuration,o=X400

PublicKeyInfo: Algorithm: ECDSA, KeySize: 384

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

Details

< Back Next > Finish Cancel

Click “Next >”

On “Send Request to a CA”, “Save PEM” to the folder “c:\IsodeCerts” (Linux : “/root/IsodeCerts”)

Click “Next >”

Return to Sodium CA:

Change to “Certificate Requests” Tab

Press “Refresh”

Ensure that the Certificate request is selected

Click “Issue Certificate...”

Certificate Signing Request

Certificate Signing Request
The following is the Certificate Request for which a Certificate will be issued

Subject: mHSGivenName=User+mHSSurname=One,pRMDName=X400,aDMDName=ISODE,c=GB,cn=Main Routing Tree,cn=Messaging Configuration,o=X400

PublicKeyInfo: Algorithm: ECDSA, KeySize: 384

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

Details

< Back Next > Finish Cancel

Click “Next >”

Select and add Subject Alternative Names

Select and add Subject Alternative Names
This page allows you to edit subject DN if required, select subject alternative names from the CSR and add new ones

Subject: mHSGivenName=User+mHSSurname=One,pRMDName=X400,aDMDName=ISODE,c=GB,cn=Main Routing Tree,cn=Messaging Configuration,o=X400

Following are the available subject alternative names:

- ☒ OR Address: /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/

Add other subject alternative names to appear in the certificate:

Add... Edit... Remove

< Back Next > Finish Cancel

Press “Next >”

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

Press “Next >”

Set signature algorithm

Set Validity and Signature Algorithm for the Certificate
Set the validity and Signature Algorithm for the Certificate and choose to delete the CSR

Valid From: 4 August 2026, 10:03 Edit...
Valid To: 4 August 2027, 10:03 Edit...
Lifetime
Years: 1 Months: 0 Days: 0 Hours: 0 Reset

Signature Algorithm: SHA384WITHRSA

☒ Delete the CSR after the Certificate generation

< Back Next > Finish Cancel

In the “Signature Algorithm” dropdown select “SHA384WITHRSA”

Click “Next >”

Generated Certificate

Generated Certificate
The following certificate will be generated.

| | |
|--------------------|--|
| Subject | mHSGivenName=User+ mHSSurname=One, pRMDName=X400, af |
| Issuer | cn=X400 EVAL CA, o=X400 |
| Valid from | Tue Aug 04 10:03:53 BST 2026 |
| Valid to | Sat Aug 04 10:03:53 BST 2035 |
| Serial | 31:B8:99:7D:42:33:43:1B:A2:B2 |
| PublicKeyInfo | Algorithm: ECDSA, KeySize: 384 |
| SignatureAlgorithm | SHA384WITHRSA |
| CertificateType | Version v3 (Not a CA Certificate) |

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 “Export to Disk” select “Write Certificate chain in PEM format”

Click “Finish”

On “CSR Signed” press “OK”

Back in Mconsole :

Select “The CA has provided a certificate”

Click “Next >”

On “User Certificate” click “Next >”

Other certificates

Create Identity for mHSGivenName=User+mHSSurname=One.pRMDName=X400.aDMDName=ISODE,c=GB.cn=Main Routing Tree.cn=Messaging Configuration,o=X400

Other certificates

Specify other certificates to be used for the trust chain

The identity must include a chain of certificates that contains at least one CA certificate. A complete chain includes all certificates from the end entity certificate to a self-signed CA certificate.
The wizard has found a self-signed CA certificate and so has a complete certificate chain for the new identity.

| | | |
|----------------|---|--------------------|
| Type | Certificate | Add certificate... |
| End entity | mHSGivenName=User+mHSSurname=One.pRMDName=X400.aDMDName=ISODE,c=GB.cn=Main Routing Tree.cn=M... | |
| Self Signed CA | cn=X400 EVAL CA,o=X400 | |

Chain status: Certificate chain is complete

< Back

Next >

Finish

Cancel

Click “Next >”

On “Save Identity information” leave the default “Save to Security Database”

Click “Finish”

Navigate to the Security database

Press “Refresh”

User certificate added

Security Database Configuration

Reset Database Accessing Security Database using SOM connection to ISODE-X400-EVAL.X400.NET

| TLS Configuration | Role | Subject Directory Name | DNS Name | Valid To | |
|--|-----------------|----------------------------------|---|----------|----------|
| default | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,c... | ISODE-X400-EVAL.X400.NET;/C=GB/ADMD=ISODE/PRMD=X... | 202 | + Create |
| | Trust Anchor | cn=X400 EVAL CA,o=X400 | | 203 | Import |
| x400p1 | PKCS12 Identity | cn=ISODE-X400-EVAL.X400.NET,c... | ISODE-X400-EVAL.X400.NET;/C=GB/ADMD=ISODE/PRMD=X... | 202 | Export |
| | Trust Anchor | cn=MIXER EVAL CA,o=MIXER | | 203 | Remove |
| | Unassigned | cn=ISODE-MIXER-EVL.MIXER.NE... | ISODE-MIXER-EVL.MIXER.NET;/C=GB/ADMD=ISODE/PRMD=... | 203 | |
| /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/ | PKCS12 Identity | mHSGivenName=User+mHSSurn... | /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/ | 203 | View |

Param

Note that a certificate has been added for the user.

Repeat the above steps to create a certificate in the Certificate database for User Two.

Configure and Test P₃ Strong Authentication Between MTA and Message Store

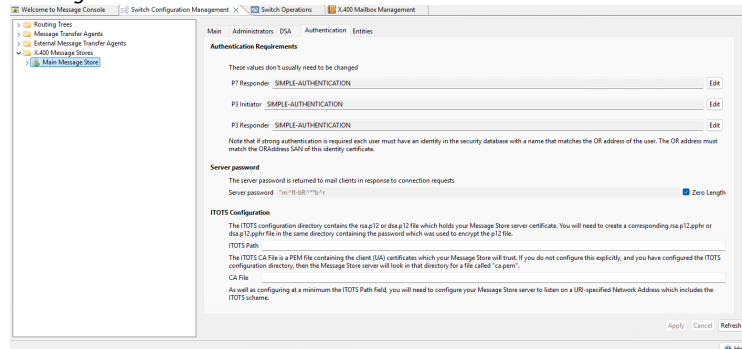
Messages are delivered from the MTA to M-Store using the P₃ protocol via the P₃ deliver channel. This transaction can be authenticated more securely in the following way :

To allow the Message store to respond to a strong bind request :

Select the “Main Message Store” in the Mconsole

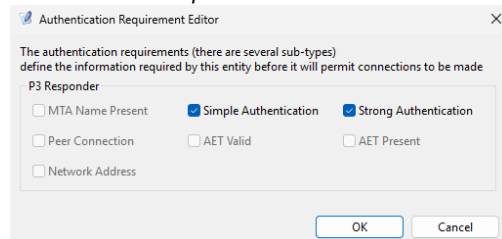
Then select the “Authentication” tab.

Message store Authentication tab



Press “Edit” to the right of “P₃ Responder”

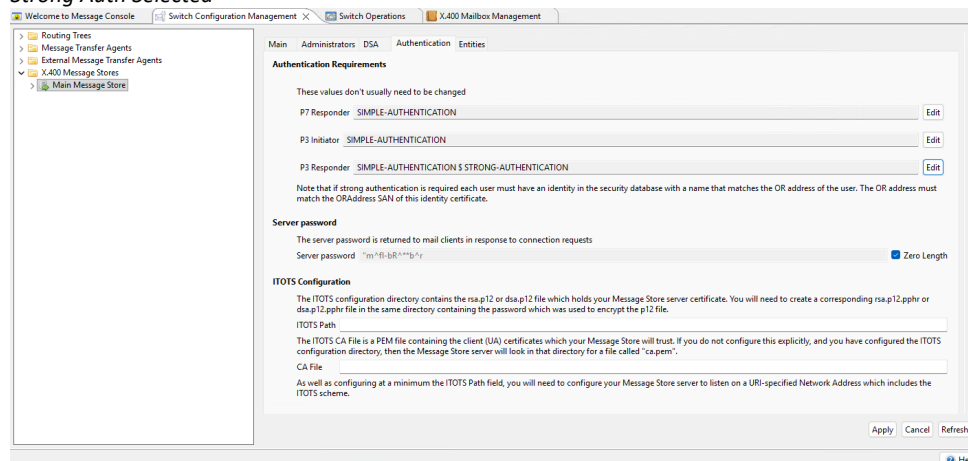
Authentication Requirements Editor



Check the “Strong Authentication” box

Press “OK”

Strong Auth Selected



Press “Apply”.

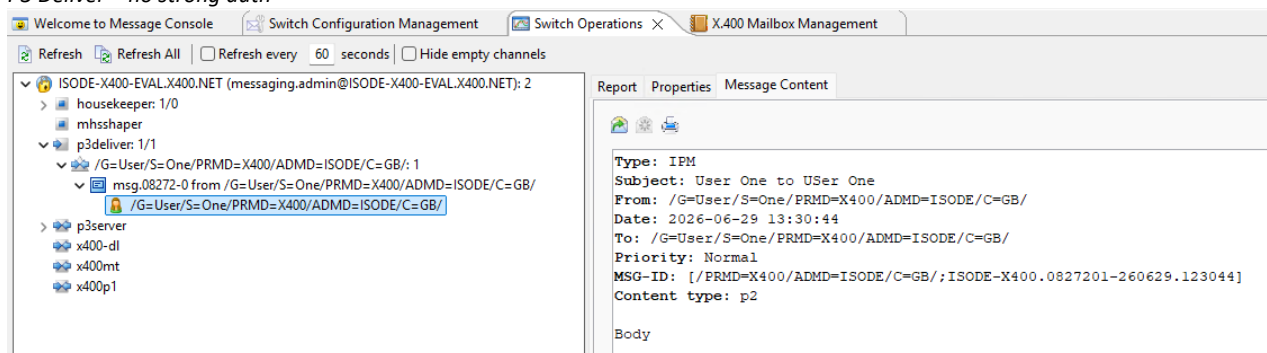
Note that the “Simple Authentication” and “Strong Authentication” options are mutually exclusive. Selection of “Strong” will override “Simple”

Repeat the above step to enable “Strong Authentication” for the “P3 Initiator”

Use Xuxa to send a message from user one to user one.

Note that the message is “Stuck” in the p3 deliver channel :

P3 Deliver – no strong auth



This logging sequence is shown in the mta-event log :

```

2026-08-04 11:01:20 p3delive 06532 (#0 ) E-MTA_X400-
InternalError Internal error, cannot load security info - invalid
identity 'p3deliver'
  
```

```

2026-08-04 11:01:20 p3delive 06532 (#0 ) F-MTA-ProcDying
Process dying on signal 11 ()
  
```

```

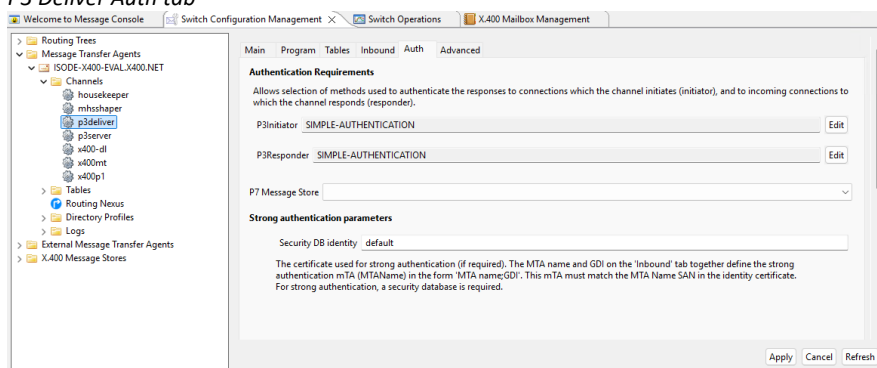
2026-08-04 11:01:21 pp.qmgr 05024 (#0 ) F-IOevent-IOerror
Error occurred on connection in rcv; System-WSAECONNRESET An
existing connection was forcibly closed by the remote host.
  
```

Expand to the p3 Deliver channel in Mconsole and select it

Select the “Auth” tab

We will use the default certificate already generated for the MTA.

P3 Deliver Auth tab

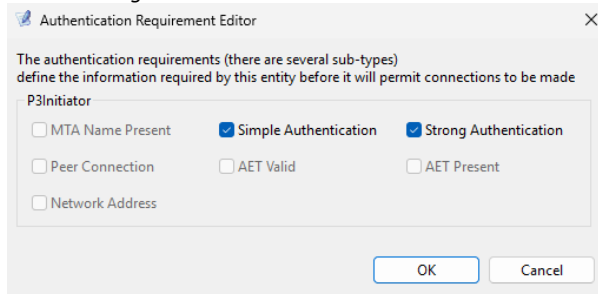


In “Security DB identity” type “default”

Press “Apply”

To the right of “P3 Initiator”, press “Edit”

Enable Strong authentication

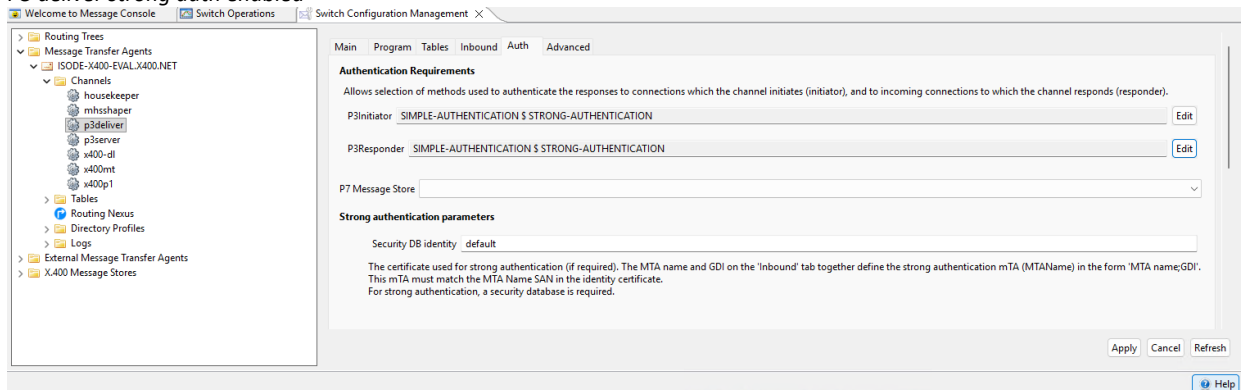


Check “Strong Authentication”

Press “OK”

Repeat the above step for the “P3 responder”

P3 deliver strong auth enabled

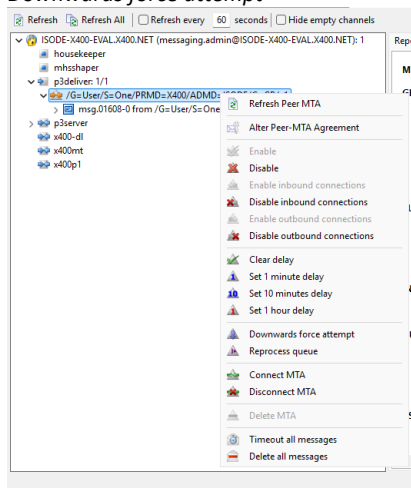


Press “Apply”

Note that the message will now be delivered.

It may be necessary to perform a “Downwards force attempt” in the “Switch Operations View” to trigger that to happen.

Downwards force attempt



Configure and Test Strong Authentication from Xuxa

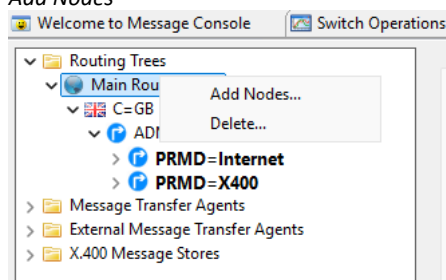
For this part of the guide we will use mailbox addresses that follow the addressing schemes of the aviation industry

Prepare the system

Extend the Switch Routing Tree for aviation mailboxes

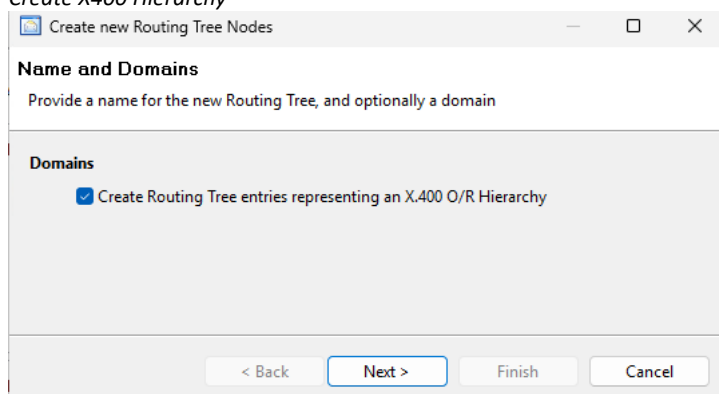
In Mconsole, select “Main Routing Tree”

Add Nodes



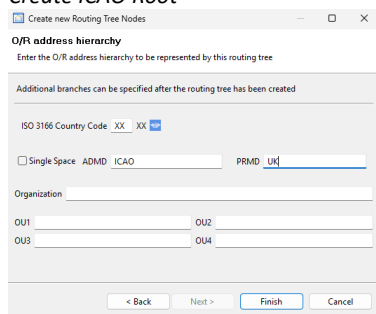
Select “Add Nodes ...”

Create X400 Hierarchy



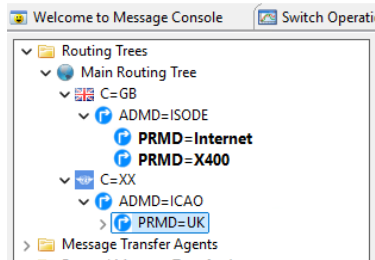
Press “Next >”

Create ICAO Root



Provide the node “C=XX, ADMD=ICAO;PRMD=UK”

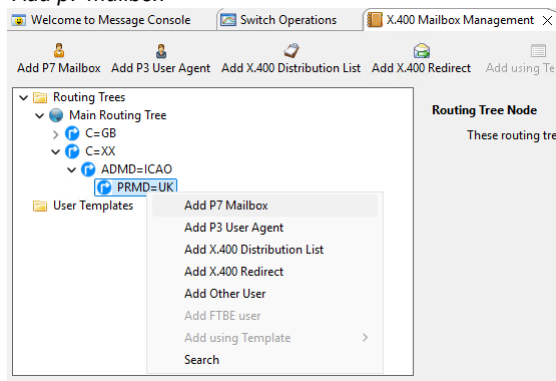
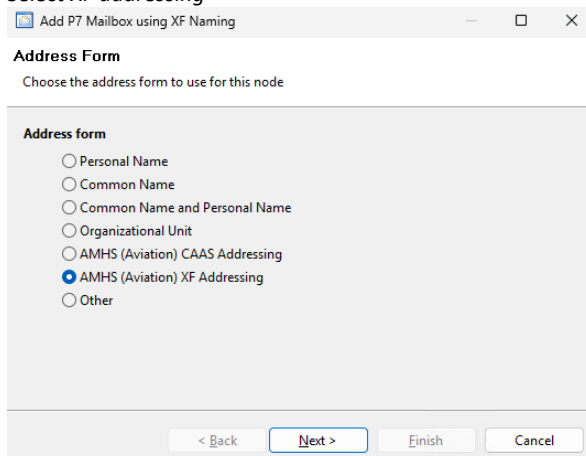
Press “Finish”

Tree created**Create an aviation P7 mailbox**

Go to the “X.400 Mailbox Management” view

Collapse and then expand the “Main Routing Tree” to make the new routing nodes appear

Create a new P7 mailbox under the node “C=XX, ADMD=ICAO, PRMD=UK”

Add p7 mailbox**Select “Add P7 Mailbox”***Select XF addressing***Select “AMHS (Aviation) XF Addressing”**

Press “Next >”

Name the mailbox

Provide the AFTN Address “EGTTZQZX”

Press “Next >”

Add white pages entry

Press “Next >”

Message Store Details

Press “Next >”

Passwords

Add P7 Mailbox using XF Naming

Passwords
Set the User's P7 and P3 passwords.
These are used for simple authentication.

P7 Message Store Password Secret1+ Hide

P3 Access Password Secret1+ Hide

< Back Next > Finish Cancel

Provide the mailbox password

Press “Finish”

Mailbox created

Welcome to Message Console **Switch Operations** **X.400 Mailbox Management**

Add P7 Mailbox Add P3 User Agent Add X.400 Distribution List Add X.400 Redirect Add using Ten

Routing Trees

- Main Routing Tree
 - C=GB
 - C=XX
 - ADMD=ICAO
 - PRMD=UK
 - O=AFTN
 - OU=EGTTZQZX

User Templates

Create an aviation P3 mailbox

Follow the above steps but press “Add P3 User Agent” instead of the “Add P7 Mailbox” button. Use the AFTN Address “EGTTZQTT”.

In this case, only a “Supporting MTA” will be required.

Define supporting MTA

Add P3 User Agent using Personal Name Naming

MTA Details
Configure which MTA this user will use

Supporting MTA

cn=ISODE-X400-EVAL.X400.NET,cn=Messaging Configuration,o=X400

< Back Next > Finish Cancel

Click “Next >”

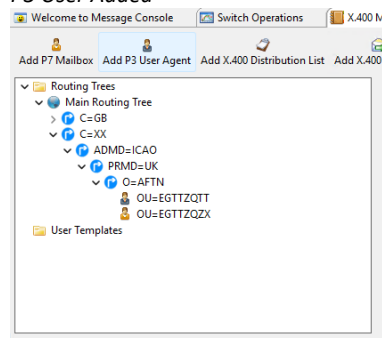
Provide password

Provide a password to authenticate to the P₃ channel

Select “Make this User Permanent”

Press “Finish”

P3 User Added



Create the M-Store Certificates

Follow the earlier section “Enable Mailboxes for Strong Authentication

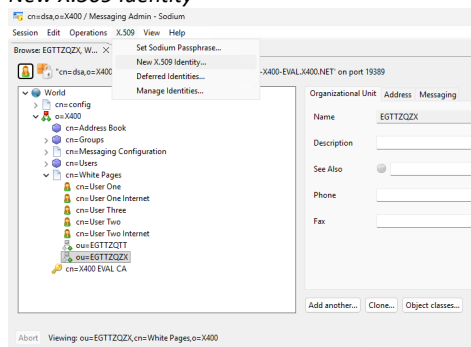
/Create User Certificate” to create a certificate for the mailbox “EGTTZQZX”

Create the PKCS₁₂ mailbox identities

Open Sodium

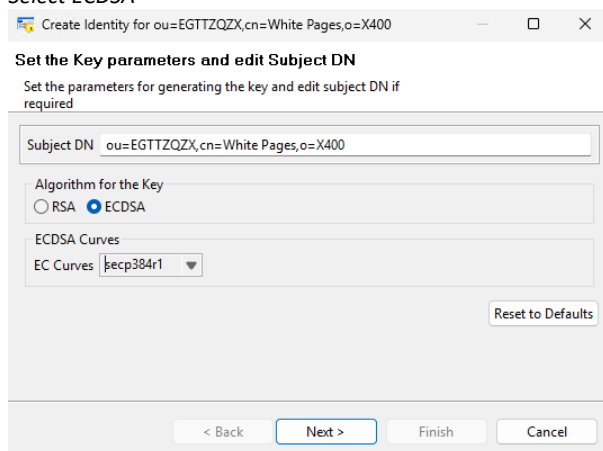
Browse to “EGTTZQZX” under “White Pages”

New X.509 Identity



From the top menu select “X.509/New X.509 Identity ...”

Select ECDSA

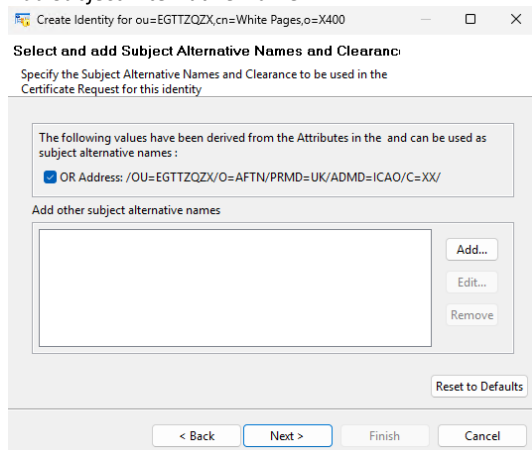


Select Algorithm “ECDSA”

Select EC Curve “secp384r1”

Click “Next >”

Add Subject Alternative Name



Check the box next to “O/R address:”

Press “Next >”

Certificate Request Contents

Press “Next >”

On “send Request to a CA” press “Save PEM”

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

Press “Next >”

Use Sodium CA to Issue the certificate.

Remember to select the “Signature Algorithm” SHA384WITHECDSA which is mandated by the ICAO.

Signature Algorithm

Back in Mconsole :

Select “The CA has provided a certificate”

Press “Next >”

On “User Certificate” press “Next >”

On “Other certificates” press “Next >”

Select a different user

Check “a different user ..”

Press “Next >”

Create PKCS12 file

For “Output Directory” browse to “C:\IsodeCerts” (Linux : “/root/IsodeCerts”)

In “Passphrase” provide a password

Press “Next >”

Save Identity information

Press “Finish”

On “Identity File Written” press “OK”

Repeat the above steps to create a PKCS#12 file containing certificates and private key for “EGTTZQTT”.

Configure and test xuxa P7 Strong Authentication

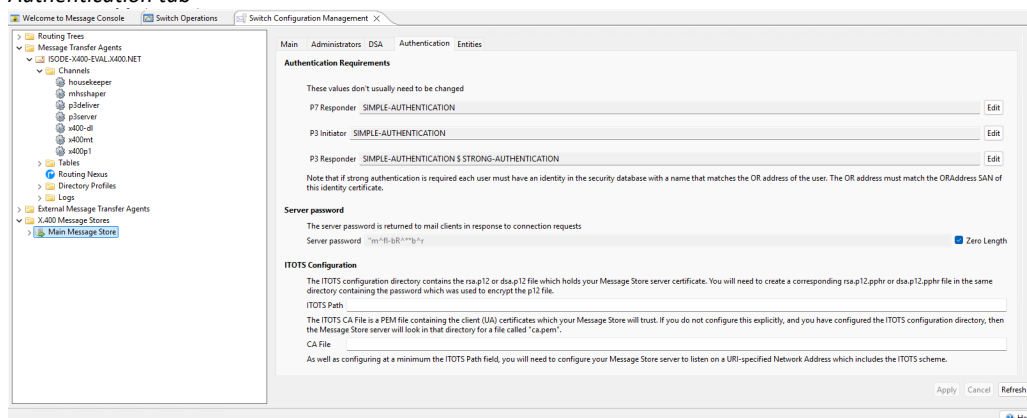
Configure M-Store for Strong P7 Authentication

Change to the “Switch Configuration Management” view

In the left-hand pane, select “Main Message Store”

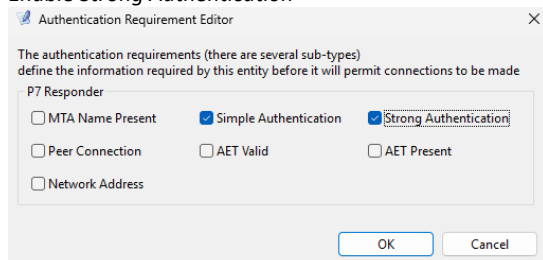
Select the “Authentication” tab

Authentication tab



To the right of “P7 Responder” press “Edit”

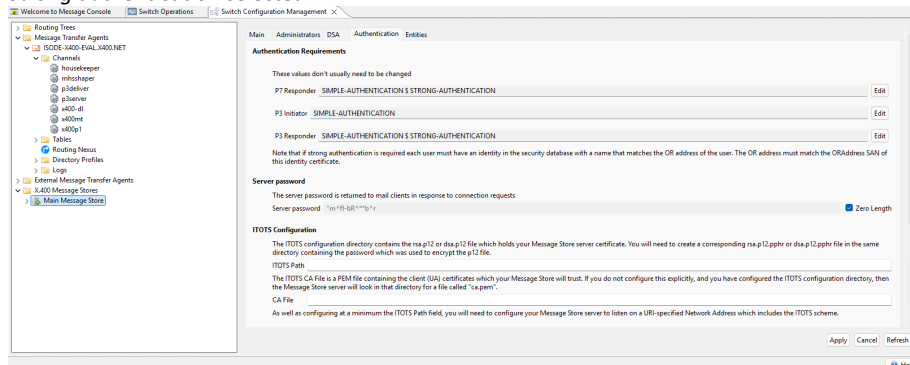
Enable Strong Authentication



Check “Strong Authentication”

Press “OK”

Strong authentication selected



Press “Apply”

Configure xuxa profile for P7 Strong Authentication

Create a P7 xuxa profile for “EGTTZQZX” by following the steps earlier in the document.

Xuxa P7 Configuration

P7 Message Store

Connection Information
 Message Store Presentation Address: "3001"/URI=0000+URL=not/ISODE-X400-EVALX400.NET:3001
 Message Store User (O/R): /OU=EGTTZQZX/O=AFTN/PRMD=UK/ADMD=ICAO/C=XX/ Edit
 Message Store User Password: Secret1+
 Message Store User DN: ou=EGTTZQZX, cn=White Pages, ou=X400 Pick
 Bind to the Message Store Search

X.400 P7 Bind Authentication Level
☒ Simple Authentication ☐ Strong Authentication

☐ Check for messages at startup
☐ Disable configuration requests in bind operations
☐ Use a new connection for each message submission
☐ Use a new MS connection for Get Mail
☐ Don't confirm message deletion
☐ Register an autoalert for new messages
☐ Pop up an alert window when an autoalert is received

☐ Automatically check for new every check period (Below)
 Check period (in seconds) 0

The messages will be fetched
☒ at startup time ☐ on demand
 Maximum mailbox size 0

Restore Defaults Apply
 Apply and Close Cancel

Use the O/R address : “/OU=EGTTZQZX/O=AFTN/PRMD=UK/ADMD=ICAO/C=XX/”

Select “Security”

Xuxa Security

Security

PKCS#12 File Name: C:\IsodeCerts\EGTTZQZX.p12 Browse...
 PKCS#12 certificate password: Secret1+
 Trusted CA Certificate directory: C:\IsodeCerts Browse...

MTA Name:
 Global Domain Identifier:

Default Security settings when composing a message
☒ Unsigned ☐ Signed With Moac ☐ Signed With Message Token
☐ Signed With Both ☐ Signed Extended ATS

Restore Defaults Apply
 Apply and Close Cancel

For “PKCS#12 File Name” browse to “c:\IsodeCerts\EGTTZQZX.p12” (Linux : “/root/IsodeCerts/EGTTZQZX.p12”)

Provide the PKCS#12 password

For “Trusted CA Certificate directory” browse to “C:\IsodeCerts” (Linux : “/root/IsodeCerts/”)

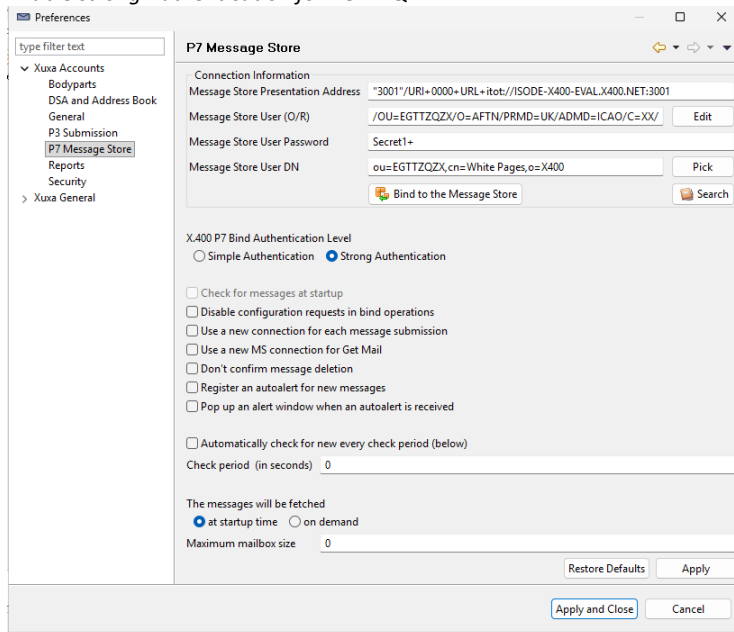
Press “Apply and Close”

Test the profile by sending yourself a message.

Go back to the xuxa mailbox configuration

Select “P7 Message Store”

Enable strong Authentication for EGTZQZX



Select “Strong Authentication”

Press “Apply and Close”

It is advisable to check that this configuration change has been made. If not, try again.

To test, send a message from EGTZQZX to EGTZQZX

It's possible to check that a strong authentication occurred by finding these entries in the mta-event log:

```
2026-08-04 12:30:29 pumice 04584 (#0 ) N-Dsap-Notice
Strong credentials presented

2026-08-04 12:30:29 pumice 04584 (#0 ) N-Dsap-Notice P7
strong credentials accepted
```

Note that the public certificate provided during the bind is cached in the Security database :

Cached Public Certificate

| Security Database Configuration | | | | |
|--|-----------------|--|-------------------------|---------------------|
| Reset Database Accessing Security Database using SOM connection to ISODE-X400-EVAL.X400.NET | | | | |
| TLS Configuration | Role | Subject Directory Name | DNS Name | Valid Until |
| | Trust Anchor | cn=MIXER EVAL CA,o=MIXER | | 2036-07-15 15:17:54 |
| | Unassigned | cn=ISODE-MIXER-EVL.MIXER.NET,cn=Messagi... | ISODE-MIXER-EVL.MIXE... | 2035-07-15 15:28:13 |
| /G=User/S=One/PRMD=X400/AD... | PKCS12 Identity | mHSGivenName=User+mHSSurname= One,pR... | /G=User/S=One/PRMD... | 2035-08-04 10:03:53 |
| /G=User/S=Two/PRMD=X400/AD... | PKCS12 Identity | mHSGivenName=User+mHSSurname= Two,pR... | /G=User/S=Two/PRMD... | 2035-08-04 10:16:02 |
| /OU=EGTTZQZX/O=AFTN/PRMD=... | PKCS12 Identity | mHSOrganizationalUnitName=EGTTZQZX,mH... | /OU=EGTTZQZX/O=AF... | 2035-08-04 12:17:07 |
| | Unassigned | ou=EGTTZQZX,cn=White Pages,o=X400 | /OU=EGTTZQZX/O=AF... | 2035-08-04 11:51:41 |

Configure and test xuxa P3 Strong Authentication

Configure the P3 server channel

For convenience we will use the previously generated default certificate.

In Mconsole, expand the local MTA and select the “P3 server” channel

Select the “Auth” tab

In “Security DB Identity” type “default”

Press “Edit” to the right of “P3Initiator”

Select “Strong Authentication”

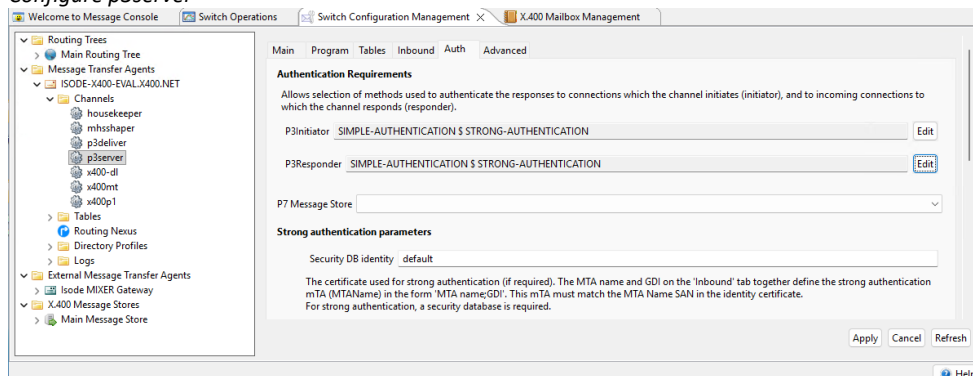
Press “OK”

Press “Edit” to the right of “P3Responder”

Select “Strong Authentication”

Press “OK”

Configure p3server



Press “Apply”

Configure xuxa profile for P3 Strong Authentication

Create a P3 xuxa profile for “EGTTZQTT” by following the steps earlier in the document.

Xuxa P3 Configuration

P3 Submission

P3 Channel Presentation Address: "593"/URI+0000+URL+itot//ISODE-X400-EVAL.X400.NET

P3 User O/R address: /OU=EGTTZQTT/O=AFTN/PRMD=UK/ADMD=ICAO/C=XX/

P3 User Password: Secret1+

X.400 P3 Bind Authentication Level: ☒ Simple Authentication ☐ Strong Authentication

☒ Force sending using P3, instead of via the P7 Message Store

P3 Delivery

If you want to read messages queued on the MTA's P3 channel for this user then unset the values in the user parameters in the P7 Message Store tab. If no P7 user values are found, the P3 Submission information will be used instead.

NOTE: Receiving messages via P3 (delivery) requires the routing in the MTA to be correctly set, in particular the PP Channel of the user should be p3server, not p3deliver

Buttons: Restore Defaults, Apply, Apply and Close, Cancel

Use the O/R address : “/OU=EGTTZQTT/O=AFTN/PRMD=UK/ADMD=ICAO/C=XX/”

Select “Security”

Xuxa P3 Security

Security

PKCS#12 File Name: C:\IsodeCerts\EGTTZQTT.p12

PKCS#12 certificate password: Secret1+

Trusted CA Certificate directory: C:\IsodeCerts

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

Global Domain Identifier: /C=GB/ADMD=ISODE/PRMD=X400/

Default Security settings when composing a message: ☒ Unsigned ☐ Signed With Moac ☐ Signed With Message Token ☐ Signed With Both ☐ Signed Extended ATS

Buttons: Restore Defaults, Apply, Apply and Close, Cancel

For “PKCS#12 File Name” browse to c:\IsodeCerts\EGTTZQTT.p12 (Linux : “/root/IsodeCerts/EGTTZQTT.p12”)

Provide the PKCS#12 password

For “Trusted CA Certificate directory” browse to “C:\IsodeCerts” (Linux : “/root/IsodeCerts/”)

In “MTA Name” type “ISODE-X400-EVAL.X400.NET”

In “Global Domain Identifier” type “/C=GB/ADMD=ISODE/PRMD=X400/”

Press “Apply and Close”

Test the profile by sending yourself a message.

Go back to the xuxa mailbox configuration

Select “P3 Submission”

Enable strong Authentication for EGTZQT

P3 Submission

P3 Channel Presentation Address: *593*/URI=0000+URL+Rtc//ISODE-X400-EVAL

P3 User O/R address: /OU=EGTTZQT/O=AFTN/PRMD=UK/ADMD=ICAO/C=XX

P3 User Password: Secret1+

X400 P3 Bind Authentication Level
☐ Simple Authentication ☒ Strong Authentication

☒ Force sending using P3, instead of via the P7 Message Store

P3 Delivery

If you want to read messages queued on the MTA's P3 channel for this user then unset the values in the user parameters in the P7 Message Store tab. If no P7 user values are found, the P3 Submission information will be used instead.

NOTE: Receiving messages via P3 (delivery) requires the routing in the MTA to be correctly set, in particular the PP Channel of the user should be p3server, not p3deliver

Select “Strong Authentication”

Press “Apply and Close”

It is advisable to check that this configuration change has been made. If not, try again.

To test, send a message from EGTZQZZ to EGTZQZZ

It's possible to check that a strong authentication occurred by finding these entries in the mta-event log:

```
2026-08-04 13:25:23 p3server 05528 (#0 ) N-Dsap-Notice
Received P3 strong authentication credentials
2026-08-04 13:25:23 p3server 05528 (#0 ) N-Dsap-Notice
Validating P3 strong authentication credentials
2026-08-04 13:25:23 p3server 05528 (#0 ) N-Dsap-Notice calling
P3 UA->MTA strong auth validation callback
2026-08-04 13:25:23 p3server 05528 (#0 ) N-Dsap-Notice
validate_credentials: done (SUCCESS)
```

Note that the public certificate provided during the bind is cached in the Security database :

Cached Public Certificate

| Security Database Configuration | | | | |
|---|-----------------|--------------------------------|--|--------------------|
| Reset Database Accessing Security Database using SOM connection to ISODE-X400-EVAL.X400.NET | | | | |
| TLS Configuration | Role | Subject Directory Name | DNS Name | Valid Until |
| /G=User/S=One/PRMD=X... | Unassigned | cn=ISODE-MIXER-EVL.MIXER.NE... | ISODE-MIXER-EVL.MIXER.NET;/C=GB/ADMD=ISODE/... | 2035-07-15 15:28:1 |
| /G=User/S=Two/PRMD=X... | PKCS12 Identity | mHSGivenName=User+mHSSurn... | /G=User/S=One/PRMD=X400/ADMD=ISODE/C=GB/ | 2035-08-04 10:03:5 |
| /OU=EGTTZQZX/O=AFTN... | PKCS12 Identity | mHSGivenName=User+mHSSurn... | /G=User/S=Two/PRMD=X400/ADMD=ISODE/C=GB/ | 2035-08-04 10:16:0 |
| | Unassigned | mHSOrganizationalUnitName=E... | /OU=EGTTZQZX/O=AFTN/PRMD=UK/ADMD=ICAO/... | 2035-08-04 12:17:0 |
| | Unassigned | ou=EGTTZQZX,cn=White Pages,... | /OU=EGTTZQZX/O=AFTN/PRMD=UK/ADMD=ICAO/... | 2035-08-04 11:51:4 |
| | Unassigned | ou=EGTTZQT,cn=White Pages,... | /OU=EGTTZQT/O=AFTN/PRMD=UK/ADMD=ICAO/... | 2035-08-04 11:56:3 |

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.