Isode

R19.0 M-Switch User Server Evaluation Guide

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

Contents

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 ACP127, ACP142/S4406 and ACP142/mule.
2. Added local “field.net” and “mmhs.field.net” users with mappings to ACP127 and S4406 using Cobalt.
3. Created an External ACP127 Station.
4. Created an External ACP142 S4406 Annex E MTA for Military traffic
5. Created an External ACP142 S4406 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 ACP127 and S4406 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	S4406 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=S4406/A=FIELD/C=GB/
FIELD RADIO OPERATOR	radio.operator@mmhs.field.net	RIFIELD	FIELD RADIO OPERATOR	/CN=FIELD RADIO OPERATOR /P=S4406/A=FIELD/C=GB/
BLACK PEARL	blackpearl@mmhs.field.net	RIFIELD	BLACK PEARL	/CN=BLACK PEARL /P=S4406/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=S4406/A=HEADQUARTERS/C=GB/
HEADQUARTERS RADIO OPERATOR	radio.operator@mmhs.headquarters.net	RIHEADQ	HEADQUARTERS RADIO OPERATOR	/CN=HEADQUARTERS RADIO OPERATOR /P=S4406/A=HEADQUARTERS/C=GB/
SERVICE MESSAGES	service.messages@mmhs.headquarters.net	RIHEADQ	N/A	N/A
HOME GUARD	homeguard@mmhs.headquarters.net	RIHEADQ	HOME GUARD	/CN=HOME GUARD /P=S4406/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

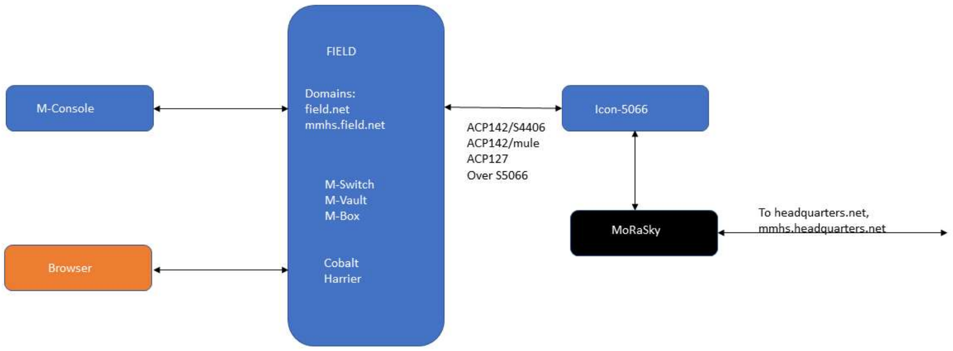
It also uses the following Organizational Relationships

Organization	Member Role Capabilities
BLACK PEARL	FIELD CAPTAIN (Can Release, Always Sends Direct) FIELD RADIO OPERATOR (Can Draft)
HOME GUARD	HEADQUARTERS CAPTAIN (Can Release, Always Sends Direct) HEADQUARTERS RADIO OPERATOR (Can Draft)

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*. 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. In a Windows 2025 environment, please also install the “WMIC” optional feature. For this guide, the following products were used:

Messaging Activation Server 1.1v1

M-Vault 19.0v21

M-Switch 19.0v21

M-Box 19.0v21

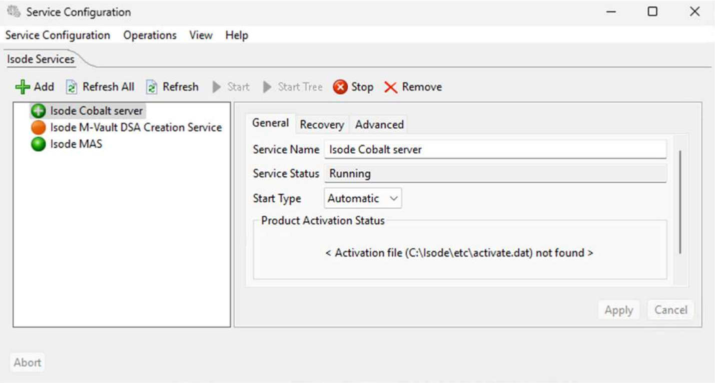
Cobalt 1.5v3

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



Service Name: Isode Cobalt server

Service Status: Running

Start Type: Automatic

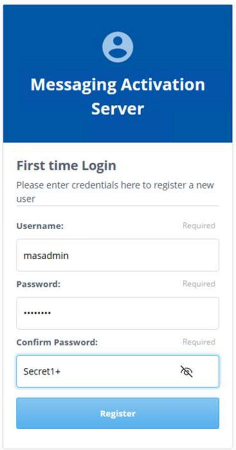
Product Activation Status

< Activation file (C:\Isode\etc\activate.dat) not found >

Browse to "https://localhost:9000"

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

MAS First Time Log in



First time Login

Please enter credentials here to register a new user

Username: Required

masadmin

Password: Required

········

Confirm Password: Required

Secret1+

In "Username" type "masadmin"

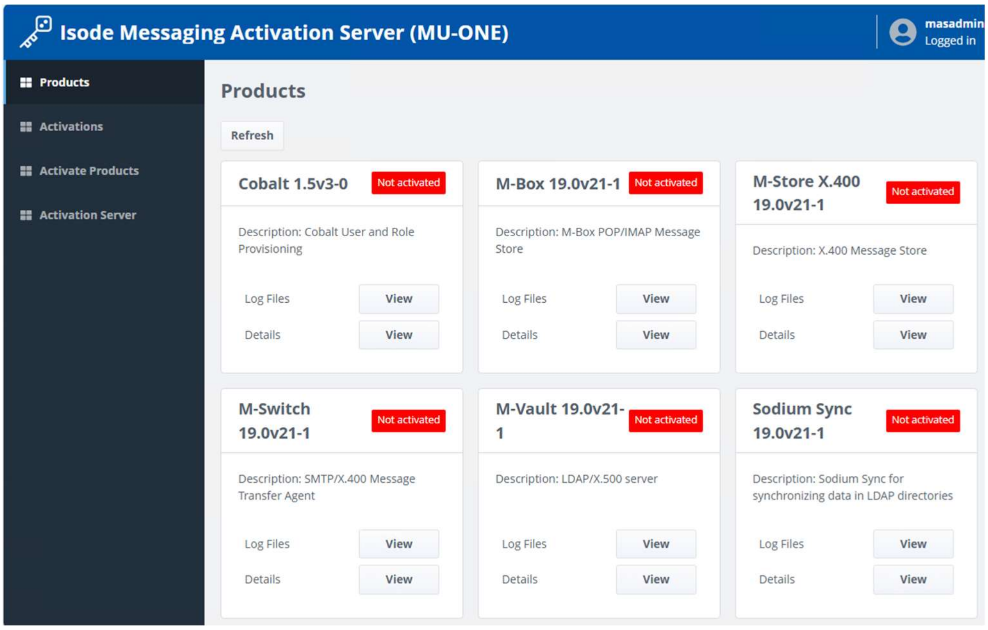
In "Password" type "Secret1+"

In "Confirm Password" type "Secret1+"

Press "Register"

You will be presented with a list of installed products.

View installed Product List



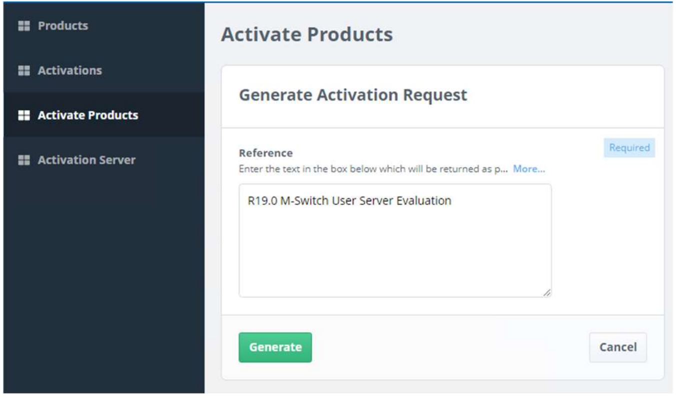
Products

Product	Status	Description
Cobalt 1.5v3-0	Not activated	Description: Cobalt User and Role Provisioning
M-Box 19.0v21-1	Not activated	Description: M-Box POP/IMAP Message Store
M-Store X.400 19.0v21-1	Not activated	Description: X.400 Message Store
M-Switch 19.0v21-1	Not activated	Description: SMTP/X.400 Message Transfer Agent
M-Vault 19.0v21-1	Not activated	Description: LDAP/X.500 server
Sodium Sync 19.0v21-1	Not activated	Description: Sodium Sync for synchronizing data in LDAP directories

Select “Activate Products”

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

Populate Activation Reference



Activate Products

Generate Activation Request

Reference

Required

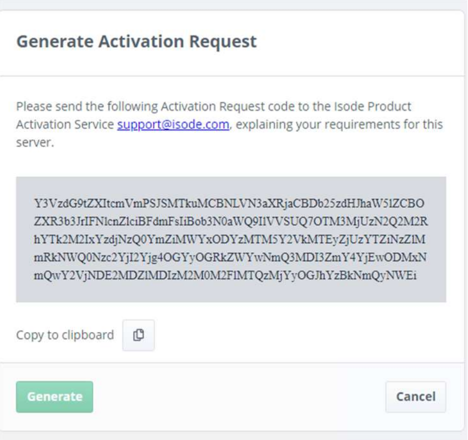
Enter the text in the box below which will be returned as p... More...

R19.0 M-Switch User Server Evaluation

Press “Generate”

Copy the activation request code to your clipboard.

Generate Activation Request



Generate Activation Request

Please send the following Activation Request code to the Isode Product Activation Service support@isode.com, explaining your requirements for this server.

```
Y3VzdG9tZXItcmVmPSJSMTkuMCBNLVN3aXRjaCBDb25zdHJhaW51ZCBO
ZXR3b3JrIFNlcnZlciBFdmFsIiBob3N0aWQ9IlVVSUQ7OTM3MjUzN2Q2M2R
hYTk2M2IxYzdjNzQ0YmZiMWYxODYzMTM5Y2VkMTEyZjUzYTZiNzZlM
mRkNWQ0Nzc2YjI2Yjg4OGYyOGRkZWYwNmQ3MDI3ZmY4YjEwODMxN
mQwY2VjNDE2MDZlMDIzM2M0M2FlMTQzMjYyOGJhYzBkNmQyNWEi
```

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 and Cobalt for a “R19.0 M-Switch User Server Evaluation”. Include the activation request code.

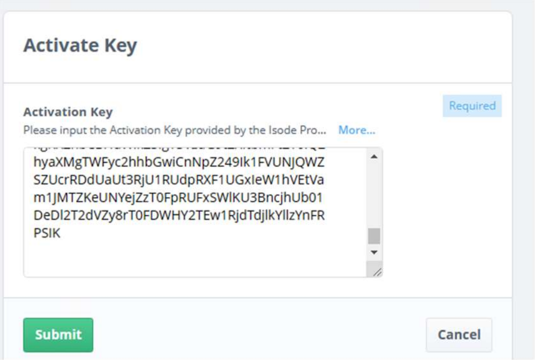
Isode support will supply a set of Product Activation keys

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



Activate Key

Activation Key

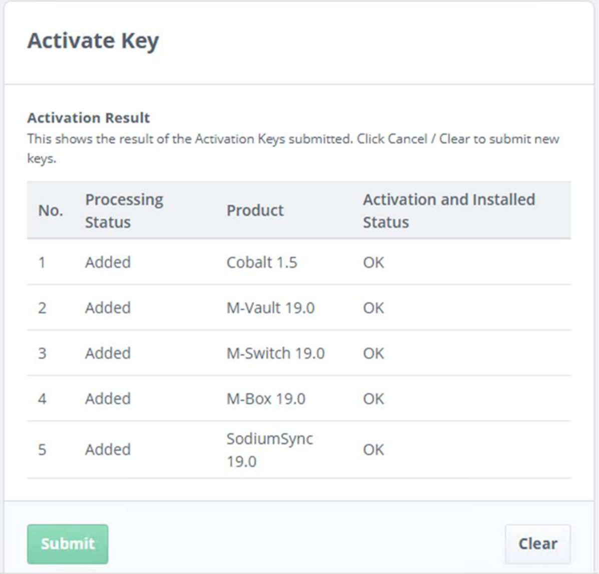
Please input the Activation Key provided by the Isode Pro... More...

```
hyaXMgTWFyc2hhbGwiCnNpZ249Ik1FVUNJQWZ
SZUcrRDdUaUt3RjU1RUdpRXF1UGxleW1hVEtVa
m1JMTZKeUNYejZzT0FpRUFxSWlKU3BncjhUb01
DeDl2T2dVZy8rT0FDWHY2TEw1RjdTdjlkYllzYnFR
PSIK
```

Press “Submit”.

You will be presented with an “Activation Result”

Activation result



Activate Key

Activation Result

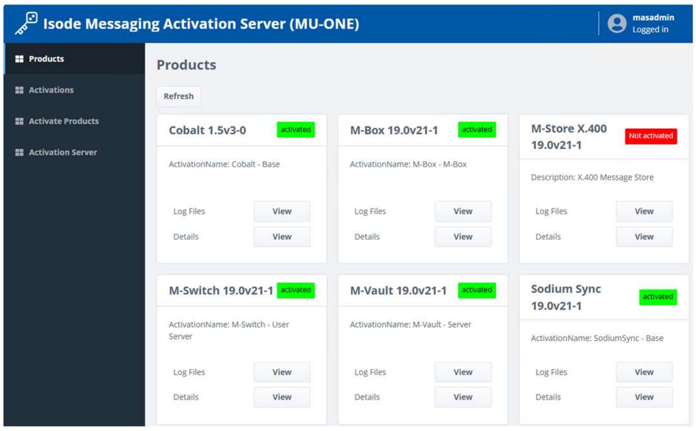
This shows the result of the Activation Keys submitted. Click Cancel / Clear to submit new keys.

No.	Processing Status	Product	Activation and Installed Status
1	Added	Cobalt 1.5	OK
2	Added	M-Vault 19.0	OK
3	Added	M-Switch 19.0	OK
4	Added	M-Box 19.0	OK
5	Added	SodiumSync 19.0	OK

Select “Products”

The products that have been activated should appear in green.

Activated Product List



Isode Messaging Activation Server (MU-ONE)

masadmin Logged in

Products

Cobalt 1.5v3-0 activated
ActivationName: Cobalt - Base

M-Box 19.0v21-1 activated
ActivationName: M-Box - M-Box

M-Store X.400 19.0v21-1 Not activated
Description: X.400 Message Store

M-Switch 19.0v21-1 activated
ActivationName: M-Switch - User Server

M-Vault 19.0v21-1 activated
ActivationName: M-Vault - Server

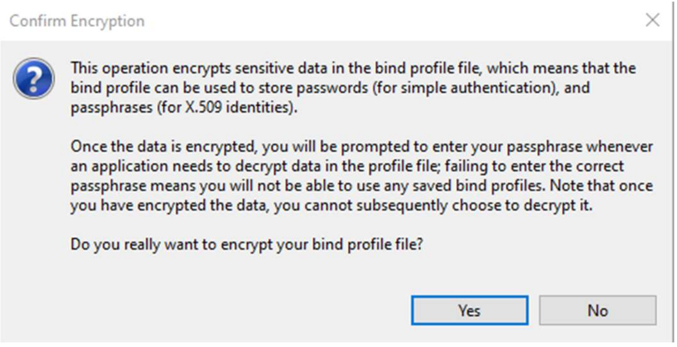
Sodium Sync 19.0v21-1 activated
ActivationName: SodiumSync - Base

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



Confirm Encryption

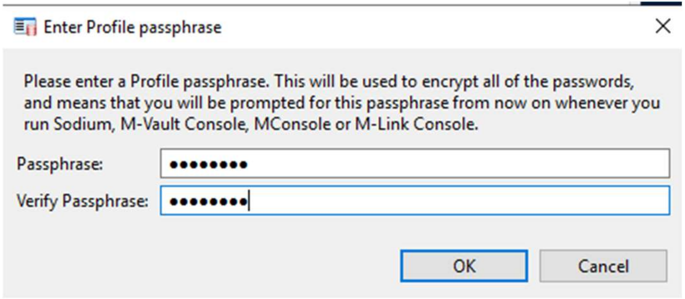
This operation encrypts sensitive data in the bind profile file, which means that the bind profile can be used to store passwords (for simple authentication), and passphrases (for X.509 identities).

Once the data is encrypted, you will be prompted to enter your passphrase whenever an application needs to decrypt data in the profile file; failing to enter the correct passphrase means you will not be able to use any saved bind profiles. Note that once you have encrypted the data, you cannot subsequently choose to decrypt it.

Do you really want to encrypt your bind profile file?

Click "Yes".

Enter a Passphrase for the Bind Profile



Enter Profile passphrase

Please enter a Profile passphrase. This will be used to encrypt all of the passwords, and means that you will be prompted for this passphrase from now on whenever you run Sodium, M-Vault Console, MConsole or M-Link Console.

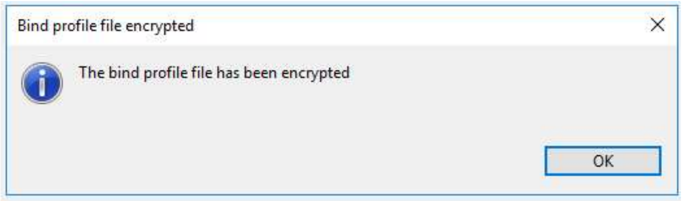
Passphrase: ••••••••

Verify Passphrase: ••••••••

Enter and verify the password "Secret1+"

Click "OK".

Bind Profile encryption confirmation

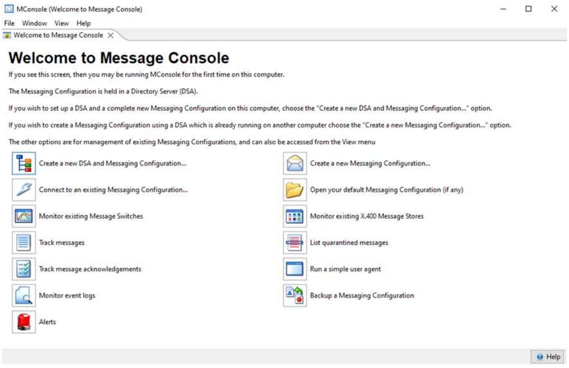


Bind profile file encrypted

The bind profile file has been encrypted

Click "OK".

MConsole "Welcome" screen


MConsole (Welcome to Message Console)
File Window View Help
Welcome to Message Console
Create a new DSA and Messaging Configuration...
Create a new Messaging Configuration...
Connect to an existing Messaging Configuration...
Open your default Messaging Configuration (if any)
Monitor existing Message Switches
Monitor existing X.400 Message Stores
Track messages
List quarantined messages
Track message acknowledgements
Run a simple user agent
Monitor event logs
Backup a Messaging Configuration
Alerts
Help

Welcome to Message Console

If you see this screen, then you may be running MConsole for the first time on this computer.

The Messaging Configuration is held in a Directory Server (DSA).

If you wish to set up a DSA and a complete new Messaging Configuration on this computer, choose the "Create a new DSA and Messaging Configuration..." option.

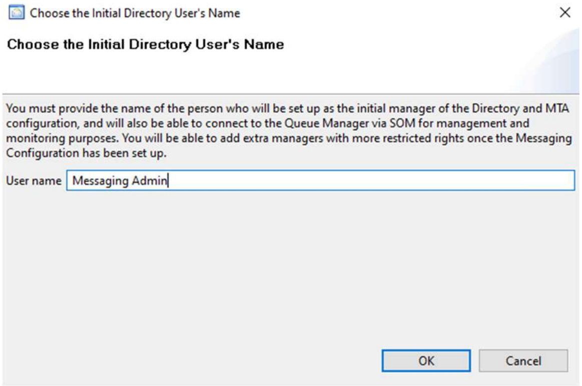
If you wish to create a Messaging Configuration using a DSA which is already running on another computer choose the "Create a new Messaging Configuration..." option.

The other options are for management of existing Messaging Configurations, and can also be accessed from the View menu

Create the DSA

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

Choose the initial Directory Users name



Choose the Initial Directory User's Name

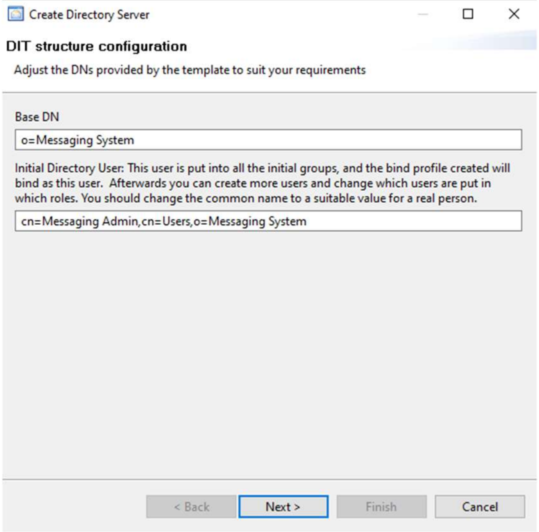
You must provide the name of the person who will be set up as the initial manager of the Directory and MTA configuration, and will also be able to connect to the Queue Manager via SOM for management and monitoring purposes. You will be able to add extra managers with more restricted rights once the Messaging Configuration has been set up.

User name: Messaging Admin

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



DIT structure configuration

Adjust the DNs provided by the template to suit your requirements

Base DN: o=Messaging System

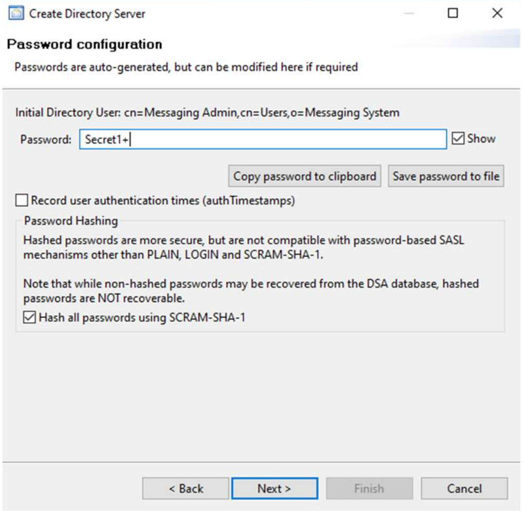
Initial Directory User: This user is put into all the initial groups, and the bind profile created will bind as this user. Afterwards you can create more users and change which users are put in which roles. You should change the common name to a suitable value for a real person.

cn=Messaging Admin,cn=Users,o=Messaging System

Enter a "Base DN" of your choice.

Click "Next >".

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.

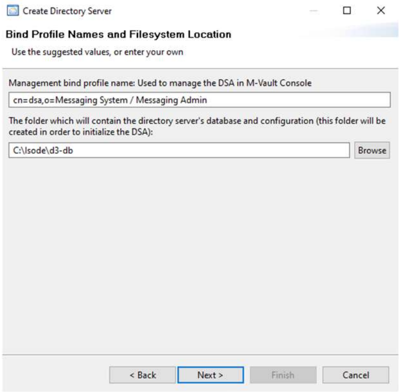
Note that while non-hashed passwords may be recovered from the DSA database, hashed passwords are NOT recoverable.

☑ 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



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

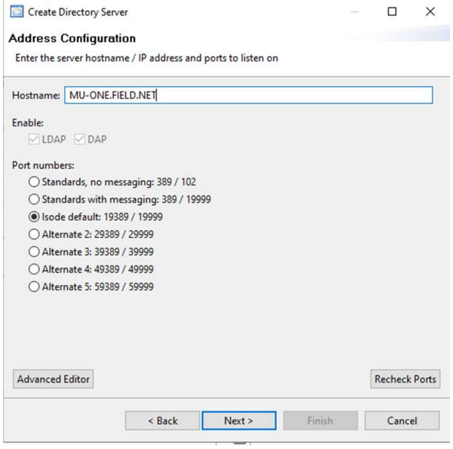
The folder which will contain the directory server's database and configuration (this folder will be created in order to initialize the DSA):

C:\Isode\d3-db

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

Click “Next >”.

Provide address configuration



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:

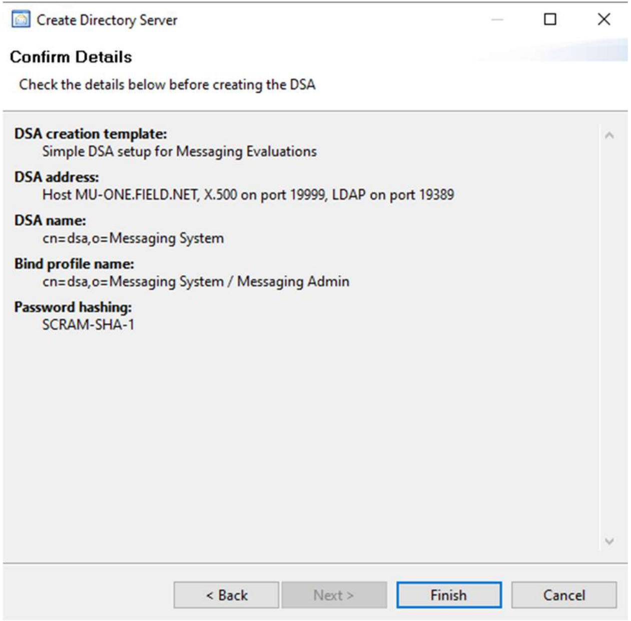
- ○ Standards, no messaging: 389 / 102
- ○ Standards with messaging: 389 / 19999
- ● Isode default: 19389 / 19999
- ○ Alternate 2: 29389 / 29999
- ○ Alternate 3: 39389 / 39999
- ○ Alternate 4: 49389 / 49999
- ○ Alternate 5: 59389 / 59999

Type the hostname “MU-ONE.FIELD.NET”

Click “Next >”

The summary of your DSA configuration is shown.

Confirm details



Confirm Details

Check the details below before creating the DSA

DSA creation template:
Simple DSA setup for Messaging Evaluations

DSA address:
Host MU-ONE.FIELD.NET, X.500 on port 19999, LDAP on port 19389

DSA name:
cn=dsa,o=Messaging System

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

Password hashing:
SCRAM-SHA-1

Click “Finish”.

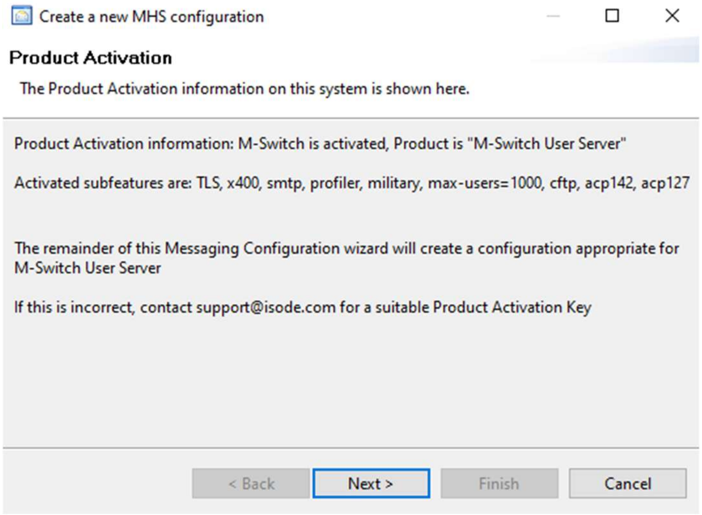
The DSA is created and started.

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



Product Activation

The Product Activation information on this system is shown here.

Product Activation information: M-Switch is activated, Product is "M-Switch User Server"

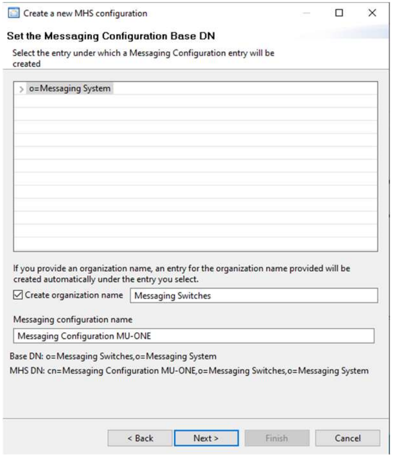
Activated subfeatures are: TLS, x400, smtp, profiler, military, max-users=1000, cftp, acp142, acp127

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

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

Click “Next >”

Set Messaging Configuration Base DN



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

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

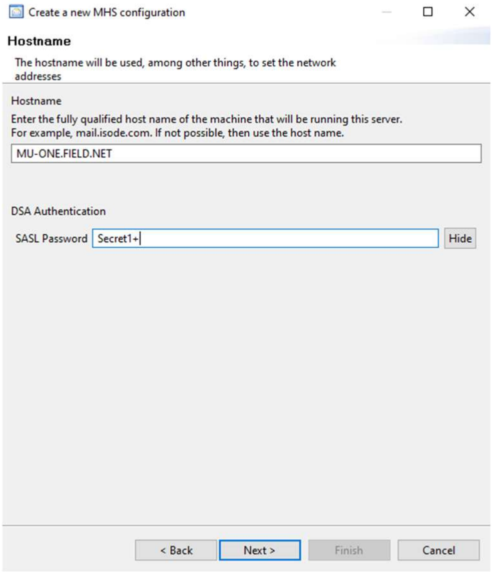
Select “Create Organization Name”

Set the organization name as “Messaging Switches”

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

Click “Next >”.

Provide Hostname



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

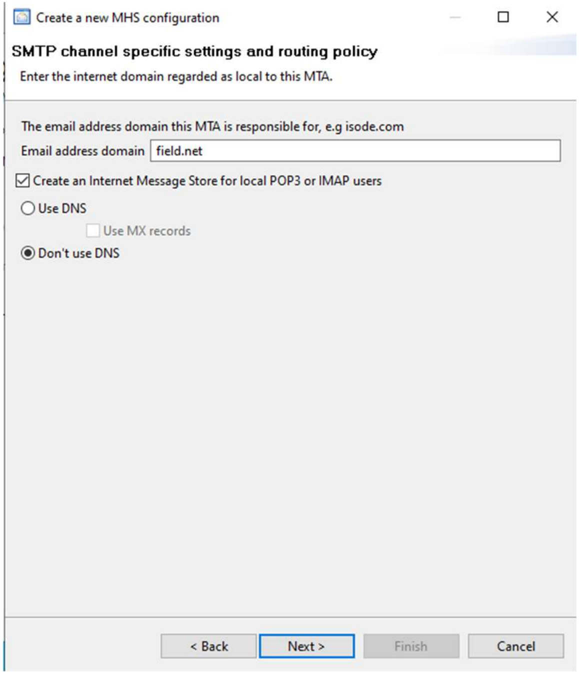
SASL Password: Secret1+

In “hostname” type “MU-ONE.FIELD.NET”

In “SASL Password” type “Secret1+

Click “Next >”

smtp channel specific settings



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: field.net

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

○ Use DNS

□ Use MX records

● Don't use DNS

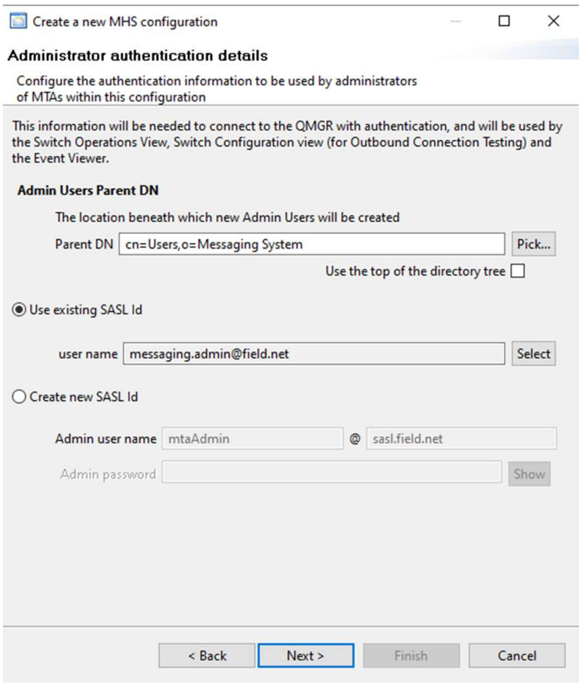
Enter “field.net” in “Email address domain”.

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



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: cn=Users,o=Messaging System

Use the top of the directory tree □

● Use existing SASL Id

user name: messaging.admin@field.net

○ Create new SASL Id

Admin user name: mtaAdmin @ sasl.field.net

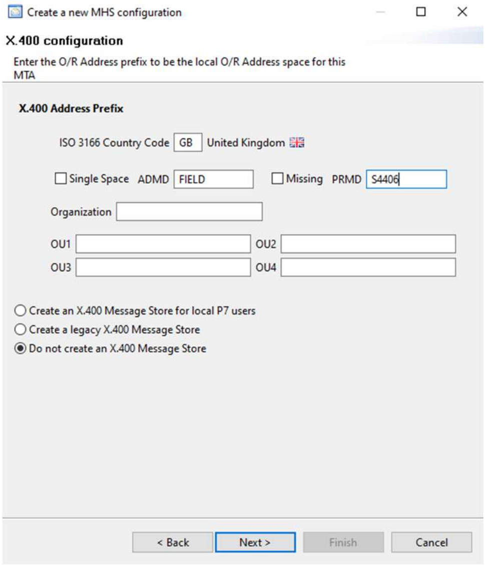
Admin password:

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 GB United Kingdom

□ Single Space ADMD FIELD □ Missing PRMD S4406

Organization

OU1 OU2

OU3 OU4

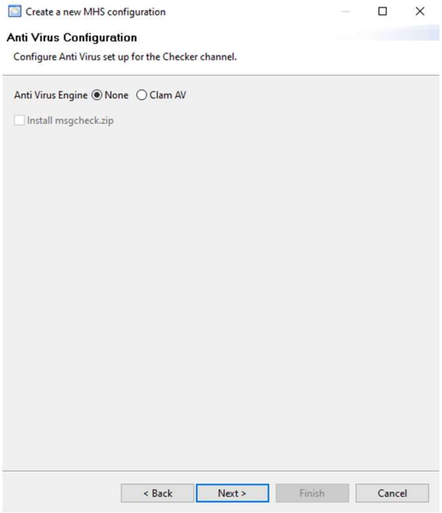
○ Create an X.400 Message Store for local P7 users
○ Create a legacy X.400 Message Store
● Do not create an X.400 Message Store

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.

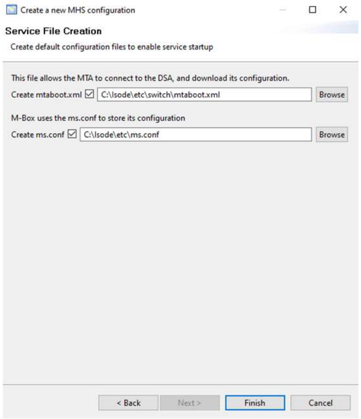
Anti Virus Engine ● None ○ Clam AV

□ Install msgcheck.zip

On “Antivirus Configuration” Select “None”

Click “Next >”.

Service File Creation



Create a new MHS configuration

Service File Creation

Create default configuration files to enable service startup

This file allows the MTA to connect to the DSA, and download its configuration.

Create mtaboot.xml ☑ C:\Isode\etc\switch\mtaboot.xml

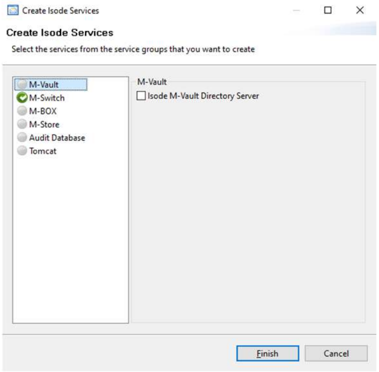
M-Box uses the ms.conf to store its configuration

Create ms.conf ☑ C:\Isode\etc\ms.conf

On “Service file creation” leave the defaults

Click “Finish”.

Create Isode Services



Create Isode Services

Create Isode Services

Select the services from the service groups that you want to create

- ○ M-Vault
- ✓ M-Switch
- ○ M-BOX
- ○ M-Store
- ○ Audit Database
- ○ Tomcat

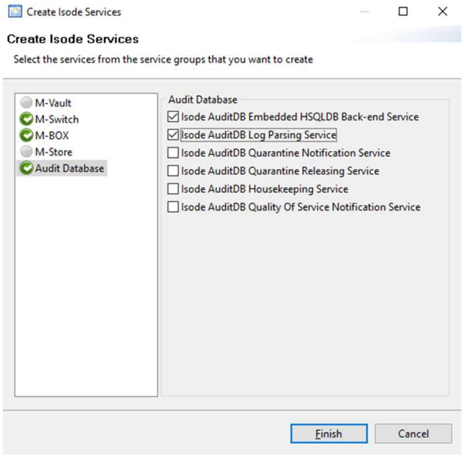
M-Vault

☐ Isode M-Vault Directory Server

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



Create Isode Services

Create Isode Services

Select the services from the service groups that you want to create

- ○ M-Vault
- ✓ M-Switch
- ✓ M-BOX
- ○ M-Store
- ✓ Audit Database

Audit Database

☑ Isode AuditDB Embedded HSQLDB Back-end Service

☑ Isode AuditDB Log Parsing Service

☐ Isode AuditDB Quarantine Notification Service

☐ Isode AuditDB Quarantine Releasing Service

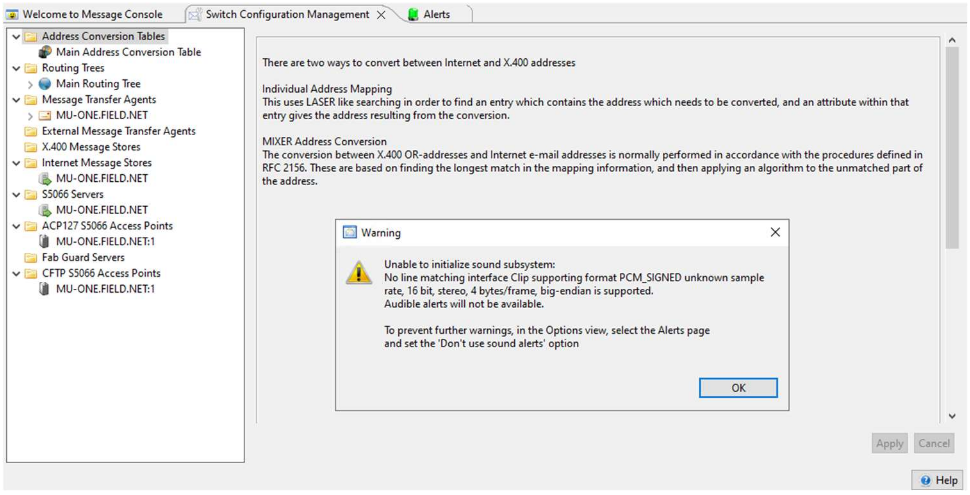
☐ Isode AuditDB Housekeeping Service

☐ Isode AuditDB Quality Of Service Notification Service

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

Click “Finish”.

Initial switch configuration



- Address Conversion Tables
  - Main Address Conversion Table
- Routing Trees
  - Main Routing Tree
- Message Transfer Agents
  - MU-ONE.FIELD.NET
- External Message Transfer Agents
- X.400 Message Stores
- Internet Message Stores
  - MU-ONE.FIELD.NET
- S5066 Servers
  - MU-ONE.FIELD.NET
- ACP127 S5066 Access Points
  - MU-ONE.FIELD.NET:1
- Fab Guard Servers
- CFTP S5066 Access Points
  - MU-ONE.FIELD.NET:1

There are two ways to convert between Internet and X.400 addresses

Individual Address Mapping
This uses LASER like searching in order to find an entry which contains the address which needs to be converted, and an attribute within that entry gives the address resulting from the conversion.

MIXER Address Conversion
The conversion between X.400 OR-addresses and Internet e-mail addresses is normally performed in accordance with the procedures defined in RFC 2156. These are based on finding the longest match in the mapping information, and then applying an algorithm to the unmatched part of the address.

Warning

Unable to initialize sound subsystem:
No line matching interface Clip supporting format PCM_SIGNED unknown sample rate, 16 bit, stereo, 4 bytes/frame, big-endian is supported.
Audible alerts will not be available.

To prevent further warnings, in the Options view, select the Alerts page and set the 'Don't use sound alerts' option

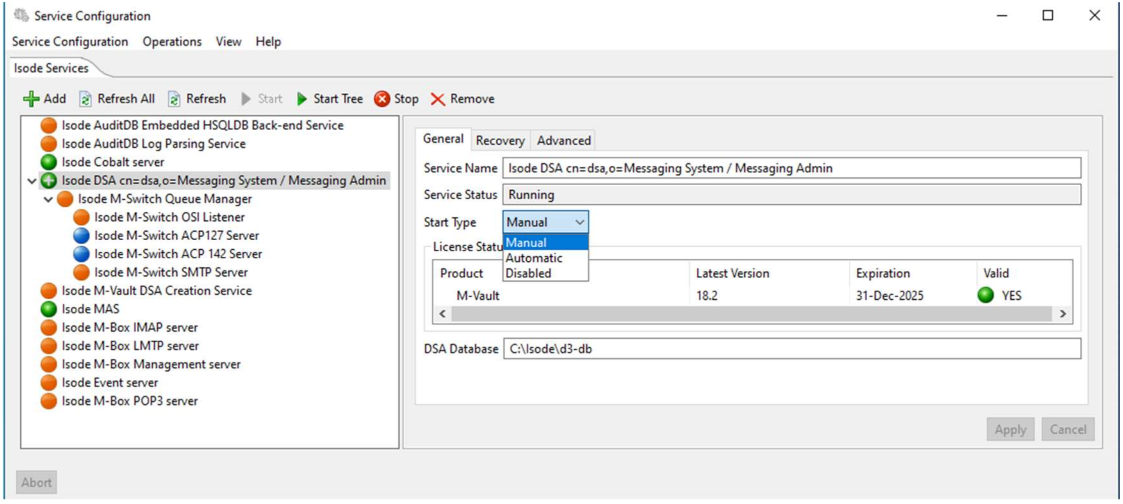
OK

If you receive the “Unable to initialize sound subsystem:” warning, Click “OK”

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



- Isode AuditDB Embedded HSQLDB Back-end Service
- Isode AuditDB Log Parsing Service
- Isode Cobalt server
- Isode DSA cn=dsa,o=Messaging System / Messaging Admin
  - Isode M-Switch Queue Manager
    - Isode M-Switch OSI Listener
    - Isode M-Switch ACP127 Server
    - Isode M-Switch ACP 142 Server
    - Isode M-Switch SMTP Server
- Isode M-Vault DSA Creation Service
- Isode MAS
- Isode M-Box IMAP server
- Isode M-Box LMTP server
- Isode M-Box Management server
- Isode Event server
- Isode M-Box POP3 server

Service Name: Isode DSA cn=dsa,o=Messaging System / Messaging Admin

Service Status: Running

Start Type: Manual

License Statu

Product	Latest Version	Expiration	Valid
M-Vault	18.2	31-Dec-2025	● YES

DSA Database: C:\Isode\d3-db

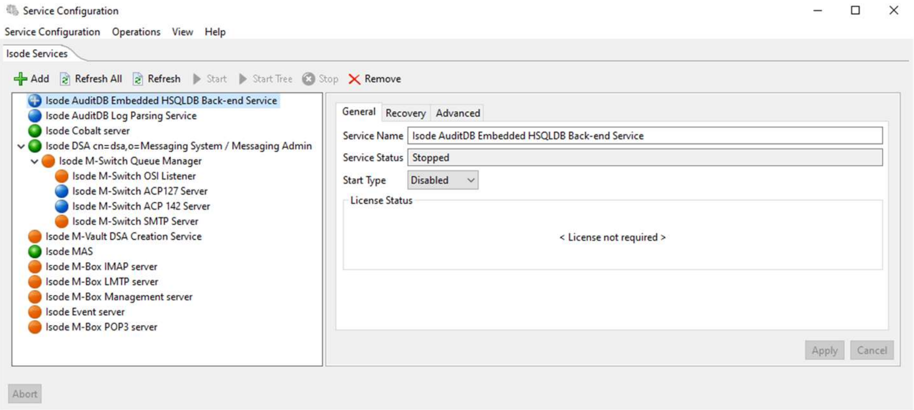
Change the “Isode DSA” Service to “Automatic” from the “Start Type” dropdown

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

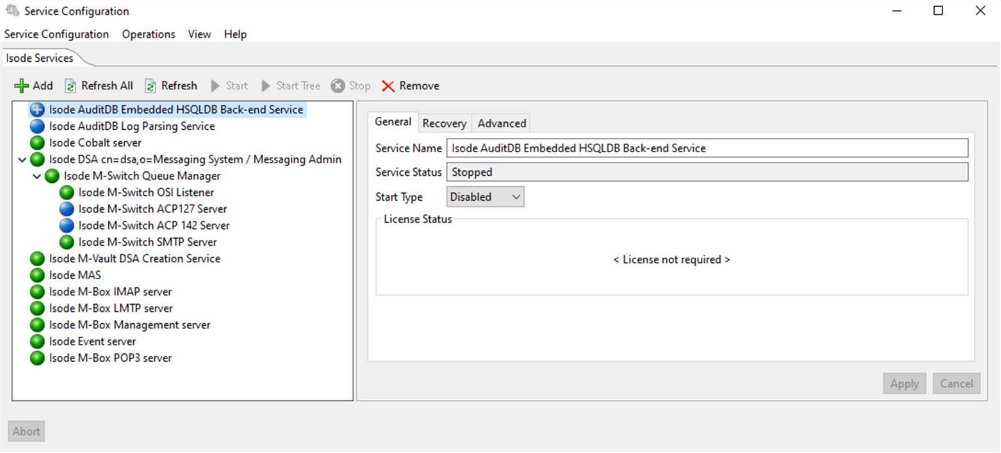

Service Configuration
Service Configuration Operations View Help
Isode Services
Add Refresh All Refresh Start Start Tree Stop Remove
General Recovery Advanced
Apply Cancel
Abort

- Isode AuditDB Embedded HSQLDB Back-end Service
- Isode AuditDB Log Parsing Service
- Isode Cobalt server
- Isode DSA cn=dsa,o=Messaging System / Messaging Admin
  - Isode M-Switch Queue Manager
    - Isode M-Switch OSI Listener
    - Isode M-Switch ACP127 Server
    - Isode M-Switch ACP 142 Server
    - Isode M-Switch SMTP Server
- Isode M-Vault DSA Creation Service
- Isode MAS
- Isode M-Box IMAP server
- Isode M-Box LMTP server
- Isode M-Box Management server
- Isode Event server
- Isode M-Box POP3 server

Service Name: Isode AuditDB Embedded HSQLDB Back-end Service
Service Status: Stopped
Start Type: Disabled
License Status: < License not required >

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

Services Configuration after services started


Service Configuration
Service Configuration Operations View Help
Isode Services
Add Refresh All Refresh Start Start Tree Stop Remove
General Recovery Advanced
Apply Cancel
Abort

- Isode AuditDB Embedded HSQLDB Back-end Service
- Isode AuditDB Log Parsing Service
- Isode Cobalt server
- Isode DSA cn=dsa,o=Messaging System / Messaging Admin
  - Isode M-Switch Queue Manager
    - Isode M-Switch OSI Listener
    - Isode M-Switch ACP127 Server
    - Isode M-Switch ACP 142 Server
    - Isode M-Switch SMTP Server
- Isode M-Vault DSA Creation Service
- Isode MAS
- Isode M-Box IMAP server
- Isode M-Box LMTP server
- Isode M-Box Management server
- Isode Event server
- Isode M-Box POP3 server

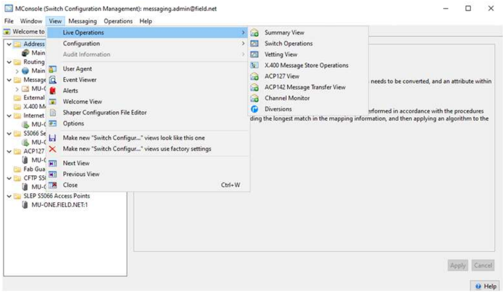
Service Name: Isode AuditDB Embedded HSQLDB Back-end Service
Service Status: Stopped
Start Type: Disabled
License Status: < License not required >

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.

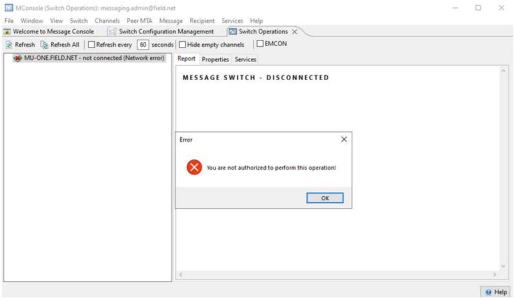
From the MConsole top menu select View→Live Operations→Switch Operations.

Open switch operations view



The following error is expected.

Initial Switch operations view

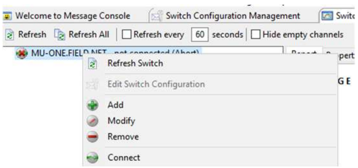

MConsole (Switch Operations): messaging.admin@field.net
File Window View Switch Channels Peer MTA Message Recipient Services Help
Welcome to Message Console
Switch Configuration Management
Switch Operations
Refresh
Refresh All
□ Refresh every 60 seconds
□ Hide empty channels
□ EMCON
MU-ONE.FIELD.NET - not connected (Network error)
Report
Properties
Services
MESSAGE SWITCH - DISCONNECTED
Error
OK
Help

You are not authorized to perform this operation!

Click "OK" to clear it.

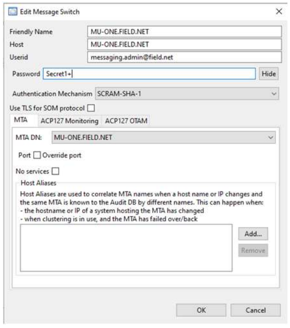
Right Click on the Switch displayed and select "Modify"

Connect to switch


Welcome to Message Console
Switch Configuration Management
Refresh
Refresh All
□ Refresh every 60 seconds
□ Hide empty channels
MU-ONE.FIELD.NET - not connected (Abort)
Refresh Switch
Edit Switch Configuration
Add
Modify
Remove
Connect

Enter the password you entered when creating the "Initial Directory User"

Provide Connection Password



Friendly Name: MU-ONE.FIELD.NET
Host: MU-ONE.FIELD.NET
Userid: messaging.admin@field.net
Password: Secret1+
Authentication Mechanism: SCRAM-SHA-1
Use TLS for SOM protocol □
MTA DN: MU-ONE.FIELD.NET
Port □ Override port
No services □

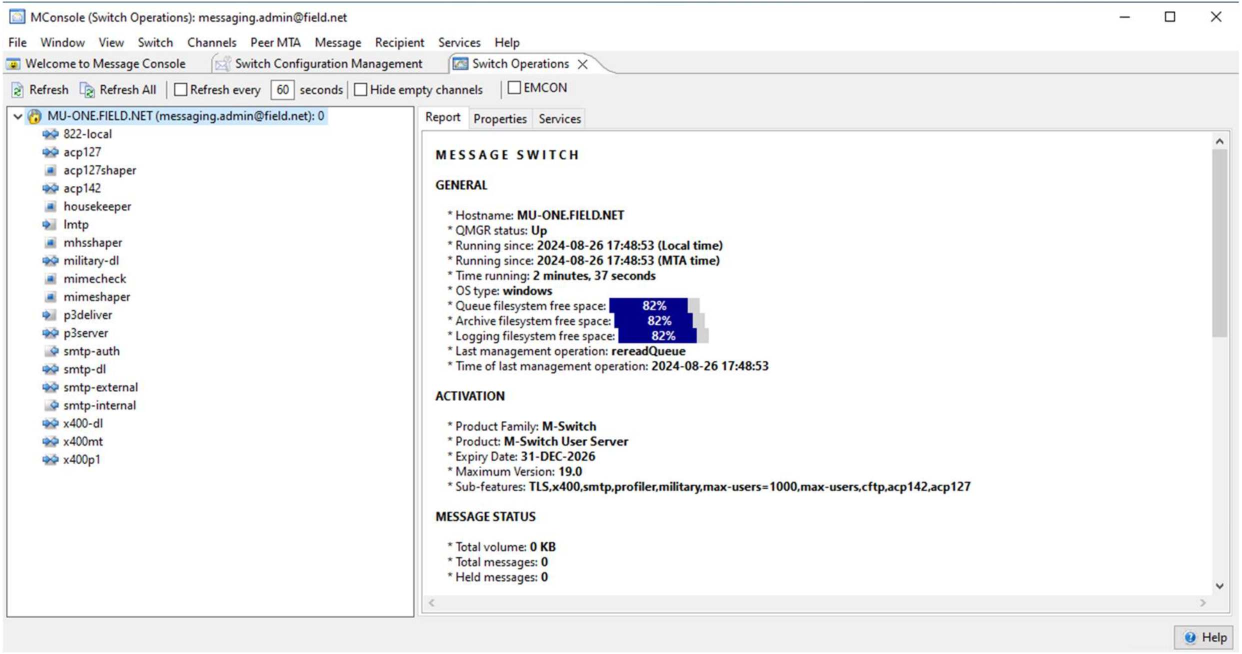
Host Aliases

Host Aliases are used to correlate MTA names when a host name or IP changes and the same MTA is known to the Audit DB by different names. This can happen when:
- the hostname or IP of a system hosting the MTA has changed
- when clustering is in use, and the MTA has failed over/back

Click “OK”.

The following screen will be displayed.

Switch operations view connected



□ Refresh every 60 seconds □ Hide empty channels □ EMCON

MU-ONE.FIELD.NET (messaging.admin@field.net): 0
- 822-local
- acp127
- acp127shaper
- acp142
- housekeeper
- lmtp
- mhsshaper
- military-dl
- mimecheck
- mimeshaper
- p3deliver
- p3server
- smtp-auth
- smtp-dl
- smtp-external
- smtp-internal
- x400-dl
- x400mt
- x400p1

MESSAGE SWITCH

GENERAL

- Hostname: **MU-ONE.FIELD.NET**
- QMGR status: **Up**
- Running since: **2024-08-26 17:48:53 (Local time)**
- Running since: **2024-08-26 17:48:53 (MTA time)**
- Time running: **2 minutes, 37 seconds**
- OS type: **windows**
- Queue filesystem free space: 82%
- Archive filesystem free space: 82%
- Logging filesystem free space: 82%
- Last management operation: **rereadQueue**
- Time of last management operation: **2024-08-26 17:48:53**

ACTIVATION

- Product Family: **M-Switch**
- Product: **M-Switch User Server**
- Expiry Date: **31-DEC-2026**
- Maximum Version: **19.0**
- Sub-features: **TLS,x400,smtp,profiler,military,max-users=1000,max-users,cftp,acp142,acp127**

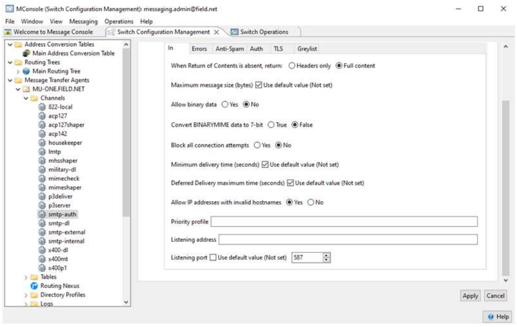
MESSAGE STATUS

- Total volume: **0 KB**
- Total messages: **0**
- Held messages: **0**

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



When Return of Contents is absent, return: ○ Headers only ● Full content

Maximum message size (bytes) ☑ Use default value (Not set)

Allow binary data ○ Yes ● No

Convert BINARYMIME data to 7-bit ○ True ● False

Block all connection attempts ○ Yes ● No

Minimum delivery time (seconds) ☑ Use default value (Not set)

Deferred Delivery maximum time (seconds) ☑ Use default value (Not set)

Allow IP addresses with invalid hostnames ● Yes ○ No

Priority profile

Listening address

Listening port □ Use default value (Not set) 587

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

Click “Apply”.

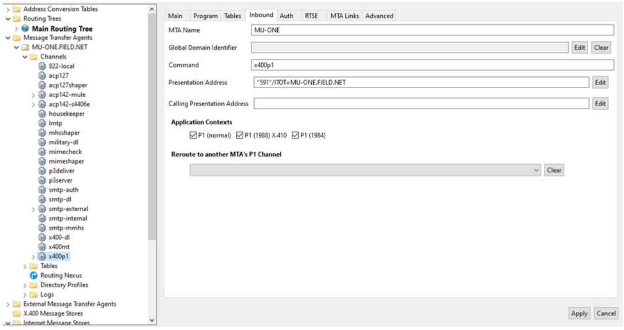
Modify the MTA Name for P1 Connections

Select the Channel “x400p1”

Select the “Inbound” tab.

Change the “MTA Name” to “MU-ONE”

X400p1 inbound tab



MTA Name: MU-ONE

Global Domain Identifier:

Command: x400p1

Presentation Address: "591"/ITOT=MU-ONE.FIELD.NET

Calling Presentation Address:

Application Contexts

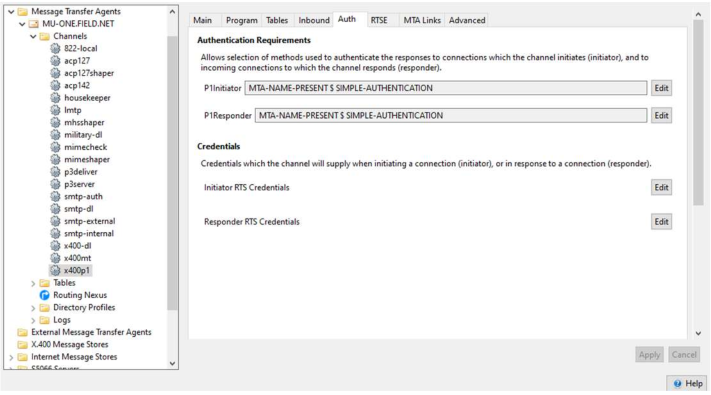
☑ P1 (normal) ☑ P1 (1988) X.410 ☑ P1 (1984)

Reroute to another MTA's P1 Channel

Press “Apply”

Change to the “Auth” tab.

X400p1 auth tab



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

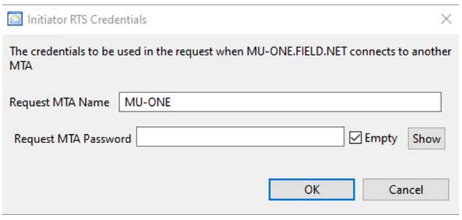
Credentials which the channel will supply when initiating a connection (initiator), or in response to a connection (responder).

Initiator RTS Credentials

Responder RTS Credentials

Press “Edit” next to “Initiator RTS Credentials”

Initiator RTS Credentials



The credentials to be used in the request when MU-ONE.FIELD.NET connects to another MTA

Request MTA Name: MU-ONE

Request MTA Password: ☑ Empty

Change the “Request MTA Name” to “MU-ONE”

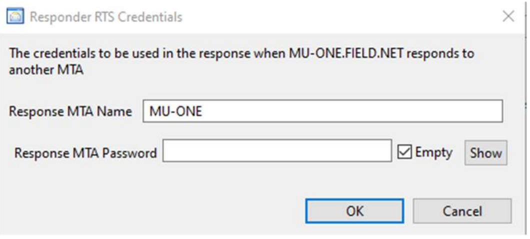
Check “Empty”

On the warning “No Password Specified” Press “OK”

Press “OK”

Press “Edit” next to “Responder RTS Credentials”

Responder RTS Credentials



The credentials to be used in the response when MU-ONE.FIELD.NET responds to another MTA

Response MTA Name: MU-ONE

Response MTA Password: ☑ Empty

Change “Response MTA Name” to “MU-ONE”

Check “Empty”

On the warning “No Password Specified” press “OK”

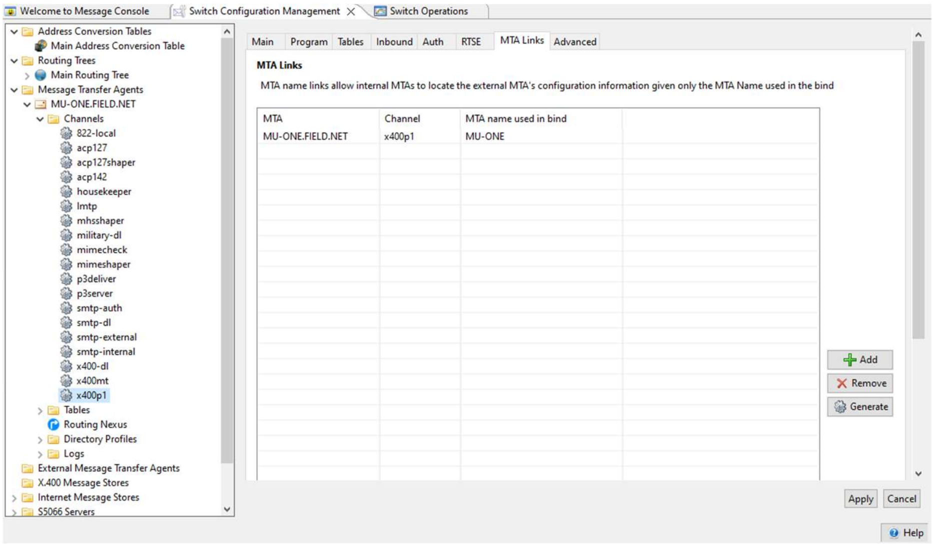
Press “OK”

Press “Apply”

Change to the “MTA Links” tab.

Press “Generate”

Generate mta links



MTA Links

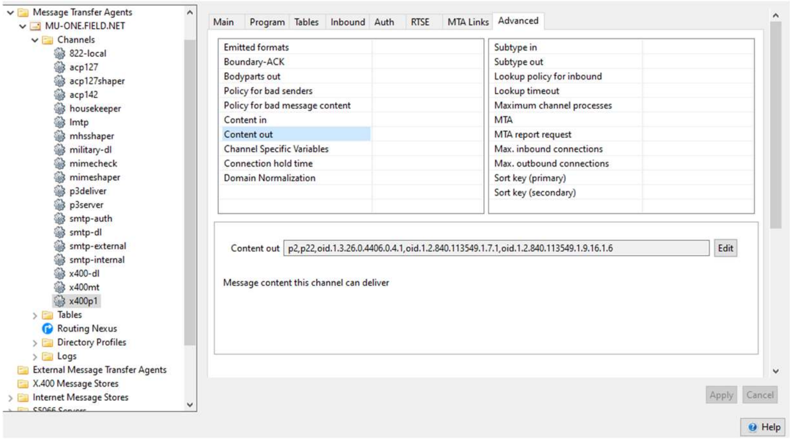
MTA name links allow internal MTAs to locate the external MTA's configuration information given only the MTA Name used in the bind

MTA	Channel	MTA name used in bind
MU-ONE.FIELD.NET	x400p1	MU-ONE

Press “Apply”

X400p1 “Advanced” tab.

X400p1 Advanced tab



Emitted formats		Subtype in	
Boundary-ACK		Subtype out	
Bodyparts out		Lookup policy for inbound	
Policy for bad senders		Lookup timeout	
Policy for bad message content		Maximum channel processes	
Content in		MTA	
Content out		MTA report request	
Channel Specific Variables		Max. inbound connections	
Connection hold time		Max. outbound connections	
Domain Normalization		Sort key (primary)	
		Sort key (secondary)	

Content out: p2,p22,oid.1.3.26.0.4406.0.4.1,oid.1.2.840.113549.1.7.1,oid.1.2.840.113549.1.9.16.1.6

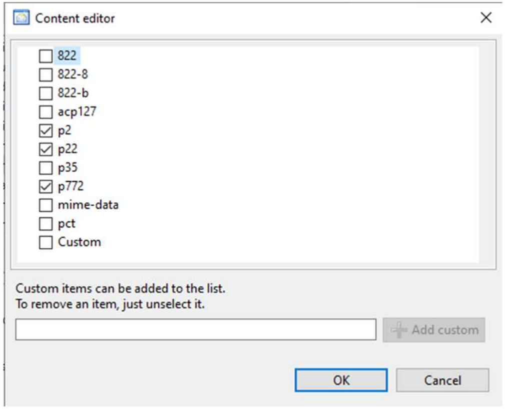
Message content this channel can deliver

Select “Content Out”

Press “Edit”

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

P1 Content types



- □ 822
- □ 822-8
- □ 822-b
- □ acp127
- ☑ p2
- ☑ p22
- □ p35
- ☑ p772
- □ mime-data
- □ pct
- □ Custom

Custom items can be added to the list.
To remove an item, just unselect it.

Press “OK”

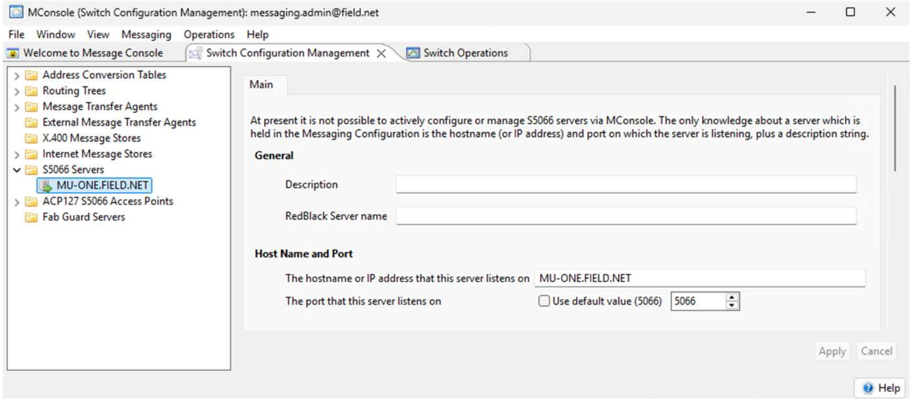
Press “Apply”

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



MConsole (Switch Configuration Management): messaging.admin@field.net
File
Window
View
Messaging
Operations
Help
Welcome to Message Console
Switch Configuration Management
Switch Operations
Address Conversion Tables
Routing Trees
Message Transfer Agents
External Message Transfer Agents
X.400 Message Stores
Internet Message Stores
S5066 Servers
MU-ONE.FIELD.NET
ACP127 S5066 Access Points
Fab Guard Servers
Main
Apply
Cancel
Help

At present it is not possible to actively configure or manage S5066 servers via MConsole. The only knowledge about a server which is held in the Messaging Configuration is the hostname (or IP address) and port on which the server is listening, plus a description string.

General

Description:

RedBlack Server name:

Host Name and Port

The hostname or IP address that this server listens on: MU-ONE.FIELD.NET

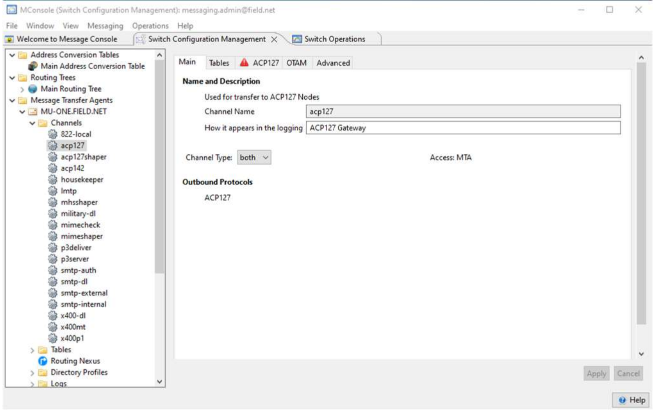
The port that this server listens on: □ Use default value (5066) 5066

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



Name and Description

Used for transfer to ACP127 Nodes

Channel Name: acp127

How it appears in the logging: ACP127 Gateway

Channel Type: both

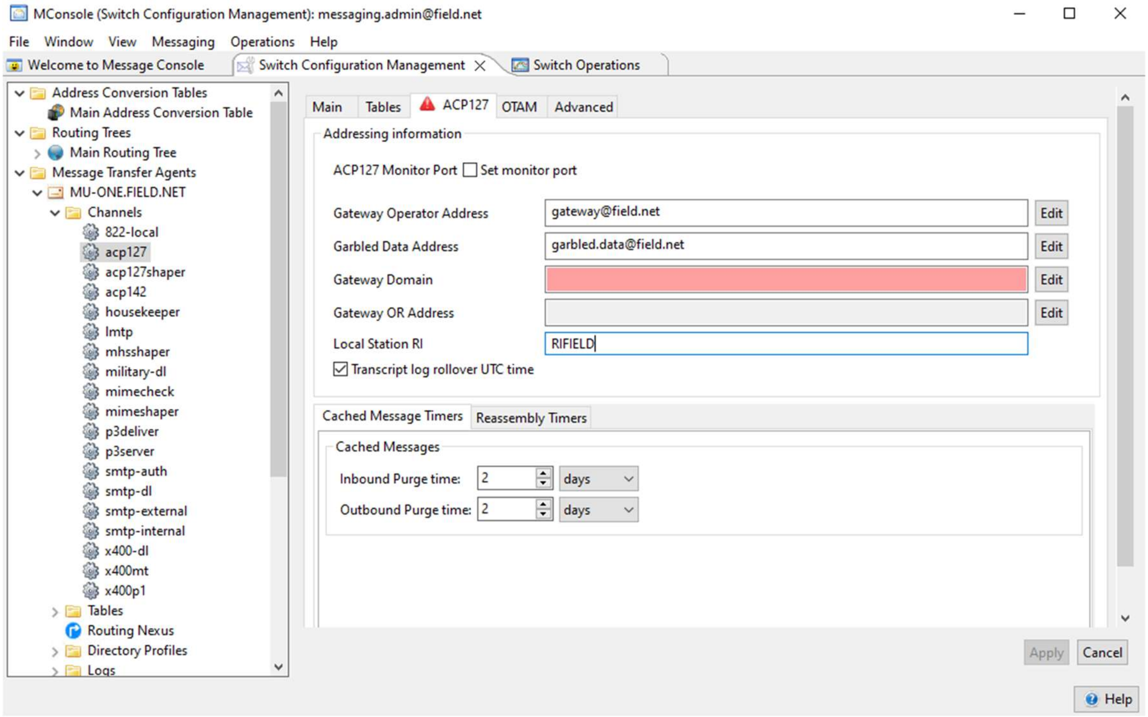
Access: MTA

Outbound Protocols

ACP127

Select the "ACP127" tab.

ACP127 channel acp127 tab



Addressing information

ACP127 Monitor Port ☐ Set monitor port

Gateway Operator Address: gateway@field.net

Garbled Data Address: garbled.data@field.net

Gateway Domain:

Gateway OR Address:

Local Station RI: RIFIELD

☑ Transcript log rollover UTC time

Cached Messages

Inbound Purge time: 2 days

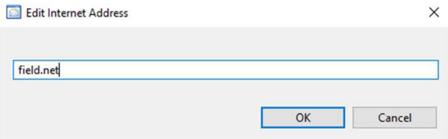
Outbound Purge time: 2 days

Enter the smtp addresses for the “Gateway Operator” and “Garbled Data” mailbox from the table at the start of this document.

Populate the “Local Station RI”

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

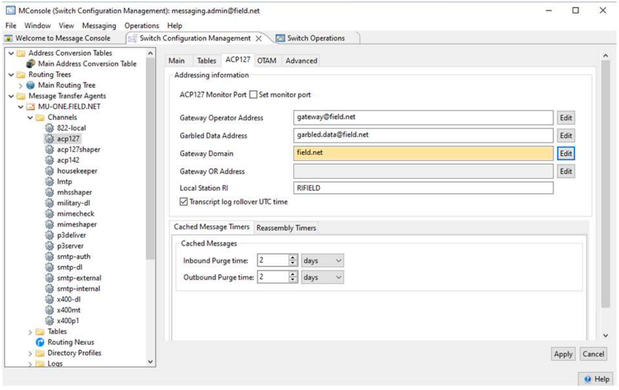
Edit gateway domain



field.net

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

Modified ACP127 tab


MConsole (Switch Configuration Management): messaging.admin@field.net
File Window View Messaging Operations Help
Welcome to Message Console
Switch Configuration Management
Switch Operations
Main
Tables
ACP127
OTAM
Advanced
Edit
Cached Message Timers
Reassembly Timers
Apply
Cancel
Help

Addressing information

ACP127 Monitor Port ☐ Set monitor port

Gateway Operator Address: gateway@field.net

Garbled Data Address: garbled.data@field.net

Gateway Domain: field.net

Gateway OR Address:

Local Station RI: RIFIELD

☑ Transcript log rollover UTC time

Cached Messages

Inbound Purge time: 2 days

Outbound Purge time: 2 days

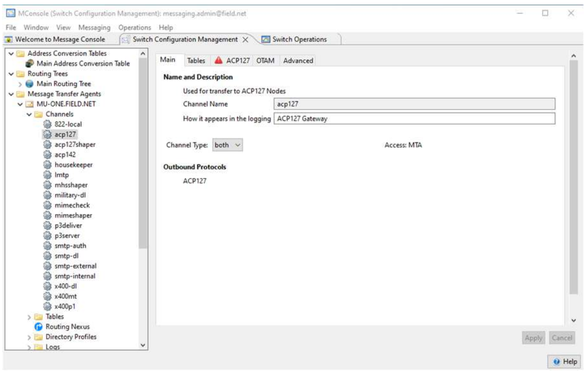
Click “Apply”.

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



Name and Description

Used for transfer to ACP127 Nodes

Channel Name: acp127

How it appears in the logging: ACP127 Gateway

Channel Type: both

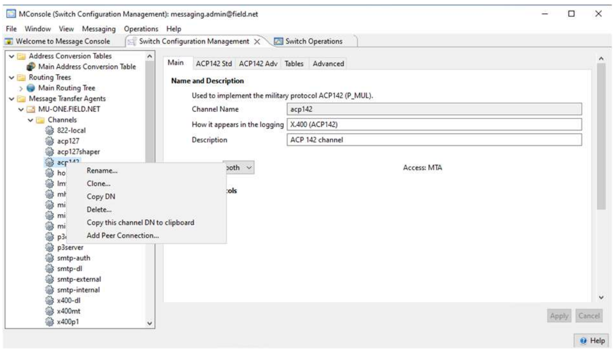
Access: MTA

Outbound Protocols

ACP127

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

ACP142 Channel Rename



Name and Description

Used to implement the military protocol ACP142 (P_MUL).

Channel Name: acp142

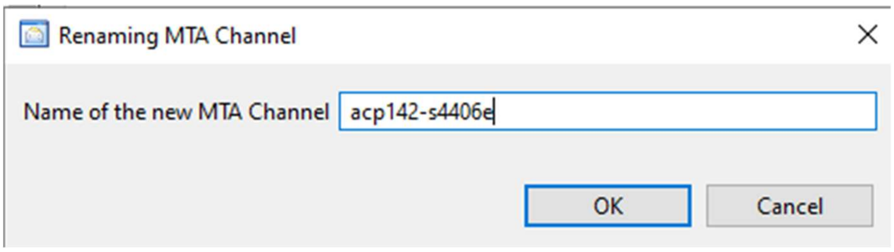
How it appears in the logging: X.400 (ACP142)

Description: ACP 142 channel

Access: MTA

Right click and from the context menu choose “Rename”

New ACP142 Channel name



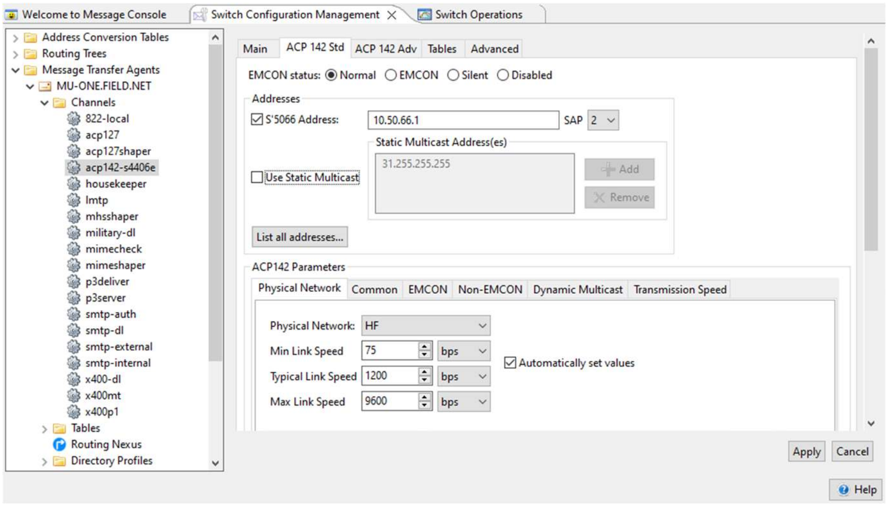
Name of the new MTA Channel: acp142-s4406e

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

Press “OK”

Select the “ACP142 Std” tab.

ACP142 std tab



EMCON status: ● Normal ○ EMCON ○ Silent ○ Disabled

☑ S'5066 Address: 10.50.66.1 SAP 2

Static Multicast Address(es): 31.255.255.255

□ Use Static Multicast

Physical Network: HF

Min Link Speed 75 bps

Typical Link Speed 1200 bps

Max Link Speed 9600 bps

☑ Automatically set values

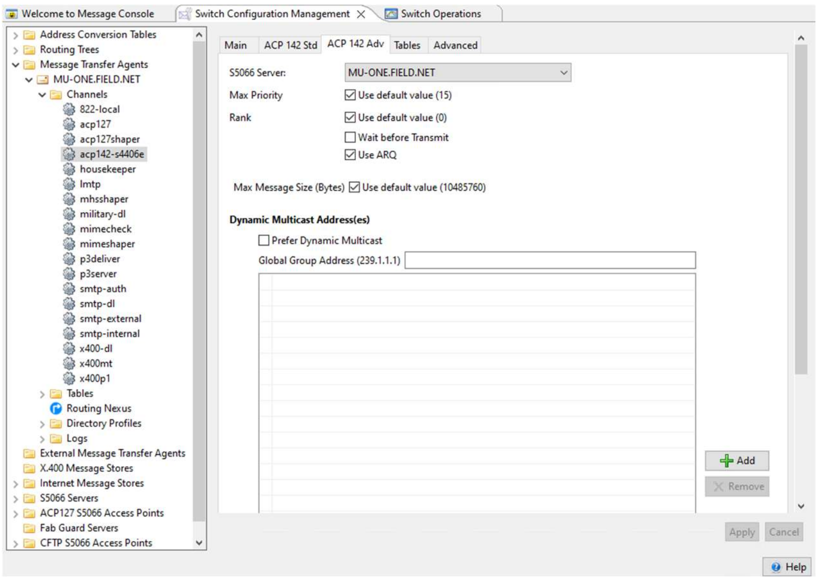
Set the “S’5066 Address” to the Node Address of your local S5066 Server

Uncheck “Use Static Multicast”.

Click “Apply”.

Select the “ACP 142 Adv” tab.

ACP142 Adv tab



S5066 Server: MU-ONE.FIELD.NET

Max Priority ☑ Use default value (15)

Rank ☑ Use default value (0)

□ Wait before Transmit

☑ Use ARQ

Max Message Size (Bytes) ☑ Use default value (10485760)

Dynamic Multicast Address(es)

□ Prefer Dynamic Multicast

Global Group Address (239.1.1.1)

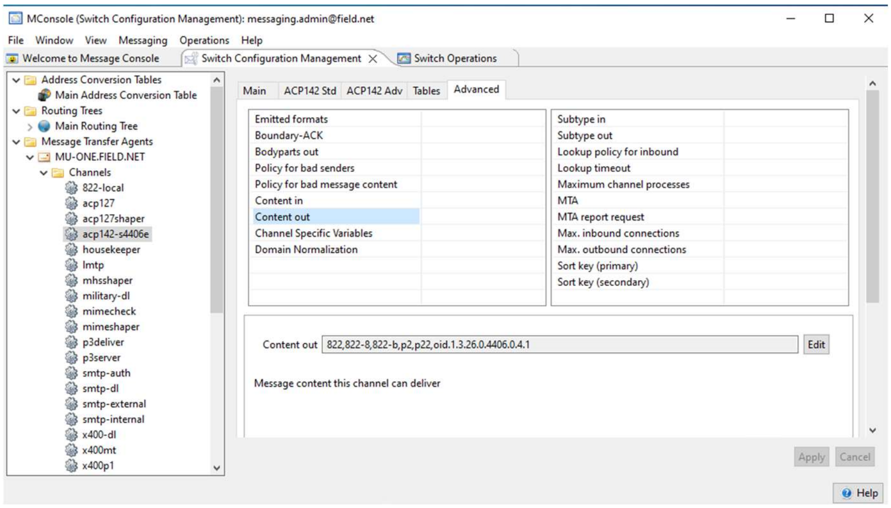
Select the S5066 Server from the drop down.

Click “Apply”.

Select the “Advanced” tab.

Select “Content out” .

Advanced tab



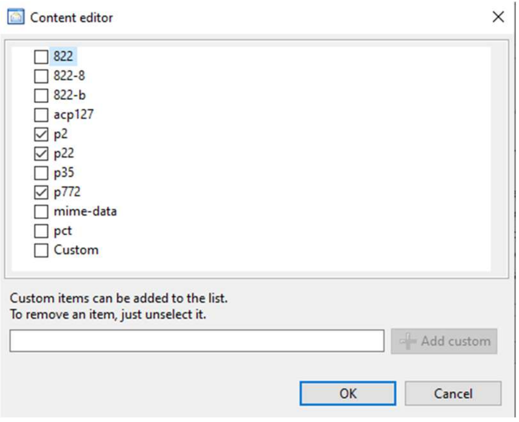
Content out 822,822-8,822-b,p2,p22,oid.1.3.26.0.4406.0.4.1

Message content this channel can deliver

Click “Edit”.

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

Select S4406 Content types



- □ 822
- □ 822-8
- □ 822-b
- □ acp127
- ☑ p2
- ☑ p22
- □ p35
- ☑ p772
- □ mime-data
- □ pct
- □ Custom

Custom items can be added to the list.
To remove an item, just unselect it.

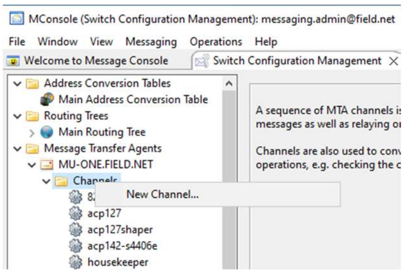
Click “OK”.

Press “Apply”.

Configure the ACP142/mule Channel for smtp traffic

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

Create new channel

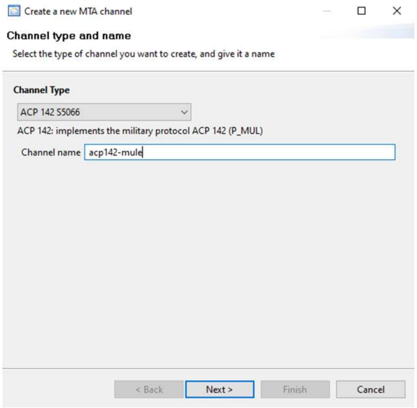

MConsole (Switch Configuration Management): messaging.admin@field.net
File Window View Messaging Operations Help
Welcome to Message Console
Switch Configuration Management
Address Conversion Tables
Main Address Conversion Table
Routing Trees
Main Routing Tree
Message Transfer Agents
MU-ONE.FIELD.NET
Channels
8
New Channel...
acp127
acp127shaper
acp142-s4406e
housekeeper

A sequence of MTA channels i
messages as well as relaying o

Channels are also used to con
operations, e.g. checking the c

Select “New Channel”

Name ACP142 mule channel



Channel type and name

Select the type of channel you want to create, and give it a name

Channel Type

ACP 142 S5066

ACP 142: implements the military protocol ACP 142 (P_MUL)

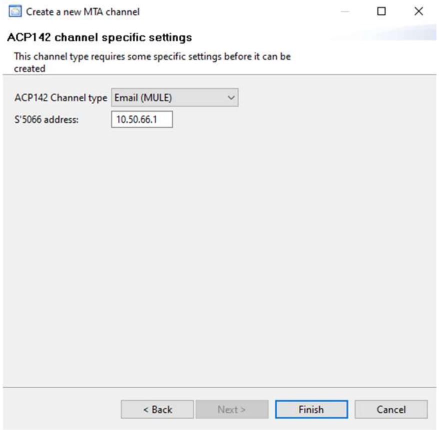
Channel name: acp142-mule

Select Channel type “ACP142 S5066”

Type channel name: “acp142-mule”

Press “Next >”

Set ACP142 mule channel address



ACP142 channel specific settings

This channel type requires some specific settings before it can be created

ACP142 Channel type: Email (MULE)

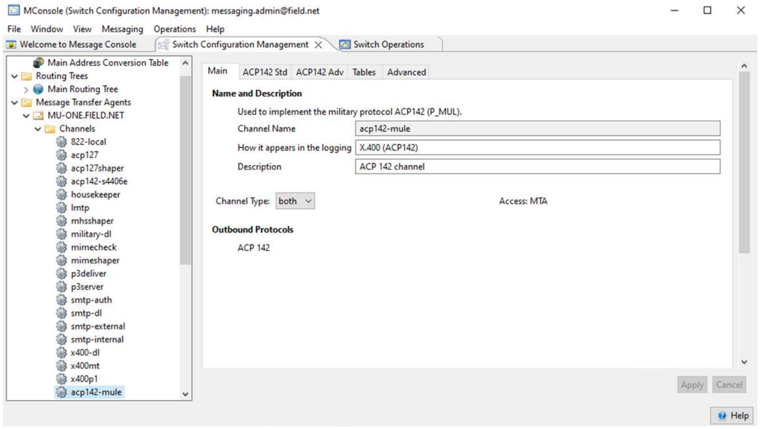
S'5066 address: 10.50.66.1

From the “ACP142 Channel type” dropdown, choose “Email (MULE)”.

In “S’5066 address” type the local S5066 Server Address.

Press “Finish”

New ACP142 mule channel



Name and Description

Used to implement the military protocol ACP142 (P_MUL).

Channel Name: acp142-mule

How it appears in the logging: X.400 (ACP142)

Description: ACP 142 channel

Channel Type: both

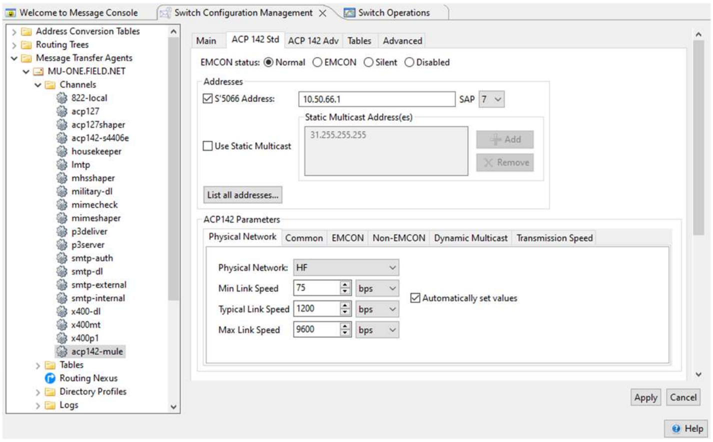
Access: MTA

Outbound Protocols

ACP 142

Select the “ACP142 Std” tab.

ACP142 std tab



EMCON status: ● Normal ○ EMCON ○ Silent ○ Disabled

Addresses

☑ S'5066 Address: 10.50.66.1 SAP 7

□ Use Static Multicast

Static Multicast Address(es): 31.255.255.255

ACP142 Parameters

Physical Network: HF

Min Link Speed 75 bps

Typical Link Speed 1200 bps

Max Link Speed 9600 bps

☑ Automatically set values

Uncheck “Use Static Multicast”

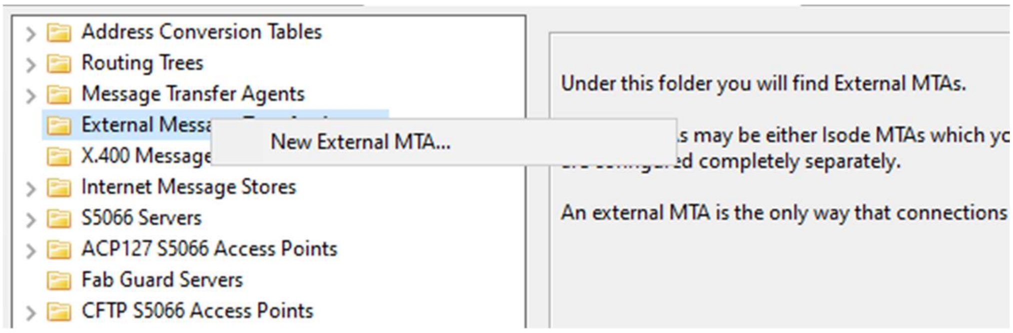
Press “Apply”.

This completes the configuration of the ACP142 Mule Channel.

Configure the External ACP127 Station

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

New external mta



- Address Conversion Tables
- Routing Trees
- Message Transfer Agents
- External Mess
- X.400 Message
- Internet Message Stores
- S5066 Servers
- ACP127 S5066 Access Points
- Fab Guard Servers
- CFTP S5066 Access Points

New External MTA...

Under this folder you will find External MTAs.

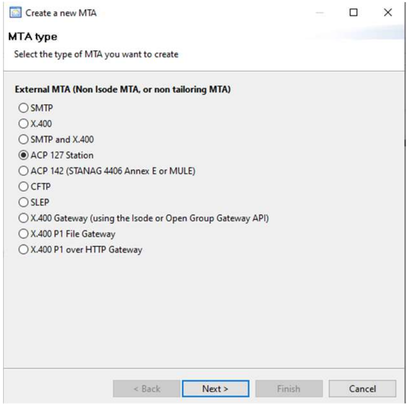
s may be either Isode MTAs which yc

ed completely separately.

An external MTA is the only way that connections

Select “New External MTA…”.

Select MTA type



Create a new MTA

MTA type

Select the type of MTA you want to create

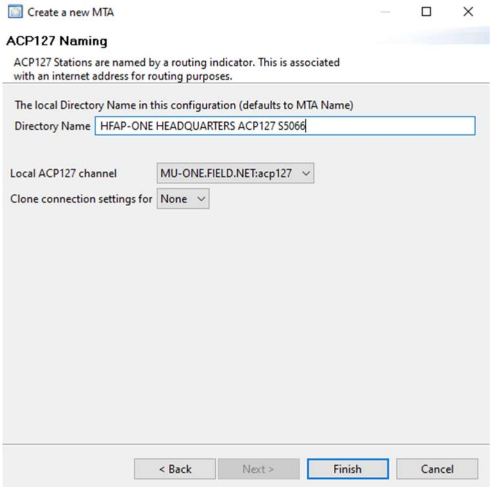
External MTA (Non Isode MTA, or non tailoring MTA)

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

On “MTA Type” dialogue, select “ACP127 station”

Click “Next >”.

Name the remote MTA



Create a new MTA

ACP127 Naming

ACP127 Stations are named by a routing indicator. This is associated with an internet address for routing purposes.

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

Directory Name: HFAP-ONE HEADQUARTERS ACP127 S5066

Local ACP127 channel: MU-ONE.FIELD.NET:acp127

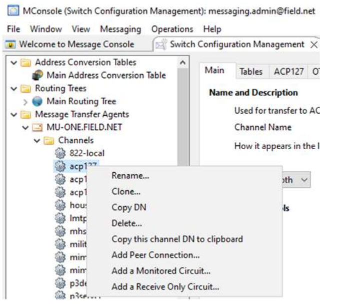
Clone connection settings for: None

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

Click “Finish”.

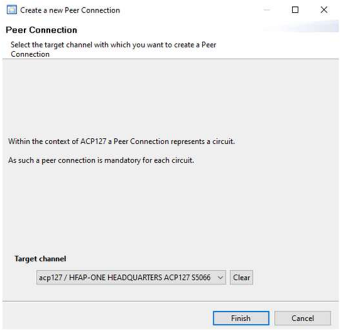
Select the ACP127 Channel

Add Peer Connection menu option


MConsole (Switch Configuration Management): messaging.admin@field.net
File Window View Messaging Operations Help
Welcome to Message Console
Switch Configuration Management
Address Conversion Tables
Main Address Conversion Table
Routing Trees
Main Routing Tree
Message Transfer Agents
MU-ONE.FIELD.NET
Channels
822-local
acp127
Main Tables ACP127
Name and Description
Used for transfer to AC
Channel Name
How it appears in the l
Rename...
Clone...
Copy DN
Delete...
Copy this channel DN to clipboard
Add Peer Connection...
Add a Monitored Circuit...
Add a Receive Only Circuit...

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

Select target channel



Peer Connection

Select the target channel with which you want to create a Peer Connection

Within the context of ACP127 a Peer Connection represents a circuit.

As such a peer connection is mandatory for each circuit.

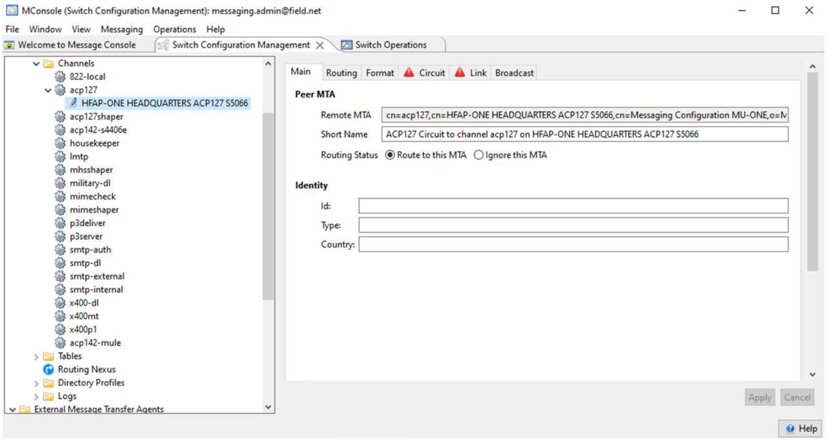
Target channel: acp127 / HFAP-ONE HEADQUARTERS ACP127 S5066

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


MConsole (Switch Configuration Management): messaging.admin@field.net
File Window View Messaging Operations Help
Welcome to Message Console
Switch Configuration Management
Switch Operations
Channels
822-local
acp127
HFAP-ONE HEADQUARTERS ACP127 S5066
acp127shaper
acp142-s4406e
housekeeper
lmtp
mhsshaper
military-dl
mimecheck
mimeshaper
p3deliver
p3server
smtp-auth
smtp-dl
smtp-external
smtp-internal
x400-dl
x400mt
x400p1
acp142-mule
Tables
Routing Nexus
Directory Profiles
Logs
External Message Transfer Agents
Main Routing Format Circuit Link Broadcast
Apply
Cancel
Help

Peer MTA

Remote MTA: cn=acp127,cn=HFAP-ONE HEADQUARTERS ACP127 S5066,cn=Messaging Configuration MU-ONE,o=M

Short Name: ACP127 Circuit to channel acp127 on HFAP-ONE HEADQUARTERS ACP127 S5066

Routing Status: ● Route to this MTA ○ Ignore this MTA

Identity

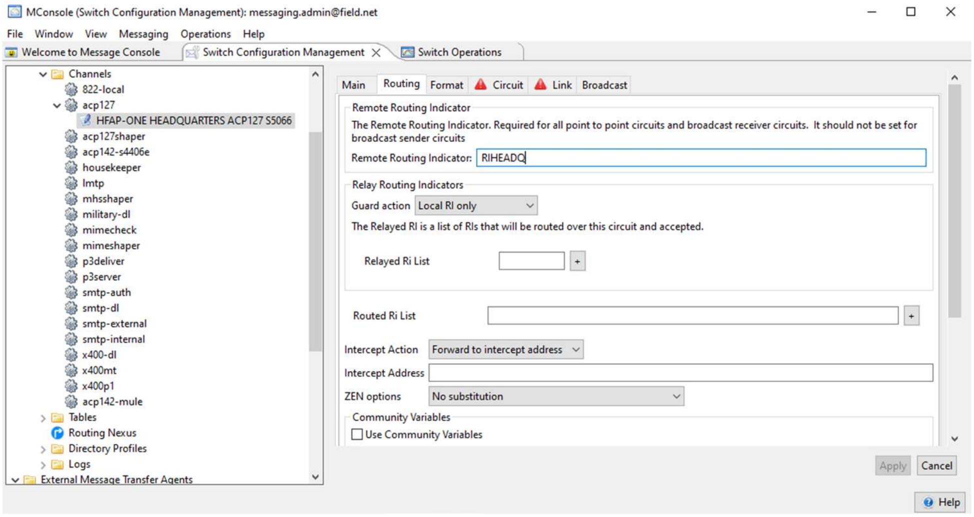
Id:

Type:

Country:

Select the "Routing" tab.

Configure ACP127 routing



Remote Routing Indicator

The Remote Routing Indicator. Required for all point to point circuits and broadcast receiver circuits. It should not be set for broadcast sender circuits

Remote Routing Indicator: RIHEADQ

Relay Routing Indicators

Guard action: Local RI only

The Relayed RI is a list of RIs that will be routed over this circuit and accepted.

Intercept Action: Forward to intercept address

Intercept Address:

ZEN options: No substitution

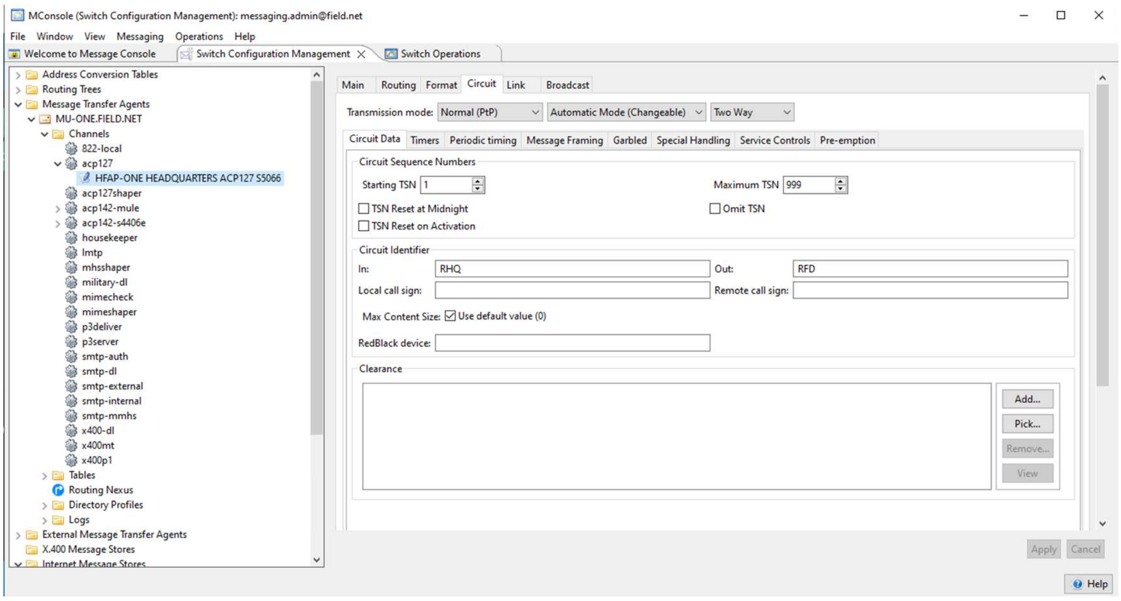
Community Variables

☐ Use Community Variables

Type the “Remote Routing Indicator” for the Remote ACP127 station.

Select the “Circuit” tab.

ACP127 Circuit tab



Transmission mode: Normal (PtP) | Automatic Mode (Changeable) | Two Way

Circuit Sequence Numbers

Starting TSN: 1 Maximum TSN: 999

☐ TSN Reset at Midnight ☐ Omit TSN

☐ TSN Reset on Activation

Circuit Identifier

In: RHQ Out: RFD

Local call sign: Remote call sign:

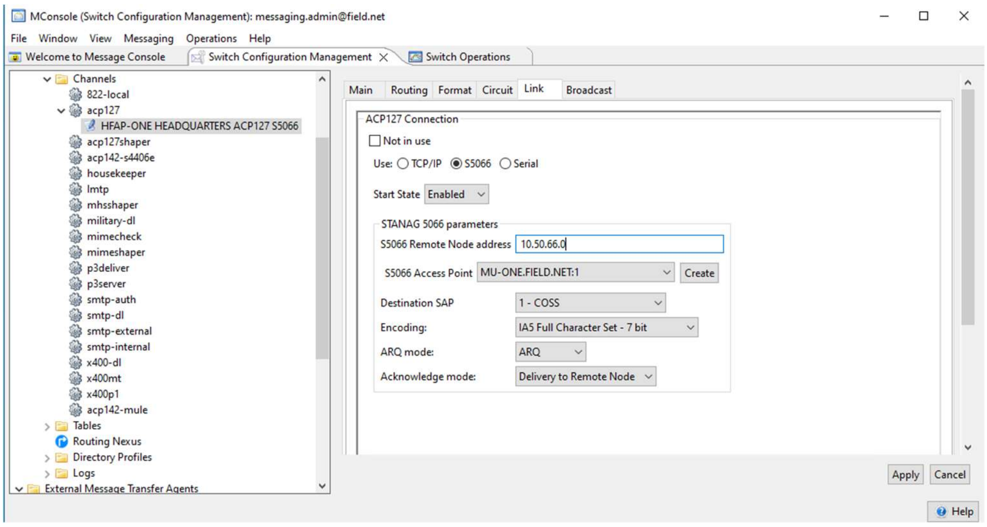
Max Content Size: ☑ Use default value (0)

RedBlack device:

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



MConsole (Switch Configuration Management): messaging.admin@field.net

ACP127 Connection

□ Not in use

Use: ○ TCP/IP ● S5066 ○ Serial

Start State: Enabled

STANAG 5066 parameters

S5066 Remote Node address: 10.50.66.0

S5066 Access Point: MU-ONE.FIELD.NET:1

Destination SAP: 1 - COSS

Encoding: IA5 Full Character Set - 7 bit

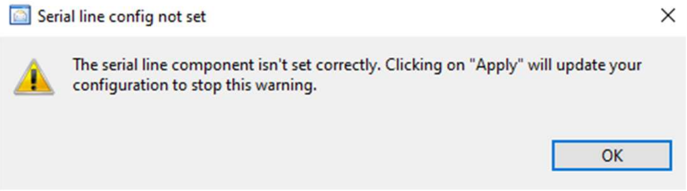
ARQ mode: ARQ

Acknowledge mode: Delivery to Remote Node

Select "S5066", then enter the Node Address of the Remote ACP127 Station.

Select the S5066 Server you have configured from the drop down.

Serial line config warning



Serial line config not set

The serial line component isn't set correctly. Clicking on "Apply" will update your configuration to stop this warning.

On the "Serial line config not set" warning Click "OK"

Click "Apply".

This completes the configuration of the Remote ACP127 Station.

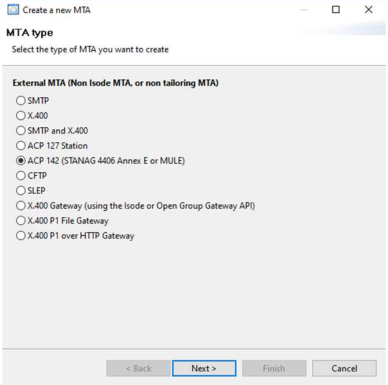
Configure the External ACP142 MTAs

Configure the external ACP142/S4406 MTA

We will now configure the External ACP142 S4406 MTA.

Right Click on the “External Message Transfer Agents “and select “New External MTA…”

Add the External ACP142 S4406 MTA



Create a new MTA

MTA type

Select the type of MTA you want to create

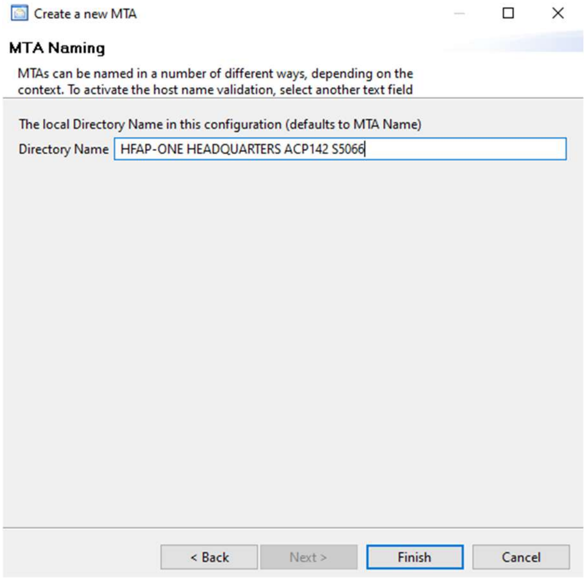
External MTA (Non Isode MTA, or non tailoring MTA)

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

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)

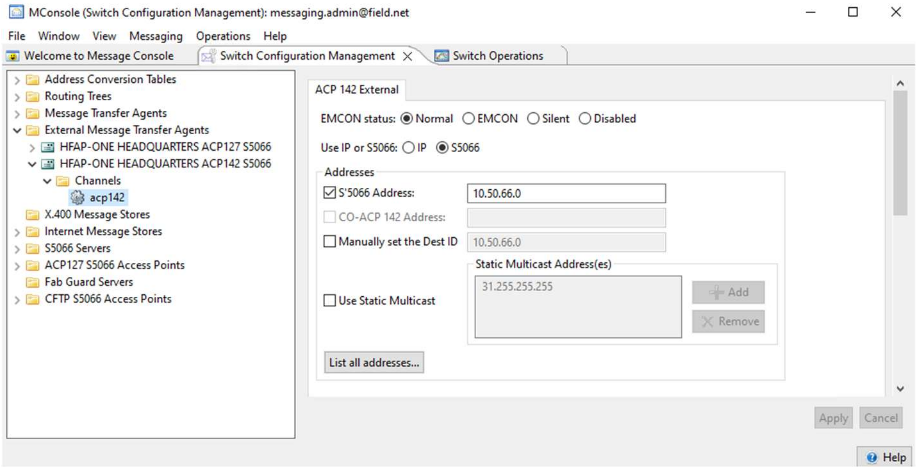
Directory Name: HFAP-ONE HEADQUARTERS ACP142 S5066

Enter a name of your choice for the Display Name

Click “Finish”.

Use the left-hand pane to navigate to the newly configured ACP142 external MTA.

Configure the External ACP142 S4406 MTA


MConsole (Switch Configuration Management): messaging.admin@field.net
File Window View Messaging Operations Help
Welcome to Message Console
Switch Configuration Management
Switch Operations
Address Conversion Tables
Routing Trees
Message Transfer Agents
External Message Transfer Agents
HFAP-ONE HEADQUARTERS ACP127 S5066
HFAP-ONE HEADQUARTERS ACP142 S5066
Channels
acp142
X.400 Message Stores
Internet Message Stores
S5066 Servers
ACP127 S5066 Access Points
Fab Guard Servers
CFTP S5066 Access Points
ACP 142 External
Add
Remove
List all addresses...
Apply
Cancel
Help

EMCON status: ● Normal ○ EMCON ○ Silent ○ Disabled

Use IP or S5066: ○ IP ● S5066

Addresses

☑ S'5066 Address: 10.50.66.0

□ CO-ACP 142 Address:

□ Manually set the Dest ID 10.50.66.0

Static Multicast Address(es): 31.255.255.255

□ Use Static Multicast

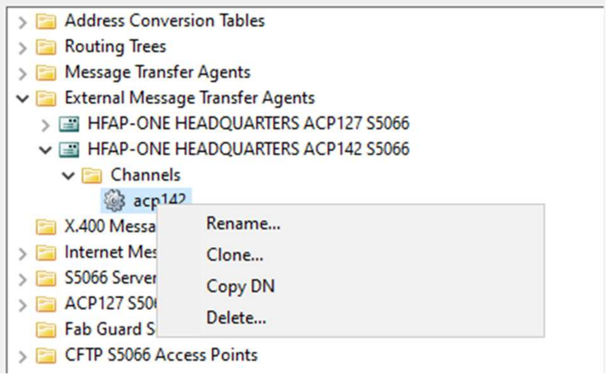
Enter the S5066 Node Address of the Remote server in “S’5066 Address”

Uncheck “Use Static Multicast”.

Click “Apply”.

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

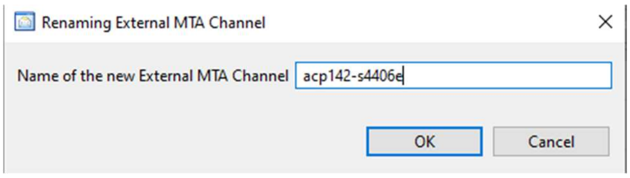
Rename channel menu option



Select “Rename …”

Rename the channel “acp142-s4406e”

Rename channel

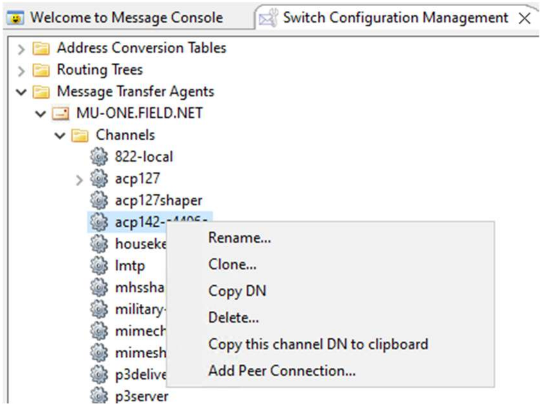


Name of the new External MTA Channel: acp142-s4406e

Press “OK”

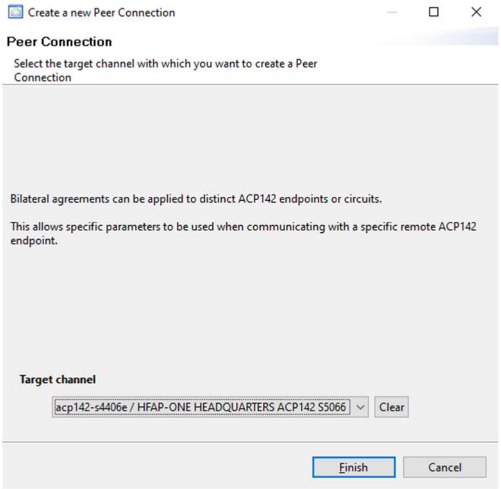
Right click on the local “acp142-s4406e” channel

Add peer connection menu option



Select "Add Peer Connection…"

Select peer connection



Peer Connection

Select the target channel with which you want to create a Peer Connection

Bilateral agreements can be applied to distinct ACP142 endpoints or circuits.

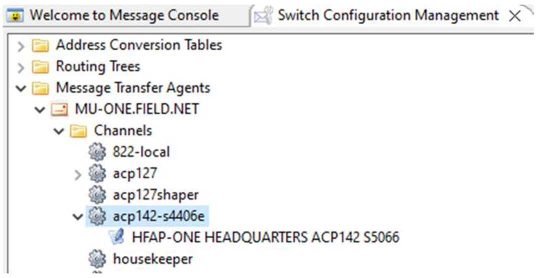
This allows specific parameters to be used when communicating with a specific remote ACP142 endpoint.

Target channel: acp142-s4406e / HFAP-ONE HEADQUARTERS ACP142 S5066

Select the "target channel" "acp142-s4406e ….."

Press "Finish"

Peer connection created

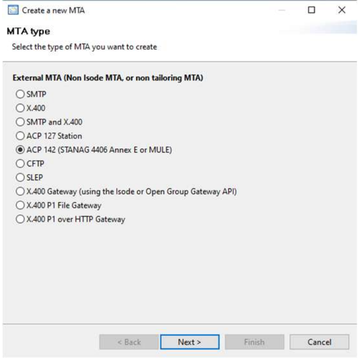

Welcome to Message Console
Switch Configuration Management
Address Conversion Tables
Routing Trees
Message Transfer Agents
MU-ONE.FIELD.NET
Channels
822-local
acp127
acp127shaper
acp142-s4406e
HFAP-ONE HEADQUARTERS ACP142 S5066
housekeeper

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



Create a new MTA

MTA type

Select the type of MTA you want to create

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

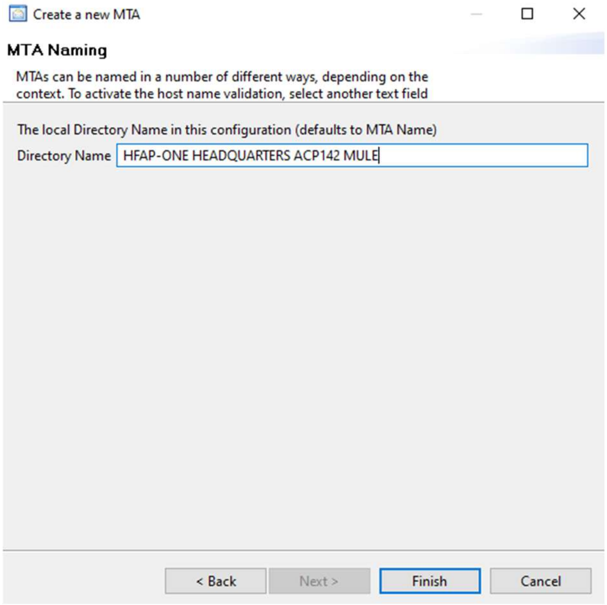
○ SMTP
○ X.400
○ SMTP and X.400
○ ACP 127 Station
● ACP 142 (STANAG 4406 Annex E or MULE)
○ CFTP
○ SLEP
○ X.400 Gateway (using the Isode or Open Group Gateway API)
○ X.400 P1 File Gateway
○ X.400 P1 over HTTP Gateway

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



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

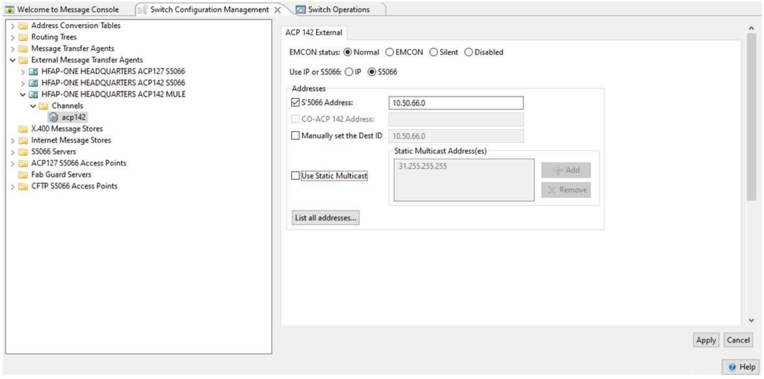
The local Directory Name in this configuration (defaults to MTA Name)

Directory Name: HFAP-ONE HEADQUARTERS ACP142 MULE

Click “Finish”.

Select the newly created acp142 mule External Message Transfer agent.

Configure the External ACP142/mule MTA



Welcome to Message Console
Switch Configuration Management
Switch Operations
Address Conversion Tables
Routing Trees
Message Transfer Agents
External Message Transfer Agents
HFAP-ONE HEADQUARTERS ACP127 S5066
HFAP-ONE HEADQUARTERS ACP142 S5066
HFAP-ONE HEADQUARTERS ACP142 MULE
Channels
acp142
X.400 Message Stores
Internet Message Stores
S5066 Servers
ACP127 S5066 Access Points
Fab Guard Servers
CFTP S5066 Access Points
ACP 142 External

EMCON status: ● Normal ○ EMCON ○ Silent ○ Disabled

Use IP or S5066: ○ IP ● S5066

Addresses

☑ S'5066 Address: 10.50.66.0

□ CO-ACP 142 Address:

□ Manually set the Dest ID 10.50.66.0

Static Multicast Address(es): 31.255.255.255

□ Use Static Multicast

Add
Remove
List all addresses...
Apply
Cancel
Help

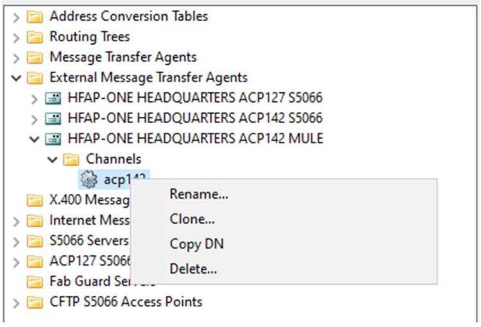
Enter the S5066 Node Address of the Remote server in “S’5066 Address”

Uncheck “Use Static Multicast”.

Click “Apply.

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

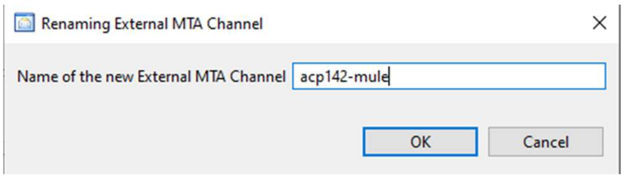
Rename channel menu option



Select “Rename …”

Rename the channel “acp142-mule”

Rename channel

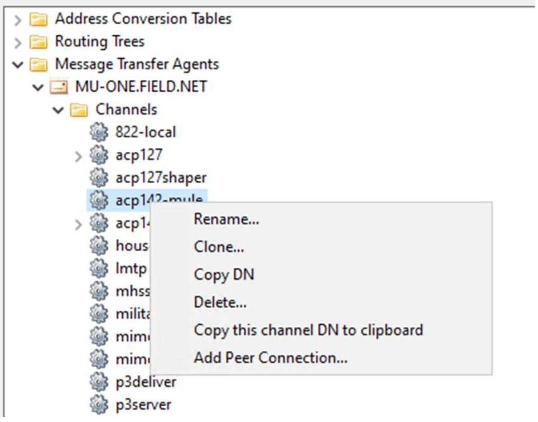

Renaming External MTA Channel

Name of the new External MTA Channel: acp142-mule

Press “OK”

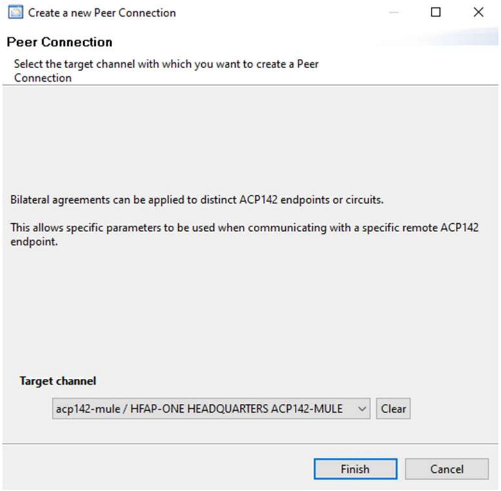
Right click on the local “acp142-mule” channel

Add peer connection menu option



Select “Add Peer Connection…”

Select peer connection



Create a new Peer Connection

Peer Connection

Select the target channel with which you want to create a Peer Connection

Bilateral agreements can be applied to distinct ACP142 endpoints or circuits.

This allows specific parameters to be used when communicating with a specific remote ACP142 endpoint.

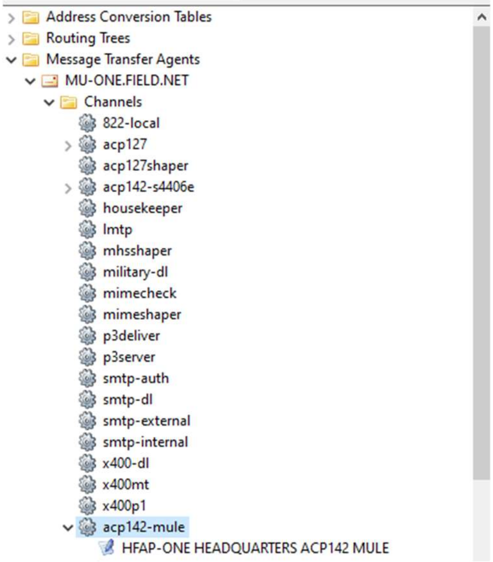
Target channel

acp142-mule / HFAP-ONE HEADQUARTERS ACP142-MULE

Select the "target channel" "acp142-mule ….."

Press "Finish"

Peer connection created



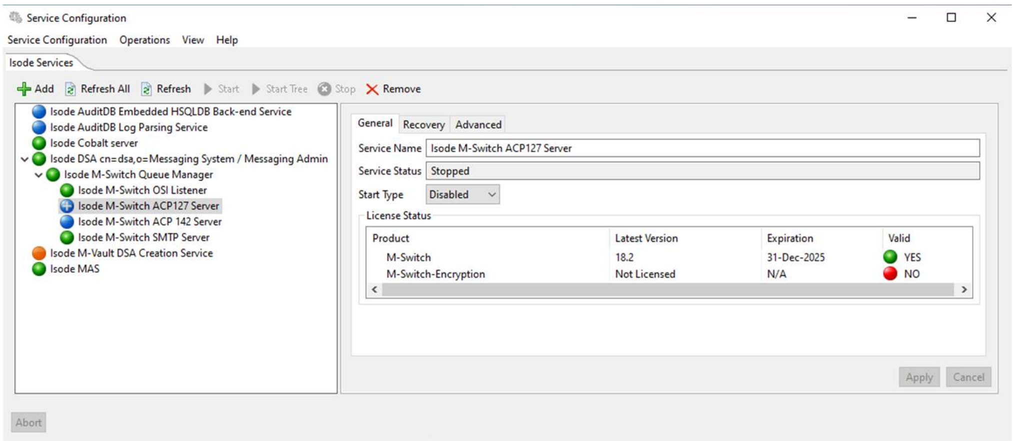
```
> Address Conversion Tables
> Routing Trees
v Message Transfer Agents
  v MU-ONE.FIELD.NET
    v Channels
        822-local
      > acp127
        acp127shaper
      > acp142-s4406e
        housekeeper
        lmtp
        mhsshaper
        military-dl
        mimecheck
        mimeshaper
        p3deliver
        p3server
        smtp-auth
        smtp-dl
        smtp-external
        smtp-internal
        x400-dl
        x400mt
        x400p1
      v acp142-mule
          HFAP-ONE HEADQUARTERS ACP142 MULE
```

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


Service Configuration
Service Configuration Operations View Help
Isode Services
Add Refresh All Refresh Start Start Tree Stop Remove
Isode AuditDB Embedded HSQLDB Back-end Service
Isode AuditDB Log Parsing Service
Isode Cobalt server
Isode DSA cn=dsa,o=Messaging System / Messaging Admin
Isode M-Switch Queue Manager
Isode M-Switch OSI Listener
Isode M-Switch ACP127 Server
Isode M-Switch ACP 142 Server
Isode M-Switch SMTP Server
Isode M-Vault DSA Creation Service
Isode MAS
General Recovery Advanced
Apply Cancel
Abort

Service Name: Isode M-Switch ACP127 Server

Service Status: Stopped

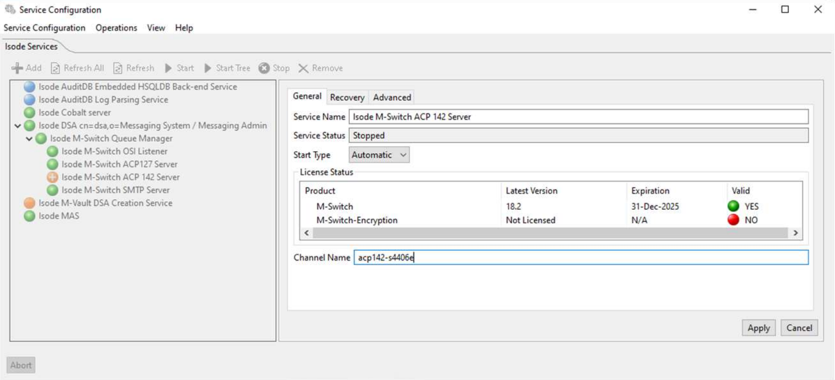
Start Type: Disabled

License Status

Product	Latest Version	Expiration	Valid
M-Switch	18.2	31-Dec-2025	● YES
M-Switch-Encryption	Not Licensed	N/A	● NO

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


Service Configuration
Service Configuration Operations View Help
Isode Services
Add Refresh All Refresh Start Start Tree Stop Remove
Isode AuditDB Embedded HSQLDB Back-end Service
Isode AuditDB Log Parsing Service
Isode Cobalt server
Isode DSA cn=dsa,o=Messaging System / Messaging Admin
Isode M-Switch Queue Manager
Isode M-Switch OSI Listener
Isode M-Switch ACP127 Server
Isode M-Switch ACP 142 Server
Isode M-Switch SMTP Server
Isode M-Vault DSA Creation Service
Isode MAS
General Recovery Advanced
Apply Cancel
Abort

Service Name: Isode M-Switch ACP 142 Server

Service Status: Stopped

Start Type: Automatic

License Status

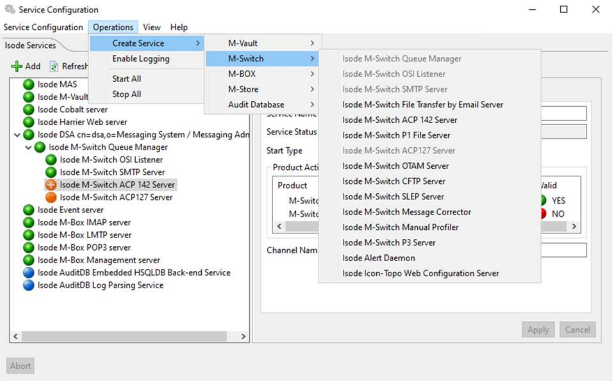
Product	Latest Version	Expiration	Valid
M-Switch	18.2	31-Dec-2025	● YES
M-Switch-Encryption	Not Licensed	N/A	● NO

Channel Name: acp142-s4406e

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

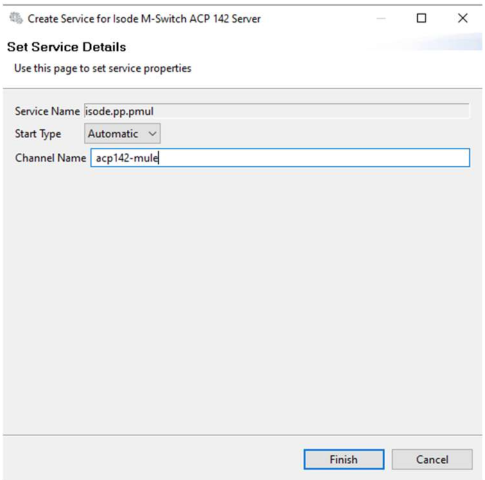
To transport non mmhs messages using mule, add an additional acp142 service.

Add ACP142 Mule service


Service Configuration
Service Configuration Operations View Help
Isode Services
Add Refresh
Create Service
Enable Logging
Start All
Stop All
M-Vault
M-Switch
M-BOX
M-Store
Audit Database
Isode M-Switch Queue Manager
Isode M-Switch OSI Listener
Isode M-Switch SMTP Server
Isode M-Switch File Transfer by Email Server
Isode M-Switch ACP 142 Server
Isode M-Switch P1 File Server
Isode M-Switch ACP127 Server
Isode M-Switch OTAM Server
Isode M-Switch CFTP Server
Isode M-Switch SLEP Server
Isode M-Switch Message Corrector
Isode M-Switch Manual Profiler
Isode M-Switch P3 Server
Isode Alert Daemon
Isode Icon-Topo Web Configuration Server
Isode MAS
Isode M-Vault
Isode Cobalt server
Isode Harrier Web server
Isode DSA cn=dsa,o=Messaging System / Messaging Adn
Isode M-Switch Queue Manager
Isode M-Switch OSI Listener
Isode M-Switch SMTP Server
Isode M-Switch ACP 142 Server
Isode M-Switch ACP127 Server
Isode Event server
Isode M-Box IMAP server
Isode M-Box LMTP server
Isode M-Box POP3 server
Isode M-Box Management server
Isode AuditDB Embedded HSQLDB Back-end Service
Isode AuditDB Log Parsing Service
Service Status
Start Type
Product Acti
Product
M-Switc
M-Switc
Valid
YES
NO
Channel Nam
Apply Cancel
Abort

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

Name the ACP142-mule Channel



Set Service Details

Use this page to set service properties

Service Name: isode.pp.pmul

Start Type: Automatic

Channel Name: acp142-mule

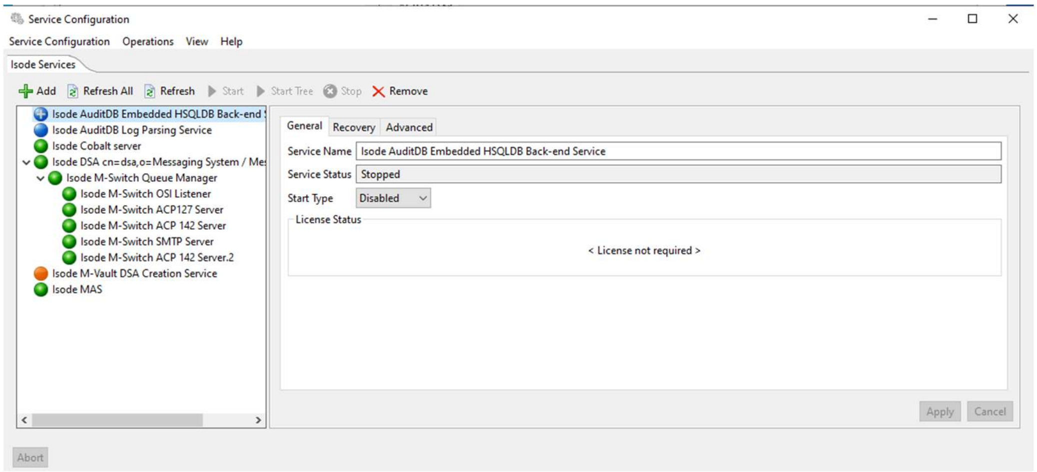
Ensure “Start Type” is “Automatic”

Name the channel “acp142-mule”

Press “Finish”

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

Services Started



- Isode AuditDB Embedded HSQLDB Back-end S
- Isode AuditDB Log Parsing Service
- Isode Cobalt server
- Isode DSA cn=dsa,o=Messaging System / Mes
  - Isode M-Switch Queue Manager
    - Isode M-Switch OSI Listener
    - Isode M-Switch ACP127 Server
    - Isode M-Switch ACP 142 Server
    - Isode M-Switch SMTP Server
    - Isode M-Switch ACP 142 Server.2
- Isode M-Vault DSA Creation Service
- Isode MAS

Service Name: Isode AuditDB Embedded HSQLDB Back-end Service

Service Status: Stopped

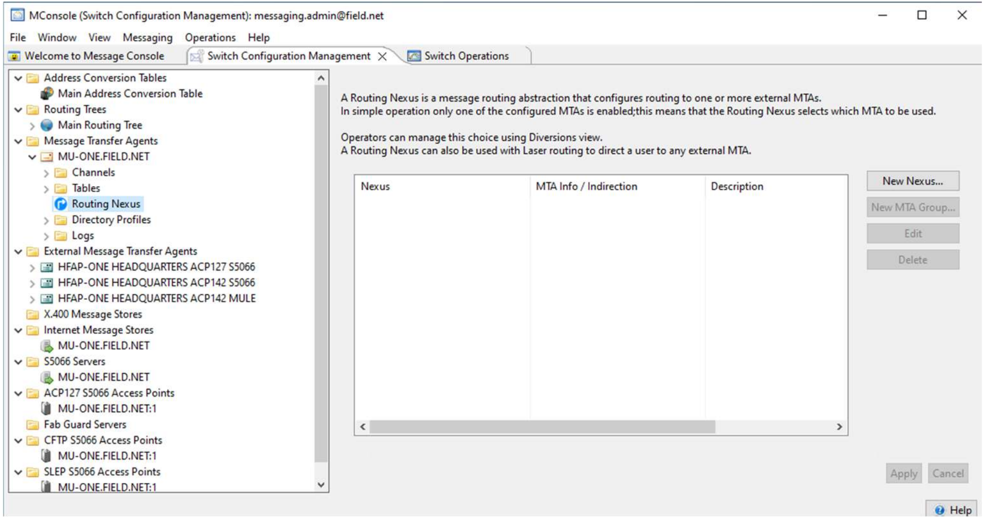
Start Type: Disabled

License Status: < License not required >

Configure the Routing Nexus

From the MConsole "Switch Configuration Management" view select "Routing Nexus".

Select the Routing Nexus

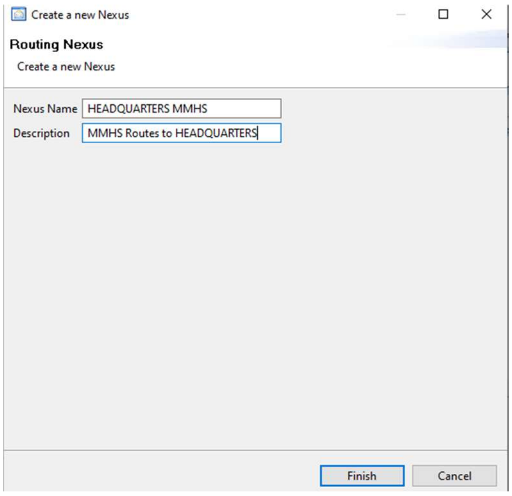


A Routing Nexus is a message routing abstraction that configures routing to one or more external MTAs.
In simple operation only one of the configured MTAs is enabled;this means that the Routing Nexus selects which MTA to be used.

Operators can manage this choice using Diversions view.
A Routing Nexus can also be used with Laser routing to direct a user to any external MTA.

Click "New Nexus..."

Name the routing Nexus



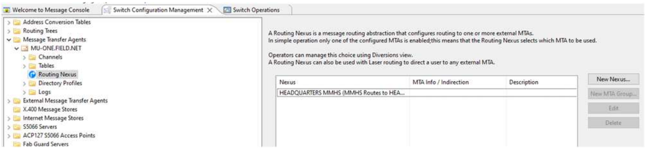
Nexus Name: HEADQUARTERS MMHS

Description: MMHS Routes to HEADQUARTERS

Enter a "Nexus Name" and Description of your choice.

Click "Finish".

New nexus created



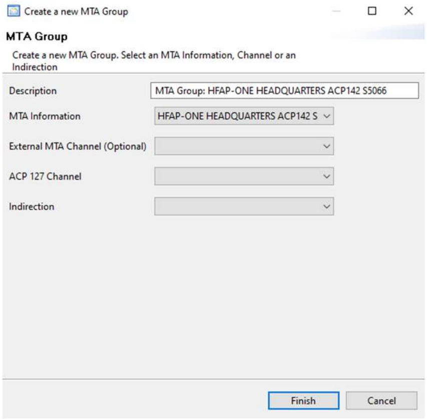
A Routing Nexus is a message routing abstraction that configures routing to one or more external MTAs.
In simple operation only one of the configured MTAs is enabled;this means that the Routing Nexus selects which MTA to be used.

Operators can manage this choice using Diversions view.
A Routing Nexus can also be used with Laser routing to direct a user to any external MTA.

Nexus	MTA Info / Indirection	Description
HEADQUARTERS MMHS (MMHS Routes to HEA...		

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

Create ACP142 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

External MTA Channel (Optional)

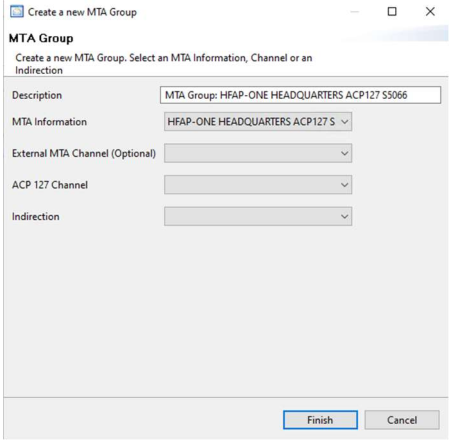
ACP 127 Channel

Indirection

Select the ACP142 S5066 MTA from the “MTA Information” dropdown and Click “Finish”.

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

Add the ACP127 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

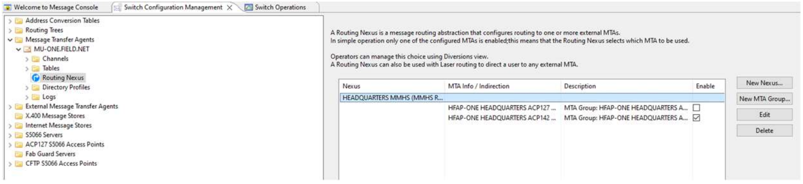
External MTA Channel (Optional)

ACP 127 Channel

Indirection

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 Diversions view.
A Routing Nexus can also be used with Laser 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...	□
	HFAP-ONE HEADQUARTERS ACP142 ...	MTA Group: HFAP-ONE HEADQUARTERS A...	☑

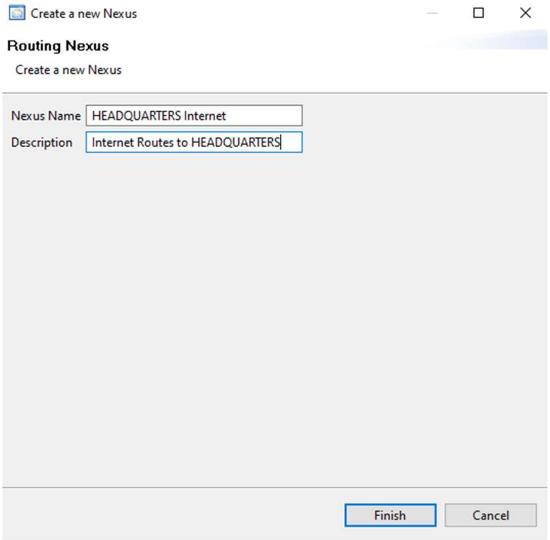
Note that the ACP142 S5066 routing group has been enabled. The switch nexus will use that group for routing unless modified.

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



Create a new Nexus

Routing Nexus

Create a new Nexus

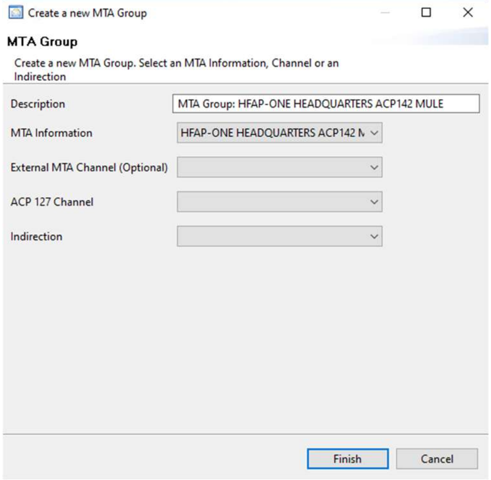
Nexus Name: HEADQUARTERS Internet

Description: Internet Routes to HEADQUARTERS

Press “Finish”

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

Mule MTA Group



Create a new MTA Group

MTA Group

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

Description: MTA Group: HFAP-ONE HEADQUARTERS ACP142 MULE

MTA Information: HFAP-ONE HEADQUARTERS ACP142 N

External MTA Channel (Optional):

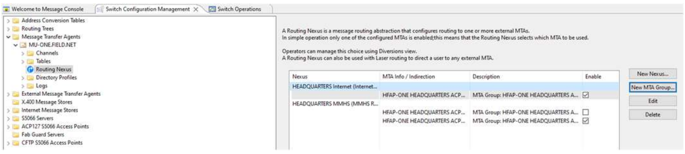
ACP 127 Channel:

Indirection:

Select the ACP142 MULE MTA.

Press “Finish”

Two nexus created



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 Diversions view.
A Routing Nexus can also be used with Laser routing to direct a user to any external MTA.

Nexus	MTA Info / Indirection	Description	Enable
HEADQUARTERS Internet (Internet...			
	HFAP-ONE HEADQUARTERS ACP...	MTA Group: HFAP-ONE HEADQUARTERS A...	☑
HEADQUARTERS MMHS (MMHS R...			
	HFAP-ONE HEADQUARTERS ACP...	MTA Group: HFAP-ONE HEADQUARTERS A...	☐
	HFAP-ONE HEADQUARTERS ACP...	MTA Group: HFAP-ONE HEADQUARTERS A...	☑

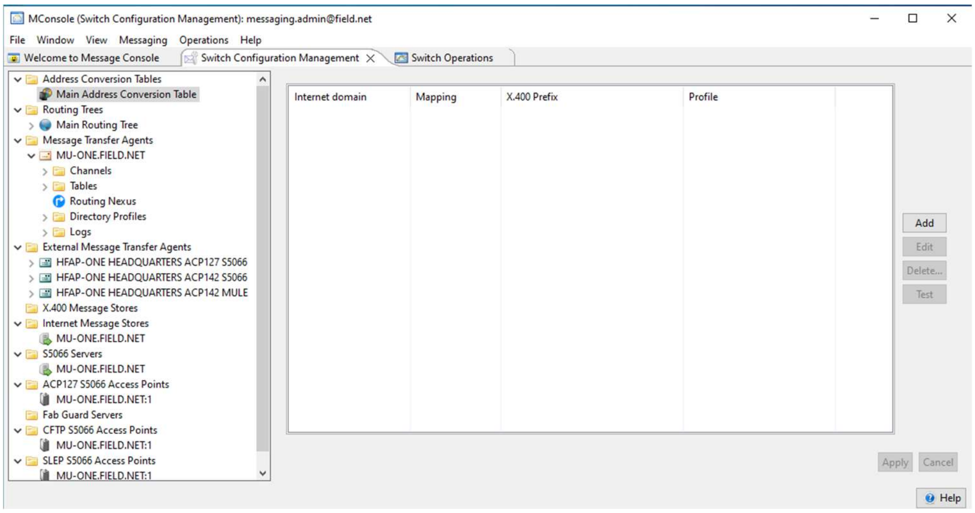
The nexus are now created and we can configure the Address Mapping.

Configure Address Mapping

Address mapping is used to convert between SMTP and X400 addresses and vice versa.

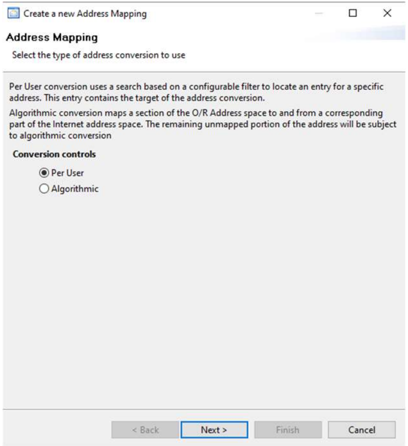
From the “Switch Configuration Management” view, select “Main Address Conversion Table”.

Select the Main Address Conversion table



Click “Add”.

Select Per User Mapping



Address Mapping

Select the type of address conversion to use

Per User conversion uses a search based on a configurable filter to locate an entry for a specific address. This entry contains the target of the address conversion.

Algorithmic conversion maps a section of the O/R Address space to and from a corresponding part of the Internet address space. The remaining unmapped portion of the address will be subject to algorithmic conversion

Conversion controls

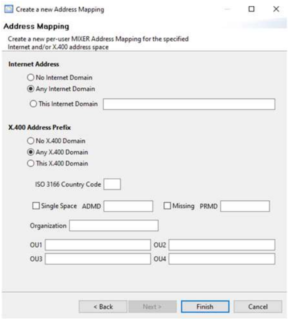
● Per User

○ Algorithmic

Leave the default settings

Click “Next >”.

Define address mapping



Create a new Address Mapping

Address Mapping

Create a new per-user MIXER Address Mapping for the specified Internet and/or X.400 address space

Internet Address

○ No Internet Domain
● Any Internet Domain
○ This Internet Domain

X.400 Address Prefix

○ No X.400 Domain
● Any X.400 Domain
○ This X.400 Domain

ISO 3166 Country Code

□ Single Space ADMD □ Missing PRMD

Organization

OU1 OU2
OU3 OU4

Leave the default settings

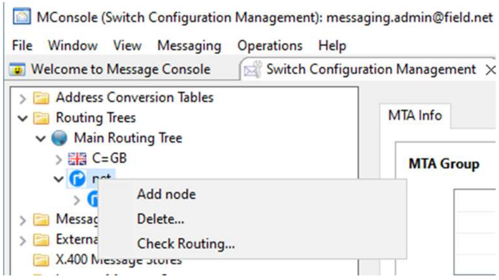
Click “Finish”.

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”.

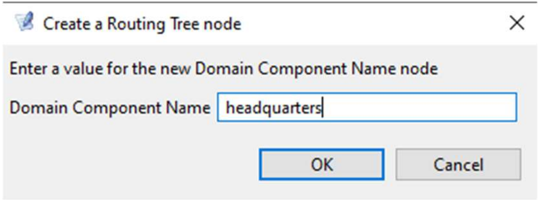
Add a routing node



MConsole (Switch Configuration Management): messaging.admin@field.net

Enter “headquarters” for the “Domain Component Name”

Add headquarters node



Create a Routing Tree node

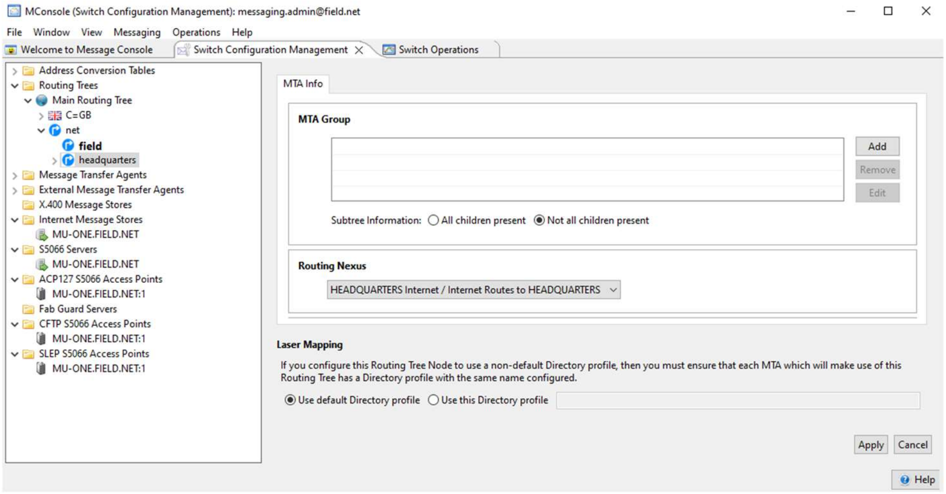
Enter a value for the new Domain Component Name node

Domain Component Name: headquarters

Click “OK”.

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

Configure headquarters route



MConsole (Switch Configuration Management): messaging.admin@field.net

Subtree Information: ○ All children present ● Not all children present

Routing Nexus: HEADQUARTERS Internet / Internet Routes to HEADQUARTERS

Laser Mapping

If you configure this Routing Tree Node to use a non-default Directory profile, then you must ensure that each MTA which will make use of this Routing Tree has a Directory profile with the same name configured.

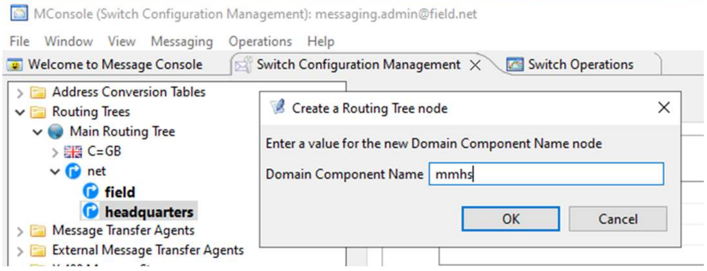
● Use default Directory profile ○ Use this Directory profile

Click “Apply”.

Right click on the new “headquarters” routing node.

Select “Add node”.

Add mmhs domain component



MConsole (Switch Configuration Management): messaging.admin@field.net

Create a Routing Tree node

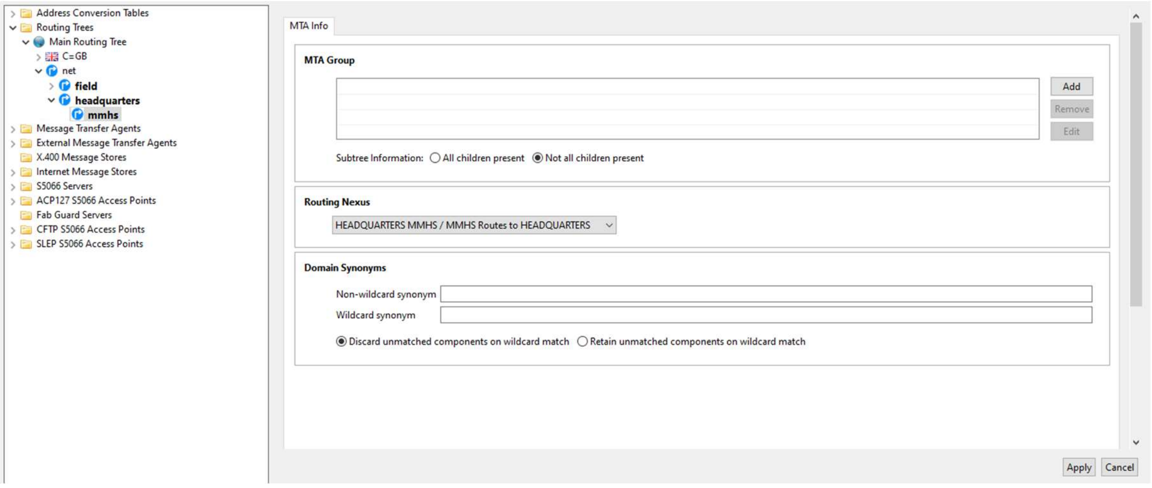
Enter a value for the new Domain Component Name node

Domain Component Name: mmhs

Enter "mmhs" for the "Domain Component Name"

Press "OK"

Edit MTA info



MTA Info

MTA Group

Subtree Information: ○ All children present ● Not all children present

Routing Nexus: HEADQUARTERS MMHS / MMHS Routes to HEADQUARTERS

Domain Synonyms

Non-wildcard synonym:

Wildcard synonym:

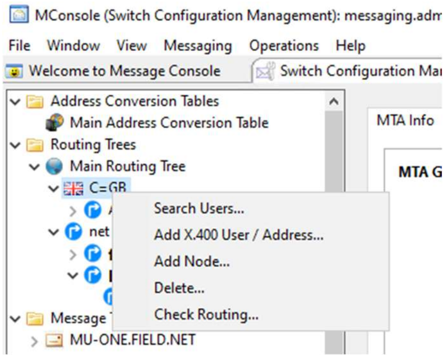
● Discard unmatched components on wildcard match ○ Retain unmatched components on wildcard match

In the "Routing Nexus" frame Select the MMHS Routing Nexus you have created

Press "Apply"

Add the X4oo routing entry "a=HEADQUARTERS" by right clicking over "C=GB" in the routing tree

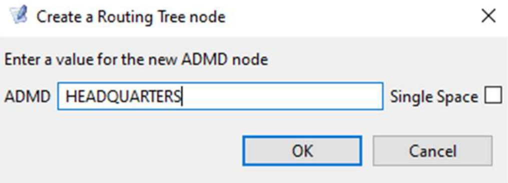
Add x400 node



MConsole (Switch Configuration Management): messaging.adm

Select "Add node"

Add ADMD



Enter a value for the new ADMD node

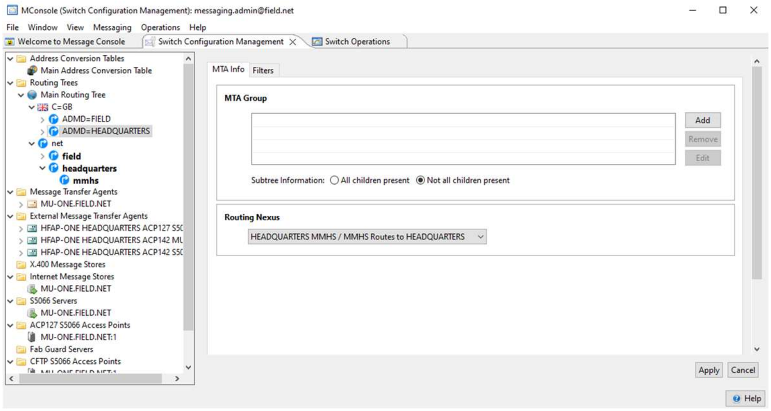
ADMD: HEADQUARTERS

Single Space □

Provide the ADMD “HEADQUARTERS”

Press “OK”

Associate with headquarters nexus



Subtree Information: ○ All children present ● Not all children present

Routing Nexus: HEADQUARTERS MMHS / MMHS Routes to HEADQUARTERS

Select the Routing Nexus “HEADQUARTERS MMHS”

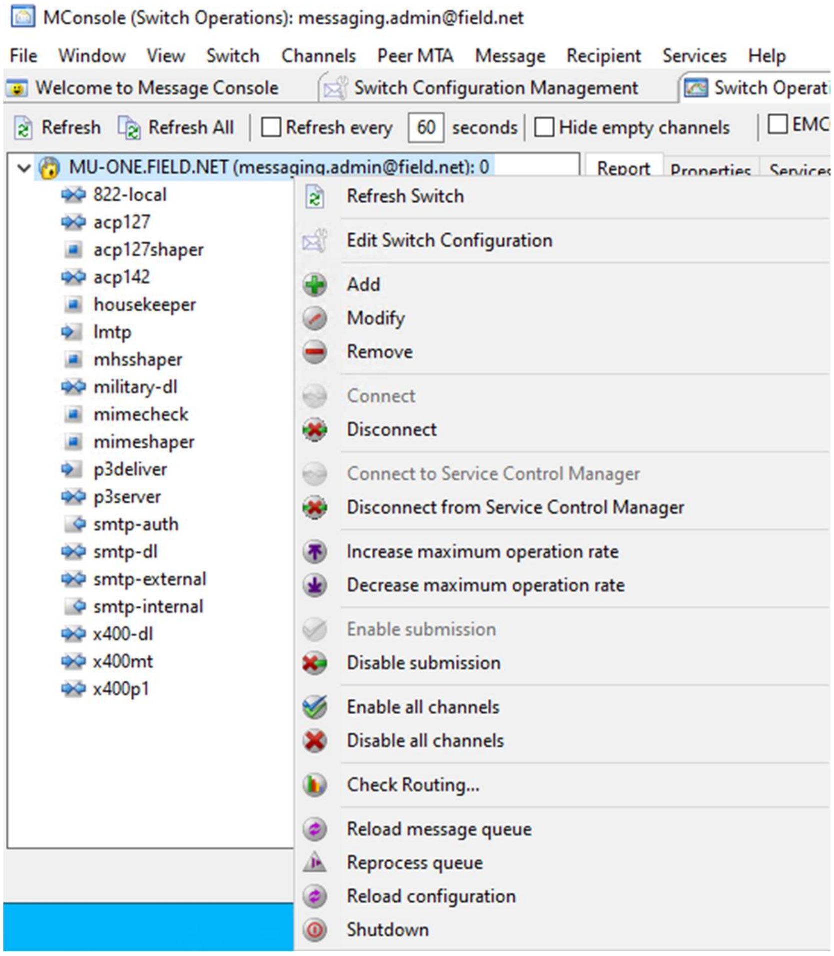
Press “Apply”

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”

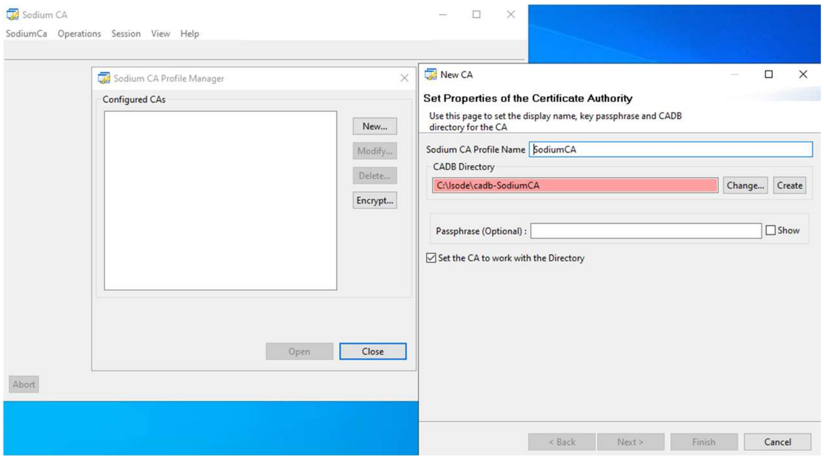
Open “Sodium CA” from the Windows start menu

Click “New”

On “Set Properties of the Certificate Authority” leave Defaults

Click “Create”

create ca



Set Properties of the Certificate Authority

Use this page to set the display name, key passphrase and CADB directory for the CA

Sodium CA Profile Name: SodiumCA

CADB Directory: C:\Isode\cadb-SodiumCA

Passphrase (Optional) :

☑ Set the CA to work with the Directory

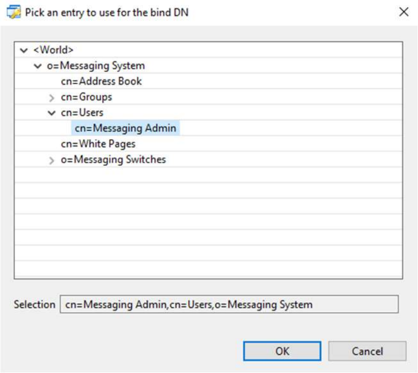
Click “Next >”

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



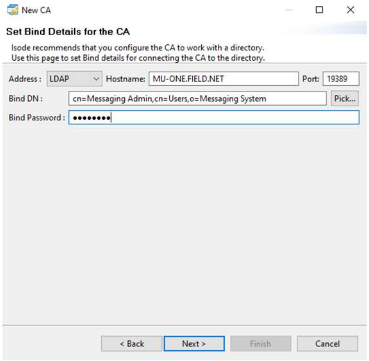
Pick an entry to use for the bind DN

<World>
- o=Messaging System
  - cn=Address Book
  - cn=Groups
  - cn=Users
    - cn=Messaging Admin
  - cn=White Pages
  - o=Messaging Switches

Selection: cn=Messaging Admin,cn=Users,o=Messaging System

Click “OK”

Define bind password



New CA

Set Bind Details for the CA

Isode recommends that you configure the CA to work with a directory.
Use this page to set Bind details for connecting the CA to the directory.

Address: LDAP Hostname: MU-ONE.FIELD.NET Port: 19389

Bind DN: cn=Messaging Admin,cn=Users,o=Messaging System

Bind Password: ••••••••

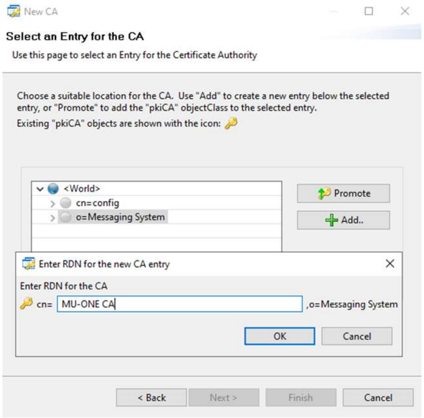
In “Bind Password” type “Secret1+”

Click “Next >”

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

Click “Add”

create ca directory entry



New CA

Select an Entry for the CA

Use this page to select an Entry for the Certificate Authority

Choose a suitable location for the CA. Use "Add" to create a new entry below the selected entry, or "Promote" to add the "pkiCA" objectClass to the selected entry.
Existing "pkiCA" objects are shown with the icon: 🔑

<World>
- cn=config
- o=Messaging System

Enter RDN for the new CA entry

Enter RDN for the CA

cn= MU-ONE CA ,o=Messaging System

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

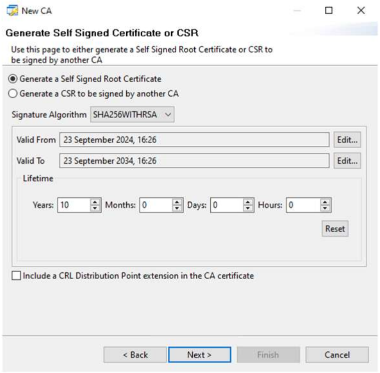
Click “Next >”

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



New CA

Generate Self Signed Certificate or CSR

Use this page to either generate a Self Signed Root Certificate or CSR to be signed by another CA

● Generate a Self Signed Root Certificate
○ Generate a CSR to be signed by another CA

Signature Algorithm: SHA256WITHRSA

Valid From: 23 September 2024, 16:26
Valid To: 23 September 2034, 16:26

Lifetime
Years: 10 Months: 0 Days: 0 Hours: 0

□ Include a CRL Distribution Point extension in the CA certificate

Leave the defaults.

Click “Next >”

On “Root CA Certificate” leave Defaults

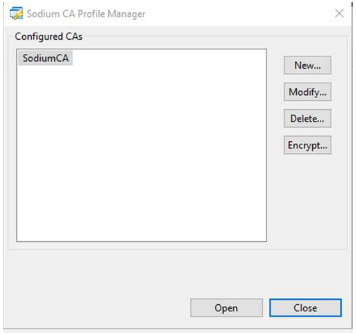
Click “Next >”

On “Finish CA Configuration” press “Finish”

On ”Sodium CA Profile Manager” select “SodiumCA”

Click “Open”

open configured ca



Sodium CA Profile Manager

Configured CAs

SodiumCA

In “Password” type “Secret1+”

Click “OK”

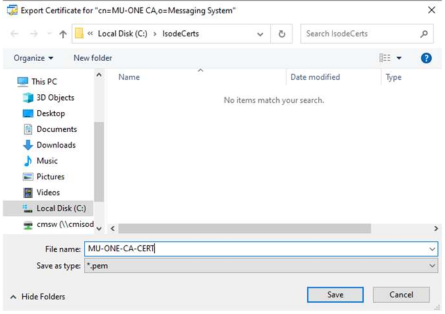
Select “Certificate for cn=MU-ONE CA, o=Messaging System”

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



Export Certificate for "cn=MU-ONE CA,o=Messaging System"

« Local Disk (C:) › IsodeCerts

No items match your search.

File name: MU-ONE-CA-CERT

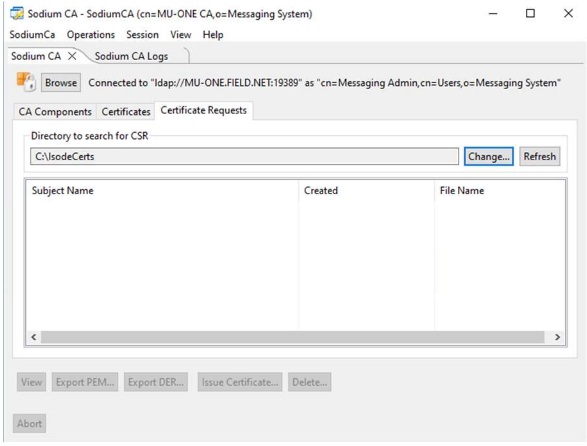
Save as type: *.pem

Press “Save”

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

Change to “Certificate Requests” tab

CSR directory changed



Sodium CA - SodiumCA (cn=MU-ONE CA,o=Messaging System)

Connected to "ldap://MU-ONE.FIELD.NET:19389" as "cn=Messaging Admin,cn=Users,o=Messaging System"

Directory to search for CSR: C:\IsodeCerts

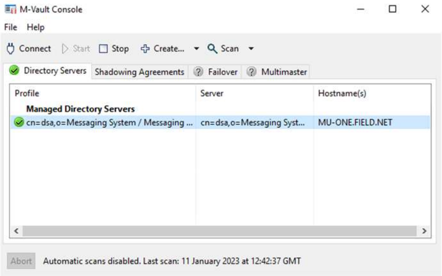
Subject Name	Created	File Name

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



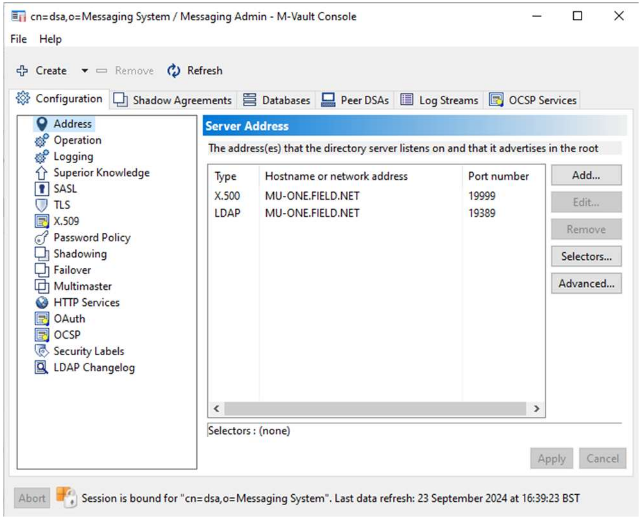
M-Vault Console

Profile	Server	Hostname(s)
Managed Directory Servers		
cn=dsa,o=Messaging System / Messaging ...	cn=dsa,o=Messaging Syst...	MU-ONE.FIELD.NET

Automatic scans disabled. Last scan: 11 January 2023 at 12:42:37 GMT

Double Click on the “Managed Directory server”

Directory configuration



Server Address

The address(es) that the directory server listens on and that it advertises in the root

Type	Hostname or network address	Port number
X.500	MU-ONE.FIELD.NET	19999
LDAP	MU-ONE.FIELD.NET	19389

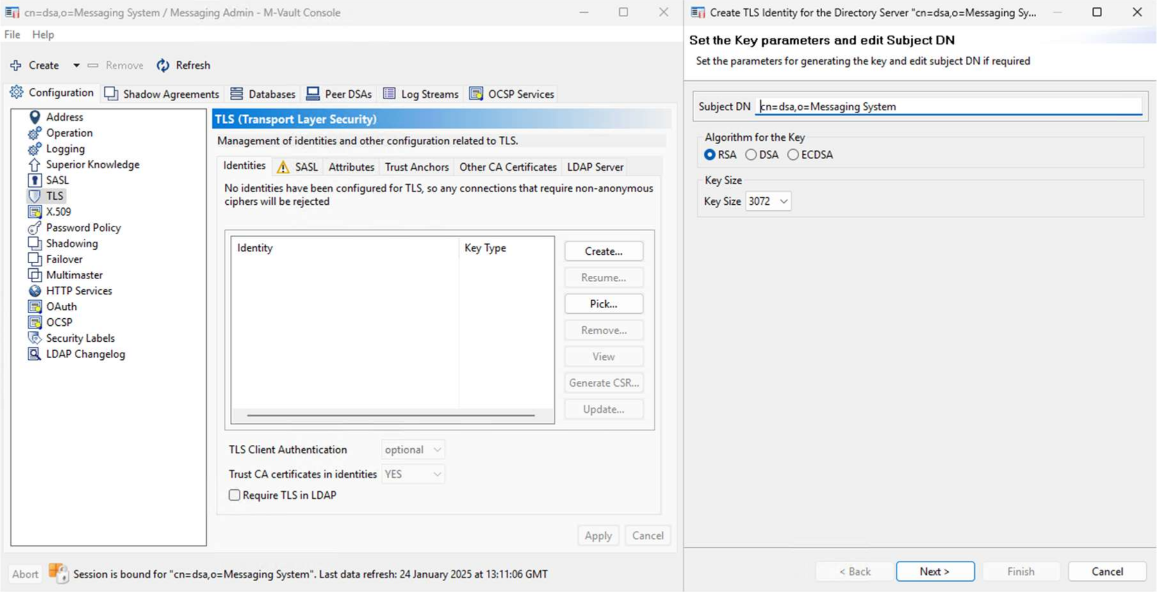
Selectors : (none)

Session is bound for "cn=dsa,o=Messaging System". Last data refresh: 23 September 2024 at 16:39:23 BST

Select “TLS” on the left-hand side of the “Configuration” tab

On the “Identities” tab Press “Create”

Create TLS identity



TLS (Transport Layer Security)

Management of identities and other configuration related to TLS.

No identities have been configured for TLS, so any connections that require non-anonymous ciphers will be rejected

Identity	Key Type

TLS Client Authentication: optional

Trust CA certificates in identities: YES

☐ Require TLS in LDAP

Session is bound for "cn=dsa,o=Messaging System". Last data refresh: 24 January 2025 at 13:11:06 GMT

Set the Key parameters and edit Subject DN

Set the parameters for generating the key and edit subject DN if required

Subject DN: cn=dsa,o=Messaging System

Algorithm for the Key: ● RSA ○ DSA ○ ECDSA

Key Size: Key Size 3072

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

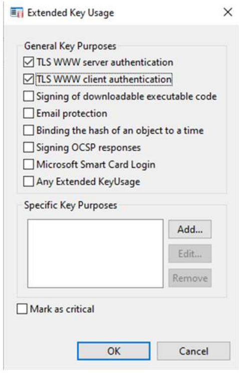
Click “Next >”

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

Click “Next >”

On “Select X.509 Extensions”, press “Edit..”

Extended Key Usage



Extended Key Usage

General Key Purposes

☑ TLS WWW server authentication
☑ TLS WWW client authentication
☐ Signing of downloadable executable code
☐ Email protection
☐ Binding the hash of an object to a time
☐ Signing OCSP responses
☐ Microsoft Smart Card Login
☐ Any Extended KeyUsage

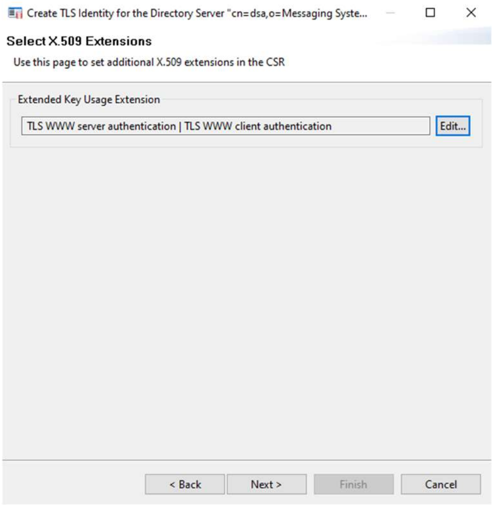
Specific Key Purposes

☐ Mark as critical

Check “TLS WWW client authentication”

Press “OK”

X.509 Extensions Selected



Create TLS Identity for the Directory Server "cn=dsa,o=Messaging Syste...

Select X.509 Extensions

Use this page to set additional X.509 extensions in the CSR

Extended Key Usage Extension

TLS WWW server authentication | TLS WWW client authentication

Press “Next >”

On “Certificate Request Contents” leave defaults

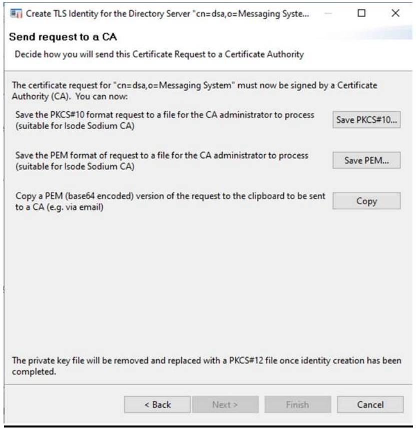
Press “Next >”

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*



Create TLS Identity for the Directory Server "cn=dsa,o=Messaging Syste...
Save PKCS#10...
Save PEM...
Copy
< Back
Next >
Finish
Cancel

Send request to a CA

Decide how you will send this Certificate Request to a Certificate Authority

The certificate request for "cn=dsa,o=Messaging System" must now be signed by a Certificate Authority (CA). You can now:

Save the PKCS#10 format request to a file for the CA administrator to process (suitable for Isode Sodium CA)

Save the PEM format of request to a file for the CA administrator to process (suitable for Isode Sodium CA)

Copy a PEM (base64 encoded) version of the request to the clipboard to be sent to a CA (e.g. via email)

The private key file will be removed and replaced with a PKCS#12 file once identity creation has been completed.

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:

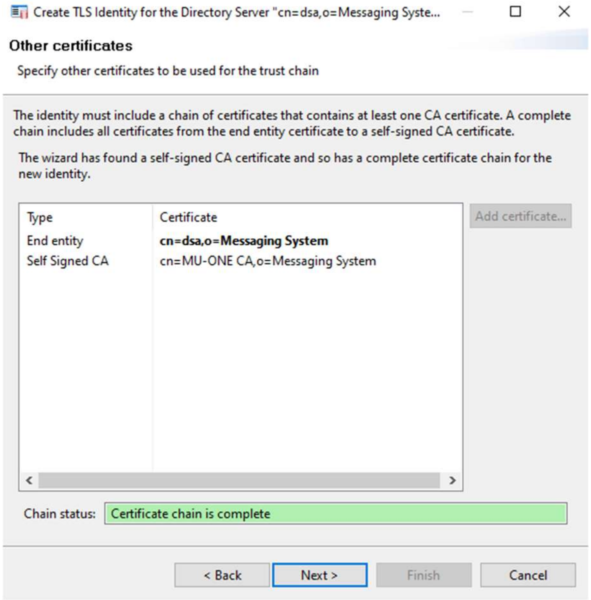
Select “The CA has provided a certificate”

Click “Next >”

On “User Certificate” leave defaults

Click “Next >”

Other certificates



Create TLS Identity for the Directory Server "cn=dsa,o=Messaging Syste...
Add certificate...
< Back
Next >
Finish
Cancel

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
End entity	**cn=dsa,o=Messaging System**
Self Signed CA	cn=MU-ONE CA,o=Messaging System

Chain status: Certificate chain is complete

On “Other Certificates” leave defaults

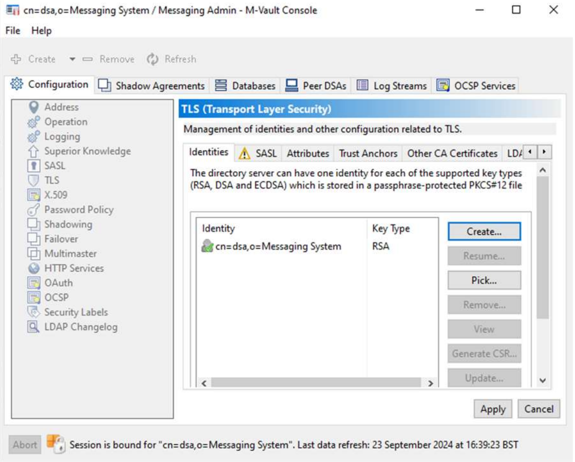
Click “Next >”

On “Finish directory servers Identity creation” leave defaults

Click “Finish”

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

apply TLS identity



TLS (Transport Layer Security)

Management of identities and other configuration related to TLS.

The directory server can have one identity for each of the supported key types (RSA, DSA and ECDSA) which is stored in a passphrase-protected PKCS#12 file

Identity	Key Type
cn=dsa,o=Messaging System	RSA

Session is bound for "cn=dsa,o=Messaging System". Last data refresh: 23 September 2024 at 16:39:23 BST

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

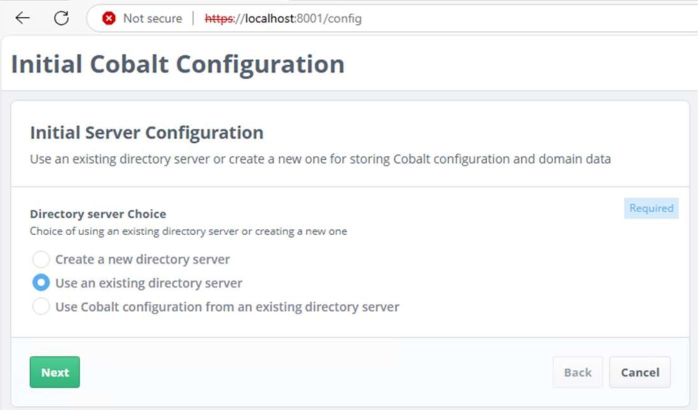
Select “Operations/Start all”

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



Not secure | ~~https~~://localhost:8001/config

Initial Cobalt Configuration

Initial Server Configuration

Use an existing directory server or create a new one for storing Cobalt configuration and domain data

Directory server Choice Required

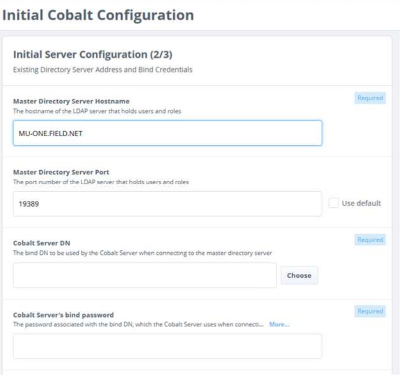
Choice of using an existing directory server or creating a new one

- ○ Create a new directory server
- ● Use an existing directory server
- ○ Use Cobalt configuration from an existing directory server

On “Initial Server Configuration” select “Use an existing directory server”

Press “Next”

Define Cobalt directory server



Initial Cobalt Configuration

Initial Server Configuration (2/3)

Existing Directory Server Address and Bind Credentials

Master Directory Server Hostname Required

The hostname of the LDAP server that holds users and roles

MU-ONE.FIELD.NET

Master Directory Server Port

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

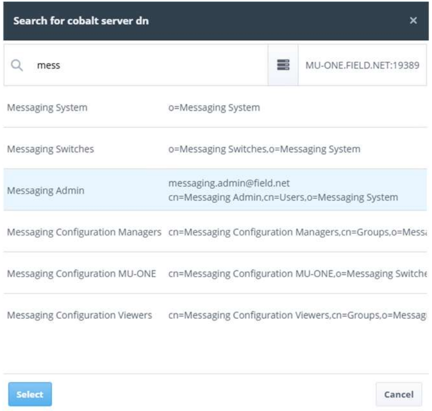
Cobalt Server's bind password Required

The password associated with the bind DN, which the Cobalt Server uses when connecti... More...

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

Click “Choose”.

Locate Messaging Admin



Search for cobalt server dn

mess | MU-ONE.FIELD.NET:19389

Messaging System	o=Messaging System
Messaging Switches	o=Messaging Switches,o=Messaging System
Messaging Admin	messaging.admin@field.net cn=Messaging Admin,cn=Users,o=Messaging System
Messaging Configuration Managers	cn=Messaging Configuration Managers,cn=Groups,o=Mess
Messaging Configuration MU-ONE	cn=Messaging Configuration MU-ONE,o=Messaging Switche
Messaging Configuration Viewers	cn=Messaging Configuration Viewers,cn=Groups,o=Messag

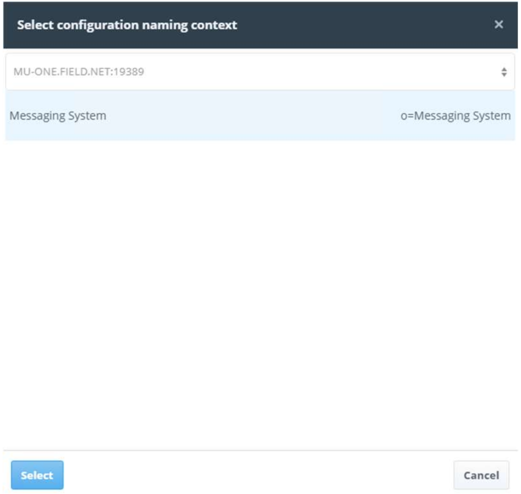
Start typing your “Initial Directory User”, Select it and Click “Select”.

Scroll down and enter the Password for the “Initial Directory User”.

Set “TLS Identity Check” to “False”

Press “Choose” next to “Configuration Naming Context”

Select configuration naming context



Select configuration naming context

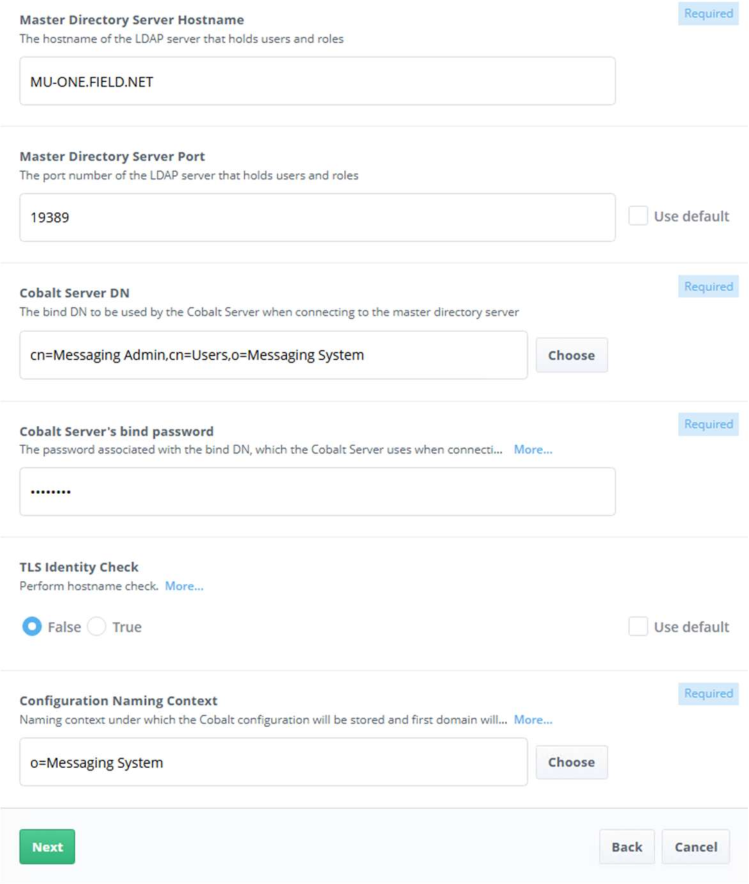
MU-ONE.FIELD.NET:19389

Messaging System	o=Messaging System

Click on “Messaging System”

Click “Select”

Configuration Naming Context Selected



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

Master Directory Server Port
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=Messaging Admin,cn=Users,o=Messaging System

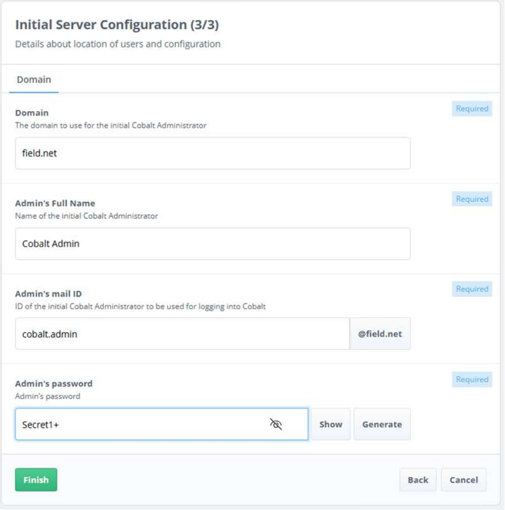
Cobalt Server's bind password (Required)
The password associated with the bind DN, which the Cobalt Server uses when connecti... More...
••••••••

TLS Identity Check
Perform hostname check. More...
● False ○ True
□ Use default

Configuration Naming Context (Required)
Naming context under which the Cobalt configuration will be stored and first domain will... More...
o=Messaging System

Click “Next”.

Define Cobalt domain



Initial Server Configuration (3/3)

Details about location of users and configuration

Domain

Domain

The domain to use for the initial Cobalt Administrator

field.net

Admin's Full Name

Name of the initial Cobalt Administrator

Cobalt Admin

Admin's mail ID

ID of the initial Cobalt Administrator to be used for logging into Cobalt

cobalt.admin @field.net

Admin's password

Admin's password

Secret1+

Set the “Domain” to be “field.net”

Enter a Name of your choice for the “Admin’s Full Name”.

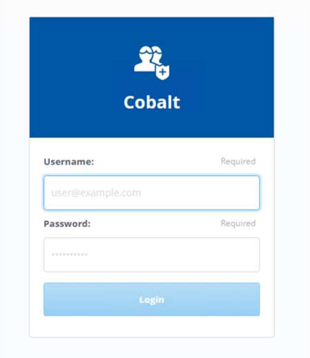
We will use “Cobalt Admin”

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



Cobalt

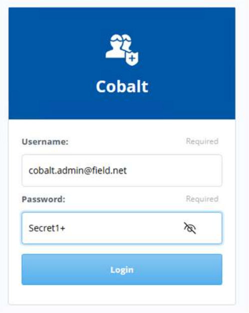
Username:

user@example.com

Password:

Enter the Cobalt Admin Email address and password

Cobalt login credentials



Cobalt

Username:

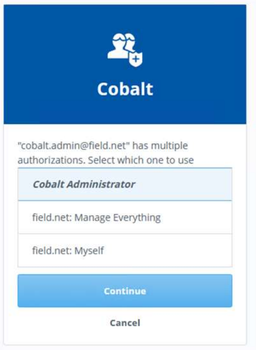
cobalt.admin@field.net

Password:

Secret1+

Click “Login”.

Cobalt Role Selection



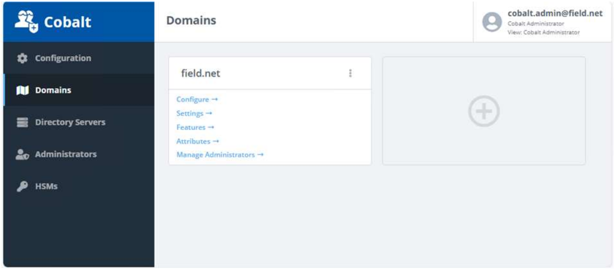
"cobalt.admin@field.net" has multiple authorizations. Select which one to use

Select “Cobalt Administrator” role.

Click “Continue”.

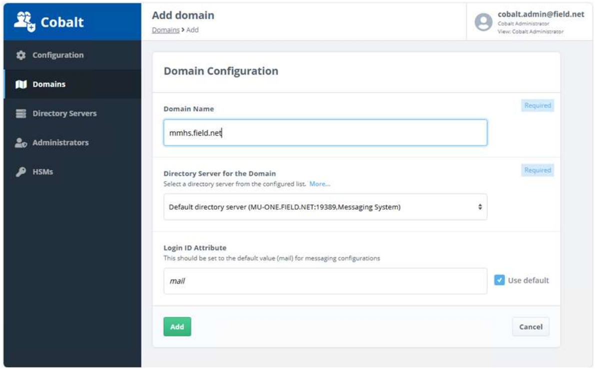
Define Cobalt Domains and Features

Initial domain configuration



Press the “+”

Configure mmhs.field.net domain



Domain Name: mmhs.field.net

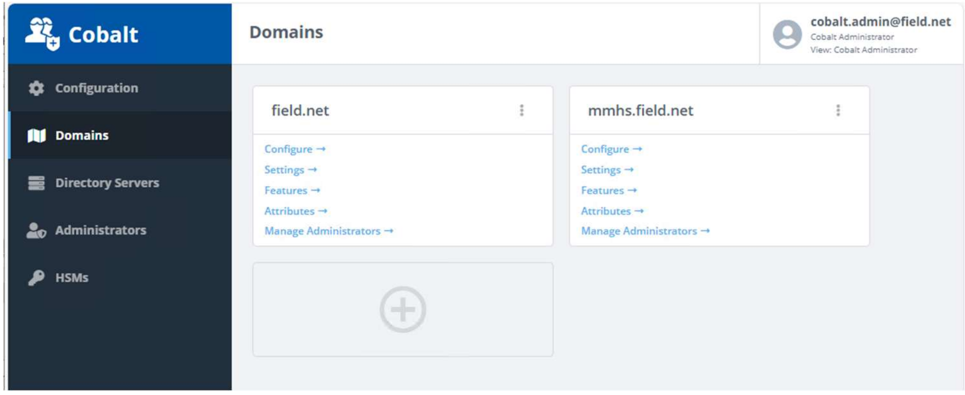
Directory Server for the Domain
Select a directory server from the configured list. More...
Default directory server (MU-ONE.FIELD.NET:19389,Messaging System)

Login ID Attribute
This should be set to the default value (mail) for messaging configurations
mail ☑ Use default

In “Domain Name” type “mmhs.field.net”

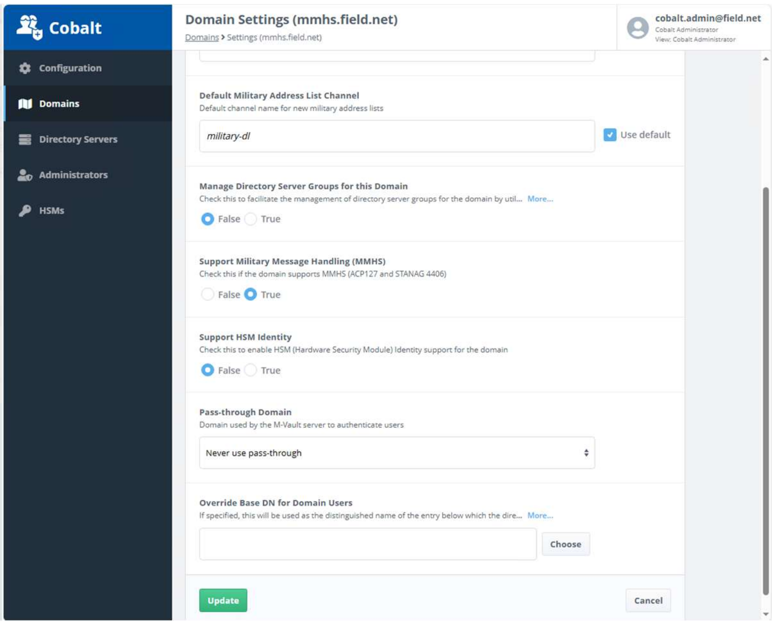
Press “Add”

mmhs.field.net domain added



Under the "mmhs.field.net" domain press "Settings"

Enable MMHS



Domain Settings (mmhs.field.net)

Domains > Settings (mmhs.field.net)

Default Military Address List Channel
Default channel name for new military address lists

military-dl ☑ Use default

Manage Directory Server Groups for this Domain
Check this to facilitate the management of directory server groups for the domain by util... More...

● False ○ True

Support Military Message Handling (MMHS)
Check this if the domain supports MMHS (ACP127 and STANAG 4406)

○ False ● True

Support HSM Identity
Check this to enable HSM (Hardware Security Module) Identity support for the domain

● False ○ True

Pass-through Domain
Domain used by the M-Vault server to authenticate users

Never use pass-through

Override Base DN for Domain Users
If specified, this will be used as the distinguished name of the entry below which the dire... More...

Choose

Update Cancel

Change "Support Military Message Handling (MMHS)" to "True"

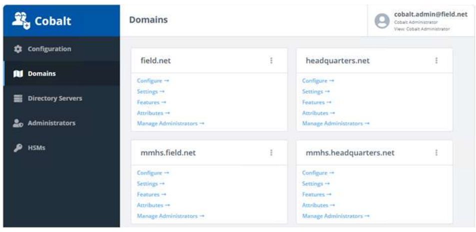
Press "Update"

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”

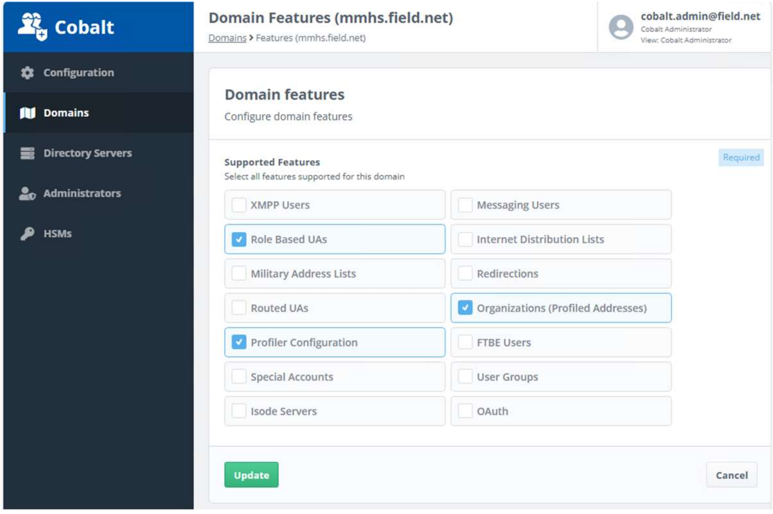
Ensure only the following domain features are checked:

Role Based UAs

Organizations (Profiled Addresses)

Profiler Configuration

mmhs.field.net domain features



Domain features

Configure domain features

Supported Features

Select all features supported for this domain

Required

☐ XMPP Users	☐ Messaging Users
☑ Role Based UAs	☐ Internet Distribution Lists
☐ Military Address Lists	☐ Redirections
☐ Routed UAs	☑ Organizations (Profiled Addresses)
☑ Profiler Configuration	☐ FTBE Users
☐ Special Accounts	☐ User Groups
☐ Isode Servers	☐ OAuth

Press “Update”

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

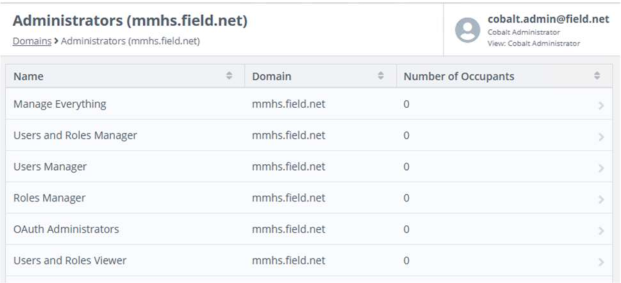
Role Based UA’s

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*



Administrators (mmhs.field.net)

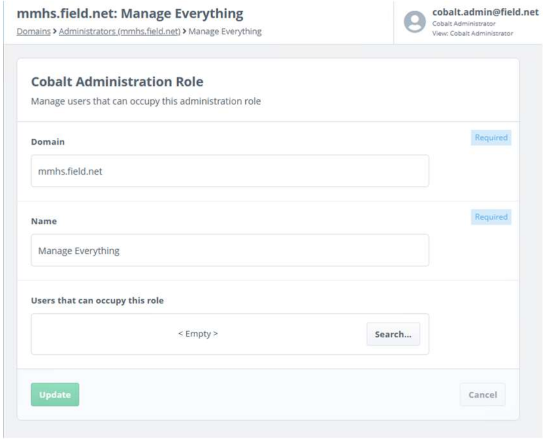
Domains > Administrators (mmhs.field.net)

cobalt.admin@field.net
Cobalt Administrator
View: Cobalt Administrator

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.admin@field.net
Cobalt Administrator
View: Cobalt Administrator

Cobalt Administration Role

Manage users that can occupy this administration role

Domain: mmhs.field.net (Required)

Name: Manage Everything (Required)

Users that can occupy this role: < Empty >

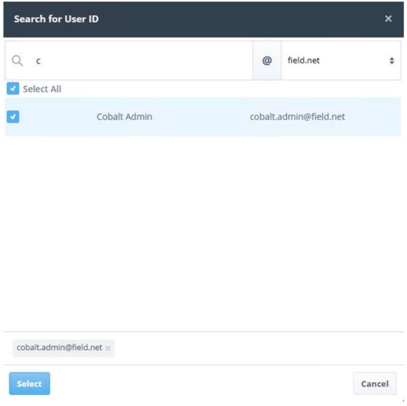
Press “Search”

Change the domain to “field.net”

Type “c” in search box

Check “Cobalt Admin”

Search for Cobalt admin



Search for User ID

c @ field.net

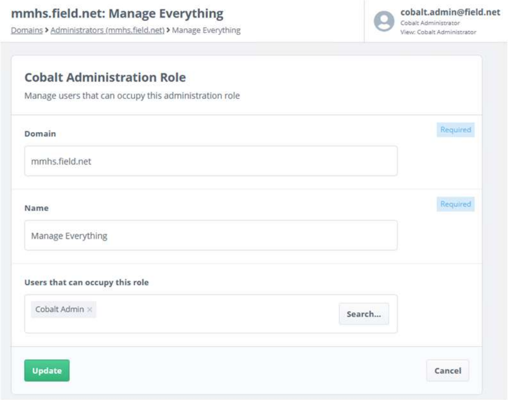
☑ Select All

☑ Cobalt Admin cobalt.admin@field.net

cobalt.admin@field.net ×

Press “Select”

Cobalt Admin Manages everything



mmhs.field.net: Manage Everything

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

Cobalt Administration Role

Manage users that can occupy this administration role

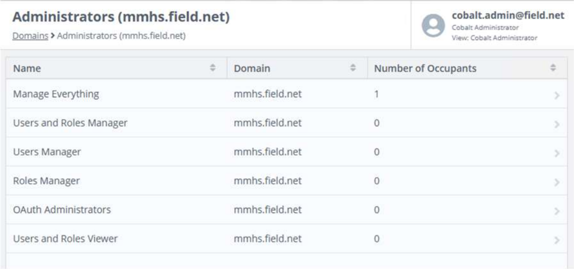
Domain (Required): mmhs.field.net

Name (Required): Manage Everything

Users that can occupy this role: Cobalt Admin ×

Press "Update"

mmhs.field.net has a manager



Administrators (mmhs.field.net)

Domains > Administrators (mmhs.field.net)

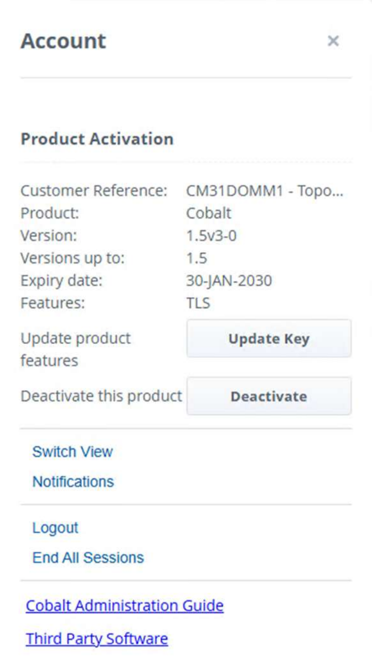
Name	Domain	Number of Occupants
Manage Everything	mmhs.field.net	1
Users and Roles Manager	mmhs.field.net	0
Users Manager	mmhs.field.net	0
Roles Manager	mmhs.field.net	0
OAuth Administrators	mmhs.field.net	0
Users and Roles Viewer	mmhs.field.net	0

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



Account ×

Product Activation

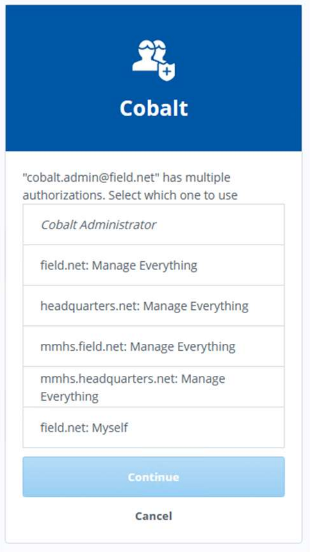
Customer Reference: CM31DOMM1 - Topo...
Product: Cobalt
Version: 1.5v3-0
Versions up to: 1.5
Expiry date: 30-JAN-2030
Features: TLS

Update product features — Update Key

Deactivate this product — Deactivate

Click "Switch View".

Switch to field.net view



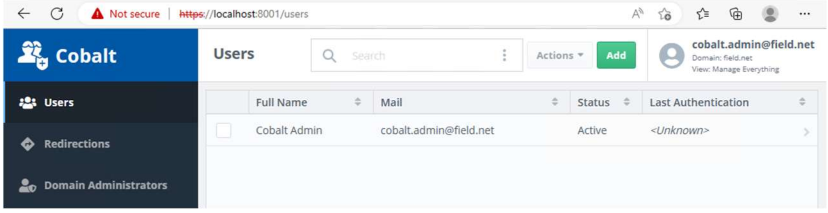
"cobalt.admin@field.net" has multiple authorizations. Select which one to use

- *Cobalt Administrator*
- field.net: Manage Everything
- headquarters.net: Manage Everything
- mmhs.field.net: Manage Everything
- mmhs.headquarters.net: Manage Everything
- field.net: Myself

Select "field.net: Manage Everything"

Click "Continue".

Field.net users



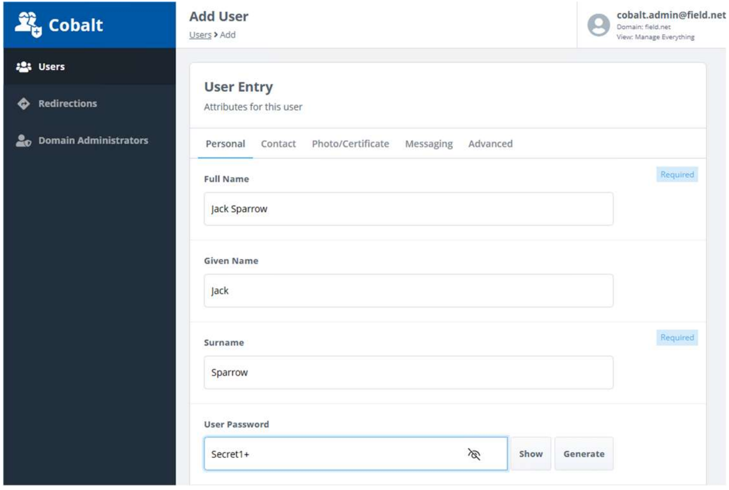
cobalt.admin@field.net
Domain: field.net
View: Manage Everything

	Full Name	Mail	Status	Last Authentication
□	Cobalt Admin	cobalt.admin@field.net	Active	<Unknown>

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



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

Full Name: Jack Sparrow

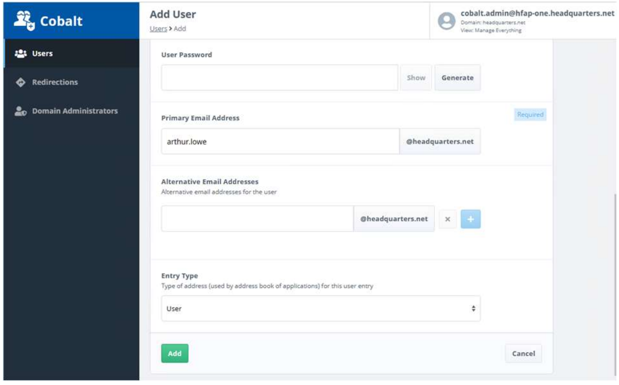
Given Name: Jack

Surname: Sparrow

User Password: Secret1+

Scroll to the bottom of the page and press "Add"

Add Jack Sparrow



cobalt.admin@hfap-one.headquarters.net
Domain: headquarters.net
View: Manage Everything

User Password:

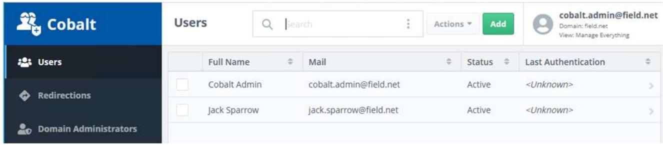
Primary Email Address: arthur.lowe @headquarters.net

Alternative Email Addresses
Alternative email addresses for the user
@headquarters.net

Entry Type
Type of address (used by address book of applications) for this user entry
User

Note that "Jack Sparrow" has been added to the directory

Jack Sparrow added

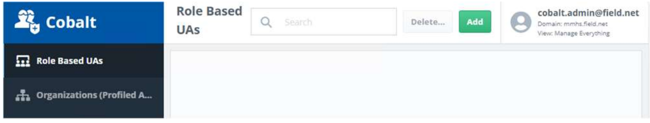


	Full Name	Mail	Status	Last Authentication
□	Cobalt Admin	cobalt.admin@field.net	Active	*<Unknown>*
□	Jack Sparrow	jack.sparrow@field.net	Active	*<Unknown>*

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

Select “Role Based UA’s”

Empty Role based UA’s

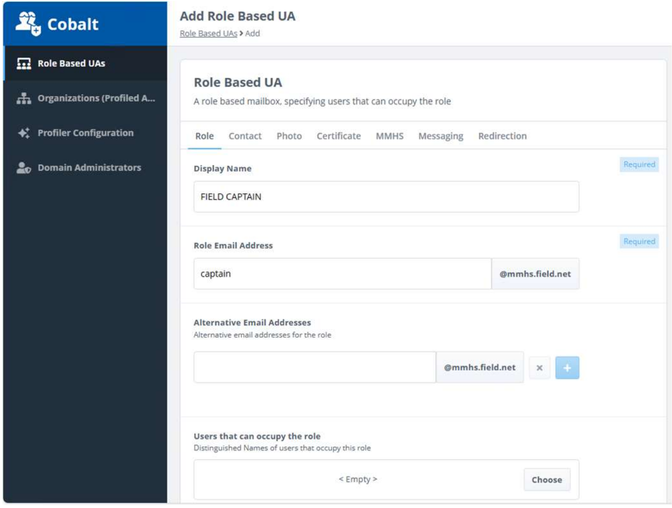


Click “Add”

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

Display Name: FIELD CAPTAIN

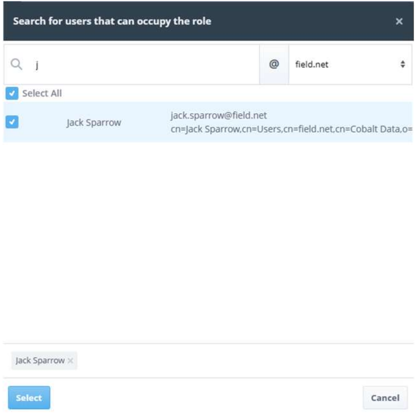
Role Email Address: captain @mmhs.field.net

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

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

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

select Role Occupant



Search for users that can occupy the role

j @ field.net

☑ Select All

☑ Jack Sparrow jack.sparrow@field.net
cn=Jack Sparrow,cn=Users,cn=field.net,cn=Cobalt Data,o=

Jack Sparrow ×

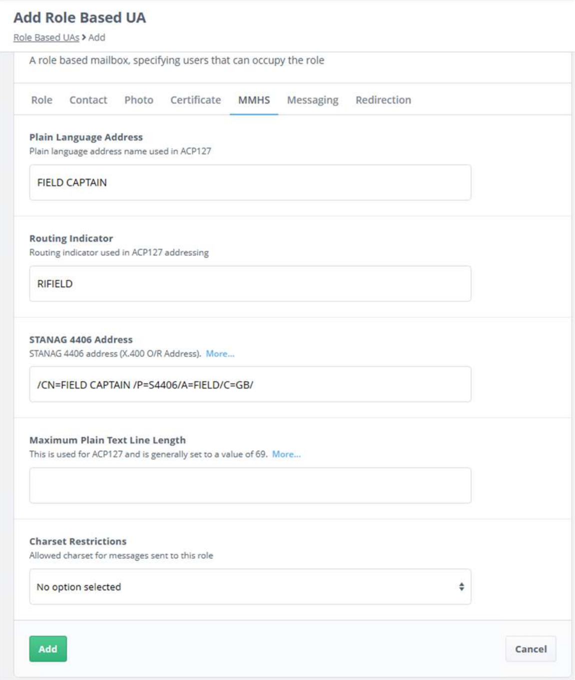
Search for “j” in domain “field.net”

Check “Jack Sparrow”

Press “Select”

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

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...

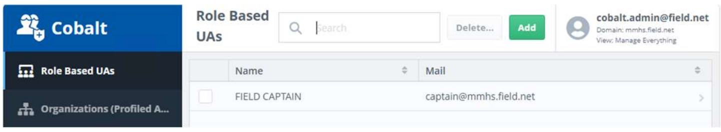
Charset Restrictions
Allowed charset for messages sent to this role
No option selected

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

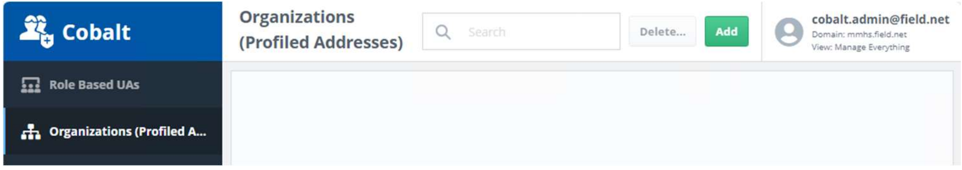


cobalt.admin@field.net
Domain: mmhs.field.net
View: Manage Everything

Name	Mail
FIELD CAPTAIN	captain@mmhs.field.net

Select “Organizations (Profiled Addresses)”

Empty Organizations



Cobalt
Role Based UAs
Organizations (Profiled A...
Organizations (Profiled Addresses)
Search
Delete...
Add

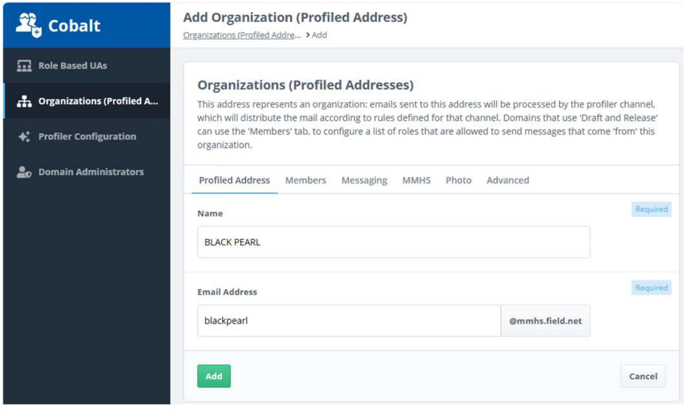
cobalt.admin@field.net
Domain: mmhs.field.net
View: Manage Everything

Click “Add”

In “Name” type “BLACK PEARL”

Ensure “Email address” is “blackpearl”

Populate Organization



Add Organization (Profiled Address)

Organizations (Profiled Addresses)

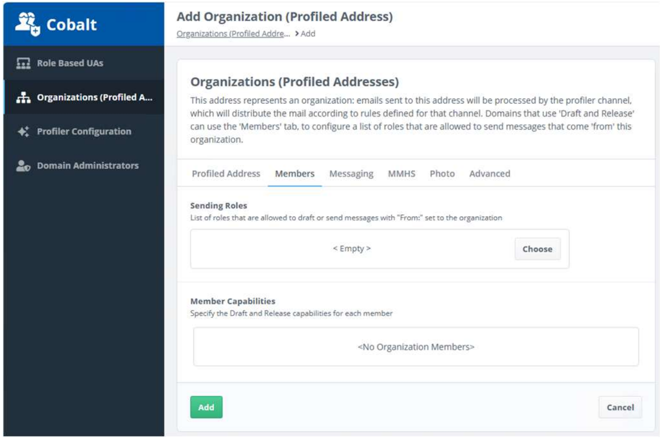
This address represents an organization: emails sent to this address will be processed by the profiler channel, which will distribute the mail according to rules defined for that channel. Domains that use 'Draft and Release' can use the 'Members' tab, to configure a list of roles that are allowed to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

Name: BLACK PEARL

Email Address: blackpearl @mmhs.field.net

Select the “Members” tab

Organization Empty Members



Add Organization (Profiled Address)

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.

Sending Roles

List of roles that are allowed to draft or send messages with "From:" set to the organization

< Empty >

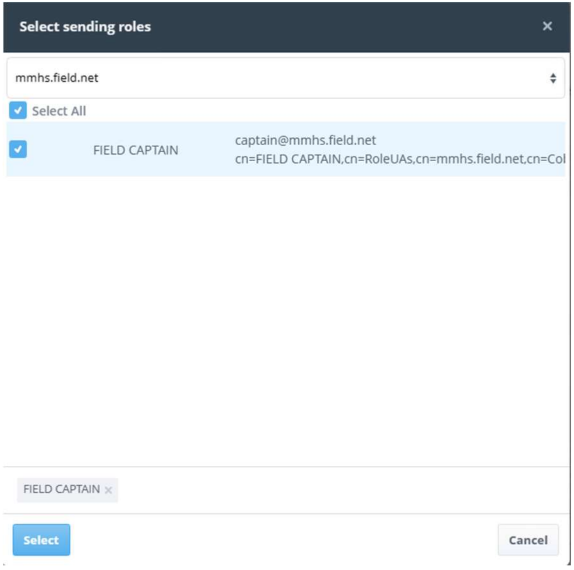
Member Capabilities

Specify the Draft and Release capabilities for each member

<No Organization Members>

Press “Choose”

Select sending roles



mmhs.field.net

☑ Select All

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

FIELD CAPTAIN ×

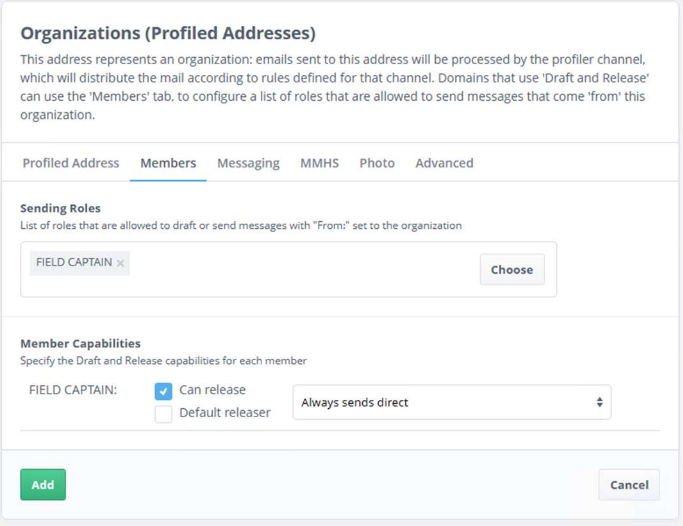
Select “FIELD CAPTAIN”

Press “Select”

Check “Can Release”

Select the dropdown and select “Always sends direct”

Populated Organization members



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.

Sending Roles

List of roles that are allowed to draft or send messages with "From:" set to the organization

FIELD CAPTAIN ×

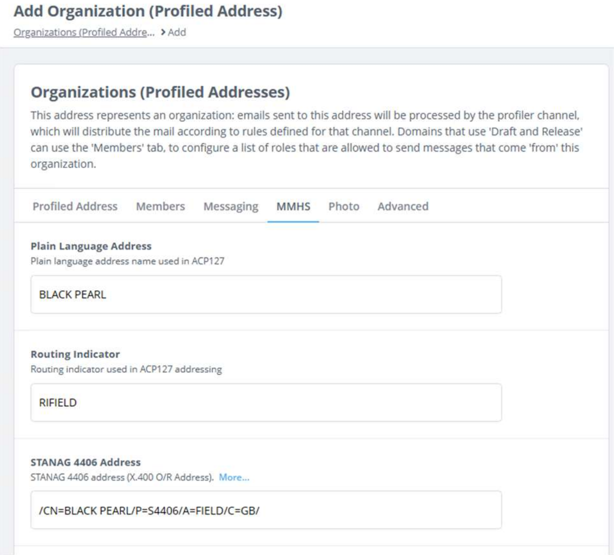
Member Capabilities

Specify the Draft and Release capabilities for each member

FIELD CAPTAIN: ☑ Can release ☐ Default releaser — Always sends direct

Change to “MMHS” tab.

Populate MMHS information



Add Organization (Profiled Address)

Organizations (Profiled Addre... > 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.

Plain Language Address

Plain language address name used in ACP127

BLACK PEARL

Routing Indicator

Routing indicator used in ACP127 addressing

RIFIELD

STANAG 4406 Address

STANAG 4406 address (X.400 O/R Address). More...

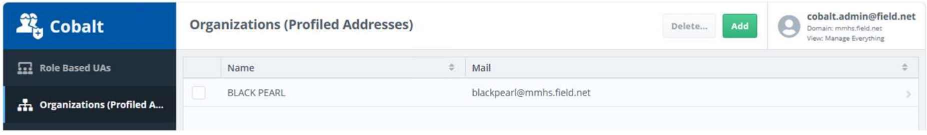
/CN=BLACK PEARL/P=S4406/A=FIELD/C=GB/

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

Press “Add”

Note that the Organization has been added to the directory.

Organization added



Organizations (Profiled Addresses)

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

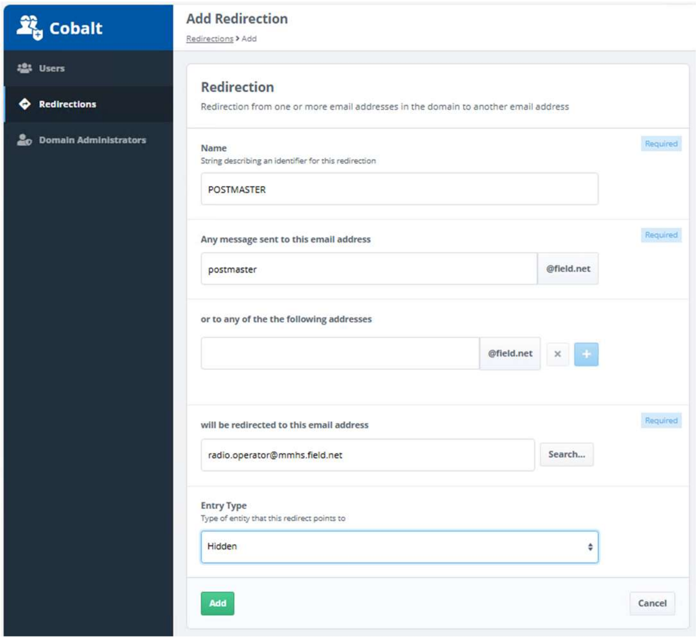
	Name	Mail
☐	BLACK PEARL	blackpearl@mmhs.field.net

Switch Cobalt view to “field.net” domain

Select “Redirections”

Press “Add”

Postmaster redirection



Add Redirection

Redirections > Add

Redirection

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

Name

String describing an identifier for this redirection

POSTMASTER

Any message sent to this email address

postmaster @field.net

or to any of the the following addresses

@field.net

will be redirected to this email address

radio.operator@mmhs.field.net

Entry Type

Type of entity that this redirect points to

Hidden

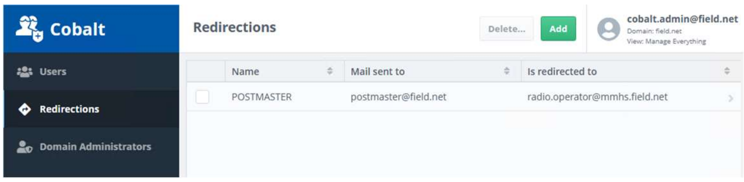
Populate the “POSTMASTER” redirection with “Name”, “address” and “redirected address” “radio.operator@mmhs.field.net”

Select Entry type “Hidden”

Press “Add”

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

Postmaster redirection added



Redirections

cobalt.admin@field.net

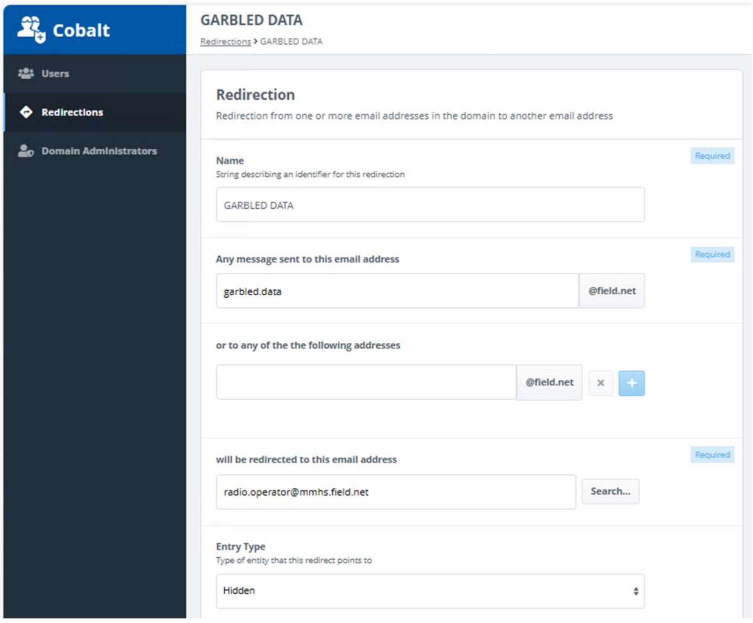
Domain: field.net

View: Manage Everything

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



GARBLED DATA

Redirection

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

Name

String describing an identifier for this redirection

GARBLED DATA

Any message sent to this email address

garbled.data @field.net

or to any of the the following addresses

@field.net

will be redirected to this email address

radio.operator@mmhs.field.net

Entry Type

Type of entity that this redirect points to

Hidden

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.

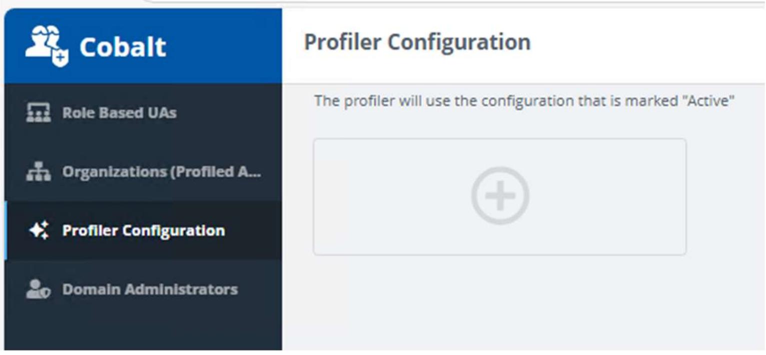
The gateway entity gateway@field.net does not require a mailbox or redirection.

Configure a Profiler Rule

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

Select “Profiler Configuration” from the left pane

Empty Profiler configuration



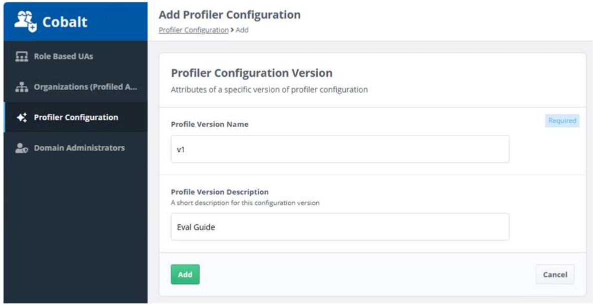
The profiler will use the configuration that is marked "Active"

Click the “+” button

In “Profile Version Name” type “v1”

In Profile Version Description” type “Eval Guide”

Add Profiler Configuration


Cobalt
Add Profiler Configuration
Profiler Configuration > Add
Role Based UAs
Organizations (Profiled A...
Profiler Configuration
Domain Administrators
Required
Add
Cancel

Profiler Configuration Version

Attributes of a specific version of profiler configuration

Profile Version Name: v1

Profile Version Description

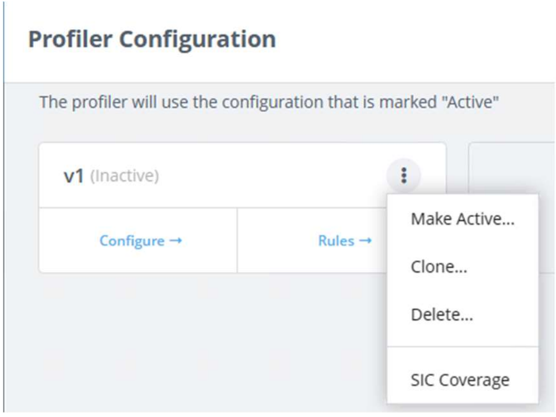
A short description for this configuration version

Eval Guide

Press “Add”

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

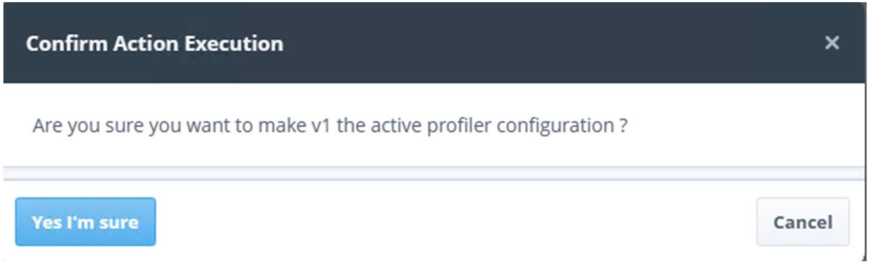
Profiler configuration



The profiler will use the configuration that is marked "Active"

Select the option “Make Active …”

Confirm Profile Activation

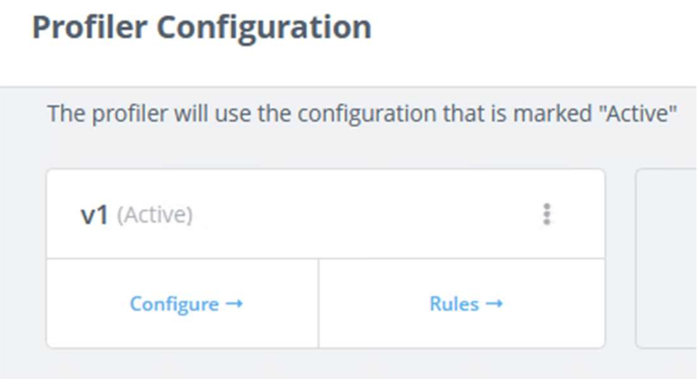


Confirm Action Execution

Are you sure you want to make v1 the active profiler configuration ?

Press “Yes I’m sure”

Profile Activated



Profiler Configuration

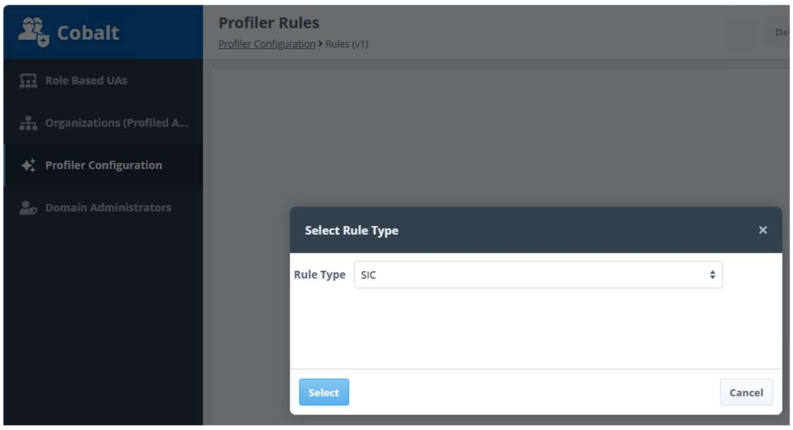
The profiler will use the configuration that is marked "Active"

v1 (Active)

Select “Rules”

Click “Add”

Add New SIC Rule



Select Rule Type

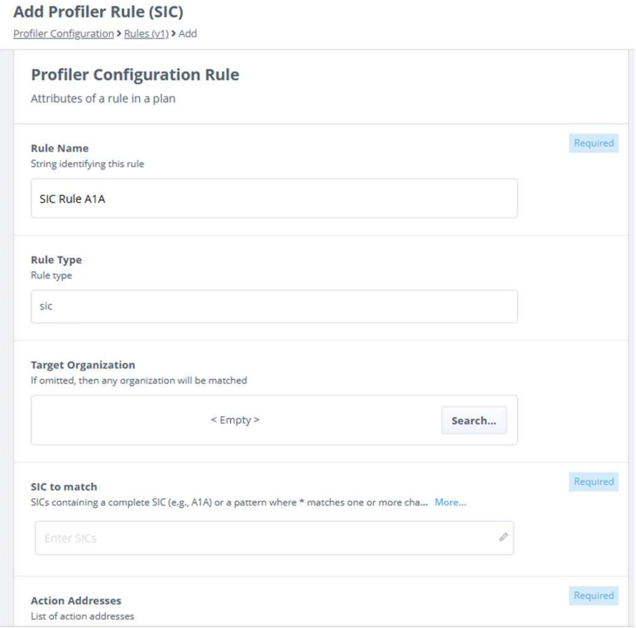
Rule Type: SIC

Set the “Rule Type” to “SIC”

Click “Select”

In “Rule Name” type “SIC Rule A1A”

New Profiler Rule



Add Profiler Rule (SIC)

Profiler Configuration > Rules (v1) > Add

Profiler Configuration Rule

Attributes of a rule in a plan

Rule Name — Required

String identifying this rule

SIC Rule A1A

Rule Type

Rule type

sic

Target Organization

If omitted, then any organization will be matched

< Empty > Search...

SIC to match — Required

SICs containing a complete SIC (e.g., A1A) or a pattern where * matches one or more cha... More...

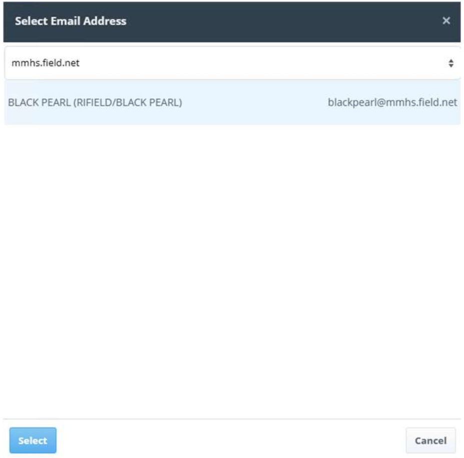
Enter SICs

Action Addresses — Required

List of action addresses

Under “Target Organization” Press “Search”

Select Organization to be Profiled



Select Email Address

mmhs.field.net

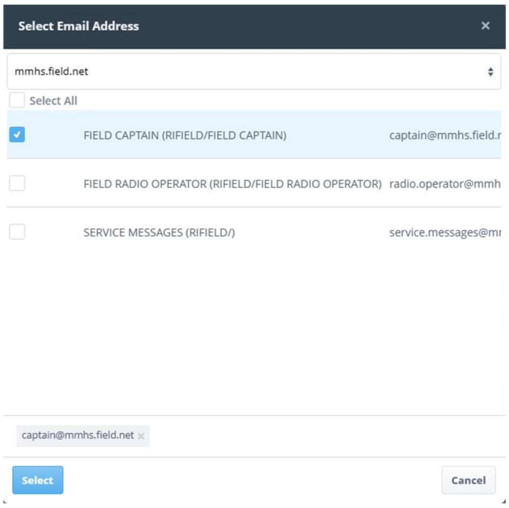
BLACK PEARL (RIFIELD/BLACK PEARL)	blackpearl@mmhs.field.net

Select “BLACK PEARL”

In “SIC to match” type “A1A”

Under “Action Addresses” press “Search”

Select Action Address



Select Email Address ×

mmhs.field.net

□ Select All

☑ FIELD CAPTAIN (RIFIELD/FIELD CAPTAIN) captain@mmhs.field.r

□ FIELD RADIO OPERATOR (RIFIELD/FIELD RADIO OPERATOR) radio.operator@mmh

□ SERVICE MESSAGES (RIFIELD/) service.messages@mı

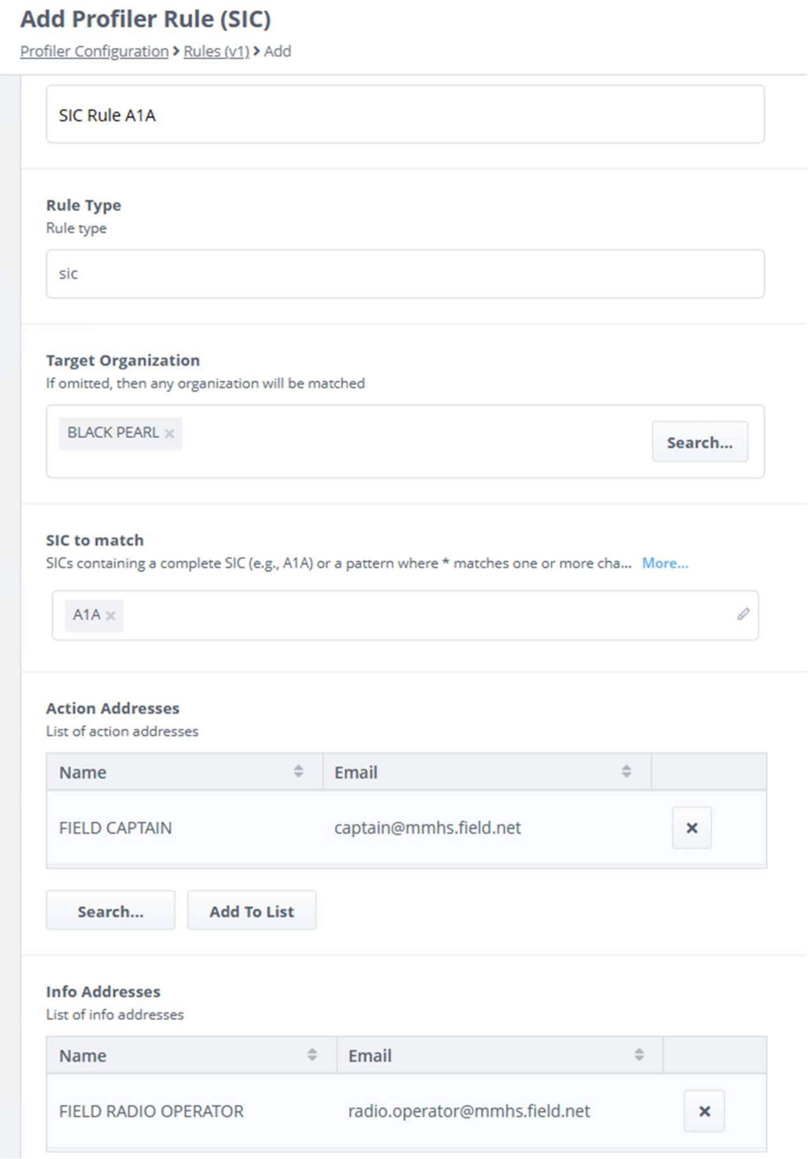
captain@mmhs.field.net ×

Check “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

sic

Target Organization
If omitted, then any organization will be matched

BLACK PEARL ×

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

A1A ×

Action Addresses
List of action addresses

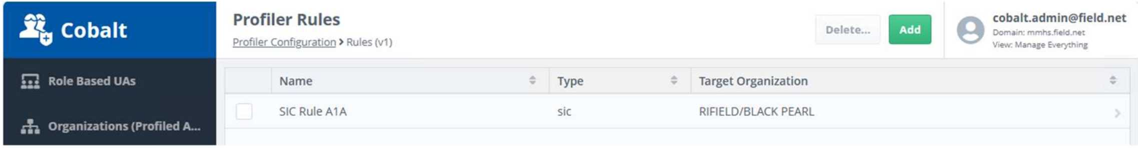
Name	Email	
FIELD CAPTAIN	captain@mmhs.field.net	×

Info Addresses
List of info addresses

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

Click “Add”

Profiler Rule Created



Profiler Rules

Profiler Configuration > Rules (v1)

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

	Name	Type	Target Organization
□	SIC Rule A1A	sic	RIFIELD/BLACK PEARL

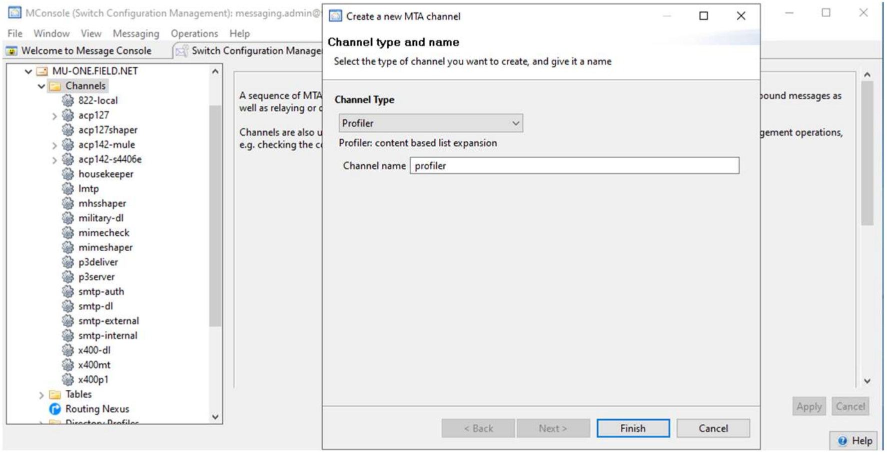
Configure the Profiler Channel

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

Select “New Channel”

Select “Profiler” from the dropdown.

Add Profiler Channel



Create a new MTA channel

Channel type and name

Select the type of channel you want to create, and give it a name

Channel Type: Profiler

Profiler: content based list expansion

Channel name: profiler

Press “Finish”

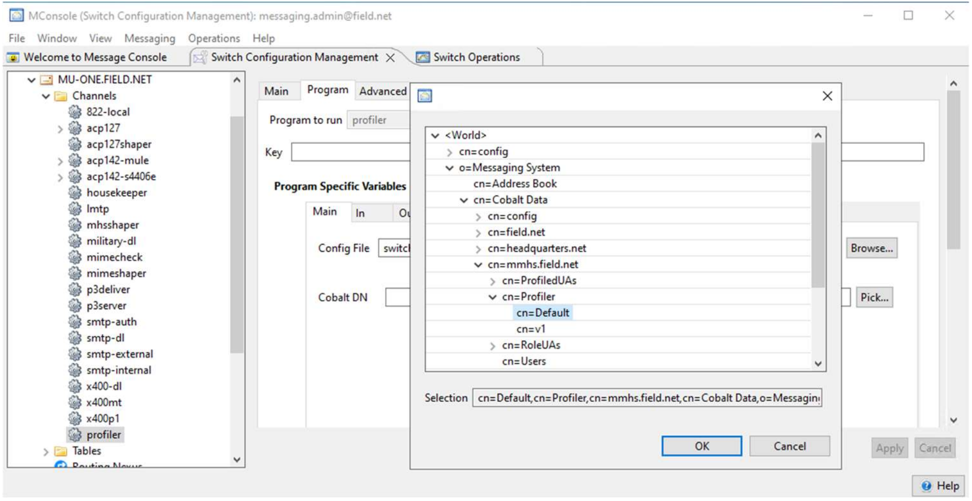
Select the new “profiler” channel.

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



Program to run: profiler

Selection: cn=Default,cn=Profiler,cn=mmhs.field.net,cn=Cobalt Data,o=Messagin

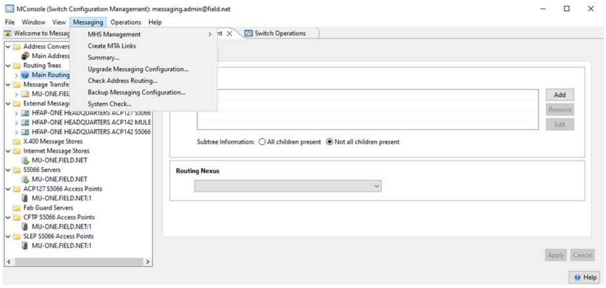
Click “OK”

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

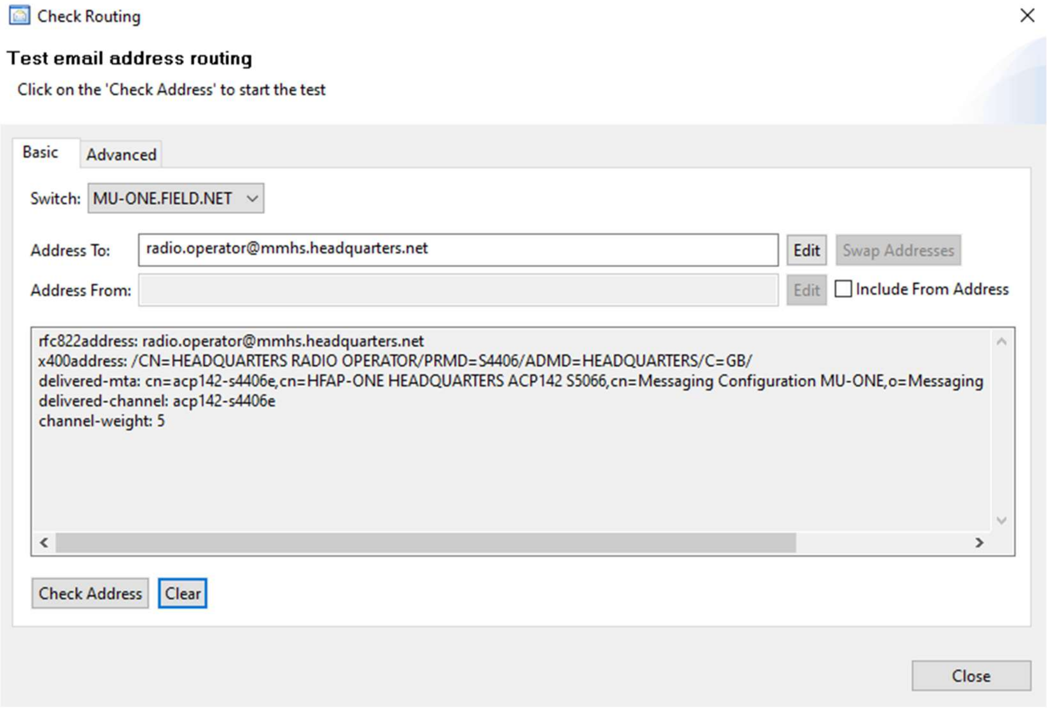


Subtree Information: ○ All children present ● Not all children present

Select “Messaging→Check Address Routing..”

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

Address Routing checked



Check Routing
Test email address routing
Click on the 'Check Address' to start the test
Basic
Advanced
Edit
Swap Addresses
Edit
Check Address
Clear
Close

Switch: MU-ONE.FIELD.NET

Address To: radio.operator@mmhs.headquarters.net

Address From:

□ Include From Address

```
rfc822address: radio.operator@mmhs.headquarters.net
x400address: /CN=HEADQUARTERS RADIO OPERATOR/PRMD=S4406/ADMD=HEADQUARTERS/C=GB/
delivered-mta: cn=acp142-s4406e,cn=HFAP-ONE HEADQUARTERS ACP142 S5066,cn=Messaging Configuration MU-ONE,o=Messaging
delivered-channel: acp142-s4406e
channel-weight: 5
```

Note the address translation and routing information provided.

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