

## R19.0 M-Switch User Server Evaluation Guide

How to create an M-Switch User Server Military Messaging System.

## Contents

Introduction.....	3
Objectives.....	4
Recipient Configuration Matrix.....	5
Environment Overview.....	7
Using Isode Support.....	8
Preparing the Server Environment.....	9
Naming the Server.....	9
Install the Isode Software.....	9
Activating the Isode Products.....	10
Building the Core Messaging System.....	14
Create the DSA.....	15
Create the Messaging Configuration.....	17
Configure the Switch Operations View.....	24
Configure the switch to allow connections from Harrier.....	26
Modify the MTA Name for P1 Connections.....	26
Configure the External Connections to “headquarters.net”.....	29
Configure an appropriate Stanag 5066 Server.....	29
Configure the ACP127 Channel.....	29
Configure a channel for mmhs ACP142/Stanag4406 traffic.....	31
Configure the ACP142/mule Channel for internet smtp traffic.....	33
Configure the External ACP127 Station.....	36
Configure the External ACP142 MTAs.....	40
Configure the external ACP142/S4406 MTA.....	40
Configure the External ACP142/Mule MTA.....	42
Complete the Service Configuration.....	46
Configure the Routing Nexus.....	48
Configure the Address Routing.....	52
Reload Configuration.....	55
Populate Recipient Information.....	56
Create an Isode PKI.....	56
Configure M-Vault to Support TLS.....	59
Initial Cobalt Configuration.....	63
Define Cobalt Domains and Features.....	66
Configure the local mailboxes and remote users.....	70
Configure a Profiler Rule.....	78
Configure the Profiler Channel.....	82
Test Message Routing.....	83
Test Profiler.....	84

## Introduction

This guide details the process for creating a “Mobile” Military Messaging System using Isode’s M-Switch User Server product. M-Switch User Server is one of a family of email messaging products which comprises:

- M-Switch SMTP (SMTP Message Transfer Agent)
- M-Box (POP/IMAP Message Store)
- M-Switch X.400 (X.400 Message Transfer Agent)
- M-Store (X.400 Message Store)
- M-Switch MIXER (message gateway providing conversion between X.400 and Internet email according to the MIXER specifications)
- M-Switch Gateway (Email Messaging for low-bandwidth and/or high-latency networks)
- Harrier (web based email client)

M-Switch products are widely deployed in the Government, Military, Intelligence, Civil Aviation and EDI markets.

---

*Use of TLS: Due to UK Export Controls we are unable to provide Evaluation Activations that support TLS to certain geographic regions. This guide is written with the assumption that the reader is not a member of those regions and by default, we will provide a product activation that supports TLS. For customers whose region we have no current export control arrangement, further configuration information may be required and provided separately.*

---

## Objectives

By the end of this guide you will have:

1. Created a new “Military Messaging System” for the military domain “mmhs.field.net” and internet mail domain “field.net” with support for ACP<sub>127</sub>, ACP<sub>142</sub>/S<sub>4406</sub> and ACP<sub>142</sub>/mule.
2. Added local “field.net” and “mmhs.field.net” users with mappings to ACP<sub>127</sub> and S<sub>4406</sub> using Cobalt.
3. Created an External ACP<sub>127</sub> Station.
4. Created an External ACP<sub>142</sub> S<sub>4406</sub> Annex E MTA for Military traffic
5. Created an External ACP<sub>142</sub> S<sub>4406</sub> Mule MTA for internet traffic
6. Created a “Routing Nexus” for the remote domains “headquarters.net” and “mmhs.headquarters.net”
7. Added remote “headquarters.net” and “mmhs.headquarters.net” users and roles with mappings to ACP<sub>127</sub> and S<sub>4406</sub> using Cobalt.
8. Been introduced to a tool to check the routing for all message routes.
9. Configured Harrier.
10. Created and Tested a Profiler Rule.

You’ll use the MConsole (Message Console) management GUI and Cobalt to configure this. MConsole is Isode's central tool for messaging system Configuration and Operational management for both Internet and X.400 Messaging deployments. Cobalt is Isode’s User Provisioning tool.

## Recipient Configuration Matrix

This guide uses the addresses and mappings as follows.

Display Name	Internet Address	RI	PLA	S44o6 O/R Address
Jack Sparrow	jack.sparrow@field.net	N/A	N/A	N/A
Elizabeth Swann	elizabeth.swann@field.net	N/A	N/A	N/A
Simon Bates	simon.bates@field.net	N/A	N/A	N/A
FIELD CAPTAIN	captain@mmhs.field.net	RIFIELD	FIELD CAPTAIN	/CN=FIELD CAPTAIN /P=S44o6/A=FIELD/C=GB/
FIELD RADIO OPERATOR	radio.operator@mmhs.field.net	RIFIELD	FIELD RADIO OPERATOR	/CN=FIELD RADIO OPERATOR /P=S44o6/A=FIELD/C=GB/
BLACK PEARL	blackpearl@mmhs.field.net	RIFIELD	BLACK PEARL	/CN=BLACK PEARL /P=S44o6/A=FIELD/C=GB/
SERVICE MESSAGES	service.messages@mmhs.field.net	RIFIELD	N/A	N/A
POSTMASTER	postmaster@field.net	N/A	N/A	N/A
Gateway	gateway@field.net	N/A	N/A	N/A
GARBLED DATA	garbled.data@field.net	N/A	N/A	N/A
Arthur Lowe	arthur.lowe@headquarters.net	N/A	N/A	N/A
Ian Lavender	ian.lavender@headquarters.net	N/A	N/A	N/A
Steve Wright	steve.wright@headquarters.net	N/A	N/A	N/A
HEADQUARTERS CAPTAIN	captain@mmhs.headquarters.net	RIHEADQ	HEADQUARTERS CAPTAIN	/CN=HEADQUARTERS CAPTAIN /P=S44o6/A=HEADQUARTERS/C=GB/
HEADQUARTERS RADIO OPERATOR	radio.operator@mmhs.headquarters.net	RIHEADQ	HEADQUARTERS RADIO OPERATOR	/CN=HEADQUARTERS RADIO OPERATOR /P=S44o6/A=HEADQUARTERS/C=GB/
HOME GUARD	homeguard@mmhs.headquarters.net	RIHEADQ	HOME GUARD	/CN=HOME GUARD /P=S44o6/A=HEADQUARTERS/C=GB/

It also uses the following Role Occupant Relationships

Role	Role Occupant
FIELD CAPTAIN	Jack Sparrow
FIELD RADIO OPERATOR	Elizabeth Swann
SERVICE MESSAGES	None
HEADQUARTERS CAPTAIN	Arthur Lowe
HEADQUARTERS RADIO OPERATOR	Ian Lavender

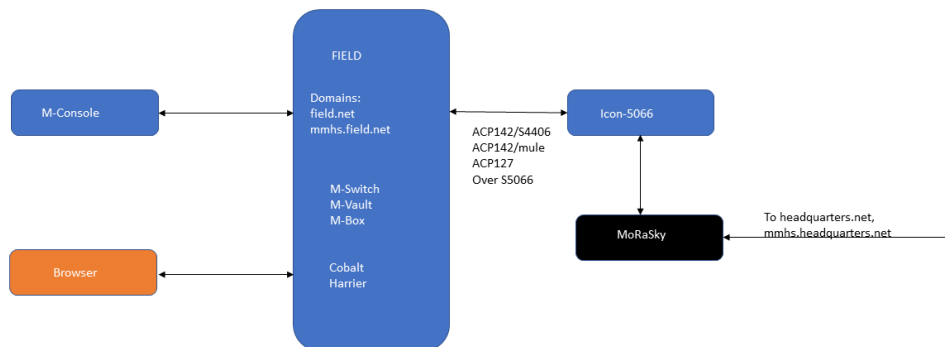
It also uses the following Organizational Relationships

Organization	Member Role
BLACK PEARL	FIELD CAPTAIN (Releaser, Always Sends Direct) FIELD RADIO OPERATOR (Drafter)
HOME GUARD	HEADQUARTERS CAPTAIN (Releaser, Always Sends Direct) HEADQUARTERS RADIO OPERATOR (Drafter)

## Environment Overview

The following diagram show the high-level overview of what you will be building.

### High Level Overview



Typically, the “To headquarters.net, mmhs.headquarters.net” connection would be over HF Radio. You will need to have an existing Icon-5066 Server for use or build one on the Local Server.

This guide is not intended to resemble a real world HF Military Messaging System but to give you a basic environment you can test with and get used to how the Isode products and configuration GUIs work.

Where passwords are required, the guide will assume “Secret1+”

## **Using Isode Support**

You will be given access to Isode support resources when carrying out your evaluation. Any queries you have during your evaluation should be sent to [support@isode.com](mailto: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

### Naming the Server

Make the machine name: MU-ONE

Make the primary dns suffix for the server FIELD.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. Remember to install an appropriate java runtime engine first (refer to product release notes) and in a Windows environment the visual c++ redistributable package. For this guide, the following products were used:

Messaging Activation Server 1.1

M-Vault 19.0v3

M-Switch 19.0v3

M-Box 19.0v3

Cobalt-1.4

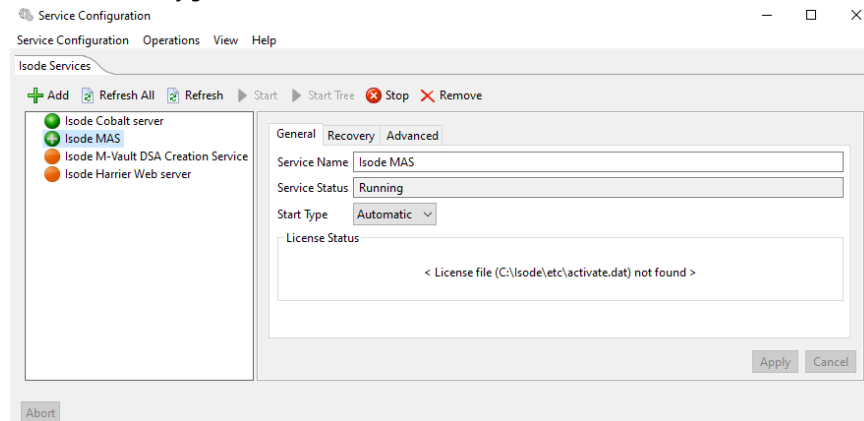
Isode-Harrier-3.3

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

## Activating the Isode Products

Ensure the MAS server has started by using the Isode Service configuration tool.

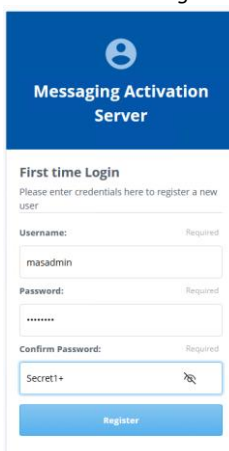
### Isode Service Configuration - MAS



Browse to “https://localhost:9000”

The browser will provide a security warning. Choose an option to override the warning

### MAS First Time Log in



In “Username” type “masadmin”

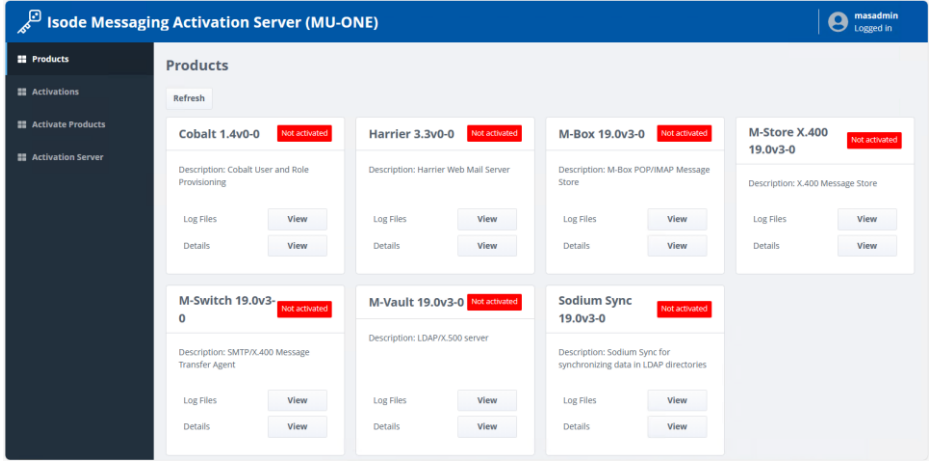
In “Password” type “Secret1+”

In “Confirm Password” type “Secret1+”

Press “Register”

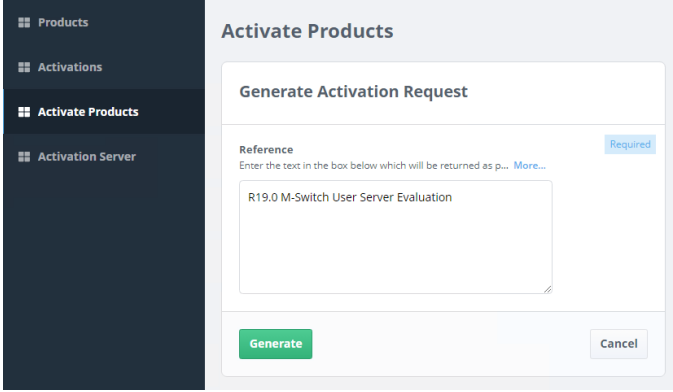
You will be presented with a list of installed products.

View installed Product List



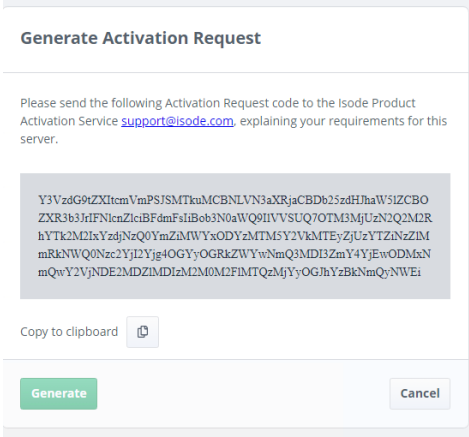
Select “Activate Products”  
In “Reference” type “R19.0 M-Switch User Server Evaluation”

Populate Activation Reference



Press “Generate”  
Copy the activation request code to your clipboard.

Generate Activation Request



Send an email to Isode support asking for an activation for M-Vault, Sodium Sync, M-Switch User Server (Options: Market type Military, X400 Messaging Protocols,

ACP127 Channels, ACP142, CFTP, Profiler), M-Box, Cobalt and Harrier for a “R19.0 M-Switch User Server Evaluation”. Include the activation request code.

Isode support will supply a set of Product Activation keys

It is likely that the session between the browser and MAS will have timed out between requesting the product activation and receiving the keys. It is therefore sensible, once the keys have been received, to close the browser window and log back into MAS again.

Select “Activate Products”

Paste the keys into the “Activation Key” field

*Submit Activation key*

Press “Submit”.

You will be presented with an “Activation Result”

*Activation result*

No.	Processing Status	Product	Activation and Installed Status
1	Added	M-Vault 19.0	OK
2	Added	SodiumSync 19.0	OK
3	Added	M-Switch 19.0	OK
4	Added	M-Box 19.0	OK
5	Added	Cobalt 1.4	OK
6	Added	Harrier-Web 3.3	OK

Select “Products”

The products that have been activated should appear in green.

Activated Product List

The screenshot shows the 'Activated Product List' in the Isode Messaging Activation Server (MU-ONE) interface. The interface has a dark blue header with the title and a user profile 'masad@ms' in the top right. A left sidebar contains navigation options: 'Products' (selected), 'Activations', 'Activated Products', and 'Activation Server'. The main content area is titled 'Products' and includes a 'Refresh' button. It displays a grid of product cards, each with a version number, a status indicator (green for active, red for inactive), and a 'View' button for logs and details.

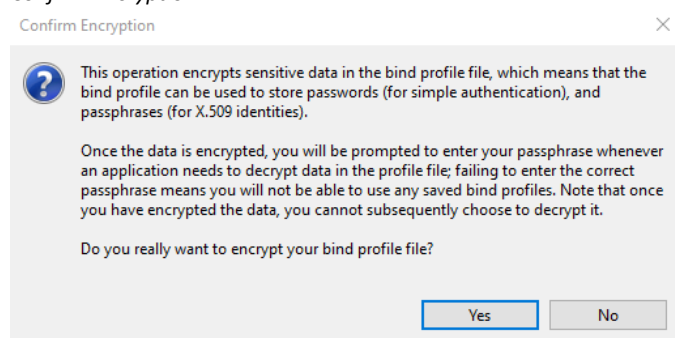
Product Name	Version	Status	Activation Name
Cobalt	1.4v0-0	Active	Cobalt - Base
Harrier	3.3v0-0	Active	Harrier Web - Harrier Web
M-Box	19.0v3-0	Active	M-Box - M-Box
M-Store X.400	19.0v3-0	Inactive	M-Store X.400 Message Store
M-Switch	19.0v3-0	Active	M-Switch - User Server
M-Vault	19.0v3-0	Active	M-Vault - Server
Sodium Sync	19.0v3-0	Active	SodiumSync - Base

## Building the Core Messaging System

You will use the MConsole GUI to build your core messaging system. Open the “MConsole” Isode application from the Windows Start menu. On Linux execute the following command:

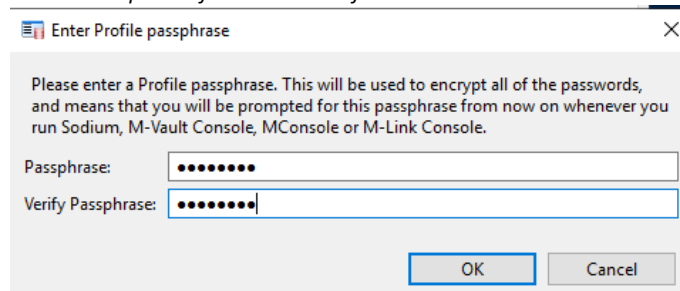
```
% /opt/isode/bin/mconsole
```

### Confirm Encryption



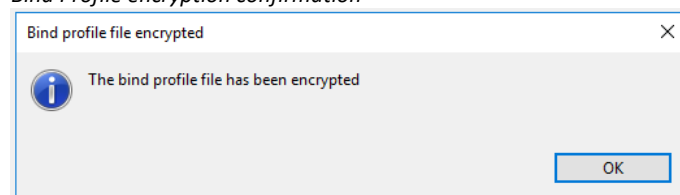
Click “Yes”.

### Enter a Passphrase for the Bind Profile



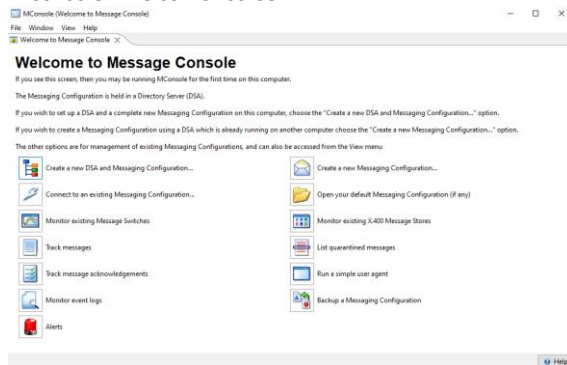
Enter and verify the password “Secret1+”  
Click “OK”.

### Bind Profile encryption confirmation



Click “OK”.

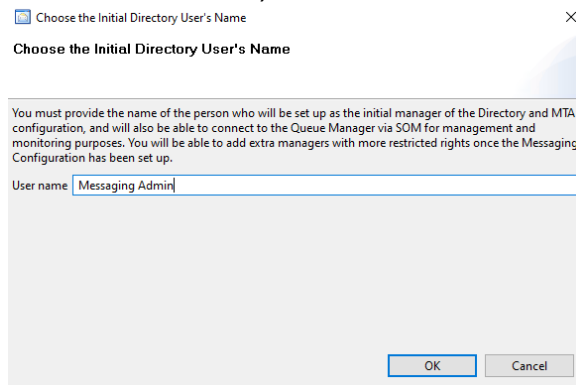
## MConsole "Welcome" screen



## Create the DSA

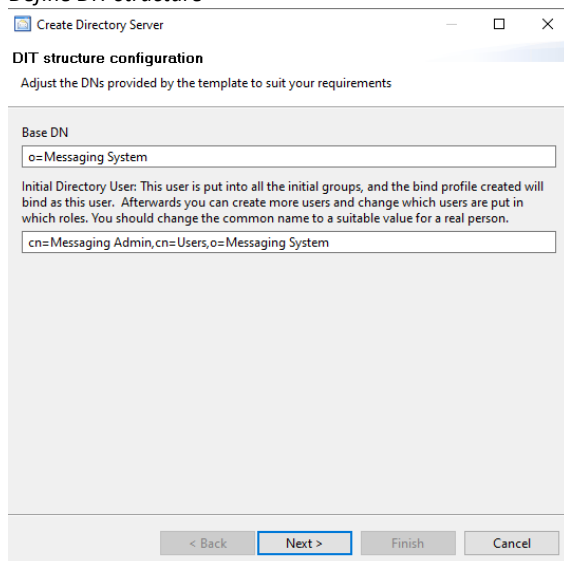
Click on the "Create a New DSA and Messaging Configuration" icon.

### Choose the initial Directory Users name



Type the name "Messaging Admin" for the initial directory user, this user will be the Master Directory User account and have full access to the Directory Server. Click "OK".

### Define DIT structure



Enter a "Base DN" of your choice. Click "Next >".

### Provide password

**Provide password**

Create Directory Server

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

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

Password: Secret1+  Show

Record user authentication times (authTimestamps)

**Password Hashing**  
Hashed passwords are more secure, but are not compatible with password-based SASL mechanisms other than PLAIN, LOGIN and SCRAM-SHA-1.

Note that while non-hashed passwords may be recovered from the DSA database, hashed passwords are NOT recoverable.

Hash all passwords using SCRAM-SHA-1

Enter a password for the “Initial Directory User” and leave the other settings as default. Click “Next >”.

### Bind profile name

**Bind profile name**

Create Directory Server

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

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

cn=dsa,o=Messaging System / Messaging Admin

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

C:\isode\d3-db

On “Bind Profile Names and Filesystem Location” leave defaults. Click “Next >”.

### Provide address configuration

**Provide address configuration**

Create Directory Server

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

Hostname: MU-ONE.FIELD.NET

Enable:  
 LDAP  DAP

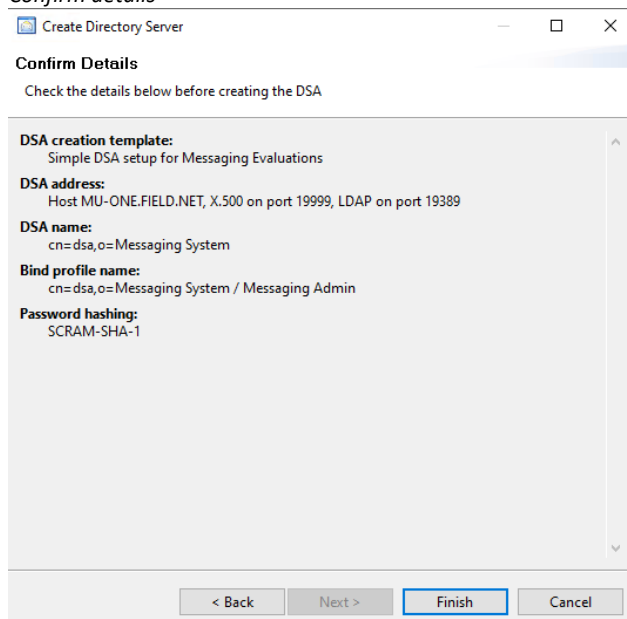
Port numbers:  
 Standards, no messaging: 389 / 102  
 Standards with messaging: 389 / 19999  
 Isode default: 19389 / 19999  
 Alternate 2: 29389 / 29999  
 Alternate 3: 39389 / 39999  
 Alternate 4: 49389 / 49999  
 Alternate 5: 59389 / 59999

Type the hostname “MU-ONE.FIELD.NET”  
Click “Next >”



The summary of your DSA configuration is shown.

### Confirm details



Click “Finish”.

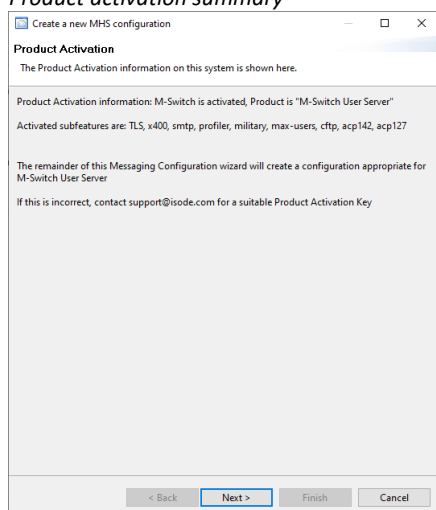
The DSA is created and started.

## Create the Messaging Configuration

Next, we will create the Messaging Configuration.

A summary will have been presented of the product components that have been activated. The activated components partially drive the contents of the final switch configuration.

### Product activation summary



Click “Next >”

## Set Messaging Configuration Base DN

Create a new MHS configuration

**Set the Messaging Configuration Base DN**

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

o=Messaging System

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

Create organization name | Messaging Switches

Messaging configuration name  
Messaging Configuration MU-ONE

Base DN: o=Messaging Switches,o=Messaging System  
MHS DN: cn= Messaging Configuration MU-ONE,o= Messaging Switches,o= Messaging System

< Back   Next >   Finish   Cancel

Select “o=Messaging System” in the browser section.

Select “Create Organization Name”

Set the organization name as “Messaging Switches”

Set “Messaging Configuration name” as “Messaging Configuration MU-ONE”

Click “Next >”.

## Provide Hostname

Create a new MHS configuration

**Hostname**

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

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

MU-ONE.FIELD.NET

DSA Authentication

SASL Password Secret1+ Hide

< Back   Next >   Finish   Cancel

In “hostname” type “MU-ONE.FIELD.NET”

In “SASL Password” type “Secret1+”

Click “Next >”

*smtp channel specific settings*

Create a new MHS configuration

**SMTP channel specific settings and routing policy**

Enter the internet domain regarded as local to this MTA.

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

Email address domain

Create an Internet Message Store for local POP3 or IMAP users

Use DNS

Use MX records

Don't use DNS

< Back   Next >   Finish   Cancel

Enter “field.net” in “Email address domain”.

Ensure “Create an Internet Message Store for local POP3 or IMAP users” is checked.

Select “Don’t use DNS”

Click “Next >”.

*Provide 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.

**Admin Users Parent DN**

The location beneath which new Admin Users will be created

Parent DN

Use the top of the directory tree

Use existing SASL Id

user name

Create new SASL Id

Admin user name  @

Admin password

< Back   Next >   Finish   Cancel

Ensure “Use Existing SASL Id” selected

Ensure “user name” is “messaging.admin@field.net”

Click “Next >”.

## Provide 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  United Kingdom

Single Space ADMD   Missing PRMD

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

Enter the details for the X.400 Address Space for your S4406 Local users. We do not require a local X.400 message store so check the “Do not create an X.400 Message Store” checkbox. Click “Next >”.

## Antivirus Configuration

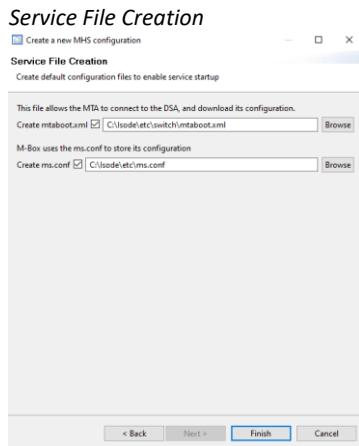
Create a new MHS configuration

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

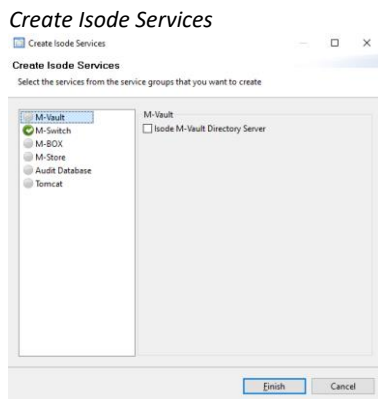
Anti Virus Engine  None  Clam AV  
 Install msgcheck.zip

< Back **Next >** Finish Cancel

On “Antivirus Configuration” Select “None” Click “Next >”.

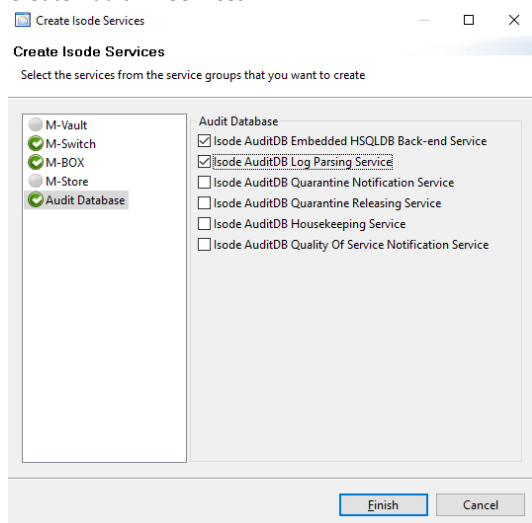


On “Service file creation” leave the defaults  
Click “Finish”.



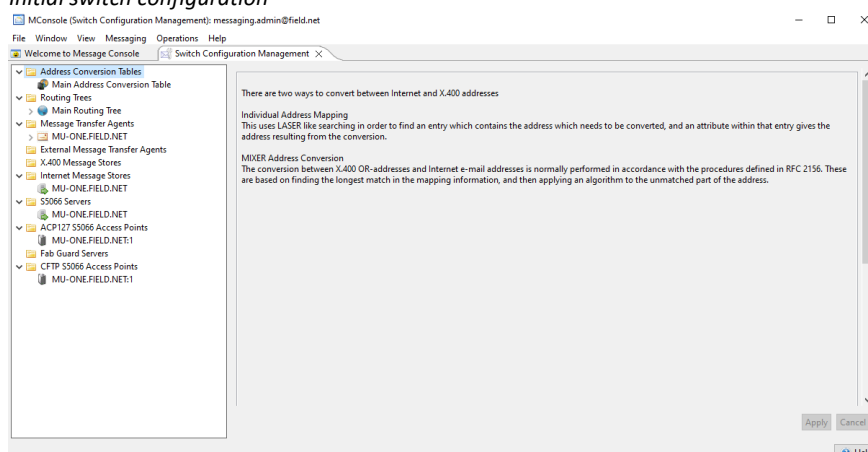
This screen allows you to configure additional Windows Services (not shown on Linux installations). The Audit Database is a useful tool and so we will create the necessary services here but not use them initially.  
Click on “Audit Database”.

## Create Audit DB Services



Check the “Isode AuditDB Embedded HSQLDB Back-end Service” and “Isode AuditDB Log Parsing Service” checkboxes  
Click “Finish”.

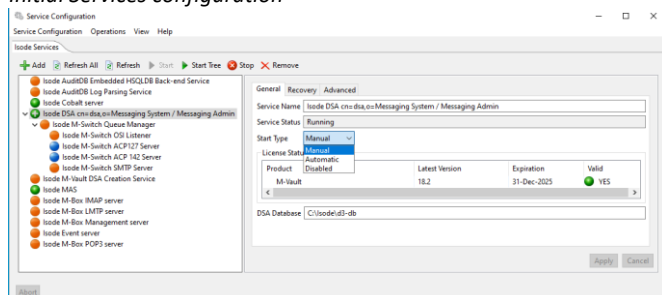
## Initial switch configuration



Your Core MTA configuration is now complete and you should configure and start the services before continuing.

Start the “Isode Service Configuration” tool.

## Initial Services configuration



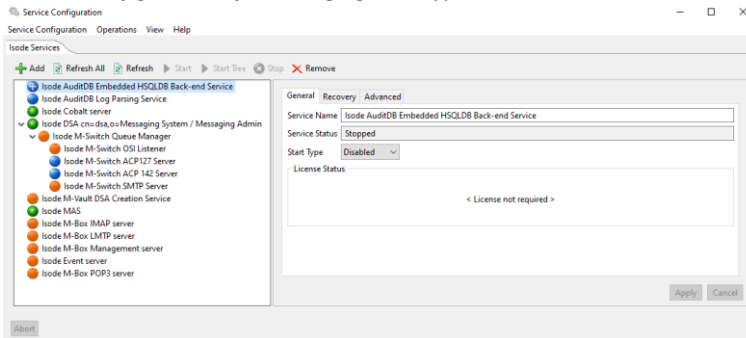
Change the “Isode DSA” Service to “Automatic” from the “Start Type” dropdown

Click “Apply”.

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

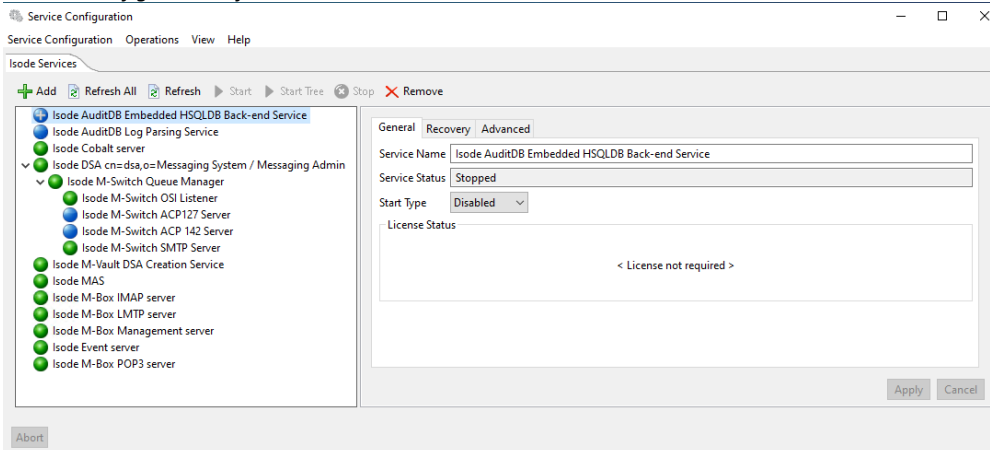
Change the “Isode AuditDB Embedded HSQLDB Back-end Service” and “Isode AuditDB Log Parsing Service” to “Disabled”.

### Services Configuration after changing Start types



Then select from the Top Menu “Operations→Start All”.

### Services Configuration after services started

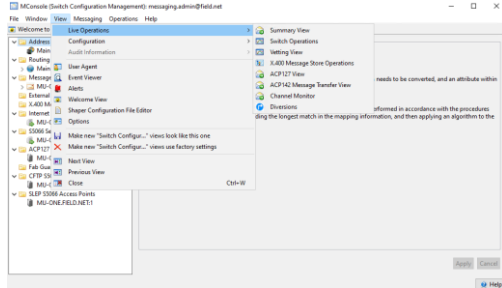


## Configure the Switch Operations View

We need to configure the “Switch operations view” in order to manage message queues and ensure that most configuration changes in MConsole are implemented immediately.

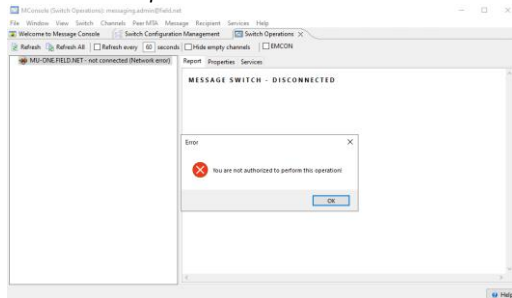
From the MConsole top menu select View → Live Operations → Switch Operations.

### Open switch operations view



The following error is expected.

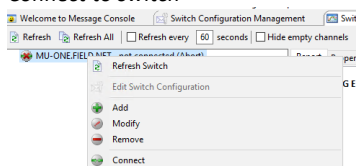
### Initial Switch operations view



Click “OK” to clear it.

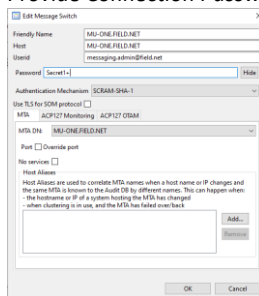
Right Click on the Switch displayed and select “Modify”

### Connect to switch



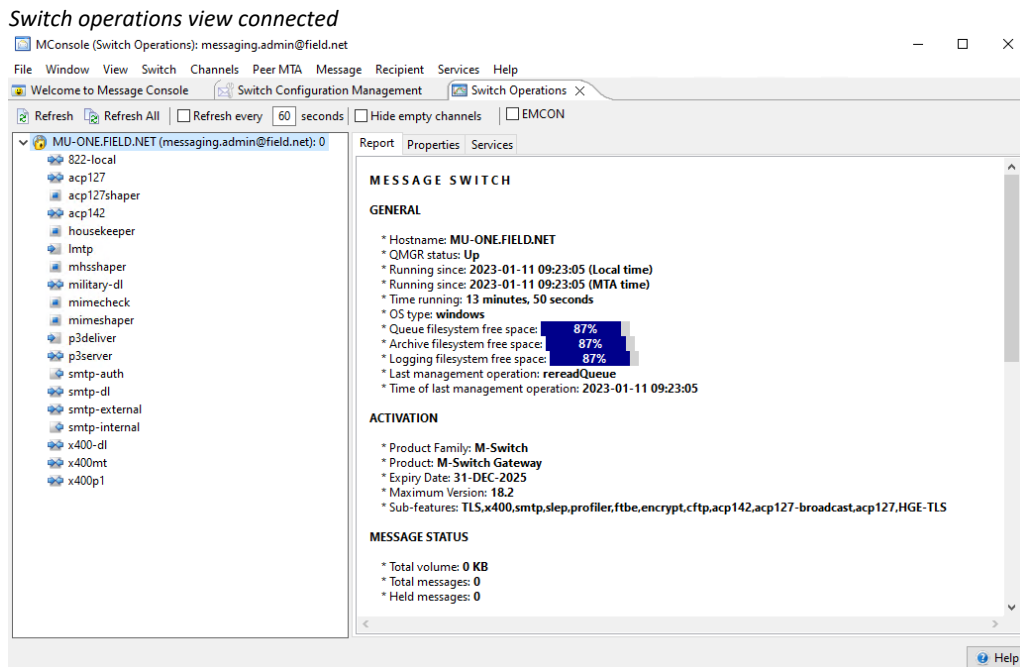
Enter the password you entered when creating the “Initial Directory User”

### Provide Connection Password





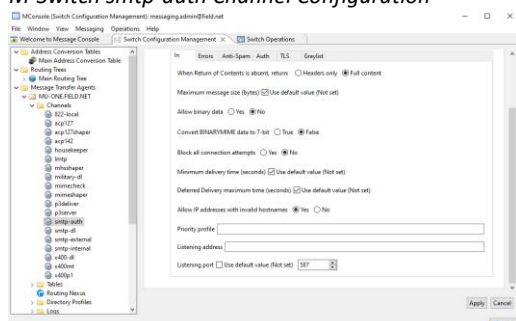
Click “OK”.  
The following screen will be displayed.



## Configure the switch to allow connections from Harrier

From the “Switch Configuration Management” View select the “smtp-auth” channel and change to the “Program” tab.

### M-Switch smtp-auth Channel Configuration



Then set the “Allow IP addresses with invalid hostnames” to “Yes”  
Click “Apply”.

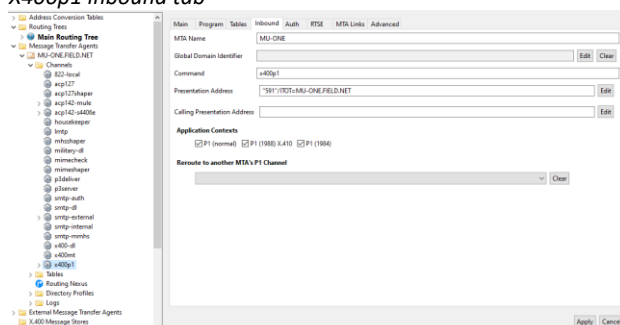
## Modify the MTA Name for P1 Connections

Select the Channel “x400p1”

Select the “Inbound” tab.

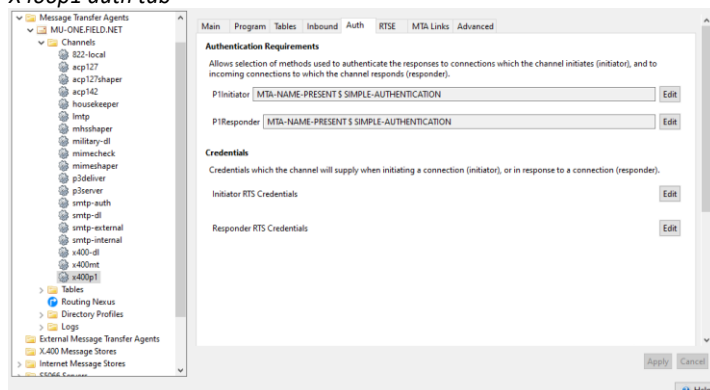
Change the “MTA Name” to “MU-ONE”

### X400p1 inbound tab



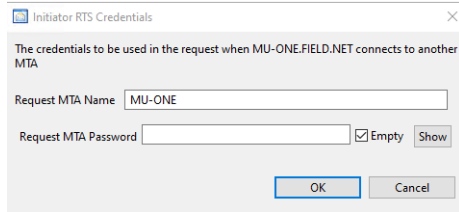
Press “Apply”  
Change to the “Auth” tab.

### X400p1 auth tab



Press “Edit” next to “Initiator RTS Credentials”

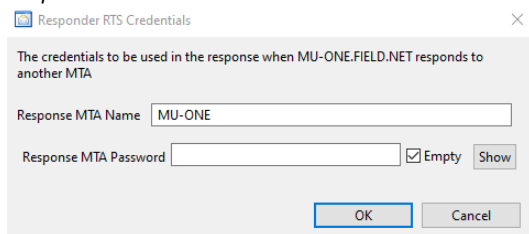
**Initiator RTS Credentials**



Change the “Request MTA Name” to “MU-ONE”  
 Check “Empty”  
 On the warning “No Password Specified” Press “OK”

Press “OK”  
 Press “Edit” next to “Responder RTS Credentials”

**Responder RTS Credentials**

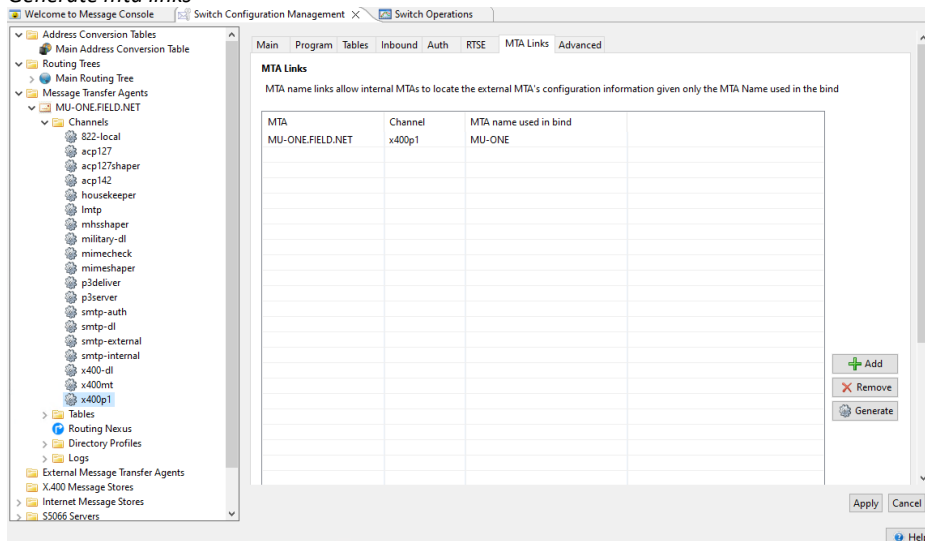


Change “Response MTA Name” to “MU-ONE”  
 Check “Empty”  
 On the warning “No Password Specified” press “OK”

Press “OK”  
 Press “Apply”

Change to the “MTA Links” tab.  
 Press “Generate”

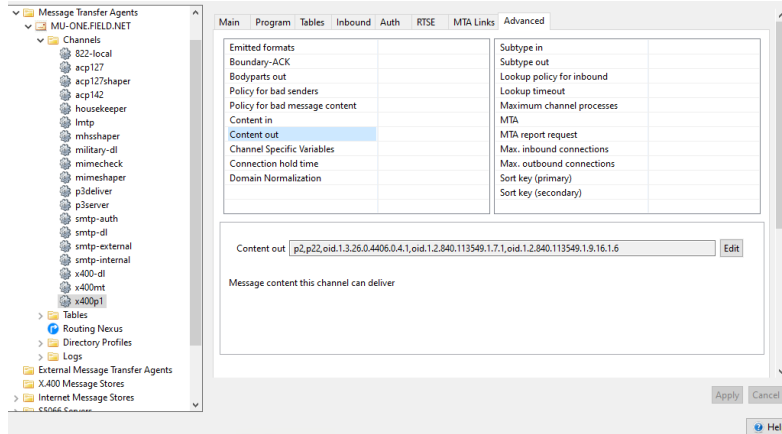
**Generate mta links**



Press “Apply”

X400p1 “Advanced” tab.

*X400p1 Advanced tab*

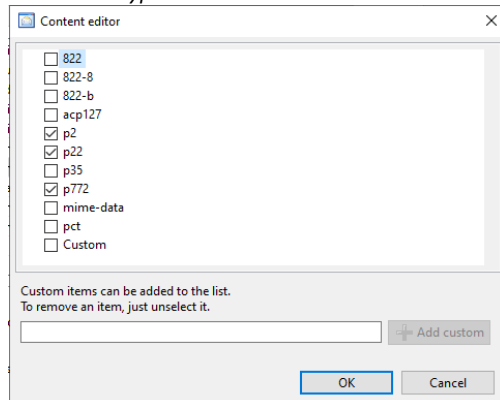


Select “Content Out”

Press “Edit”

Uncheck all but the content types “p2”, “P22”, “p772”

*P1 Content types*



Press “OK”

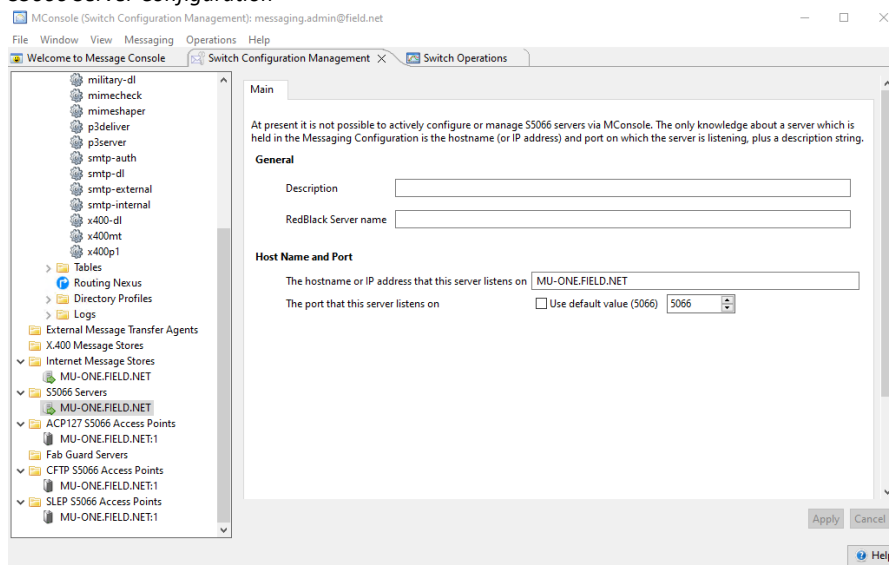
Press “Apply”

## Configure the External Connections to “headquarters.net”

### Configure an appropriate Stanag 5066 Server

From the “Switch Configuration Management” view of MConsole select the default S5066 Server.

#### S5066 Server Configuration

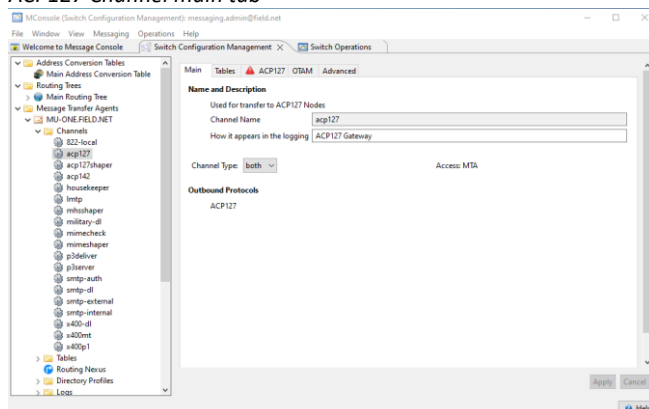


You should change these values to match the Hostname (or IP Address) and Port of the S5066 server that will be used by this MTA. If you make any changes to the default settings you will need to click “Apply”.

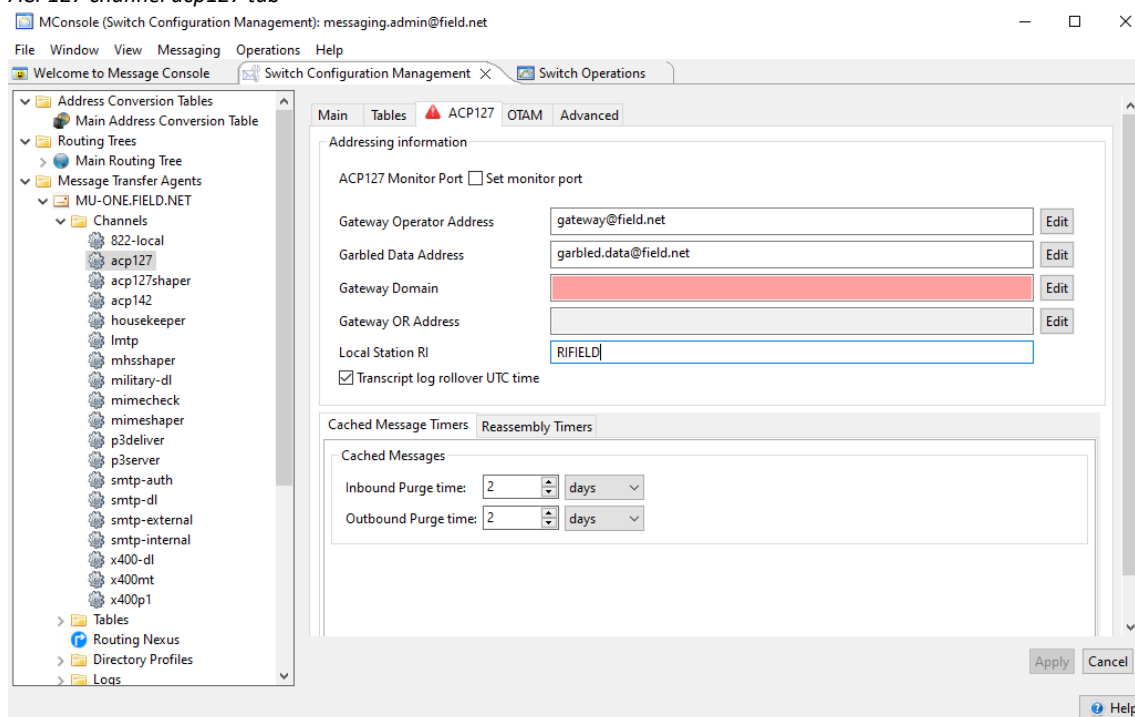
### Configure the ACP127 Channel

Select the “acp127” channel.

#### ACP127 Channel main tab



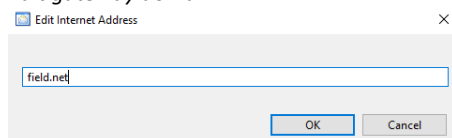
Select the “ACP127” tab.

**ACP127 channel acp127 tab**

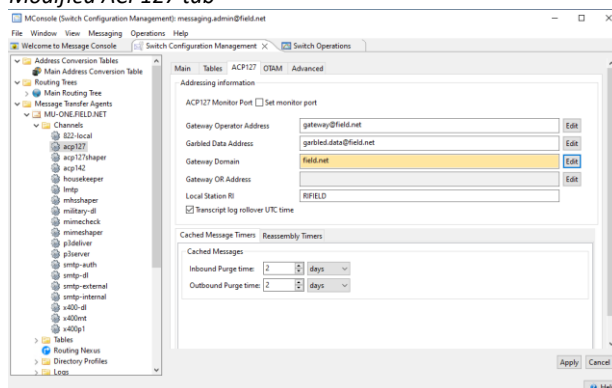
Enter the Internet Addresses for the “Gateway Operator” and “Garbled Data” from the table at the start of this document.

Populate the “Local Station RI”

Click “Edit” next to the “Gateway Domain”.

**Edit gateway domain**

Enter the Local Internet Domain “field.net” and Click “OK”.

**Modified ACP127 tab**

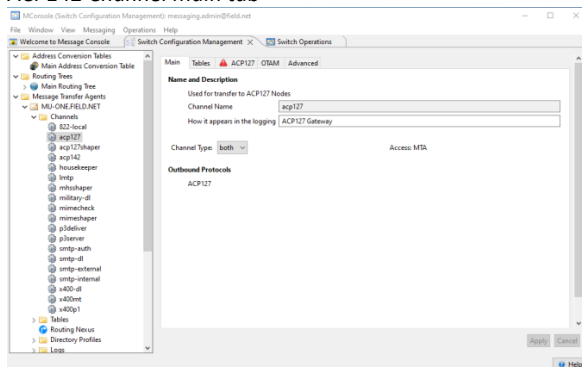
Click “Apply”.

This completes the local ACP127 Channel Configuration we will now configure the ACP142 Channels.

## Configure a channel for mmhs ACP142/Stanag4406 traffic

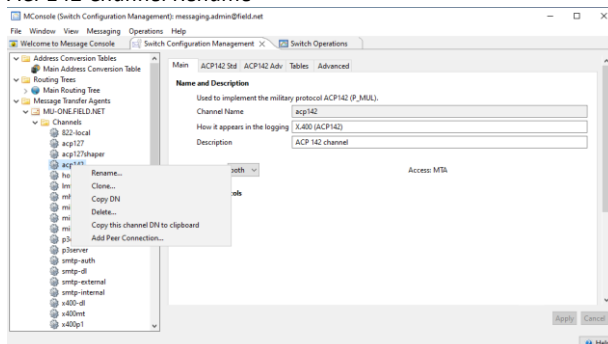
Select the “acp142” Channel on the “Switch Configuration Management” view of MConsole.

### ACP142 Channel main tab



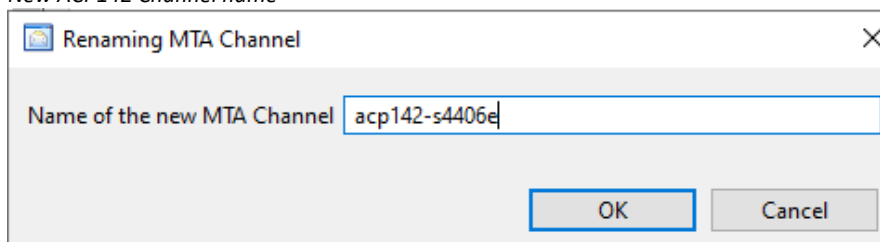
We will rename this channel “acp142-s4406e” and use it to process ACP142 Stanag 4406 Annex e messages.

### ACP142 Channel Rename



Right click and from the context menu choose “Rename”

### New ACP142 Channel name

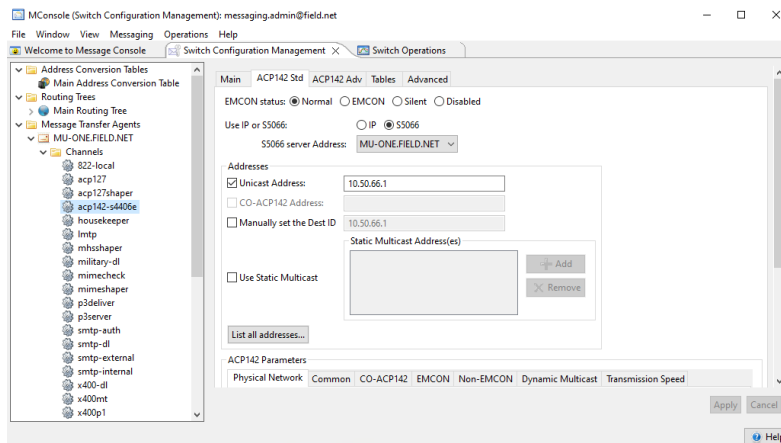


In “Name of the new MTA Channel” type “acp142-s4406e”

Press “OK”

Select the “ACP142 Std” tab.

## ACP142 std tab



Select the “S5066” Radio Button

Select the S5066 Server from the drop down

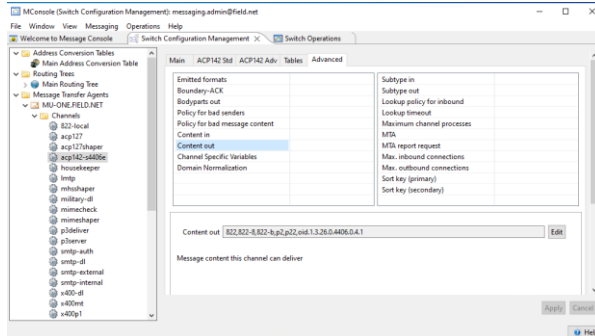
Set the “Unicast Address” to the Node Address of your local S5066 Server

Uncheck “Use Static Multicast”.

Select the “Advanced” tab.

Select “Content out”

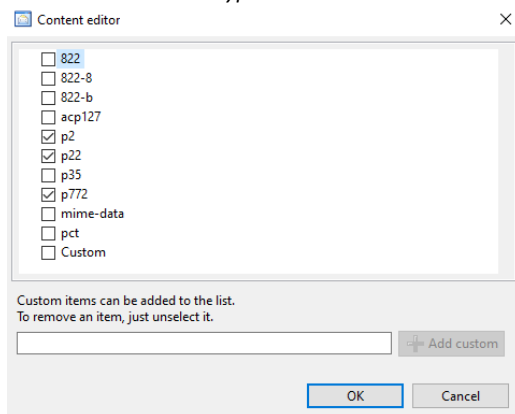
## Advanced tab



Click “Edit”.

Uncheck the “822”, “822-8” and “822-b” content types.

Select S4406 Content types



Click “OK”.

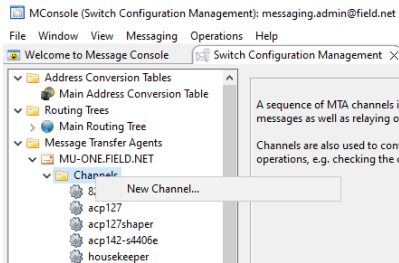
Press “Apply”



## Configure the ACP142/mule Channel for internet smtp traffic

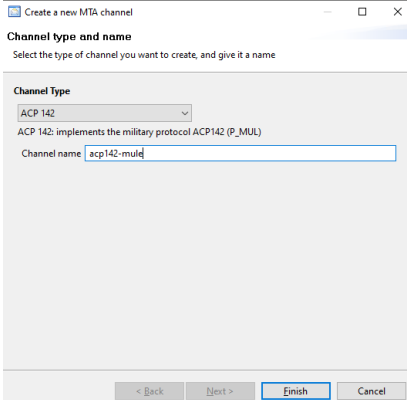
From the “Switch Configuration Management” tab right click “channels”

### Create new channel



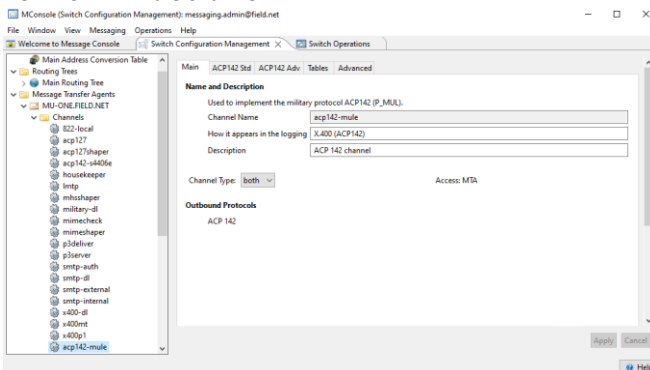
Select “New Channel”

### Name ACP142 mule channel



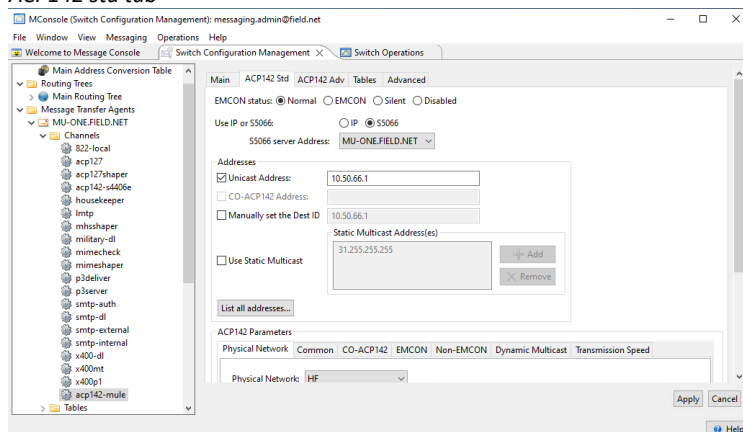
Select channel type “ACP142”  
Type channel name: “acp142-mule”  
Press “Finish”

### New ACP142 mule channel



Select the “ACP142 Std” tab.

## ACP142 std tab



Select “S5066”

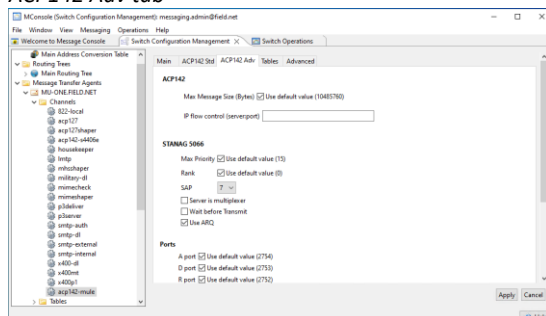
Select the local S5066 Server Address from the Drop Down

Set the Unicast Address to the Local S5066 Server “Node Address”

Uncheck “use Static Multicast”

Select the “ACP142 Adv” Tab.

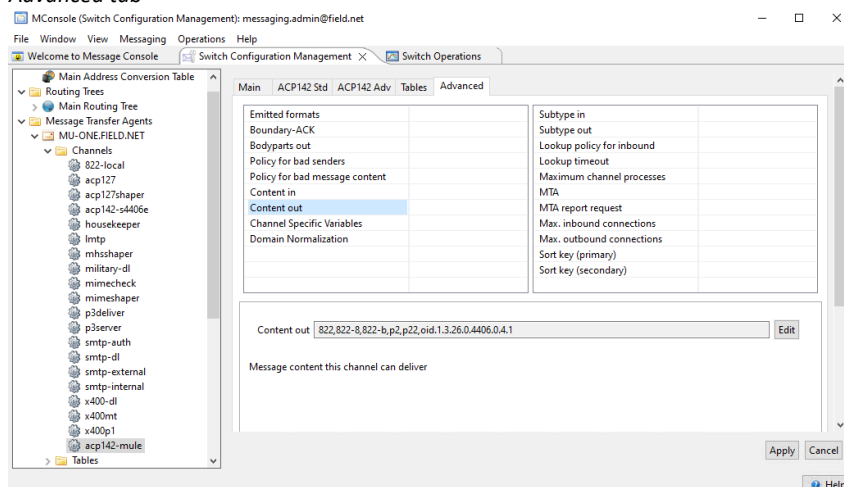
## ACP142 Adv tab



Select SAP “7”

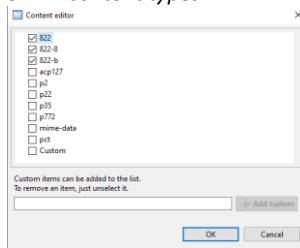
Select the “Advanced” tab and select “content out”

## Advanced tab



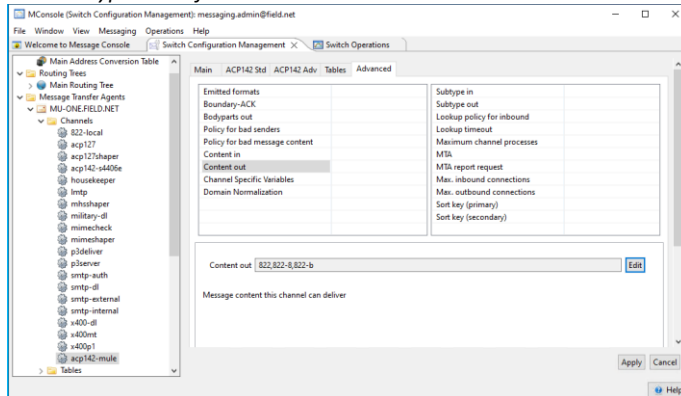
In order to force the channel to only support smtp content click “Edit”.

## SMTP content types



Uncheck “p2”, “p22” and “p772”.  
Click “OK”.

## Content types modified



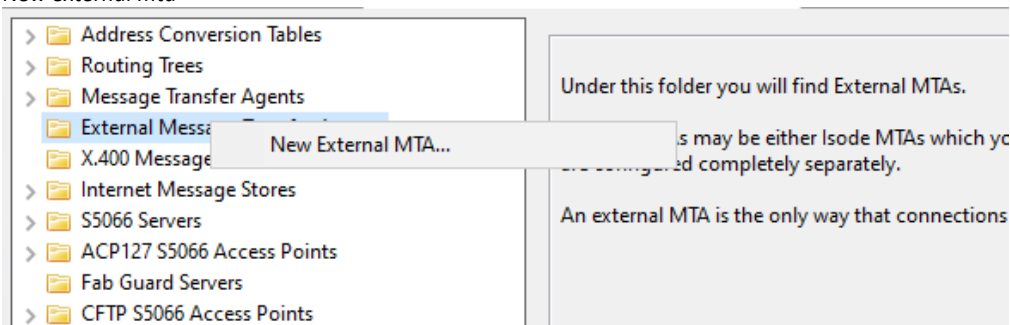
Press “Apply”

This completes the configuration of the ACP142 Mule Channel.

## Configure the External ACP<sub>127</sub> Station

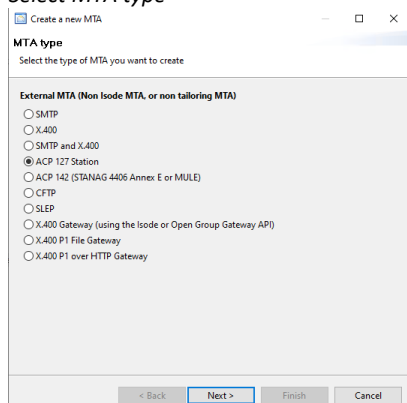
From the Switch Configuration Management View right click on the “External Message Transfer Agents”.

### New external mta



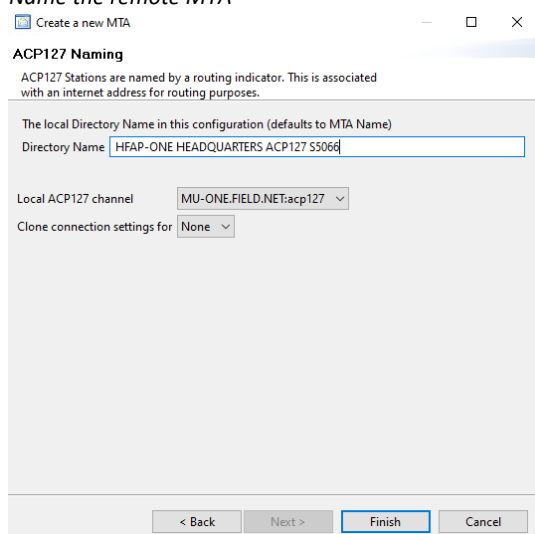
Select “New External MTA...”.

### Select MTA type



On “MTA Type” dialogue, select “ACP127 station”  
Click “Next >”.

### Name the remote MTA

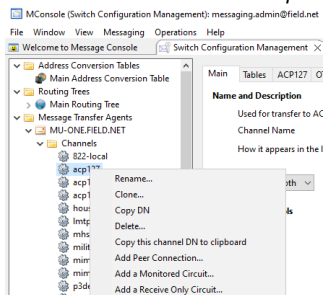


Enter a name of your choice for the “Directory Name”

Click “Finish”.

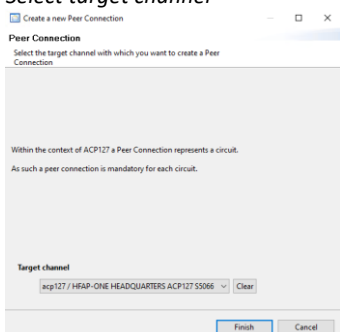
Select the ACP127 Channel

### Add Peer Connection menu option



Right click and in the context menu provided select “Add Peer Connection”

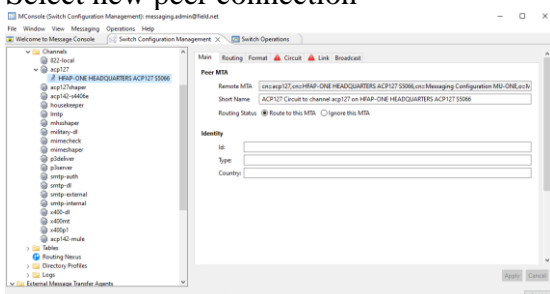
### Select target channel



In the “Create a new peer connection dialogue” select acp-127/HFAP-ONE HEADQUARTERS ACP127 S5066 ..”  
Press “Finish”

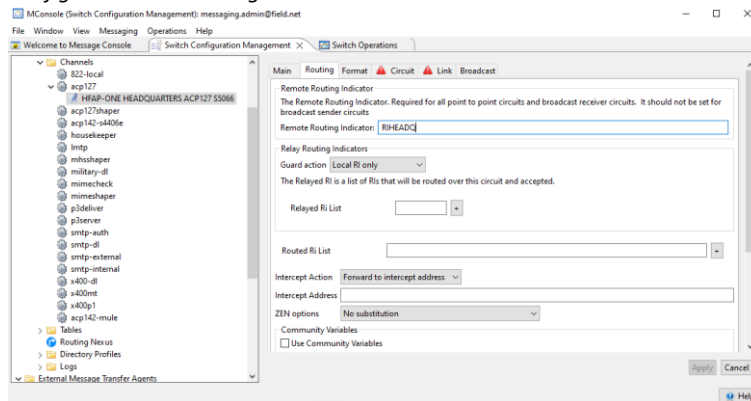
Select the New Peer Connection that has been created under the acp-127 channel

### Select new peer connection



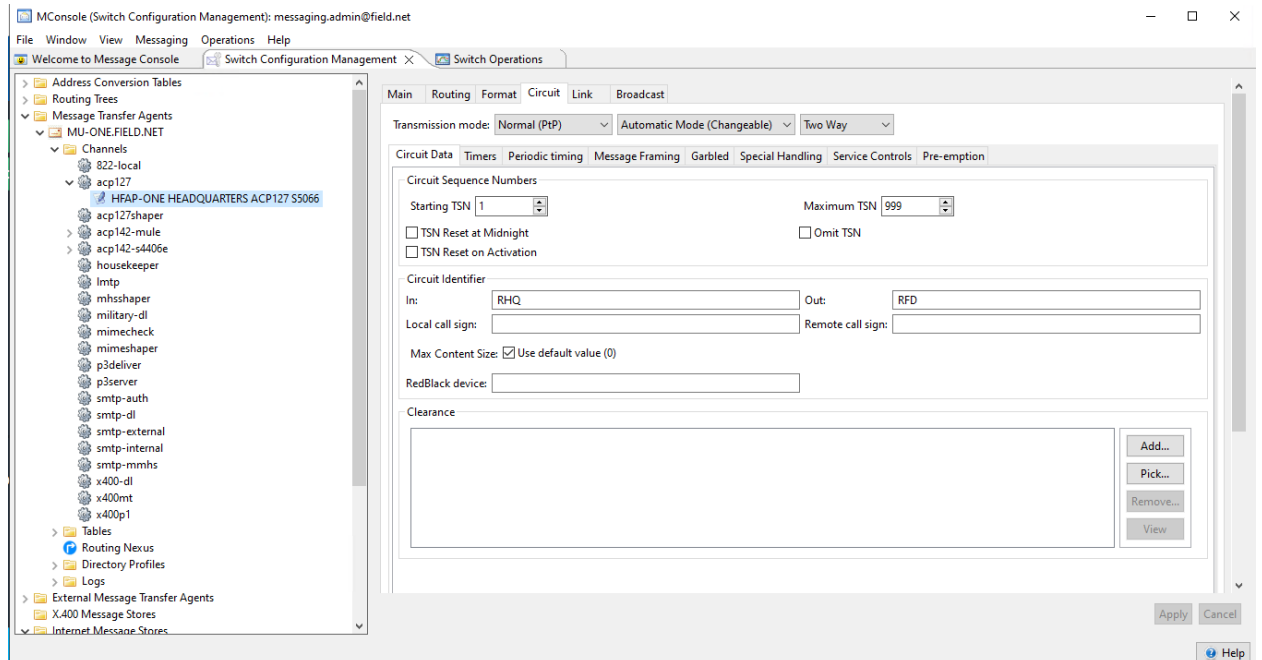
Select the “Routing” tab.

## Configure ACP127 routing

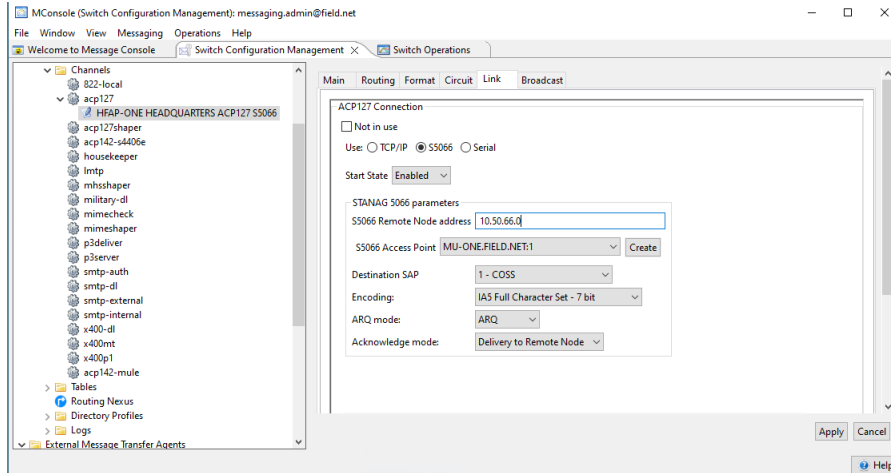


Type the “Remote Routing Indicator” for the Remote ACP127 station.  
Select the “Circuit” tab.

## ACP127 Circuit tab



Insert a Unique Identifier of your choice for the “In Circuit Identifier” and the “Out Circuit Identifier”. These will need to be configured the opposite way around on the other end.  
Select the “Link” tab.

**ACP127 link tab**

Select “S5066”, then enter the Node Address of the Remote ACP127 Station, select the S5066 Server you have configured from the drop down.

Click “Apply”.

This completes the configuration of the Remote ACP127 Station.

## Configure the External ACP<sub>142</sub> MTAs

### Configure the external ACP<sub>142</sub>/S<sub>4406</sub> MTA

We will now configure the External ACP<sub>142</sub> S<sub>4406</sub> MTA. Right Click on the “External Message Transfer Agents” and select “New External MTA...”

#### Add the External ACP<sub>142</sub> S<sub>4406</sub> MTA

Create a new MTA

**MTA type**  
Select the type of MTA you want to create

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

- SMTP
- X-400
- SMTP and X-400
- ACP 127 Station
- ACP 142 (STANAG 4406 Annex E or MULE)
- CFIP
- SLEP
- X-400 Gateway (using the Isode or Open Group Gateway API)
- X-400 P1 File Gateway
- X-400 P1 over HTTP Gateway

< Back Next > Finish Cancel

Select “ACP 142 (STANAG 4406 Annex E or MULE)”  
Click “Next >”.

#### Name the External MTA

Create a new MTA

**MTA Naming**  
MTAs can be named in a number of different ways, depending on the context. To activate the host name validation, select another text field

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

Directory Name

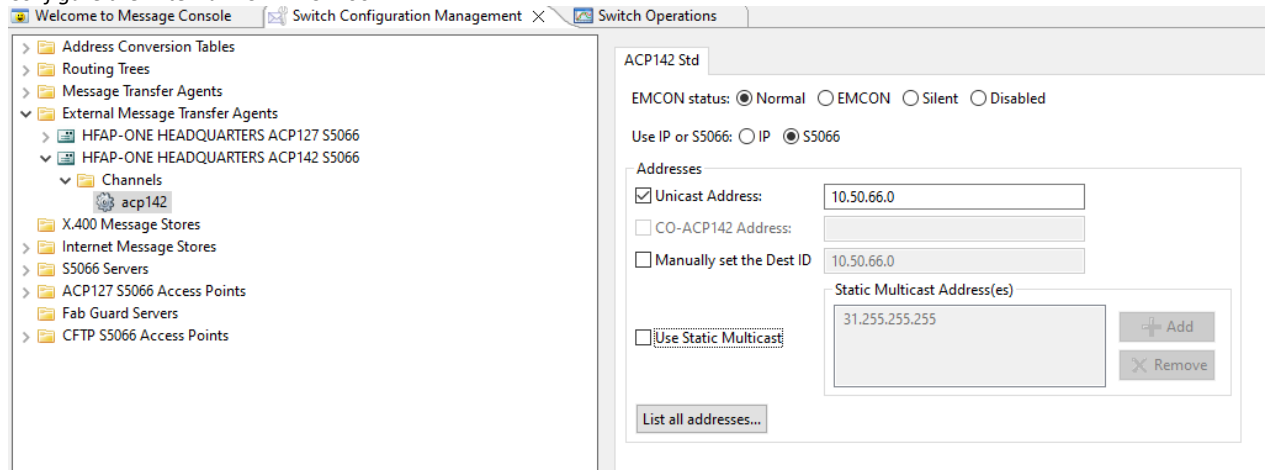
< Back Next > Finish Cancel

Enter a name of your choice for the Display Name  
Click “Finish”.

Use the left-hand pane to navigate to the newly configured ACP<sub>142</sub> external MTA.



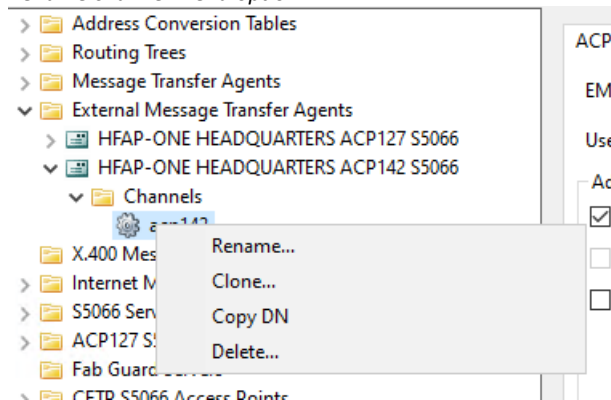
## Configure the External ACP142 S4406 MTA



Enter the S5066 Node Address of the External MTA for the “Unicast Address”  
 Uncheck “Use Static Multicast”.  
 Click “Apply”.

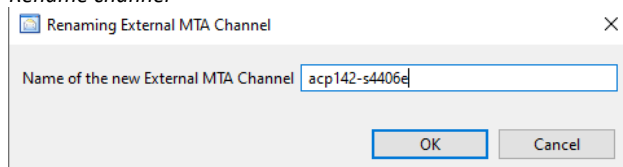
Right click on the acp142 channel in the External MTA just created.

### Rename channel menu option



Select “Rename ...”  
 Rename the channel “acp142-s4406e”

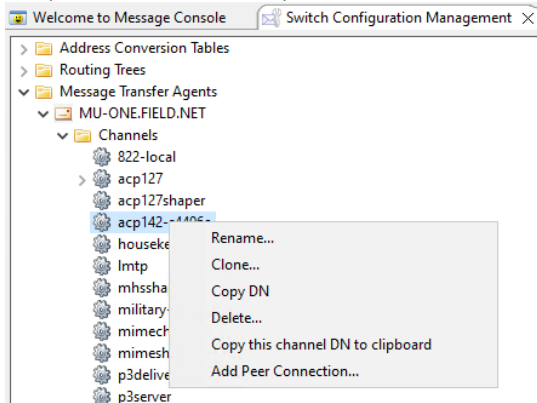
### Rename channel



Press “OK”

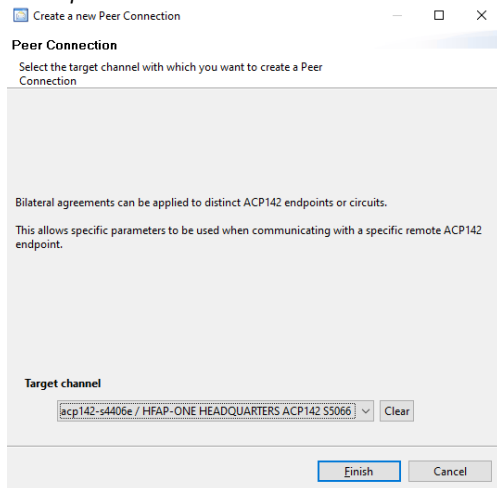
Right click on the local “acp142-s4406e” channel

## Add peer connection menu option



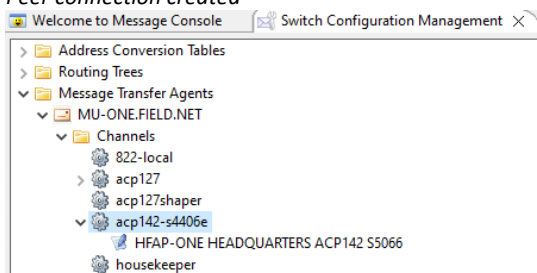
Select “Add Peer Connection...”

## Select peer connection



Select the “target channel” “acp142-s4406e .....”  
Press “Finish”

## Peer connection created

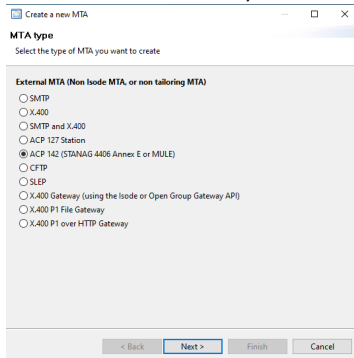


This completes the configuration of the External ACP142 S4406 MTA.

## Configure the External ACP142/Mule MTA

From the “Switch Configuration” view Right Click on “External Message Transfer Agents” and select “New External MTA”

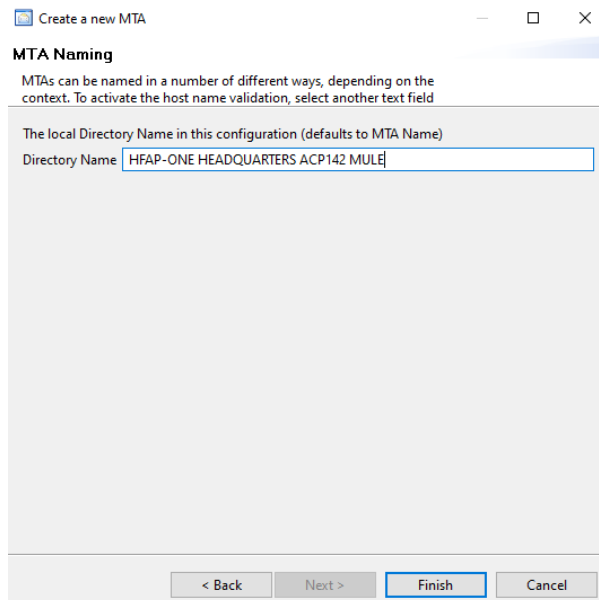
**Add the External ACP142/mule MTA**



Select "ACP 142 (STANAG 4406 Annex E or MULE)"  
Click "Next >".

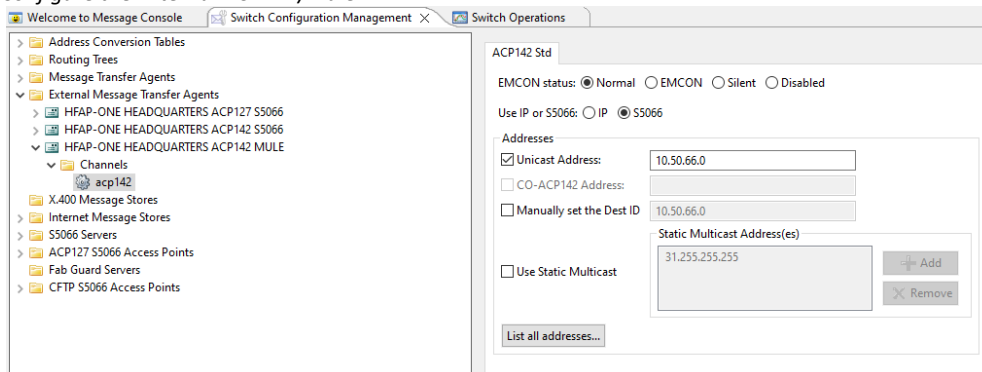
The "Directory Name" can be any name you want that best describes the Remote MTA.

**Name the External MTA**



Click "Finish".  
Select the newly created acp142 mule External Message Transfer agent.

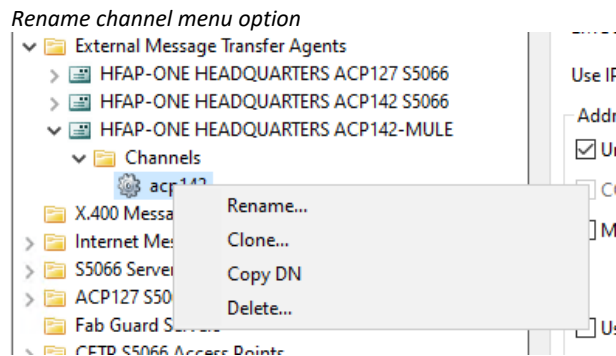
**Configure the External ACP142/mule MTA**



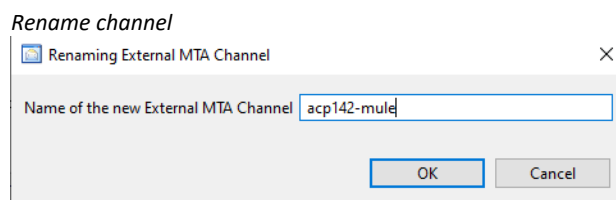
Set the "Unicast Address" to be the S5066 Server Node Address of the Remote Server

Uncheck “Use Static Multicast”.  
Click “Apply”.

Right click on the acp142 channel in the External MTA just created.

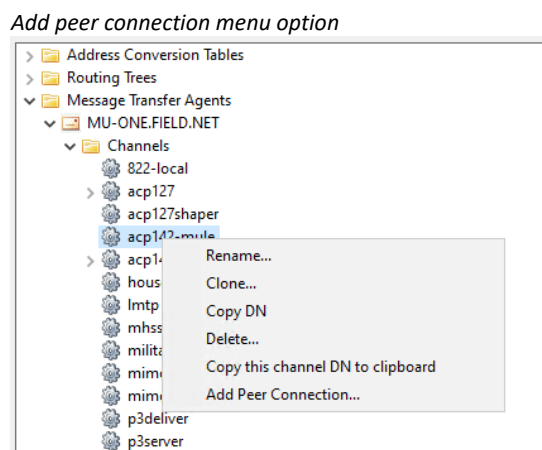


Select “Rename ...”  
Rename the channel “acp142-mule”



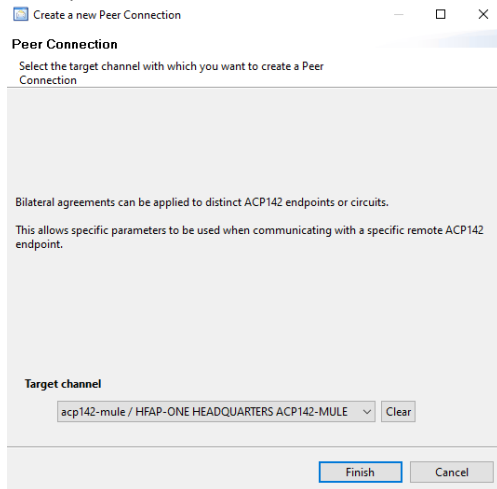
Press “OK”

Right click on the local “acp142-mule” channel



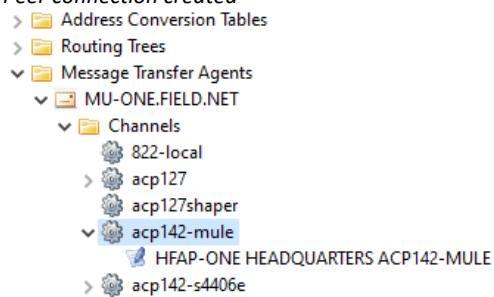
Select “Add Peer Connection...”

## Select peer connection



Select the “target channel” “acp142-mule .....”  
Press “Finish”

## Peer connection created

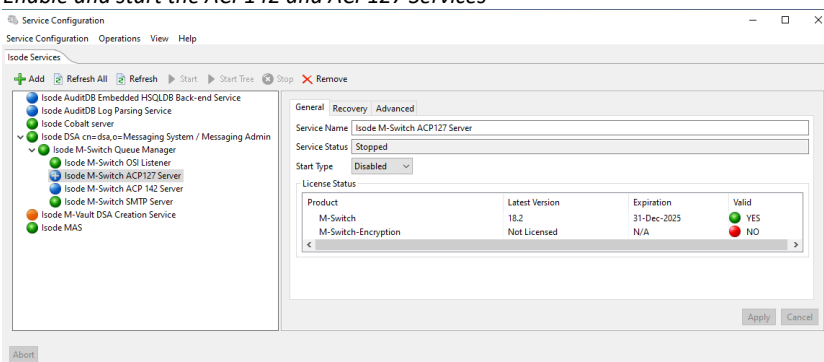


This completes configuration of the Remote ACP142/S4406 mule MTA.

## Complete the Service Configuration

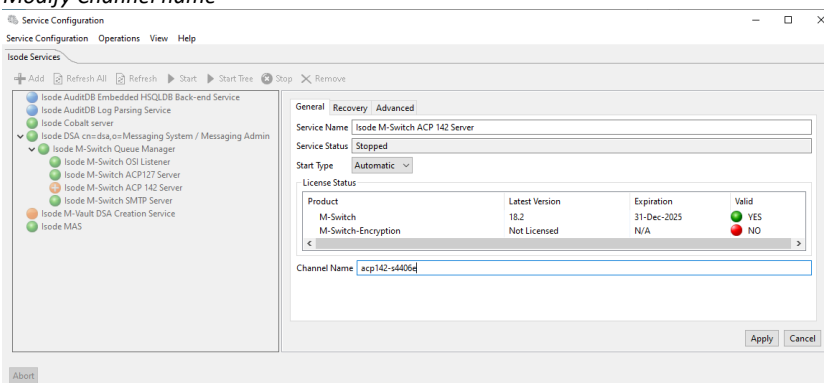
At this stage you can now start the ACP142 and ACP127 Services. Using the Isode Service Configuration Tool.

### Enable and start the ACP142 and ACP127 Services



Change the “Isode M-Switch ACP142 Server” and “Isode M-Switch ACP127 Server” “Start Type” to “Automatic” using the dropdown and click “Apply” for each.

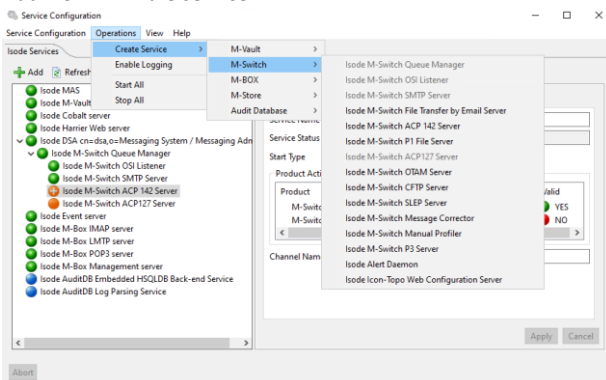
### Modify Channel name



When modifying the ACP 142 Server service, ensure that the channel name is “acp142-s4406e”

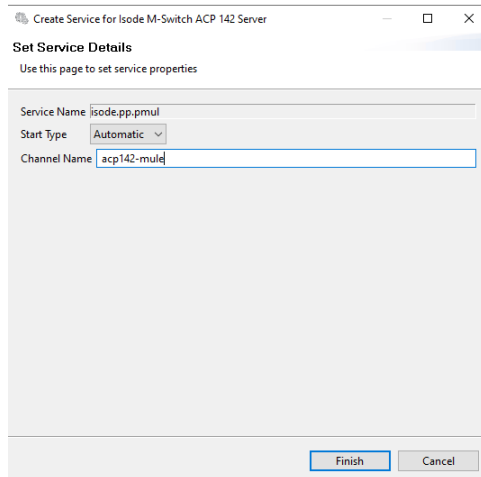
To transport non mmhs messages using mule, add an additional acp142 service.

### Add ACP142 Mule service



Select “Operations/Create Service/M-Switch/Isode M-Switch ACP142 server”.

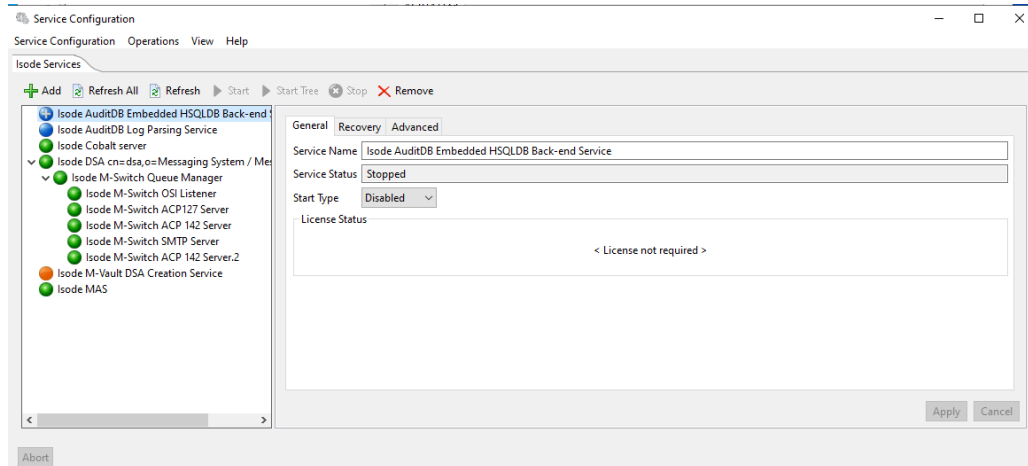
## Name the ACP142-mule Channel



Ensure “Start Type” is “Automatic”  
 Name the channel “acp142-mule”  
 Press “Finish”

Start the services using the option “Operations/Start All”

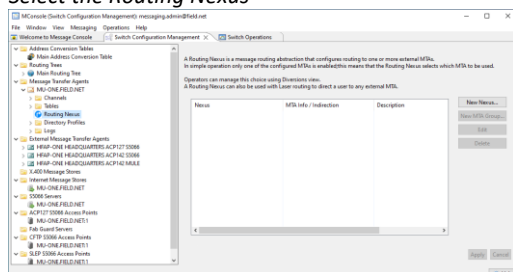
## Services Started



## Configure the Routing Nexus

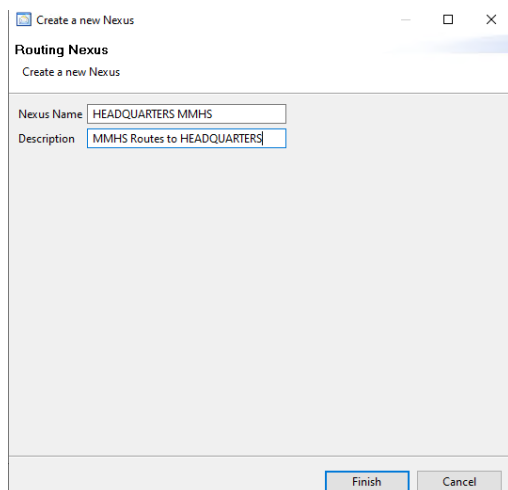
From the MConsole “Switch Configuration Management” view select “Routing Nexus”.

### Select the Routing Nexus



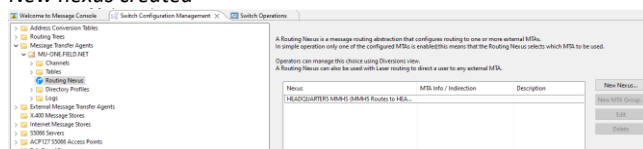
Click “New Nexus...”

### Name the routing Nexus



Enter a “Nexus Name” and Description of your choice. Click “Finish”.

### New nexus created



Select the Nexus you have just created and Click “New MTA Group...”



## Create ACP142 MTA Group

**MTA Group**  
Create a new MTA Group. Select an MTA Information, Channel or an Indirection

Description: MTA Group: HFAP-ONE HEADQUARTERS ACP142 S5066

MTA Information: HFAP-ONE HEADQUARTERS ACP142 S

ACP 127 Channel:

Indirection:

Finish Cancel

Select the ACP142 S5066 MTA and Click “Finish”.

Repeat this for the ACP127 S5066 External MTA you have created.

## Add the ACP127 MTA group

**MTA Group**  
Create a new MTA Group. Select an MTA Information, Channel or an Indirection

Description: MTA Group: HFAP-ONE HEADQUARTERS ACP127 S5066

MTA Information: HFAP-ONE HEADQUARTERS ACP127 S

ACP 127 Channel:

Indirection:

Finish Cancel

Click “Finish”.

## MMHS Nexus with Groups

A Routing Nexus is a message routing abstraction that configures routing to one or more external MTAs. In simple operation only one of the configured MTAs is enabled; this means that the Routing Nexus selects which MTA to be used. Operators can manage this choice using Divisions view. A Routing Nexus can also be used with Layer routing to direct a user to any external MTA.

Nexus	MTA Info / Indirection	Description	Enable
HEADQUARTERS MMHS MMHS R...	HFAP-ONE HEADQUARTERS ACP127	MTA Group: HFAP-ONE HEADQUARTERS A...	<input type="checkbox"/>
HEADQUARTERS MMHS MMHS R...	HFAP-ONE HEADQUARTERS ACP142	MTA Group: HFAP-ONE HEADQUARTERS A...	<input checked="" type="checkbox"/>

New Nexus...  
New MTA Group...  
Edit  
Delete

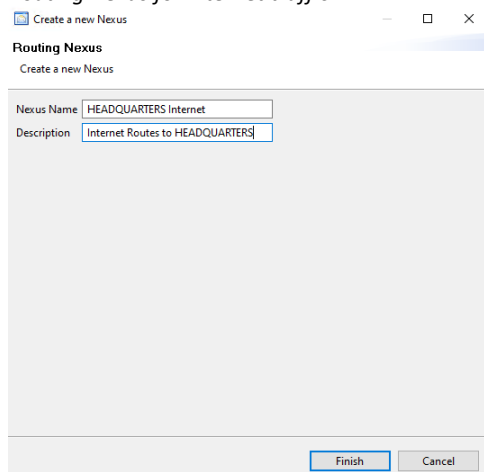
Note that the ACP142 S5066 routing group has been enabled. The switch nexus will use that group for routing unless modified.

Repeat the above steps to create a nexus for internet traffic.

Click “New Nexus...”.

Enter a “Nexus Name” and “Description” of your choice.

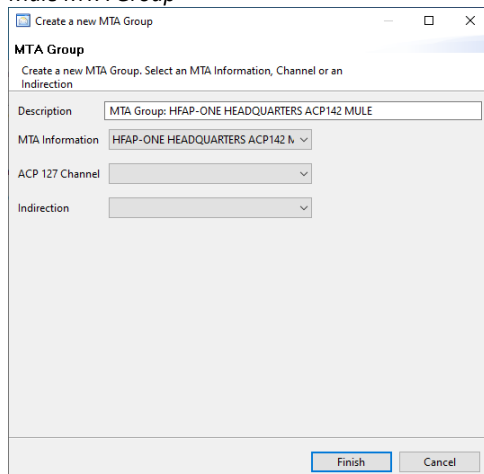
## Routing Nexus for internet traffic



Press “Finish”

Select the Nexus you have just created and Click “New MTA Group...”.

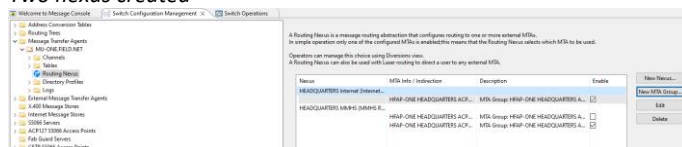
## Mule MTA Group



Select the ACP142 MULE MTA.

Press “Finish”

## Two nexus created

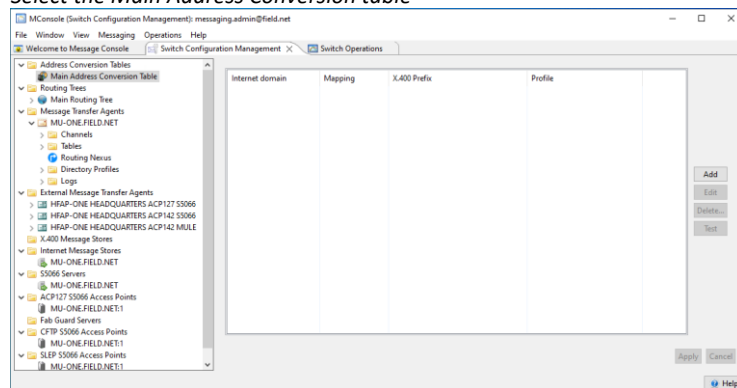


The nexus are now created and we can configure the Address Mapping.

## Configure Address Mapping

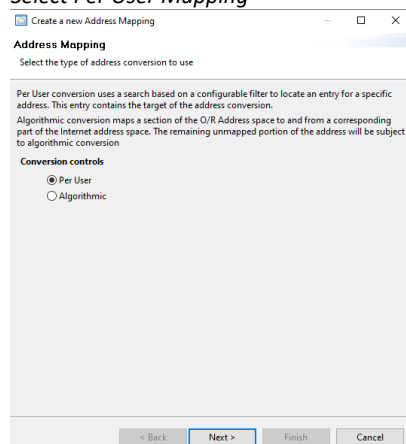
Address mapping is used to convert between SMTP and X400 addresses and vice versa. From the “Switch Configuration Management” view, select “Main Address Conversion Table”.

### Select the Main Address Conversion table



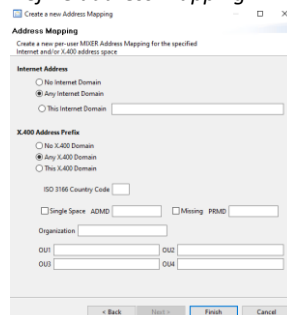
Click “Add”.

### Select Per User Mapping



Leave the default settings  
Click “Next >”.

### Define address mapping



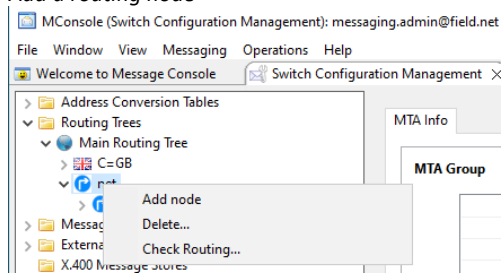
Leave the default settings  
Click “Finish”.

## Configure the Address Routing

From the Mconsole “Switch Configuration Management” view, Select “Main Routing Tree”.

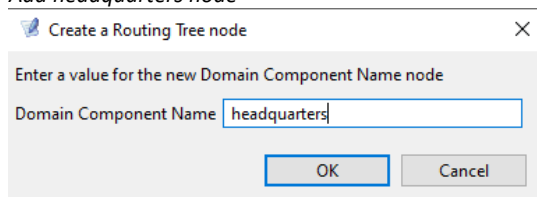
Expand the Routing Tree and right click on “net”, Select “Add node”.

### Add a routing node



Enter “headquarters” for the “Domain Component Name”

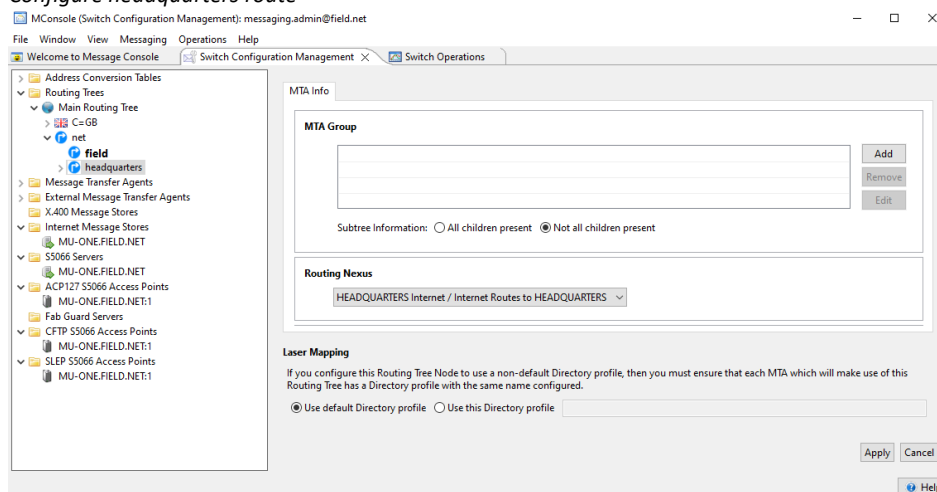
### Add headquarters node



Click “OK”.

In the “Routing Nexus” frame Select the Internet Routing Nexus you have created,

### Configure headquarters route

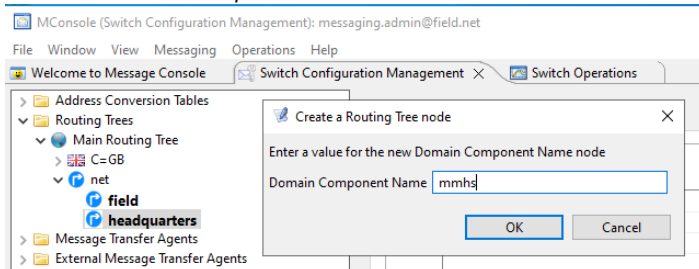


Click “Apply”.

Right click on the new “headquarters” routing node.

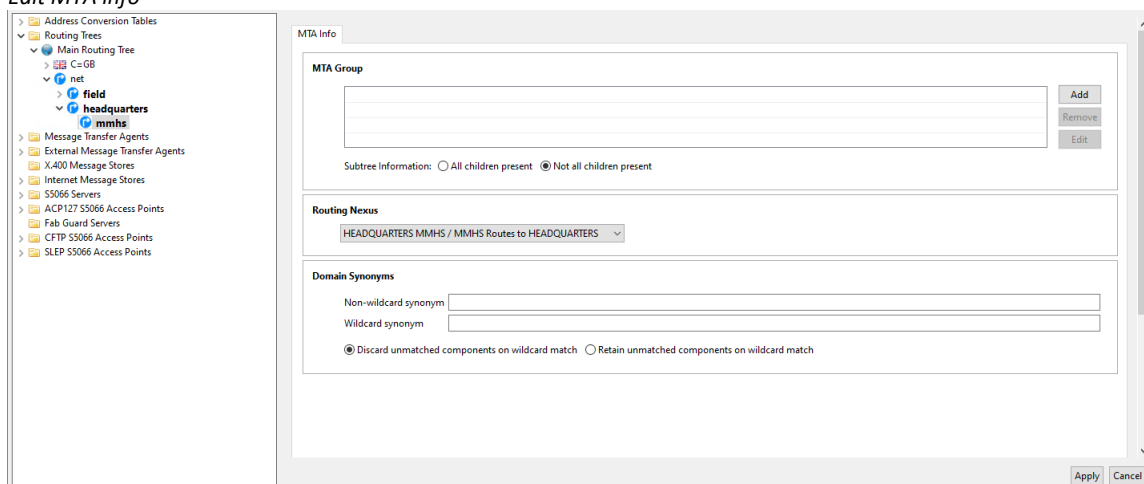
Select “Add node”.

## Add mmhs domain component



Enter “mmhs” for the “Domain Component Name”  
Press “OK”

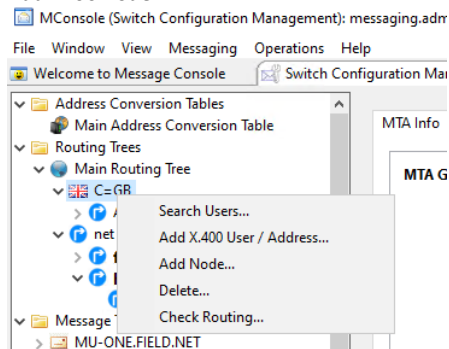
## Edit MTA info



In the “Routing Nexus” frame Select the MMHS Routing Nexus you have created  
Press “Apply”

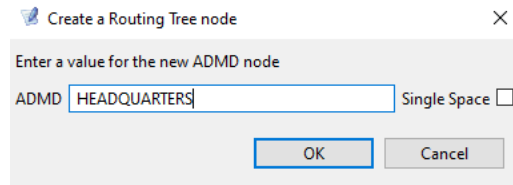
Add the X400 routing entry “a=HEADQUARTERS” by right clicking over “C=GB” in the routing tree

## Add x400 node



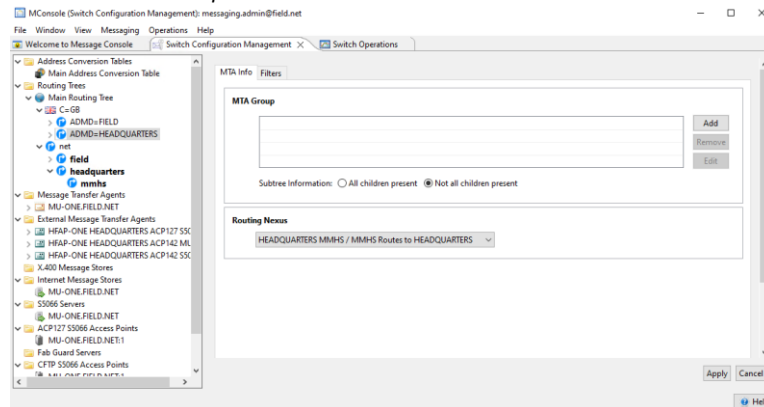
Select “Add node”

## Add ADMD



Provide the ADMD “HEADQUARTERS”  
Press “OK”

## Associate with headquarters nexus

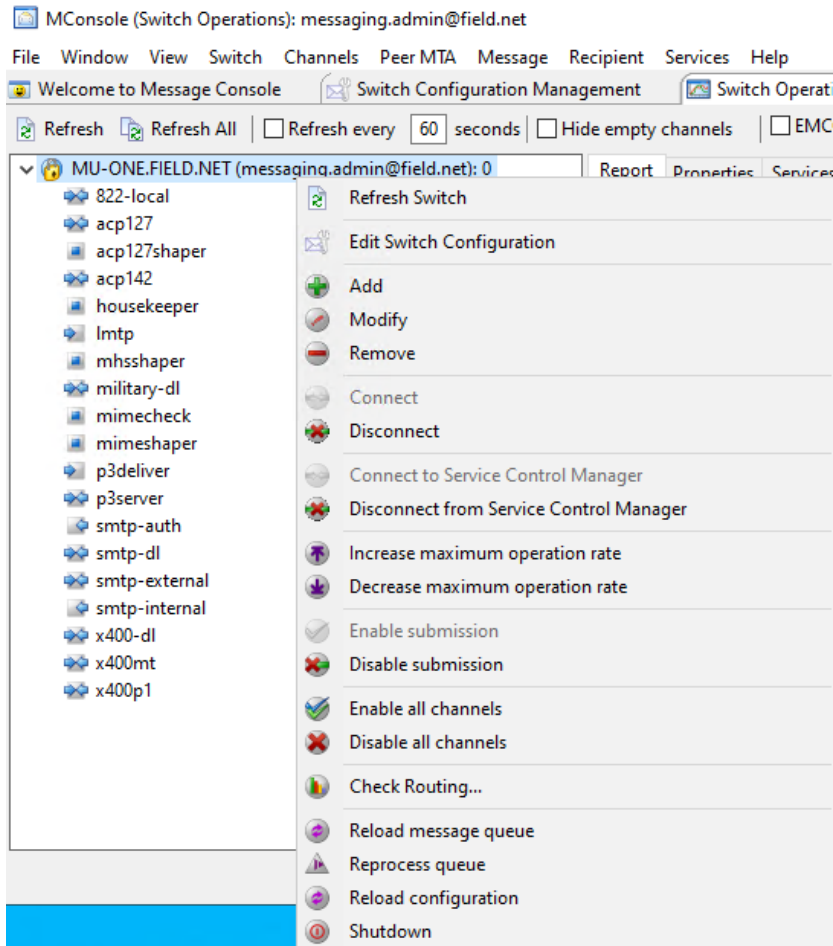


Select the Routing Nexus “HEADQUARTERS MMHS”  
Press “Apply”

## Reload Configuration

At this point it is good practice to “Reload the Configuration”  
From the “Switch Operations” view, Right Click on your MTA.

### Reload the Configuration



Select “Reload configuration”.

## Populate Recipient Information

Recipient information is populated using Cobalt.

In a default evaluation, Cobalt will use TLS when communicating with the directory. So before using Cobalt, we need to create some certificates and use them in enabling LDAP TLS support in M-Vault.

### Create an Isode PKI

These steps explain how to create an Isode PKI to generate certificates. You may skip this step if you already possess a PKI infrastructure.

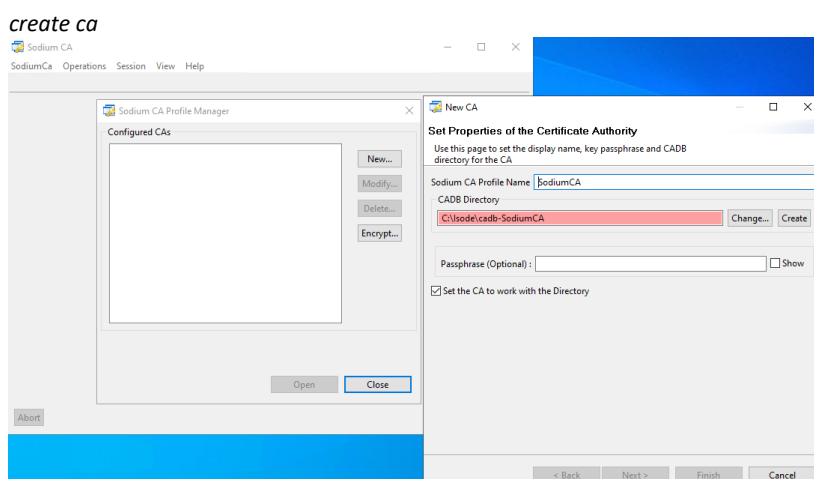
Create the directory “c:\IsodeCerts”

Open “Sodium CA” from the Windows start menu

Click “New”

On “Set Properties of the Certificate Authority” leave Defaults

Click “Create”



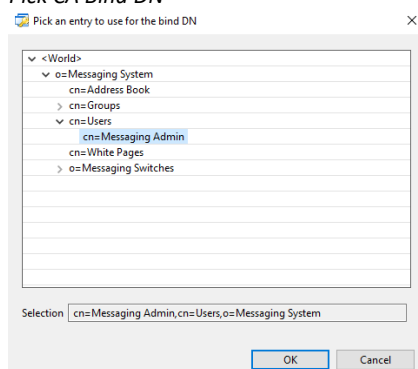
Click “Next”

In “Hostname” type the fully qualified host name (“MU-ONE.FIELD.NET”)

Click “Pick”

Browse to “cn=Messaging Admin,cn=Users,o=Messaging System”

#### *Pick CA Bind DN*



Click “OK”



**Define bind password**

In “Bind Password” type “Secret1+”  
Click “Next >”

**create ca directory entry**

On “Select an Entry for the CA” browse to and select “o=Messaging System”  
Click “Add”

On “Enter RDN for the new CA” type “MU-ONE CA”  
Click “OK”

Click “Next >”

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

On “Certificate Status Sharing” leave Defaults  
Click “Next >”

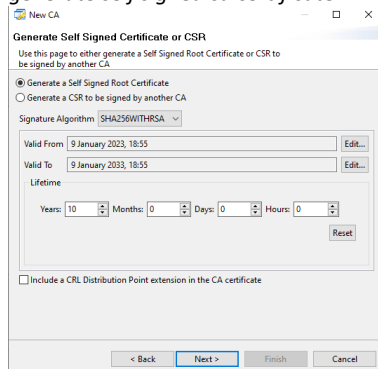
On “Set the CRL Distribution Point for the CA” leave defaults  
Click “Next >”

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

On “Set Basic Constraints and KeyUsage Extension” leave defaults  
Click “Next >”

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

## generate self signed ca certificate



Leave the defaults.

Click “Next >”

On “Root CA Certificate” leave Defaults

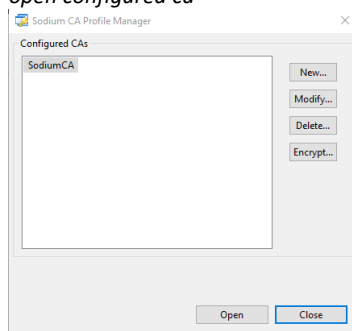
Click “Next >”

On “Finish CA Configuration” press “Finish”

On ”Sodium CA Profile Manager” select “SodiumCA”

Click “Open”

## open configured ca



In “Password” type “Secret1+”

Click “OK”

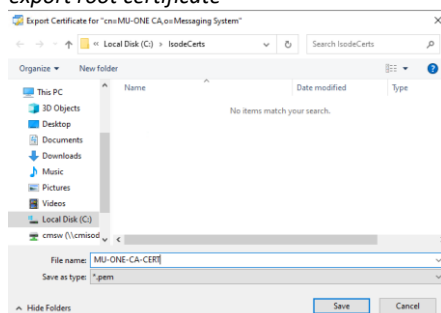
Select “Certificate for cn=MU-ONE CA, o=Messaging System”

Press “Export PEM ..”

On “Export Certificate for “cn=MU-ONE CA, o=Messaging System”, browse to “c:\IsodeCerts”

Change Filename to “MU-ONE-CA-CERT.pem”

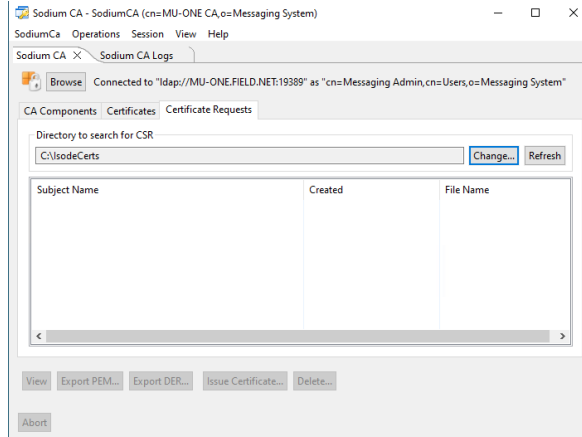
## export root certificate



Press “Save”

On “Certificate for cn=MU-ONE CA,o=Messaging System” exported Click “OK”  
Change to “Certificate Requests” tab

*CSR directory changed*

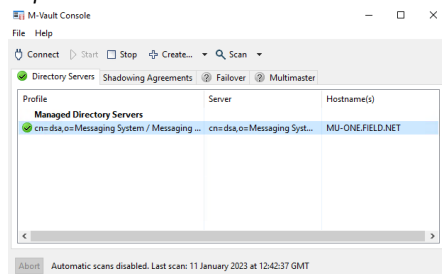


Change “Directory to Search for CSR” to “C:\IsodeCerts”

**Configure M-Vault to Support TLS**

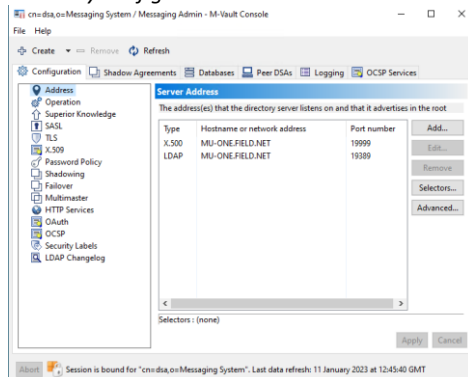
From the Windows Start menu, open “M-Vault console” and provide the password “Secret1+”

*Populated M-Vault console*

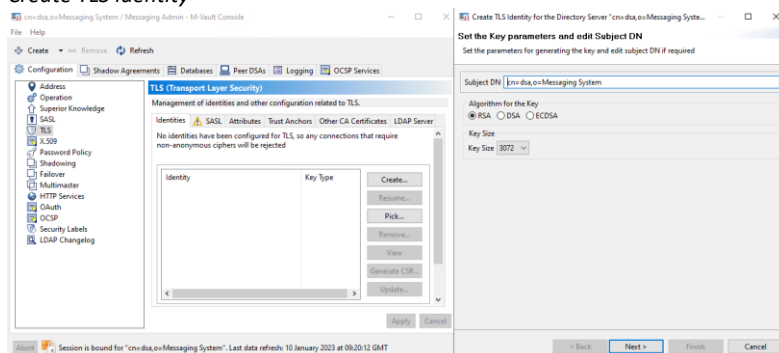


Double Click on the “Managed Directory server”

*Directory configuration*



Select “TLS” on the left-hand side of the “Configuration” tab  
On the “Identities” tab Press “Create”

**Create TLS identity**

On “Set the Key parameters and edit Subject DN” leave defaults

Click “Next >”

On “Select and add Subject Alternative names and Clearance” leave defaults

Click “Next >”

On “Select X.509 Extensions”, leave defaults

Press “Next >”

On “Certificate Request Contents” leave defaults

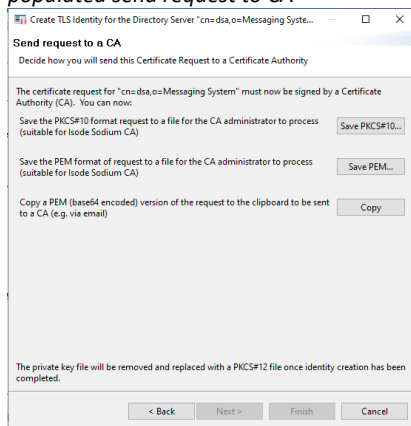
Press “Next >”

On “Send Request to a CA” press “Save PEM ...”

On “Choose a Directory” browse to “C:\IsodeCerts”

Click “Select Folder”

Back on “Send Request to CA” leave defaults

**populated send request to CA**

Click “Next >”

In 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 >”

On “Set Validity and Signature Algorithm for the Certificate” leave defaults

Click “Next >”

On “Generated Certificate” press “Finish”

On “CSR Signed” Click “OK”.

Back in in M-Vault Console:

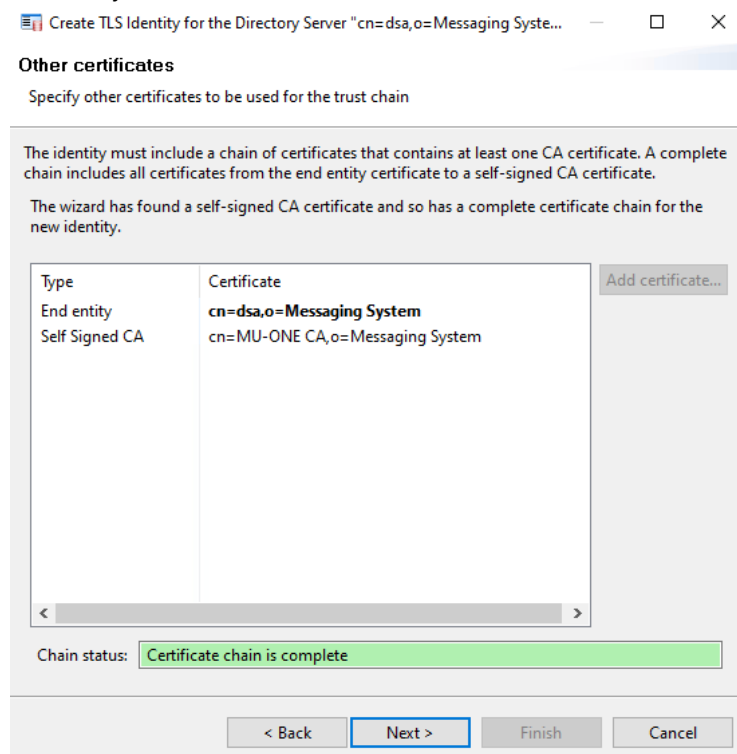
Select “The CA has provided a certificate”

Click “Next >”

On “User Certificate” leave defaults

Click “Next >”

### Other certificates



On “Other Certificates” leave defaults

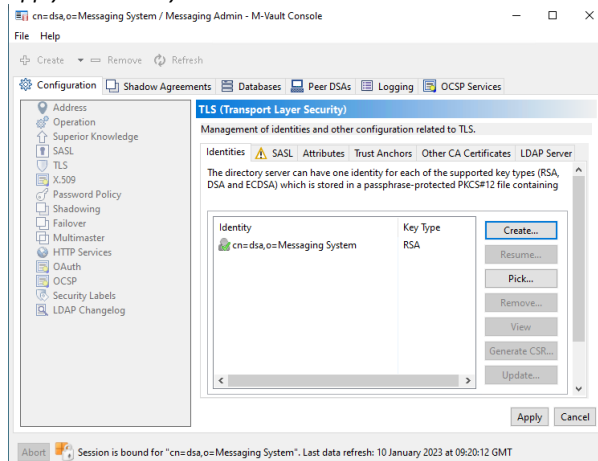
Click “Next >”

On “Finish directory servers Identity creation” leave defaults

Click “Finish”

On “Trust Root CA Certificate” dialogue click “Yes”

### apply TLS identity



On “Configuration” tab press “Apply”  
Close the “M-Vault Console” configuration dialogue

Go to the “Isode Service Configuration” tool.

Select “Operations/Stop all”

Wait for the services to stop

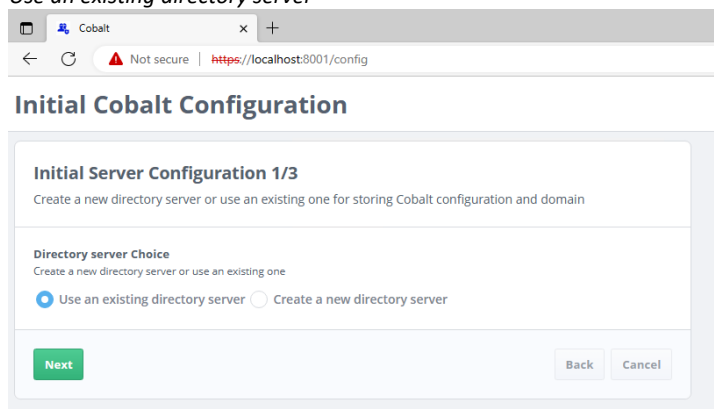
Select “Operations/Start all”

## Initial Cobalt Configuration.

Browse to “https://localhost:8001”

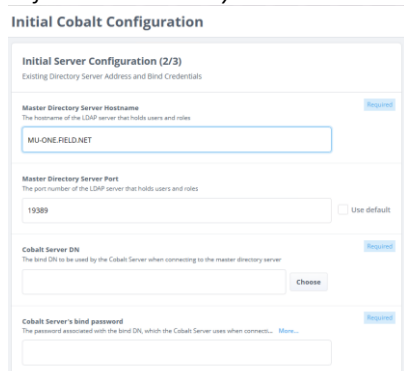
The browser will provide a security warning. Choose an option to override the warning

Use an existing directory server



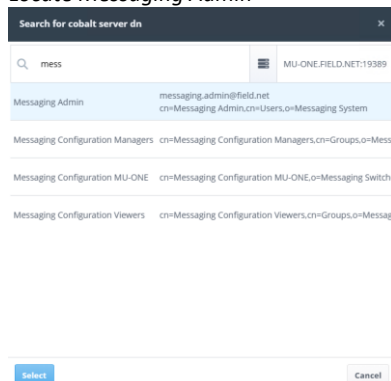
On “Initial Server Configuration” leave as “Use an existing directory server”  
Press “Next”

Define Cobalt directory server



Ensure the “Master Directory Server Hostname” correctly references your DSA  
Click “Choose”.

Locate Messaging Admin



Start typing your “Initial Directory User”, Select it and Click “Select”.

## Initial directory user selected

**Master Directory Server Hostname** (Required)  
The hostname of the LDAP server that holds users and roles  
MU-ONEFIELD.NET

**Master Directory Server Port** (Required)  
The port number of the LDAP server that holds users and roles  
19389  Use default

**Cobalt Server DN** (Required)  
The bind DN to be used by the Cobalt Server when connecting to the master directory server  
cn=MessagingAdmin,com=Users,ou=MessagingSystem

**Cobalt Server's bind password** (Required)  
The password associated with the bind DN, which the Cobalt Server uses when connect...

**TLS Identity Check** (Required)  
Perform hostname check. [More...](#)  
 False  True  Use default

Scroll down and enter the Password for the “Initial Directory User”.  
Set “TLS Identity Check” to “False”  
Click “Next”.

## Define Cobalt domain

**Initial Server Configuration (3/3)**  
Details about location of users and configuration

**Domain** (Required)  
The domain to use for the initial Cobalt Administrator  
field.net

**Admin's Full Name** (Required)  
Name of the initial Cobalt Administrator  
Cobalt Admin

**Admin's mail ID** (Required)  
ID of the initial Cobalt Administrator to be used for logging into Cobalt  
cobalt.admin @field.net

Set the “Domain” to be “field.net”  
Enter a Name of your choice for the “Admin’s Full Name”.  
We will use “Cobalt Admin”  
Scroll down.

## Specify Cobalt admin name

**Domain** (Required)  
The domain to use for the initial Cobalt Administrator  
field.net

**Admin's Full Name** (Required)  
Name of the initial Cobalt Administrator  
Cobalt Admin

**Admin's mail ID** (Required)  
ID of the initial Cobalt Administrator to be used for logging into Cobalt  
cobalt.admin @field.net

**Admin's password** (Required)  
Admin's password  
Secret1\*

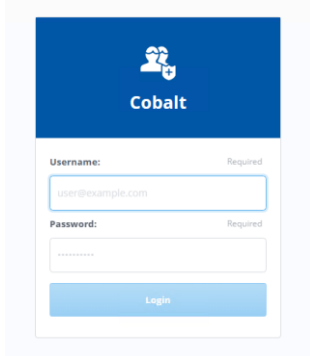
**Domain Naming Context** (Required)  
Naming context to which the domain belongs  
o=MessagingSystem

Enter a Password of your Choice for the “Admin’s Password”.  
Click “Finish”.



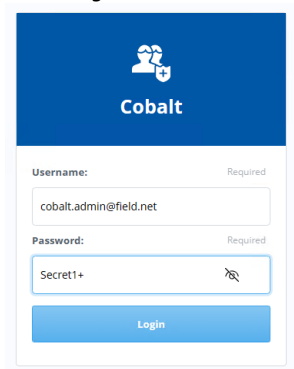
You will be presented with the Cobalt login screen.

*Cobalt Login Screen*



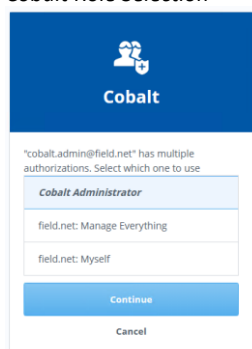
Enter the Cobalt Admin Email address and password

*Cobalt login credentials*



Click “Login”.

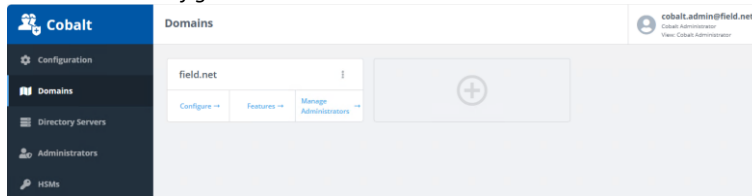
*Cobalt Role Selection*



Select “Cobalt Administrator” role.  
Click “Continue”.

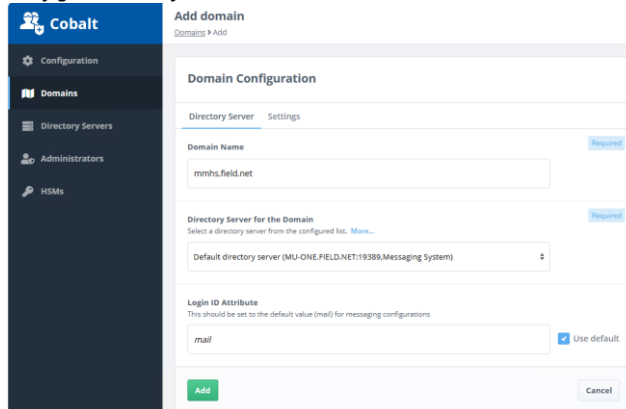
## Define Cobalt Domains and Features

### Initial domain configuration



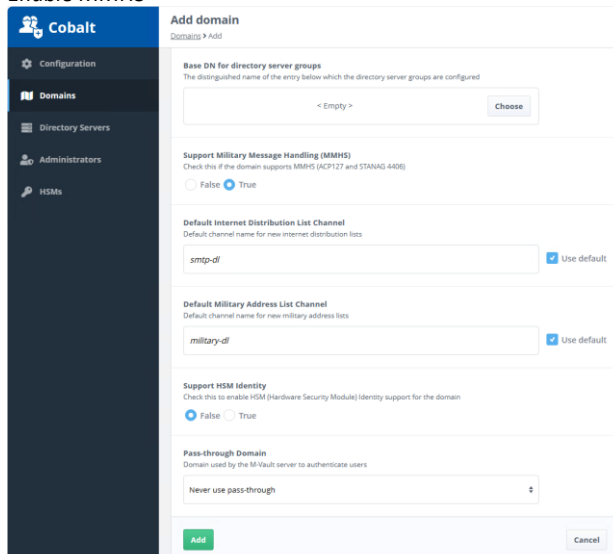
Press the “+”  
For “Domain Name” type “mmhs.field.net”

### Configure mmhs.field.net domain



Change to “Settings” tab.

### Enable MMHS



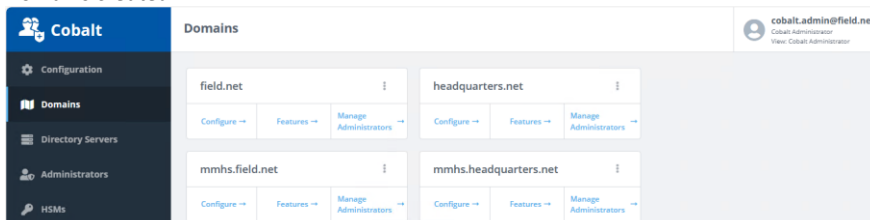
Set “Support Military Messaging Handling (MMHS)” to “True”  
Press “Add”

Repeat the above steps to add the domain “mmhs.headquarters.net”

Repeat the above steps to create the domain “headquarters.net” but for this domain, don’t enable Military Messaging.

You should now have 4 domains:

### Domains created

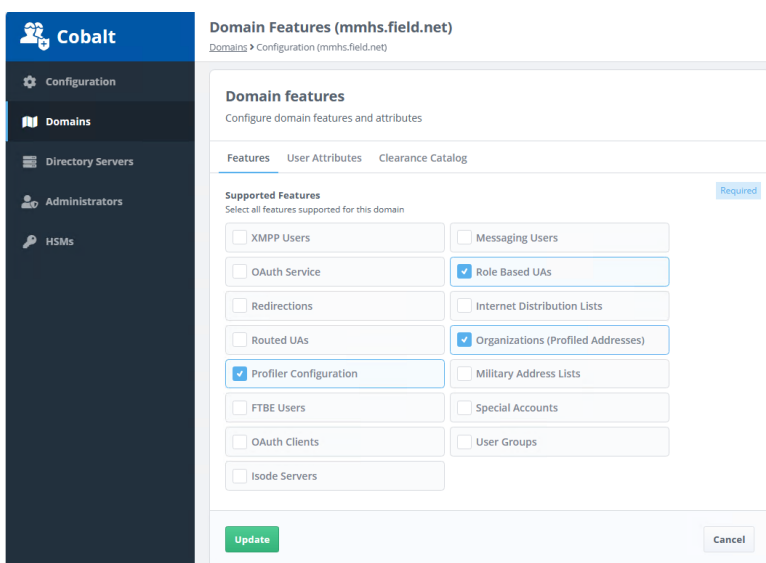


Click “Features” of the domain “mmhs.field.net”

Ensure only the following domain features are checked

- Role Based UAs
- Organizations (Profiled Addresses)
- Profiler Configuration

mmhs.field.net domain features



Press “Update”

Repeat the last steps so that the domain “mmhs.headquarters.net” has only the following features:

- Role Based UA’s
- Organizations (Profiled Addresses)

For the domain “field.net” enable only the features “Messaging Users” and “Redirections”

For the domain “headquarters.net” enable only the features “Messaging Users”

Press “Manage Administrators” under “mmhs.field.net”

### mmhs.field.net administrators

Name	Domain	Number of Occupants
Manage Everything	mmhs.field.net	0
Users and Roles Manager	mmhs.field.net	0
Users Manager	mmhs.field.net	0
Roles Manager	mmhs.field.net	0
OAuth Administrators	mmhs.field.net	0
Users and Roles Viewer	mmhs.field.net	0

Select “Manage Everything”

### Mmhs.field.net manage everything

**mmhs.field.net: Manage Everything**

Domains > Administrators (mmhs.field.net) > Manage Everything

**Cobalt Administration Role**  
Manage users that can occupy this administration role

Domain Required  
mmhs.field.net

Name Required  
Manage Everything

Users that can occupy this role  
< Empty > Search...

Update Cancel

Press “Search”

Change the domain to “field.net”

Type “c” in search box

Check “Cobalt Admin”

## Search for Cobalt admin

Press “Select”

## Cobalt Admin Manages everything

Press “Update”

## mmhs.field.net has a manager

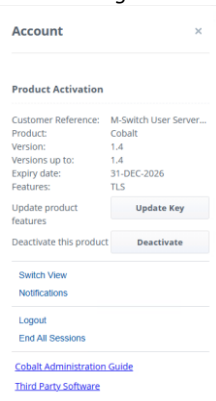
Name	Domain	Number of Occupants
Manage Everything	mmhs.field.net	1
Users and Roles Manager	mmhs.field.net	0
Users Manager	mmhs.field.net	0
Roles Manager	mmhs.field.net	0
OAuth Administrators	mmhs.field.net	0
Users and Roles Viewer	mmhs.field.net	0

Make cobalt.admin@field.net Full administrator of the domains “headquarters.net” and “mmhs.headquarters.net” by following the instructions above.

## Configure the local mailboxes and remote users

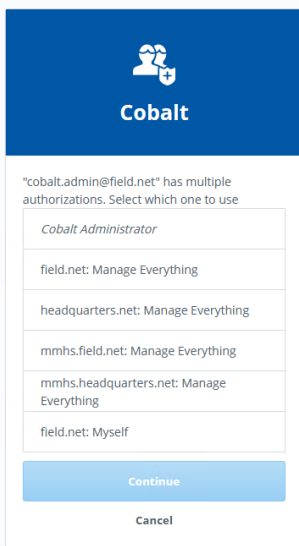
We will switch to the “field.net: Manage Everything” Role. Click on “cobalt.admin@field.net.net” in the top right corner.

### Cobalt change role



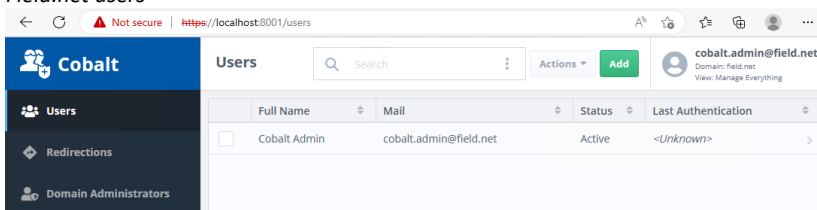
Click “Switch View”.

### Switch to field.net view



Select “field.net: Manage Everything”  
Click “Continue”.

### Field.net users



With “Users” selected on the left-hand side Click “Add”.

Populate details for “Jack Sparrow”, starting with his name. Since this is the local domain, ensure Jack is provided with a password to authenticate. You may want to add

a wide variety of user information via this dialogue, which stores information in the directory. This information may also include picture or certificate information. Please feel free to explore the tabs available to see the information that could be stored.

### Populate Jack Sparrow

The screenshot shows the 'Add User' dialog in Cobalt. The 'User Entry' section is expanded, showing the following fields:

- Full Name:** Jack Sparrow (Required)
- Given Name:** Jack
- Surname:** Sparrow (Required)
- User Password:** Secret1+ (with Show and Generate buttons)

Scroll to the bottom of the page and press “Add”

### Add Jack Sparrow

The screenshot shows the 'Add User' dialog in Cobalt for the domain 'cobalt.admin@map-one.headquarters.net'. The 'User Password' field is visible, along with the following fields:

- Primary Email Address:** arthur.love@headquarters.net (Required)
- Alternative Email Addresses:** @headquarters.net
- Entry Type:** User

Note that “Jack Sparrow” has been added to the directory

### Jack Sparrow added

Full Name	Mail	Status	Last Authentication
Cobalt Admin	cobalt.admin@field.net	Active	<Unknown>
Jack Sparrow	jack.sparrow@field.net	Active	<Unknown>

Switch Cobalt view to the “mmhs.field.net” domain  
Select “Role Based UA’s”

### Empty Role based UA’s

The screenshot shows the 'Role Based UAs' dialog in Cobalt for the domain 'cobalt.admin@field.net'. The dialog is empty, showing only the 'Add' button.

Click “Add”  
In “Display name” type “FIELD CAPTAIN”  
Ensure “Role Email address” is “captain”

## Populate Role

**Add Role Based UA**  
Role Based UAs > Add

**Role Based UA**  
A role based mailbox, specifying users that can occupy the role

Role Contact Photo Certificate MMHS Messaging Redirection

**Display Name** Required  
FIELD CAPTAIN

**Role Email Address** Required  
captain @mmhs.field.net

**Alternative Email Addresses**  
Alternative email addresses for the role  
@mmhs.field.net x +

**Users that can occupy the role**  
Distinguished Names of users that occupy this role  
< Empty > Choose

Press “Choose” to select a role occupant for “FIELD CAPTAIN”

Search for “j” in domain “field.net”

Check “Jack Sparrow”

Press “Select”

## select Role Occupant

Search for users that can occupy the role

Search: j @ field.net

Select All

<input checked="" type="checkbox"/>	Jack Sparrow	jack.sparrow@field.net cn=Jack Sparrow,cn=Users,cn=field.net,cn=Cobalt Data,ou=...
-------------------------------------	--------------	---

Jack Sparrow x

Select Cancel

Change to “MMHS” tab.



## Populate MMHS information

**Add Role Based UA**  
 Role Based UAs > Add

A role based mailbox, specifying users that can occupy the role

Role Contact Photo Certificate **MMHS** Messaging Redirection

**Plain Language Address**  
 Plain language address name used in ACP127

FIELD CAPTAIN

**Routing Indicator**  
 Routing indicator used in ACP127 addressing

RIFIELD

**STANAG 4406 Address**  
 STANAG 4406 address (X-400 O/R Address). [More...](#)

/CN=FIELD CAPTAIN /P=S4406/A=FIELD/C=GB/

**Maximum Plain Text Line Length**  
 This is used for ACP127 and is generally set to a value of 69. [More...](#)

**Charset Restrictions**  
 Allowed charset for messages sent to this role

No option selected

**Add** **Cancel**

Populate “Plain Language Address”, “Routing Indicator” and “Stanag 4406 address” from the table at the start of this guide.  
 Scroll to the bottom of the page and press “Add”

Note that the Role has been added to the directory.

## Role added

Cobalt		Role Based UAs		Delete...	Add	cobalt.admin@field.net Contact: mmhs.field.net View Manage Everything	
Name	Mail						
<input type="checkbox"/> FIELD CAPTAIN	captain@mmhs.field.net						

Select “Organizations (Profiled Addresses)”

## Empty Organizations

Cobalt		Organizations (Profiled Addresses)		Delete...	Add
<p>Role Based UAs</p> <p><b>Organizations (Profiled A...</b></p> <p>Domain Administrators</p>					

Click “Add”  
 In “Name” type “BLACK PEARL”  
 Ensure “Email address” is “blackpearl”

## Populate Organization

**Add Organization (Profiled Address)**  
Organizations (Profiled Address) → Add

**Organizations (Profiled Addresses)**  
This address represents an organization: emails sent to this address will be processed by the profiler channel, which will distribute the mail according to rules defined for that channel. Domains that use 'Draft and Release' can use the 'Members' tab, to configure a list of roles that are allowed to send messages that come 'from' this organization.

Profiled Address Members Messaging MMHS Photo Advanced

Name Required  
BLACK PEARL

Email Address Required  
blackpearl @mmhs.field.net

Add Cancel

Select the “Members” tab

## Organization Empty Members

**Add Organization (Profiled Address)**  
Organizations (Profiled Address) → Add

**Organizations (Profiled Addresses)**  
This address represents an organization: emails sent to this address will be processed by the profiler channel, which will distribute the mail according to rules defined for that channel. Domains that use 'Draft and Release' can use the 'Members' tab, to configure a list of roles that are allowed to send messages that come 'from' this organization.

Profiled Address **Members** Messaging MMHS Photo Advanced

**Sending Roles**  
List of roles that are allowed to draft or send messages with "From:" set to the organization  
< Empty > Choose

**Member Capabilities**  
Specify the Draft and Release capabilities for each member  
<No Organization Members>

Add Cancel

Press “Choose”

## Select sending roles

**Select sending roles** [X]

mmhs.field.net

Select All

FIELD CAPTAIN captain@mmhs.field.net  
cn=FIELD CAPTAIN,cn=RoleUAs,cn=mmhs.field.net,cn=Col

FIELD CAPTAIN [X]

Select Cancel

Select “FIELD CAPTAIN”

Press “Select”

Check “Can Release”  
 Select the dropdown and select “Always sends direct”

*Populated Organization members*

Change to “MMHS” tab.

*Populate MMHS information*

Populate “Plain Language Address”, “Routing Indicator” and “Stanag 4406 address”.  
 Press “Add”

Note that the Organization has been added to the directory.

Name	Mail
<input type="checkbox"/> BLACK PEARL	blackpearl@mmhs.field.net

Switch Cobalt view to “field.net” domain

Select “Redirections”  
 Press “Add”

## Postmaster redirection

**Add Redirection**

Redirection from one or more email addresses in the domain to another email address

**Name** Required  
String describing an identifier for this redirection  
POSTMASTER

**Any message sent to this email address** Required  
postmaster @field.net

or to any of the the following addresses  
@field.net x +

**will be redirected to this email address** Required  
radio.operator@mmhs.field.net Search...

**Entry Type**  
Type of entity that this redirect points to  
Role

**Add** **Cancel**

Populate the “POSTMASTER” redirection with “Name”, “address” and “redirected address” “radio.operator@mmhs.field.net”

Select Entry type “Role”

Press “Add”

Note that the redirection for “postmaster” has been added.

## Postmaster redirection added

Name	Mail sent to	Is redirected to
POSTMASTER	postmaster@field.net	radio.operator@mmhs.field.net

Repeat the above steps to add the redirection “Garbled Data”

Garbled data Redirection

**Cobalt**

Users

Redirections

Domain Administrators

**Add Redirection**

Redirections > Add

cobalt.admin@field.net  
Domain: field.net  
View: Manage Everything

Redirection from one or more email addresses in the domain to another email address

**Name** Required  
String describing an identifier for this redirection

GARbled DATA

**Any message sent to this email address** Required

garbled.data @field.net

or to any of the the following addresses

@field.net x +

**will be redirected to this email address** Required

radio.operator@mmhs.feld.net Search...

**Entry Type**  
Type of entity that this redirect points to

Role

Add the remaining users, roles and organizations into the relevant domains from the table at the start of this document. Users in the headquarters.net domain will not require a password.

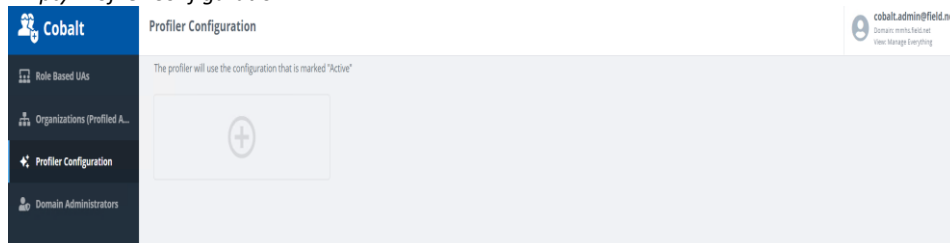
The gateway entity gateway@field.net does not require a mailbox or redirection.

## Configure a Profiler Rule

Switch Cobalt view to the “mmhs.field.net” domain

Select “Profiler Configuration” from the left pane

### Empty Profiler Configuration

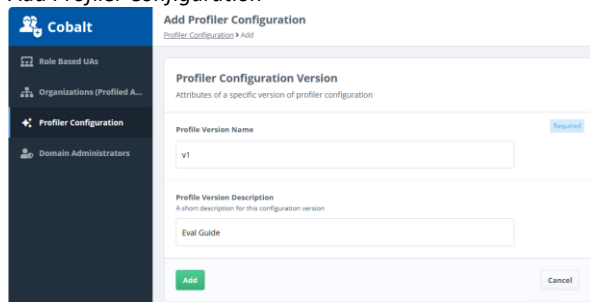


Click the “+” button

In “Profile Version Name” type “v1”

In “Profile Version Description” type “Eval Guide”

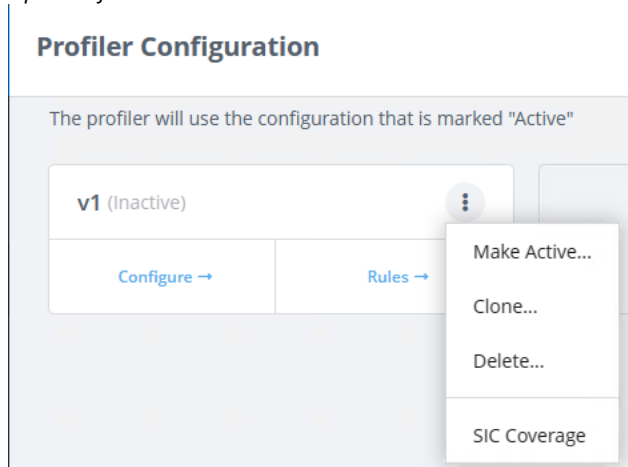
### Add Profiler Configuration



Press “Add”

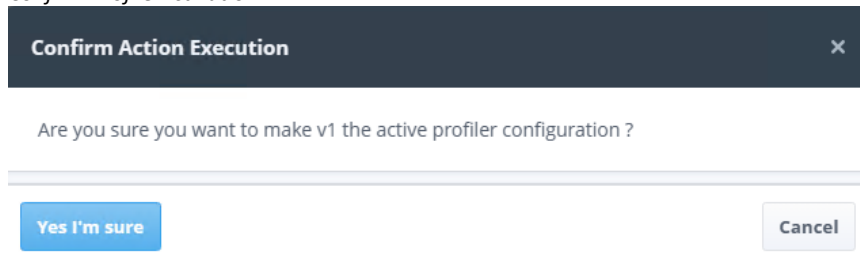
Select the 3 dots to the right of v1 (inactive)

### Open Profiler Menu



Select the option “Make Active ...”

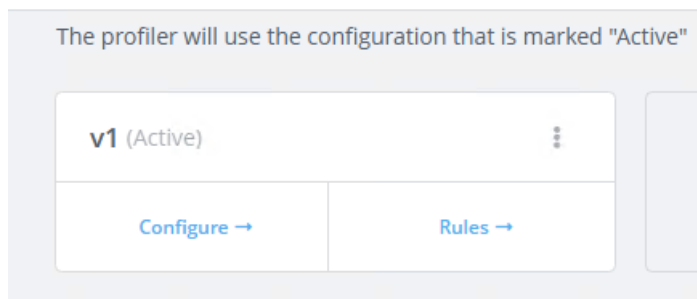
## Confirm Profile Activation



Press “Yes I’m sure”

## Profile Activated

### Profiler Configuration

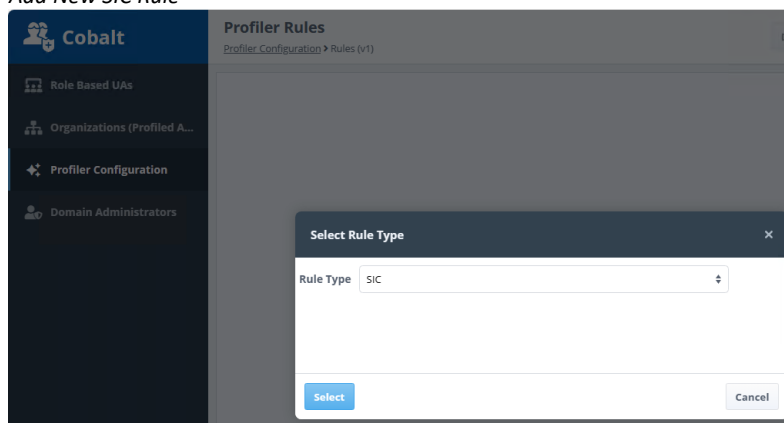


Select “Rules”

Click “Add”

Set the “Rule Type” to “SIC”

## Add New SIC Rule



Click “Select”

In “Rule Name” type “SIC Rule A1A”

## New Profiler Rule

### Add Profiler Rule (SIC)

Profiler Configuration > Rules (x) > Add

Under “Target Organization” Press “Search”

### Select Organization to be Profiled

Select “BLACK PEARL”  
In “SIC to match” type “A1A”

Under “Action Addresses” press “Search”

### Select Action Address



Select “FIELD CAPTAIN”  
Press “Select”

Add “FIELD RADIO OPERATOR” to “Info Addresses”

*Populated Profiler Rule*

**Add Profiler Rule (SIC)**

Profiler Configuration > Rules (v1) > Add

SIC Rule A1A

**Rule Type**  
Rule type

**Target Organization**  
If omitted, then any organization will be matched

Search...

**SIC to match**  
SICs containing a complete SIC (e.g., A1A) or a pattern where \* matches one or more cha... [More...](#)

**Action Addresses**  
List of action addresses

Name	Email	
FIELD CAPTAIN	captain@mmhs.field.net	✕

Search...
Add To List

**Info Addresses**  
List of info addresses

Name	Email	
FIELD RADIO OPERATOR	radio.operator@mmhs.field.net	✕

Click “Add”

*Profiler Rule Created*

**Cobalt**

Role Based UAs

Organizations (Profiled A...

**Profiler Rules**  
Profiler Configuration > Rules (v1)

Delete...
Add

Name	Type	Target Organization
<input type="checkbox"/> SIC Rule A1A	sic	RIFIELD/BLACK PEARL

**cobalt.admin@field.net**  
Domain: mmhs.field.net  
View: Manage Everything

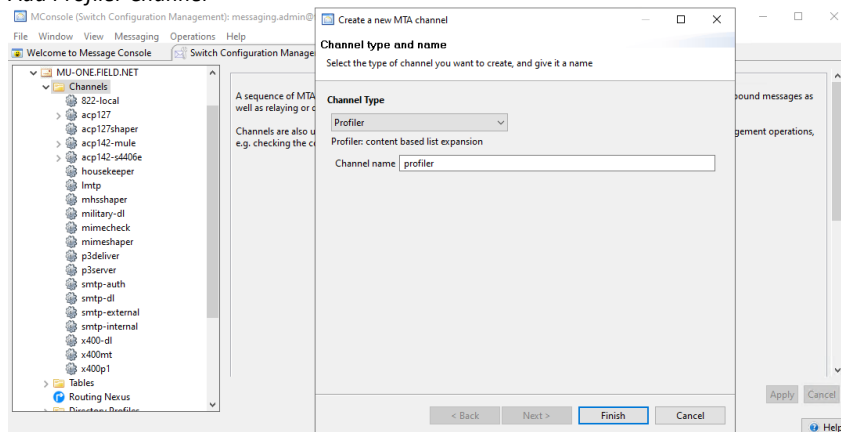
## Configure the Profiler Channel

From the “Mconsole” “Switch Configuration Management” view Right Click “Channels”

Select “New Channel”

Select “Profiler” from the dropdown.

### Add Profiler Channel



Press “Finish”

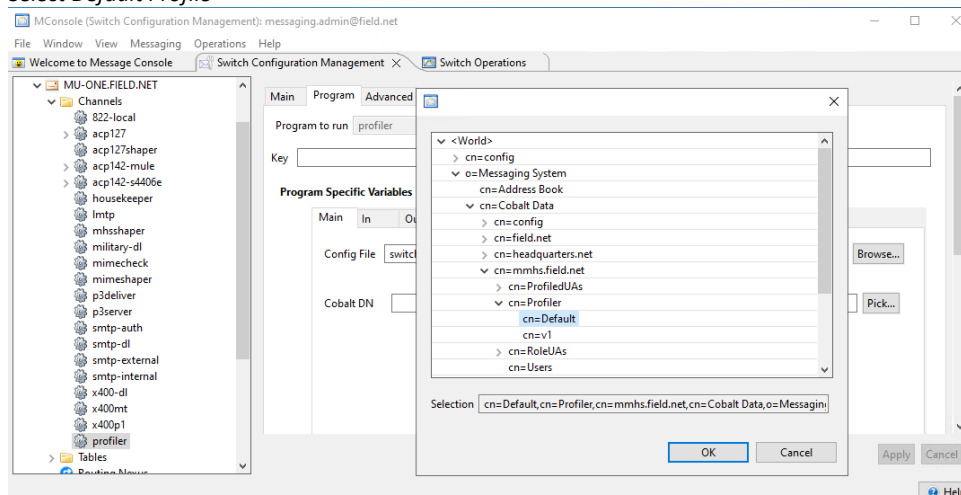
Select the new “profiler” channel.

Select the “Program” tab

Select “Pick”

Browse to “cn=Default,cn=Profiler,cn=mmhs.field.net,cn=Cobalt Data,o=Messaging System”.

### Select Default Profile



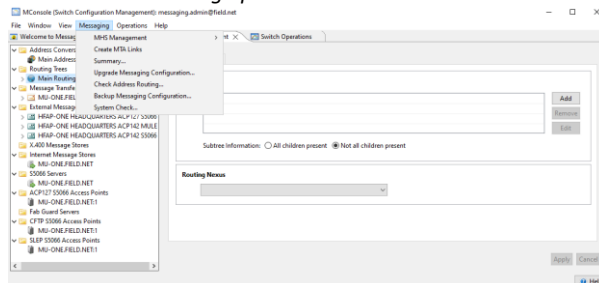
Click “OK”

Click “Apply”

## Test Message Routing

We need to check that messages are going to be routed as we expect. From the “MConsole” “Switch Configuration Management” view Top Menu.

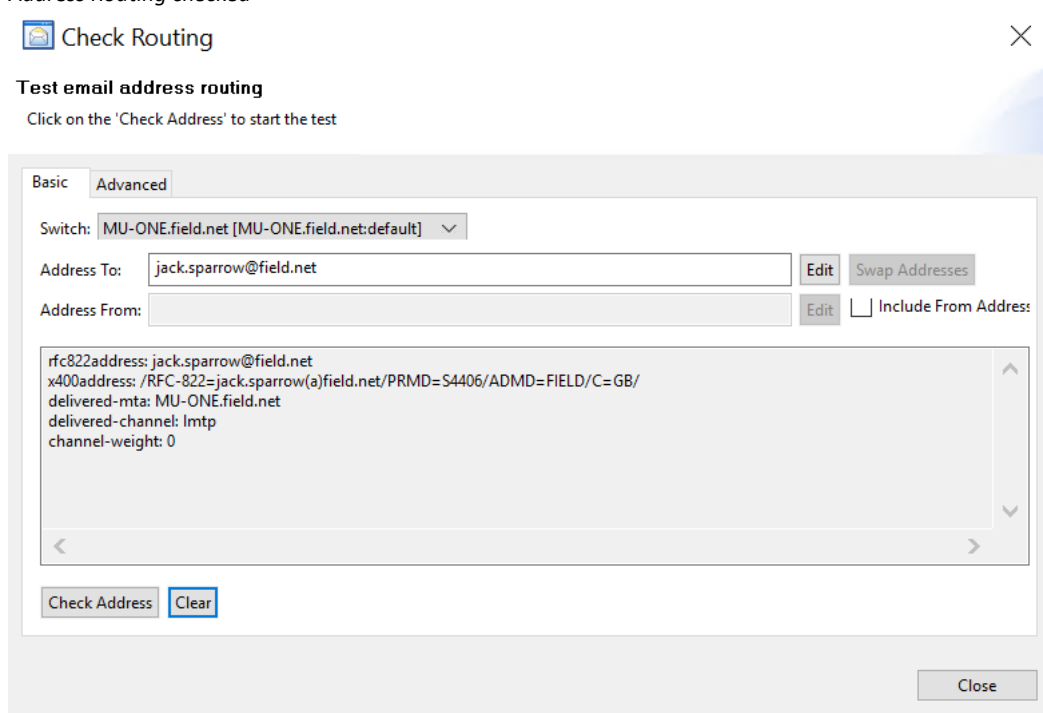
*Check address routing option*



Select “Messaging→Check Address Routing..”

Enter the Address you want to check the routing for and press “Check Address”

*Address Routing checked*



Note the address translation and routing information provided.

Changing routing nexus information will change routing generated in this tool.

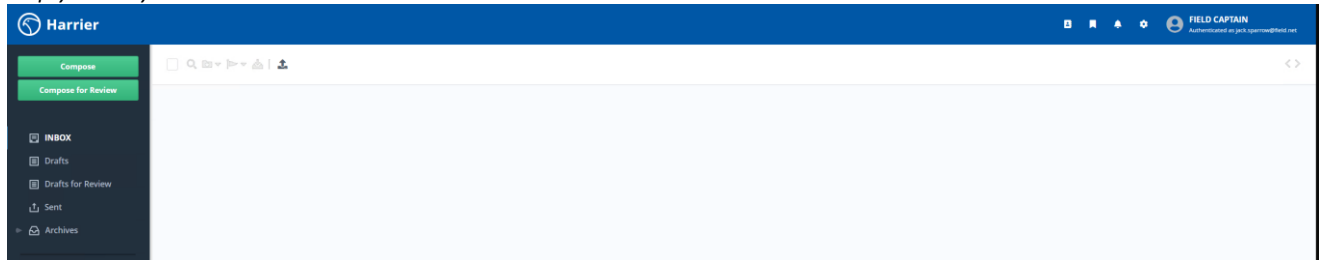
## Test Profiler

Browse to Harrier at <http://localhost:9090>

Log in as `jack.sparrow@field.net`

Jack sparrow occupies the role “FIELD CAPTAIN”. It can be seen from the top right hand corner that Harrier is presenting the “FIELD CAPTAIN” mailbox.

### Empty Military Mailbox



Click “Compose”

Populate the following field data:

FROM: BLACK PEARL

ACTION: BLACK PEARL

SICS: A1A

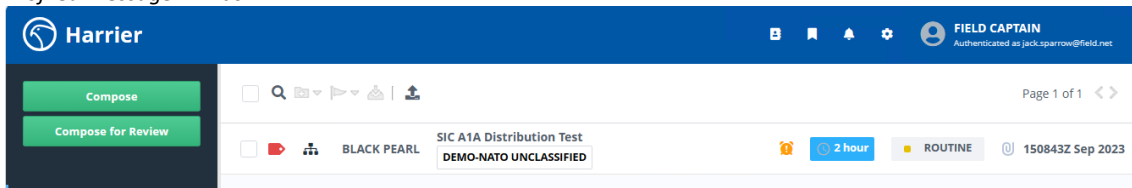
Subject: SIC A1A Distribution Test

Message: Profiler Test

### Create Military Message for Distribution

Click “Send”

## Profiled Message in Inbox



When the message arrives, note the icon indicating that the message is the result of a distribution.

Open the message  
Click “Show details” under “Profiled Message”

## Profiled Message

