

## M-Switch SMTP Evaluation Guide

---

Configuring R19.0 release of Isode's Internet Messaging Servers on Windows and Linux Platforms for use as either an Enterprise Email System or an ISP Email System.

## Contents

Introduction .....	3
Objectives .....	3
Using Isode Support.....	5
Preparing the Server Environment.....	6
Naming the Server .....	6
Install the Isode Software .....	6
Activating the Isode Products.....	6
Creating the Messaging Configuration .....	7
Running the M-Console Configuration Wizard.....	7
Services Configuration .....	20
M-Switch further Configuration .....	22
Configuring TLS on M-Vault.....	27
Provisioning Users with Cobalt.....	52
Configuring Harrier .....	62
Testing the Solution with Harrier .....	72
Configuring an External SMTP Server.....	76
Adding the External Domain in Cobalt .....	76
Adding and Configuring the External Domain in M-Console.....	82
What Next?.....	90
Whitepapers .....	90
Copyright .....	91

## Introduction

This guide is intended to give the reader basic information on how to configure Isode’s M-Switch, M-Vault, M-Box and Harrier Server Products. These Products combine to create an Internet Email Solution. You will also use Isode Cobalt Product to provision Users.

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

[www.isode.com/product/smtp-message-switch](http://www.isode.com/product/smtp-message-switch)

[www.isode.com/product/pop-imap-message-store/](http://www.isode.com/product/pop-imap-message-store/)

[www.isode.com/product/ldap-x-500-directory/](http://www.isode.com/product/ldap-x-500-directory/)

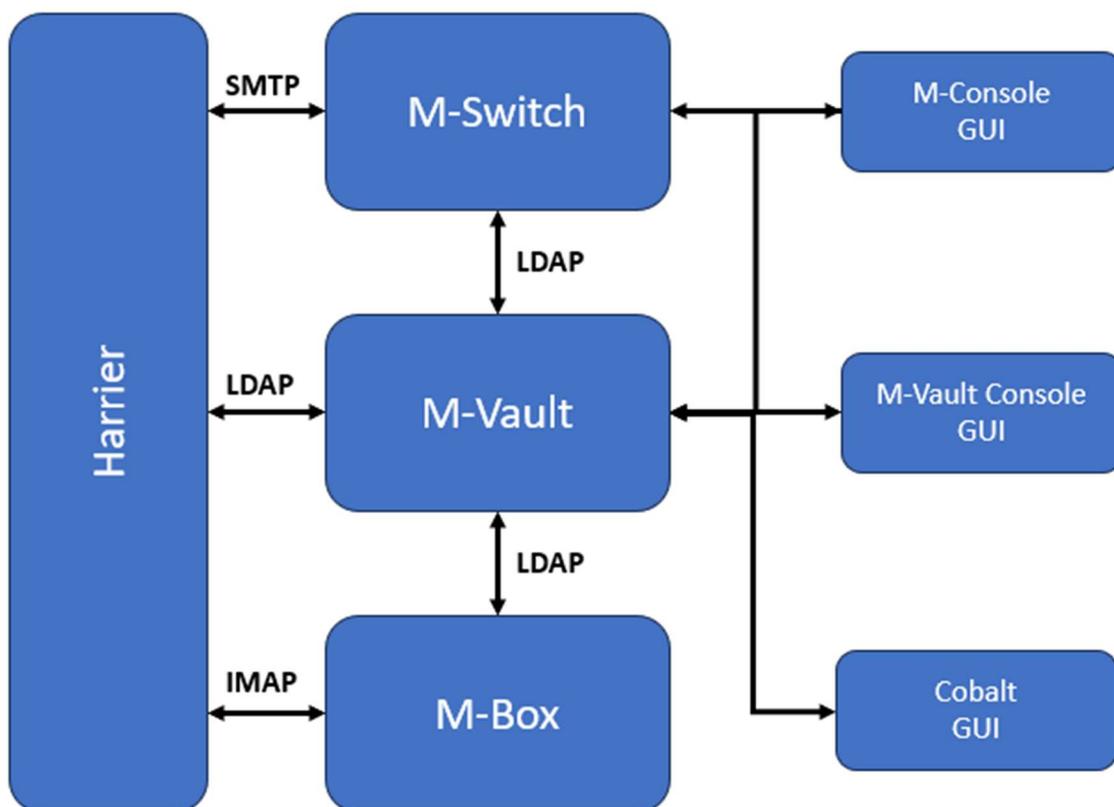
[www.isode.com/product/user-role-provisioning/](http://www.isode.com/product/user-role-provisioning/)

## Objectives

In this guide you will be shown how to configure the Internet Email domain “internet.net” and to configure connections to other Internet Domains.

The diagram below gives an overview of this setup.

*System Overview*



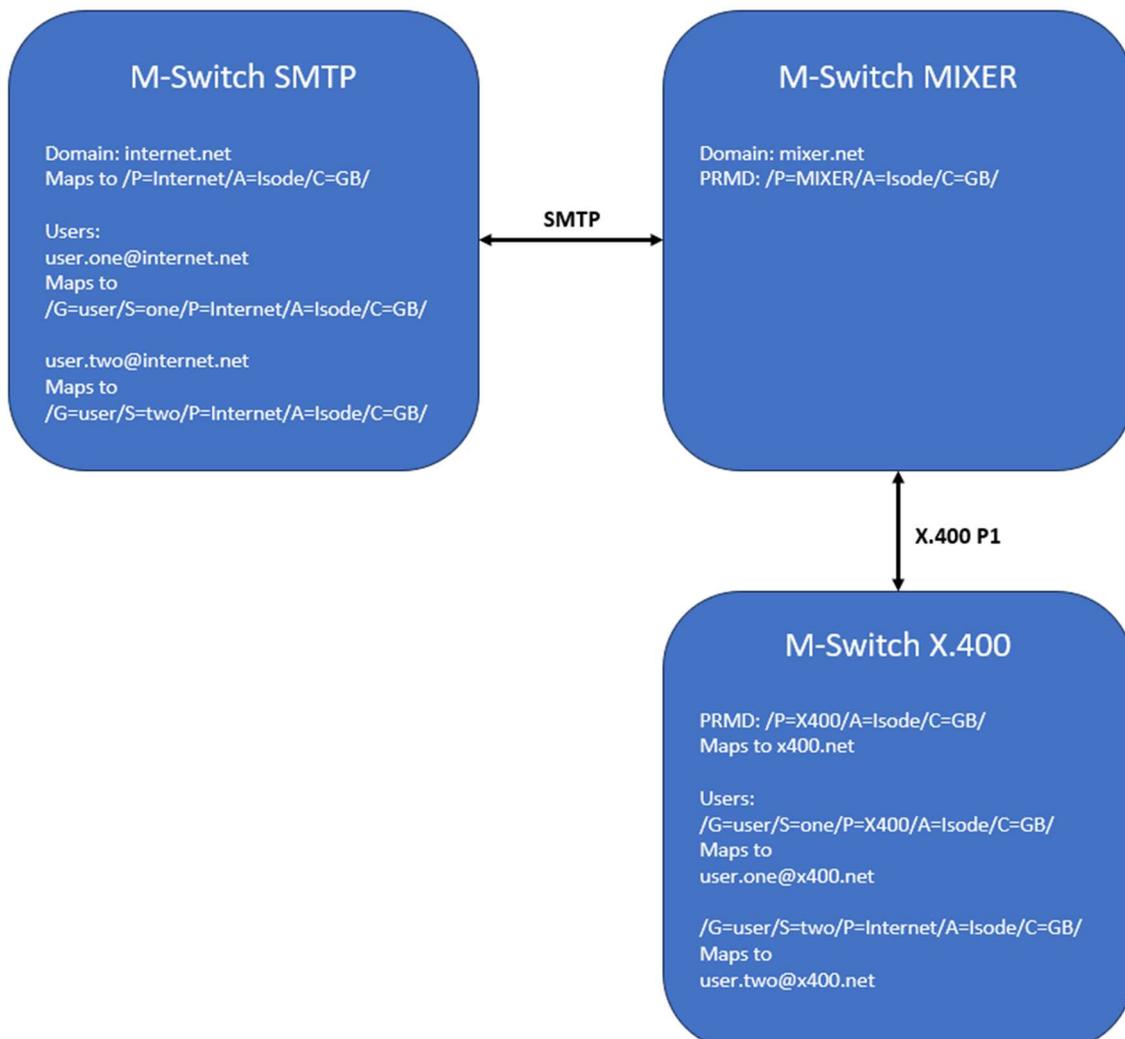
By the end of this guide you will have:

1. Installed the M-Switch, M-Vault, M-Box and Cobalt products.
2. Configured M-Switch and M-Vault using M-Console.
3. Provisioned Users using Cobalt.
4. If using TLS Configured TLS on M-Vault using Sodium CA and M-Vault Console.
5. Configured Harrier using Harrier Server Manager.
6. Logged in using Harrier
7. Created a connection to an external SMTP server (M-Switch MIXER).

For the purposes of this evaluation we have assumed this is a "clean" installation of the Isode Software on to a physical or virtual machine. If you have previously installed the Isode Software on the hardware or VM you are using for this evaluation, please make sure you have completely uninstalled that version and any configurations before proceeding.

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

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



## Using Isode Support

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

## Preparing the Server Environment

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

### Naming the Server

In this eval guide the machine name is: ISODE-SMTP-EVAL

In this eval guide there is no dns suffix for the server.

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

### Install the Isode Software

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

M-Switch 19.ov21

M-Vault 19.ov21

M-Box 19.ov21

Cobalt 1.5v3

Harrier 4.1v1

MAS 1.1

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

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

On Linux, install all the RPMs with the command:

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

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

### Activating the Isode Products

Isode Products are typically Activated using the Isode Messaging Activation Server (MAS). Some Isode Products, such as Cobalt also support local Product Activation. You should refer to the MAS Evaluation Guide for how to Activate the Products.

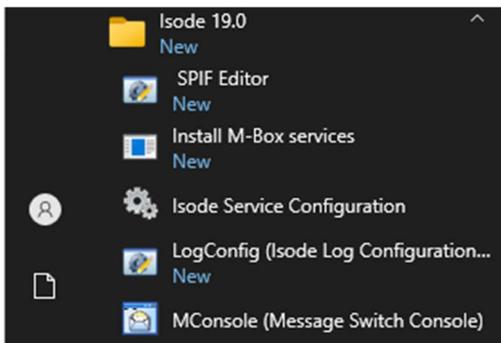
# Creating the Messaging Configuration

## Running the M-Console Configuration Wizard

In this chapter we will create the Messaging Configuration, which is held in M-Vault, and use M-Console to do this.

To start M-Console on Windows from the Windows Start Menu; Windows→Isode 19.0→M-Console

*Start M-Console*

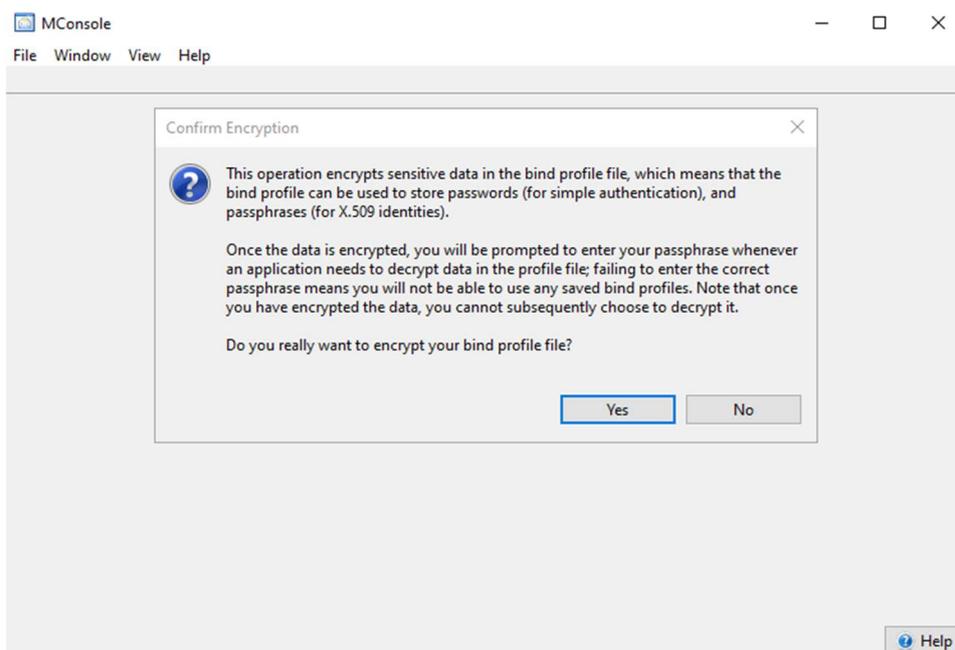


On Linux type the command:

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

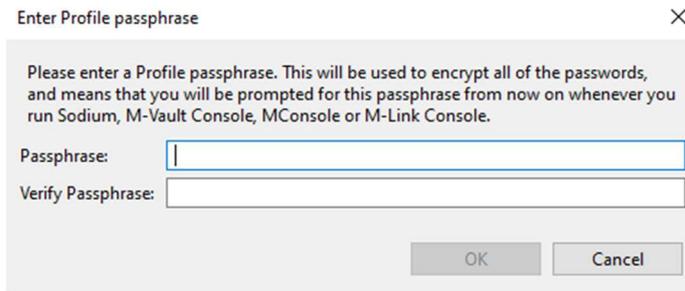
You will see the following prompt.

*Encrypt the Bind Profile*



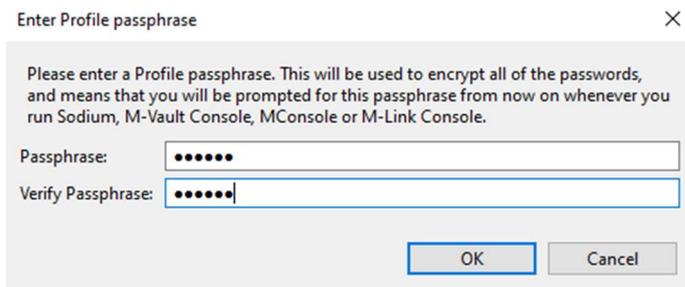
Click "Yes"

## Enter Bind Profile Passphrase



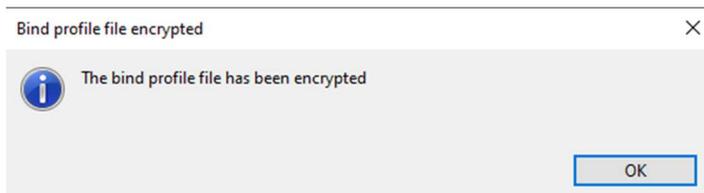
Enter your chosen passphrase, for evaluations we suggest “secret” so that if you need Isode Support we do not have to fix forgotten passwords etc.

## Bind Profile Passphrase Entered



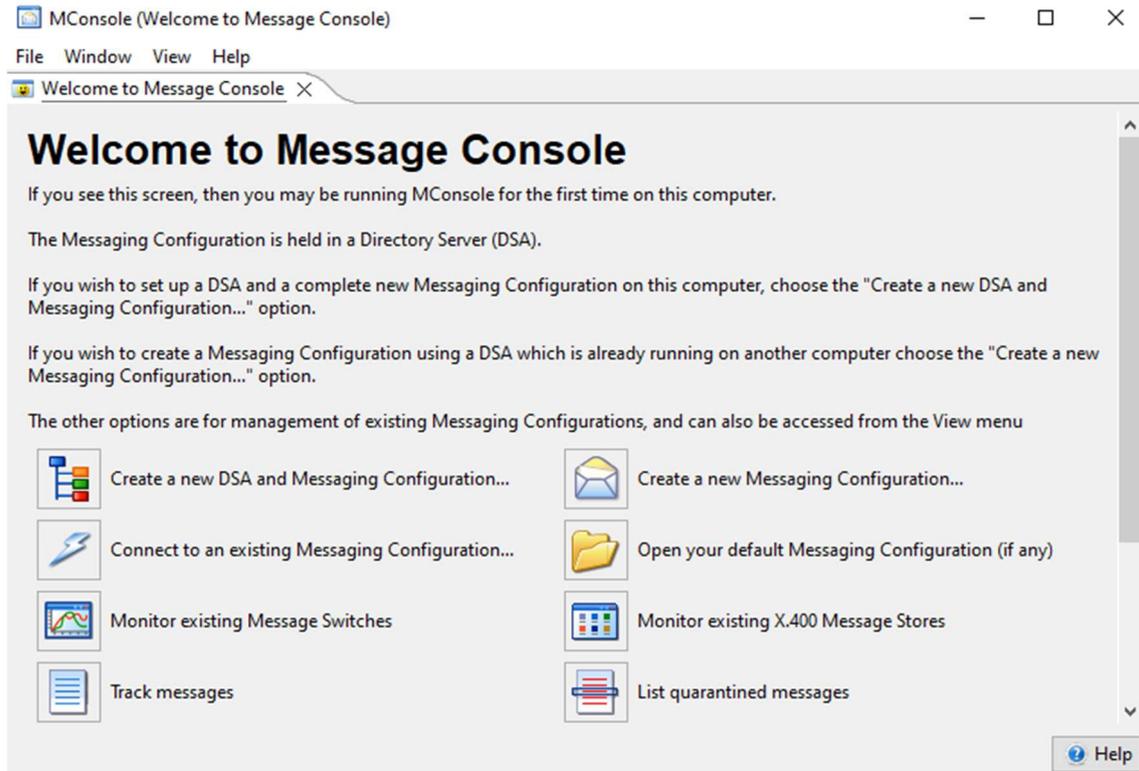
Click “OK”

## Bind Profile Encrypted



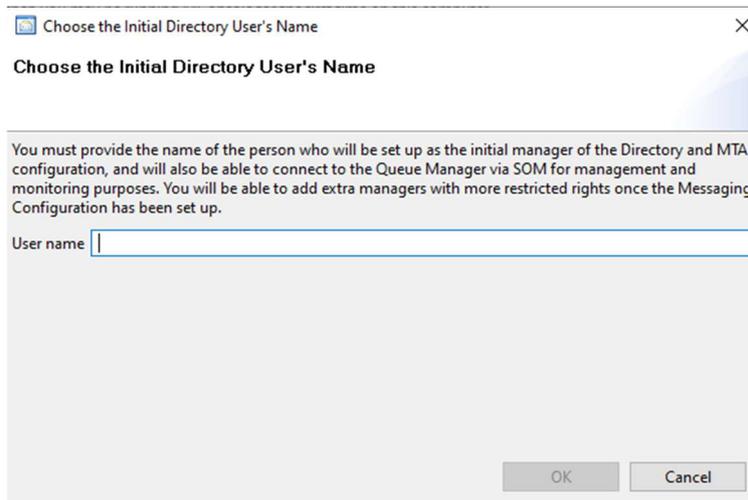
Click “OK”

## M-Console Welcome Screen



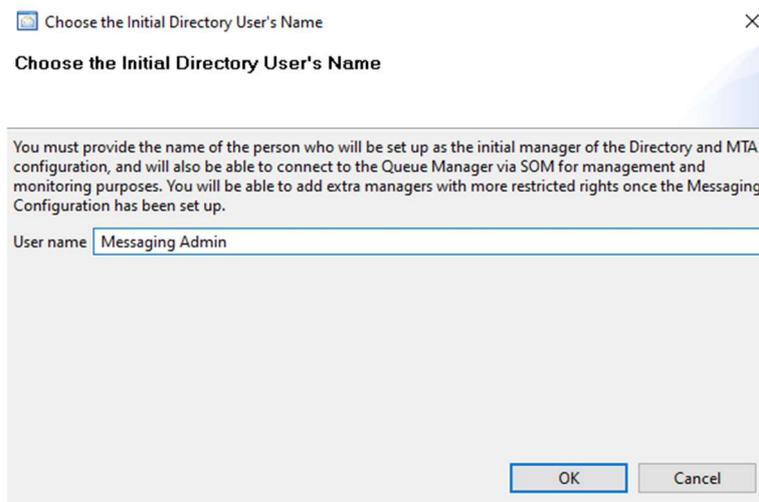
Select "Create a new DSA and Messaging Configuration."

## Enter a User Name



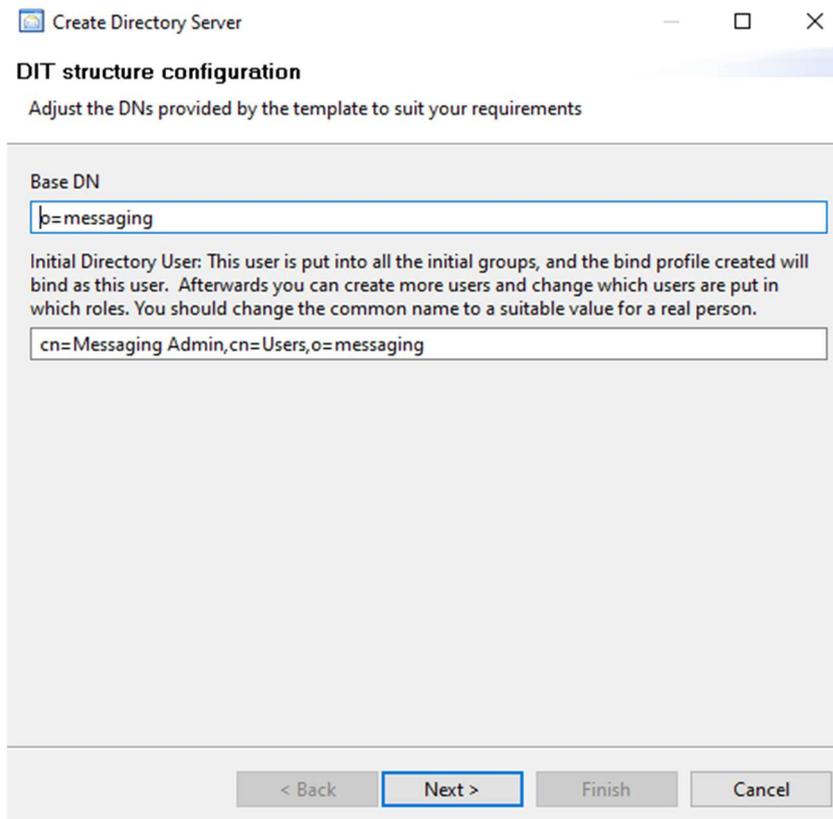
Typically, we use "Messaging Admin" here, but you can choose your own if you wish.

## User Name Entered



Enter your User Name and Click “OK”.

## Enter Base DN



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

## Base DN entered

Create Directory Server

### DIT structure configuration

Adjust the DNs provided by the template to suit your requirements

Base DN

o=Internet

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=Internet

< Back   **Next >**   Finish   Cancel

In this guide we have changed the Base DN to “Internet”. Click Next>”

## Enter Password

Create Directory Server

### Password configuration

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

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

Password: ●●●●●●  Show

Copy password to clipboard   Save password to file

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

< Back   **Next >**   Finish   Cancel

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

## Password entered

**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=Internet

Password:   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

Always check the password you have entered by checking the “Show” checkbox, then click “Next>”.

## Bind Profile Summary

**Create Directory Server**

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

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

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

Click “Next>”.

## DSA Address Configuration

Create Directory Server

### Address Configuration

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

Hostname:

Enable:

LDAP  DAP

Port numbers:

Standards, no messaging: 389 / 102

Standards with messaging: 389 / 19999

Isode default: 19389 / 19999

Alternate 2: 29389 / 29999

Alternate 3: 39389 / 39999

Alternate 4: 49389 / 49999

Alternate 5: 59389 / 59999

Click “Next>”.

## DSA Configuration Details

Create Directory Server

### Confirm Details

Check the details below before creating the DSA

**DSA creation template:**  
Simple DSA setup for Messaging Evaluations

**DSA address:**  
Host ISODE-SMTP-EVAL, X.500 on port 19999, LDAP on port 19389

**DSA name:**  
cn=dsa,o=Internet

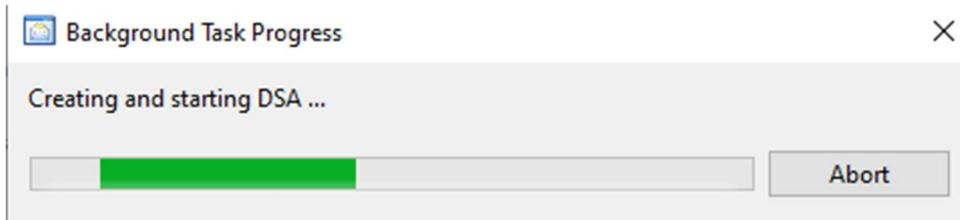
**Bind profile name:**  
cn=dsa,o=Internet / Messaging Admin

**Password hashing:**  
SCRAM-SHA-1

Click “Finish”.

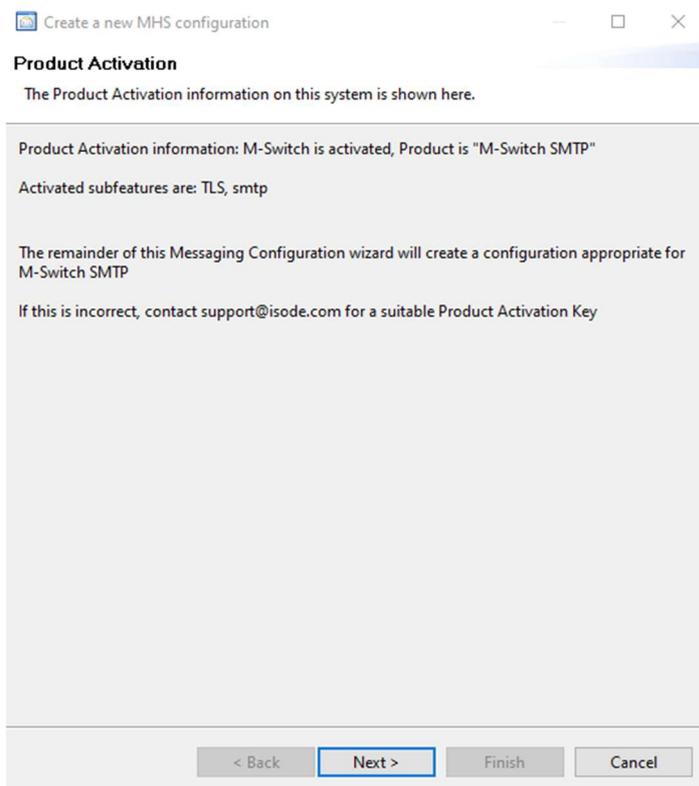
The following screen is shown.

*DSA being created*



Wait until this finishes.

*Product Activation Summary*



The summary of what features are Activated in the product is shown.

Click “Next>”.

You will now through steps to create the messaging configuration.

## Set the Messaging Configuration Base DN

Create a new MHS configuration

### Set the Messaging Configuration Base DN

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

- > o=Internet

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

Create organization name

Messaging configuration name  
Messaging Configuration

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

< Back   Next >   Finish   Cancel

In simple configuration just select the “O=Your Base DN”

## Set the Messaging Configuration Base DN

Create a new MHS configuration

### Set the Messaging Configuration Base DN

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

- > o=Internet

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

Create organization name

Messaging configuration name  
Messaging Configuration

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

< Back   Next >   Finish   Cancel

Click “Next>”.

## Set the Hostname

Create a new MHS configuration

### Hostname

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

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

ISODE-SMTP-EVAL

DSA Authentication

SASL Password [REDACTED] Show

< Back Next > Finish Cancel

The Wizard should automatically pickup your server hostname. If it does not then enter it. You do not need to change the SASL Password here or note it down.

Click “Next>”.

## SMTP Configuration

Create a new MHS configuration

### SMTP channel specific settings and routing policy

Enter the internet domain regarded as local to this MTA.

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

Email address domain isode.com

Create an Internet Message Store for local POP3 or IMAP users

Use DNS

Use MX records

Don't use DNS

< Back Next > Finish Cancel

Unless you have already set up DNS and MX Records for your domain it is best to check do not use DNS.

## SMTP Configuration

Enter your domain (we will use internet.net”) and Click “Next>”.

## Administrator details

The Wizard should auto-populate the details above.

Click “Next>”.

## Anti Virus configuration

Create a new MHS configuration

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

Anti Virus Engine  None  Clam AV

Install msgcheck.zip

< Back   Next >   **Finish**   Cancel

In evaluations we do not configure Anti Virus as this is more for production systems.

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

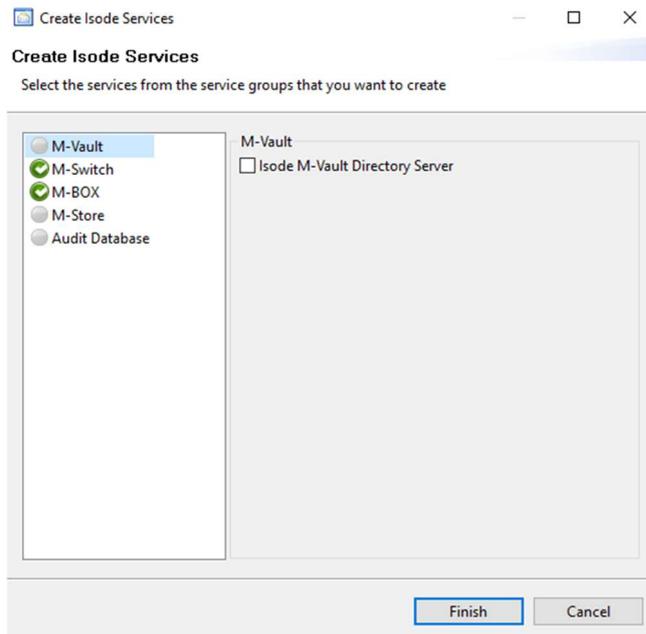
M-Box uses the ms.conf to store its configuration

Create ms.conf  C:\isode\etc\ms.conf

< Back   Next >   **Finish**   Cancel

Click “Next>”.

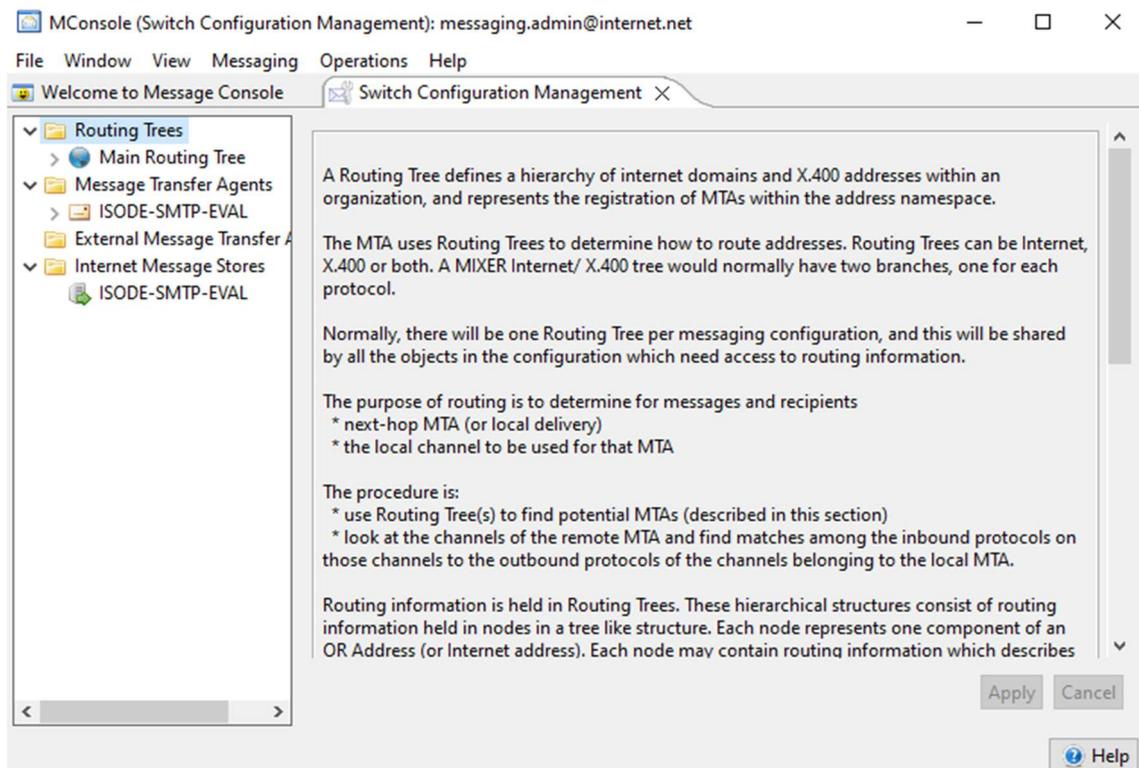
## Create Isode Services



You can now choose to create any additional Isode Services apart from the default. In more advanced configurations you may want to configure the Audit Database so that you can track messages. Isode Support can assist with this and you can manually create those services later.

Click “Finish”.

## Create Isode Services



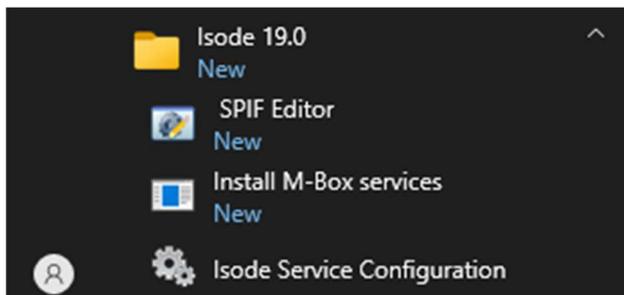
You have now completed the core configuration of your server.

## Services Configuration

On Windows you need to configure the services to auto-start.

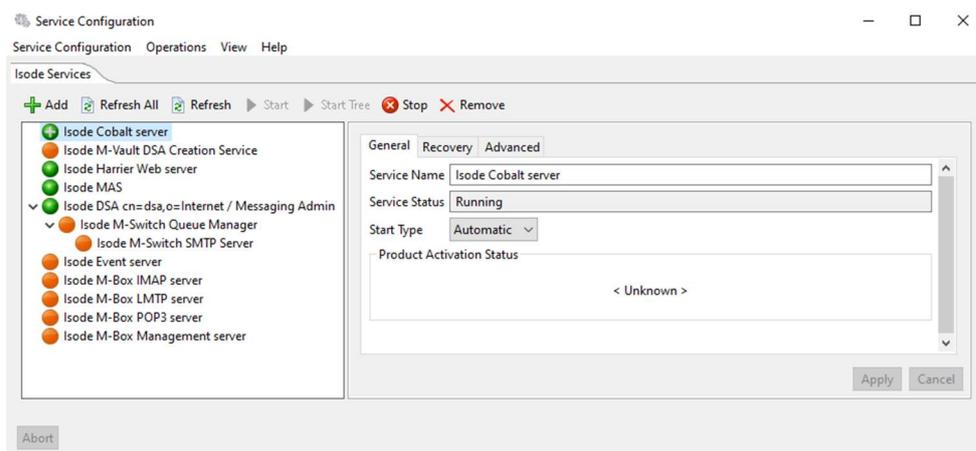
From the Start Menu Windows → Isode R19.0 → Isode Service Configuration

Create Isode Services



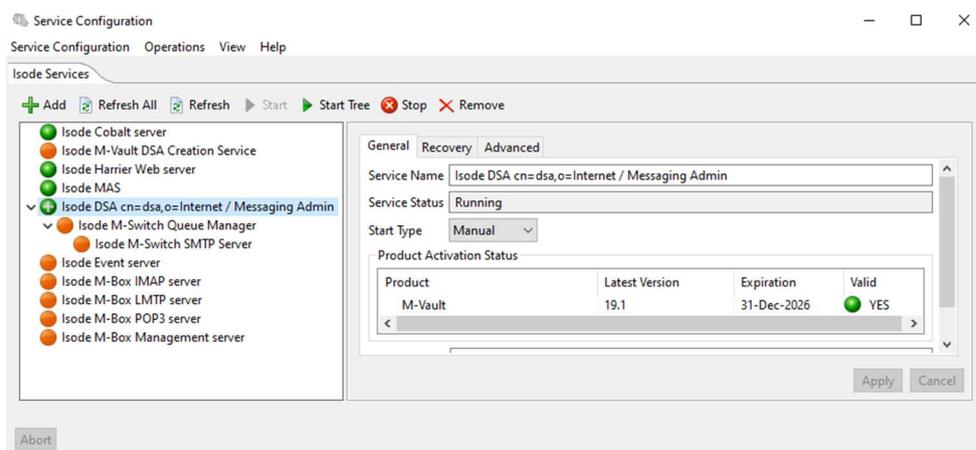
The following screen will be displayed.

Isode Service Configuration



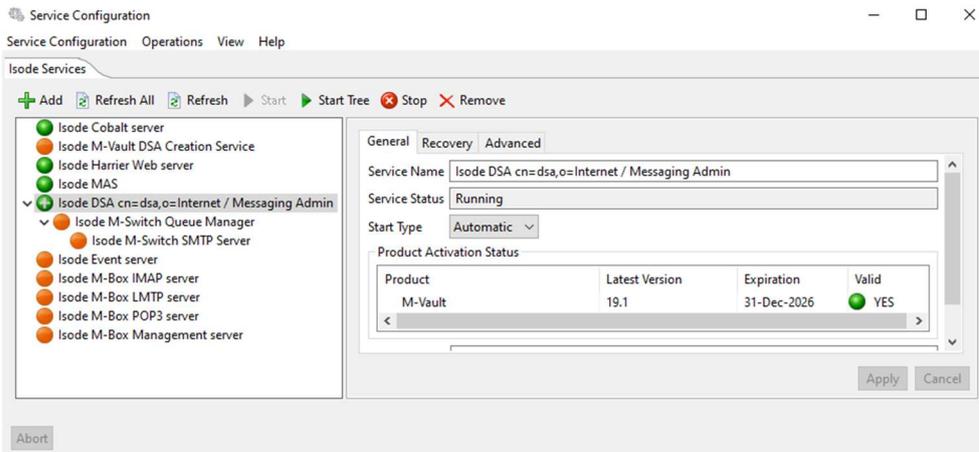
Select the Isode DSA ....service.

Isode Service Configuration



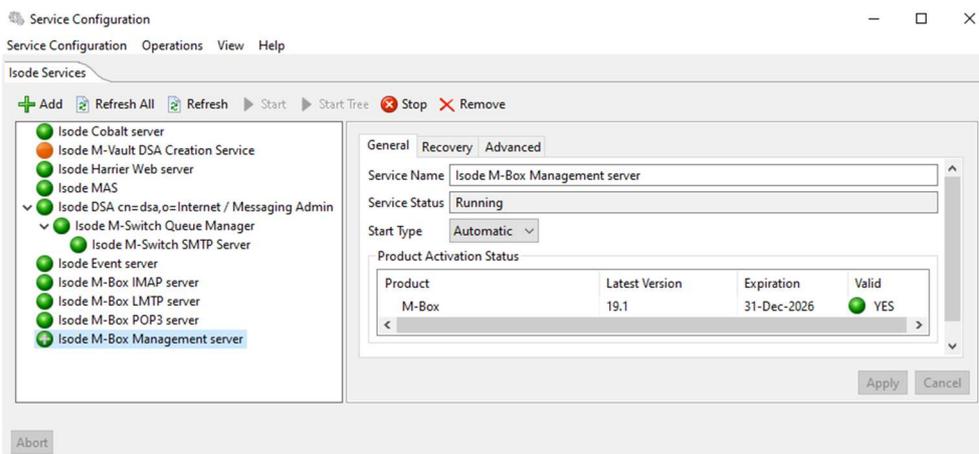
Change the start type from Manual to Automatic and Click “Apply”

## Isode Service Configuration



Repeat this for the remaining services except Isode M-Vault DSA Creation Service. Then select each service and start it. You should have the screen below.

## Isode Service Configuration

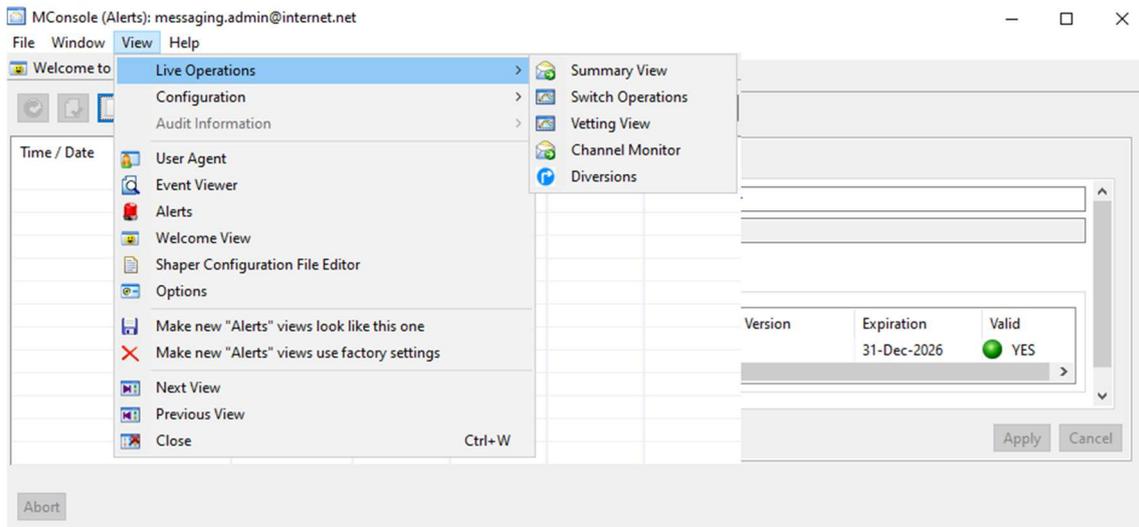


This completes the Service Configuration.

## M-Switch further Configuration

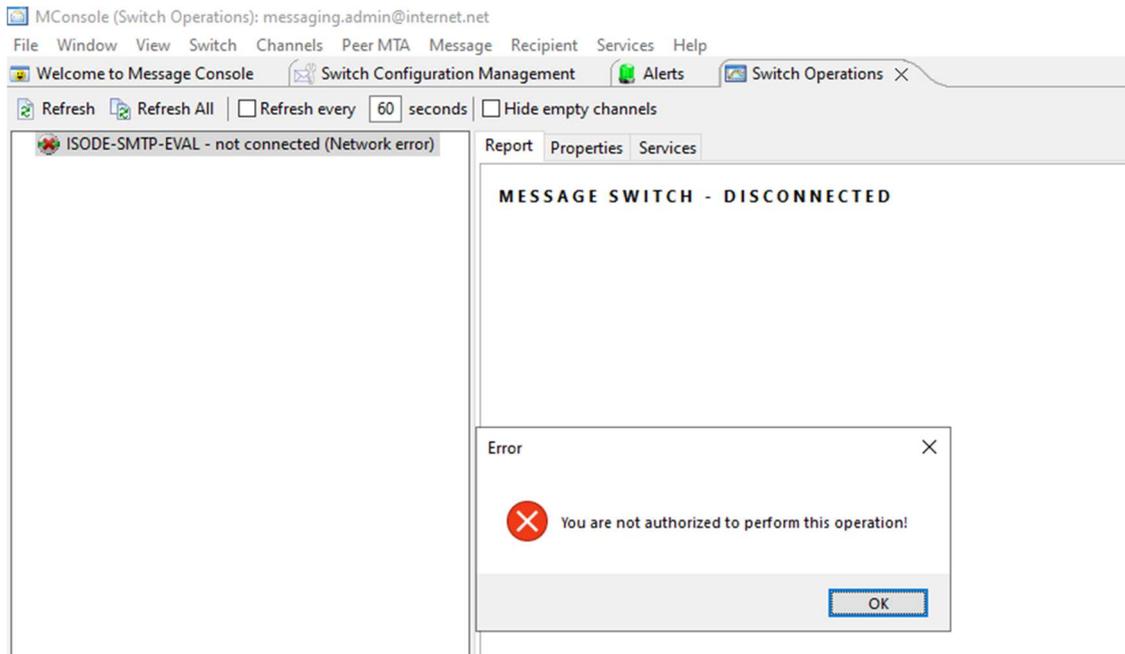
Now that the services are running you can make changes to the M-Switch Configuration and they will take effect immediately. Return to M-Console. select View→Live Operations→Switch Operations.

### M-Console Switch Operations View Setup



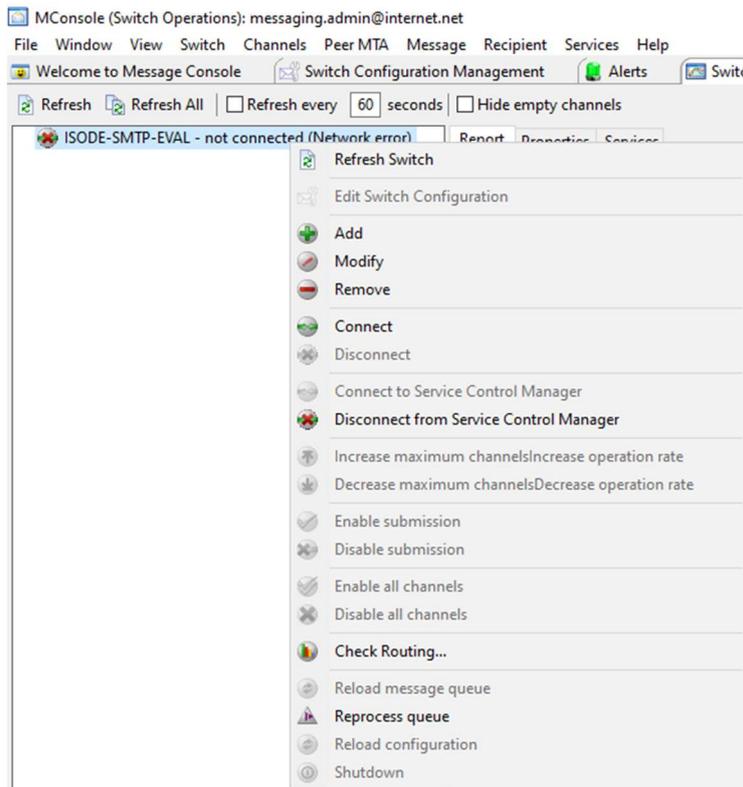
Select View→Live Operations→Switch Operations.

### M-Console Switch Operations View Setup



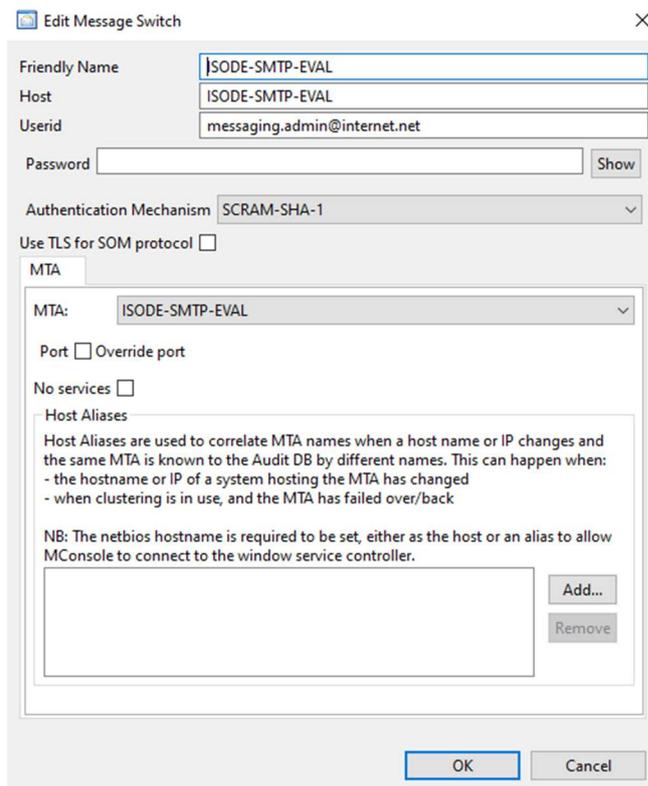
The Error is expected, click “OK”.

## M-Console Switch Operations View Setup



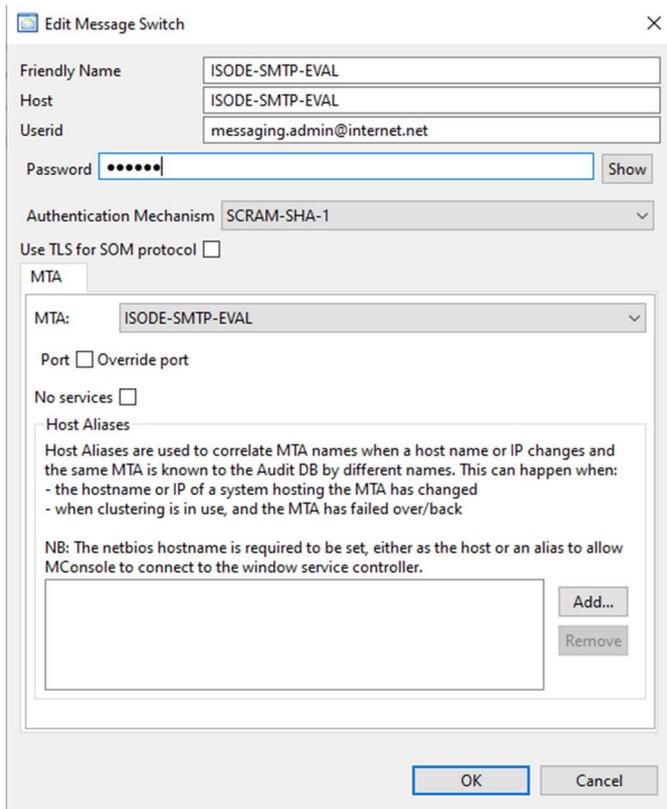
Right Click on the Switch and Select “Modify”.

## M-Console Switch Operations View Setup



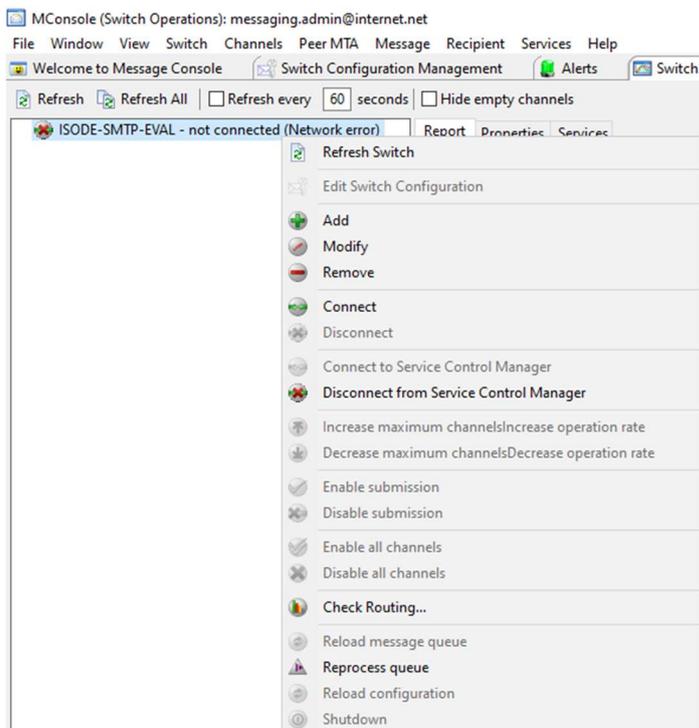
Enter the Password you set for the Messaging Admin User.

## M-Console Switch Operations View Setup



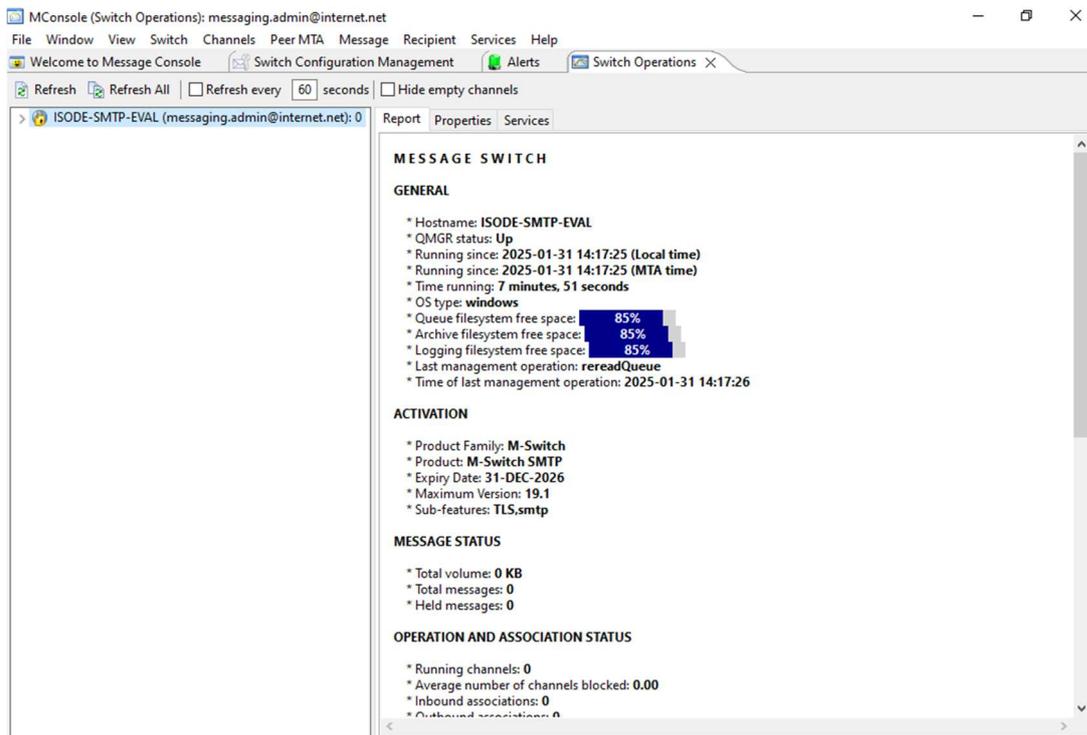
Click "OK".

## M-Console Switch Operations View Setup



Right Click on the Switch and Select "Connect".

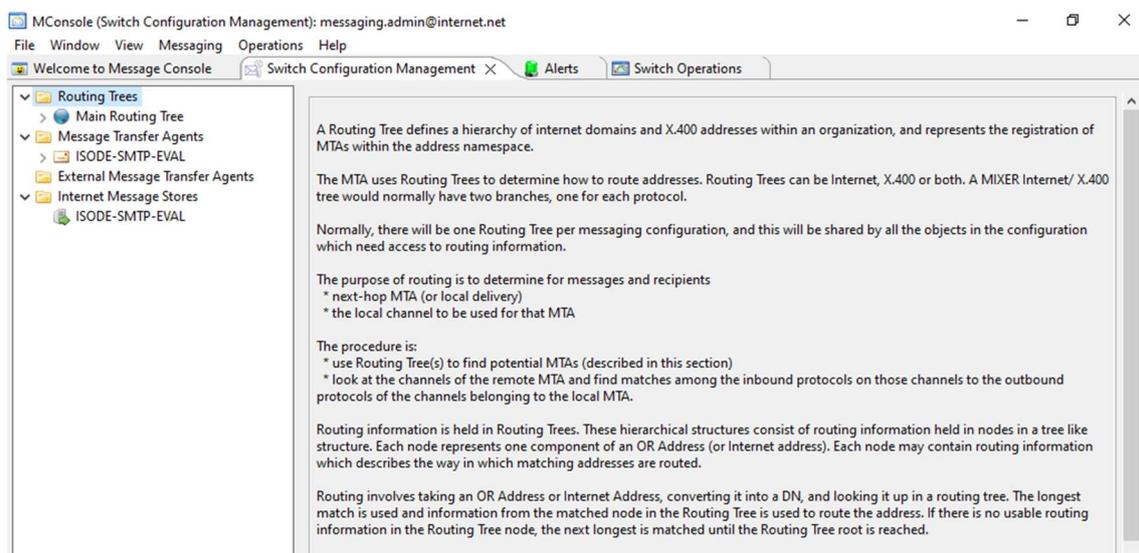
### M-Console Switch Operations View Setup



The above screen is displayed. We can now make changes to the M-Switch Configuration that will take effect immediately.

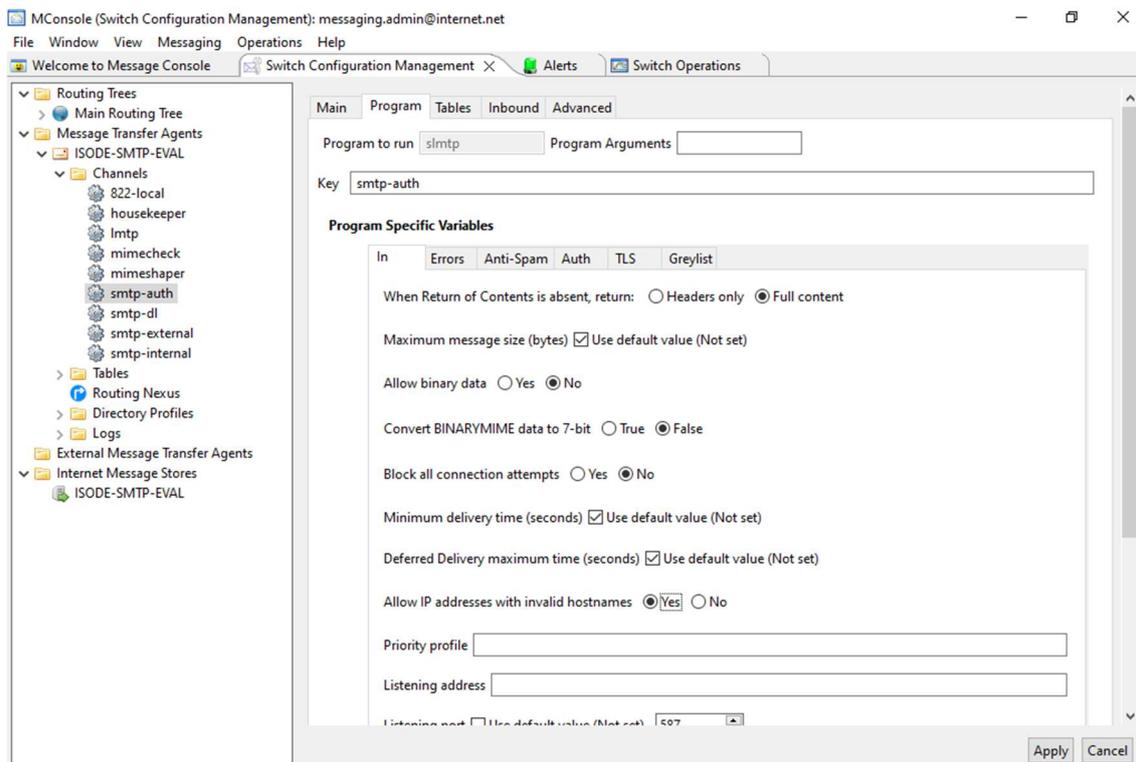
Go to the Switch Configuration Management Tab.

### M-Console Switch Configuration Management



Expand your “Message Transfer Agent” (ISODE-SMTP-EVAL) in this example and then expand the “Channels”.

### M-Console Switch Configuration Management



Select the “smtp-auth” Channel and the “Program” tab of that Channel, change the “Allow IP addresses with invalid hostname” from “No” to “Yes”. Click “Apply”.

This completes the configuration of M-Switch for “Local Users” not connecting to external SMTP Servers. We will return to M-Console later to configure the SMTP connection to the domain “x400.net”.

If you have a “TLS” enabled Activation you will need to do some configuration of M-Vault so that the Cobalt User Provisioning tool works correctly. This configuration involves creating Certificates for which you would normally require a Certification Authority (CA). Isode provides a CA in the form of Sodium CA, this is not a production CA but one suitable for use in an evaluation.

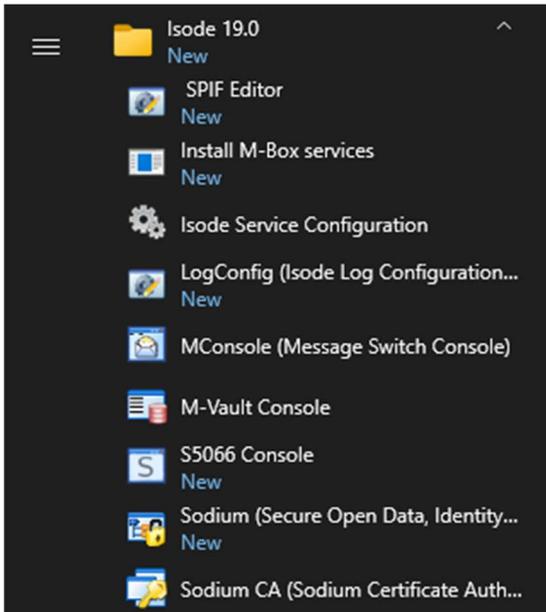
If you do not have a TLS Activation you can skip the next section and go directly to the Provisioning Users with Cobalt section.

## Configuring TLS on M-Vault

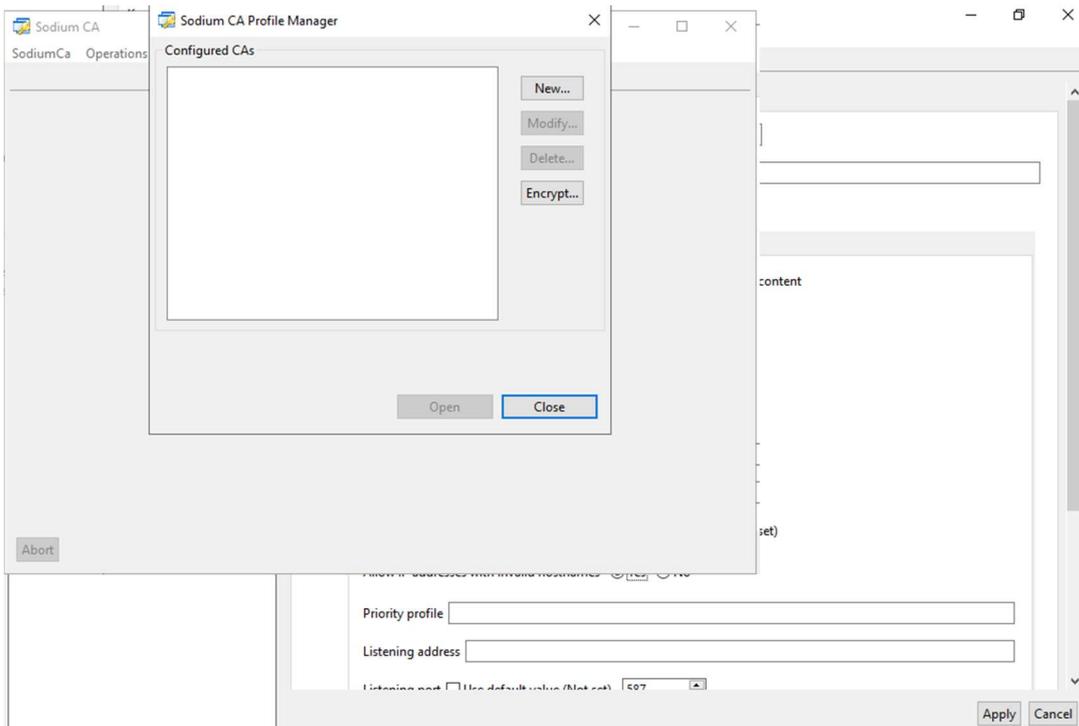
Here you will setup Sodium CA to issue Certificates from a Certificate Signing Request (CSR) and use M-Vault Console to generate this CSR and install the provided Certificate. You might want to create a dedicated folder for Certificates before you start.

From the Windows Start Menu → Isode R19.0 → Sodium CA (Sodium Certificate Authority).

Start Sodium CA



Sodium CA initial configuration



Click “New”.

## Sodium CA initial configuration

**New 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 [Change... Create]

Passphrase (Optional): [ ] Show

Set the CA to work with the Directory

< Back Next > Finish Cancel

Click “Create”, for the purposes of an Evaluation you do not need to use a Passphrase.

## Sodium CA initial configuration

**New 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 [Change... Create]

Passphrase (Optional): [ ] Show

Set the CA to work with the Directory

< Back Next > Finish Cancel

Click “Next>”.

## Sodium CA initial configuration

**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:  Hostname:  Port:

Bind DN:

Bind Password:

< Back   Next >   Finish   Cancel

Select "Pick..."

## Sodium CA initial configuration

**Pick an entry to use for the bind DN**

- <World>
  - o=Internet
    - cn=Address Book
    - > cn=Groups
    - > cn=Messaging Configuration
    - cn=Users
      - cn=Messaging Admin**
      - cn=White Pages

Selection:

Navigate to the "Messaging Admin" User. Click "OK".

## Sodium CA initial configuration

**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:  Hostname:  Port:

Bind DN:

Bind Password:

< Back **Next >** Finish Cancel

Enter the Password for the Messaging Admin User. Click “Next>”.

## Sodium CA initial configuration

**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:

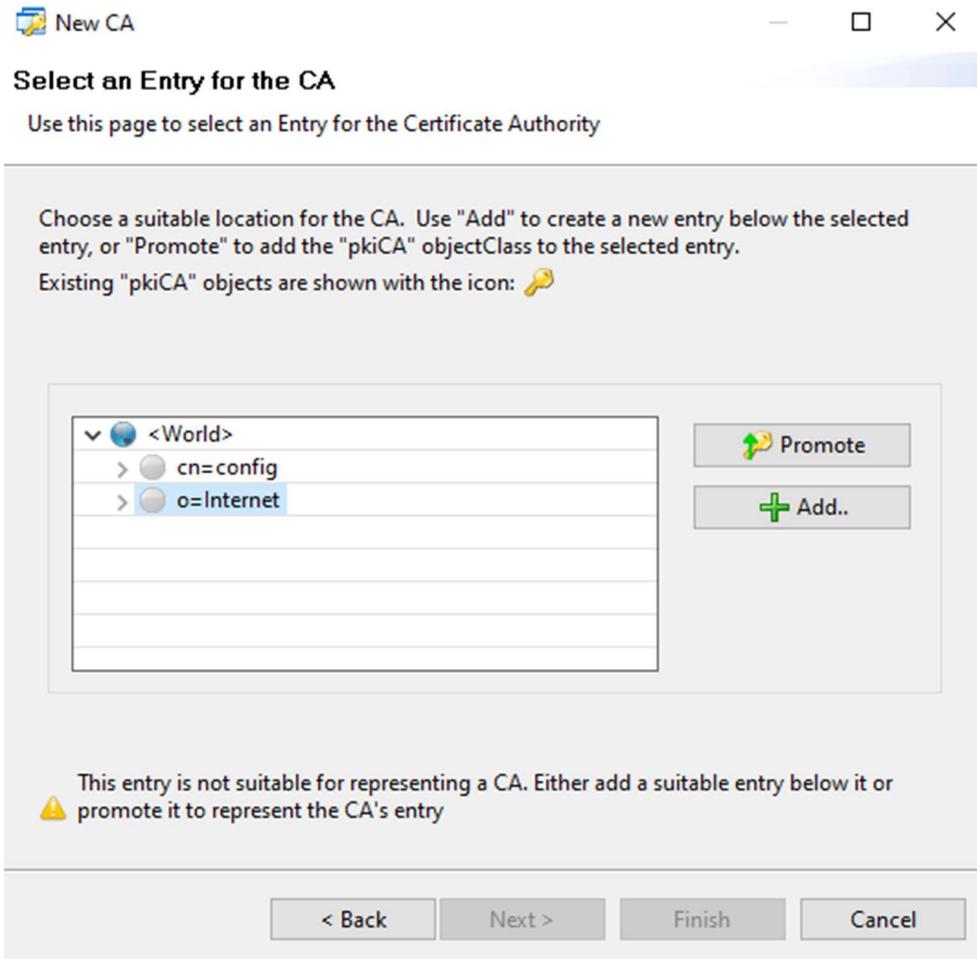
>

This entry is not suitable for representing a CA. Either add a suitable entry below it or promote it to represent the CA's entry

< Back **Next >** Finish Cancel

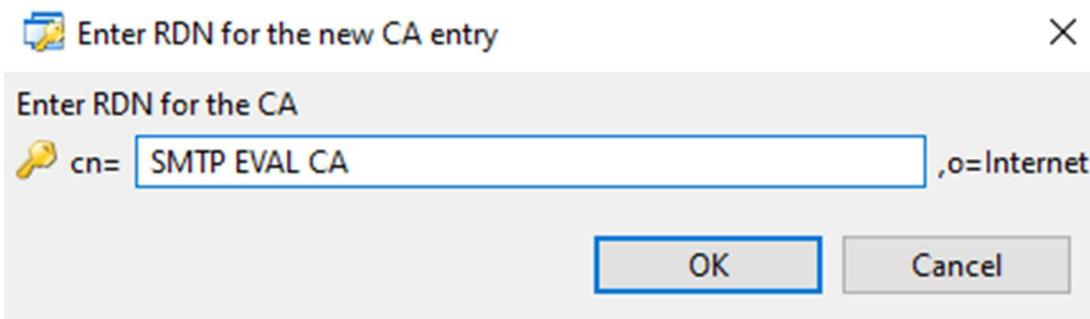
Expand the “<World>”.

Sodium CA initial configuration



Select "O=Internet", Click "+ Add..."

Sodium CA initial configuration



Enter a "cn" of your choice for the CA. Click "OK".

## Sodium CA initial configuration

**New CA** [Close] [Maximize] [Minimize]

### 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:

- o=Internet
  - cn=Address Book
  - > cn=Groups
  - > cn=Messaging Configuration
  - cn=SMTP EVAL CA
  - > cn=Users
  - cn=White Pages

Added entry "cn=SMTP EVAL CA,o=Internet"

Select cn=SMTP EVAL CA,o=Internet to represent the CA's entry

Click "Next>".

## Sodium CA initial configuration

**New CA** [Close] [Maximize] [Minimize]

### Set Key type, Subject and Subject Alternative Names

Use this page to set Key type, Subject and Subject Alternative Names for the CA

Subject DN

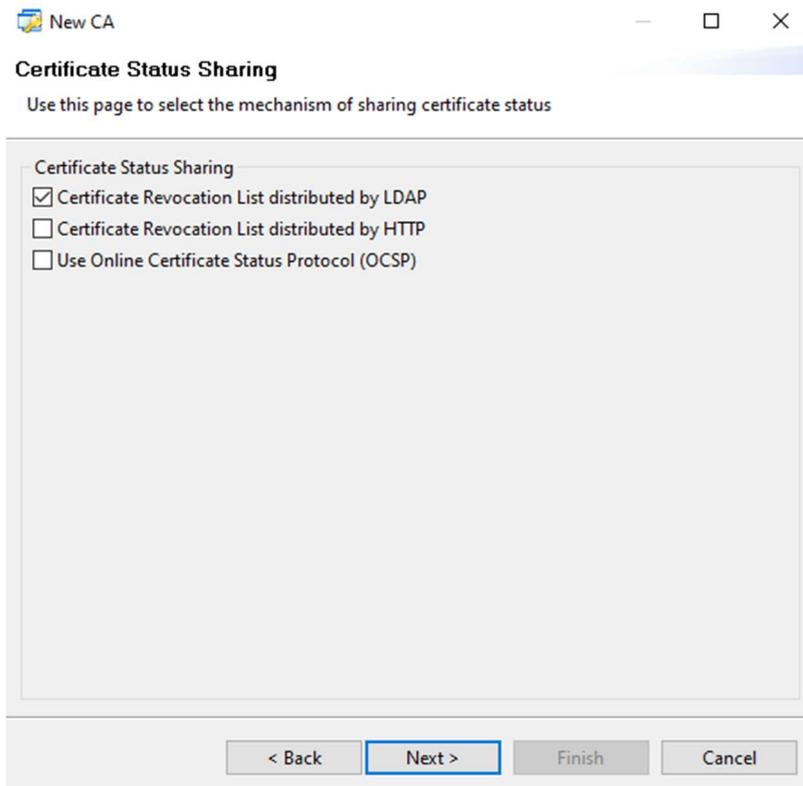
Algorithm for the Key  
 RSA  DSA  ECDSA

Key Size  
 Key Size

Add Subject Alternative Names for the CA

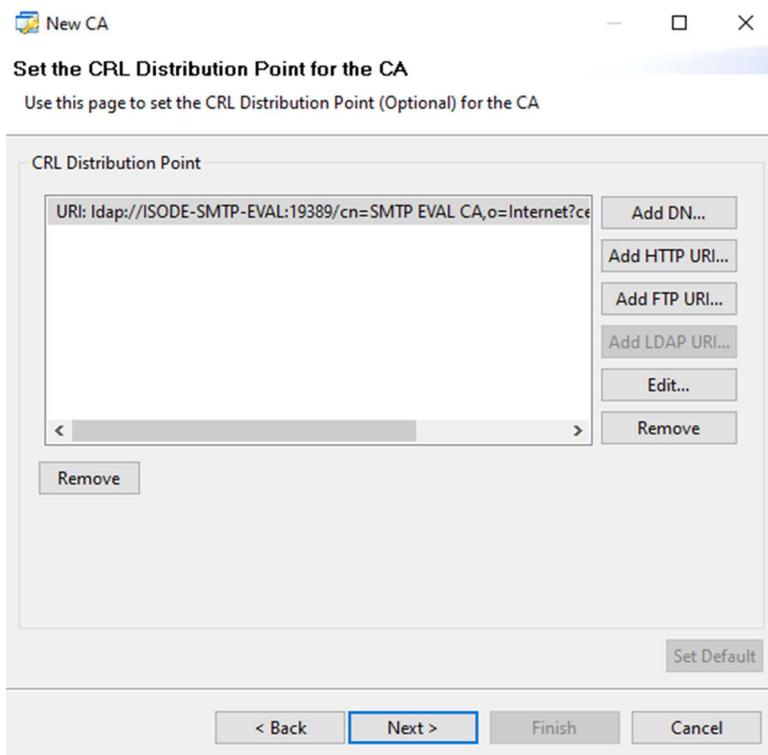
Accept the defaults and Click "Next>".

## Sodium CA initial configuration



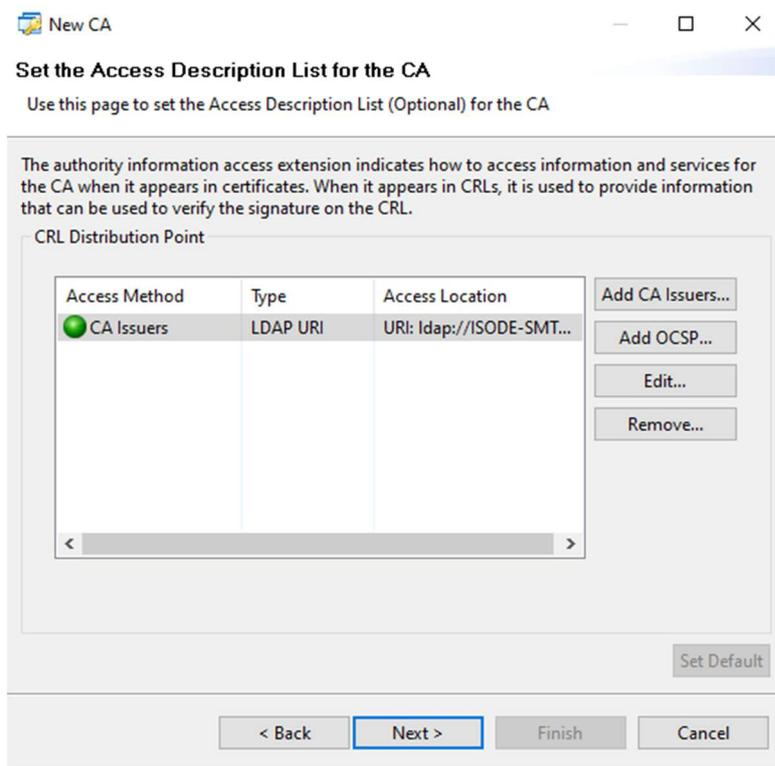
Accept the default and Click “Next>”.

## Sodium CA initial configuration



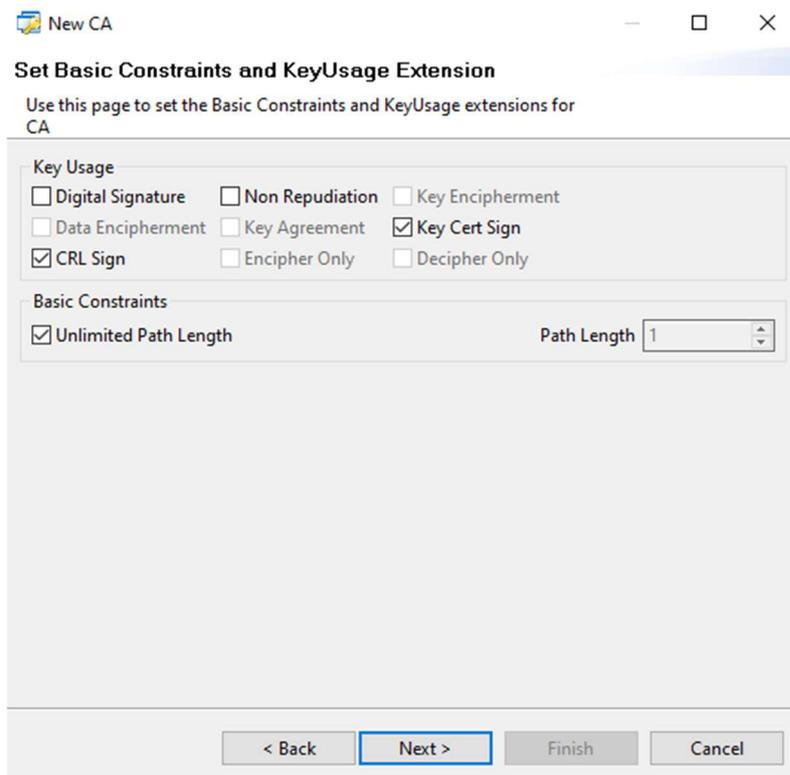
Accept the default and Click “Next>”.

## Sodium CA initial configuration



Accept the default and Click “Next>”.

## Sodium CA initial configuration



Accept the default and Click “Next>”.

## Sodium CA initial configuration

**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

Select “Generate a Self Signed Root Certificate”

## Sodium CA initial configuration

**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: 31 January 2025, 16:19

Valid To: 31 January 2035, 16:19

Lifetime

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

Include a CRL Distribution Point extension in the CA certificate

Accept the defaults and Click “Next>”.

## Sodium CA initial configuration

**New CA**

**Root CA Certificate**

The following is the Self Signed Root CA Certificate that will be generated as part of this wizard

You can either use this Certificate as a CA certificate or import another Certificate for the generated key pair later by using the Menu options on the "CA Menu".

Subject	cn=SMTP EVAL CA,o=Internet
Issuer	cn=SMTP EVAL CA,o=Internet
Valid from	Fri Jan 31 16:19:48 GMT 2025
Valid to	Wed Jan 31 16:19:48 GMT 2035
Serial	10:BF:A8:9F:84:D9:F9:B8:46:D4
PublicKeyInfo	Algorithm: RSA, KeySize: 3072
SignatureAlgorithm	SHA256WITHRSA
CertificateType	Version v3 (CA Certificate)

Display Detailed Information

< Back   **Next >**   Finish   Cancel

Click "Next>".

## Sodium CA initial configuration

**New CA**

**Finish CA Configuration**

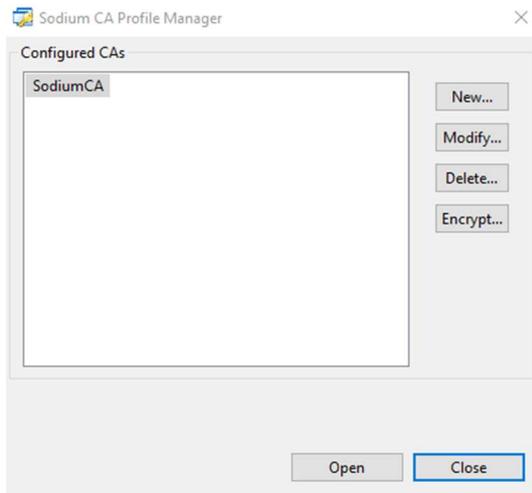
Finish Configuring the Entry for the CA being managed

When you press "Finish", the directory entry "cn=SMTP EVAL CA,o=Internet" will be added to contain information for this CA.

< Back   Next >   **Finish**   Cancel

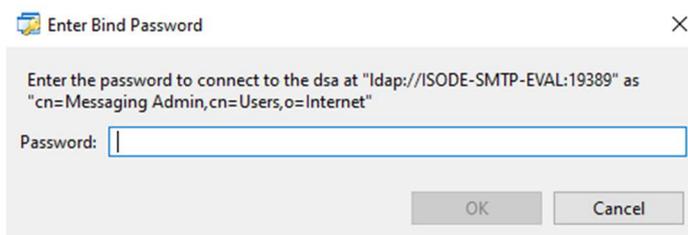
Click "Finish".

## Sodium CA initial configuration



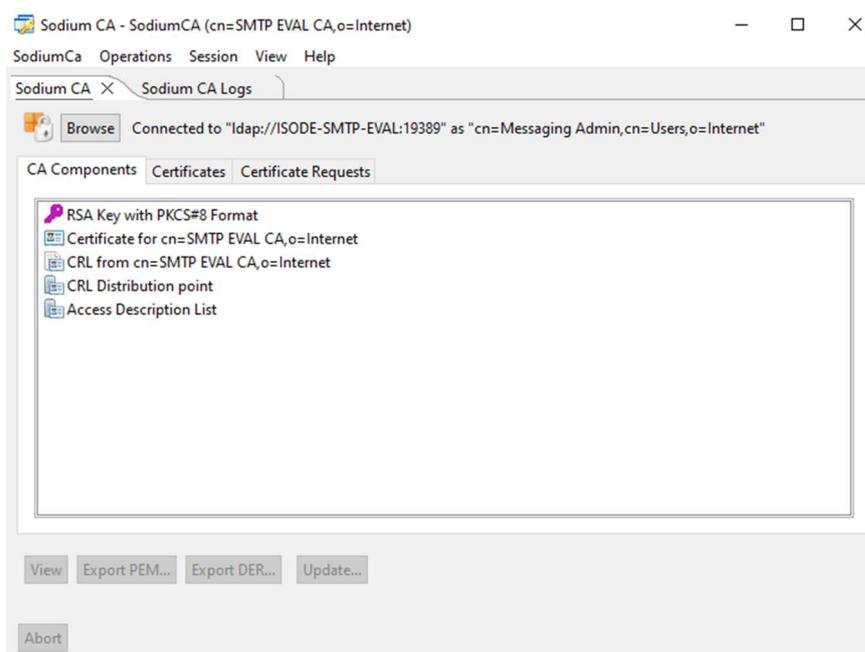
Select you newly created CA (SodiumCA) and Click “Open”.

## Sodium CA initial configuration



Enter the Password for the Messaging Admin User and Click “OK”.

## Sodium CA initial configuration

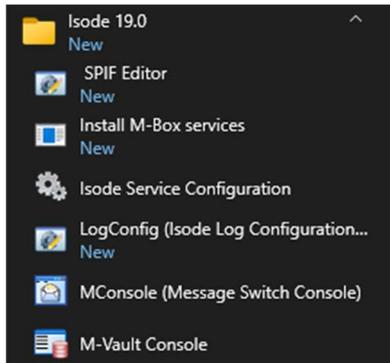


You now have your CA, leave this open and start M-Vault Console.

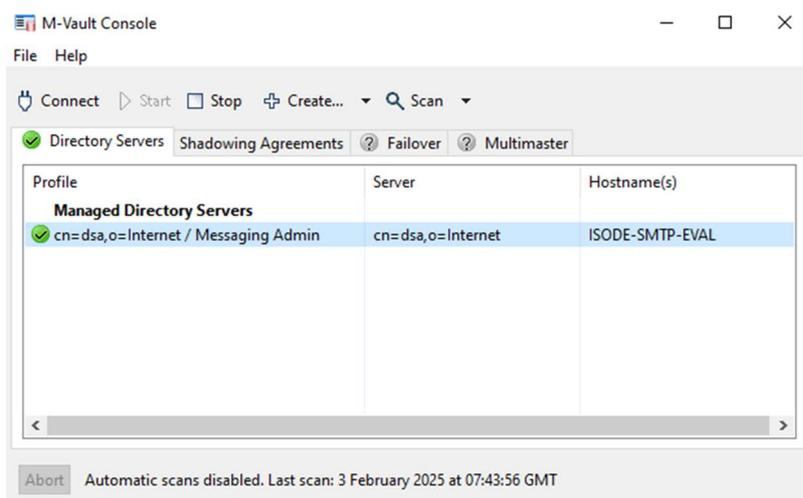
M-Vault Console is started on Windows as follows.

From the Windows Start Menu → Isode R19.0 → M-Vault Console.

### Start M-Vault Console

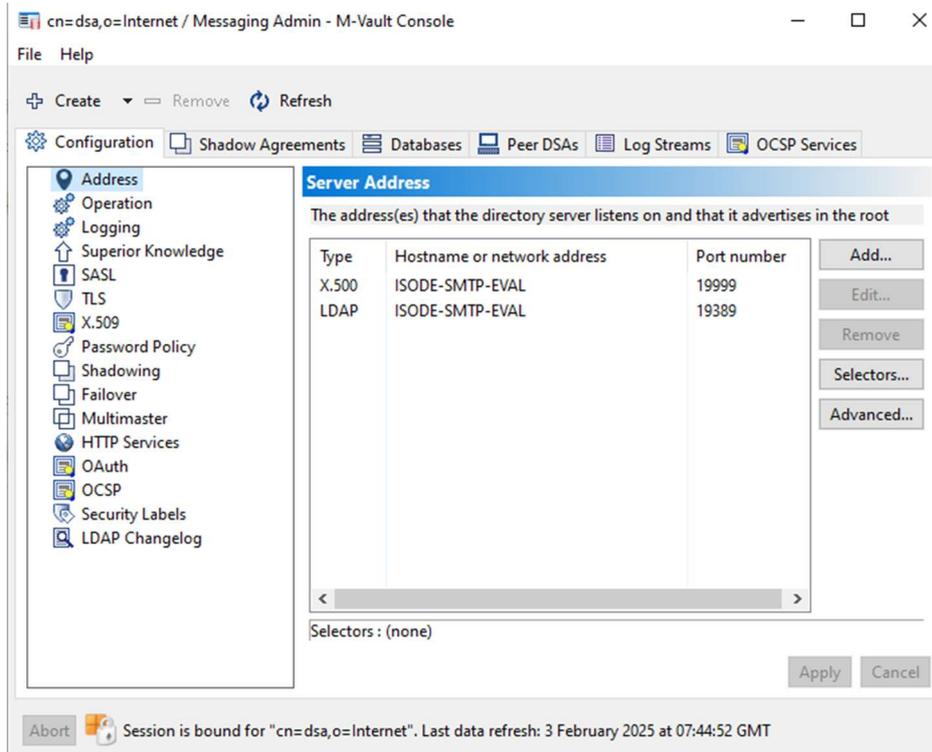


### M-Vault Console Initial Screen



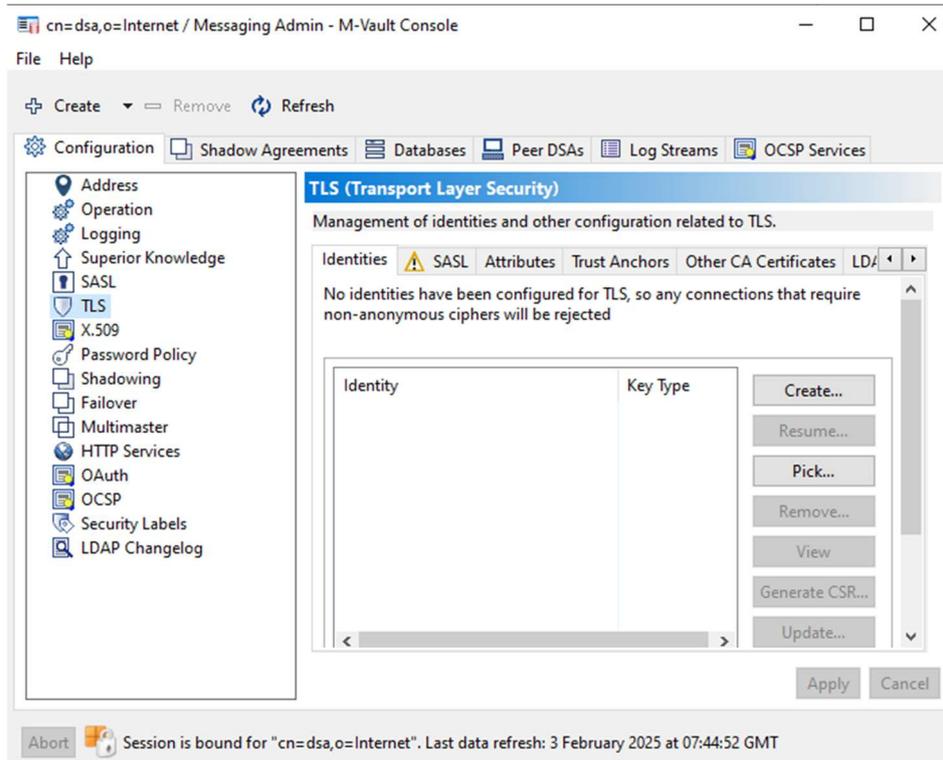
Double Click your Directory Server with the Green Tick below Managed Directory Servers.

## M-Vault Console Initial Screen



Select "TLS".

## M-Vault TLS Configuration



Select "Create..."

## M-Vault TLS Configuration

**Create TLS Identity for the Directory Server "cn=dsa,o=Internet"**

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

Subject DN:

Algorithm for the Key:  
 RSA  DSA  ECDSA

Key Size:  
 Key Size:

< Back **Next >** Finish Cancel

Click "Next>".

## M-Vault TLS Configuration

**Create TLS Identity for the Directory Server "cn=dsa,o=Internet"**

**Select and add Subject Alternative Names and Clearance**  
Specify the Subject Alternative Names and Clearance to be used in the Certificate Request for this identity

The following values have been derived from the Attributes in the entry and can be used as subject alternative names :

- DNS Name: ISODE-SMTP-EVAL
- IP Address: 2a02:c7c:1a5c:b900:c7c:bb4e:654b:83d6
- IP Address: 192.168.0.111
- IP Address: fd63:df21:78e7:0:c7c:bb4e:654b:83d6

Add other subject alternative names

Add... Edit... Remove

You can specify a custom clearance to be included in the Subject Directory Attributes Extension

None

Reset to Defaults

< Back **Next >** Finish Cancel

Accept the defaults, Click "Next>".

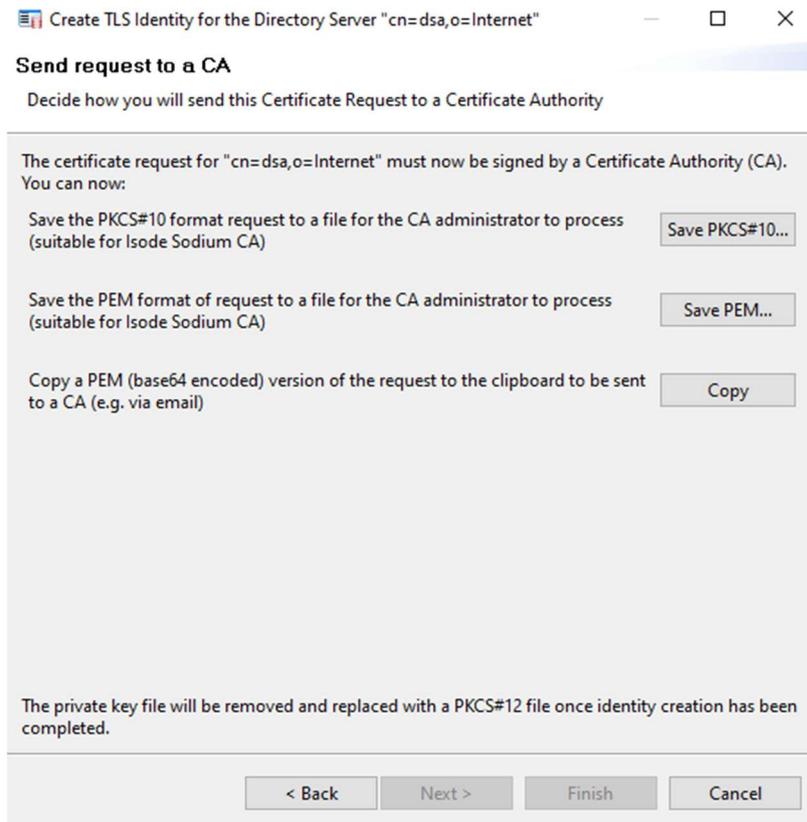
## M-Vault TLS Configuration

Click “Next>”.

## M-Vault TLS Configuration

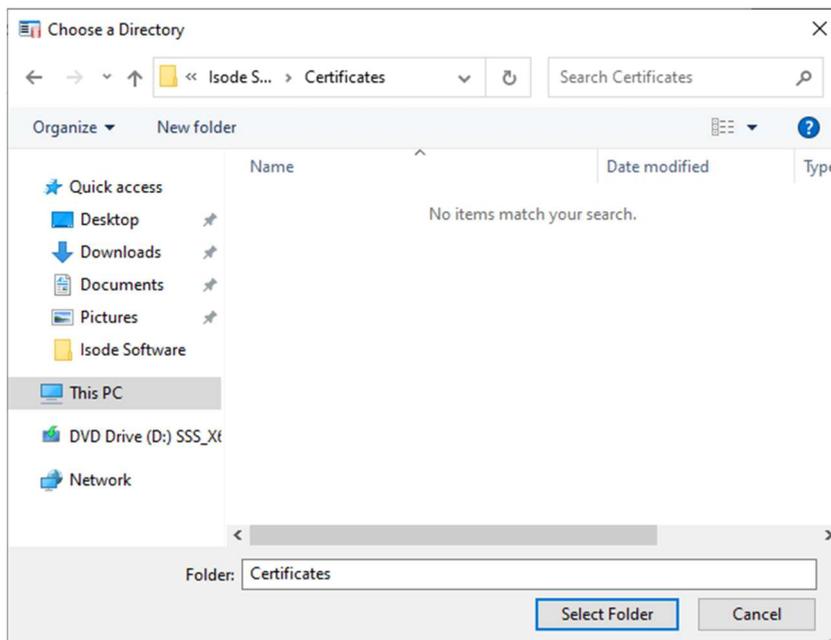
Click “Next>”.

## M-Vault TLS Configuration



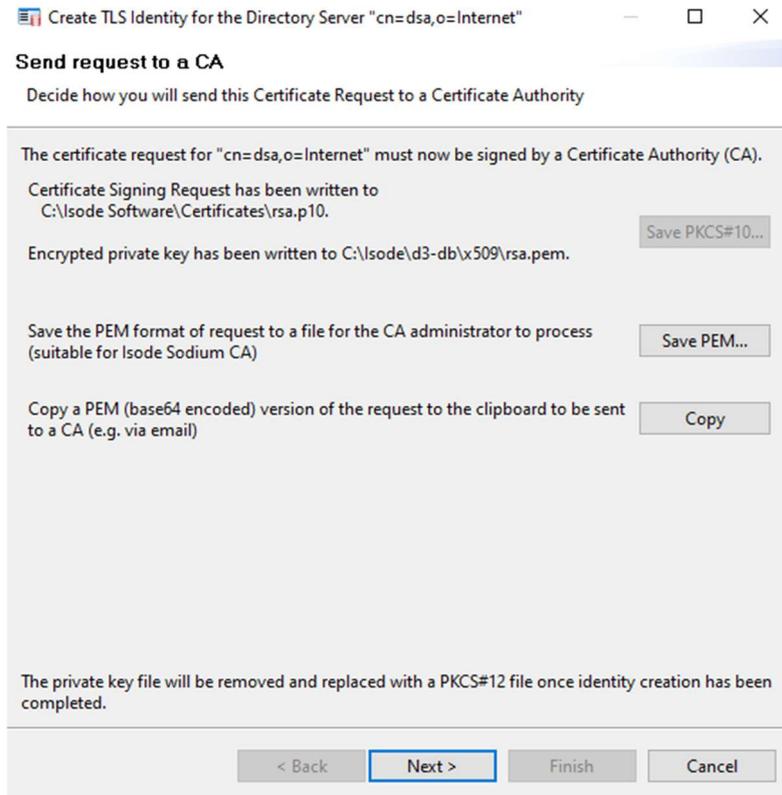
Click “Save PKCS10...”

## M-Vault TLS Configuration



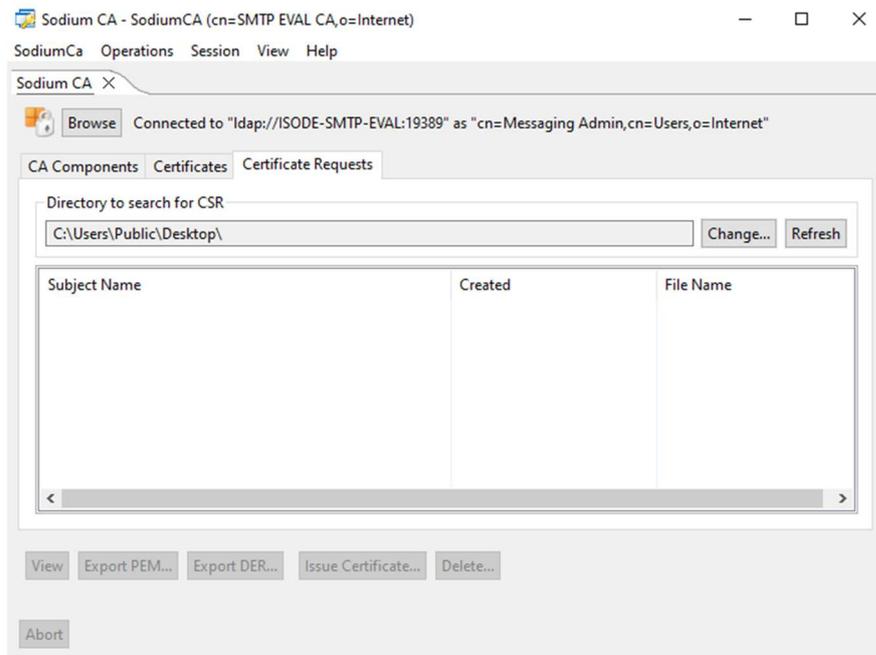
Browse to your Certificates Folder and Click “Select Folder”.

## M-Vault TLS Configuration



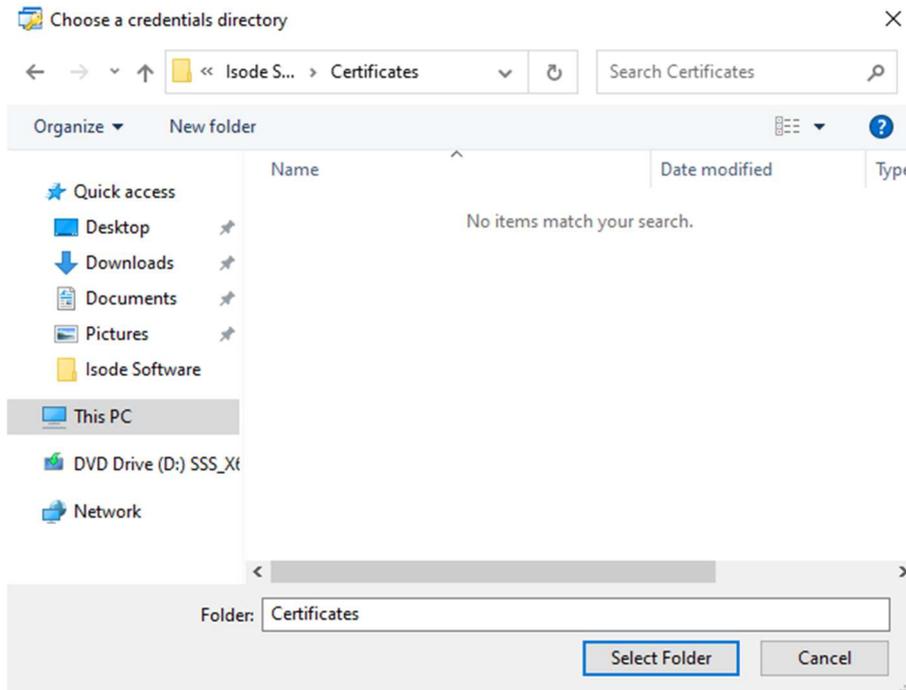
Now we return to Sodium CA.

## Sodium CA Issue Certificate



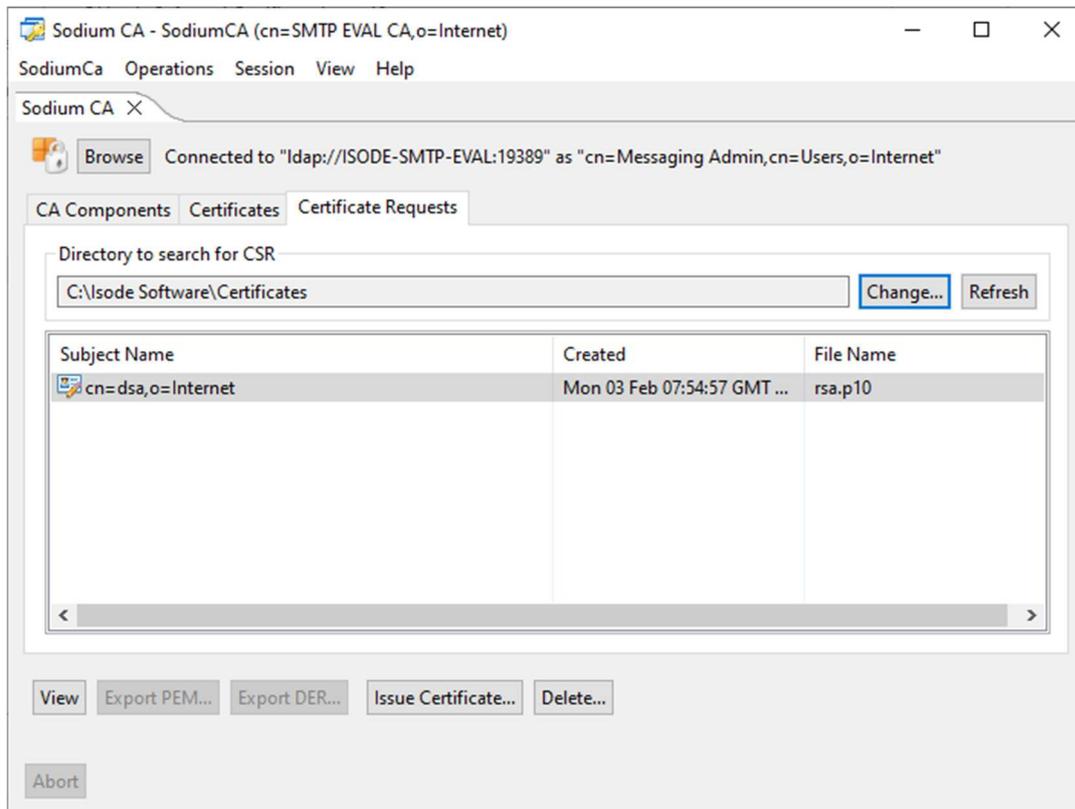
Select the Certificate Requests Tab and Click "Change..." for the CSR Folder.

## Sodium CA Issue Certificate



Browse to your Certificates Folder and Click “Select Folder”.

## Sodium CA Issue Certificate



You should see your Certificate request there, select it and click “Issue Certificate...”.

## Sodium CA Issue Certificate

**Issue Certificate for a CSR**

**Certificate Signing Request**

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

Subject:

PublicKeyInfo:

DNS Name:

The certificate request for "cn=dsa,o=Internet" has the following subject key identifier:  
F2:54:2F:7D:91:24:98:6C:64:E7:4A:C1:F1:2D:49:AE:2B:7B:59:B1

Click "Next>".

## Sodium CA Issue Certificate

**Issue Certificate for a CSR**

**Select and add Subject Alternative Names**

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

Subject:

Following are the available subject alternative names :

DNS Name: ISODE-SMTP-EVAL

Add other subject alternative names to appear in the certificate:

Click "Next>".

## Sodium CA Issue Certificate

Issue Certificate for a CSR

**Select and Create X.509 Extensions**  
Use this page to set X.509 Extensions in the Certificate

CA Certificate  
 End Entity Certificate

Key Usage

Digital Signature     Non Repudiation     Key Encipherment  
 Data Encipherment     Key Agreement     Key Cert Sign  
 CRL Sign     Encipher Only     Decipher Only

Extended Key Usage Extension

TLS WWW server authentication Edit...

Add OCSF No Check Extension

CA Extensions

Select the extensions to be included in the certificate

CRL Distribution Points  
 Authority Information Access

< Back    **Next >**    Finish    Cancel

Click “Next>”.

## Sodium CA Issue Certificate

Issue Certificate for a CSR

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

Valid From: 3 February 2025, 07:58 Edit...

Valid To: 3 February 2026, 07:58 Edit...

Lifetime

Years: 1    Months: 0    Days: 0    Hours: 0

Reset

Signature Algorithm: SHA256WITHRSA

Delete the CSR after the Certificate generation

< Back    **Next >**    Finish    Cancel

Accept the defaults, Click “Next>”.

## Sodium CA Issue Certificate

**Generated Certificate**  
The following certificate will be generated.

Subject	cn=dsa,o=Internet
Issuer	cn=SMTP EVAL CA,o=Internet
Valid from	Mon Feb 03 07:58:42 GMT 2025
Valid to	Tue Feb 03 07:58:42 GMT 2026
Serial	06:2B:55:19:10:9E:F9:19:C4:C6
PublicKeyInfo	Algorithm: RSA, KeySize: 3072
SignatureAlgorithm	SHA256WITHRSA
CertificateType	Version v3 (Not a CA Certificate)

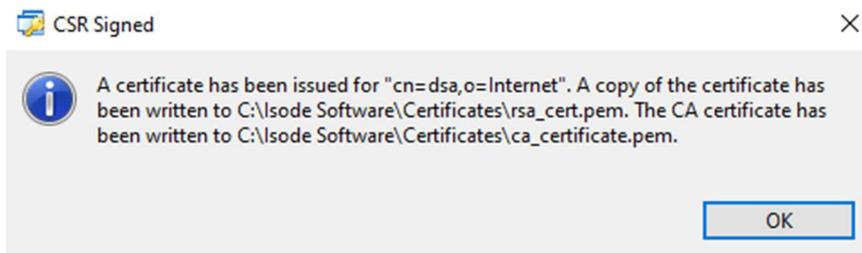
Display Detailed Information

Export to disk: Write certificate in PEM format

< Back   Next >   **Finish**   Cancel

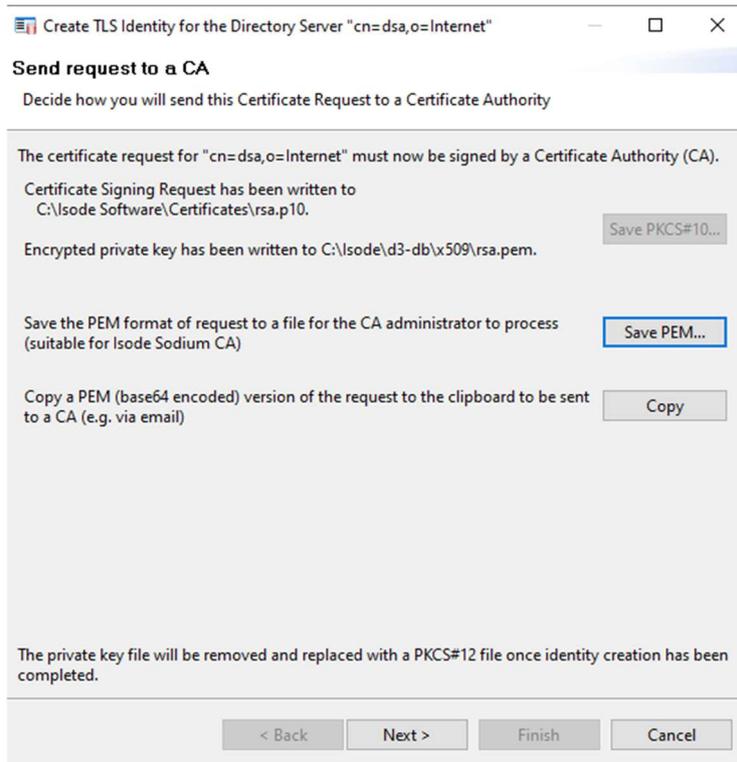
Click “Finish”.

## Sodium CA Issue Certificate



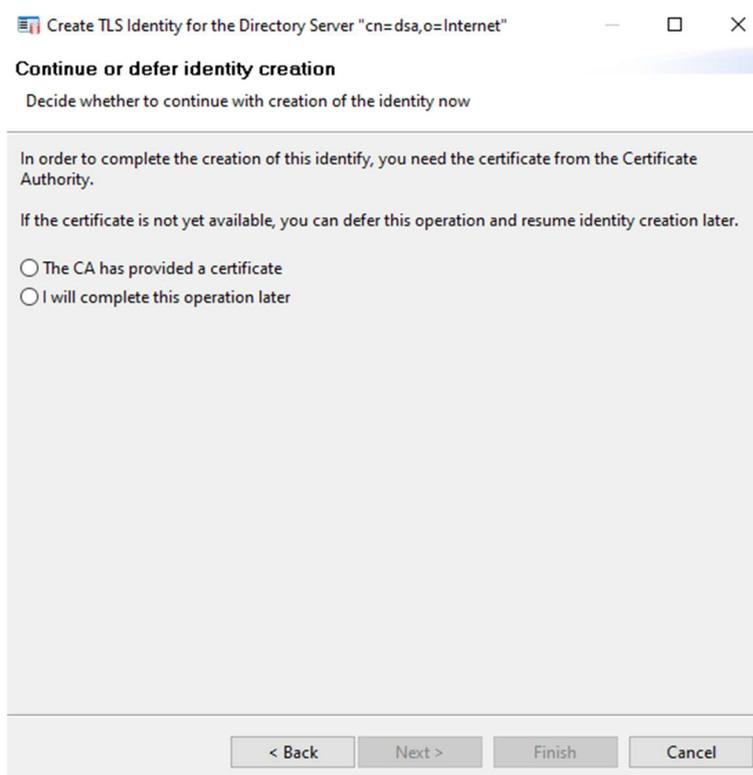
Click “OK” and return to M-Vault Console.

## M-Vault Console Certificate Import



Select "Next>"

## M-Vault Console Certificate Import



Select the CA has provided a certificate and Click "Next>"

## M-Vault Console Certificate Import

Create TLS Identity for the Directory Server "cn=dsa,o=Internet"

### User Certificate

The following certificate matches the certificate request for this identity

Subject	cn=dsa,o=Internet
Issuer	cn=SMTP EVAL CA,o=Internet
Valid from	Mon Feb 03 07:58:42 GMT 2025
Valid to	Tue Feb 03 07:58:42 GMT 2026
Serial	4F:A6:C4:C6:F8:0F:C2:42:E6:64
PublicKeyInfo	Algorithm: RSA, KeySize: 3072
SignatureAlgorithm	SHA256WITHRSA
CertificateType	Version v3 (Not a CA Certificate)

Display Detailed Information

< Back   Next >   Finish   Cancel

Click "Next>".

## M-Vault Console Certificate Import

Create TLS Identity for the Directory Server "cn=dsa,o=Internet"

### 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=Internet
Self Signed CA	cn=SMTP EVAL CA,o=Internet

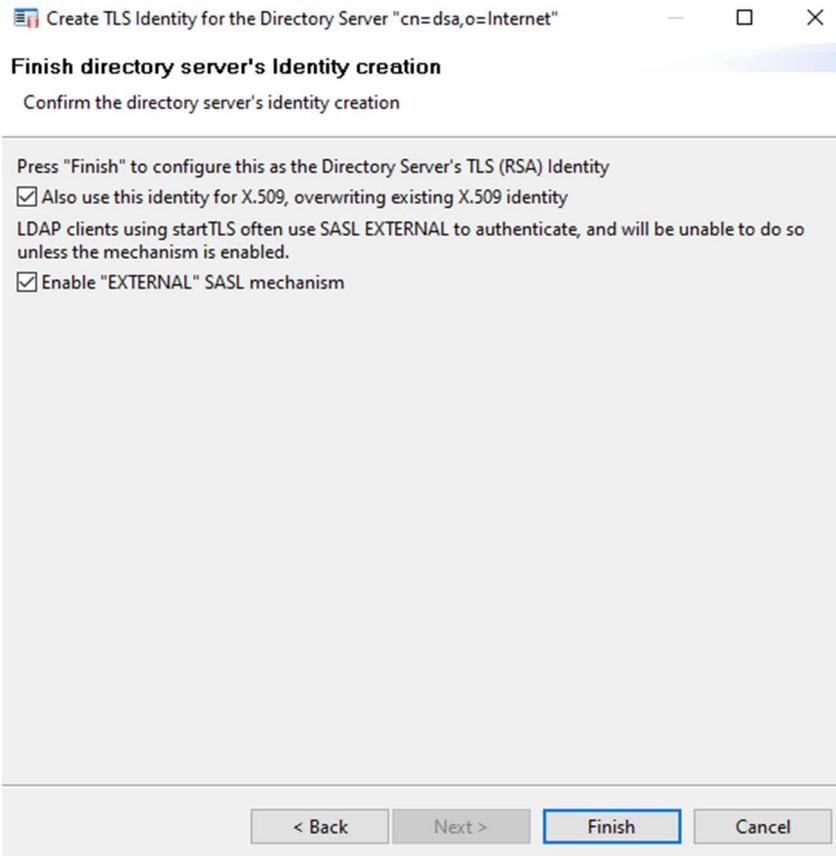
Add certificate...

Chain status: Certificate chain is complete

< Back   Next >   Finish   Cancel

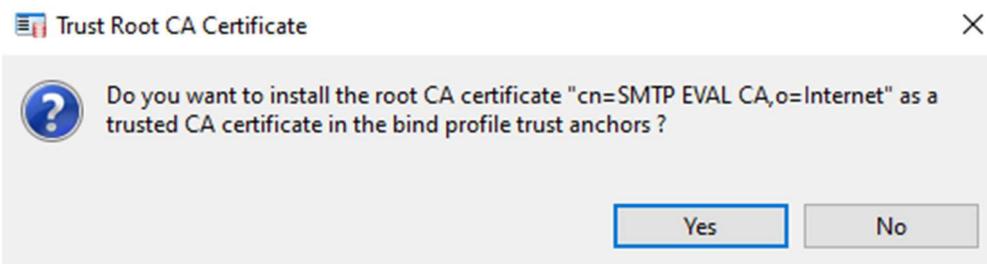
Click "Next>".

## M-Vault Console Certificate Import



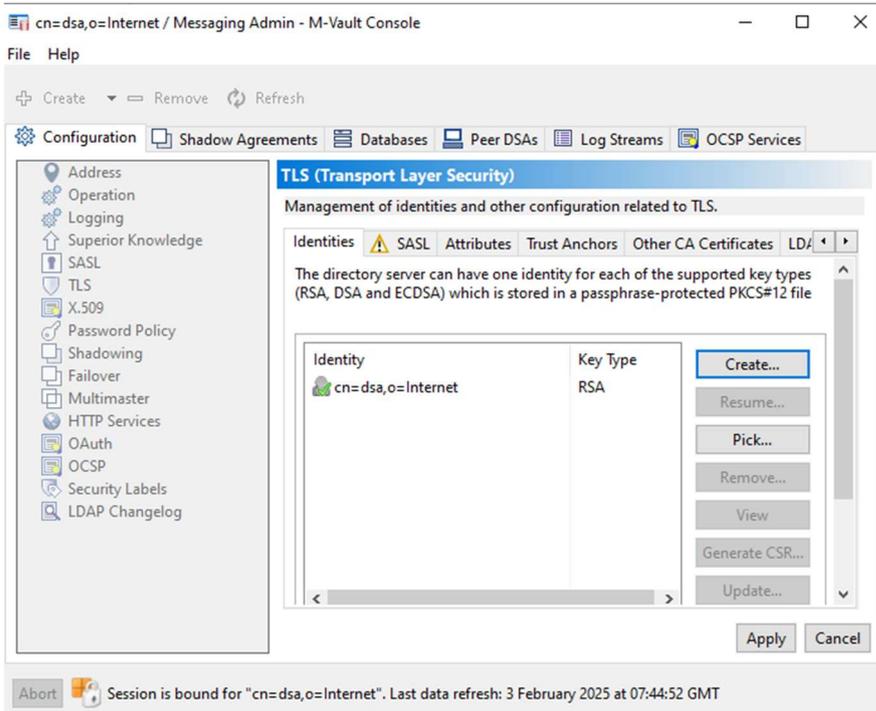
Uncheck the "Enable "EXTERNAL" SASL mechanism". Click "Finish".

## M-Vault Console Certificate Import



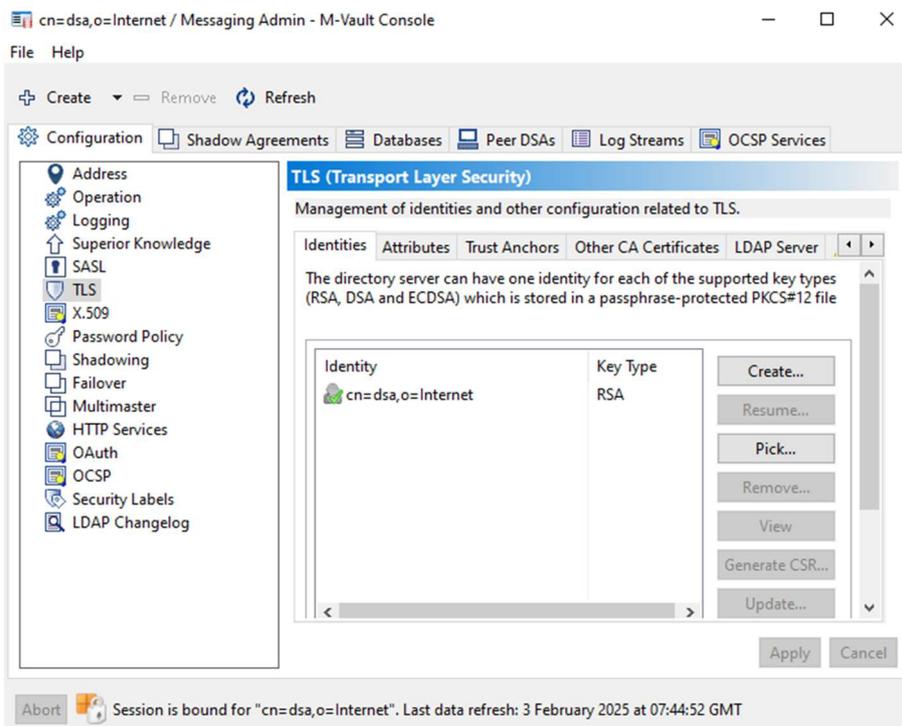
Click "Yes".

## M-Vault Console Certificate Import



Click “Apply”

## M-Vault Console Certificate Import



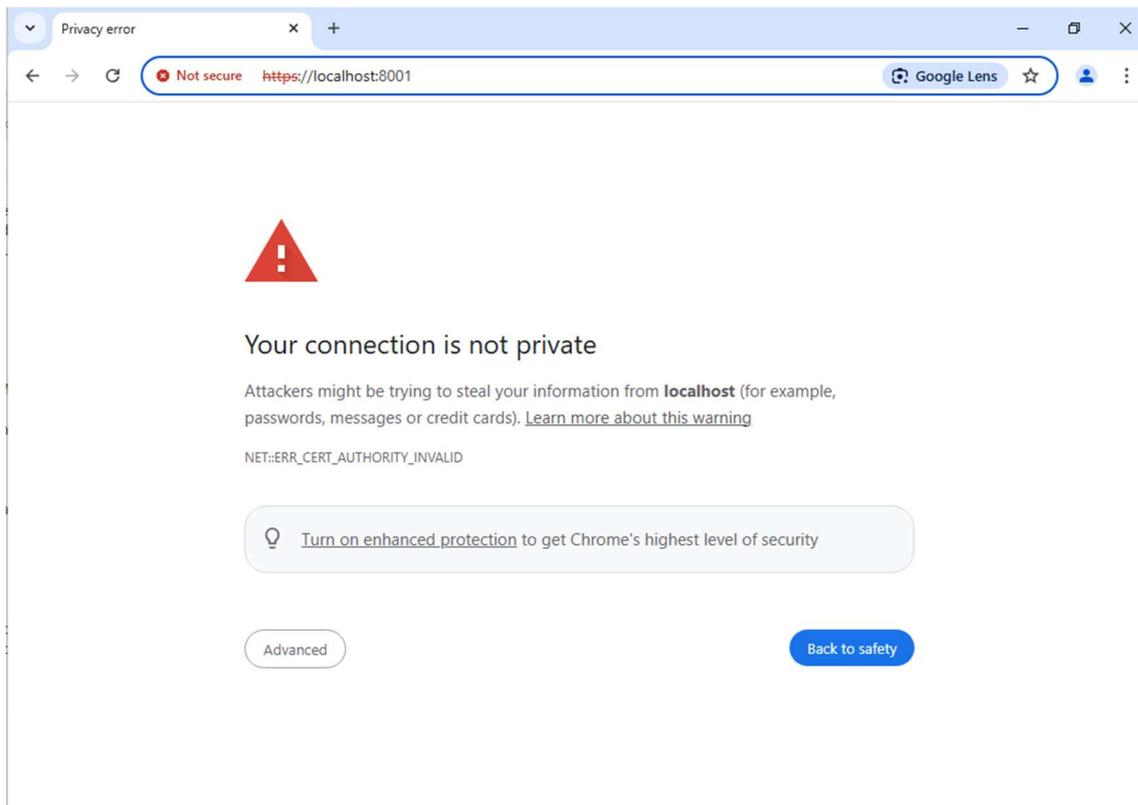
Your M-Vault Server now has TLS configured and you are ready to proceed to configuring Users with Cobalt.

## Provisioning Users with Cobalt

You will now provision two Users for this Messaging System using Cobalt. Point your Browser to the URL below.

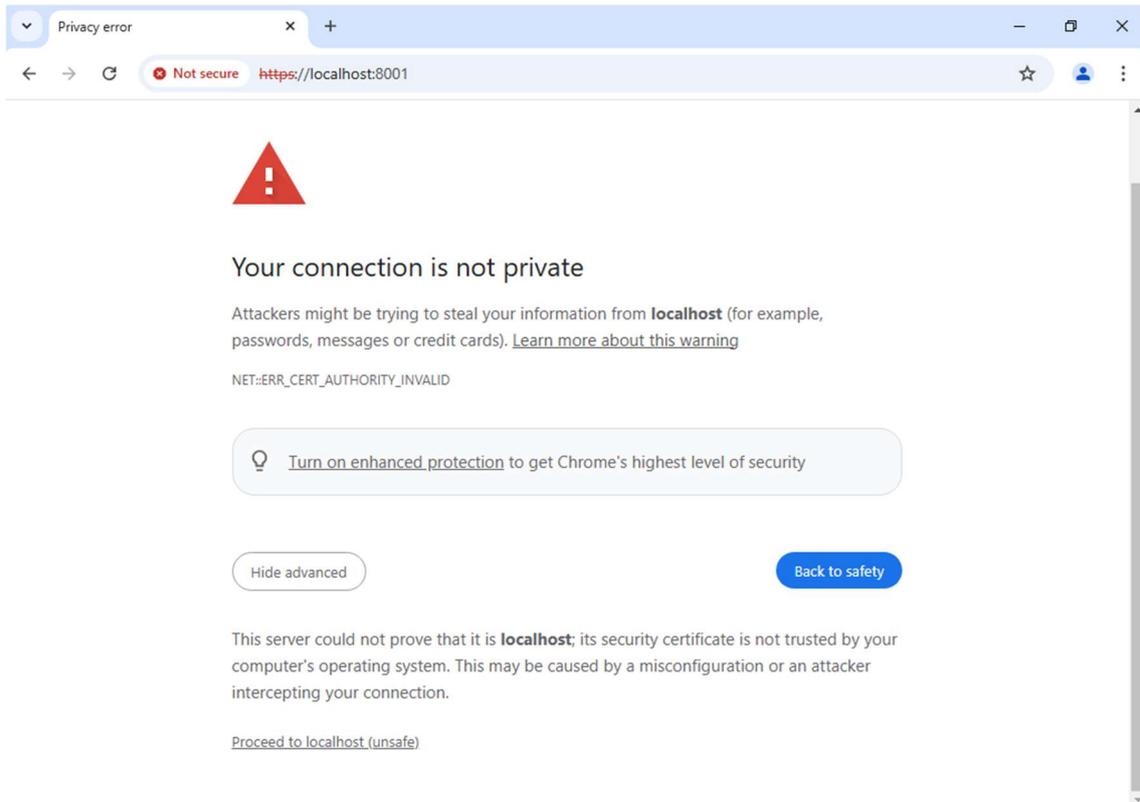
`https://localhost:8001`

*Cobalt Initial Setup.*



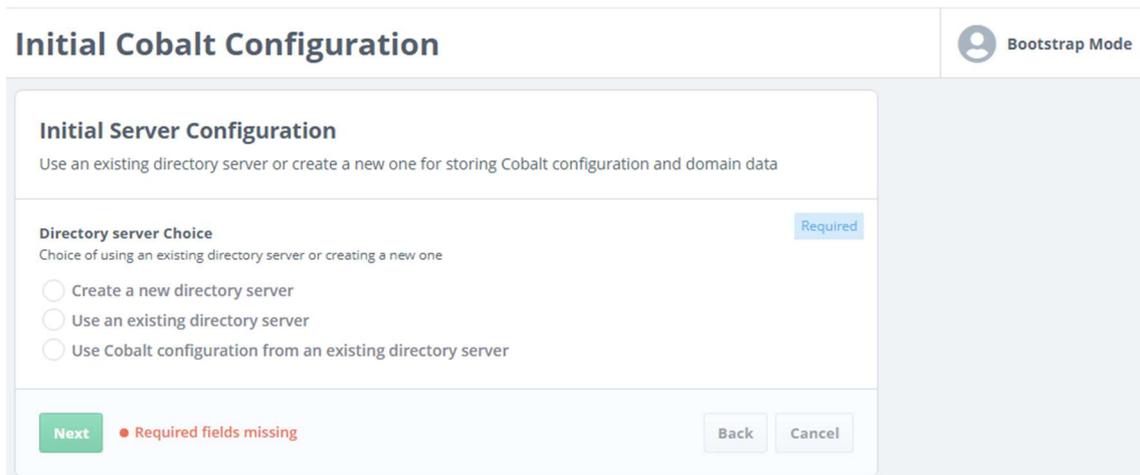
Click “Advanced”.

*Cobalt Initial Setup.*



Click "Proceed to localhost (unsafe)".

*Cobalt Initial Setup.*



Select "Use an existing directory server".

*Cobalt Initial Setup.*

## Initial Cobalt Configuration

Bootstrap Mode

### 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

**Master Directory Server Port**

The port number of the LDAP server that holds users and roles

 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

Check the “Hostname” matches your server. Next to the Cobalt Server DN Click “Choose”.

*Cobalt Initial Setup.*

**Search for cobalt server dn**
×

ISODE-SMTP-EVAL:19389

Messaging Configuration	cn=Messaging Configuration,o=Internet
Messaging Admin	messaging.admin@internet.net cn=Messaging Admin,cn=Users,o=Internet
Messaging Configuration Managers	cn=Messaging Configuration Managers,cn=Groups,o=Interr
Messaging Configuration Viewers	cn=Messaging Configuration Viewers,cn=Groups,o=Internet

Start typing “mess” and then Select “Messaging Admin”.

Evaluation Guide: M-Switch SMTP

Page 54 of 91

*Cobalt Initial Setup.*

**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=Internet
Choose

**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...](#)

Choose

Next
● Required fields missing
Back
Cancel

Enter the Messaging Admin Password and Click Choose next to the Configuration Naming Context.

*Cobalt Initial Setup.*

**Select configuration naming context**
×

ISODE-SMTP-EVAL:19389

Internet
o=Internet

Select
Cancel

Select "Internet" and Click "Select".

## Cobalt Initial Setup.

**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...](#)

**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...](#)

Click “Next”.

## Cobalt Initial Setup.

### Initial Cobalt Configuration

**Initial Server Configuration (3/3)**

Details about location of users and configuration

**Domain**

**Domain** Required

The domain to use for the initial Cobalt Administrator

**Admin's Full Name** Required

Name of the initial Cobalt Administrator

**Admin's mail ID** Required

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

On this screen enter “internet.net” for the domain and your choice for the Cobalt Admin Name. The Admin’s mail ID will auto-populate. Then scroll down.

## Cobalt Initial Setup.

<b>Domain</b> <small>The domain to use for the initial Cobalt Administrator</small>	Required
<input type="text" value="internet.net"/>	
<b>Admin's Full Name</b> <small>Name of the initial Cobalt Administrator</small>	Required
<input type="text" value="Cobalt Admin"/>	
<b>Admin's mail ID</b> <small>ID of the initial Cobalt Administrator to be used for logging into Cobalt</small>	Required
<input type="text" value="cobalt.admin"/> <input type="text" value="@internet.net"/>	
<b>Admin's password</b> <small>Admin's password</small>	Required
<input type="password" value="....."/> <input type="button" value="Show"/> <input type="button" value="Generate"/>	
<input type="button" value="Finish"/> <input type="button" value="Back"/> <input type="button" value="Cancel"/>	

Enter a Password of your choice (again we suggest “secret”) and Click “Show” to check it. Then Click “Finish”. The following screen will be displayed.

## Cobalt Login.

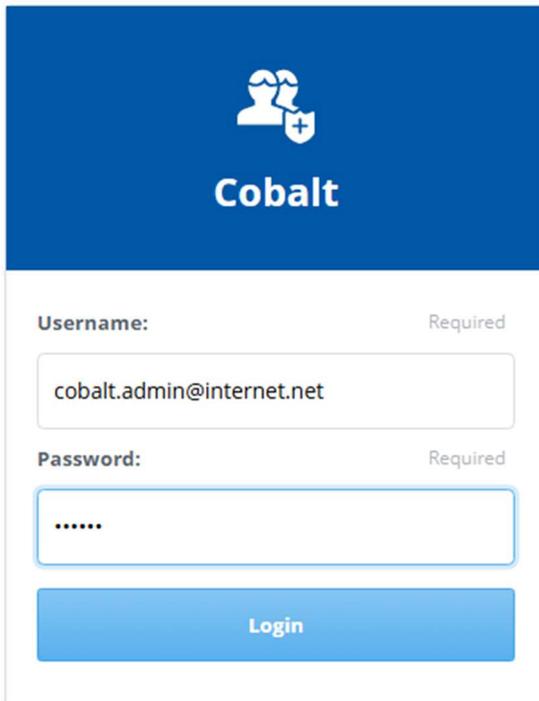


# Cobalt

<b>Username:</b>	Required
<input type="text" value="user@example.com"/>	
<b>Password:</b>	Required
<input type="password" value="....."/>	
<input type="button" value="Login"/>	

Enter the Login details you just created.

*Cobalt Login.*



**Cobalt**

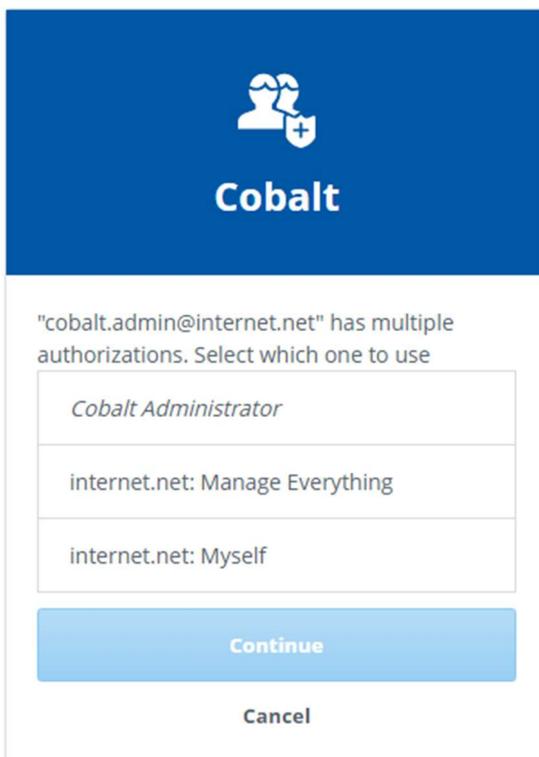
Username: Required  
cobalt.admin@internet.net

Password: Required  
.....

Login

Click “Login”.

*Cobalt Login.*



**Cobalt**

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

Cobalt Administrator

internet.net: Manage Everything

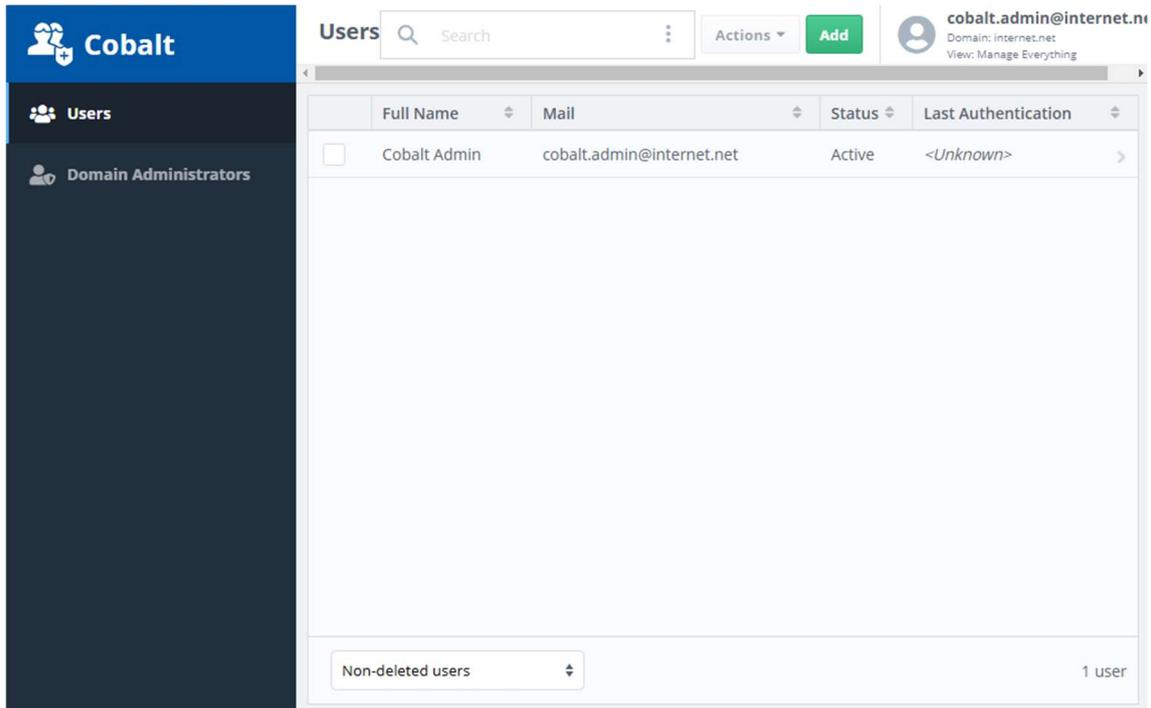
internet.net: Myself

Continue

Cancel

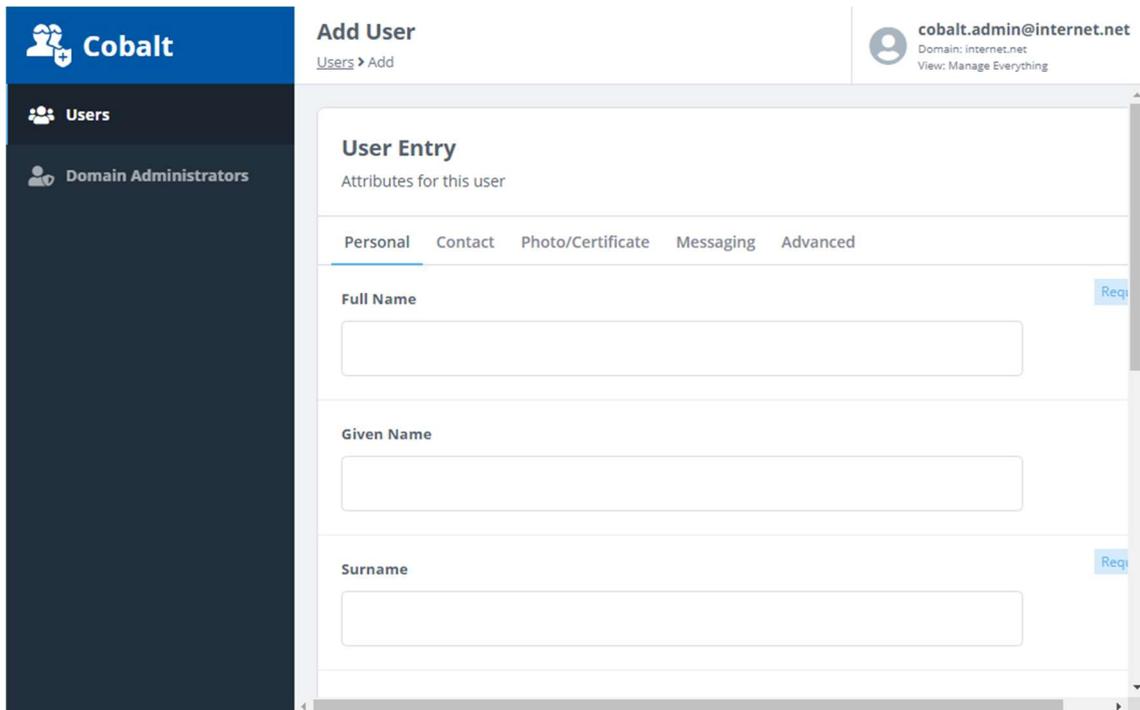
Select “internet.net: Manage Everything”, Click “Continue”.

*Cobalt User Provisioning.*



Click “Add”.

*Cobalt User Provisioning.*



Type a Full Name, in this guide “User One”, the other fields will auto-populate.

*Cobalt User Provisioning.*

The screenshot shows the 'Add User' interface in Cobalt. The left sidebar contains 'Users' and 'Domain Administrators'. The main content area is titled 'Add User' and 'Users > Add'. The user profile at the top right shows 'cobalt.admin@internet.net'. The 'User Entry' section is active, showing 'Attributes for this user' with tabs for 'Personal', 'Contact', 'Photo/Certificate', 'Messaging', and 'Advanced'. The 'Personal' tab is selected, containing three required fields: 'Full Name' (with value 'User One'), 'Given Name' (with value 'User'), and 'Surname' (with value 'One').

Scroll down, and enter a Password, we suggest “secret”.

*Cobalt User Provisioning.*

This screenshot shows the lower portion of the 'Add User' form. The 'Full Name' field is partially visible with a masked password '.....'. Below it are the 'Primary Email Address and XMPP JID' section, which includes a text input for 'user.one' and a dropdown for '@internet.net'. The 'Alternative Email Addresses' section has a sub-header 'Alternative email addresses for the user' and a single entry field with '@internet.net', 'x', and '+' buttons. The 'Entry Type' section has a dropdown menu set to 'User'. At the bottom, there are 'Add' and 'Cancel' buttons.

Click “Add”.

*Cobalt User Provisioning.*

The screenshot shows the Cobalt user provisioning interface. On the left is a dark sidebar with the 'Cobalt' logo and navigation options for 'Users' and 'Domain Administrators'. The main area is titled 'Users' and contains a search bar, an 'Add' button, and a table of users. The table has columns for 'Full Name', 'Mail', 'Status', and 'Last Authentication'. Two users are listed: 'Cobalt Admin' with email 'cobalt.admin@internet.net' and 'User One' with email 'user.one@internet.net'. Both are 'Active' and have '<Unknown>' for their last authentication.

	Full Name	Mail	Status	Last Authentication
<input type="checkbox"/>	Cobalt Admin	cobalt.admin@internet.net	Active	<Unknown>
<input type="checkbox"/>	User One	user.one@internet.net	Active	<Unknown>

User One has now been successfully added.

Repeat the Process for User Two.

*Cobalt User Provisioning.*

This screenshot is similar to the previous one but includes a third user, 'User Two', with email 'user.two@internet.net'. The table now lists three users, all with 'Active' status and '<Unknown>' last authentication.

	Full Name	Mail	Status	Last Authentication
<input type="checkbox"/>	Cobalt Admin	cobalt.admin@internet.net	Active	<Unknown>
<input type="checkbox"/>	User One	user.one@internet.net	Active	<Unknown>
<input type="checkbox"/>	User Two	user.two@internet.net	Active	<Unknown>

User Two has now been successfully added.

This completes the provisioning for the Domain internet.net we will return towards the end of this guide to Add Users for x400.net, these will act as Address Book entries only.

We will now configure the Harrier Server for this domain.

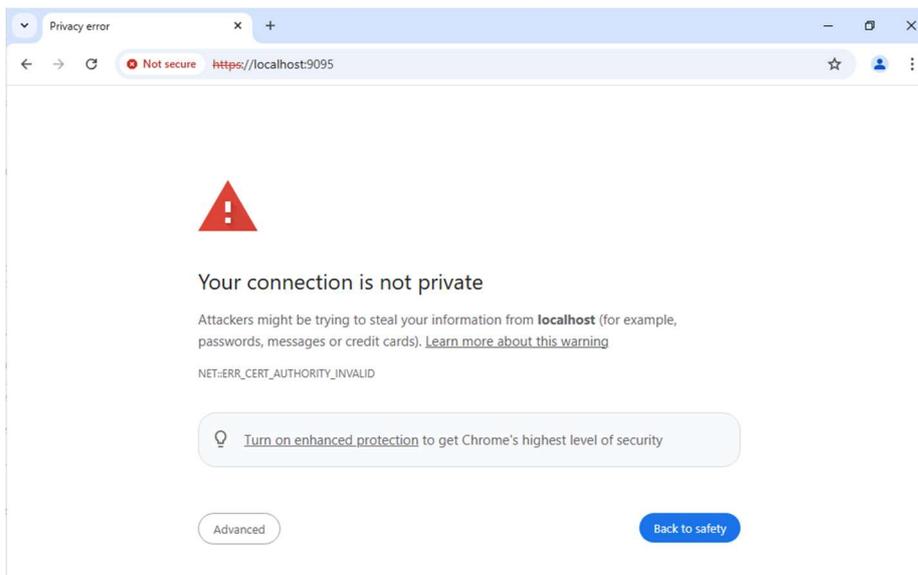
## Configuring Harrier

The Harrier Server needs to be configured before it can be used to connect to M-Switch/M-Vault/M-Box. The Harrier Service is automatically started on Windows and is started with the Command below on Linux.

```
# systemctl start harrier
```

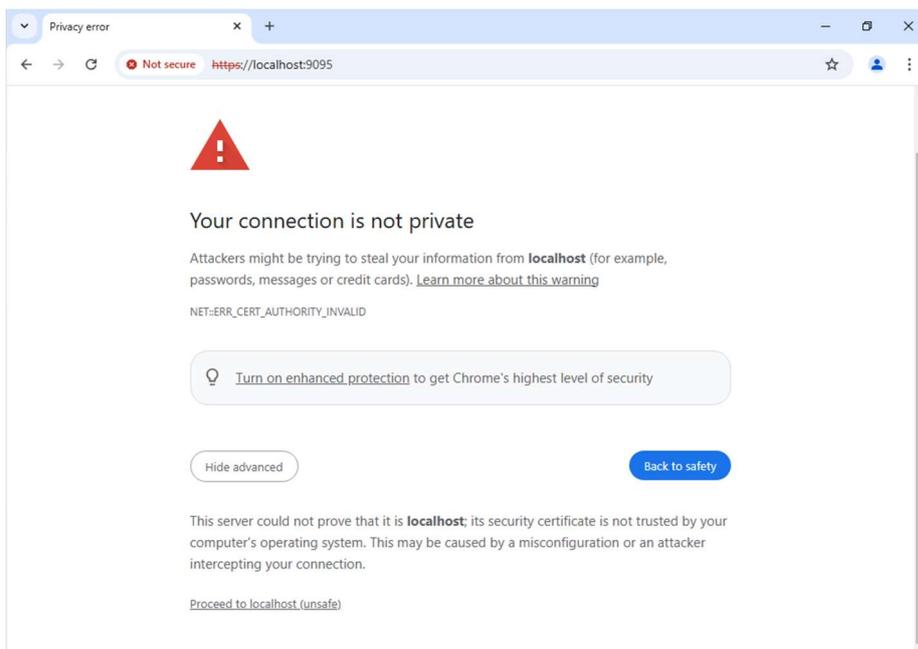
To Start configuring Harrier point your browser to <https://localhost:9095> .

*Initial Harrier Screen.*



Click “Advanced”.

*Initial Harrier Screen.*



Click “Proceed to localhost (unsafe)”.

Register Initial Harrier Admin.

### Register initial administrator user

These initial manager credentials will be used to log in to the manager interface, for initial configuration of the server.

**Login** Required

Manager login (letters, numbers and symbols other than ... [More...](#))

**Password** Required

Manager password (no character restrictions)

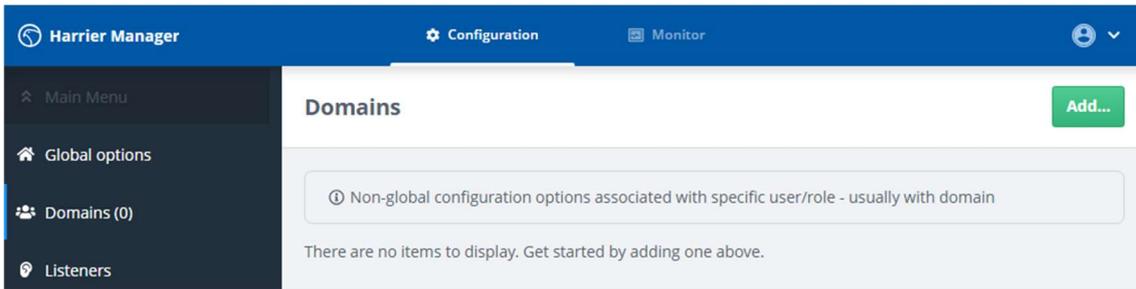
Choose a Login name of your choice or accept the default and a password (again we suggest “secret”). Click “Submit”. The following screen is displayed

Initial Harrier Screen.

The screenshot shows the Harrier Manager interface. The top navigation bar includes 'Harrier Manager', 'Configuration', and 'Monitor'. A left-hand sidebar menu lists various settings: Main Menu, Global options, Domains (0), Listeners, TLS, PKCS#11, Proxy (0), S/MIME, Manager, and Logging Streams (2). The 'Global Options' section is expanded, showing 'Server configuration' with the following fields: 'Server name' (value: Harrier, checkbox: Use default), 'Server host' (checkbox: Use default), 'Default login domain' (checkbox: Use default), and 'Runtime user' (checkbox: Use default). Each field has a 'More...' link for additional information.

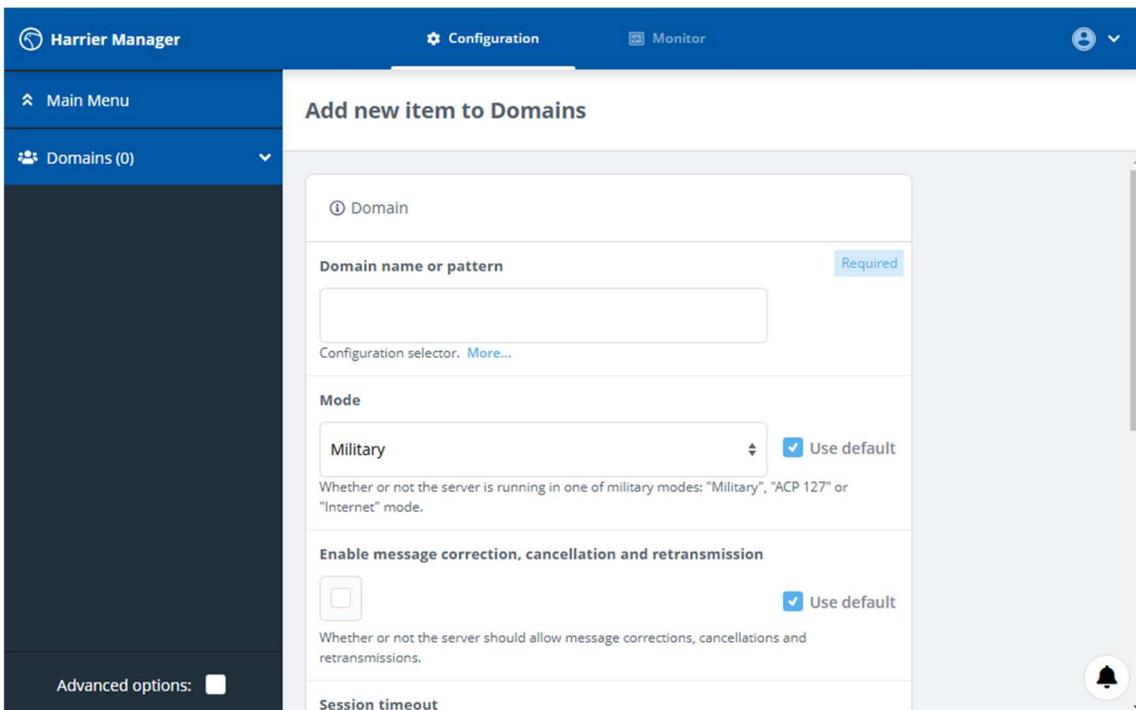
From the left-hand menu select “Domains”.

## Harrier Domain Configuration.



Click “Add...”

## Harrier Domain Configuration.



Enter “internet.net” for the “Domain name or pattern” and select “Internet” for the “Mode”.

Harrier Domain Configuration.

The screenshot shows the 'Add new item to Domains' configuration form in Harrier Manager. The form includes the following sections:

- Domain:** A header section with an information icon.
- Domain name or pattern:** A text input field containing 'internet.net', marked as 'Required'. Below it is a 'Configuration selector' with a 'More...' link.
- Mode:** A dropdown menu set to 'Internet', with a 'Use default' checkbox.
- Enable message correction, cancellation and retransmission:** A checkbox that is currently unchecked, with a 'Use default' checkbox checked.
- Session timeout:** A section partially visible at the bottom of the form.

Scroll down.

Harrier Domain Configuration.

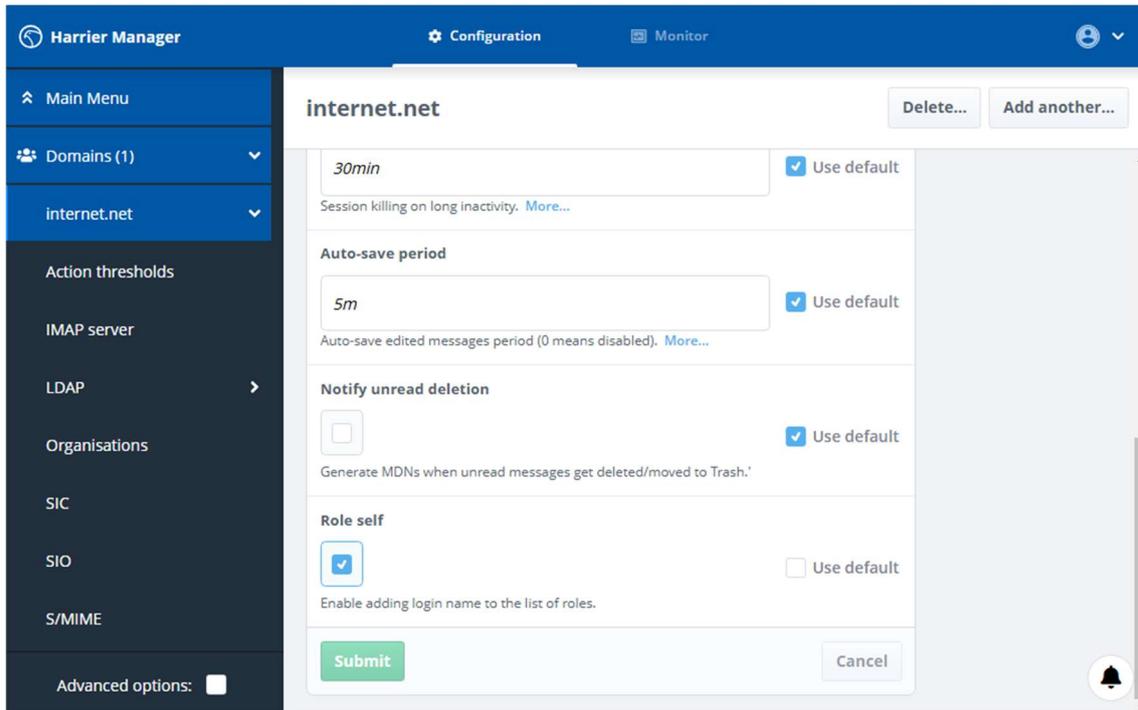
The screenshot shows the 'Add new item to Domains' configuration form in Harrier Manager, scrolled down to show additional options:

- Session killing on long inactivity:** A text input field containing '30min', with a 'Use default' checkbox checked.
- Auto-save period:** A text input field containing '5m', with a 'Use default' checkbox checked.
- Notify unread deletion:** A checkbox that is currently unchecked, with a 'Use default' checkbox checked.
- Role self:** A checkbox that is currently checked, with a 'Use default' checkbox unchecked.

At the bottom of the form, there are two buttons: a green 'Add' button and a grey 'Cancel' button.

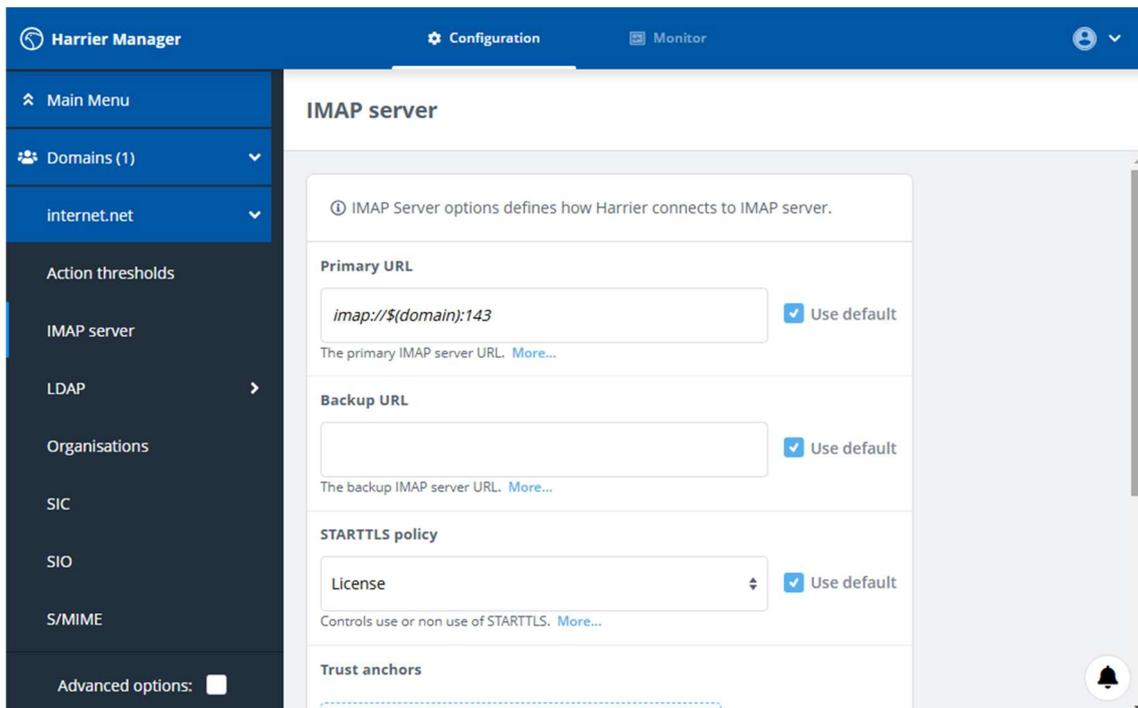
Make sure "Role self" is checked and click "Add".

## Harrier Domain Configuration.



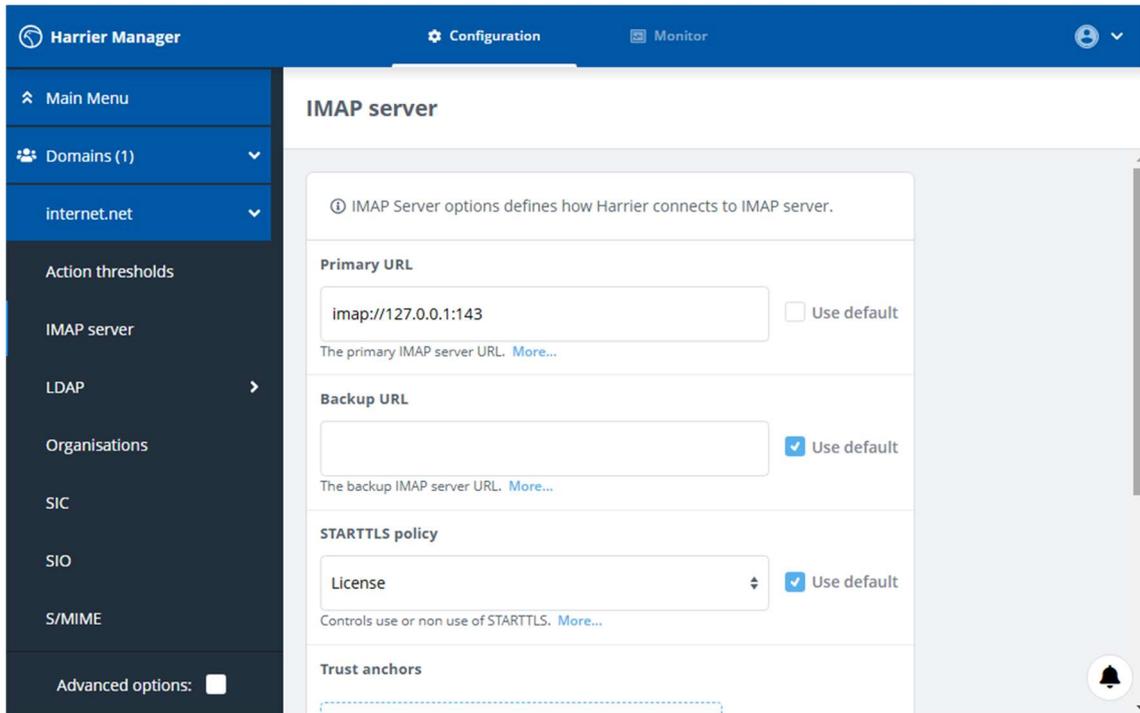
From the left-hand menu select “IMAP Server”.

## Harrier Domain Configuration – IMAP Server.



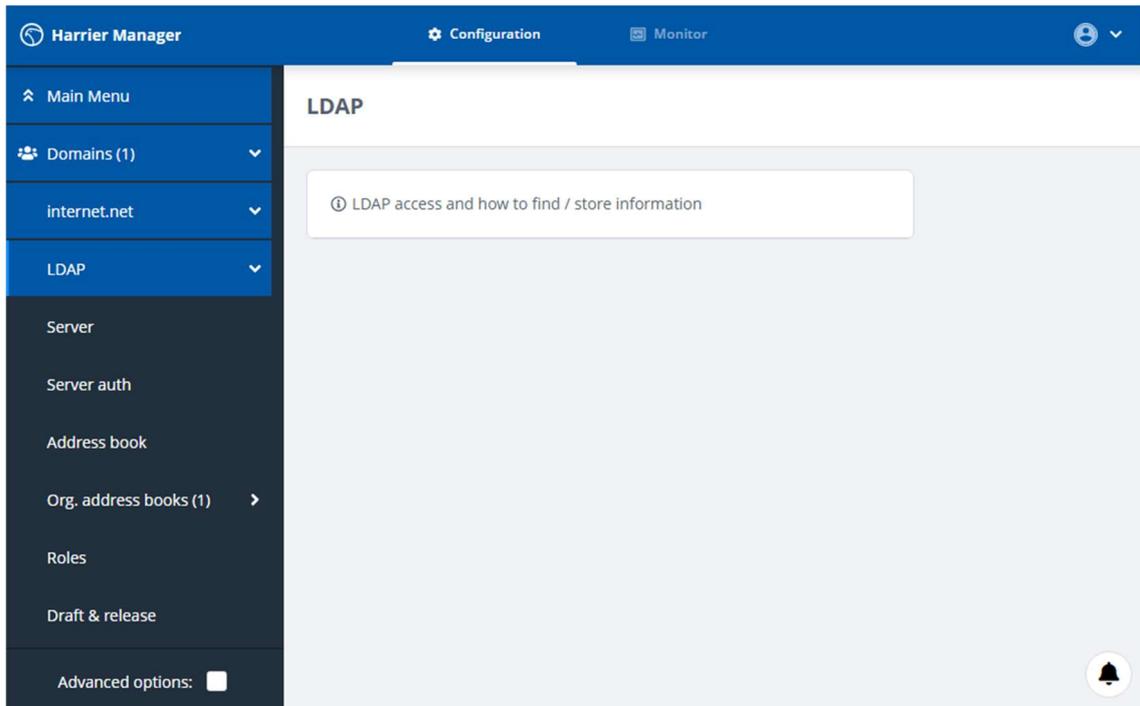
Enter “imap://127.0.0.1:143” for the “Primary URL”.

Harrier Domain Configuration – IMAP Server.



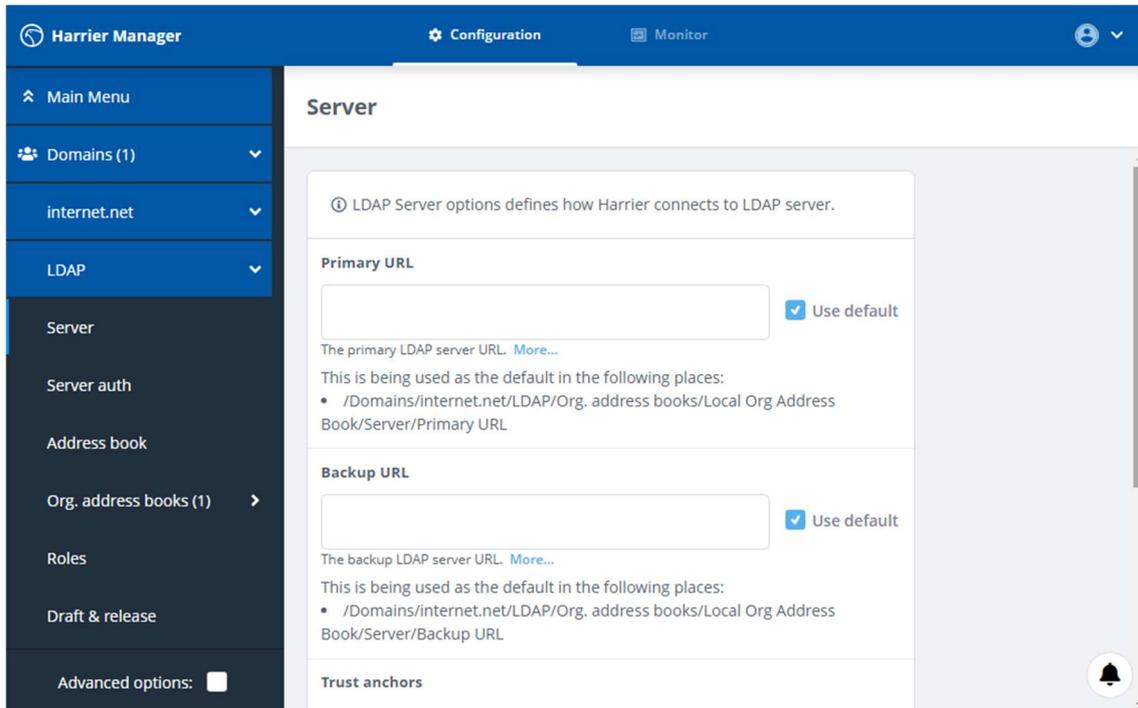
Scroll down, Click Submit and then from the left-hand menu select “LDAP”.

Harrier Domain Configuration – LDAP Server.



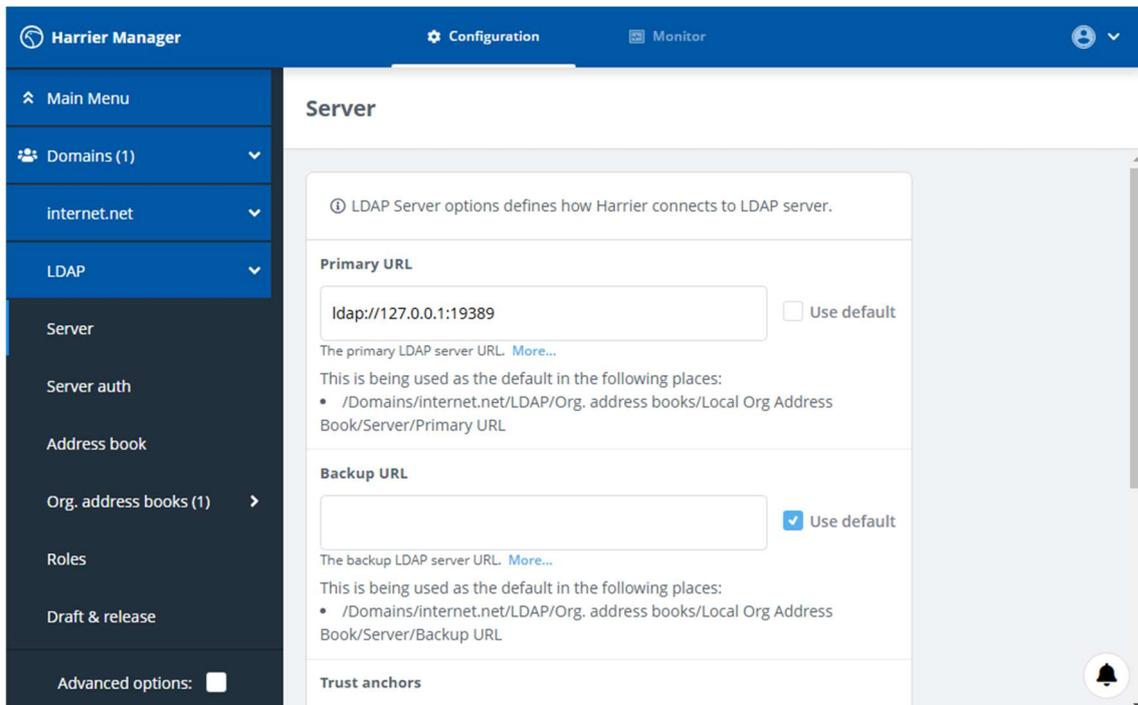
From the left-hand menu select “Server”.

## Harrier Domain Configuration – LDAP Server.



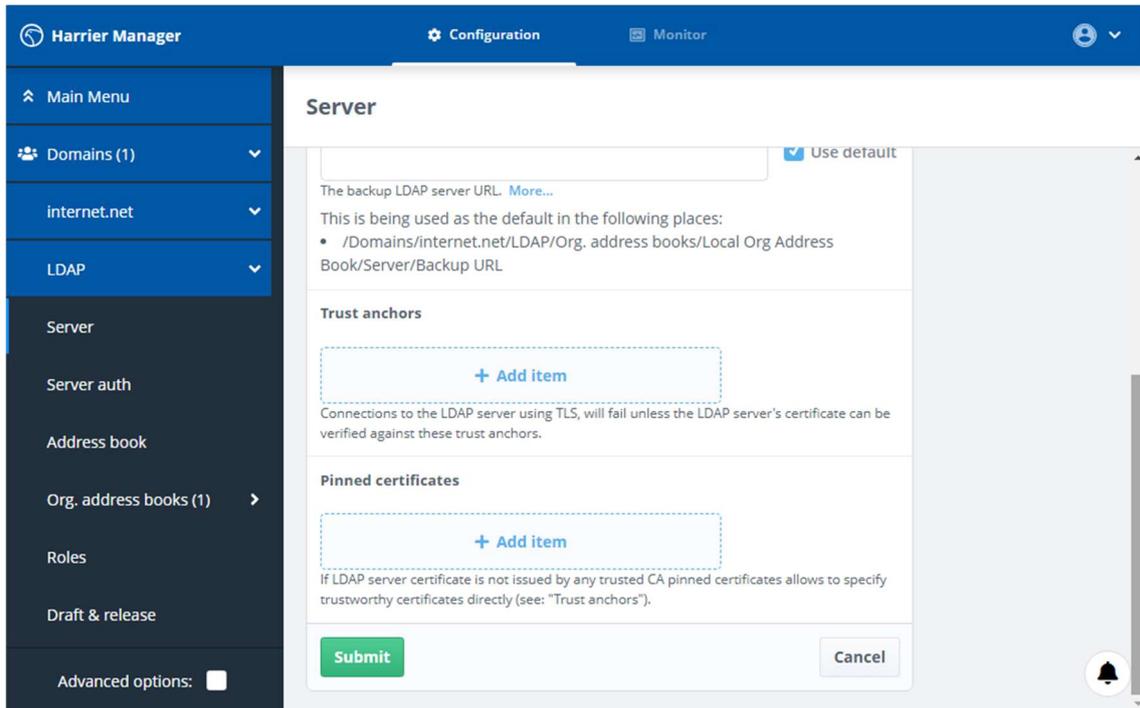
Enter “ldap://127.0.0.1:19389” for the “Primary URL”.

## Harrier Domain Configuration – LDAP Server.



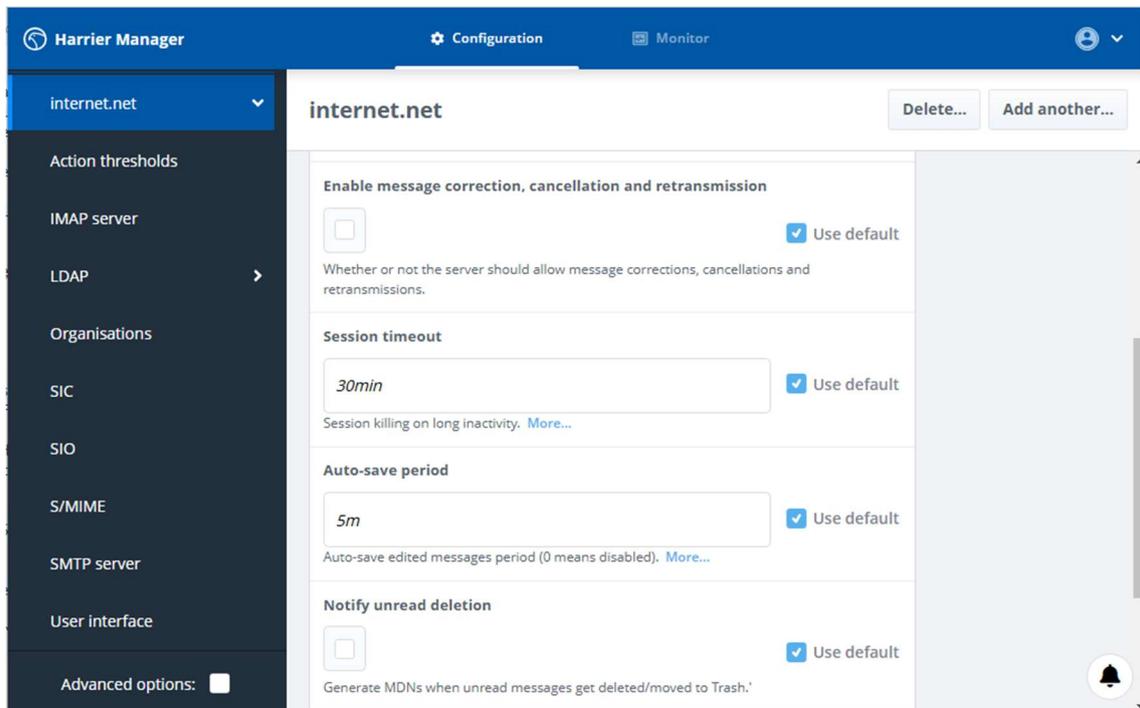
Scroll to the bottom.

Harrier Domain Configuration – LDAP Server.



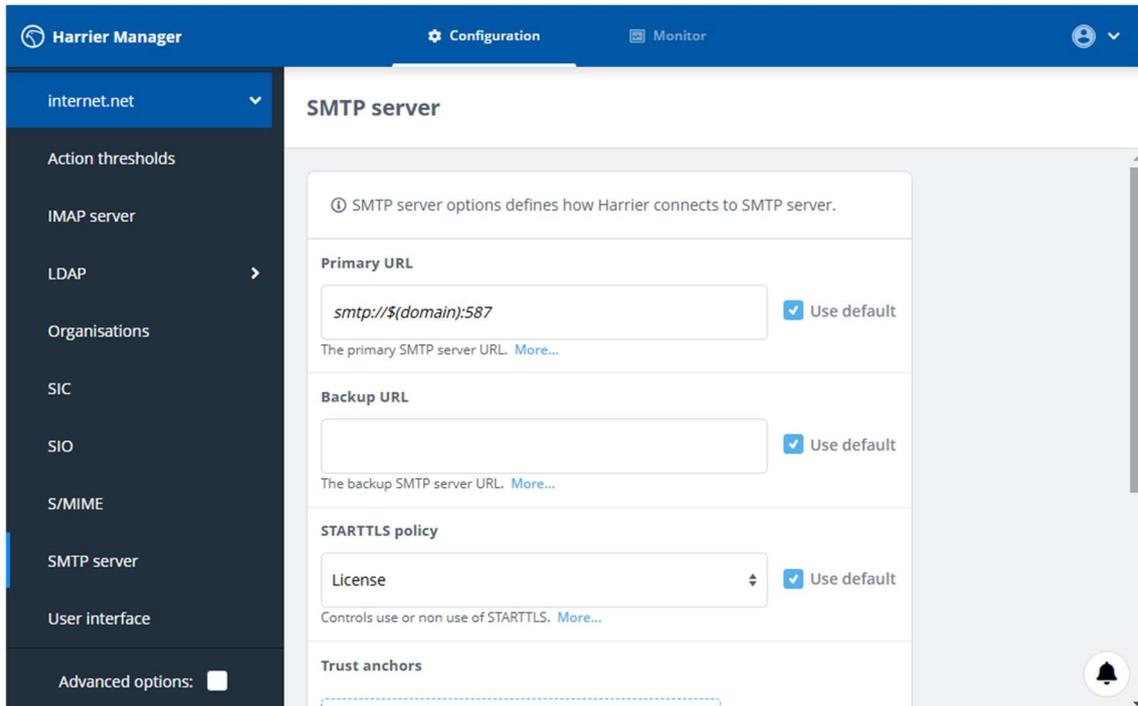
Click “Submit”. Return to the “internet.net” configuration level on the left-hand menu

Harrier Domain Configuration – SMTP Server.



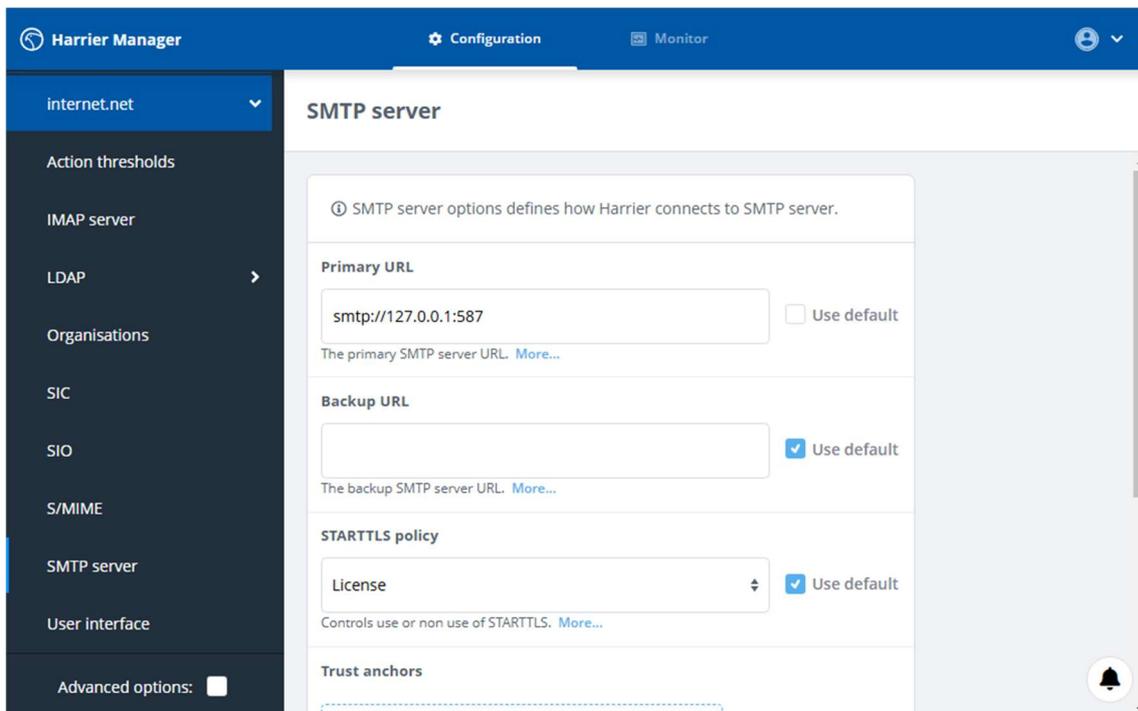
From the left-hand menu select “SMTP server”

## Harrier Domain Configuration – SMTP Server.



Enter “smtp://127.0.0.1:587” for the “Primary URL”.

## Harrier Domain Configuration – SMTP Server.



Scroll down to the bottom.

*Harrier Domain Configuration – SMTP Server.*

The screenshot shows the Harrier Manager configuration page for the SMTP server. The interface has a dark blue header with 'Harrier Manager', 'Configuration', and 'Monitor' tabs. A left sidebar contains a navigation menu with items: 'internet.net', 'Action thresholds', 'IMAP server', 'LDAP', 'Organisations', 'SIC', 'SIO', 'S/MIME', 'SMTP server', and 'User interface'. The 'SMTP server' item is selected. The main content area is titled 'SMTP server' and contains three sections: 'STARTTLS policy' with a 'License' dropdown and a checked 'Use default' checkbox; 'Trust anchors' with a '+ Add item' button and explanatory text; and 'Pinned certificates' with another '+ Add item' button and explanatory text. At the bottom of the form are 'Submit' and 'Cancel' buttons. An 'Advanced options' checkbox is visible at the bottom left of the sidebar.

Click “Submit”.

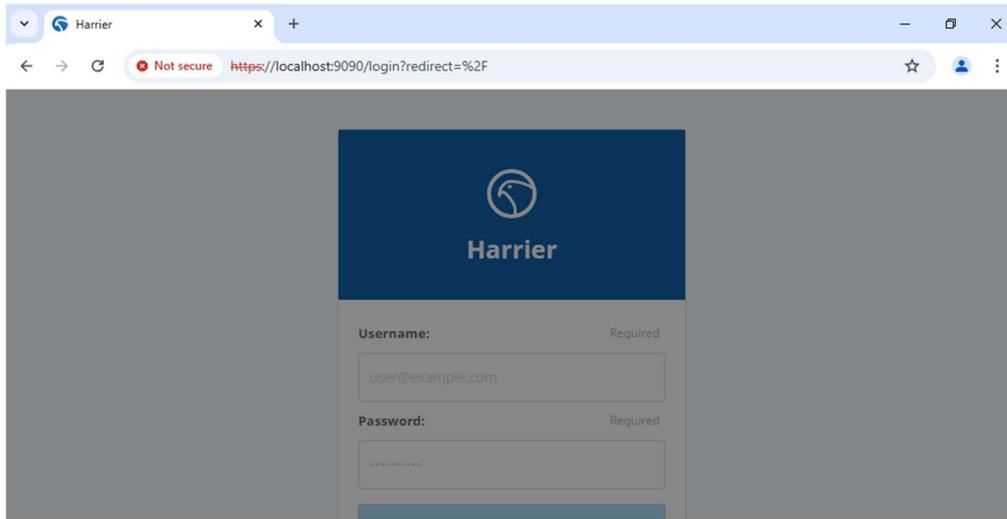
This completes the configuration of the Harrier Server. We are not ready to test the solution.

## Testing the Solution with Harrier

We will now login to Harrier as the User `user.one@internet.net` and send a message to `user.two@internet.net` .

Point your browser at `https://localhost:9090`

*Harrier login.*



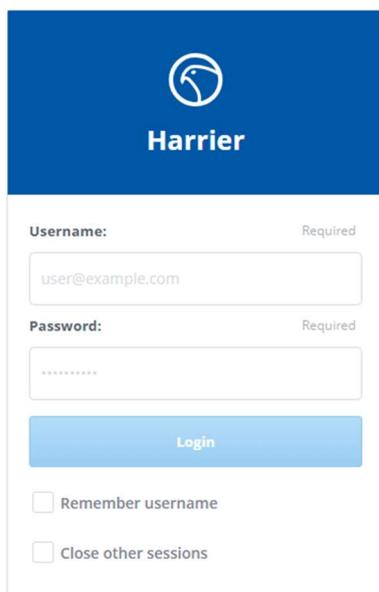
This application uses cookies

Harrier uses cookies to track session state. This does not include personal information.

Acknowledge

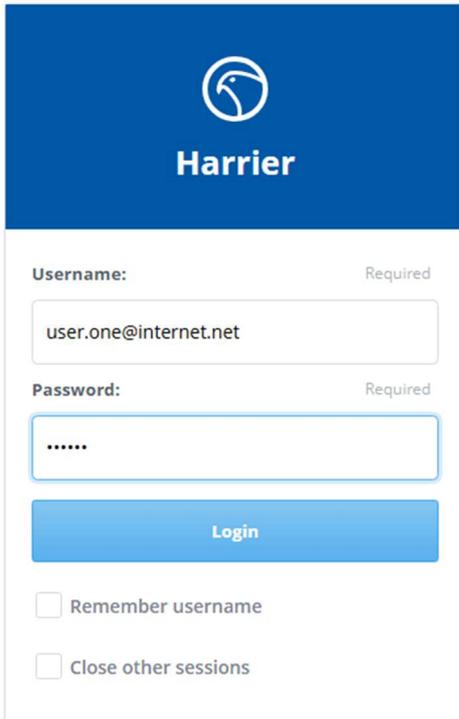
Click “Acknowledge”.

*Harrier login.*



Enter `user.one@internet.net` and the Password you set for this User.

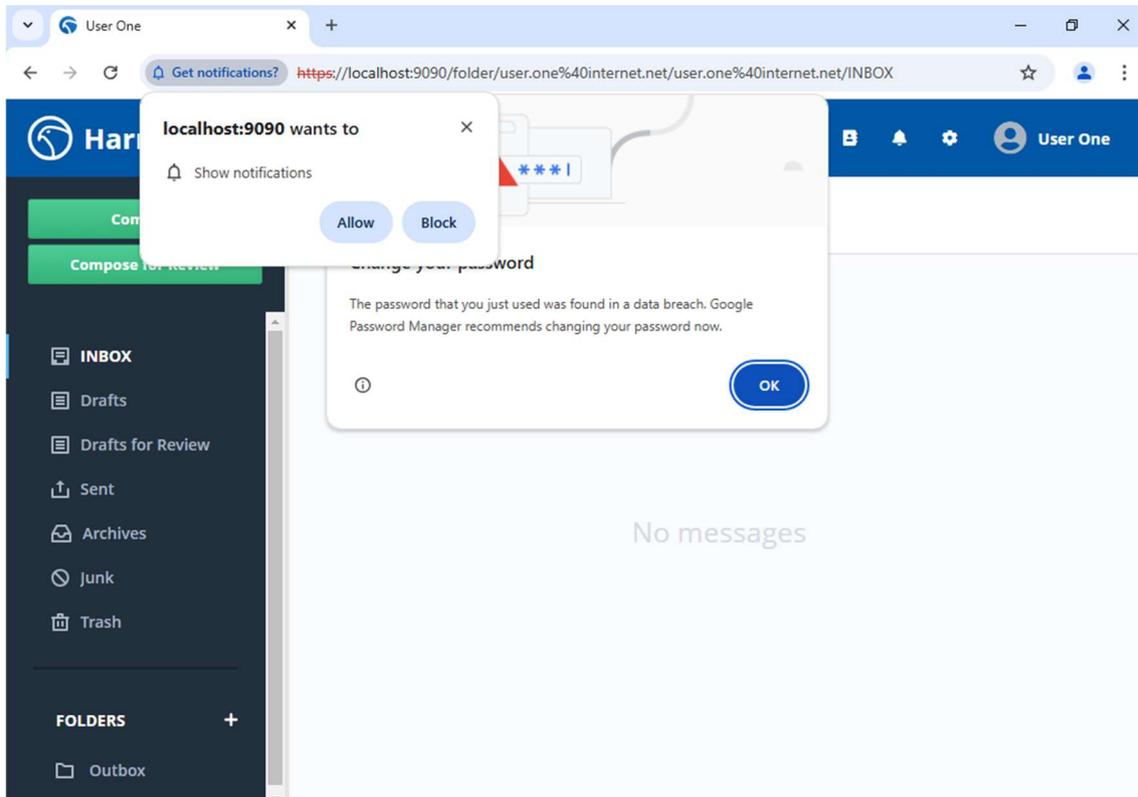
Harrier login.



The Harrier login form features a blue header with the Harrier logo and name. Below the header, there are two input fields: 'Username:' with the value 'user.one@internet.net' and 'Password:' with masked characters. A blue 'Login' button is positioned below the password field. At the bottom, there are two checkboxes: 'Remember username' and 'Close other sessions'.

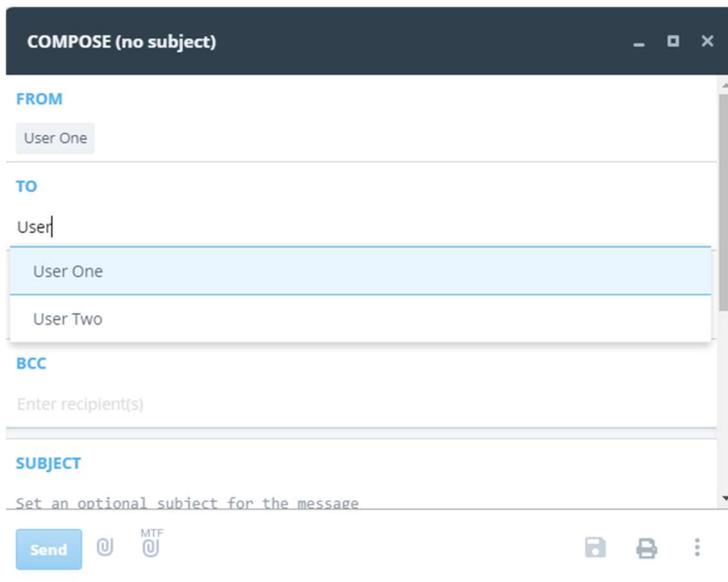
Click “Login”

Harrier Client Inbox.



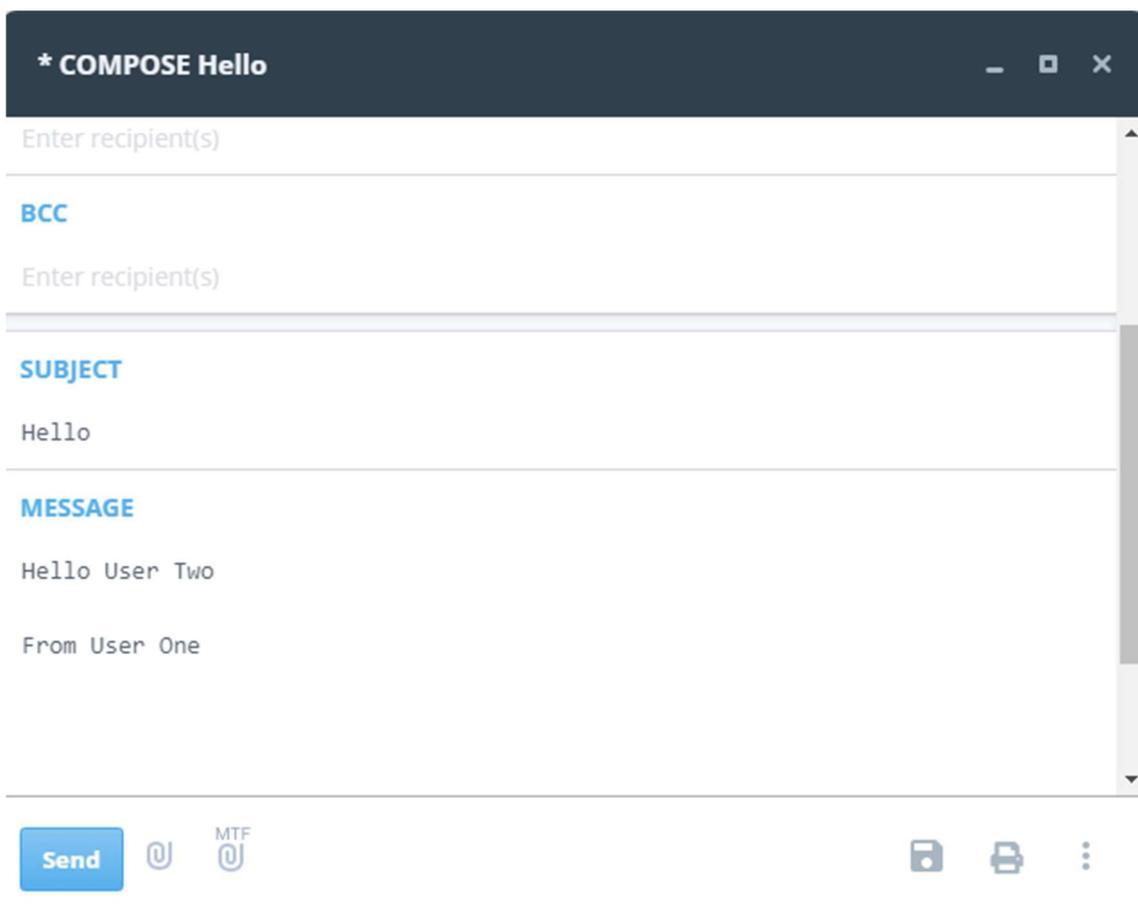
Click “Allow” for Notifications and “OK” for the weak password, then click “Compose”.

Harrier Client Compose.



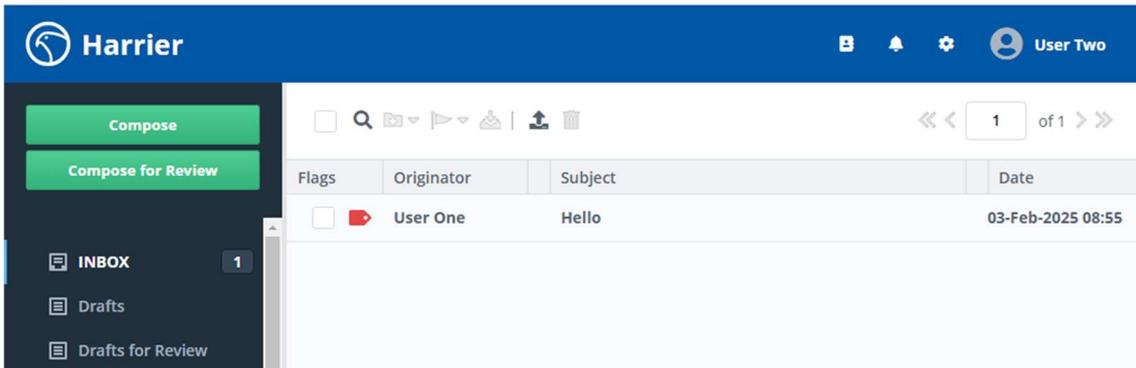
Start typing in the “To” field and Address Matches will appear, select the one you want to send to.

Harrier Client Compose.



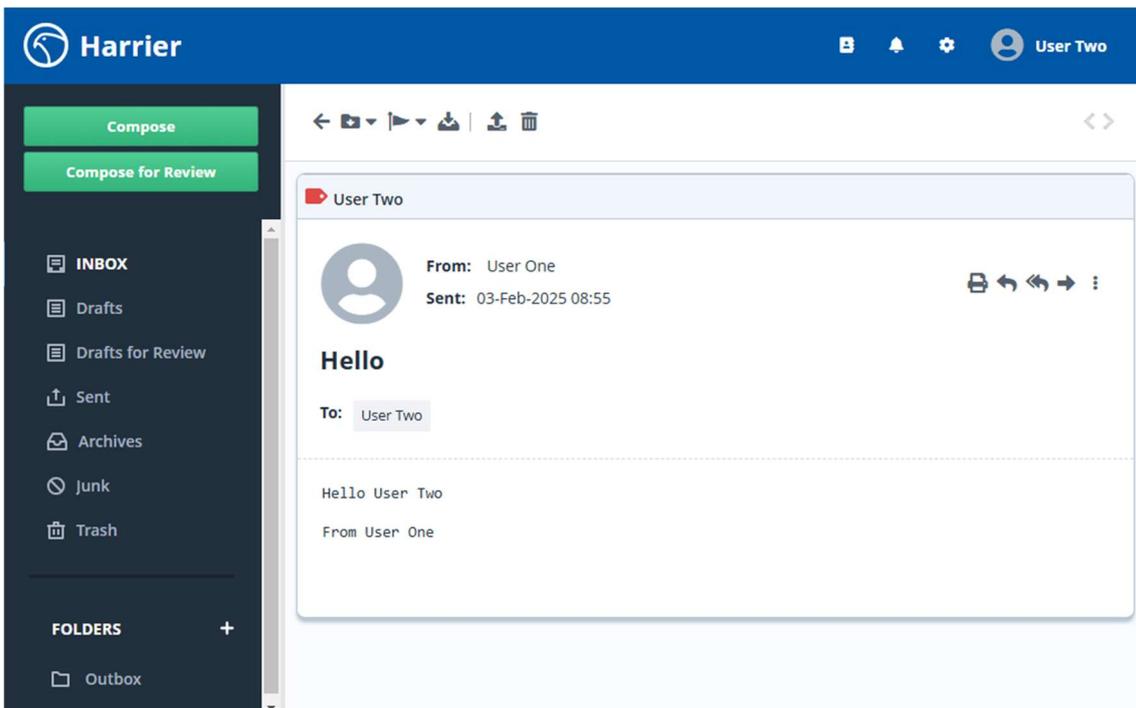
Complete the Subject and Message fields and Click “Send”. Then open a New Browser Tab and Login as User Two.

Harrier Client Inbox.



The message is received. Select the Message to display it.

Harrier Client Message Display.



Your SMTP server is now ready for use.

External SMTP Servers can be connected using DNS or Manually specified. In the next section we will configure an external SMTP Server Manually.

## Configuring an External SMTP Server

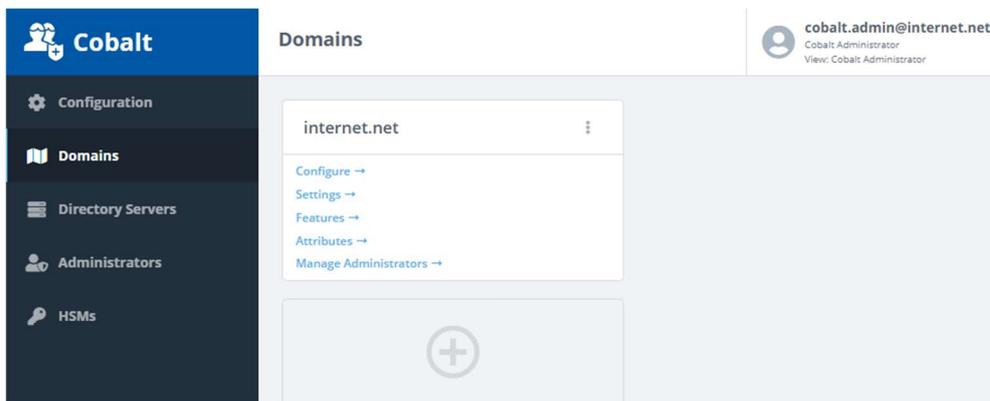
In this section we will manually configure an External SMTP Server. The External domain we will use is x400.net and will involve the following steps.

- Adding the x400.net domain and Users to Cobalt so that the Address book provides Harrier with the remote addresses.
- Configure the Routing Tree and External MTA in M-Console.

### Adding the External Domain in Cobalt

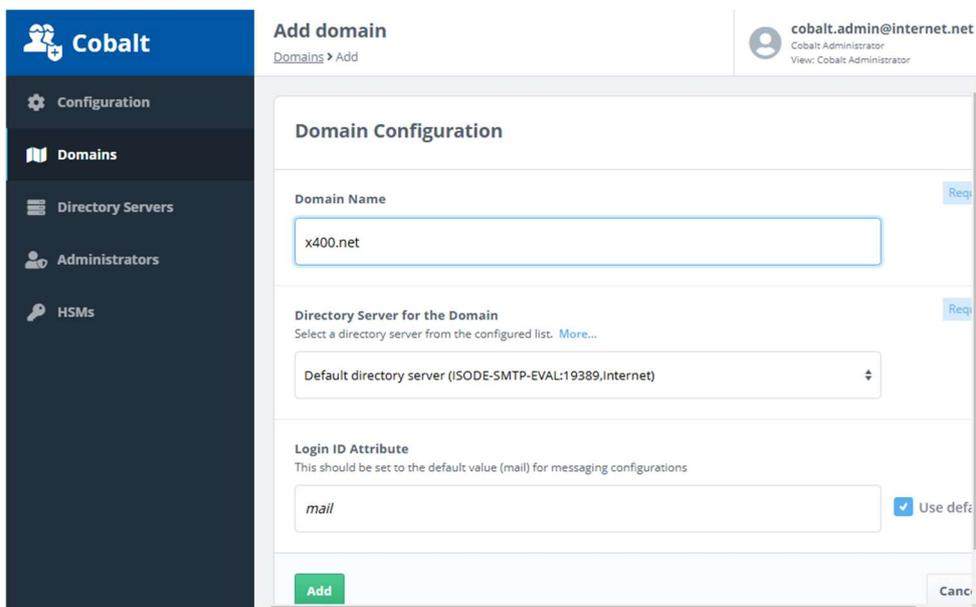
Login to Cobalt as the Cobalt Administrator

*Cobalt Administrator Login.*



Then from the “Domains” Menu Click “+”.

*Cobalt Domain Add.*



Enter the External Domain (x400.net) in this example. Click Add.

Cobalt Domain Add.

Click “Manage Administrators”.

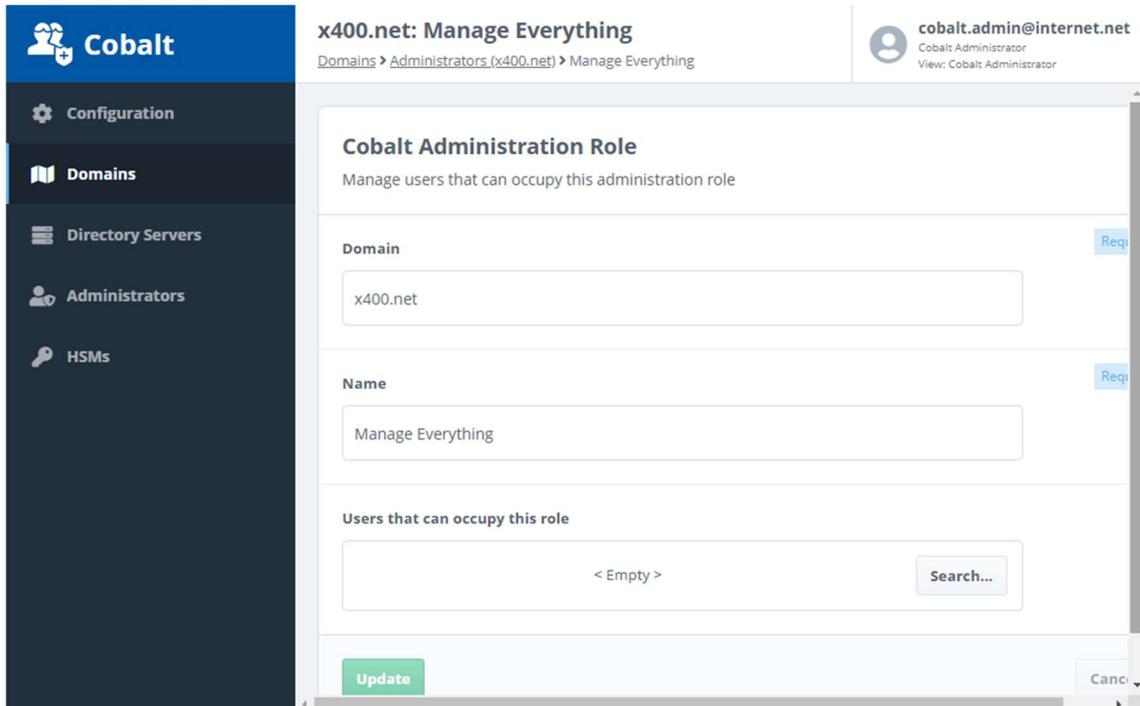
Cobalt Domain Add.

Name	Domain	Number of Occupants
Manage Everything	x400.net	0
Users and Roles Manager	x400.net	0
Users Manager	x400.net	0
Roles Manager	x400.net	0
OAuth Administrators	x400.net	0
Users and Roles Viewer	x400.net	0

6 managers

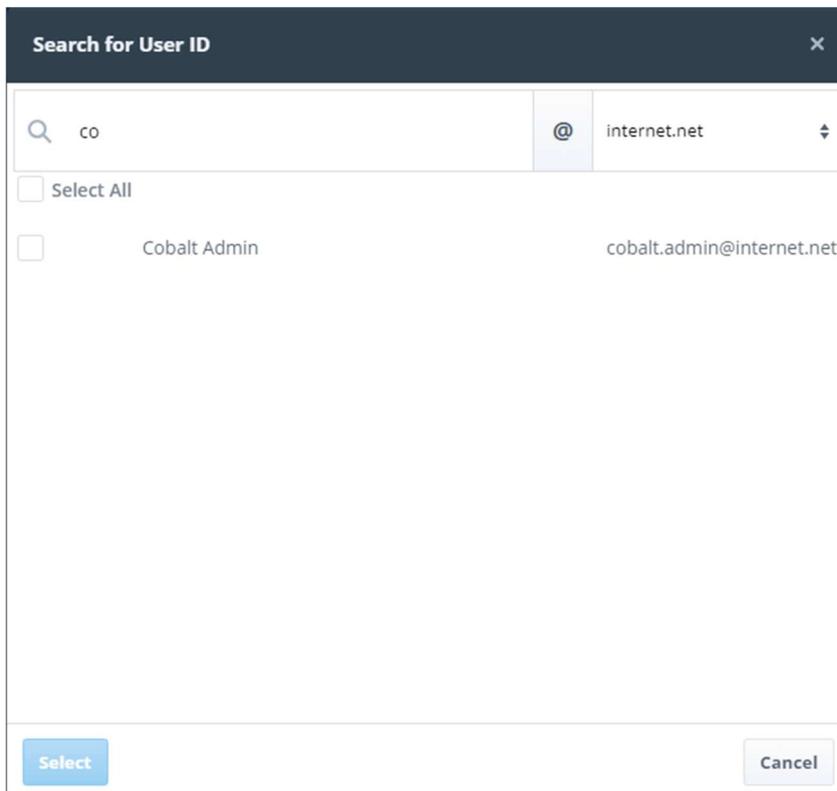
Select “Manage Everything”.

Cobalt Domain Add.



Click “Search”.

Cobalt Domain Add.



From the drop down menu on the top right select “internet.net” and start typing “co...” and the entry “Cobalt Admin” will display.

Cobalt Domain Add.

**Search for User ID**
✕

@

✓ Select All

✓ Cobalt Admin cobalt.admin@internet.net

Select
Cancel

Select it and the Click “Select”.

*Cobalt Domain Add.*

**Cobalt**

- ⚙️ Configuration
- 📖 Domains
- 📁 Directory Servers
- 👤 Administrators
- 🔑 HSMs

**x400.net: Manage Everything**

Domains > Administrators (x400.net) > Manage Everything

**cobalt.admin@internet.net**  
Cobalt Administrator  
View: Cobalt Administrator

**Cobalt Administration Role**

Manage users that can occupy this administration role

**Domain** Req

**Name** Req

**Users that can occupy this role**

Search...

Update
Cancel

Click “Update”.

Cobalt Domain Add.

Name	Domain	Number of Occupants
Manage Everything	x400.net	1
Users and Roles Manager	x400.net	0
Users Manager	x400.net	0
Roles Manager	x400.net	0
OAuth Administrators	x400.net	0
Users and Roles Viewer	x400.net	0

Click on the Username Box in the Top Right.

Cobalt External Domain Users Add.

**Account** ×

---

**Product Activation**

Customer Reference: Eval Guides update  
 Product: Cobalt  
 Version: 1.5v3-0  
 Versions up to: 1.6  
 Expiry date: 31-DEC-2026  
 Features: TLS

Update product features

Deactivate this product

---

[Switch View](#)

[Notifications](#)

---

[Logout](#)

[End All Sessions](#)

---

[Cobalt Administration Guide](#)

[Third Party Software](#)

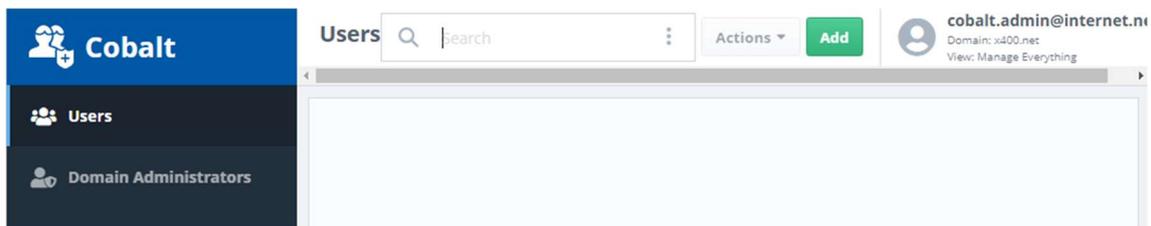
Select "Switch View".

Cobalt External Domain Users Add.



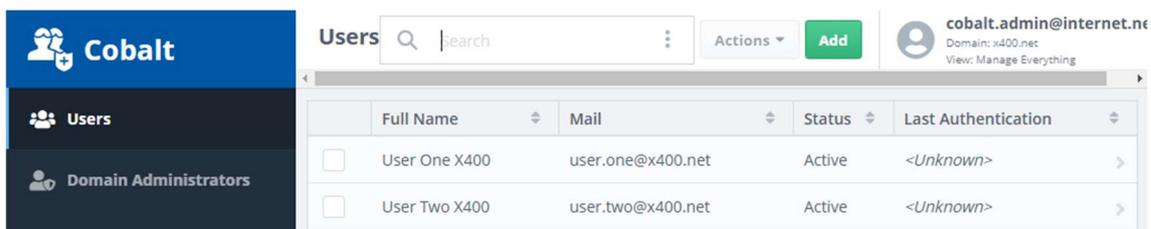
Select “x400.net: Manage Everything”. Click “Continue”.

Cobalt External Domain Users Add.



Now Add the Users “User One X.400” and “User Two X.400” in the same way as you added the Users for “internet.net” making sure their email addresses are “user.one@x400.net” and “user.two.@x400.net”.

Cobalt External Domain Users Add.

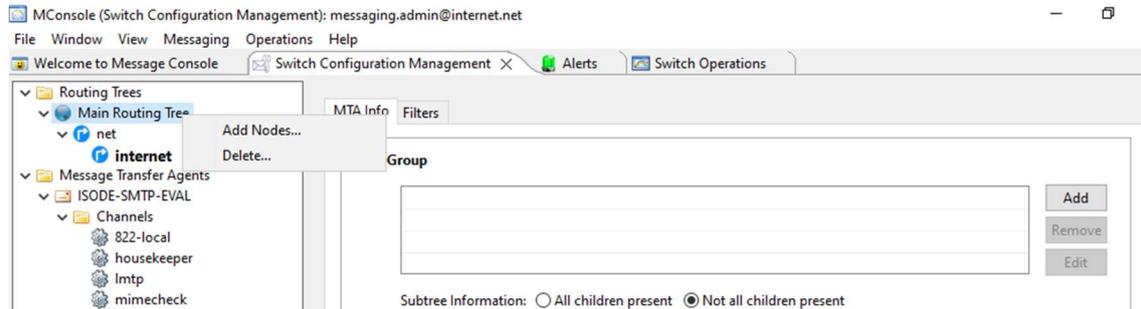


You have now added the External Users and can now go to M-Console to Configure the Routing and External MTA.

## Adding and Configuring the External Domain in M-Console

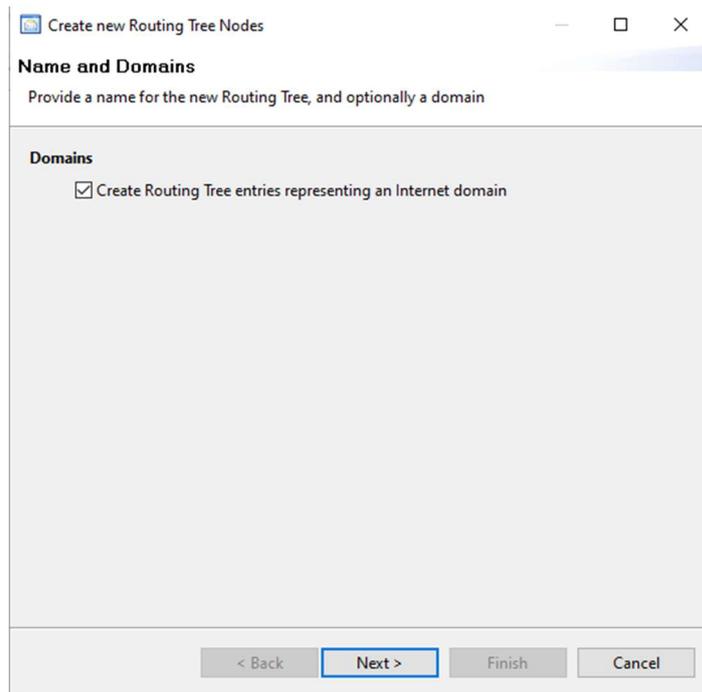
From M-Console Switch Configuration Management.

*M-Console Configure Routing Tree Entry.*



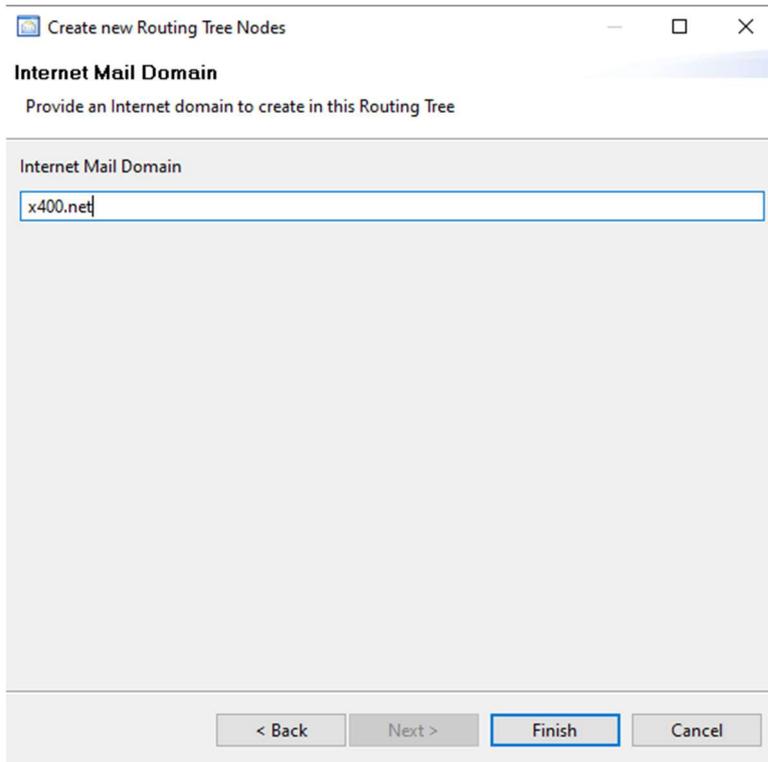
Right Click on the “Main Routing Tree”, Click “Add Nodes...”

*M-Console Configure Routing Tree Entry.*



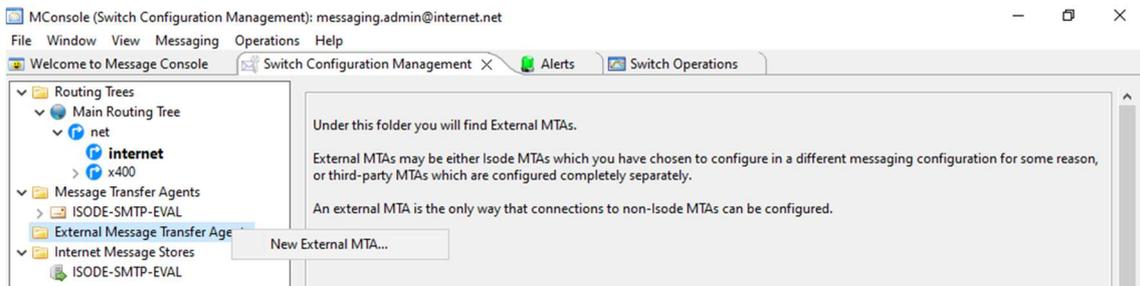
Click “Next>”.

*M-Console Configure Routing Tree Entry.*



Enter “x400.net”, Click “Finish”.

*M-Console Configure External MTA.*



Eight Click on “External Message Transfer Agents”, Click “New External MTA...”.

*M-Console Configure External MTA.*

The screenshot shows a window titled "Create a new MTA" with standard window controls. Below the title bar, the text "MTA type" is followed by the instruction "Select the type of MTA you want to create". A section titled "External MTA (Non Isode MTA, or non tailoring MTA)" contains three radio button options: "SMTP" (which is selected), "CFTP", and "SLEP". At the bottom of the window, there are four buttons: "< Back", "Next >" (highlighted in blue), "Finish", and "Cancel".

Select "SMTP", Click "Next>".

*M-Console Configure External MTA.*

The screenshot shows the "Create a new MTA" window at the "MTA Naming" step. The title bar and window controls are the same. Below the title bar, the text "MTA Naming" is followed by the instruction "An External Internet MTA can be given an arbitrary name in your Messaging Configuration". A section titled "The local name for the external MTA in this configuration" contains a text input field labeled "Directory Name". Below this, a paragraph explains: "The mail domain or host name to which messages queued to this MTA will be transferred. It is also possible to specify an IP address, but that will require the use of an SMTP channel which has the 'nomx' flag set to communicate with this MTA". This is followed by a text input field labeled "Destination". Below that, a section titled "Optional local description for the new MTA" contains a text input field labeled "Description". At the bottom, there are four buttons: "< Back", "Next >" (highlighted in blue), "Finish", and "Cancel".

Enter a friendly name for the "Directory Name" and the hostname or IP Address of where that MTA is.

## M-Console Configure External MTA.

**MTA Naming**

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

The local name for the external MTA in this configuration

Directory Name

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

Destination

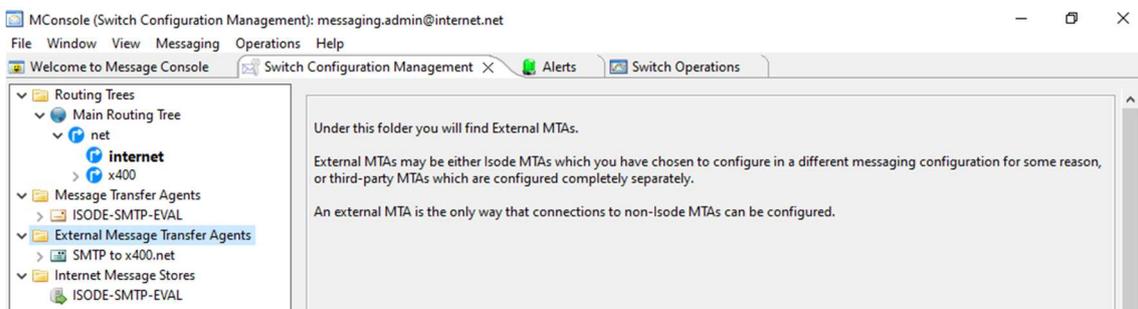
Optional local description for the new MTA

Description

< Back   Next >   **Finish**   Cancel

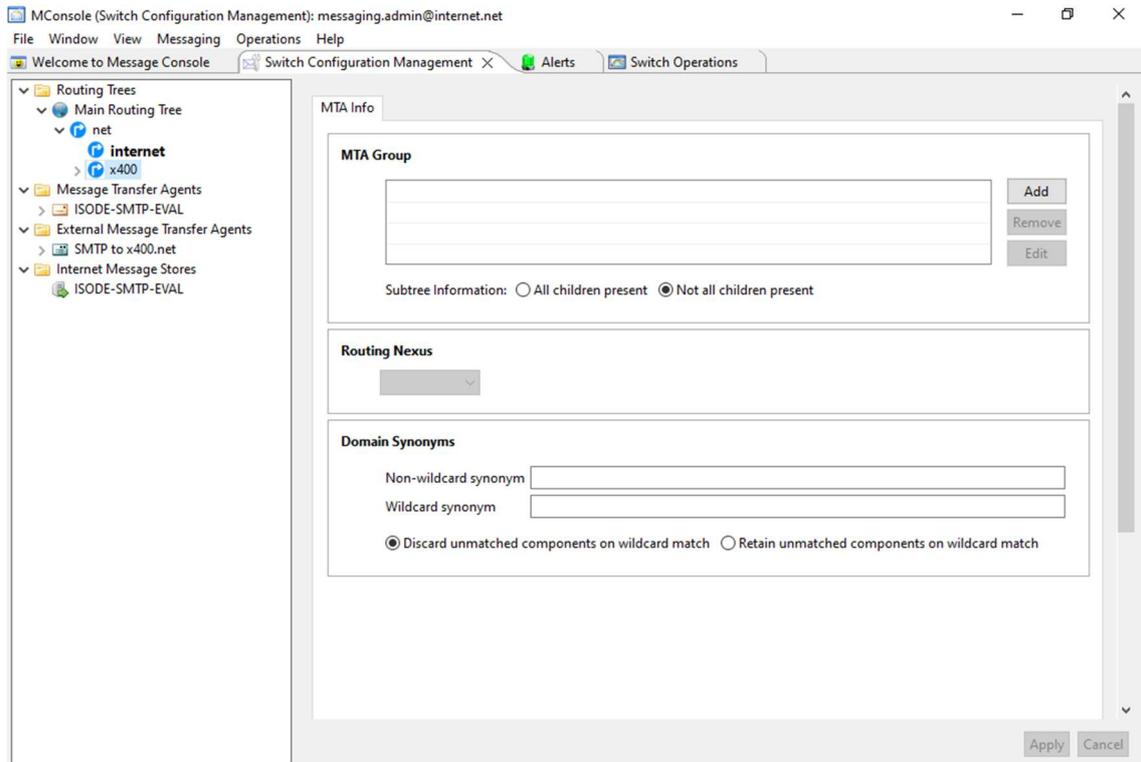
Click "Finish".

## M-Console Configure External MTA.



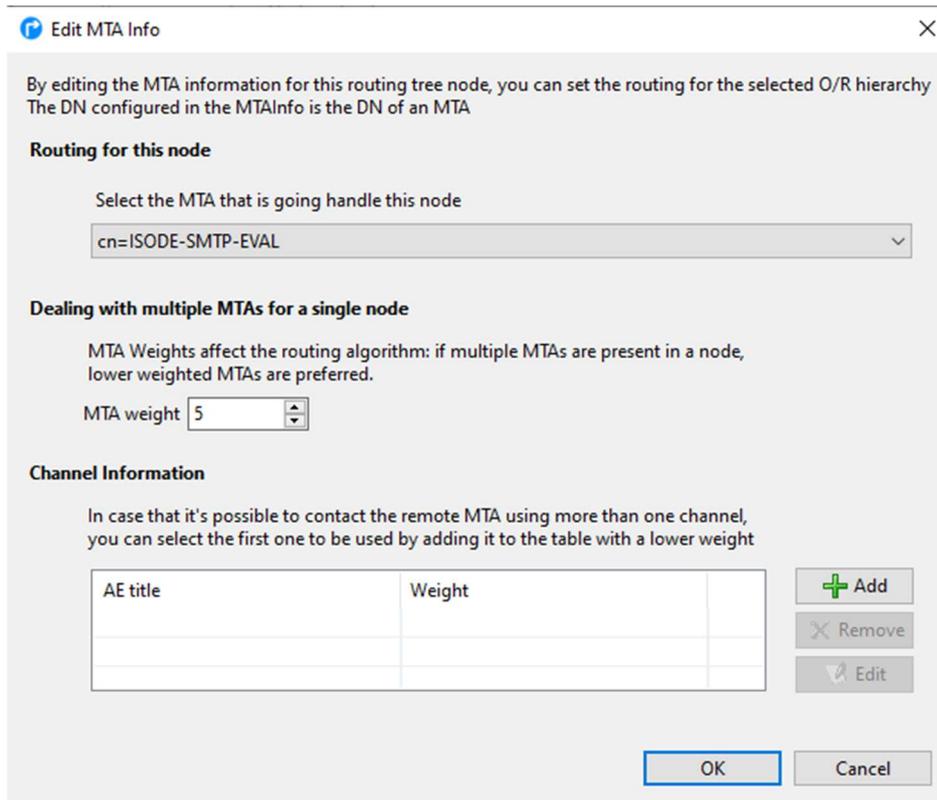
Select the "x400" entry on the "Main Routing Tree".

M-Console Configure External MTA.



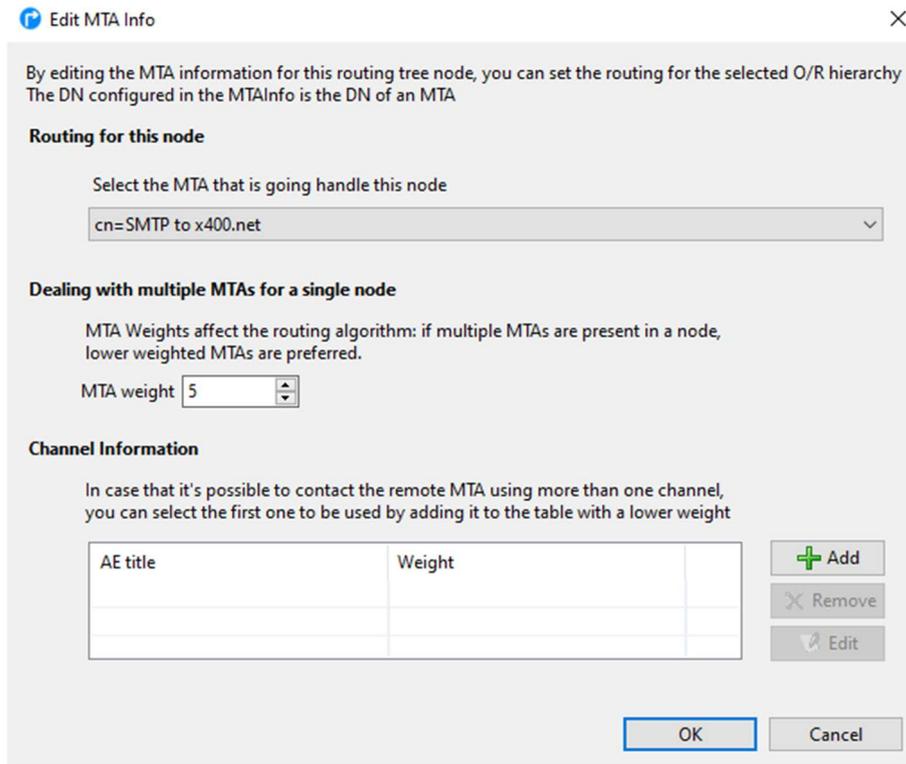
Click "Add".

M-Console Configure External MTA.



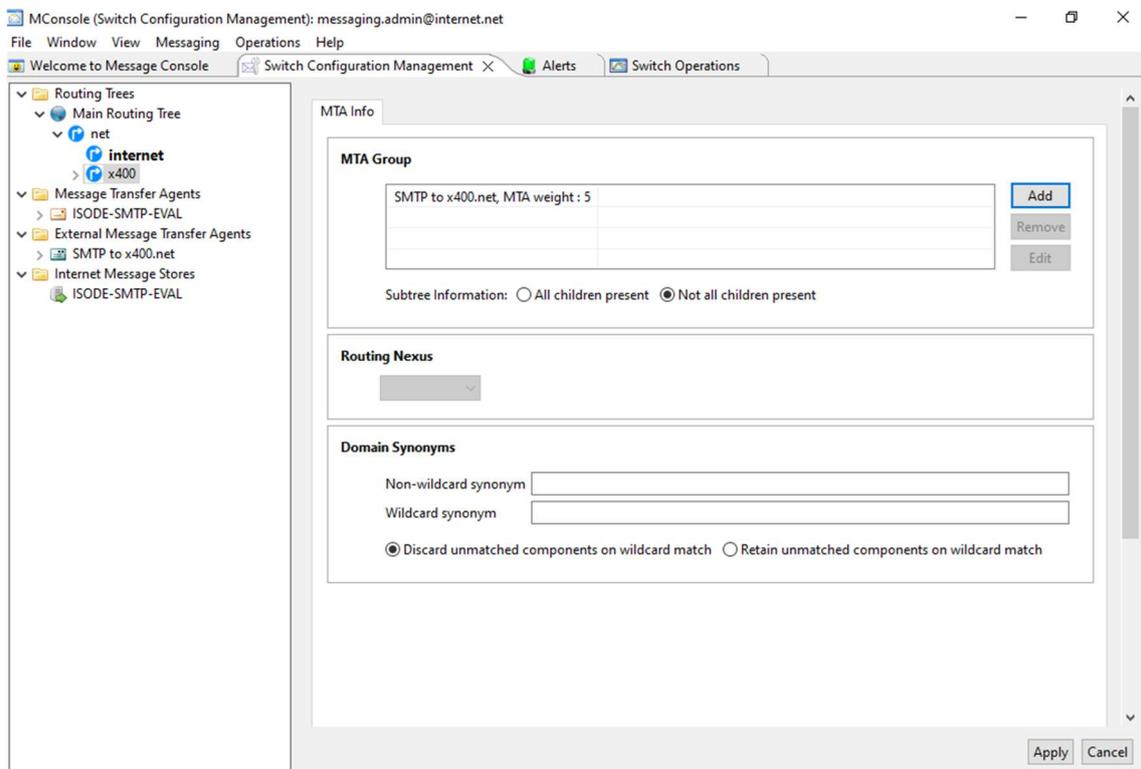
Change the "Routing for this node" to your newly created External MTA from the Drop Down.

M-Console Configure External MTA.



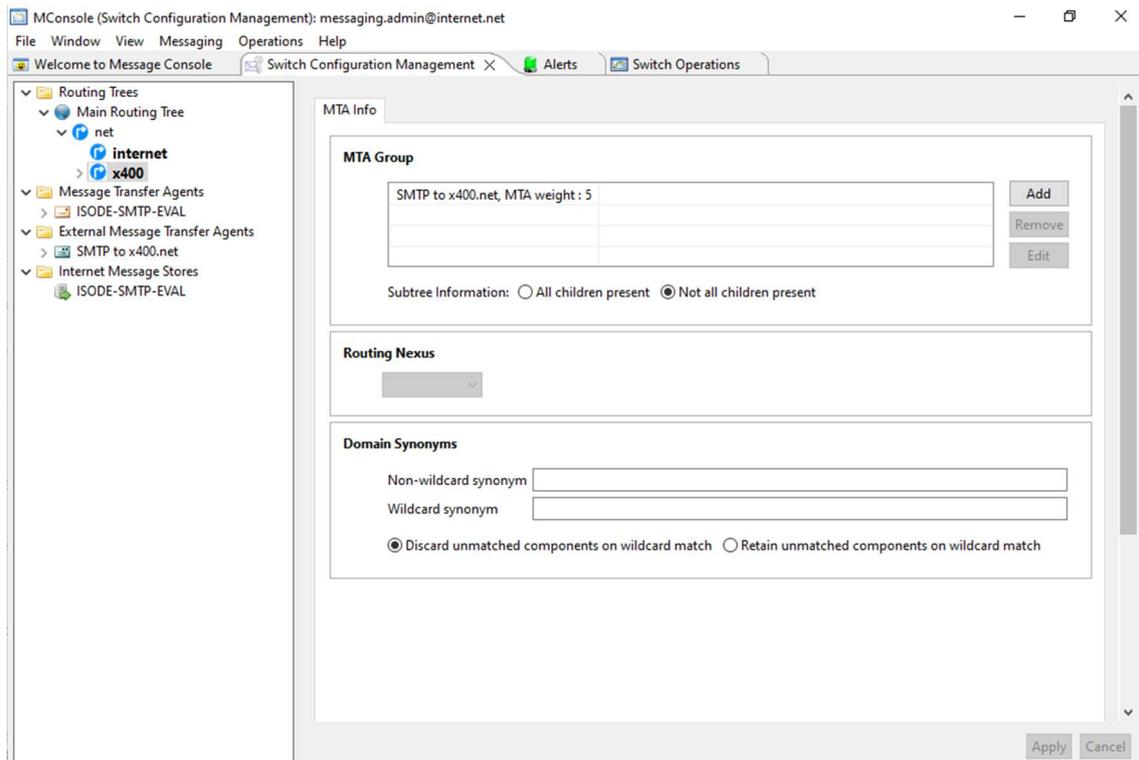
Click "OK".

M-Console Configure External MTA.



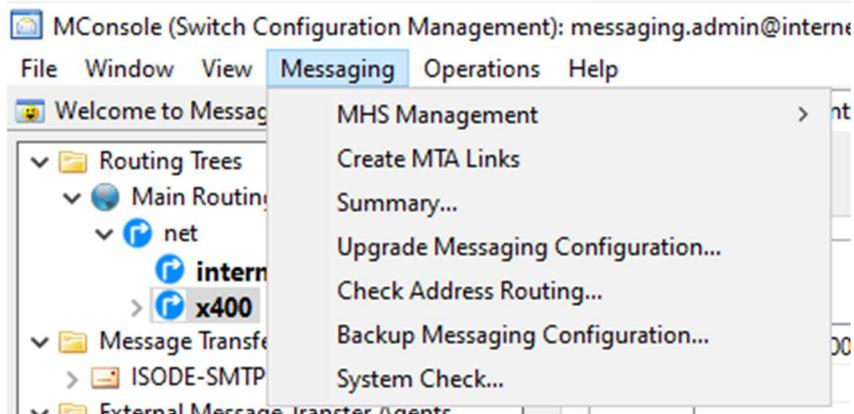
Click "Apply".

## M-Console Configure External MTA.



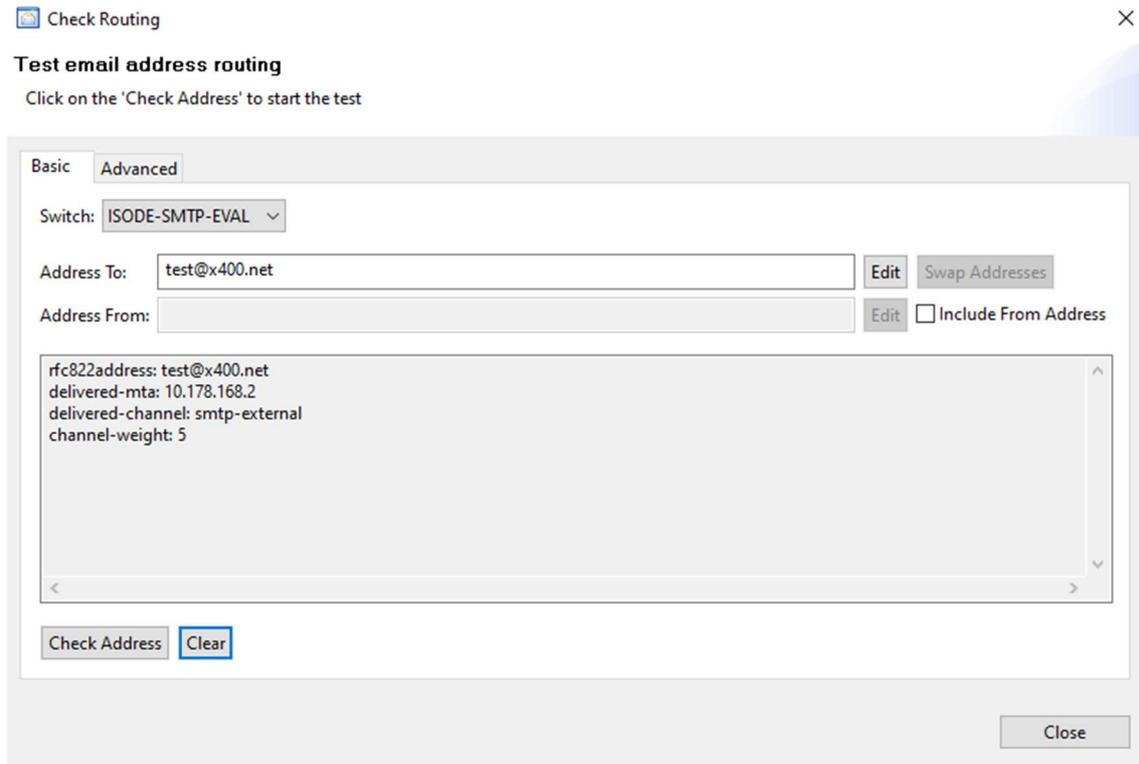
Now we need to check the Routing is working. From the very top Menu Right Click on “Messaging”.

## M-Console Check Routing.



Select Check Address Routing.

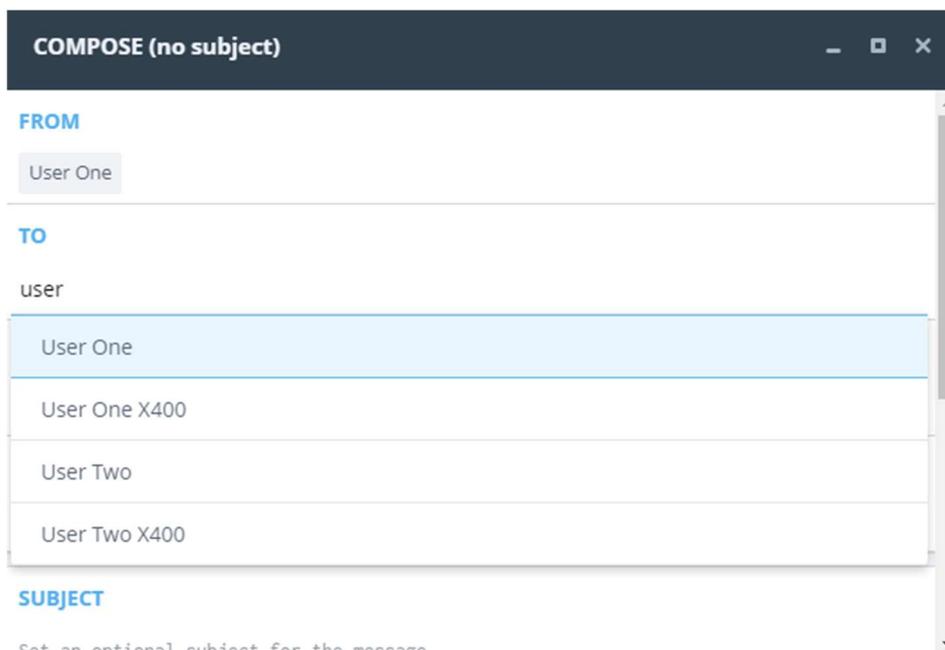
## M-Console Check Routing.



Enter “test@x400.net for the “Address To:” and Click “Check Address”. You should see something like the above.

In Harrier you should see the new Address appear when entering the “To:” Address.

## Harrier New Addresses.



This completes this guide.

## What Next?

More information on Icon-5066 can be found on the Isode website at <https://www.isode.com/product/stanag-5066-server/>.

## Whitepapers

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

## Copyright

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

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

Isode software is © copyright Isode Limited 2002-2025, All rights reserved.

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

This manual is © copyright Isode Limited 2025.