Isode

M-Switch SMTP Evaluation Guide

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

Contents

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

www.isode.com/product/pop-imap-message-store/

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

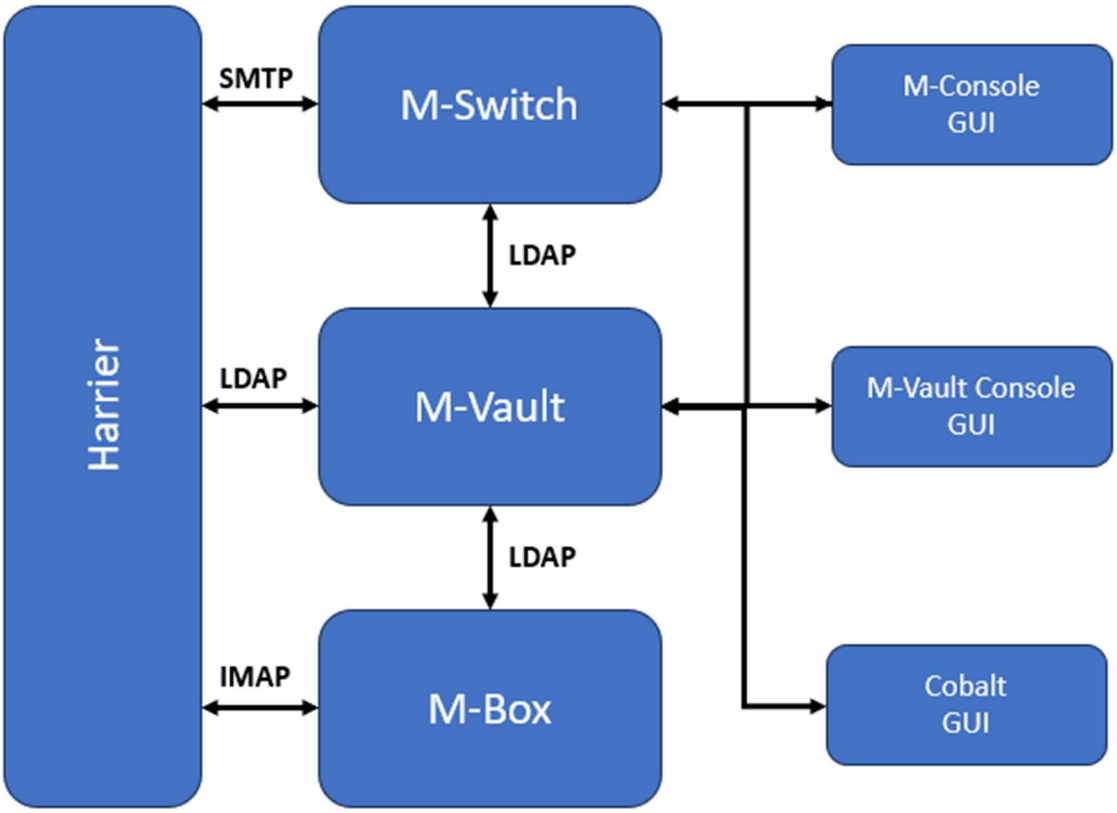
www.isode.com/product/user-role-provisioning/

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



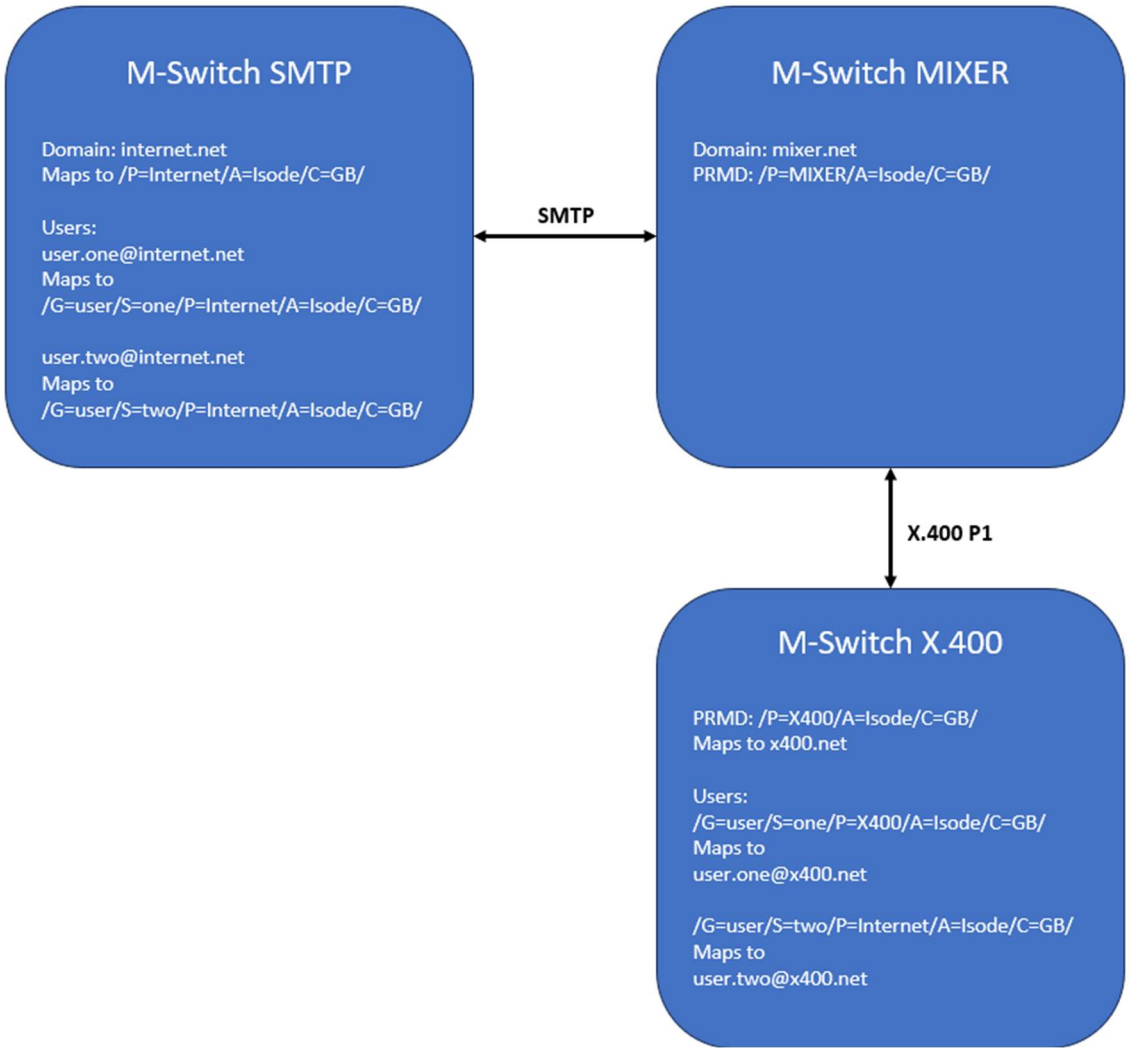
By the end of this guide you will have:

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. Configued 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*. 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 19.0v21
M-Vault 19.0v21
M-Box 19.0v21
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.

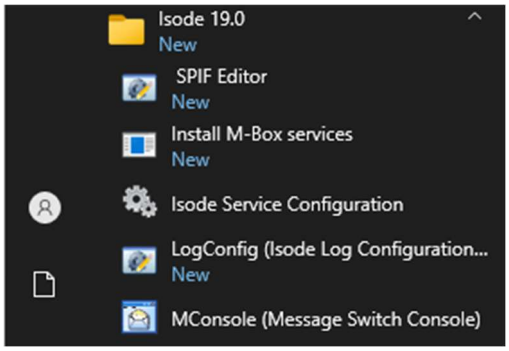
Creating the Messaging Configuration

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

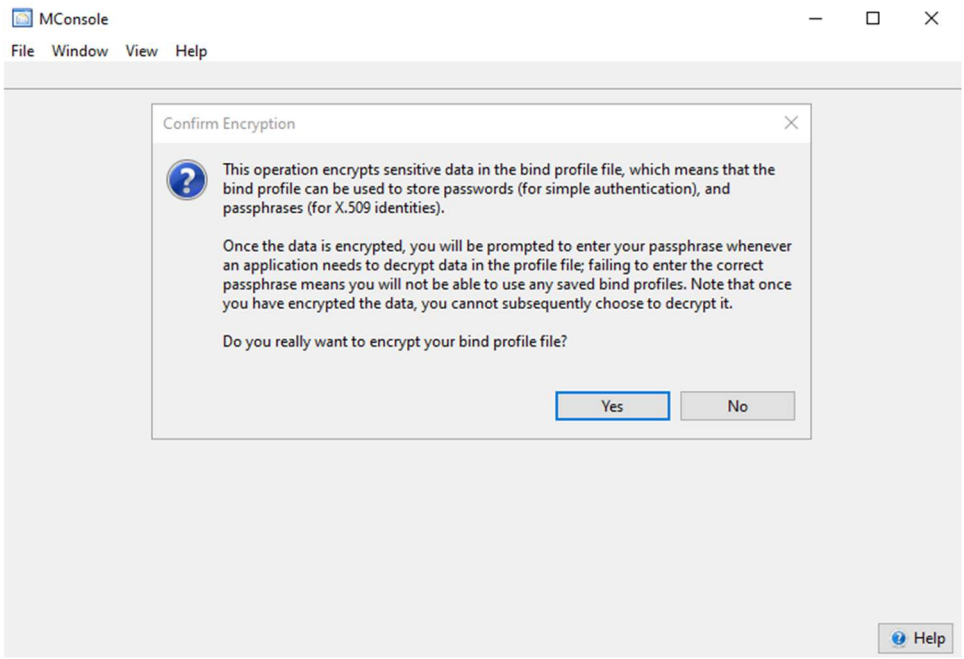


On Linux type the command:

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

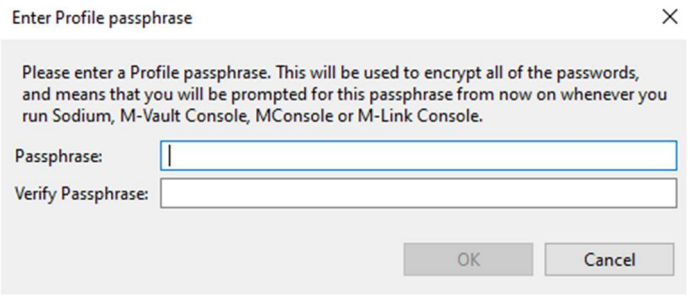
You will see the following prompt.

Encrypt the Bind Profile



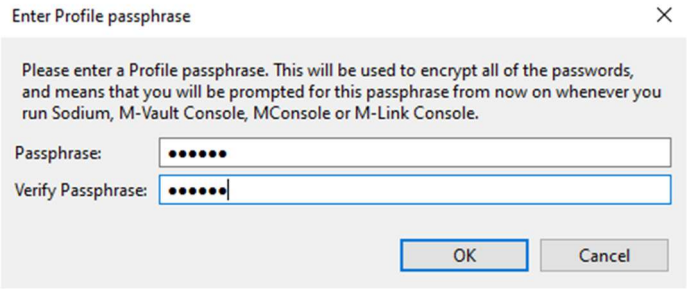
Click “Yes”

Enter Bind Profile Passphrase



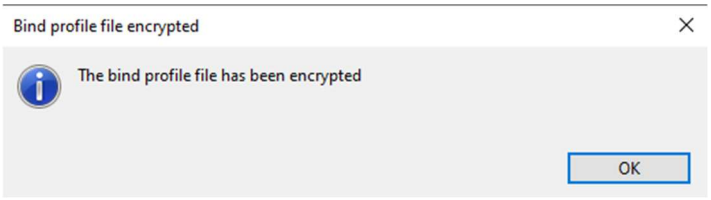
Enter your chosen passphrase, for evaluations we suggest "secret" so that if you need Isode Support we do not have to fix forgotten passwords etc.

Bind Profile Passphrase Entered



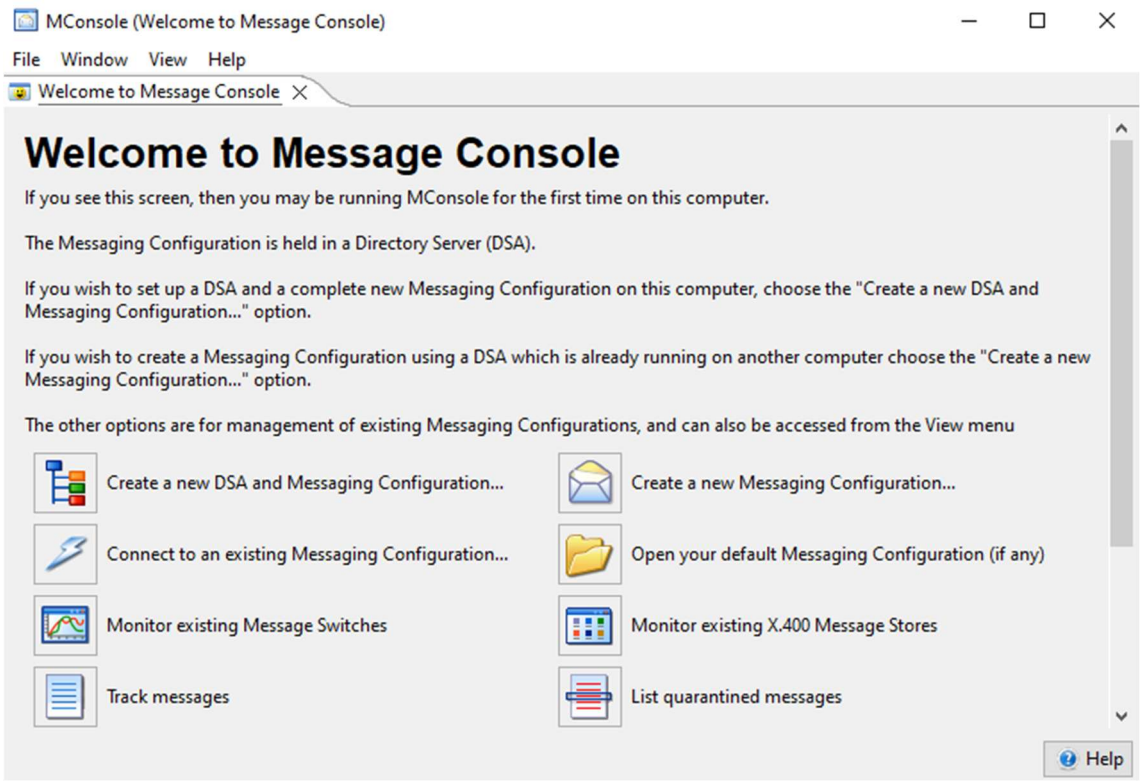
Click "OK"

Bind Profile Encrypted



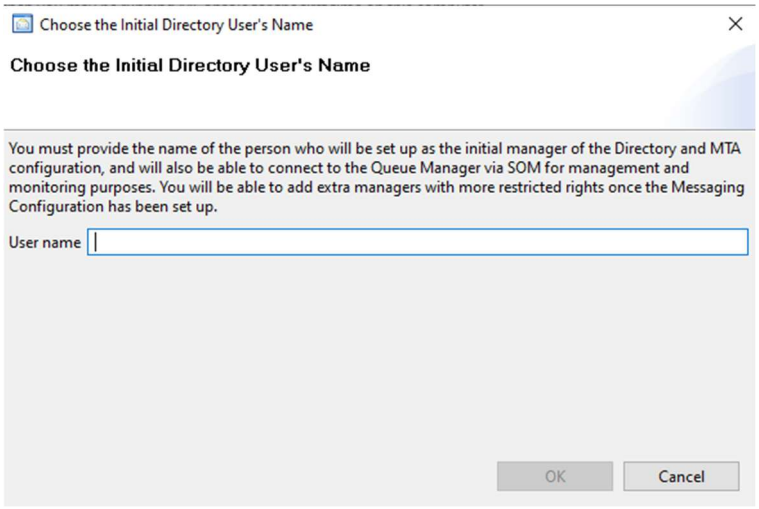
Click "OK"

M-Console Welcome Screen



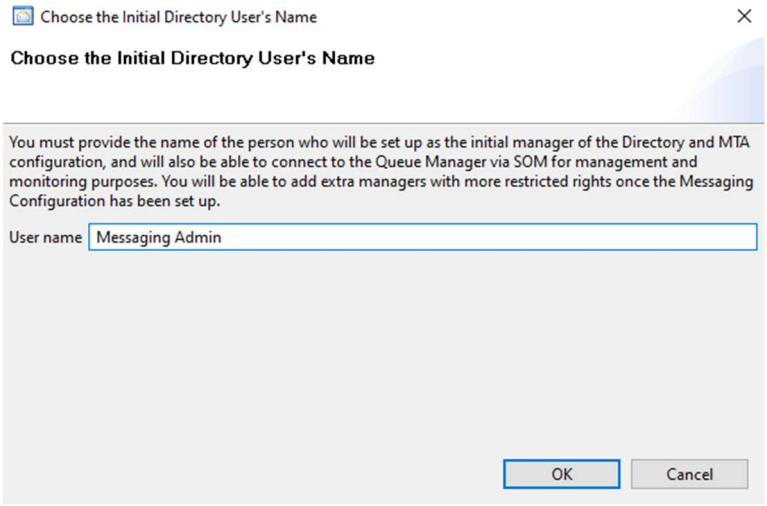
Select “Create a new DSA and Messaging Configuration.

Enter a User Name



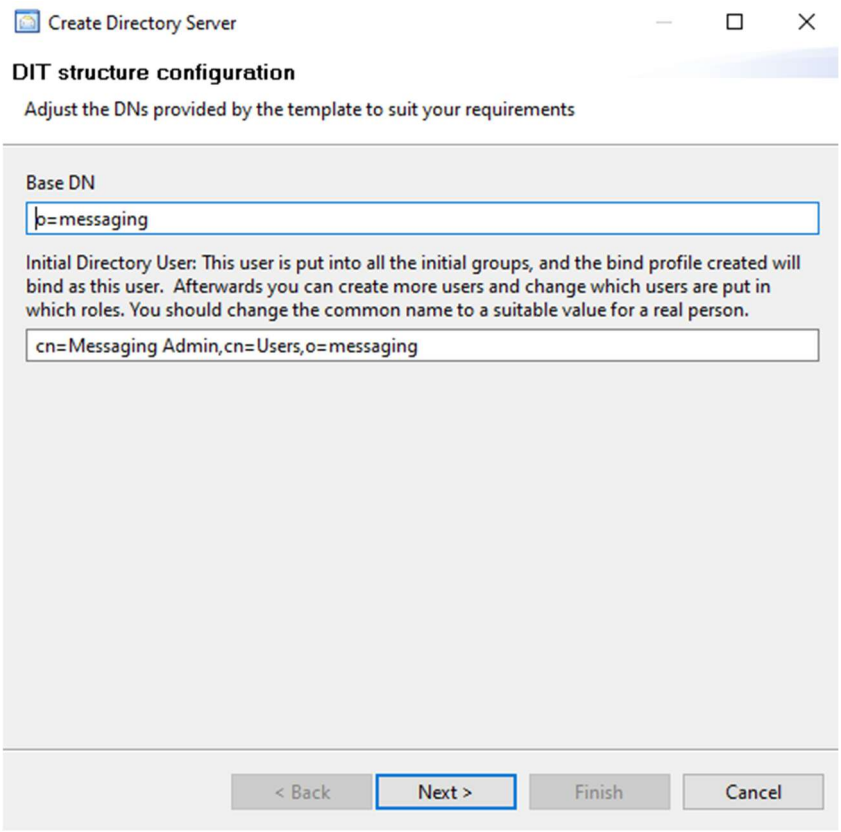
Typically, we use “Messaging Admin” here, but you can choose your own if you wish.

User Name Entered



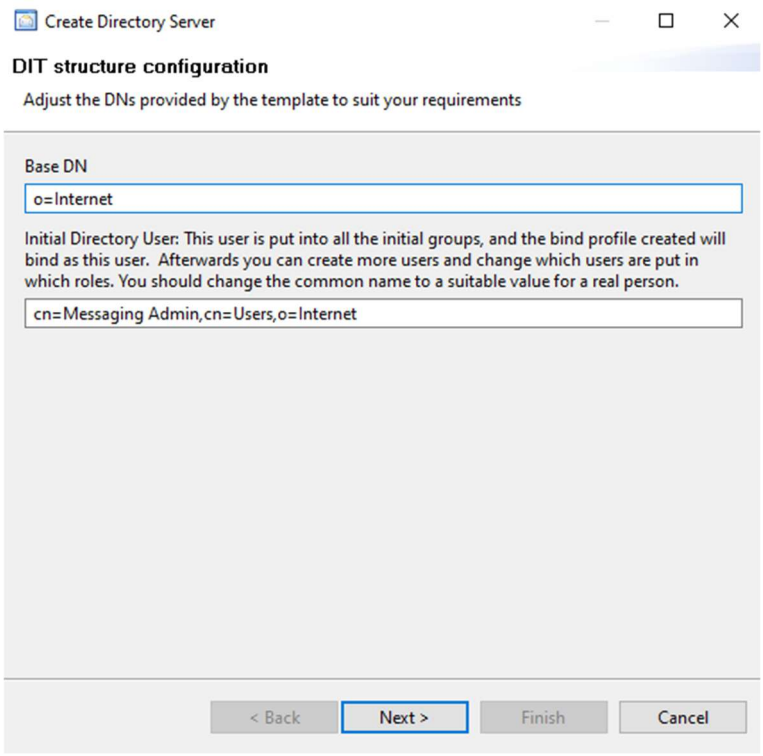
Enter your User Name and Click "OK".

Enter Base DN



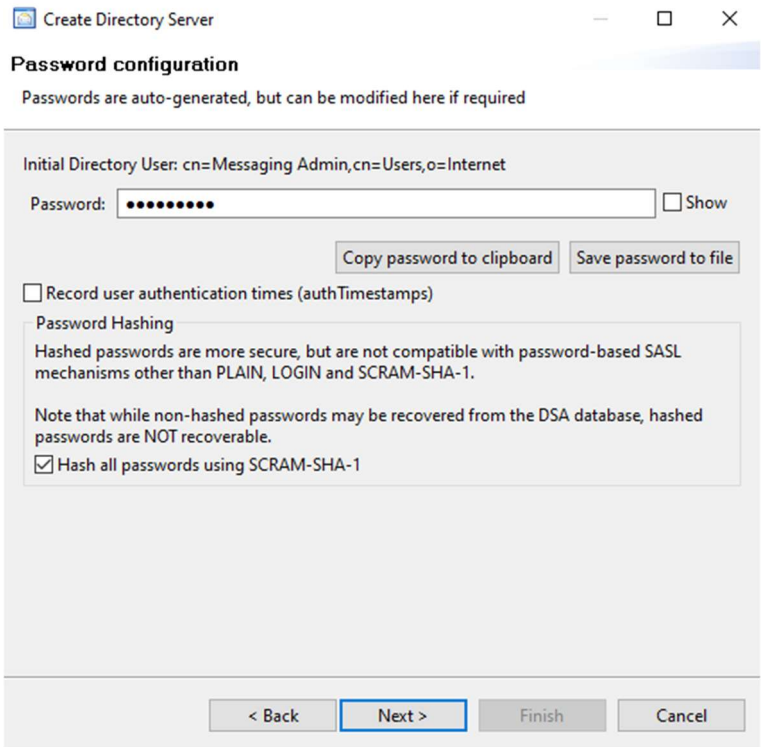
Enter the Base "Distinguished Name" (DN) for your directory server. You can use the default or choose one of your own.

Base DN entered



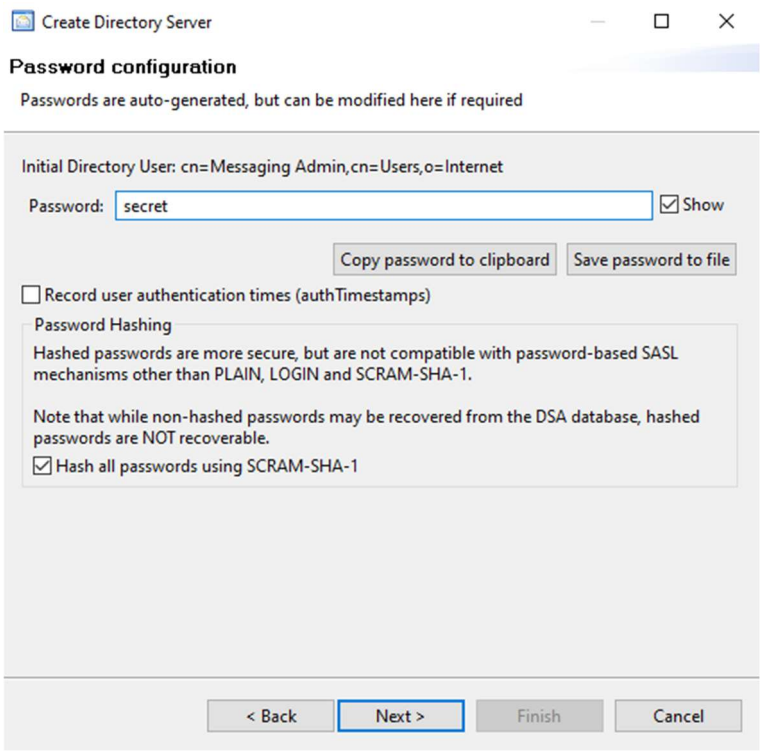
In this guide we have changed the Base DN to “Internet”. Click Next>”

Enter Password



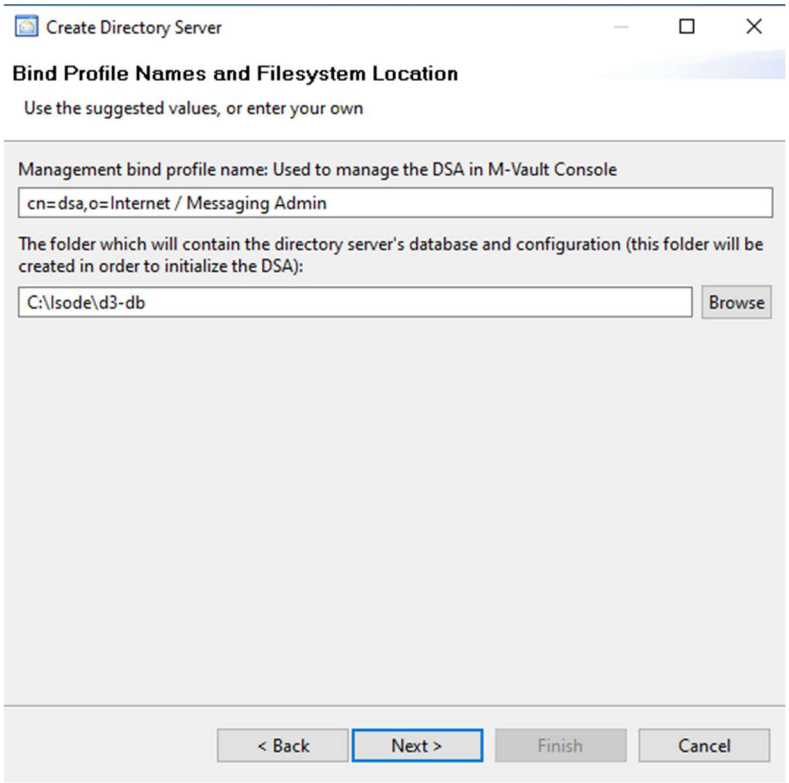
The GUI will auto-create a Password for the initial directory user – but you can change this to one of your own. In this guide we will use “secret”.

Password entered



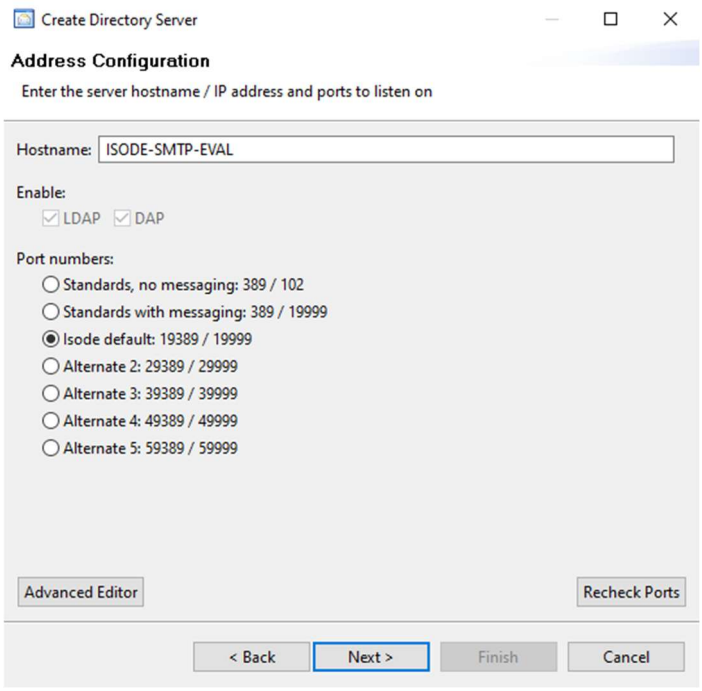
Always check the password you have entered by checking the "Show" checkbox, then click "Next>".

Bind Profile Summary



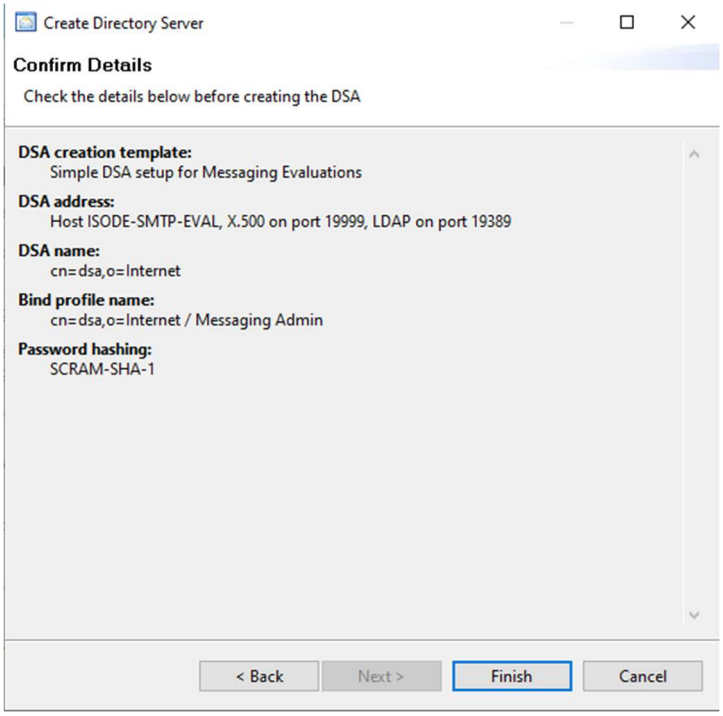
Click "Next>".

DSA Address Configuration



Click “Next>”.

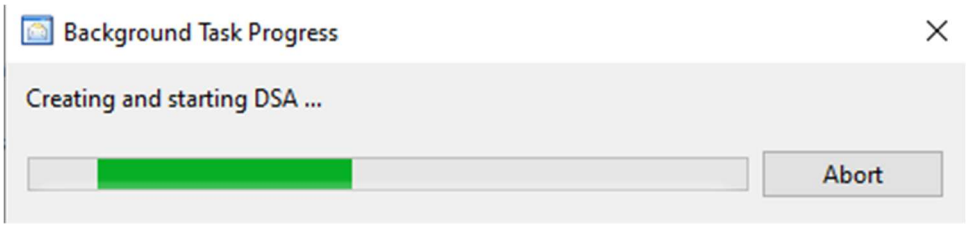
DSA Configuration Details



Click “Finish”.

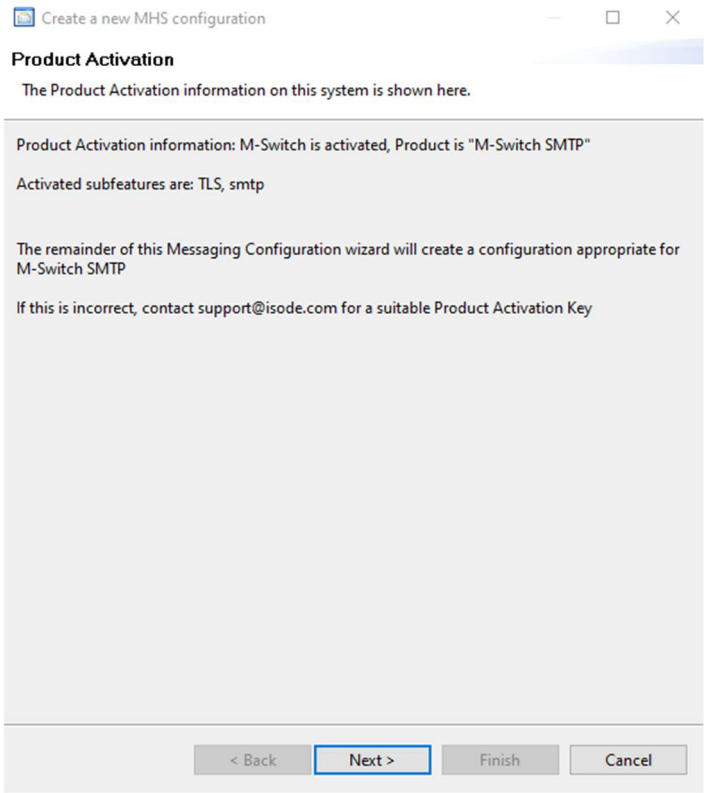
The following screen is shown.

DSA being created



Wait until this finishes.

Product Activation Summary

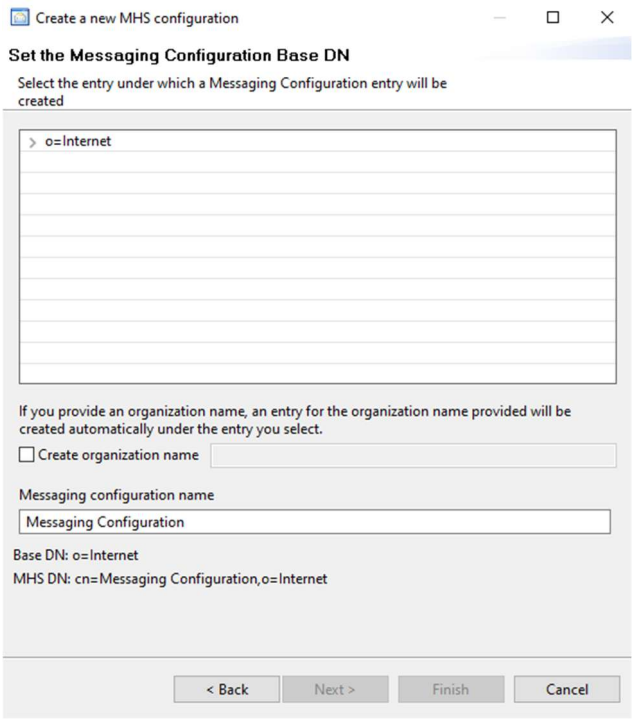


The summary of what features are Activated in the product is shown.

Click “Next>”.

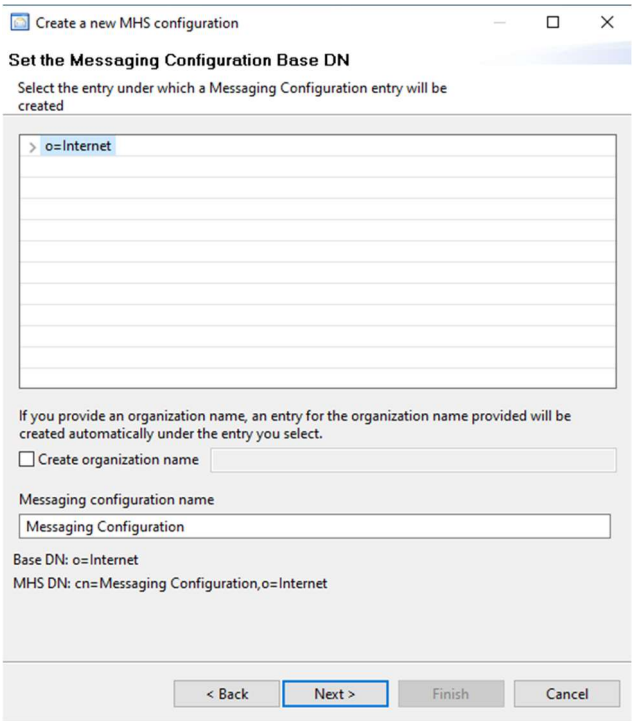
You will now through steps to create the messaging configuration.

Set the Messaging Configuration Base DN



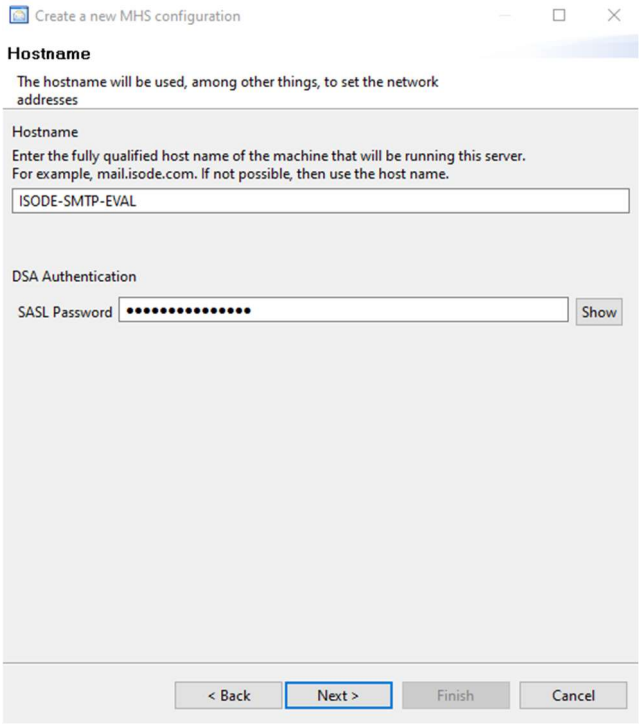
In simple configuration just select the "O=*Your Base DN*"

Set the Messaging Configuration Base DN



Click "Next>".

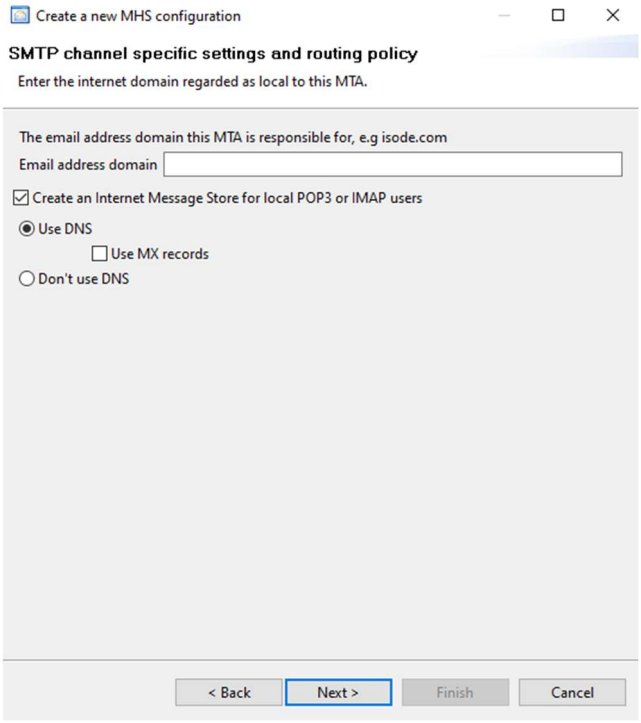
Set the Hostname



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.

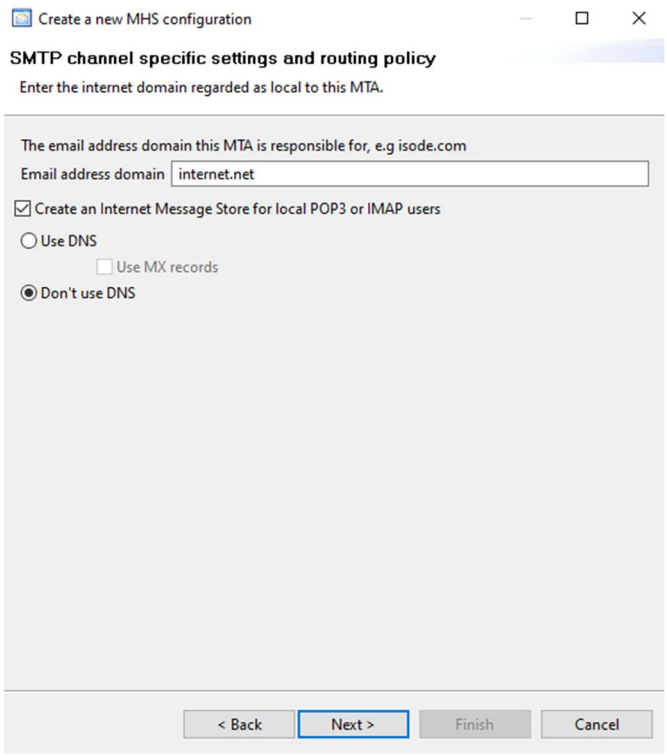
Click “Next>”.

SMTP Configuration



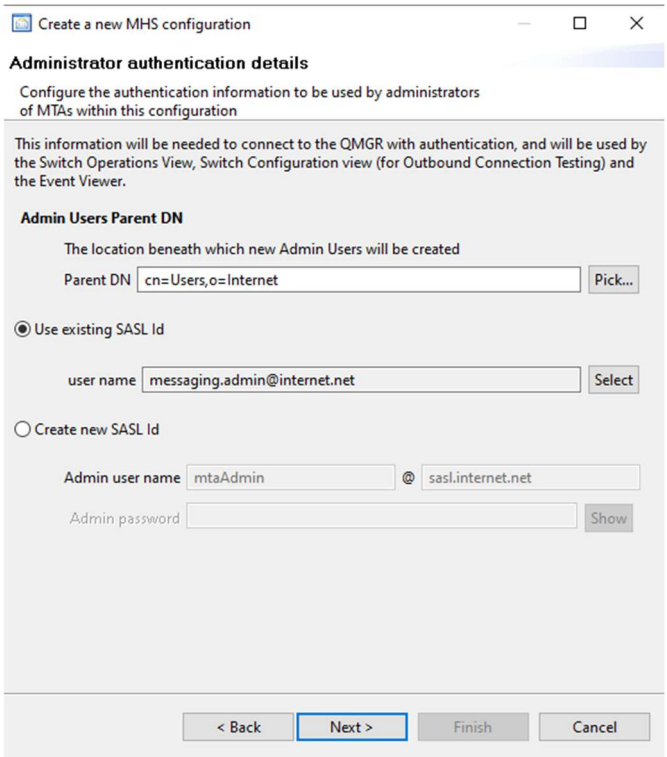
Unless you have already set up DNS and MX Records for your domain it is best to check do not use DNS.

SMTP Configuration



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

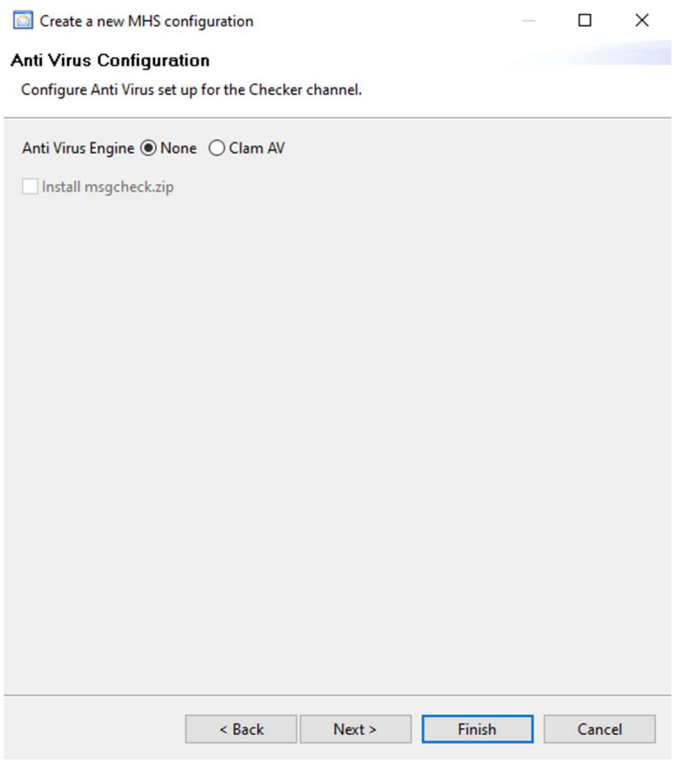
Administrator details



The Wizard should auto-populate the details above.

Click "Next>".

Anti Virus configuration



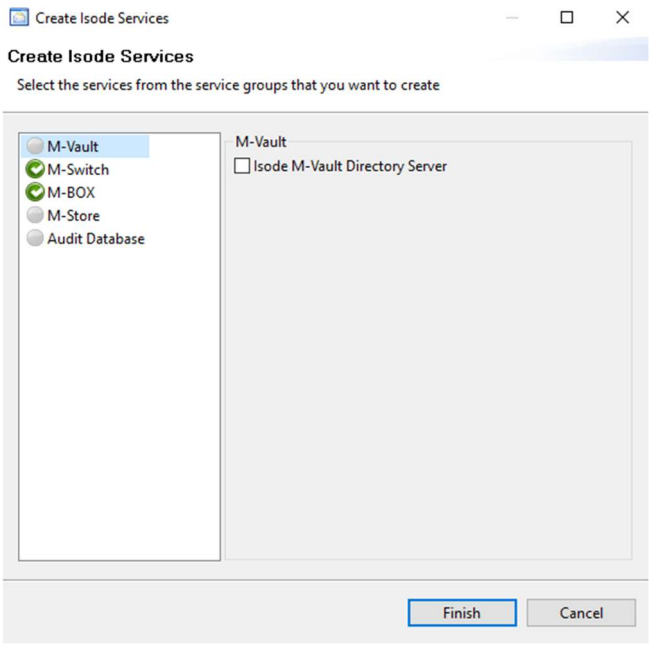
In evaluations we do not configure Anti Virus as this is more for production systems.

Click “Next>”.

Service File Creation

Click “Next>”.

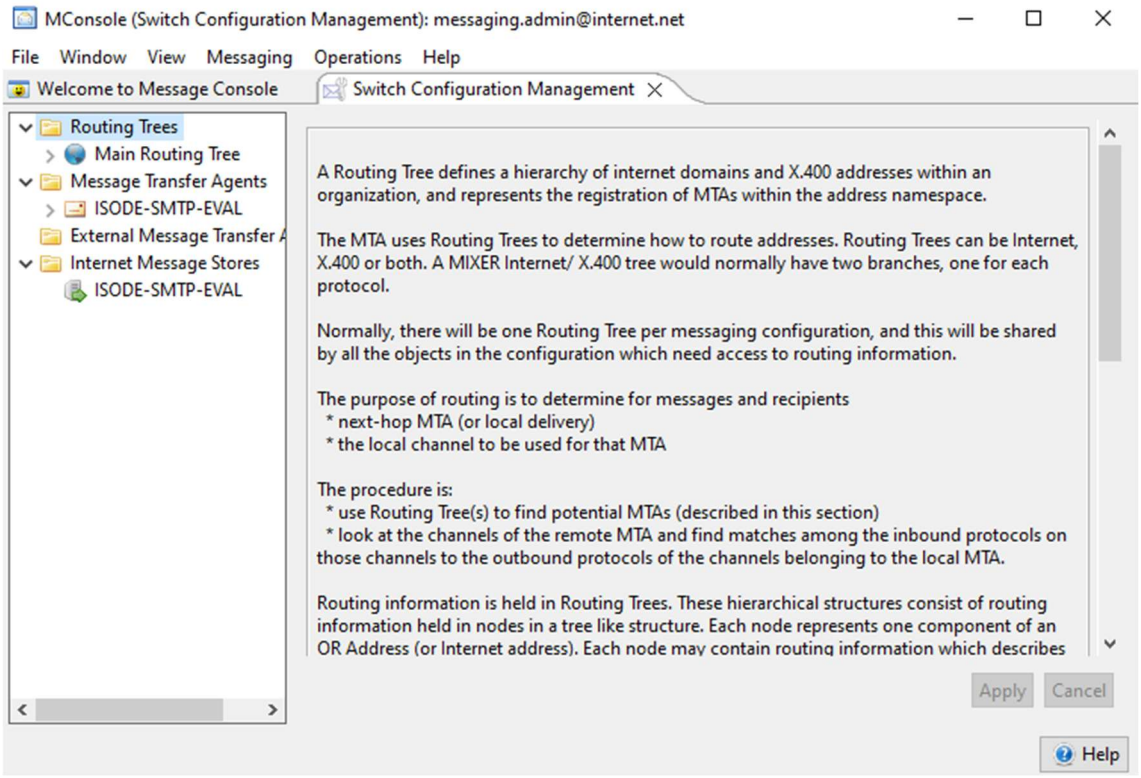
Create Isode Services



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



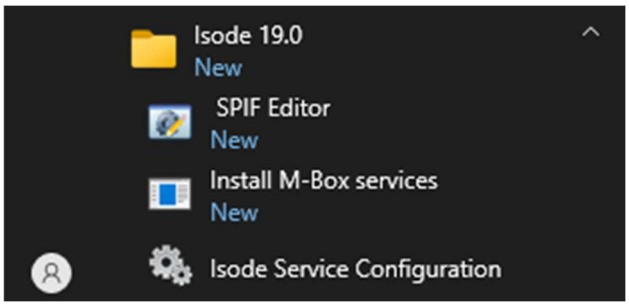
You have now completed the core configuration of your server.

Services Configuration

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

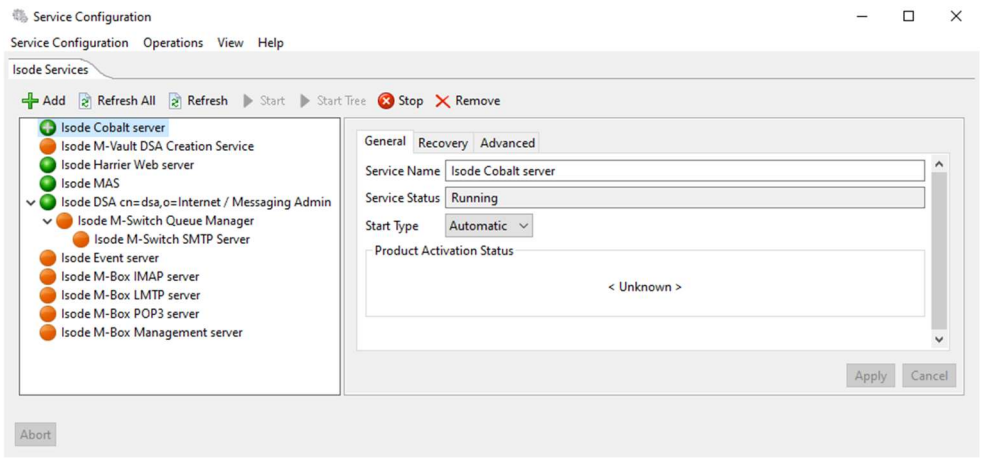
From the Start Menu Windows→Isode R19.0→Isode Service Configuration

Create Isode Services



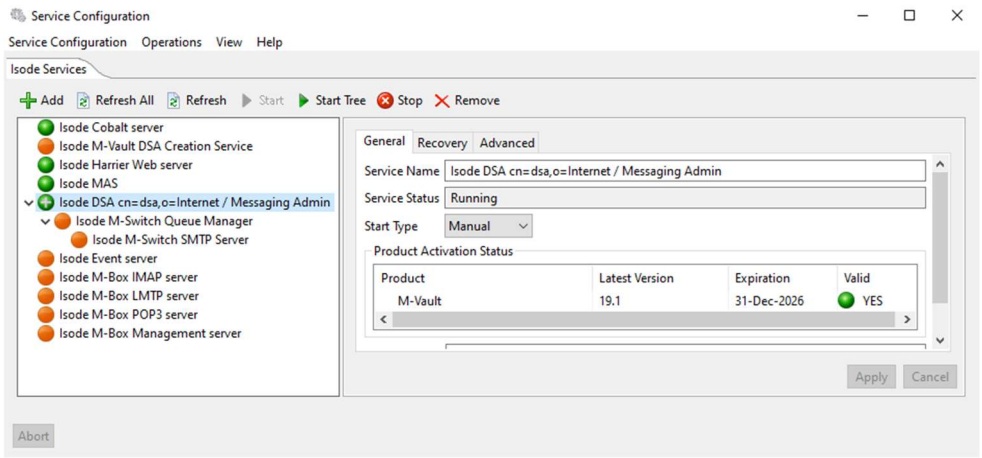
The following screen will be displayed.

Isode Service Configuration



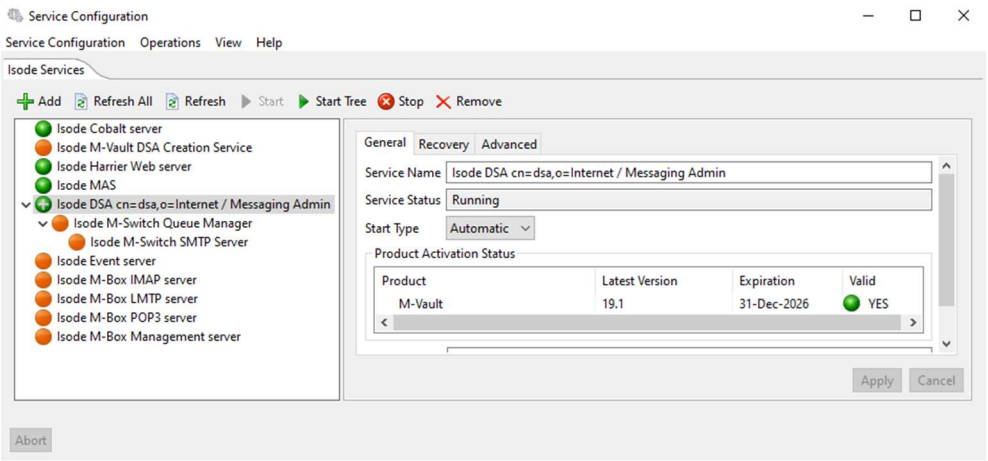
Select the Isode DSA ….service.

Isode Service Configuration



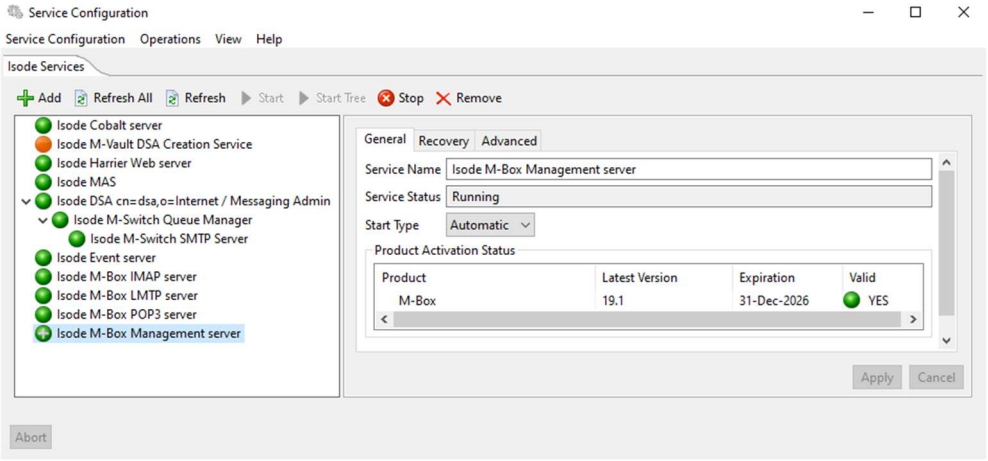
Change the start type from Manual to Automatic and Click “Apply”

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

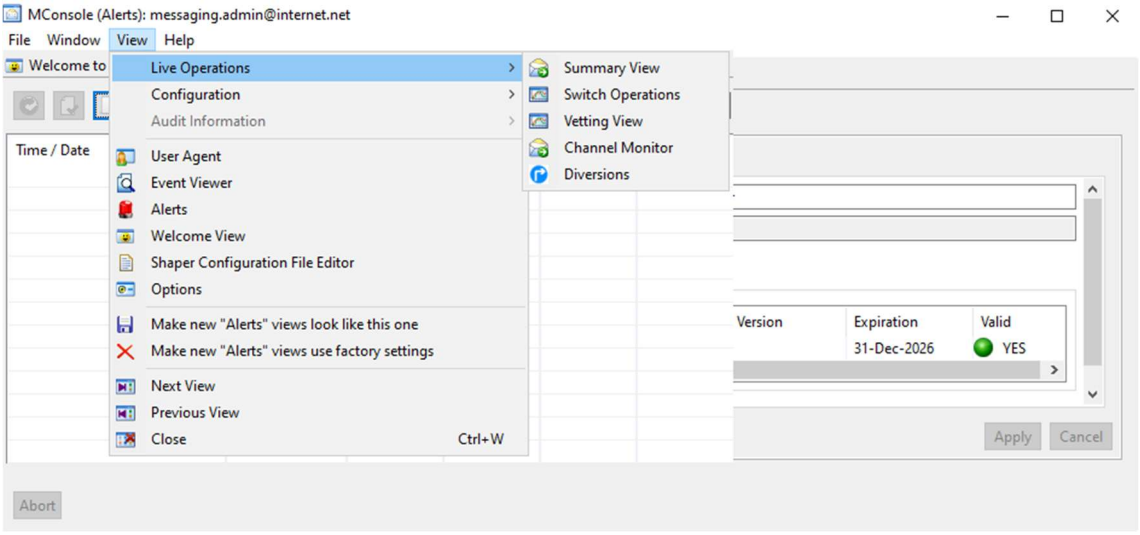


This completes the Service Configuration.

M-Switch further Configuration

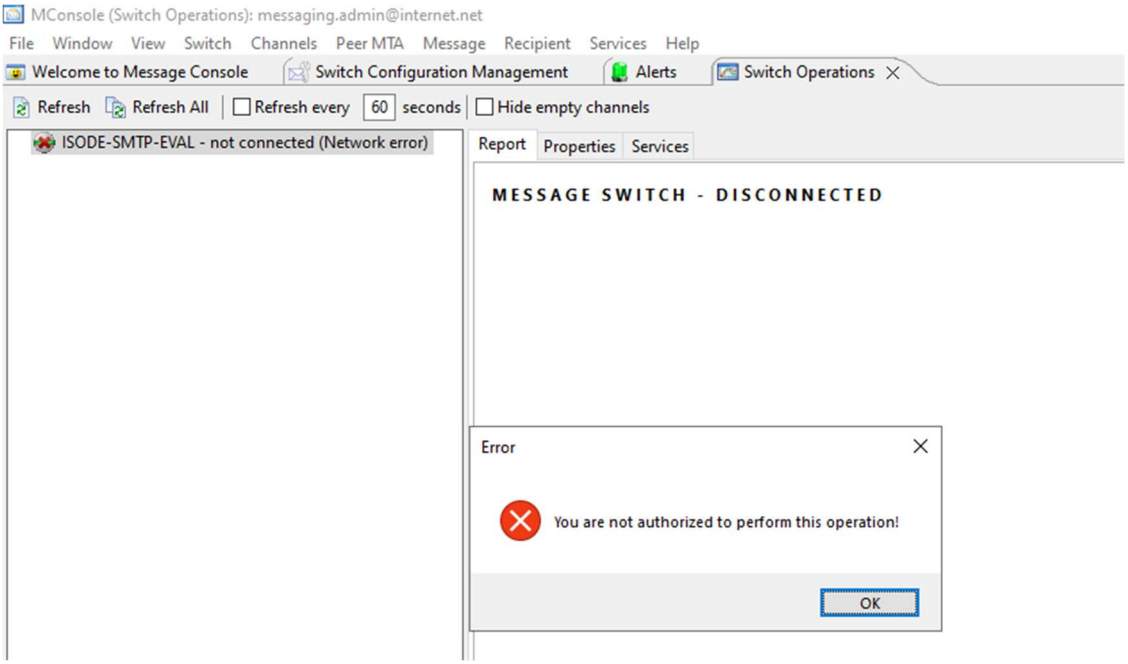
Now that the services are running you can make changes to the M-Switch Configuration and they will take effect immediately. Return to M-Console. select View→Live Operations→Switch Operations.

M-Console Switch Operations View Setup



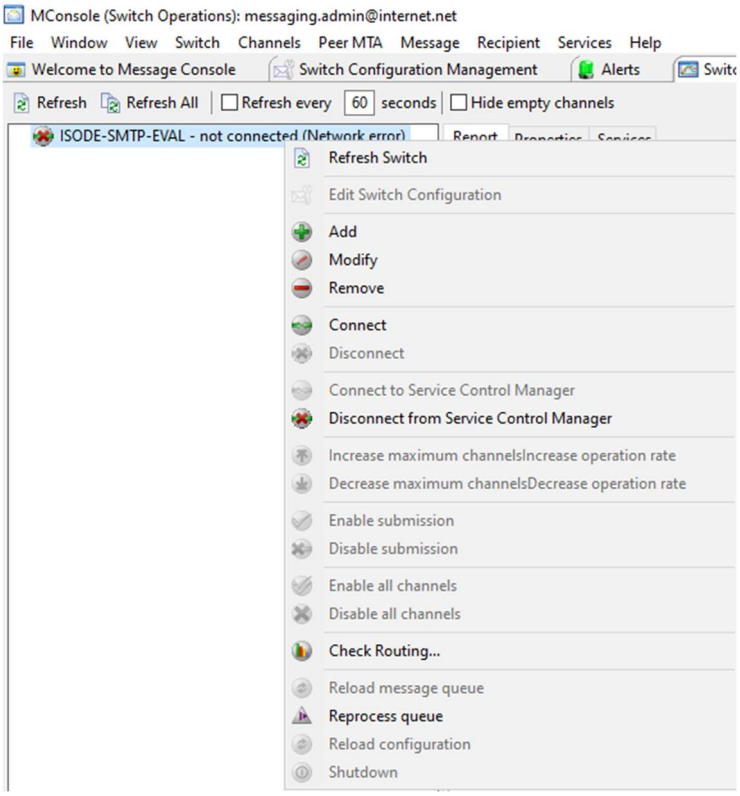
Select View→Live Operations→Switch Operations.

M-Console Switch Operations View Setup



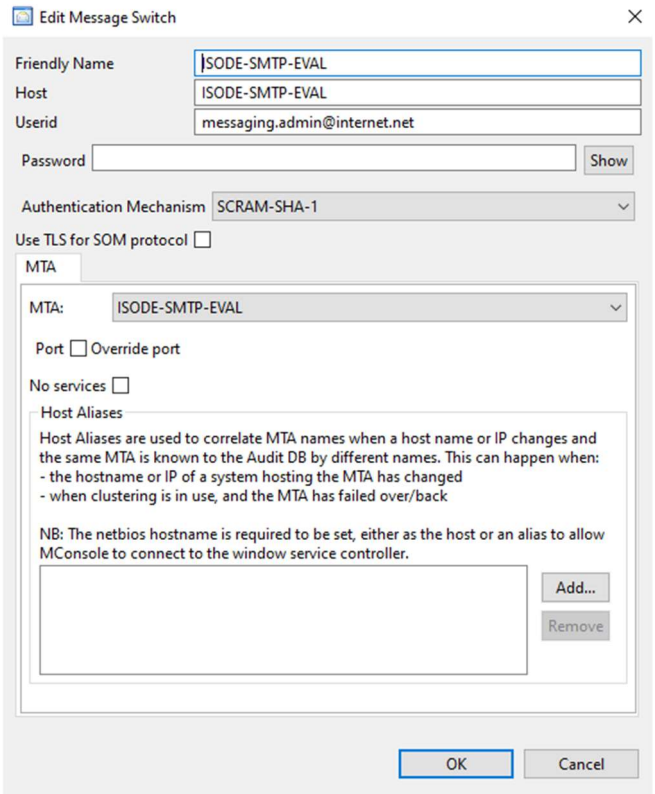
The Error is expected, click “OK”.

M-Console Switch Operations View Setup



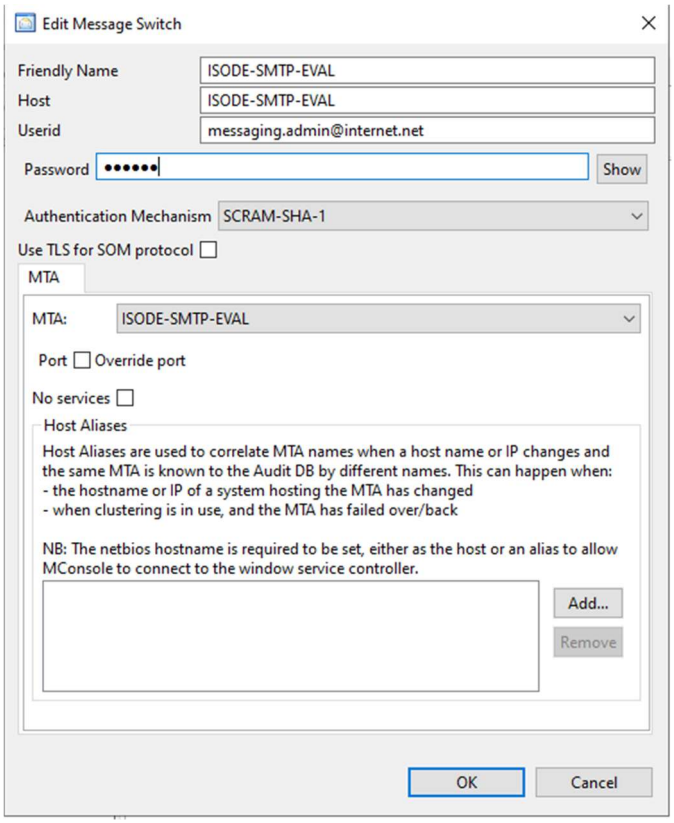
Right Click on the Switch and Select “Modify”.

M-Console Switch Operations View Setup



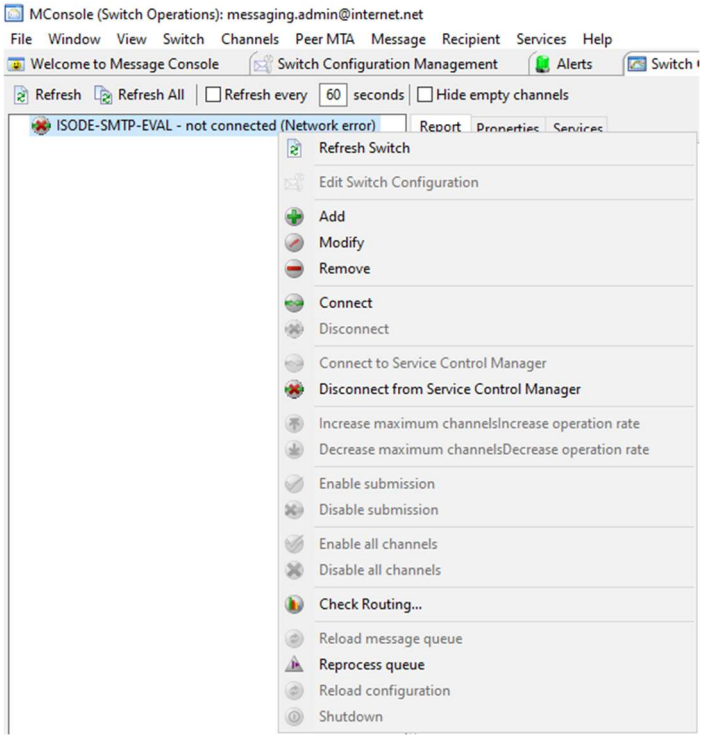
Enter the Password you set for the Messaging Admin User.

M-Console Switch Operations View Setup



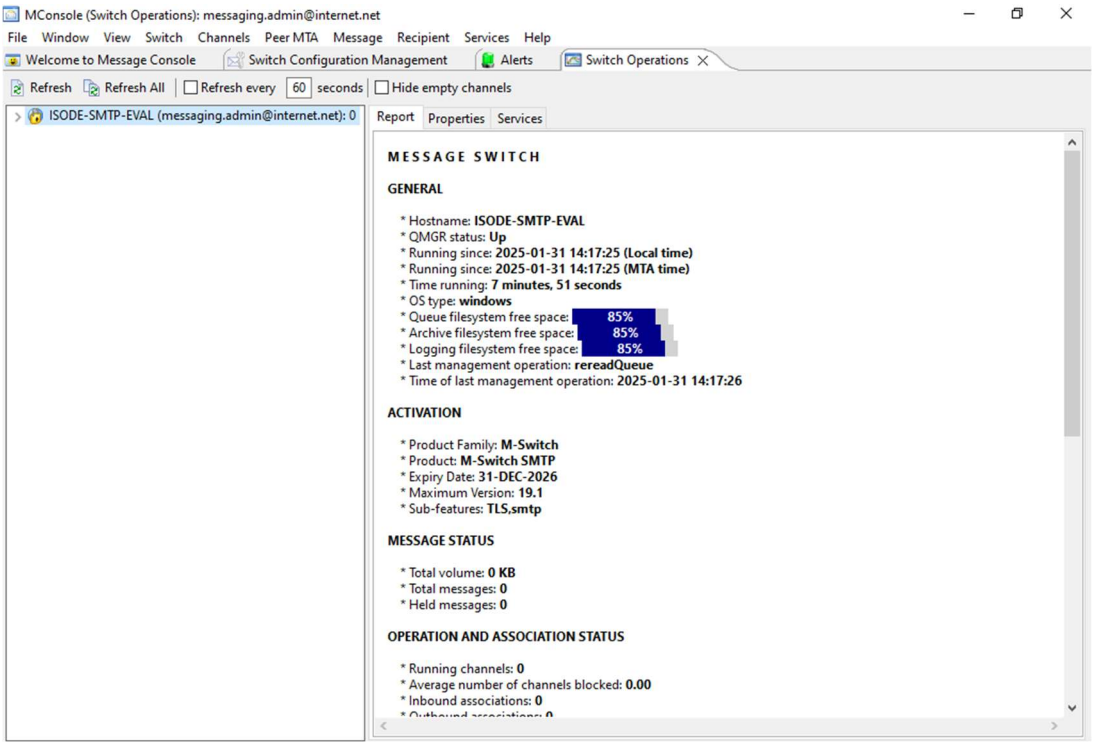
Click “OK”.

M-Console Switch Operations View Setup



Right Click on the Switch and Select “Connect”.

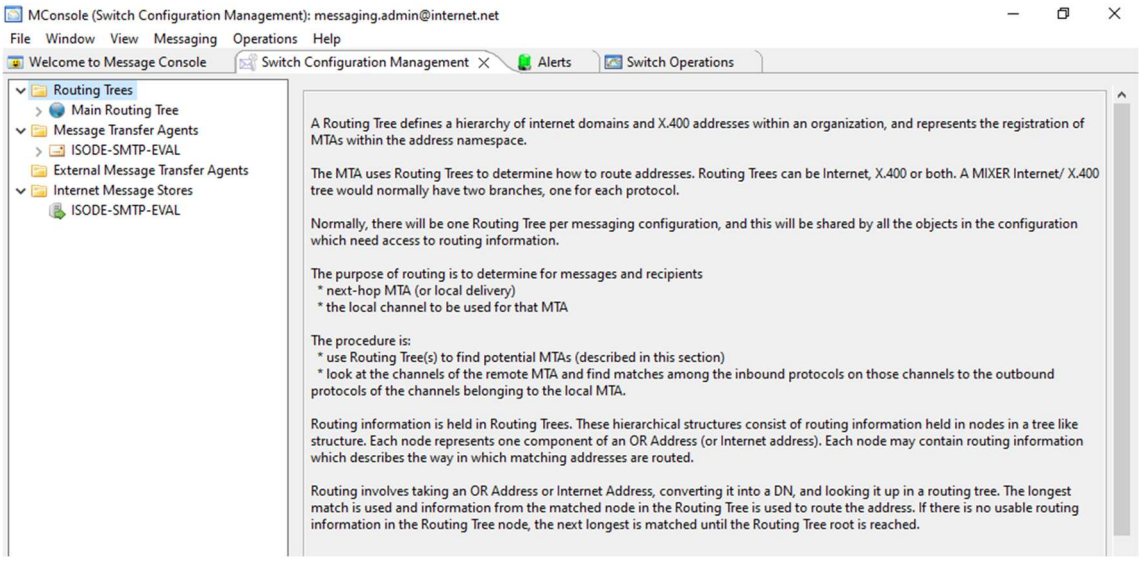
M-Console Switch Operations View Setup



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

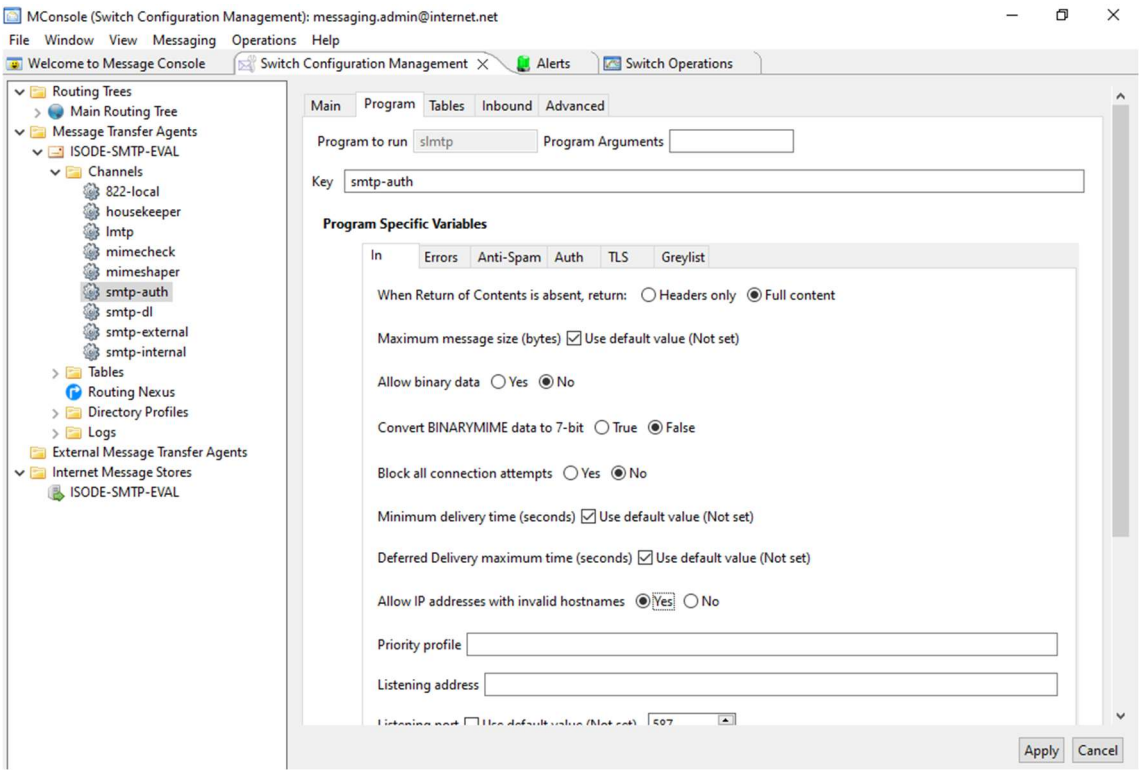
Go to the Switch Configuration Management Tab.

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.

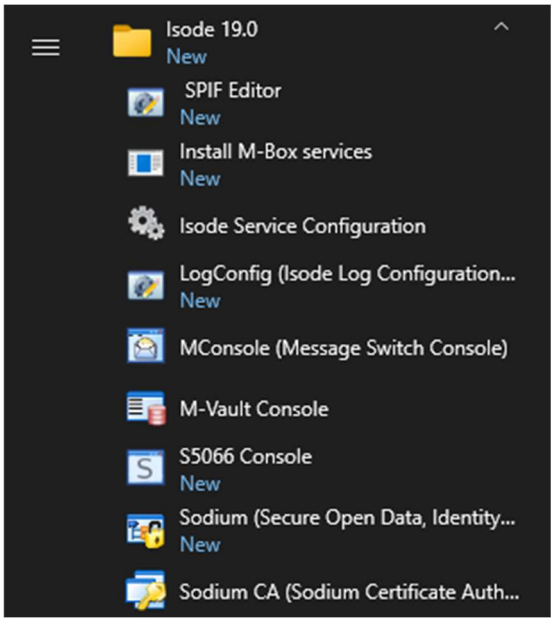
If you do not have a TLS Activation you can skip the next section and go directly to the Provisioning Users with Cobalt section.

Configuring TLS on M-Vault

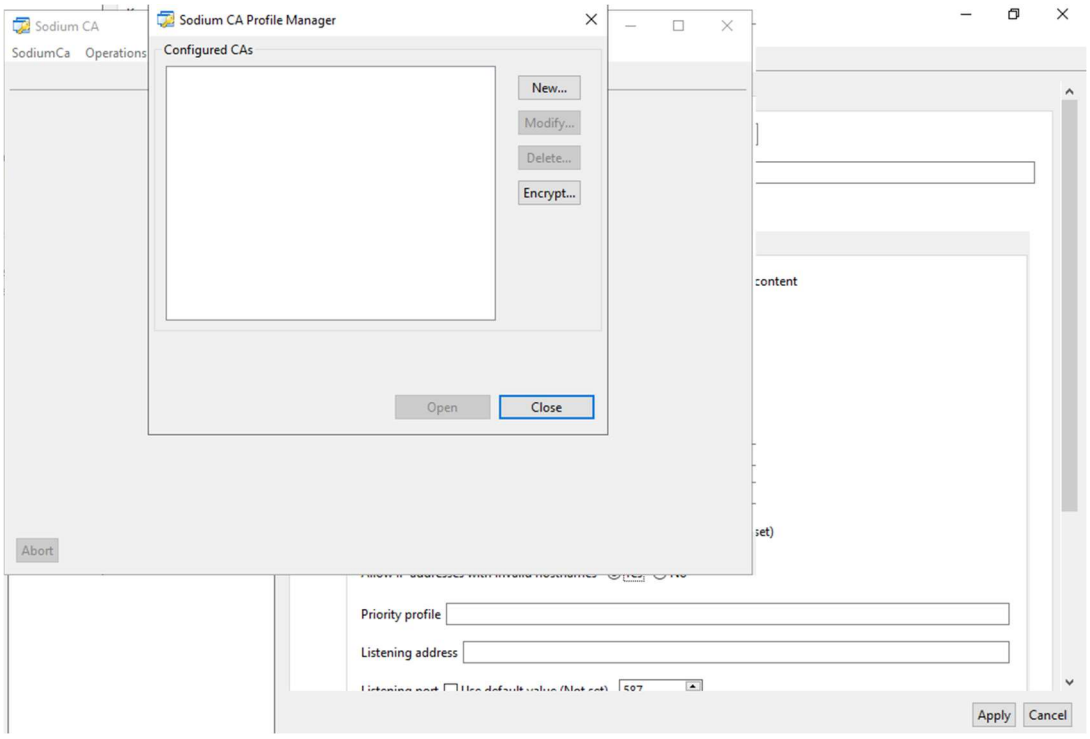
Here you will setup Sodium CA to issue Certificates from a Certificate Signing Request (CSR) and use M-Vault Console to generate this CSR and install the provided Certificate. You might want to create a dedicated folder for Certificates before you start.

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

Start Sodium CA

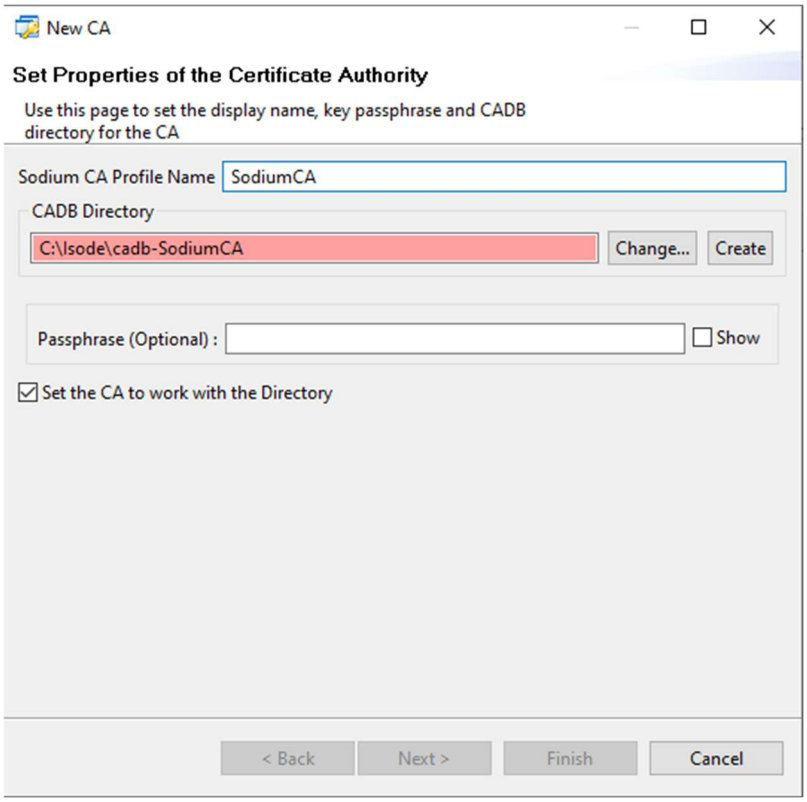


Sodium CA initial configuration



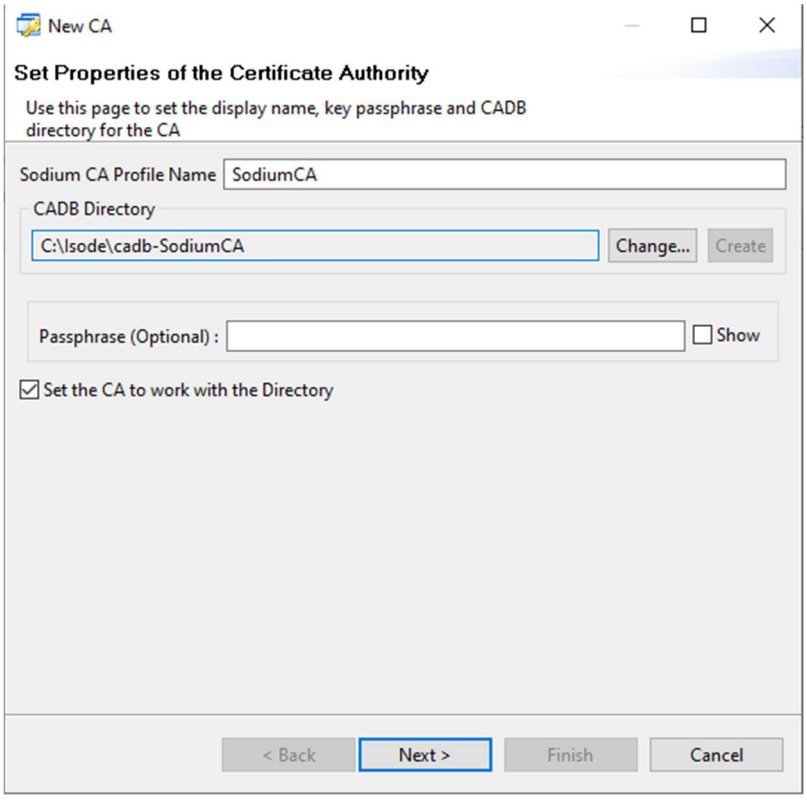
Click “New”.

Sodium CA initial configuration



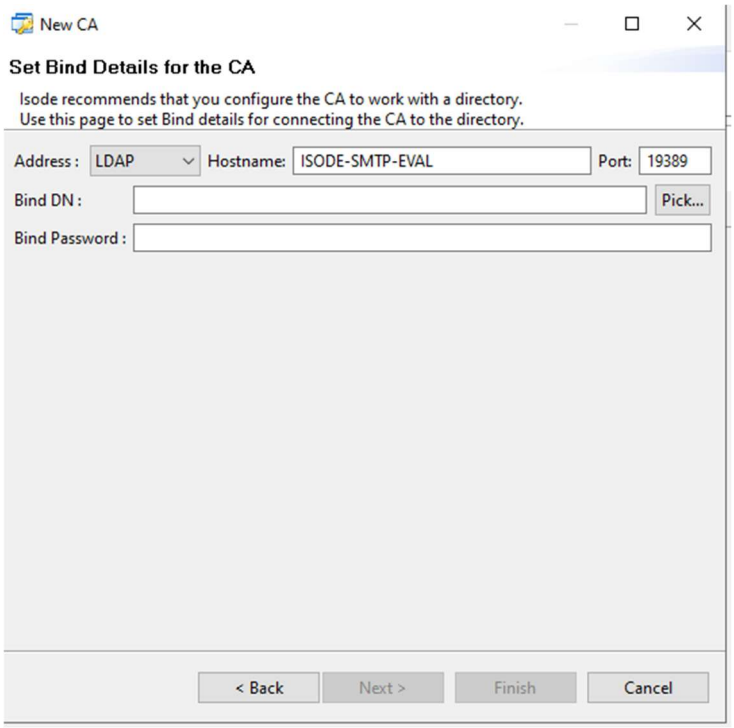
Click “Create”, for the purposes of an Evaluation you do not need to use a Passphrase.

Sodium CA initial configuration



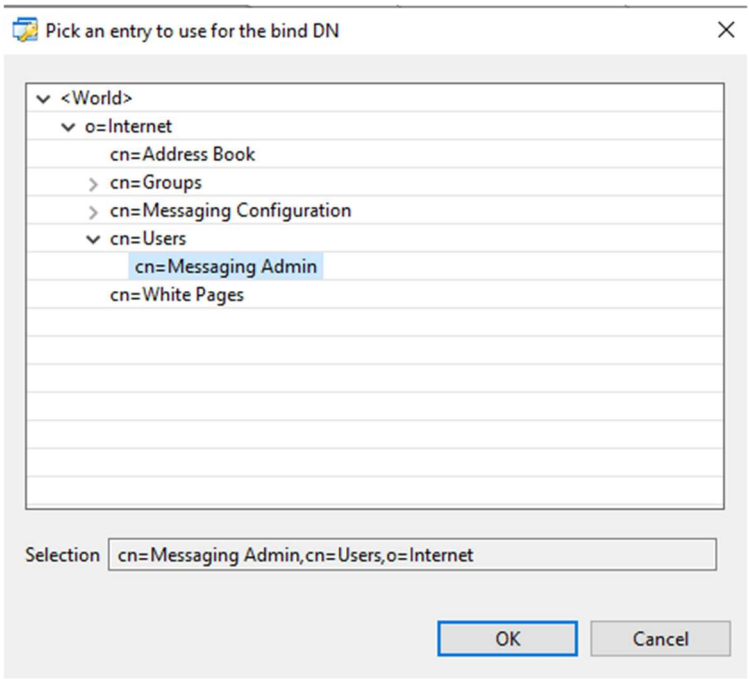
Click “Next>”.

Sodium CA initial configuration



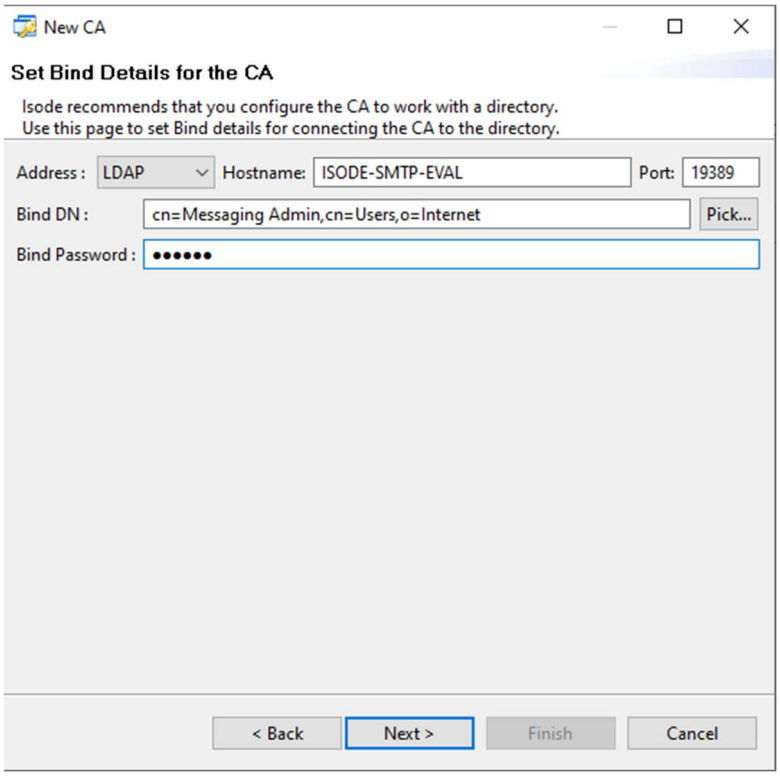
Select “Pick...”.

Sodium CA initial configuration



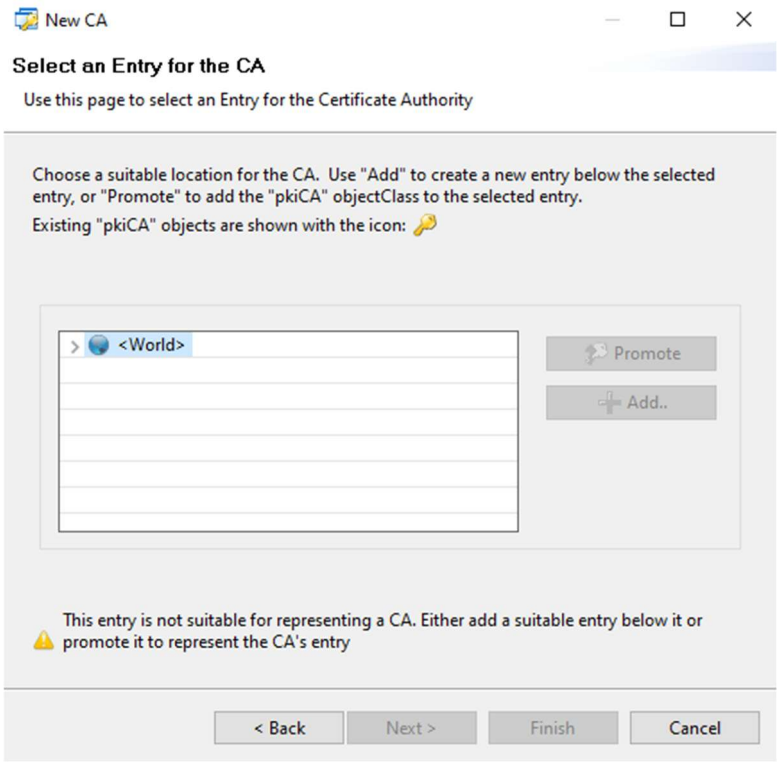
Navigate to the “Messaging Admin” User. Click “OK”.

Sodium CA initial configuration



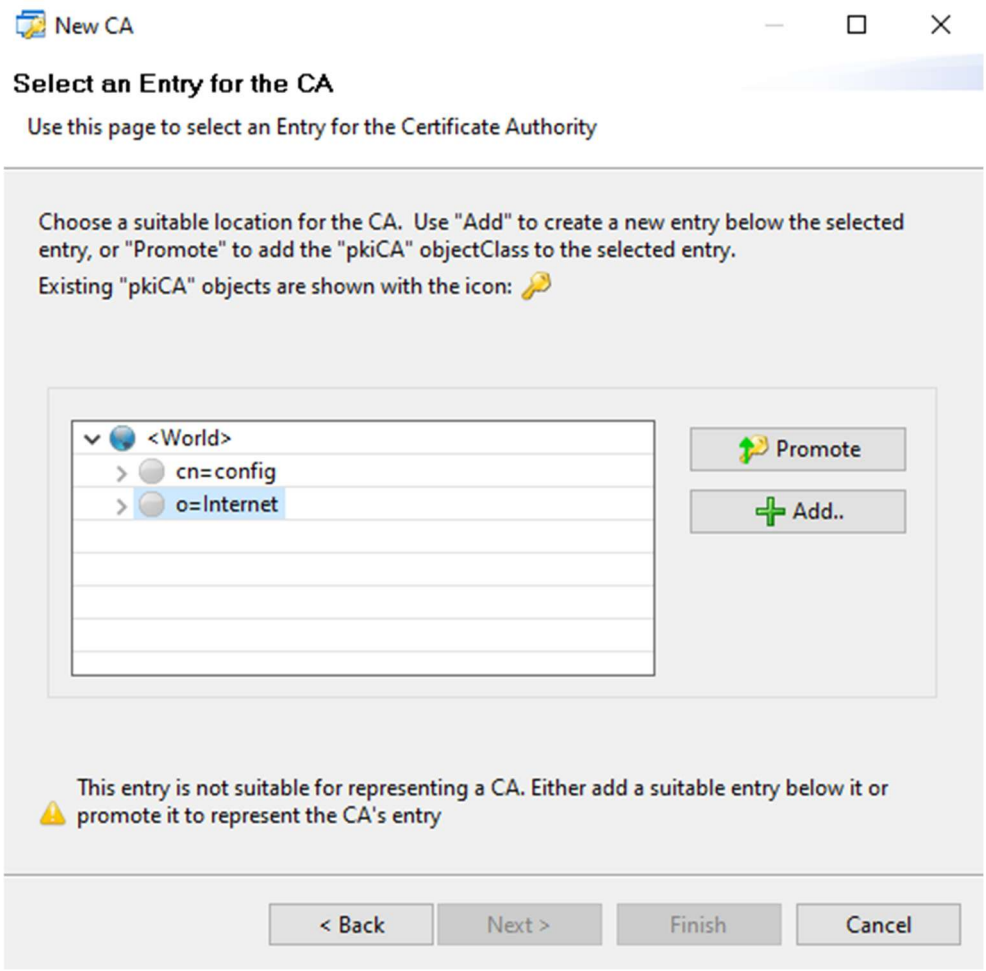
Enter the Password for the Messaging Admin User. Click “Next>”.

Sodium CA initial configuration



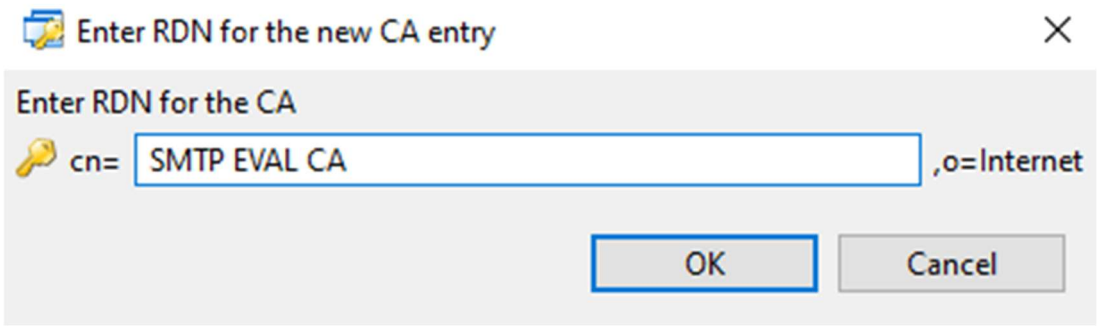
Expand the “<World>”.

Sodium CA initial configuration



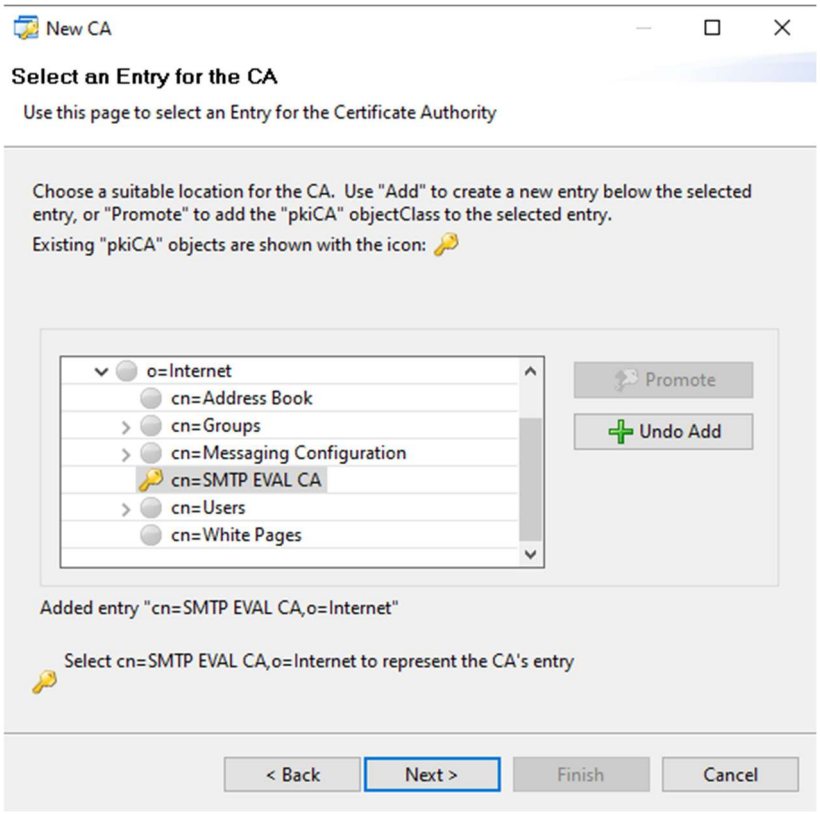
Select “O=Internet”, Click “+ Add...”

Sodium CA initial configuration



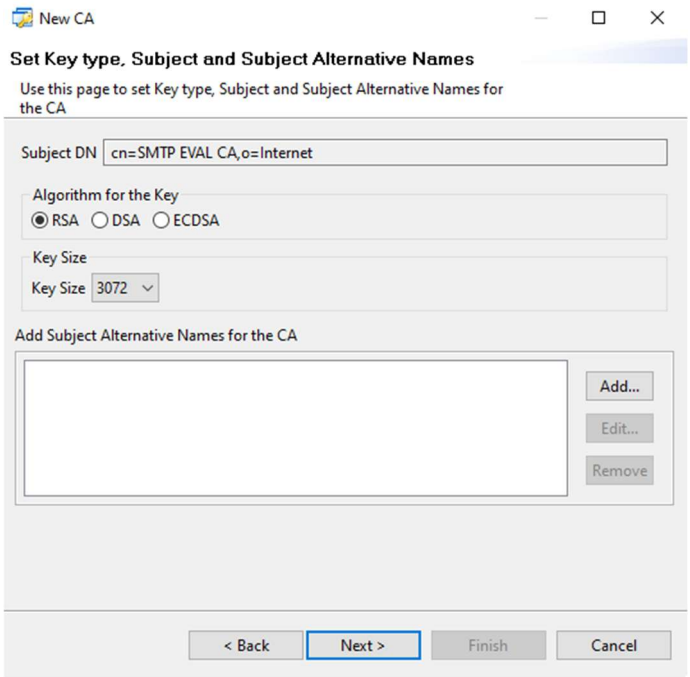
Enter a “cn” of your choice for the CA. Click “OK”.

Sodium CA initial configuration



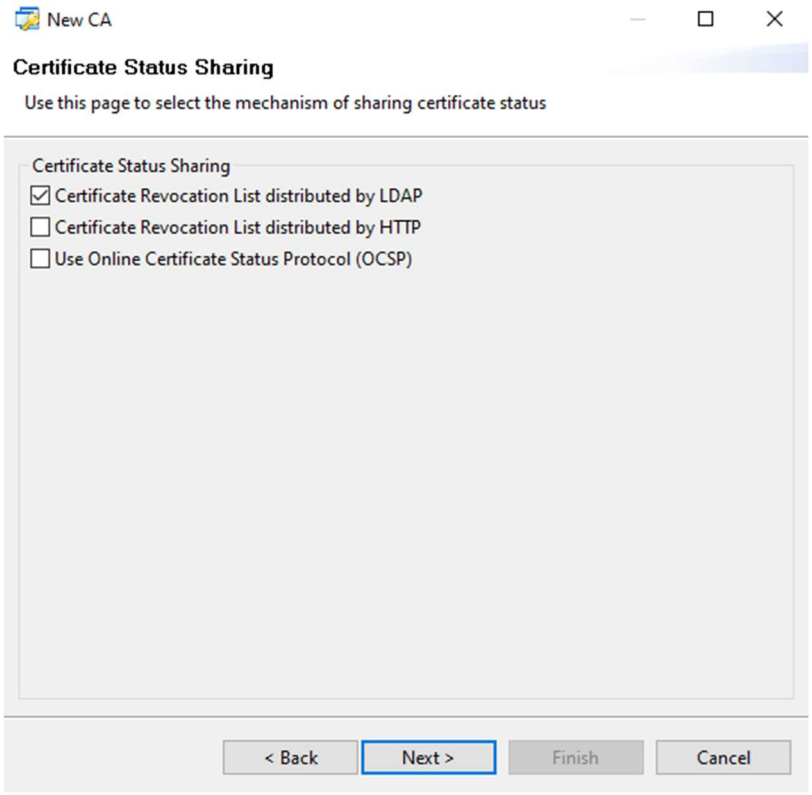
Click “Next>”.

Sodium CA initial configuration



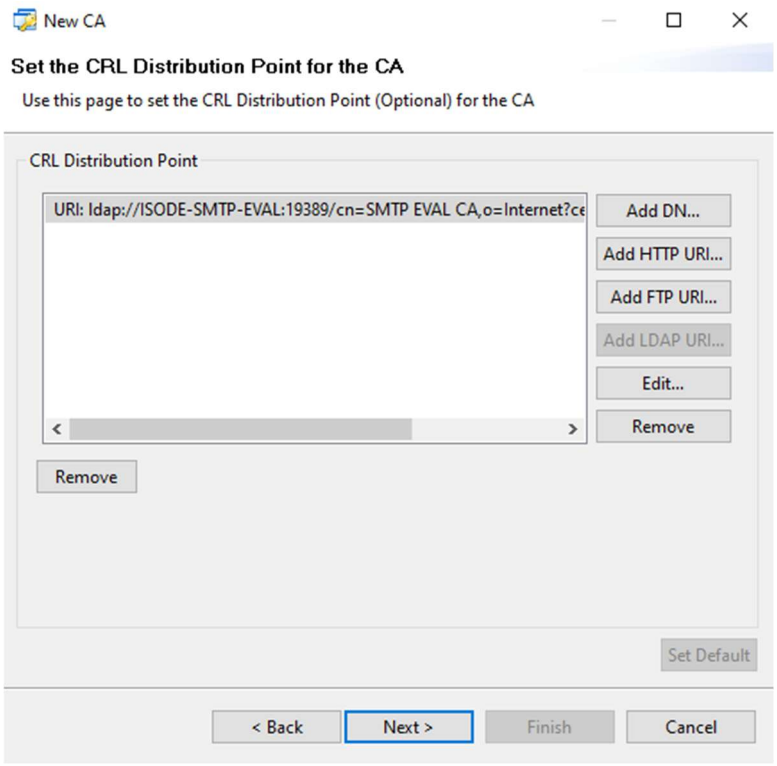
Accept the defaults and Click “Next>”.

Sodium CA initial configuration



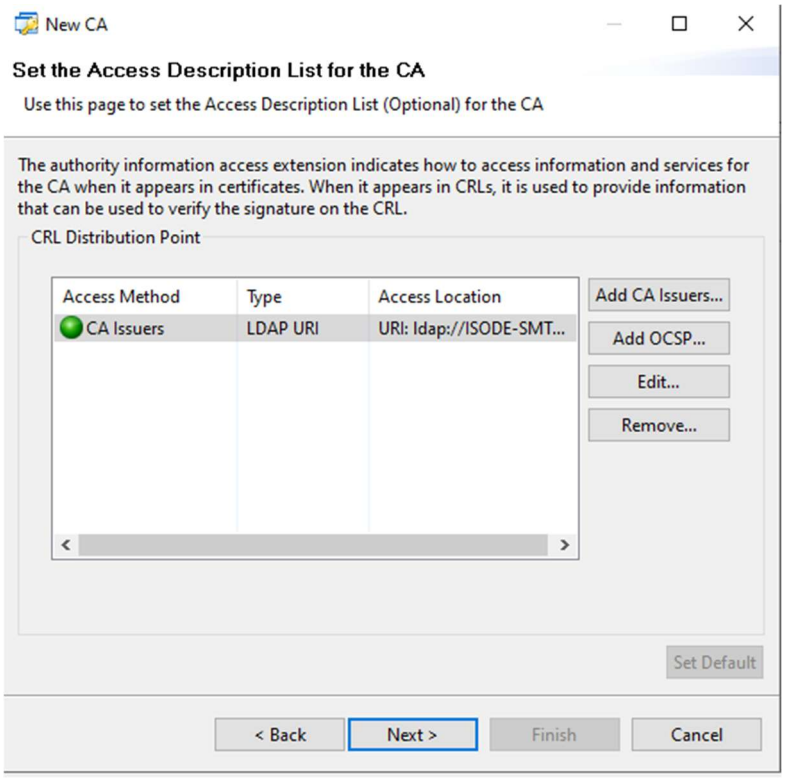
Accept the default and Click “Next>”.

Sodium CA initial configuration



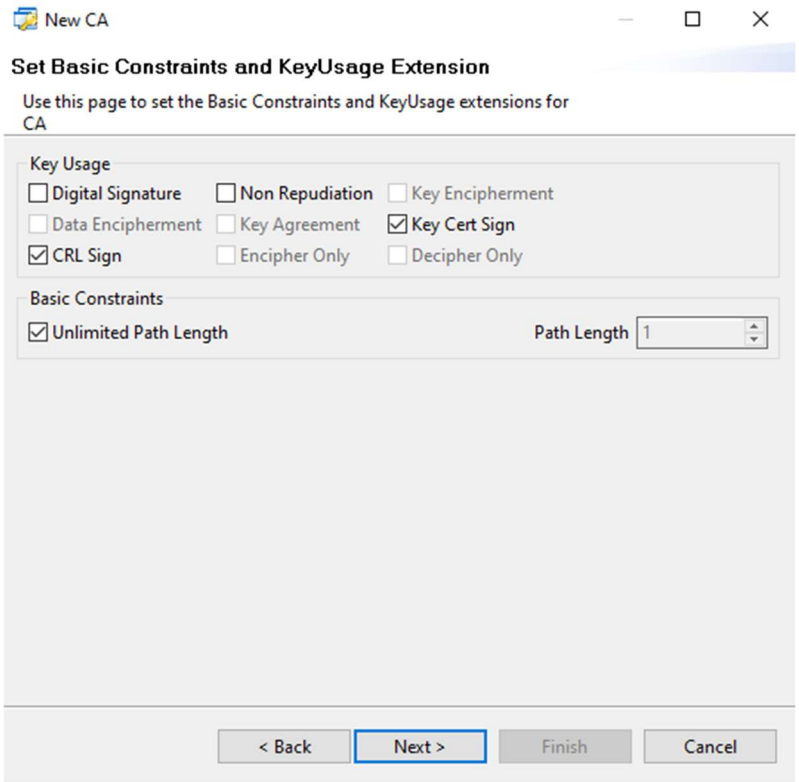
Accept the default and Click “Next>”.

Sodium CA initial configuration



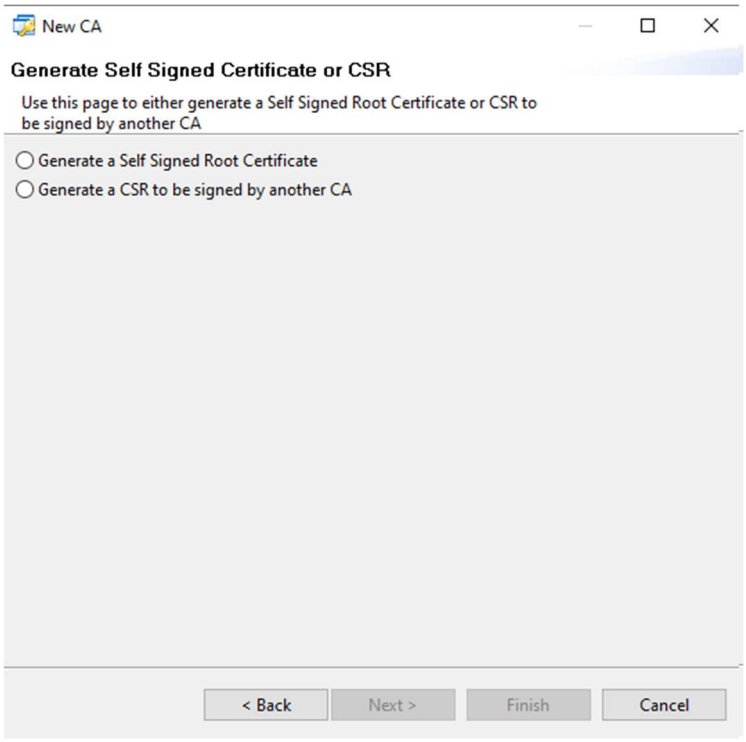
Accept the default and Click “Next>”.

Sodium CA initial configuration



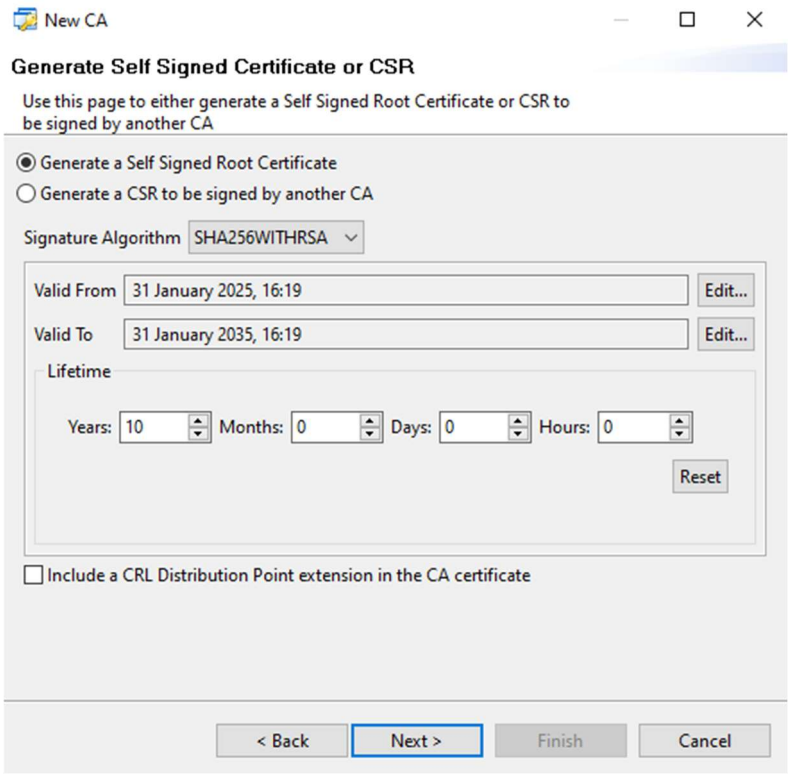
Accept the default and Click “Next>”.

Sodium CA initial configuration



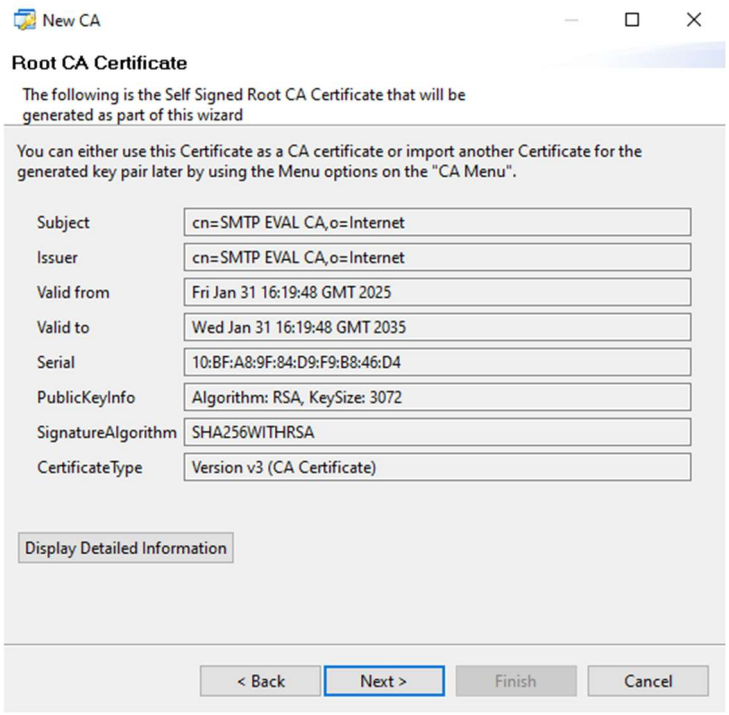
Select “Generate a Self Signed Root Certificate”

Sodium CA initial configuration



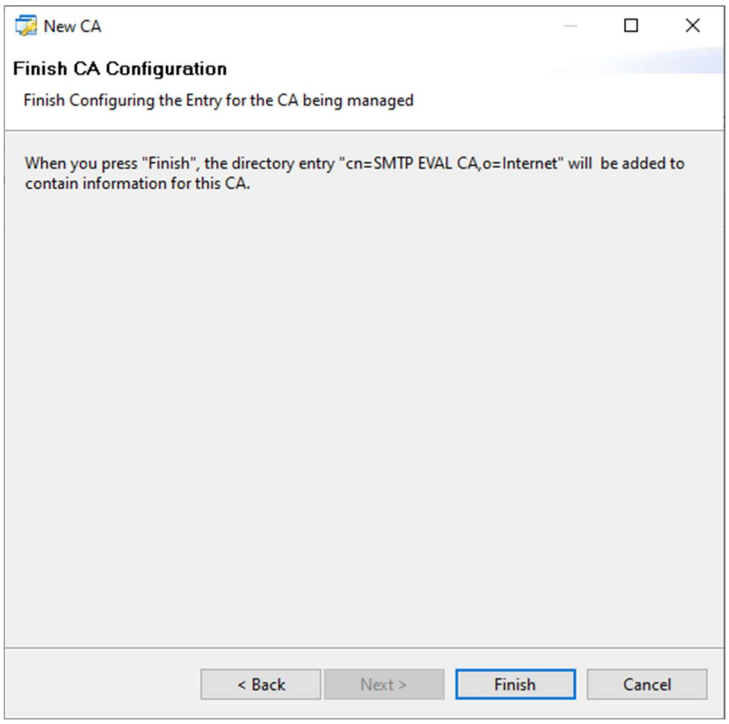
Accept the defaults and Click “Next>”.

Sodium CA initial configuration



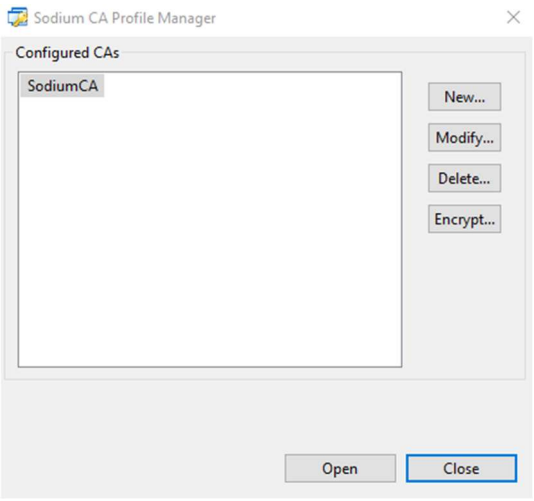
Click “Next>”.

Sodium CA initial configuration



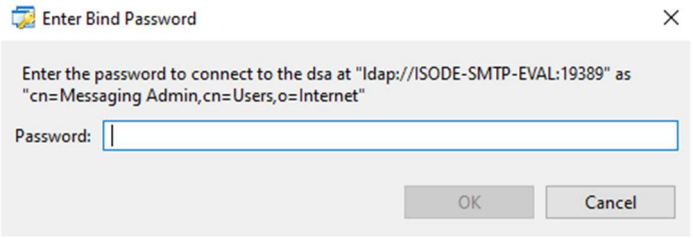
Click “Finish”.

Sodium CA initial configuration



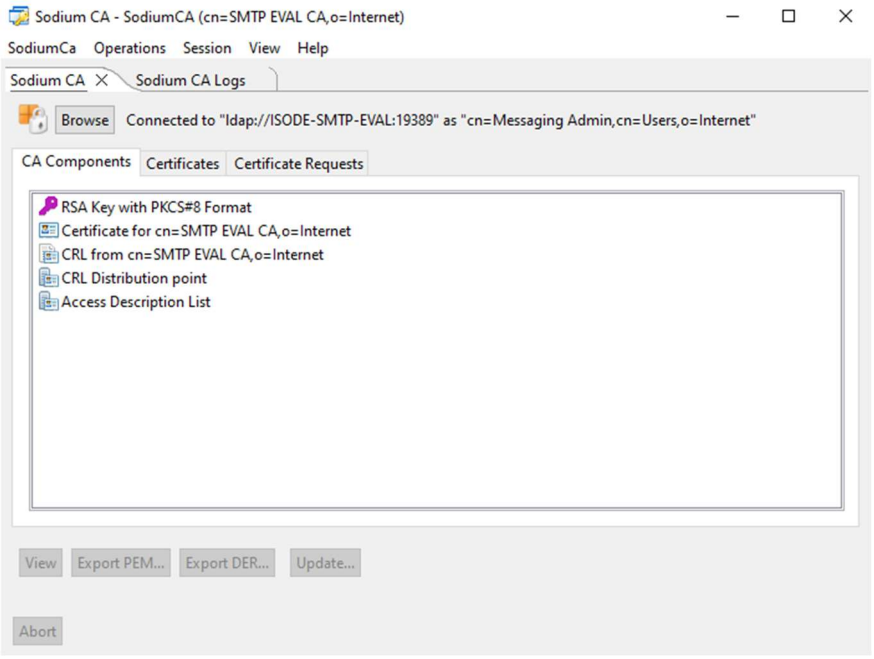
Select you newly created CA (SodiumCA) and Click “Open”.

Sodium CA initial configuration



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

Sodium CA initial configuration

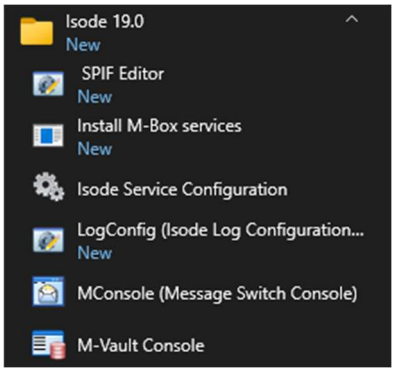


You now have your CA, leave this open and start M-Vault Console.

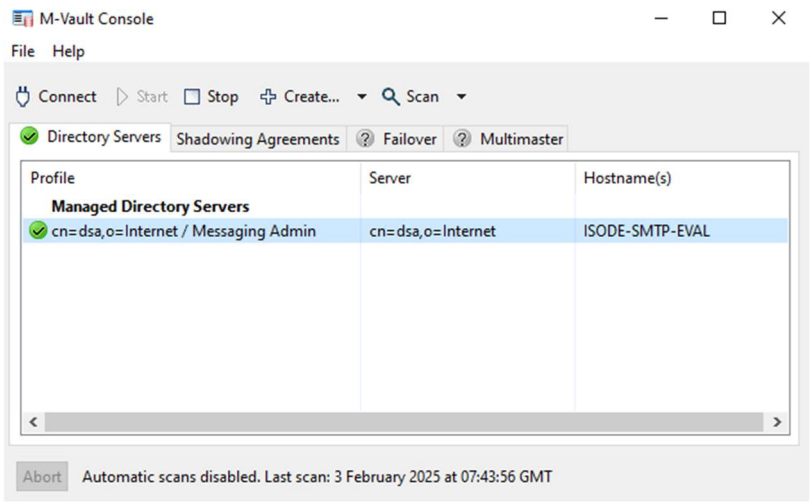
M-Vault Console is started on Windows as follows.

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

Start M-Vault Console

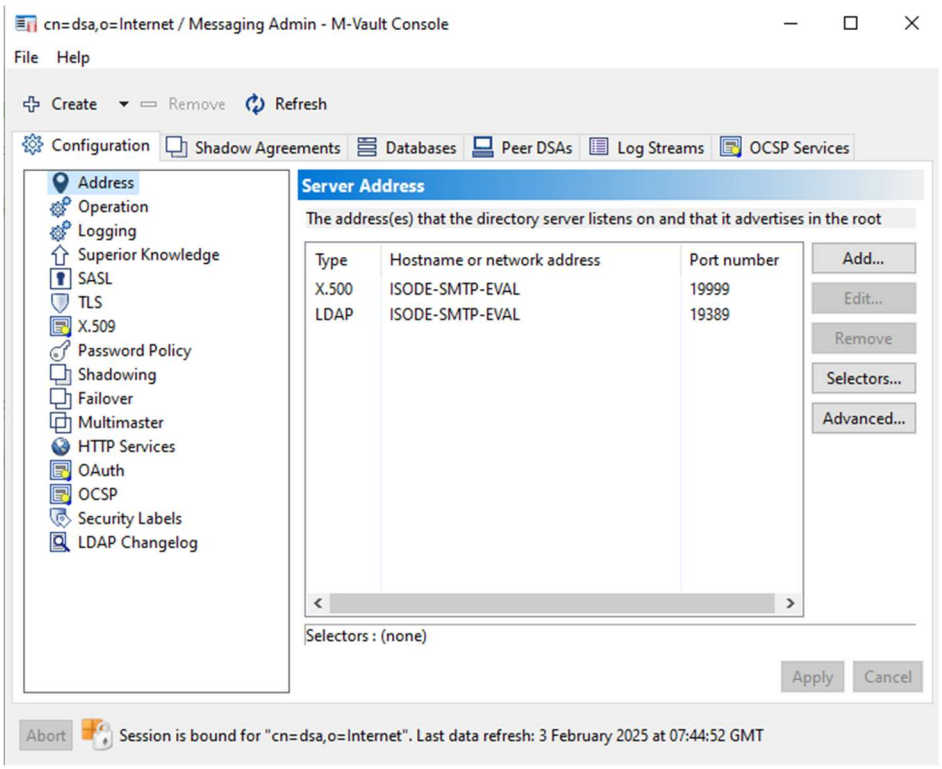


M-Vault Console Initial Screen



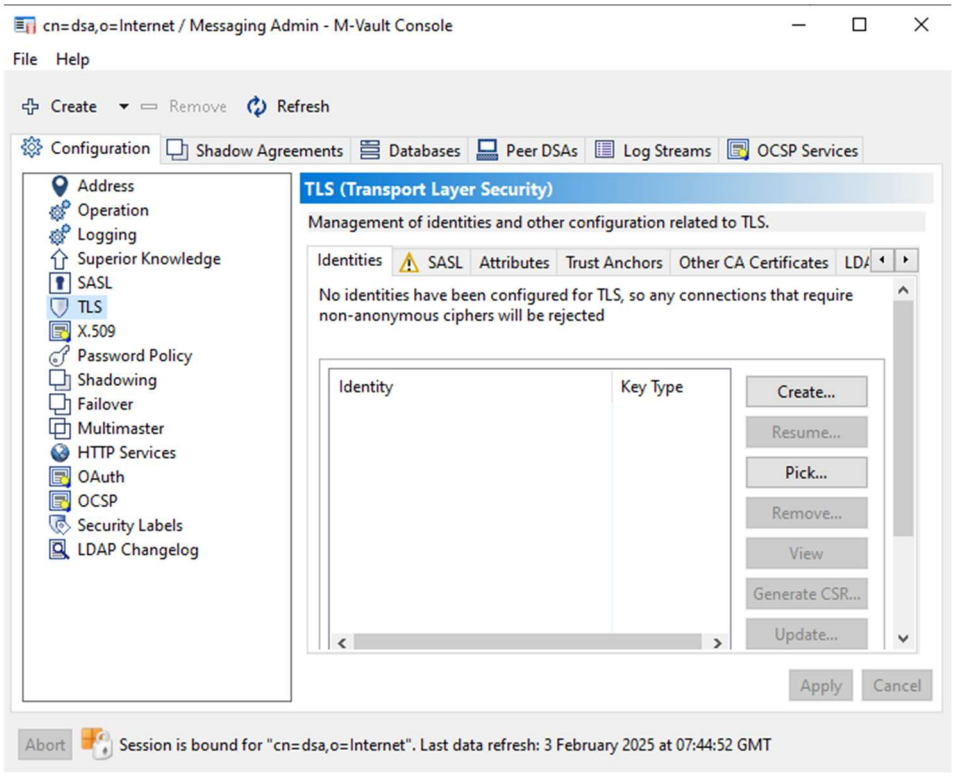
Double Click your Directory Server with the Green Tick below Managed Directory Servers.

M-Vault Console Initial Screen



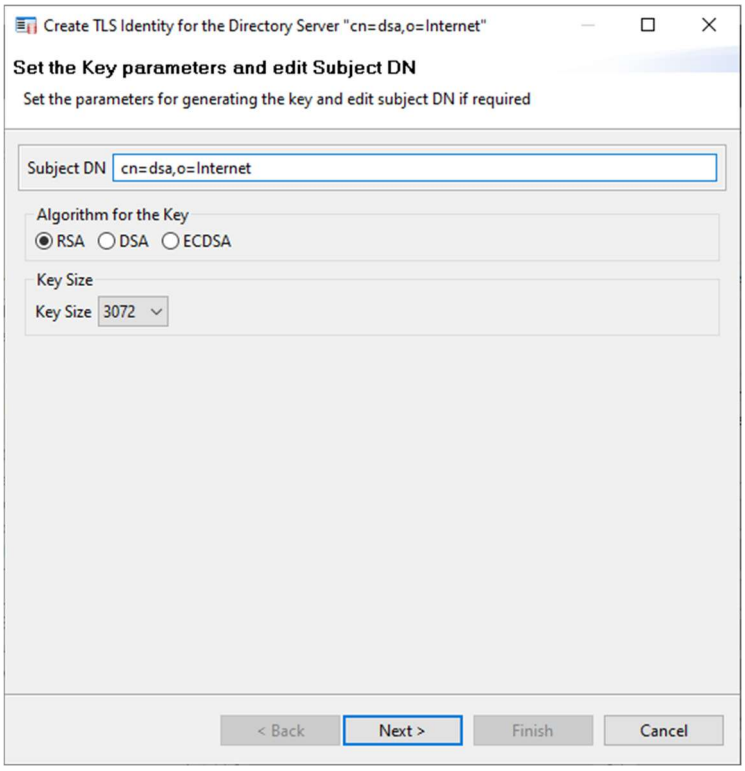
Select “TLS”.

M-Vault TLS Configuration



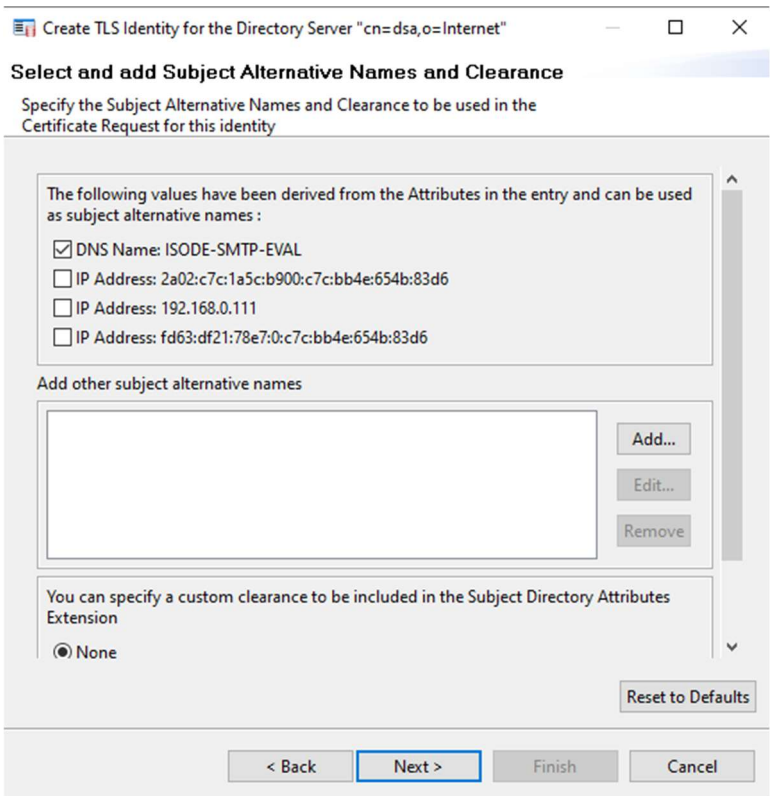
Select “Create…”

M-Vault TLS Configuration



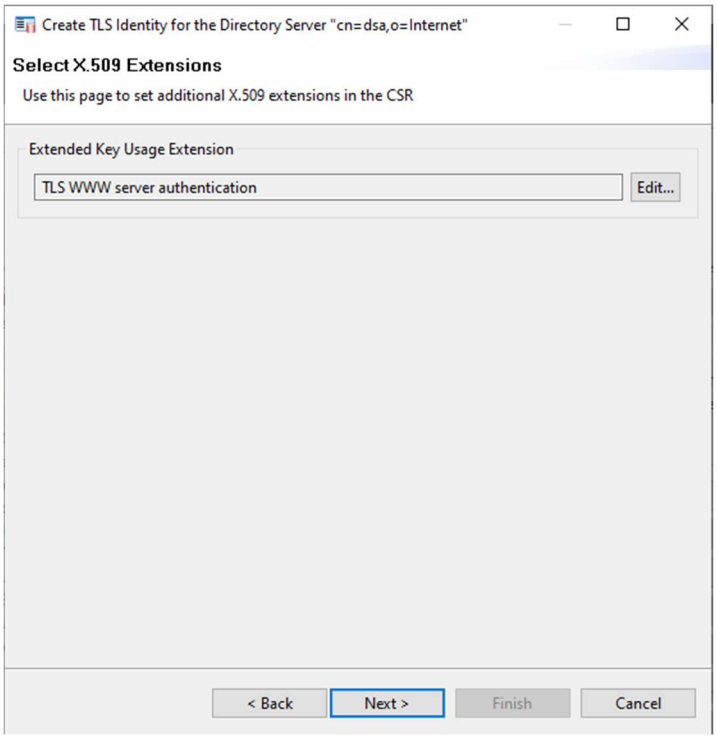
Click “Next>”.

M-Vault TLS Configuration



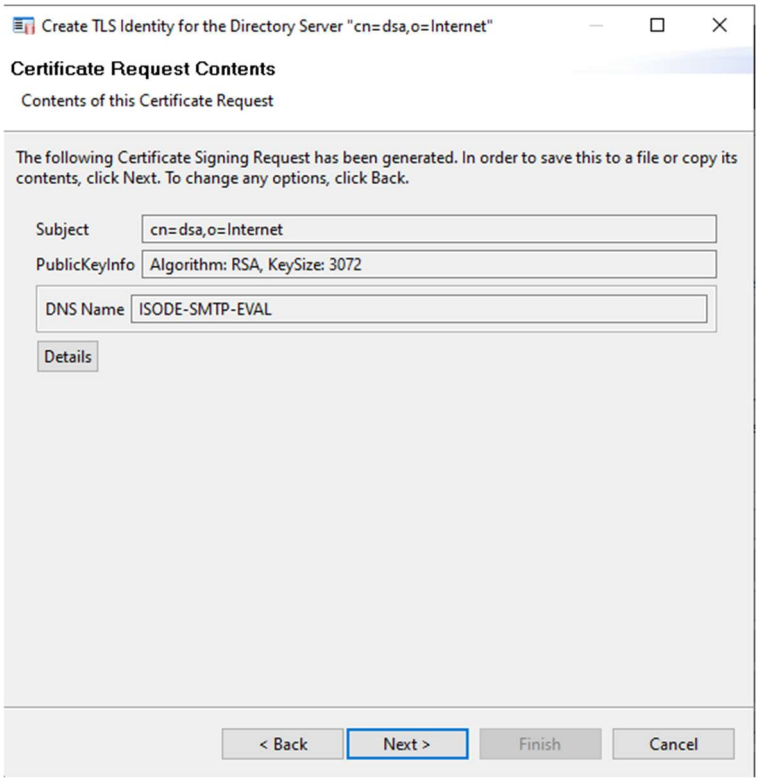
Accept the defaults, Click “Next>”.

M-Vault TLS Configuration



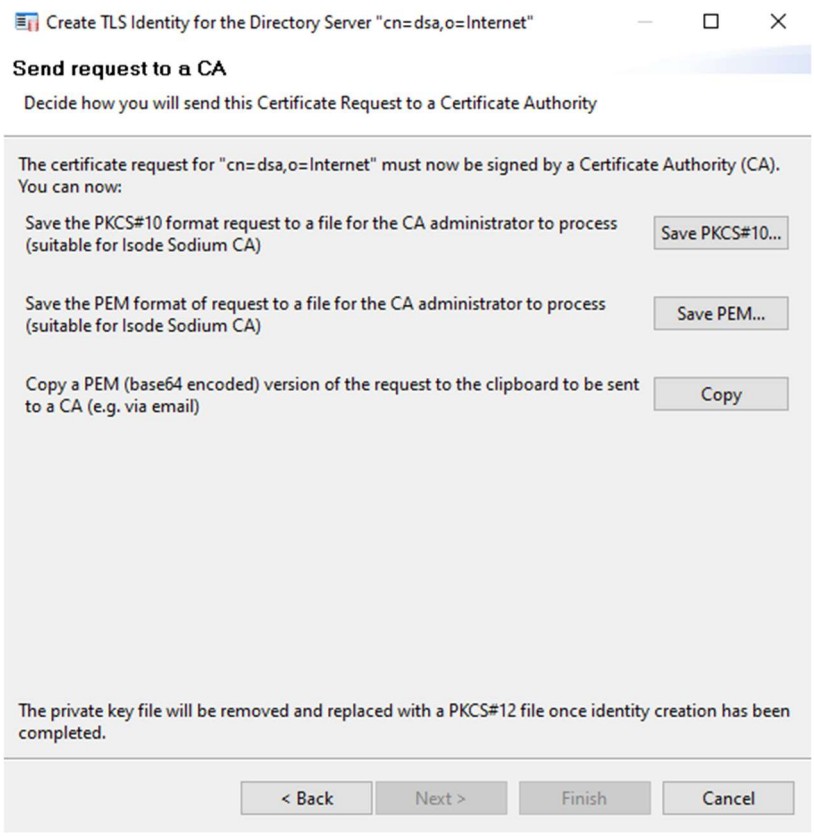
Click “Next>”.

M-Vault TLS Configuration



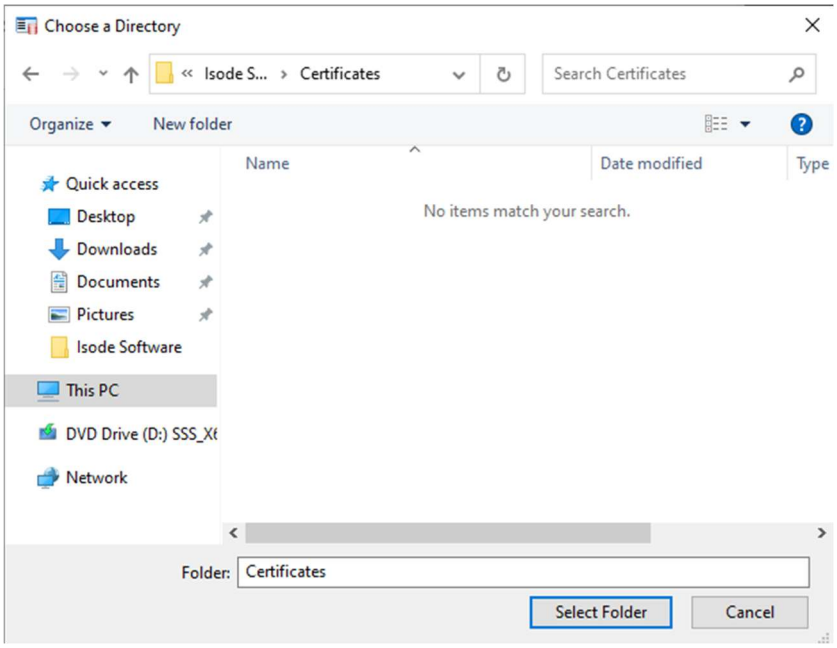
Click “Next>”.

M-Vault TLS Configuration



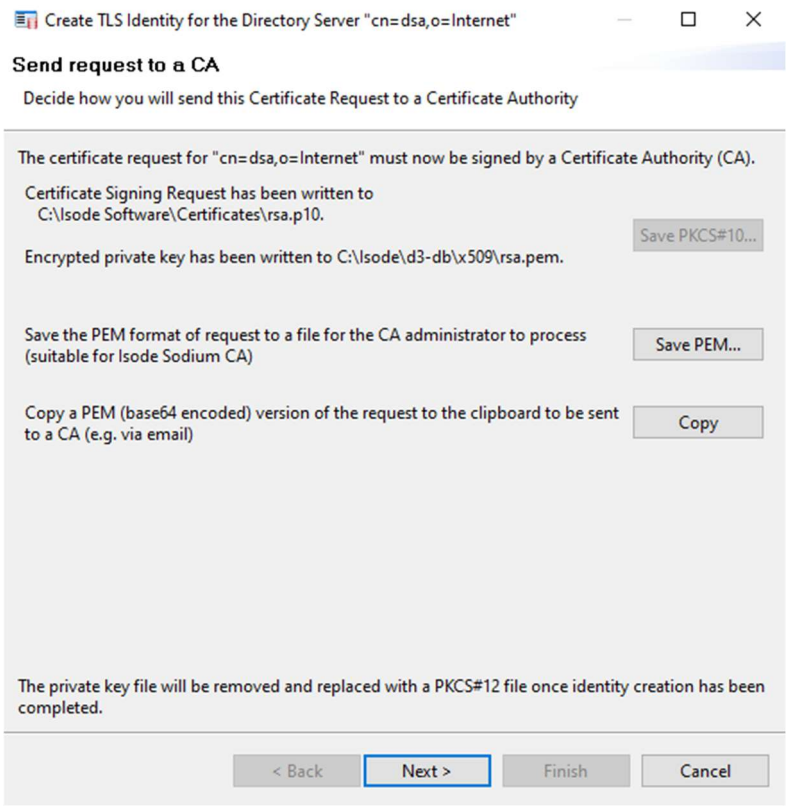
Click "Save PKCS10..."

M-Vault TLS Configuration



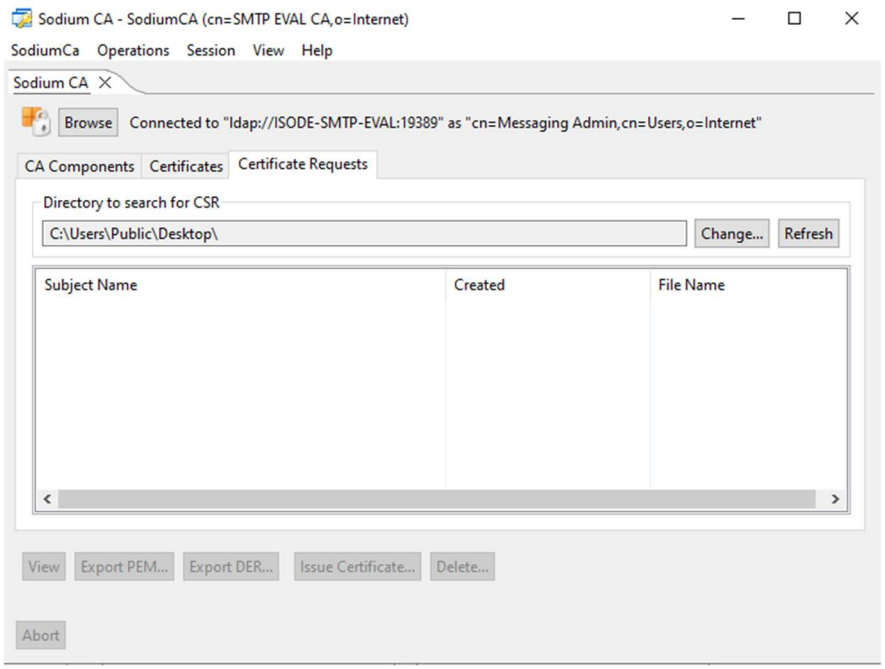
Browse to your Certificates Folder and Click "Select Folder".

M-Vault TLS Configuration



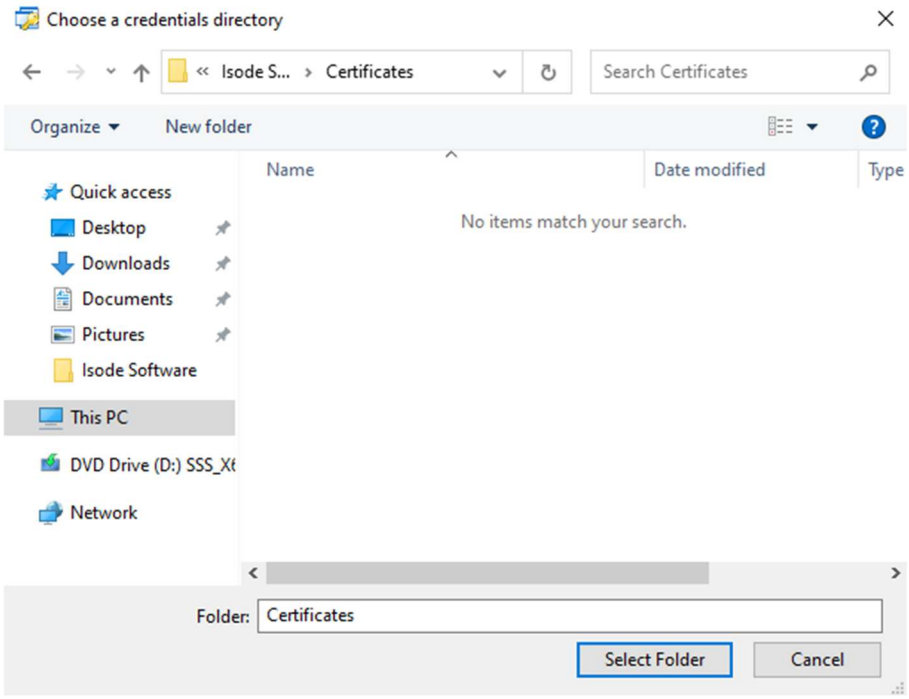
Now we return to Sodium CA.

Sodium CA Issue Certificate



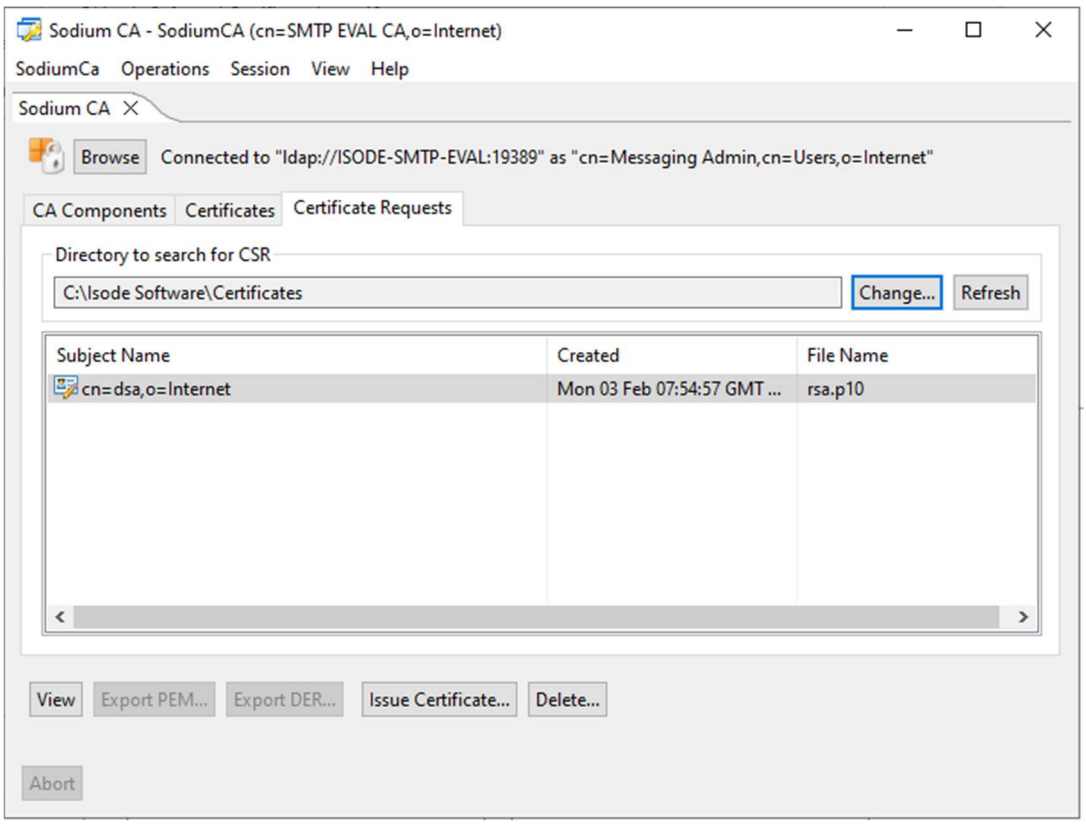
Select the Certificate Requests Tab and Click “Change…” for the CSR Folder.

Sodium CA Issue Certificate



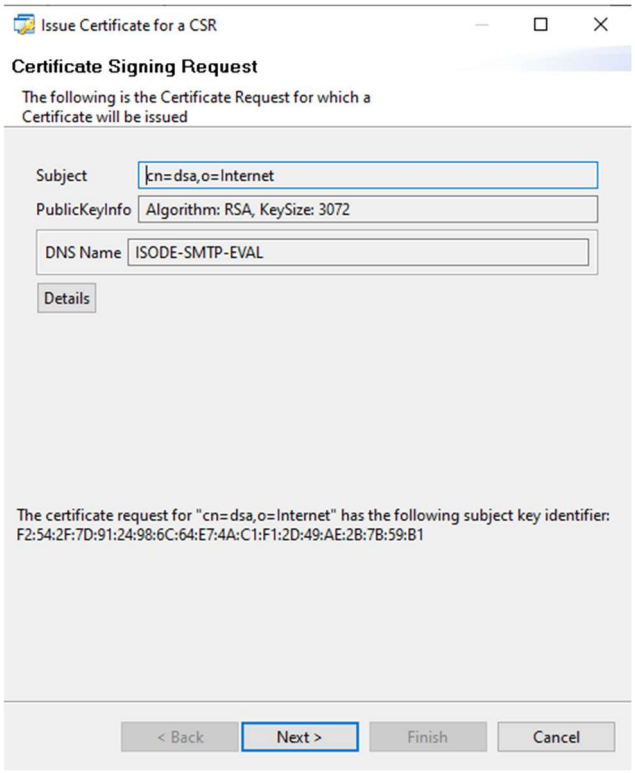
Browse to your Certificates Folder and Click “Select Folder”.

Sodium CA Issue Certificate



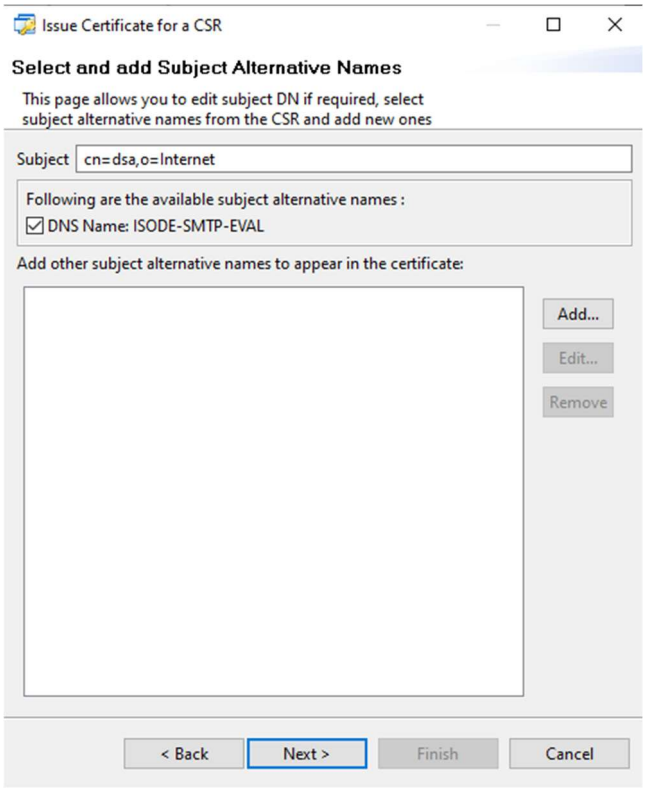
You should see your Certificate request there, select it and click “Issue Certificate…”.

Sodium CA Issue Certificate



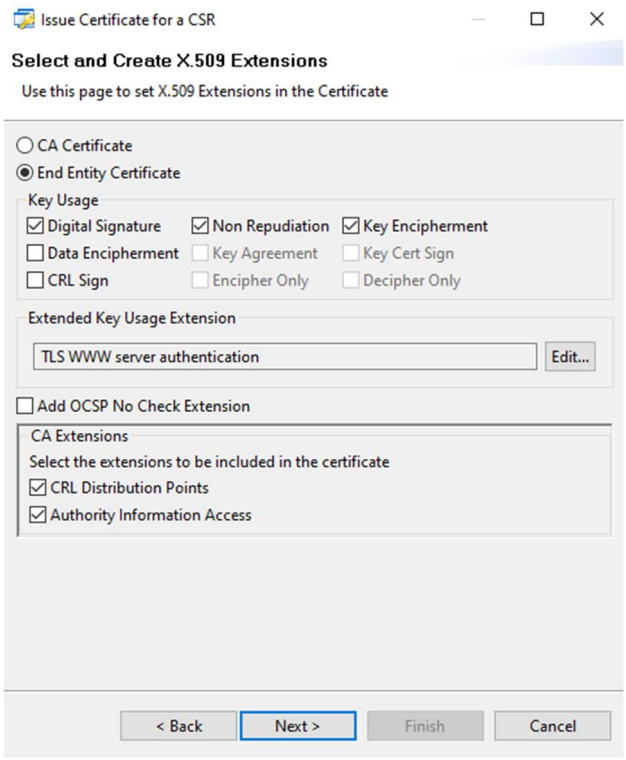
Click “Next>”.

Sodium CA Issue Certificate



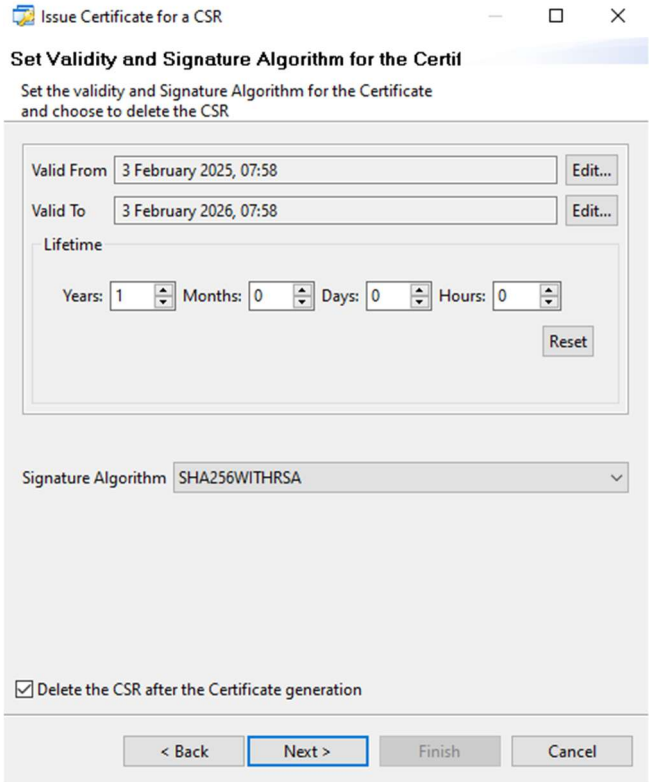
Click “Next>”.

Sodium CA Issue Certificate



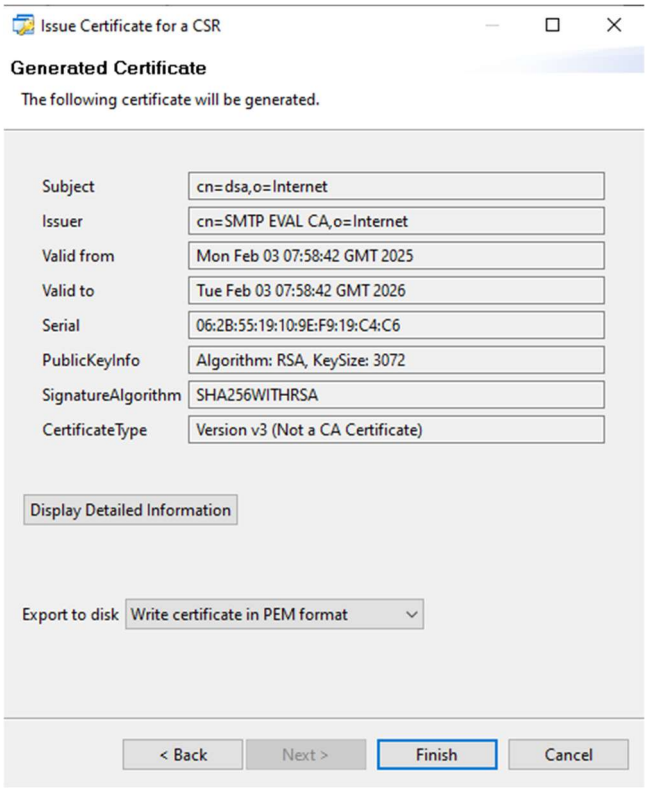
Click “Next>”.

Sodium CA Issue Certificate



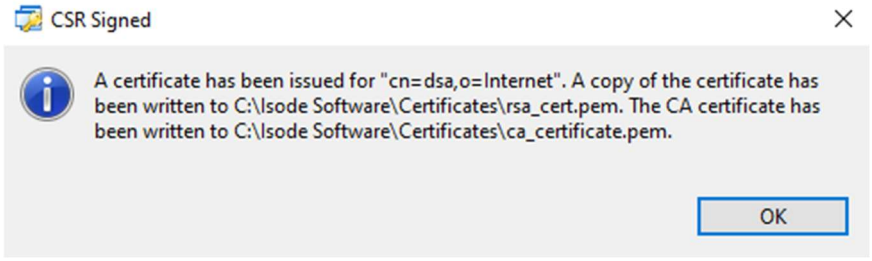
Accept the defaults, Click “Next>”.

Sodium CA Issue Certificate



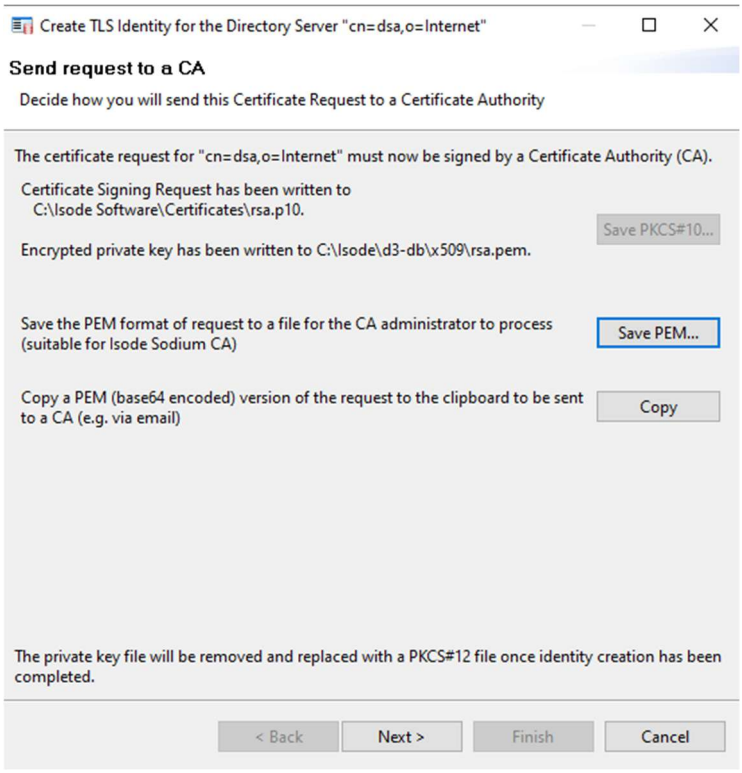
Click “Finish”.

Sodium CA Issue Certificate



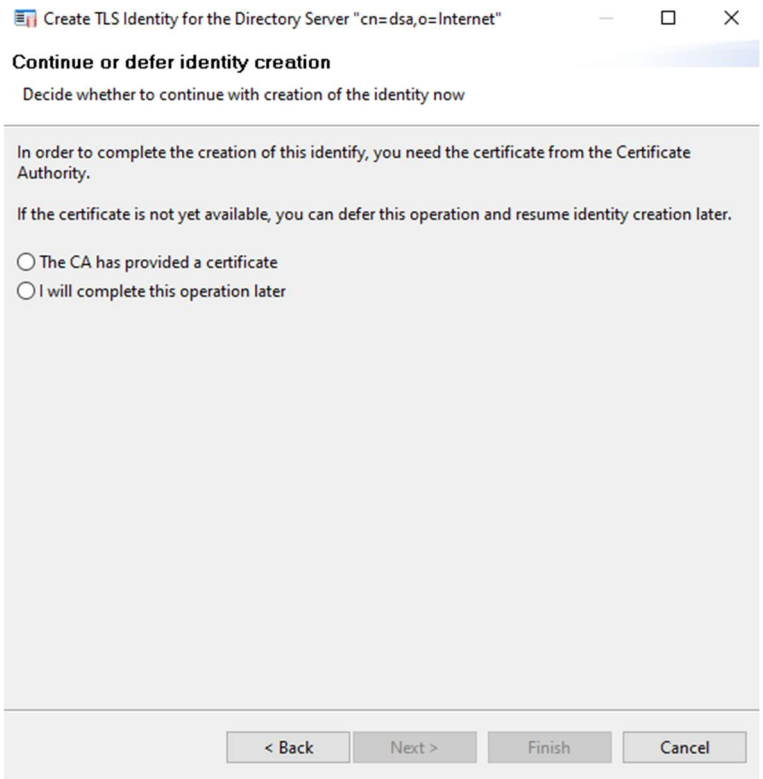
Click “OK” and return to M-Vault Console.

M-Vault Console Certificate Import



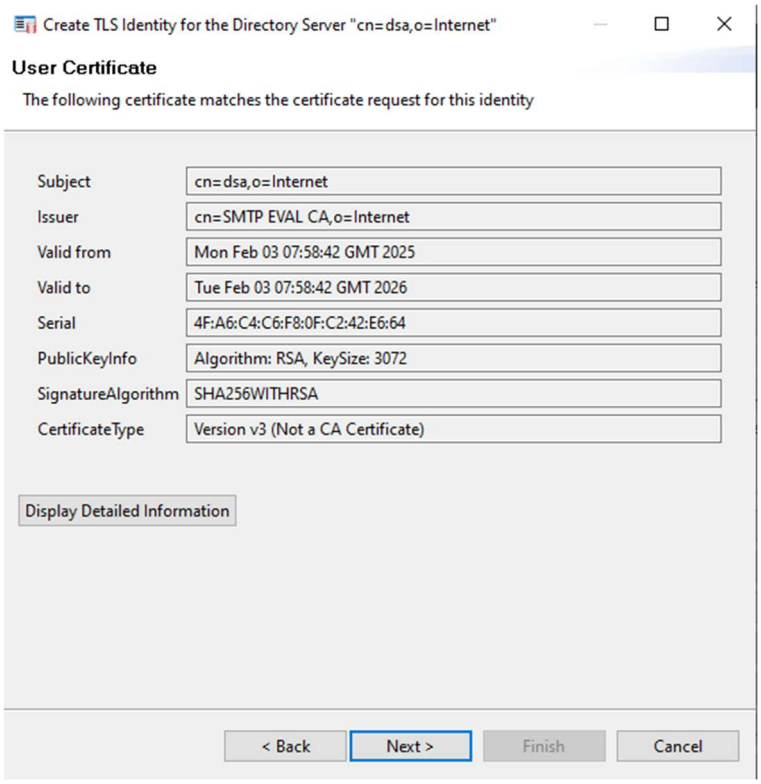
Select "Next>"

M-Vault Console Certificate Import



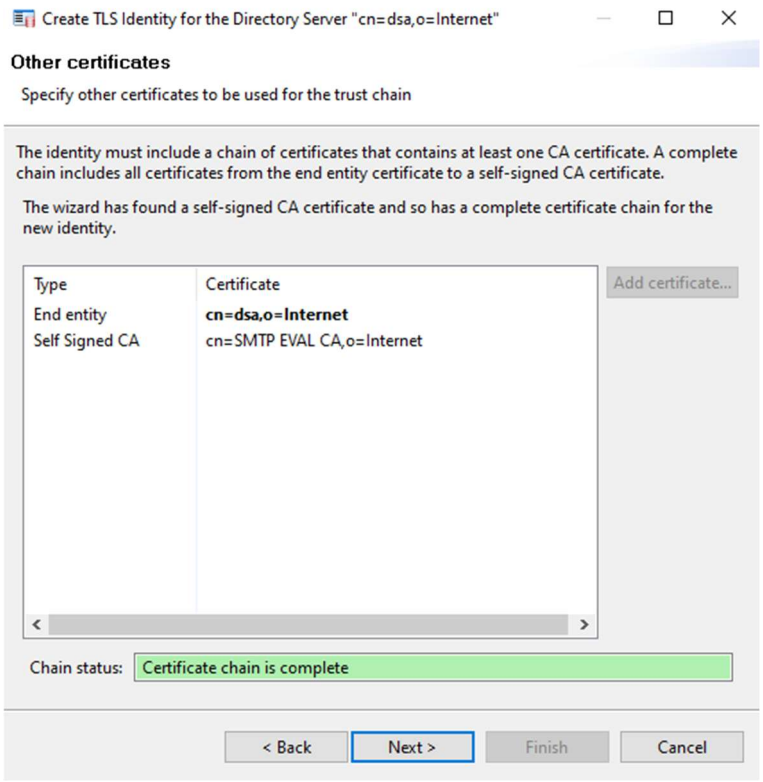
Select the CA has provided a certificate and Click "Next>".

M-Vault Console Certificate Import



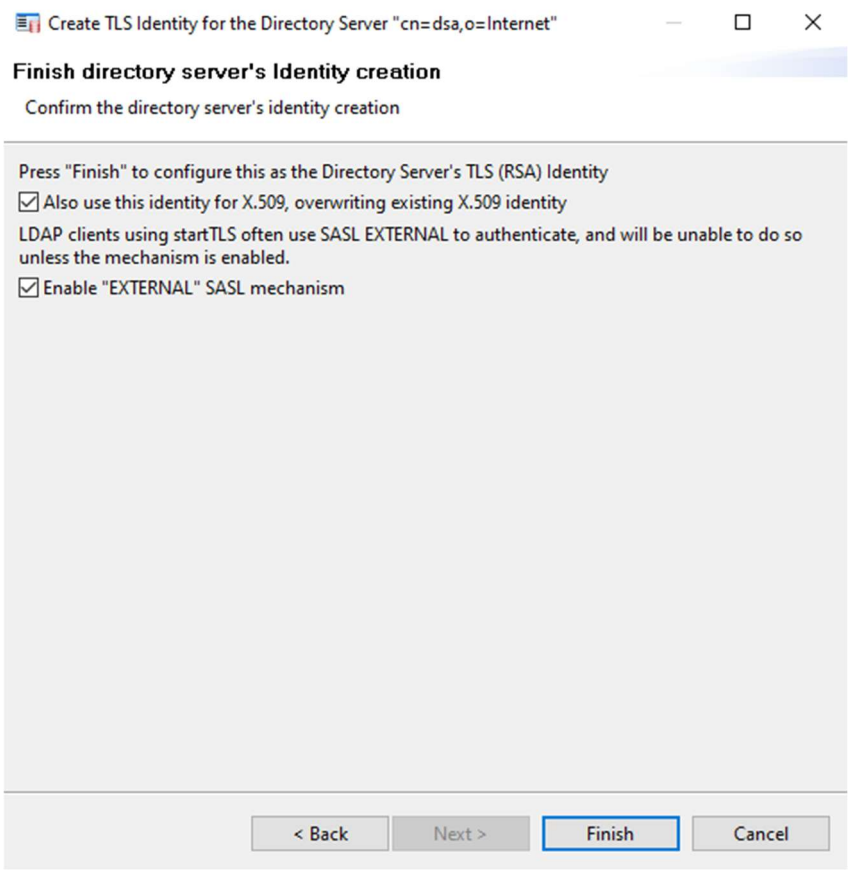
Click “Next>”.

M-Vault Console Certificate Import



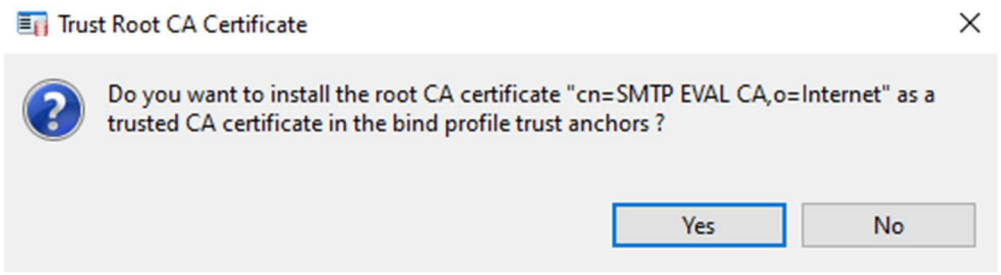
Click “Next>”.

M-Vault Console Certificate Import



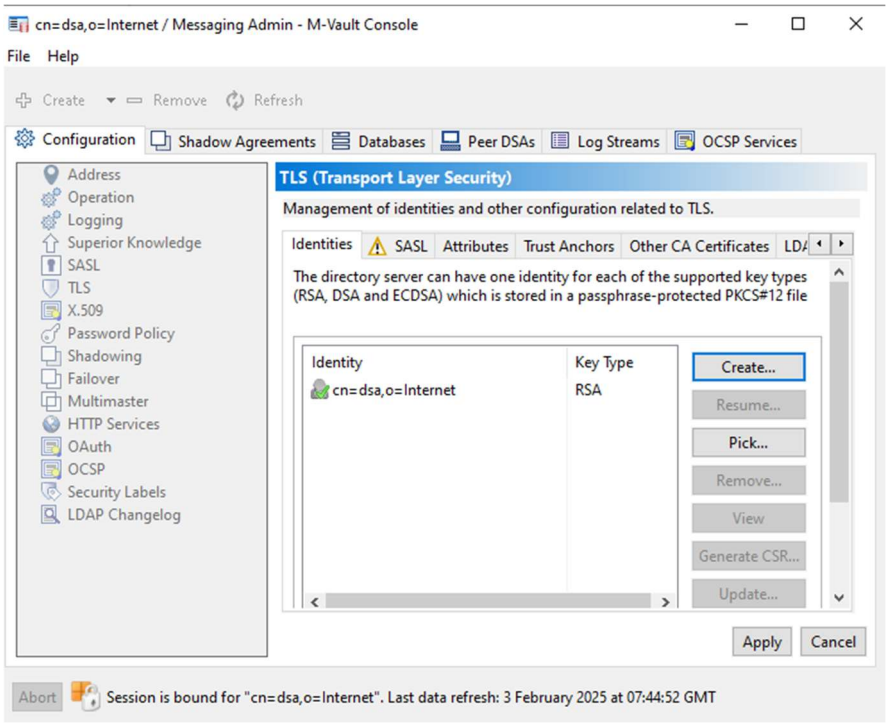
Uncheck the “Enable “EXTERNAL” SASL mechanism”. Click “Finish”.

M-Vault Console Certificate Import



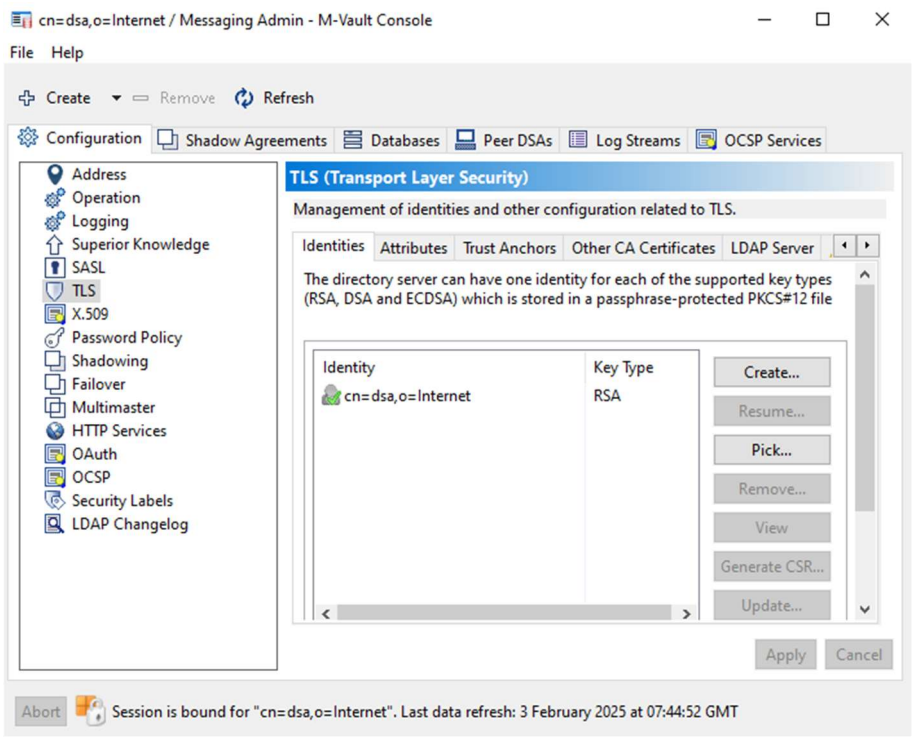
Click “Yes”.

M-Vault Console Certificate Import



Click “Apply”

M-Vault Console Certificate Import



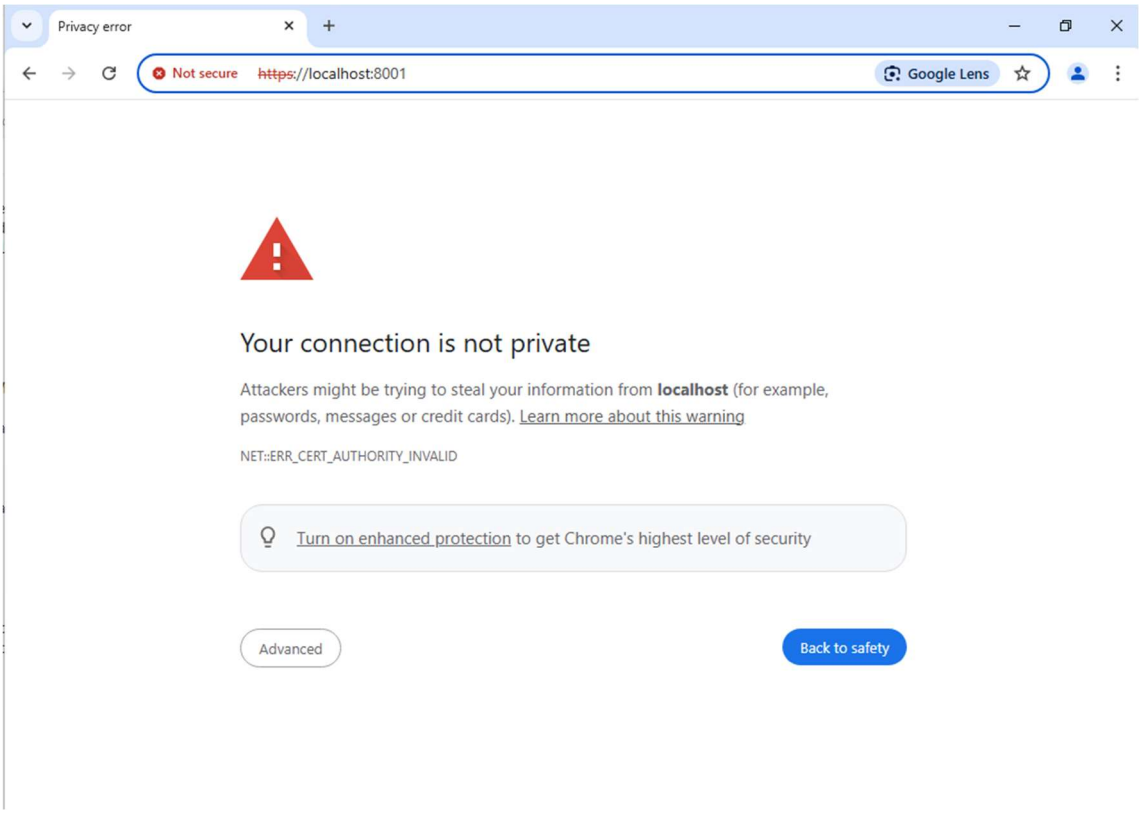
Your M-Vault Server now has TLS configured and you are ready to proceed to configuring Users with Cobalt.

Provisioning Users with Cobalt

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

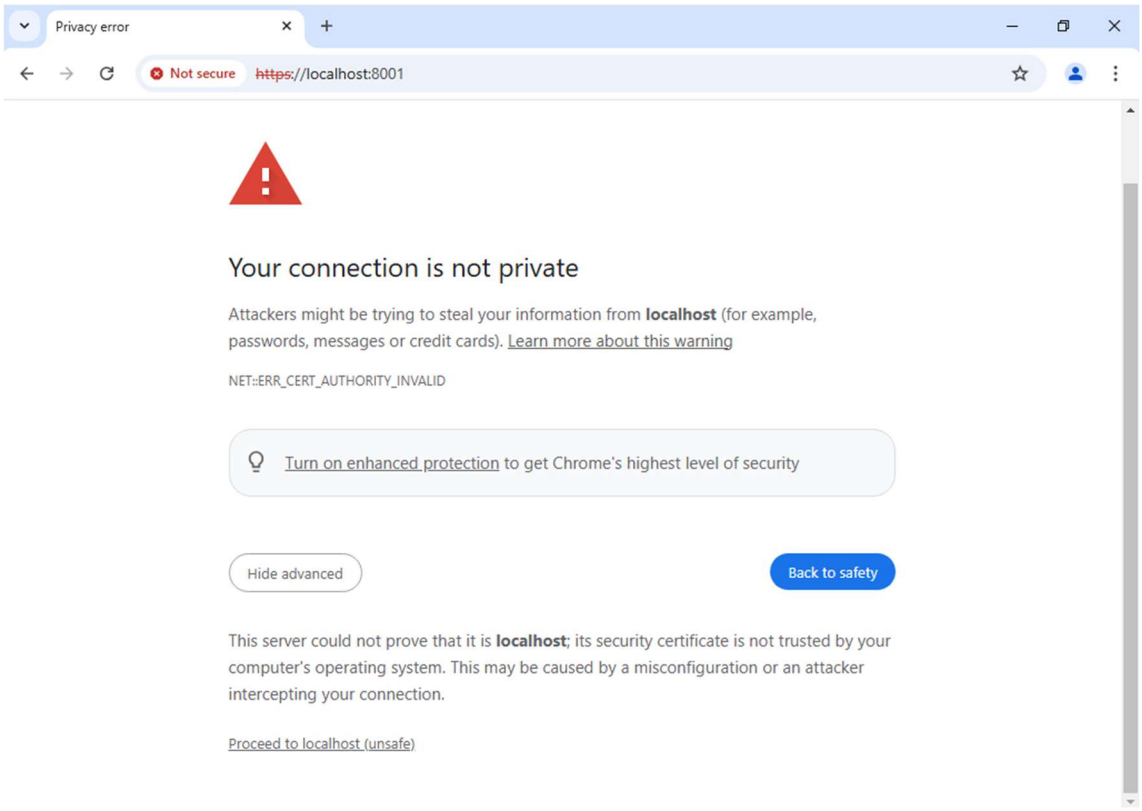
https://localhost:8001

Cobalt Initial Setup.



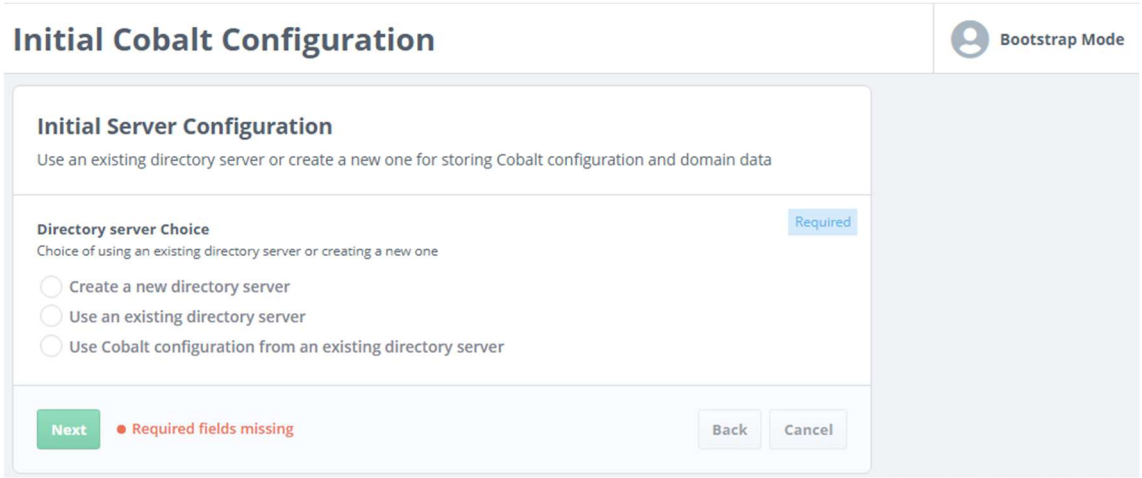
Click “Advanced”.

Cobalt Initial Setup.



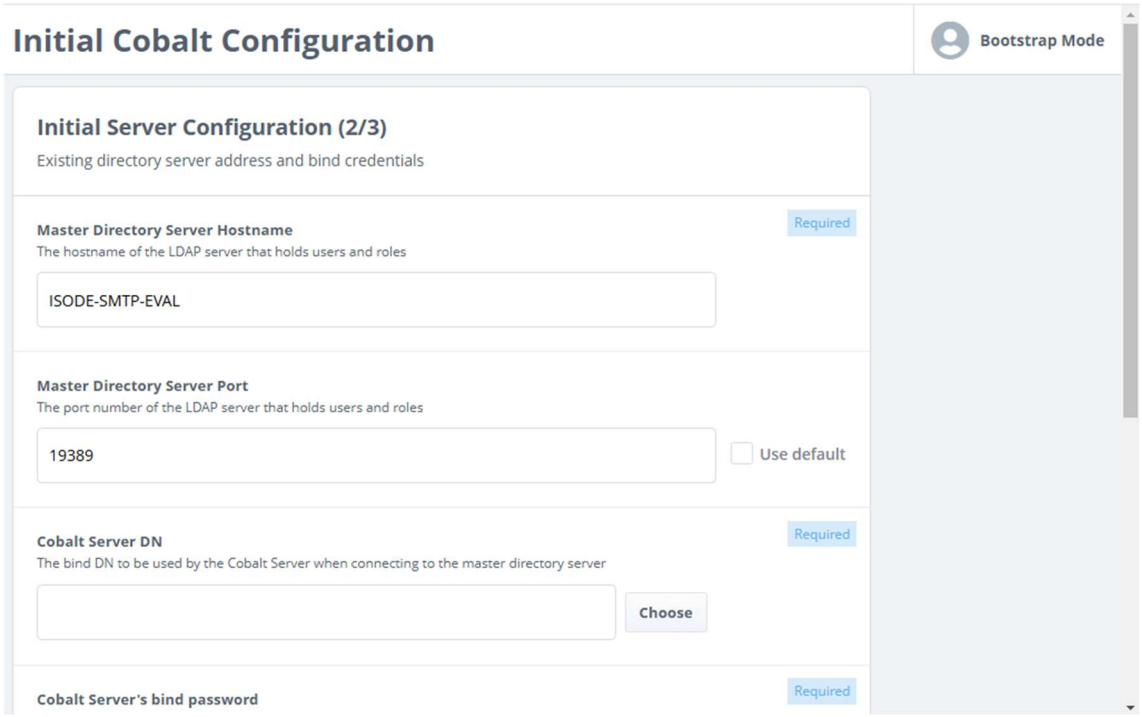
Click "Proceed to localhost (unsafe)".

Cobalt Initial Setup.



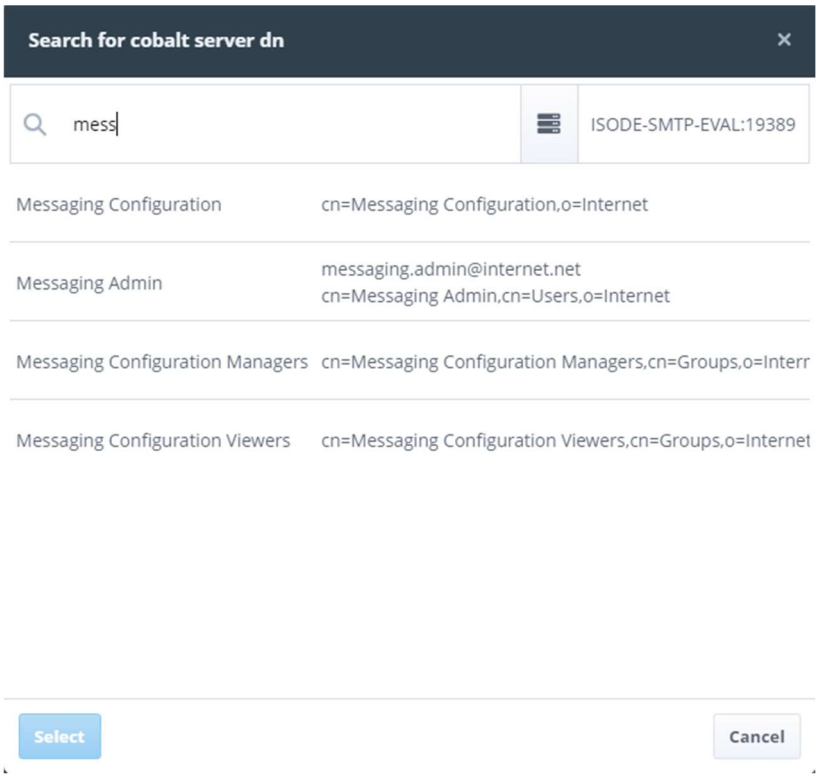
Select "Use an existing directory server".

Cobalt Initial Setup.



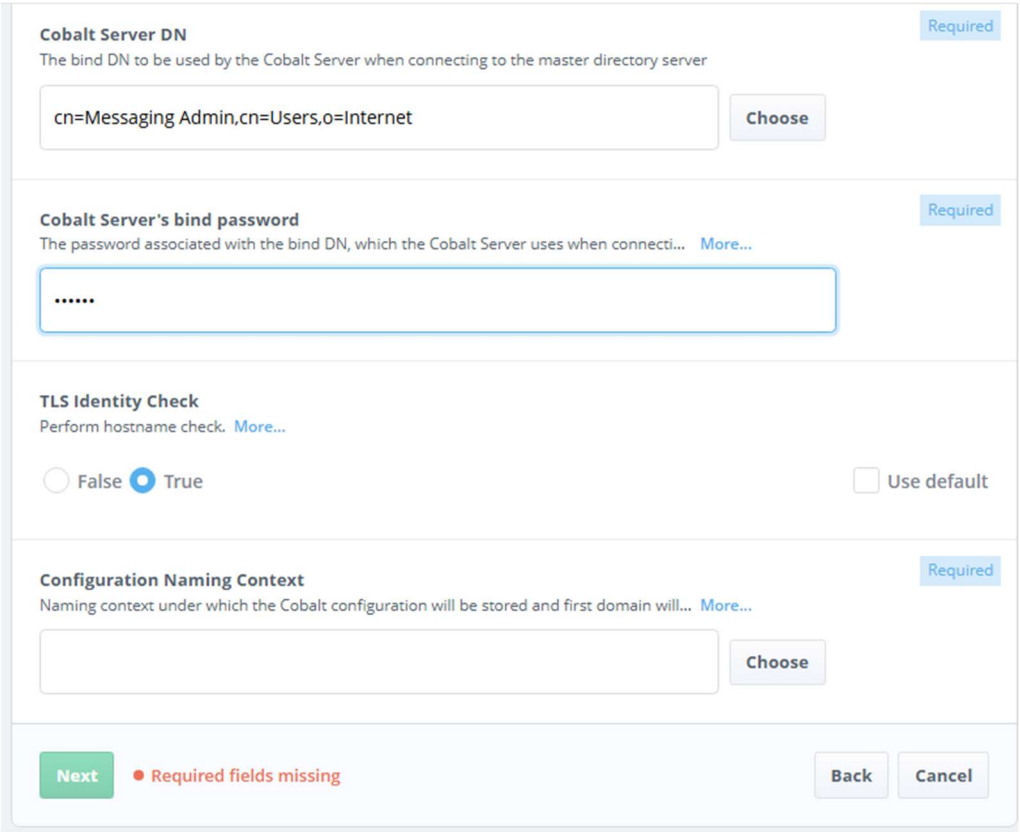
Check the “Hostname” matches your server. Next to the Cobalt Server DN Click “Choose”.

Cobalt Initial Setup.



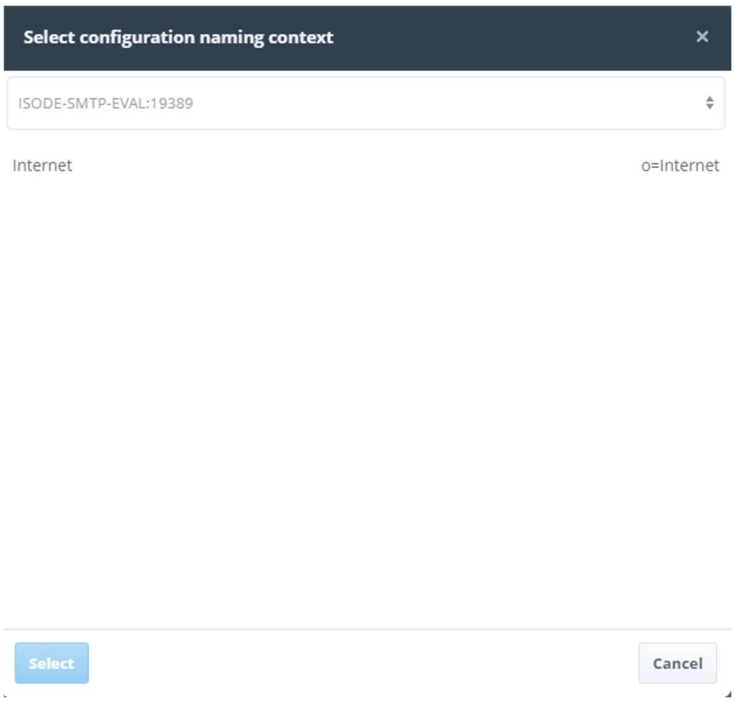
Start typing “mess” and then Select “Messaging Admin”.

Cobalt Initial Setup.



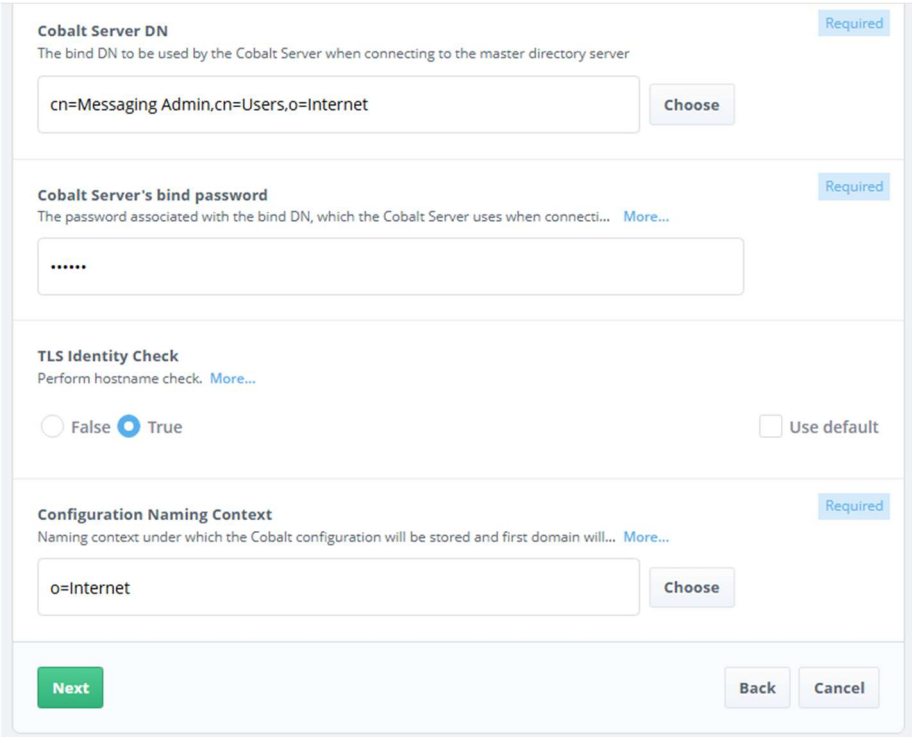
Enter the Messaging Admin Password and Click Choose next to the Configuration Naming Context.

Cobalt Initial Setup.



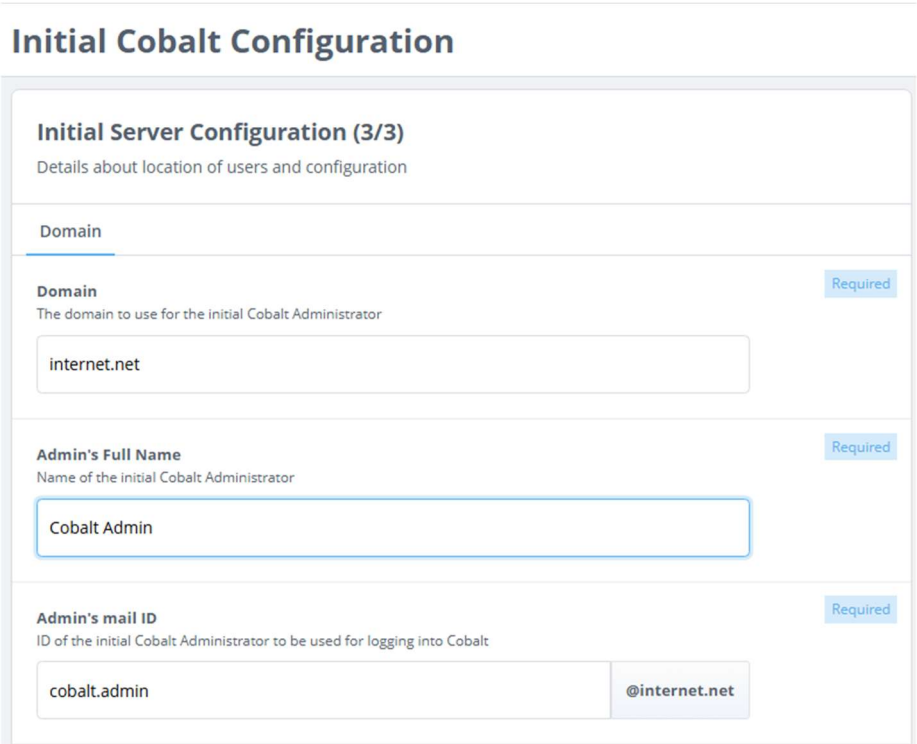
Select “Internet” and Click “Select”.

Cobalt Initial Setup.



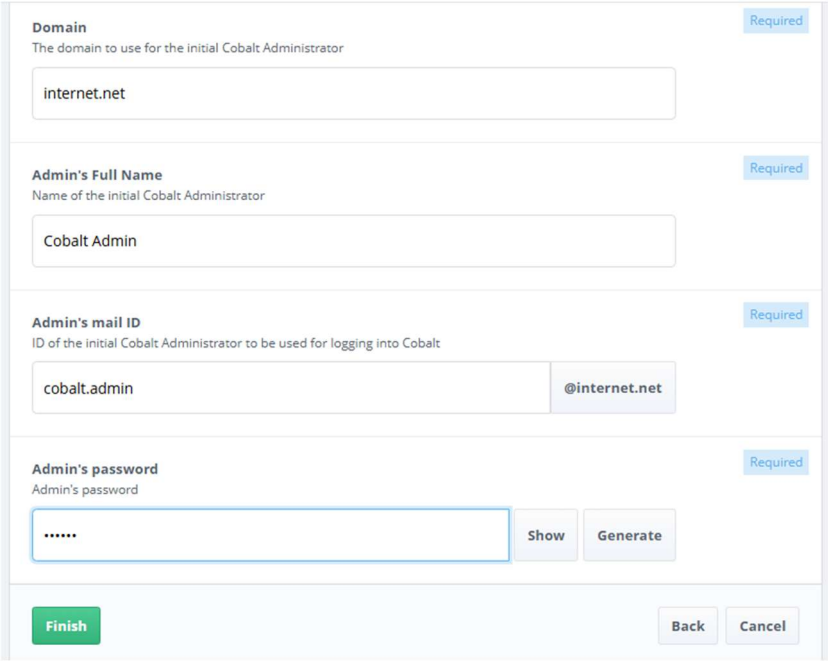
Click "Next".

Cobalt Initial Setup.



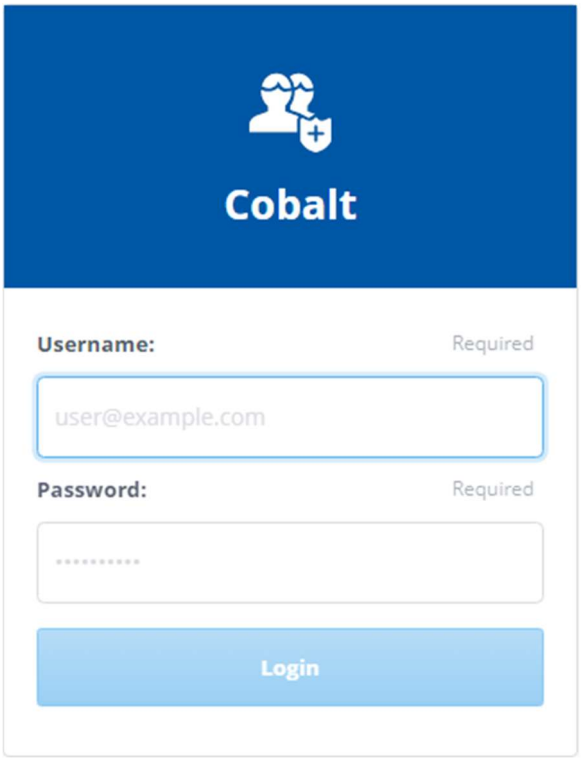
On this screen enter "internet.net" for the domain and your choice for the Cobalt Admin Name. The Admin's mail ID will auto-populate. Then scroll down.

Cobalt Initial Setup.



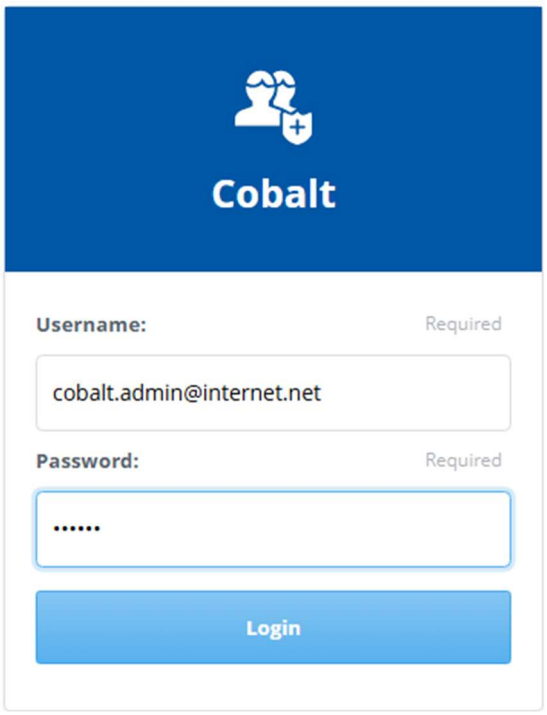
Enter a Password of your choice (again we suggest "secret") and Click "Show" to check it. Then Click "Finish". The following screen will be displayed.

Cobalt Login.



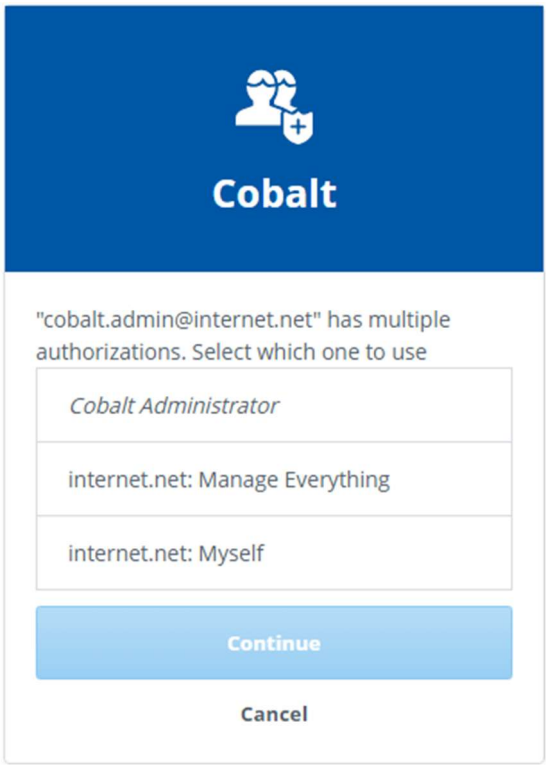
Enter the Login details you just created.

Cobalt Login.



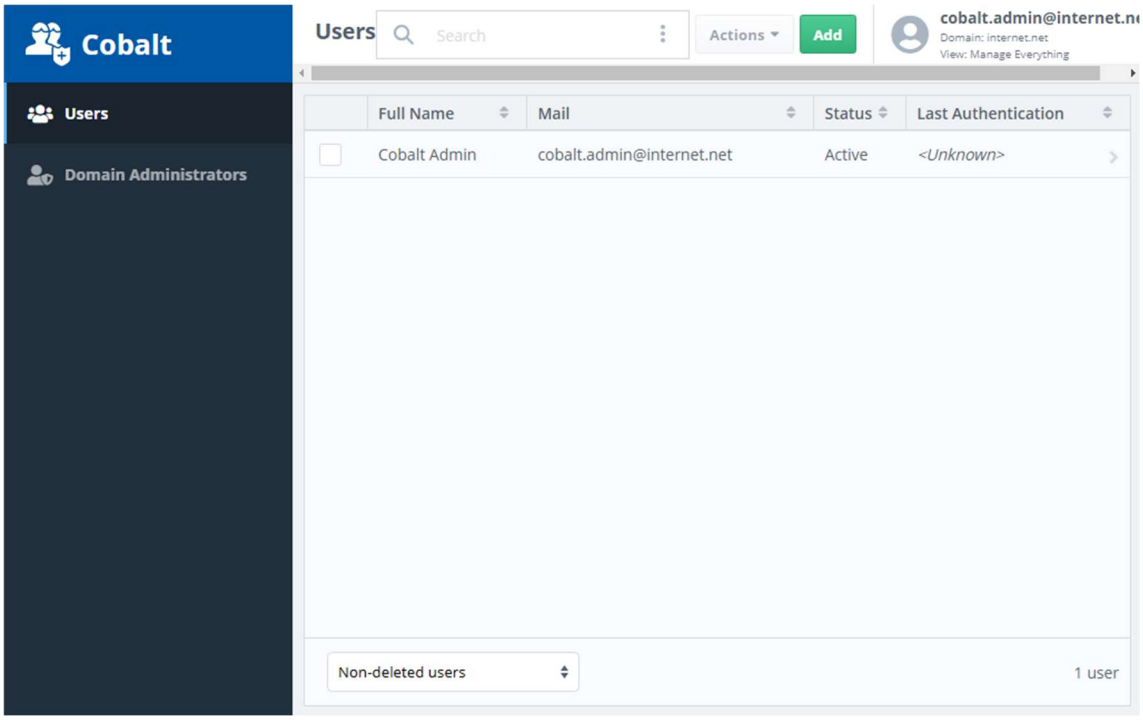
Click “Login”.

Cobalt Login.



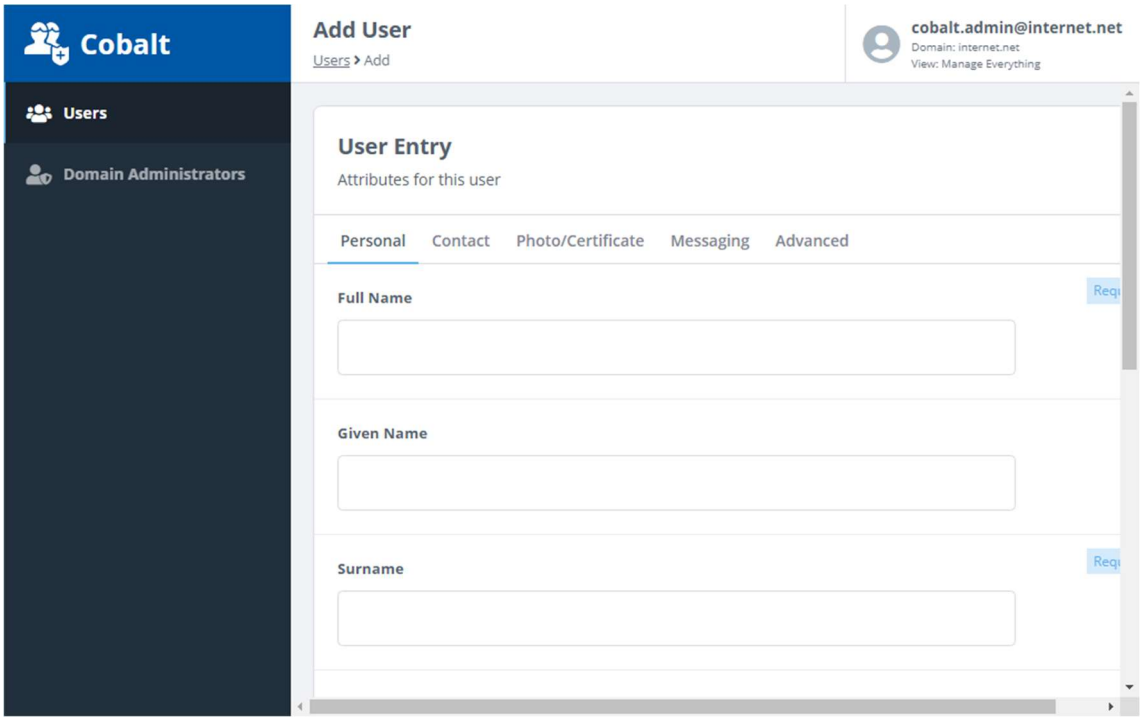
Select “internet.net: Manage Everything”, Click “Continue”.

Cobalt User Provisioning.



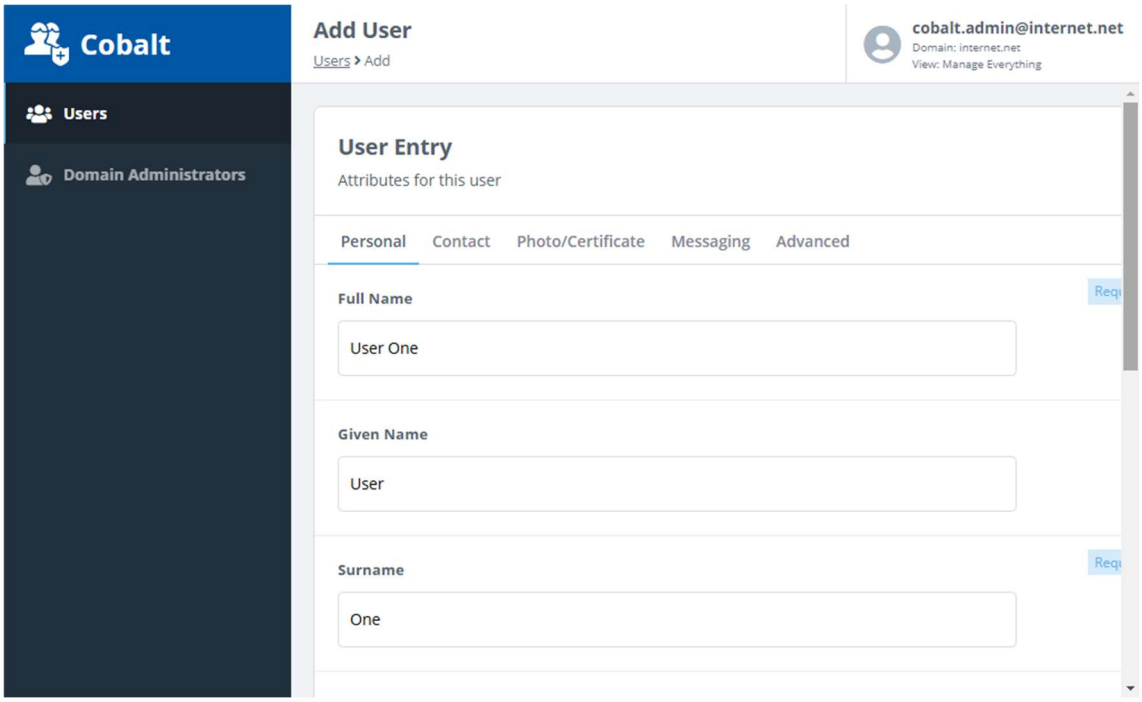
Click “Add”.

Cobalt User Provisioning.



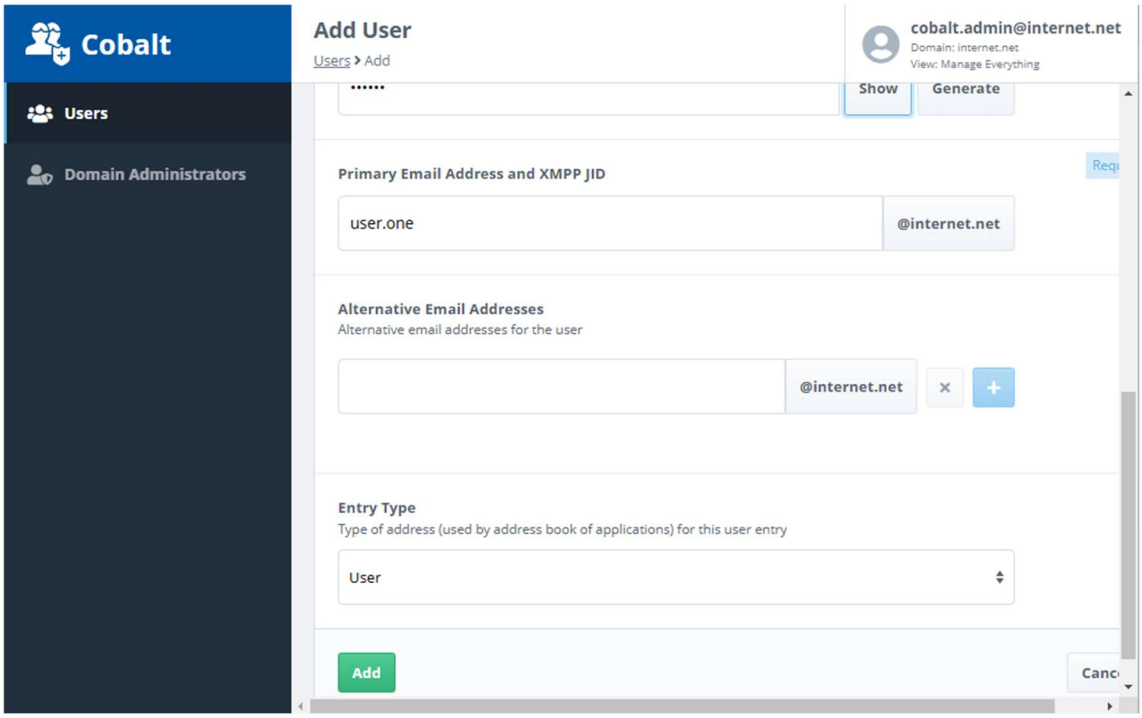
Type a Full Name, in this guide “User One”, the other fields will auto-populate.

Cobalt User Provisioning.



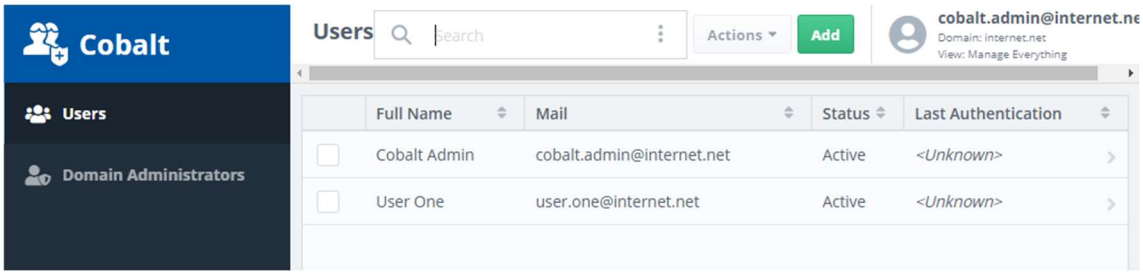
Scroll down, and enter a Password, we suggest “secret”.

Cobalt User Provisioning.



Click “Add”.

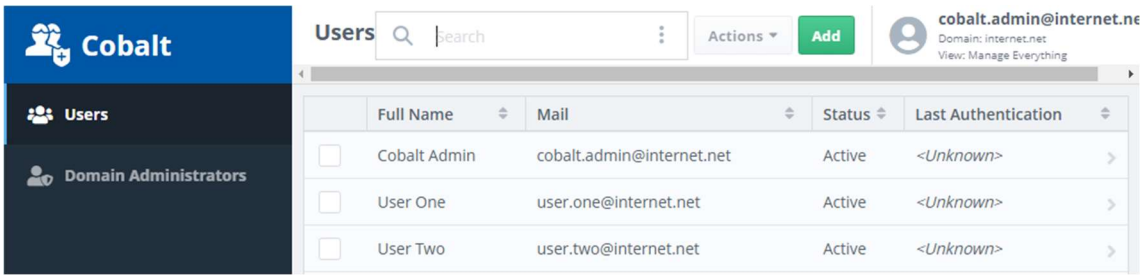
Cobalt User Provisioning.



User One has now been successfully added.

Repeat the Process for User Two.

Cobalt User Provisioning.



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.

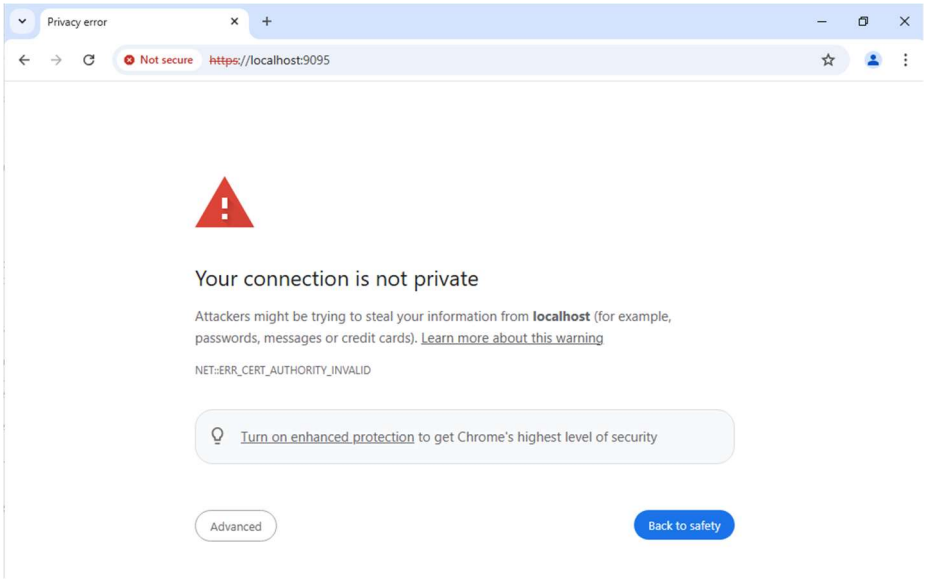
Configuring Harrier

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

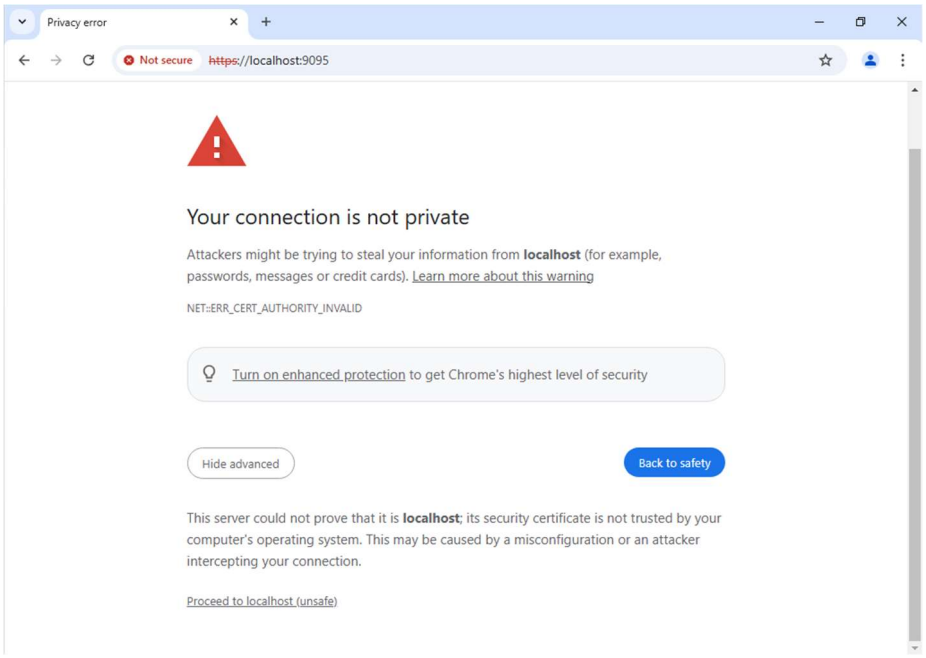
To Start configuring Harrier point your browser to https://localhost:9095 .

Initial Harrier Screen.



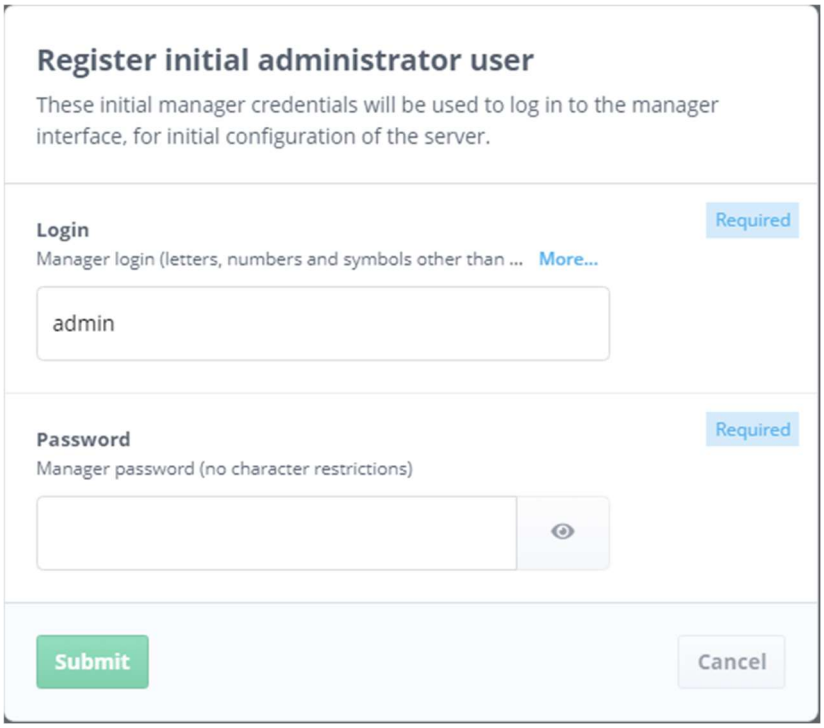
Click “Advanced”.

Initial Harrier Screen.



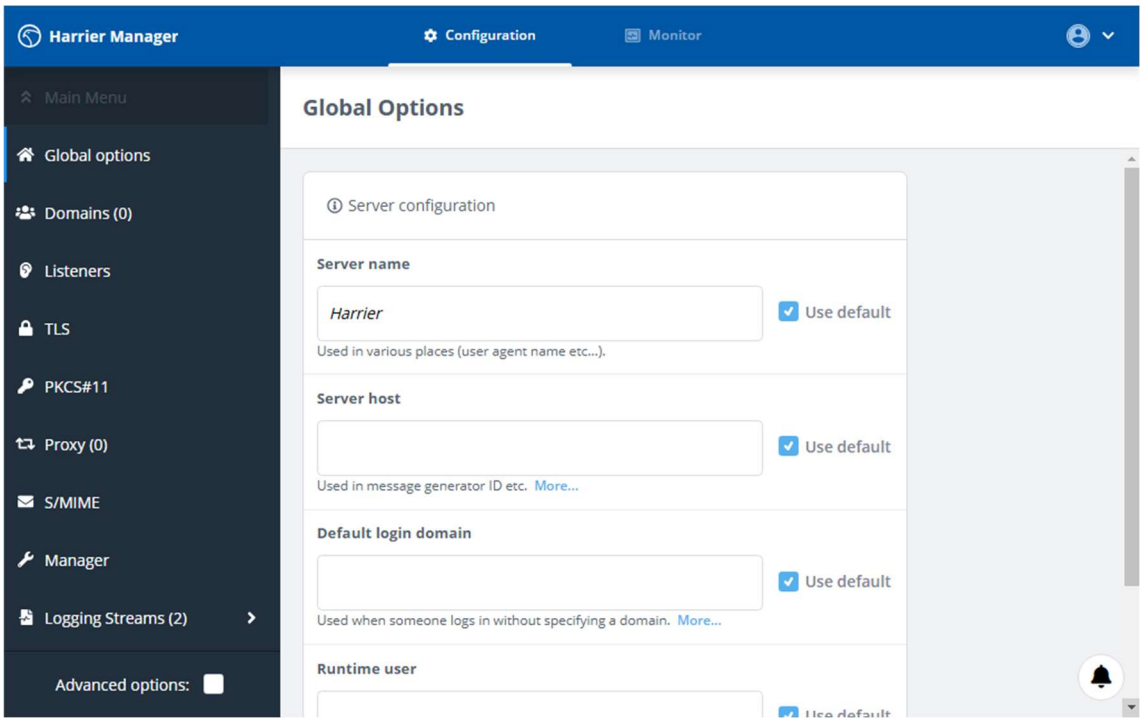
Click “Proceed to localhost (unsafe)”.

Register Initial Harrier Admin.



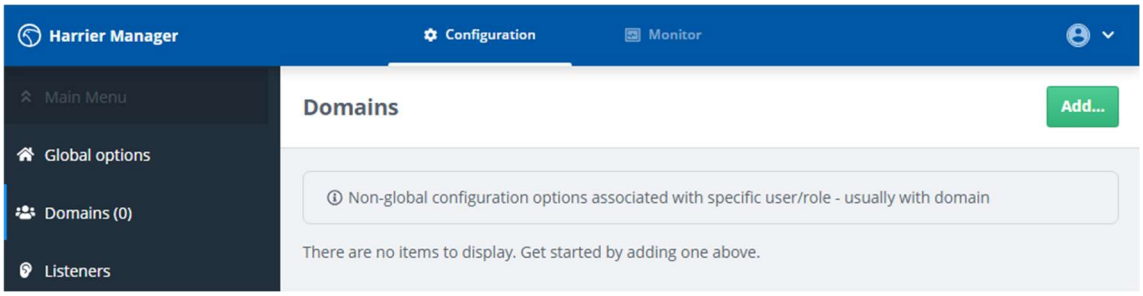
Choose a Login name of you choice or accept the default and a password (again we suggest "secret"). Click "Submit". The follwing screen is displayed

Initial Harrier Screen.



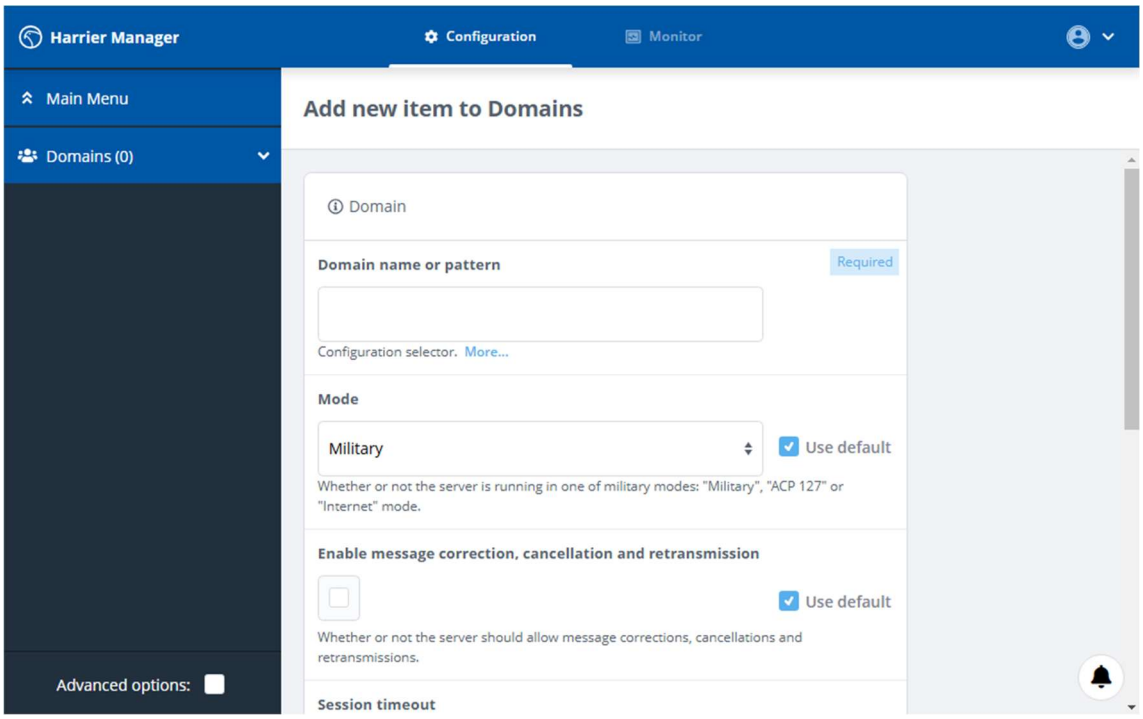
From the left-hand menu select "Domains".

Harrier Domain Configuration.



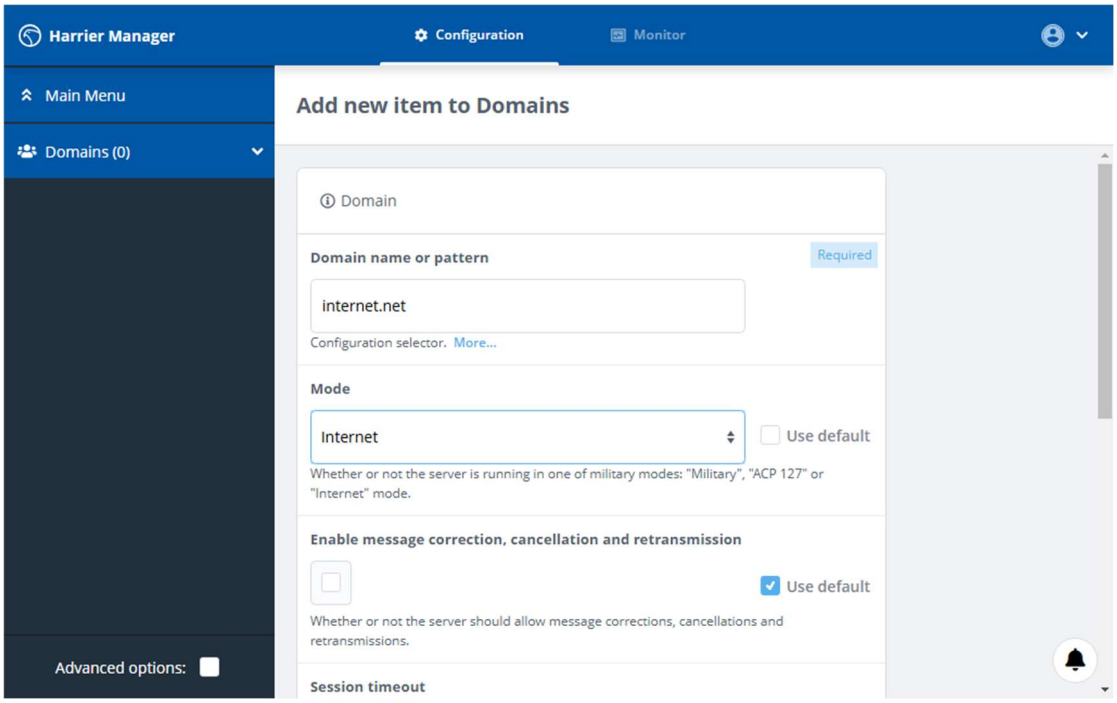
Click “Add...”

Harrier Domain Configuration.



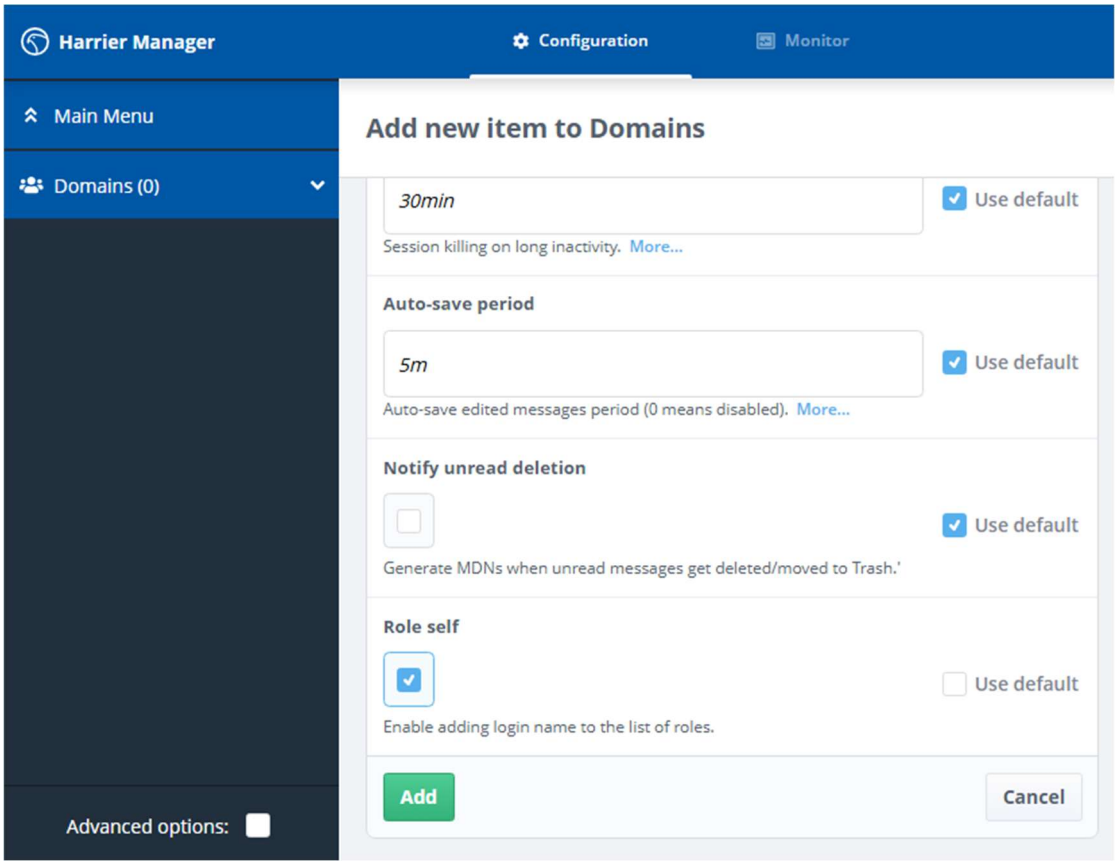
Enter “internet.net” for the “Domain name or pattern” and select “Internet” for the “Mode”.

Harrier Domain Configuration.



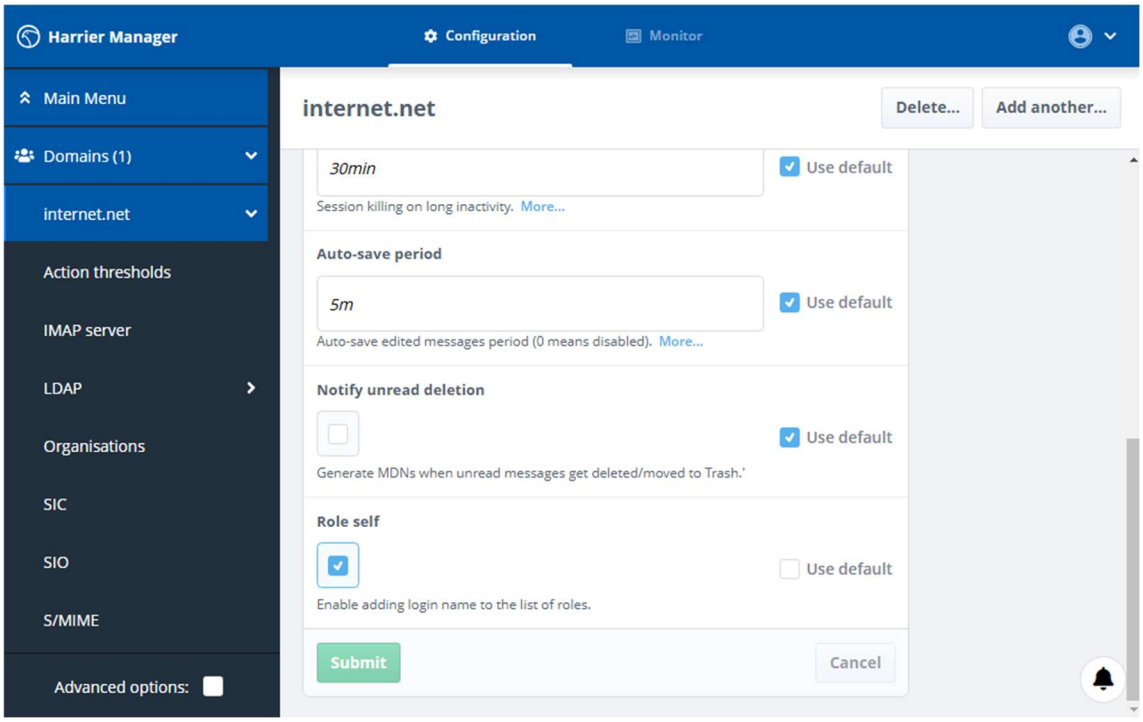
Scroll down.

Harrier Domain Configuration.



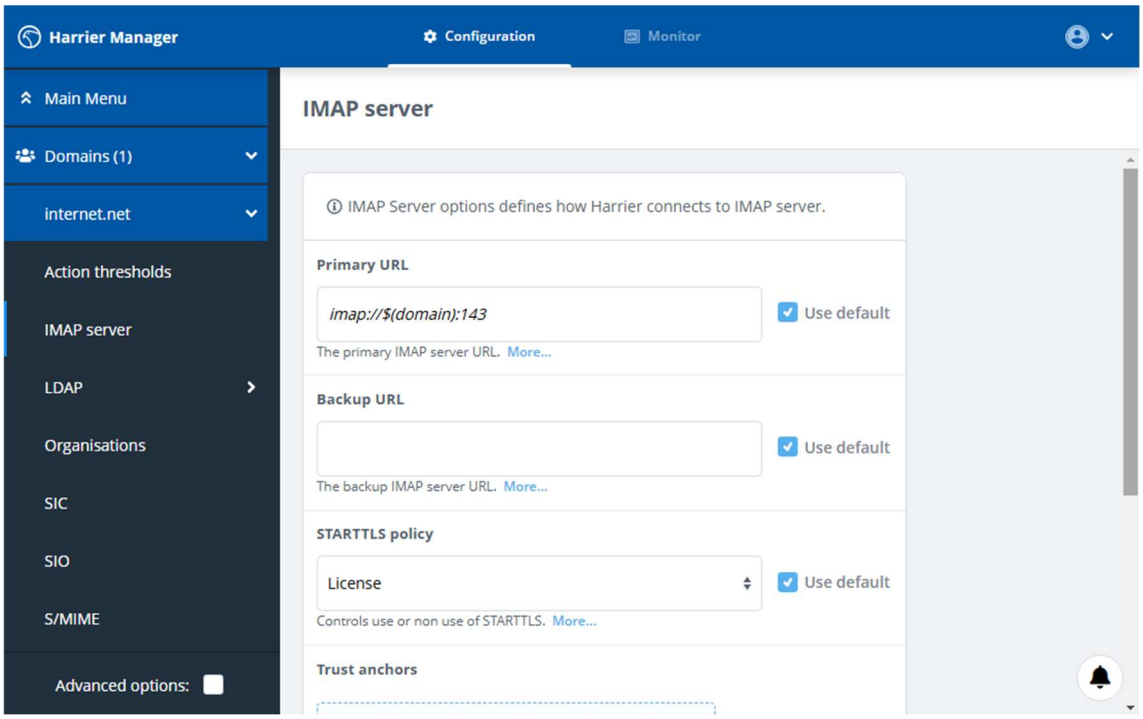
Make sure “Role self” is checked and click “Add”.

Harrier Domain Configuration.



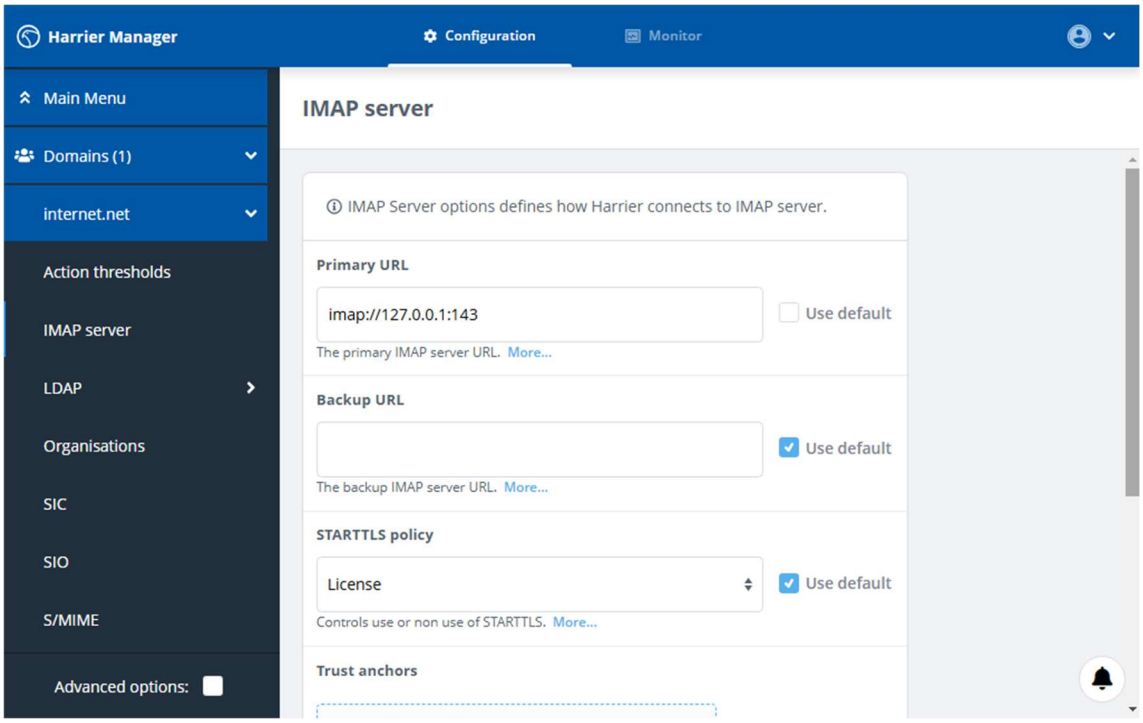
From the left-hand menu select “IMAP Server”.

Harrier Domain Configuration – IMAP Server.



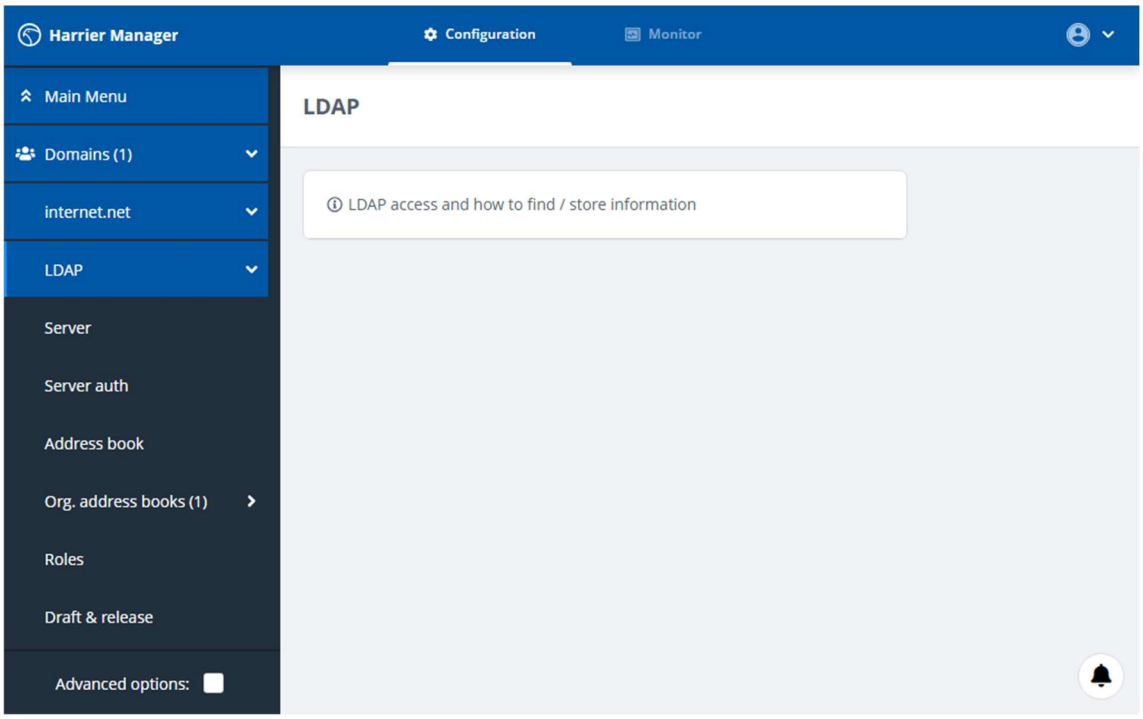
Enter “imap://127.0.0.1:143” for the “Primary URL”.

Harrier Domain Configuration – IMAP Server.



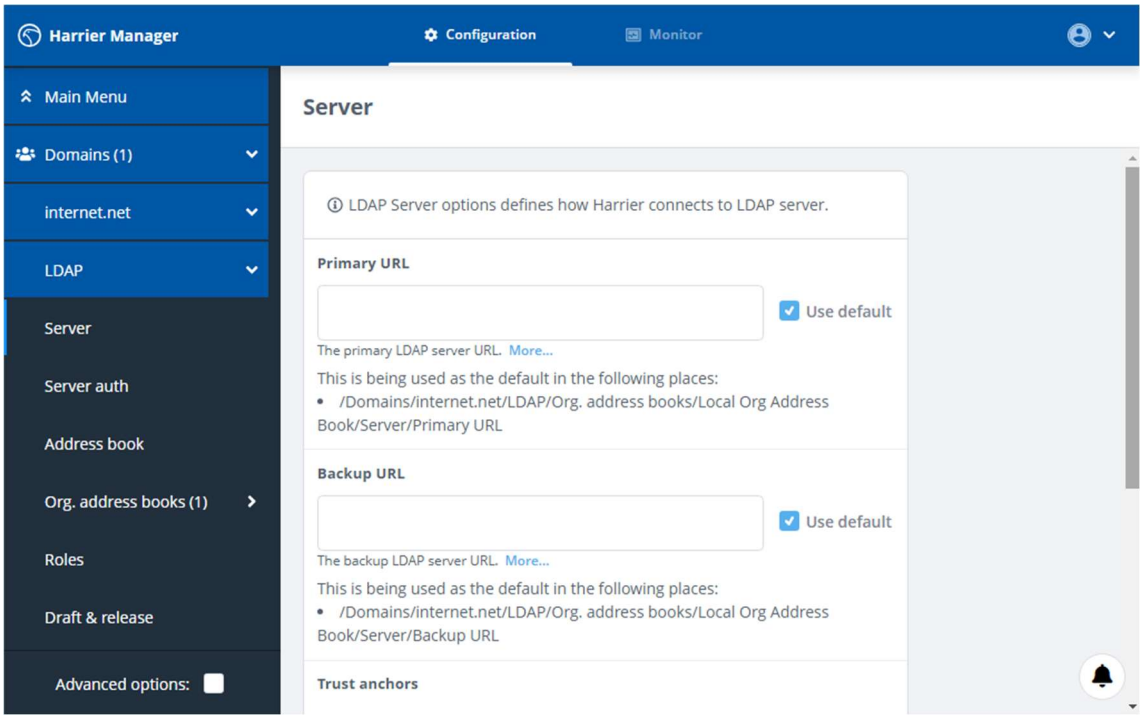
Scroll down, Click Submit and then from the left-hand menu select “LDAP”.

Harrier Domain Configuration – LDAP Server.



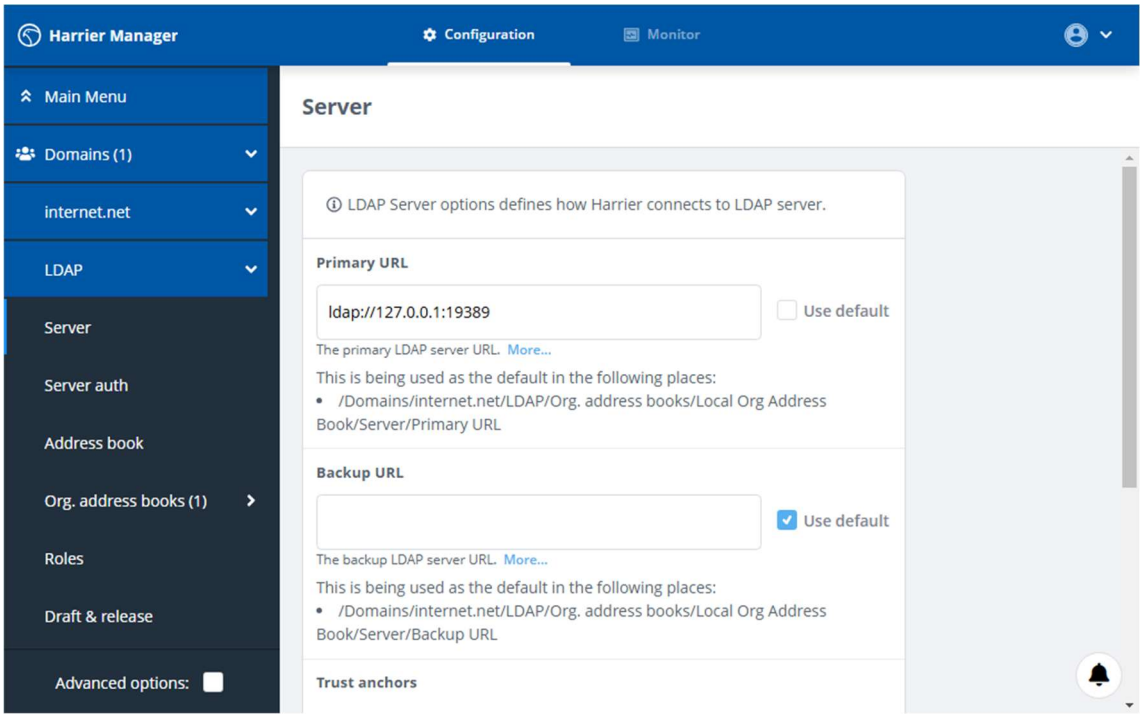
From the left-hand menu select “Server”.

Harrier Domain Configuration – LDAP Server.



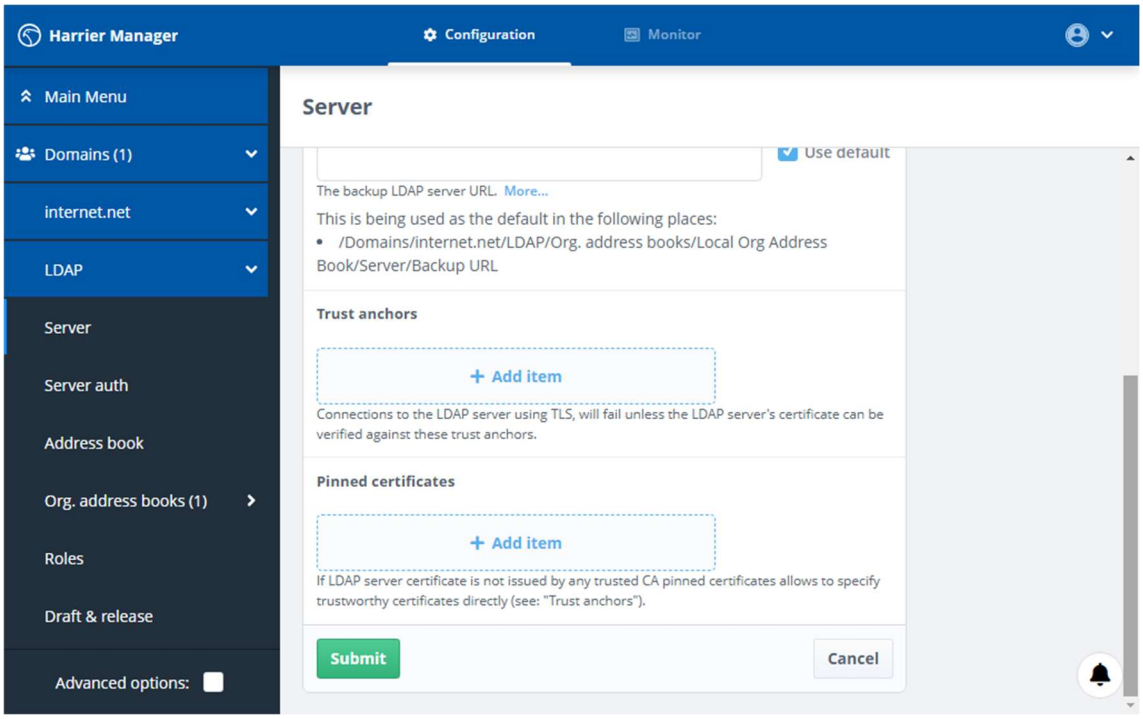
Enter "ldap://127.0.0.1:19389" for the "Primary URL".

Harrier Domain Configuration – LDAP Server.



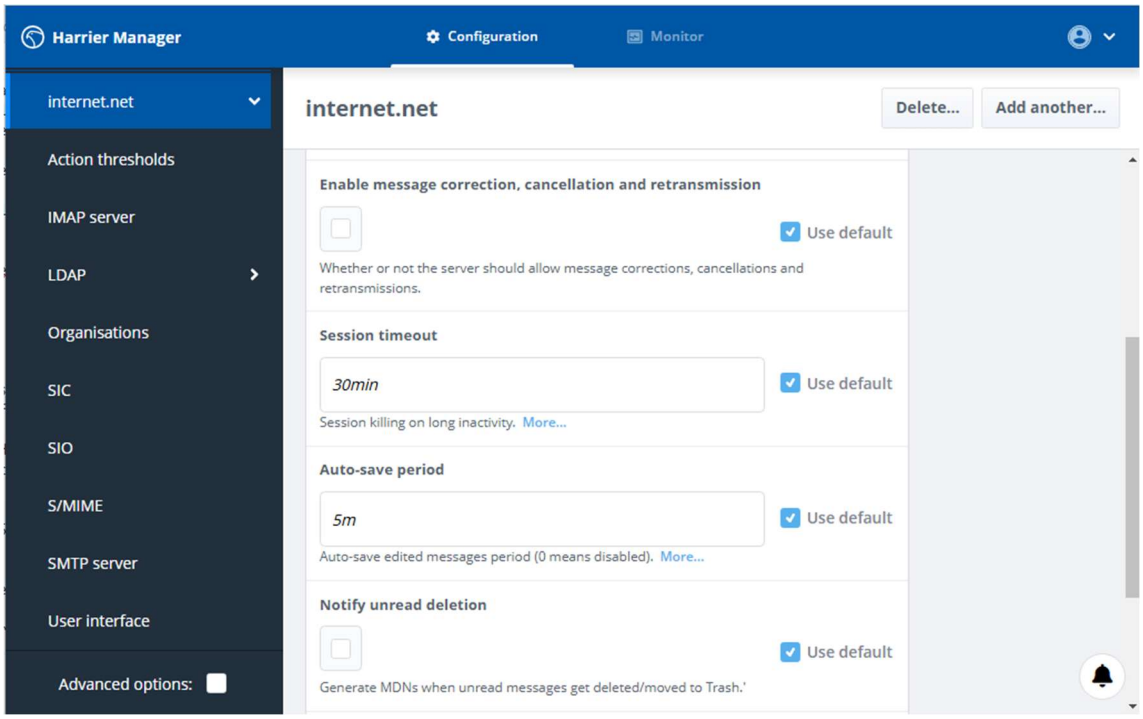
Scroll to the bottom.

Harrier Domain Configuration – LDAP Server.



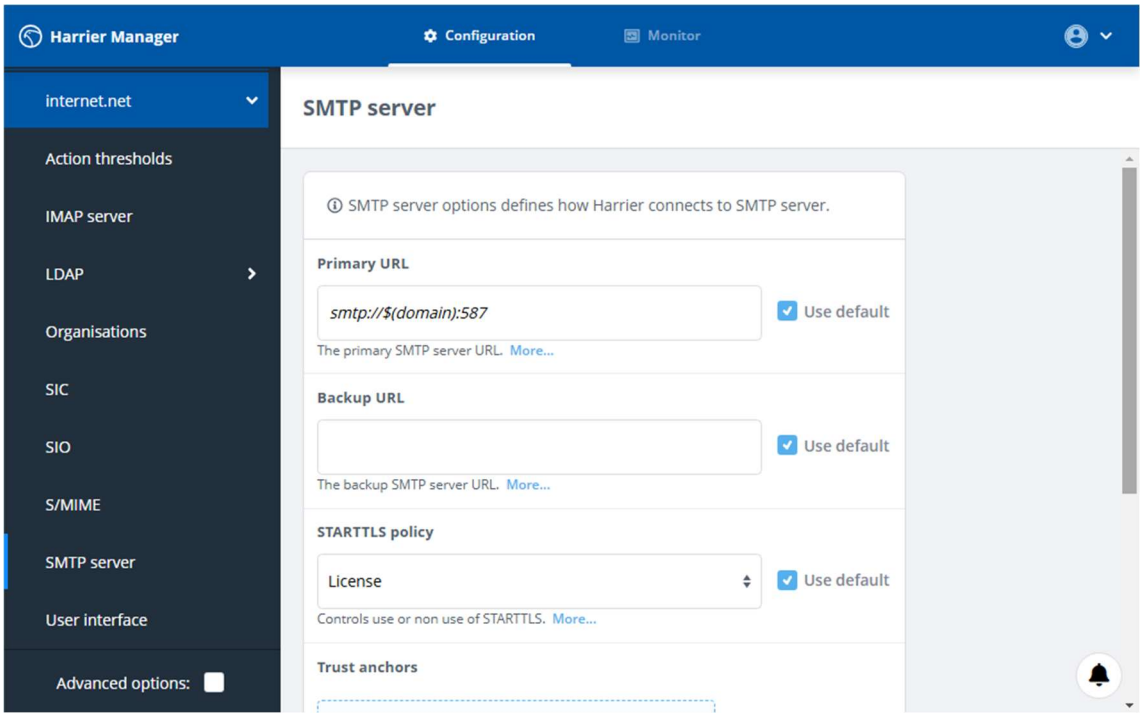
Click "Submit". Return to the "internet.net" configuration level on the left-hand menu

Harrier Domain Configuration – SMTP Server.



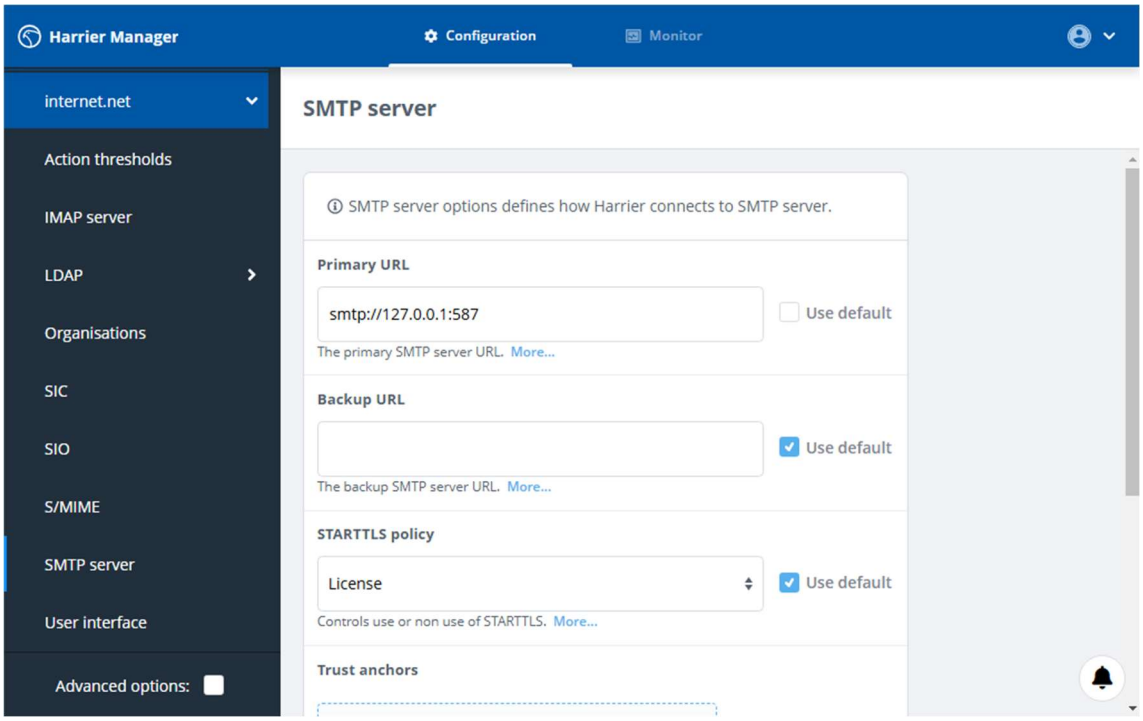
From the left-hand menu select "SMTP server"

Harrier Domain Configuration – SMTP Server.



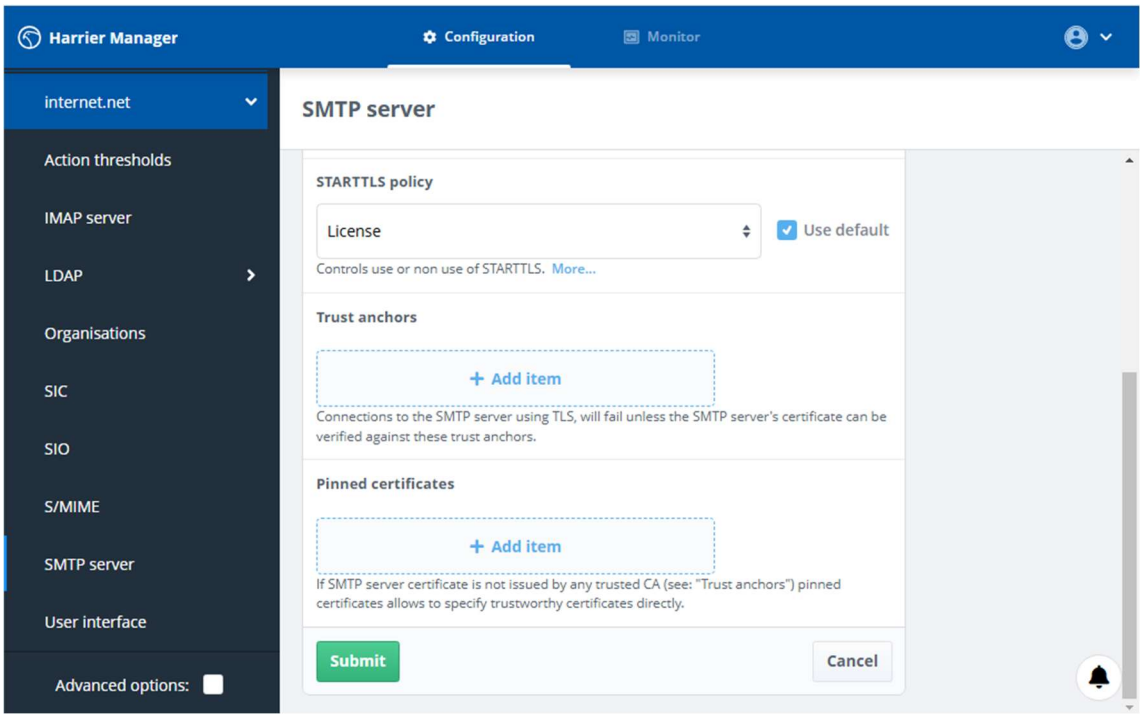
Enter "smtp://127.0.0.1:587" for the "Primary URL".

Harrier Domain Configuration – SMTP Server.



Scroll down to the bottom.

Harrier Domain Configuration – SMTP Server.



Click “Submit”.

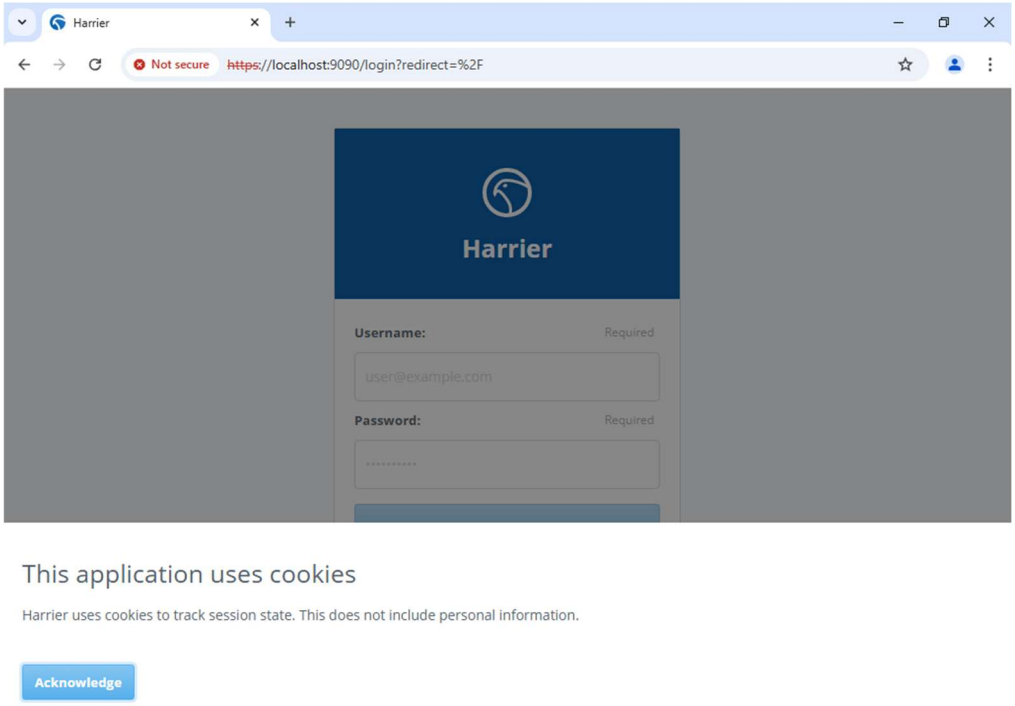
This completes the configuration of the Harrier Server. We are not ready to test the solution.

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 .

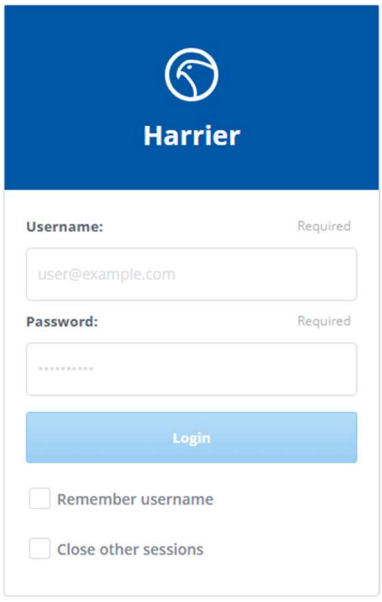
Point your browser at https://localhost:9090

Harrier login.



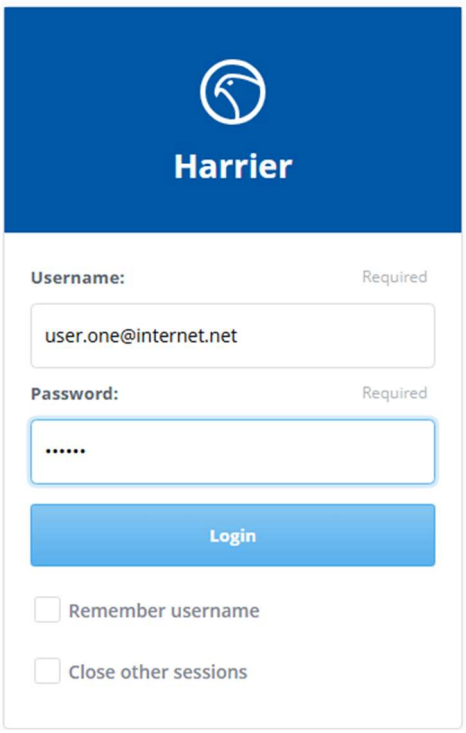
Click “Acknowledge”.

Harrier login.



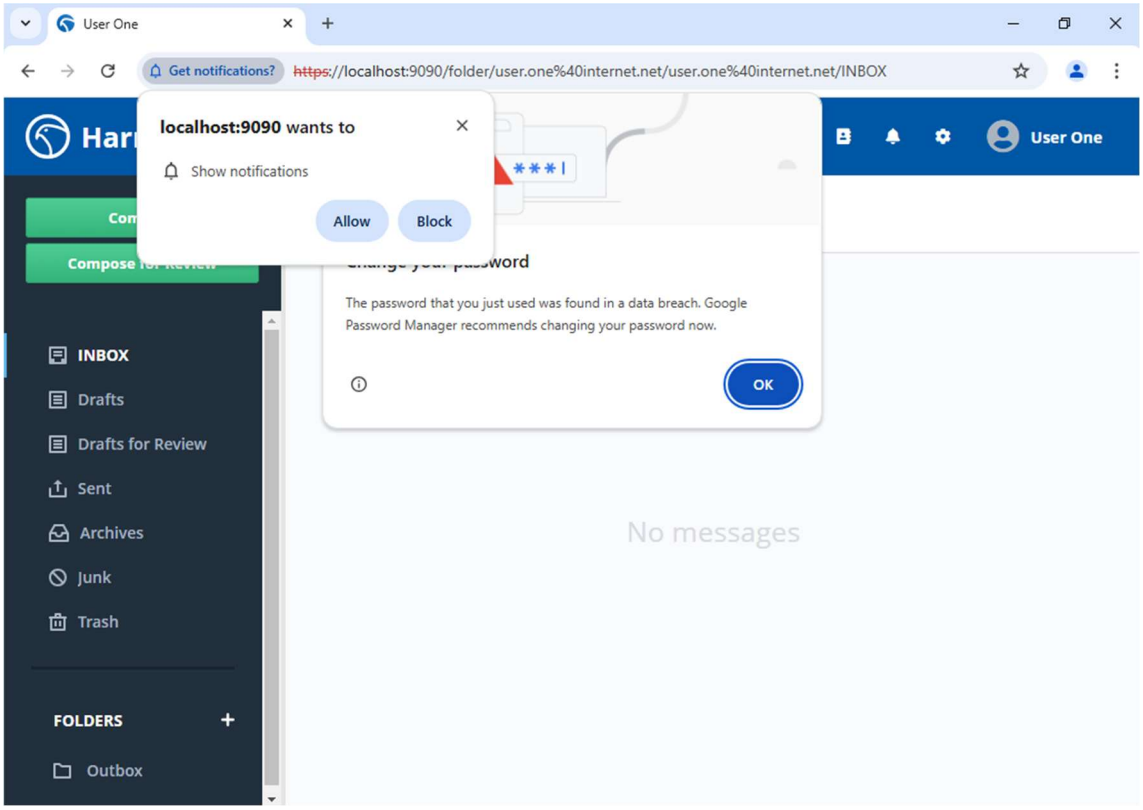
Enter user.one@internet.net and the Password you set for this User.

Harrier login.



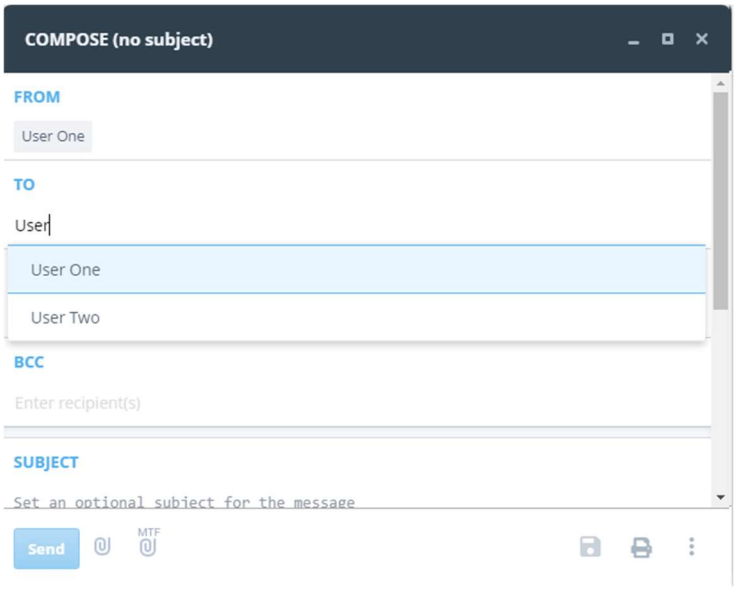
Click “Login”

Harrier Client Inbox.



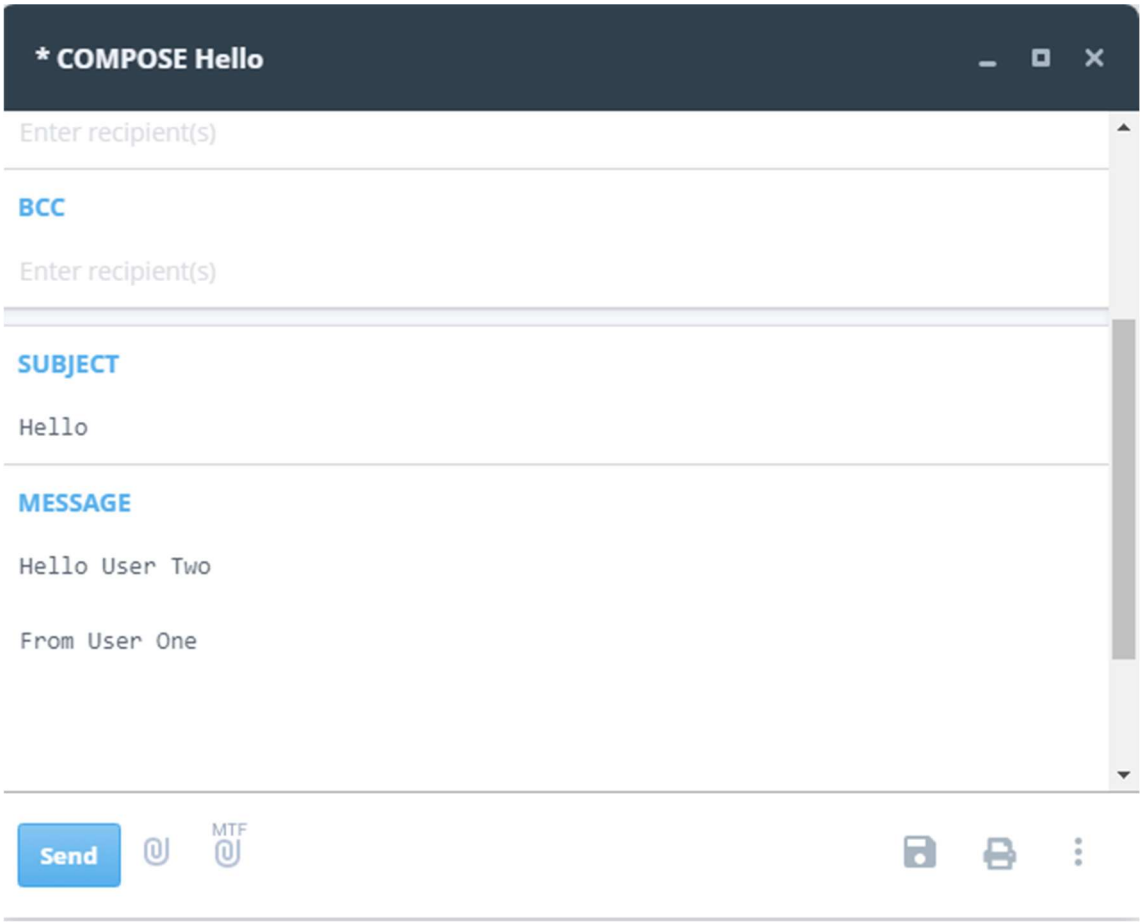
Click “Allow” for Notifications and “OK” for the weak password, then click “Compose”.

Harrier Client Compose.



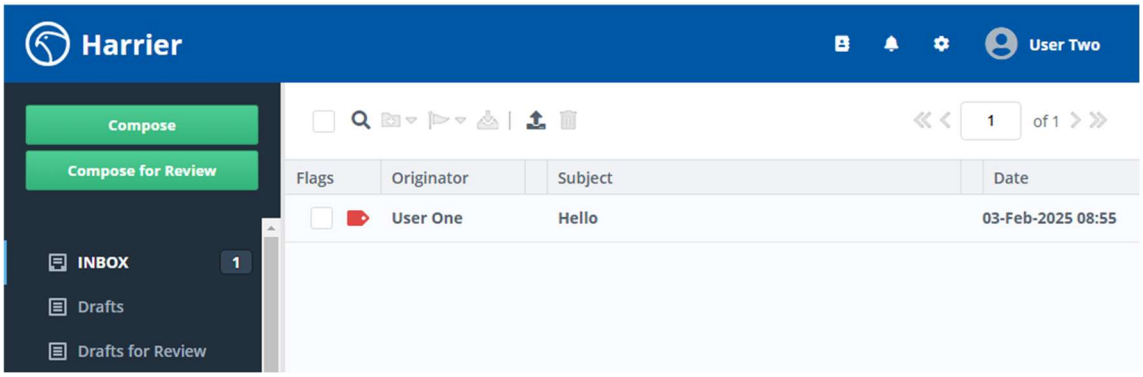
Start typing in the "To" field and Address Matches will appear, select the one you want to send to.

Harrier Client Compose.



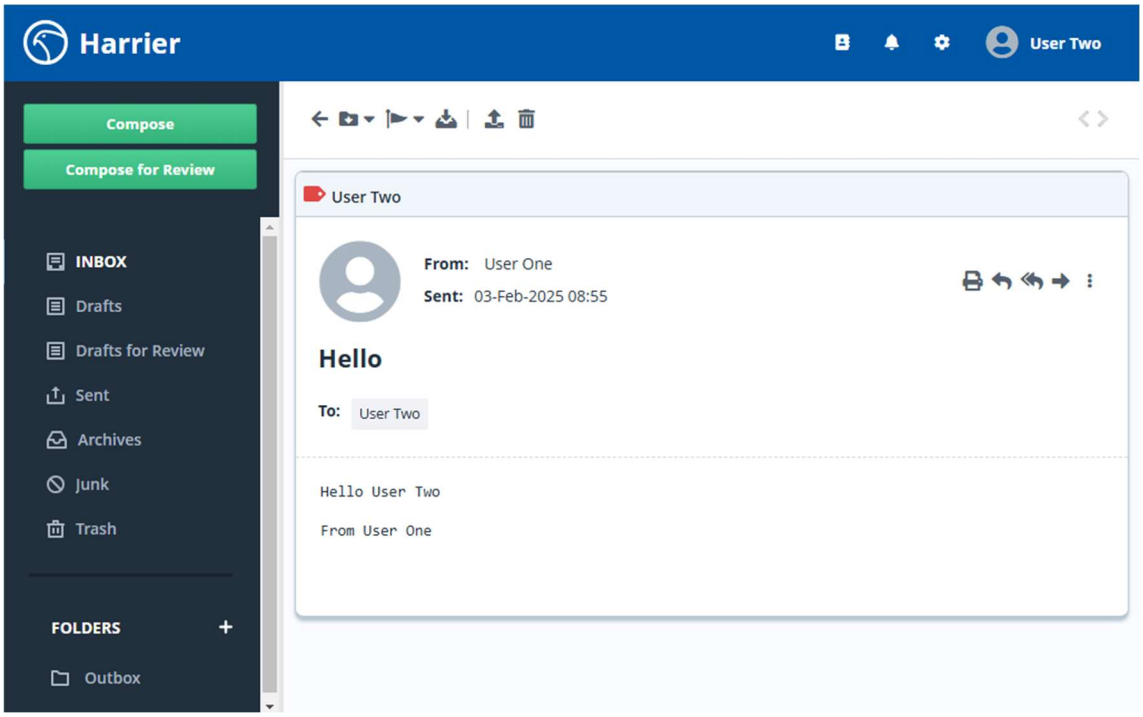
Complete the Subject and Message fields and Click "Send". Then open a New Browser Tab and Login as User Two.

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

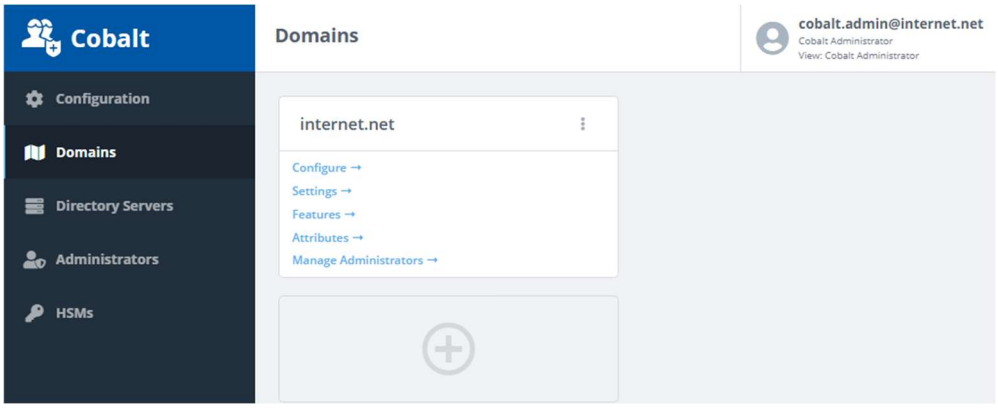
In this section we will manually configure an External SMTP Server. The External domain we will use is x400.net and will involve the following steps.

- 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

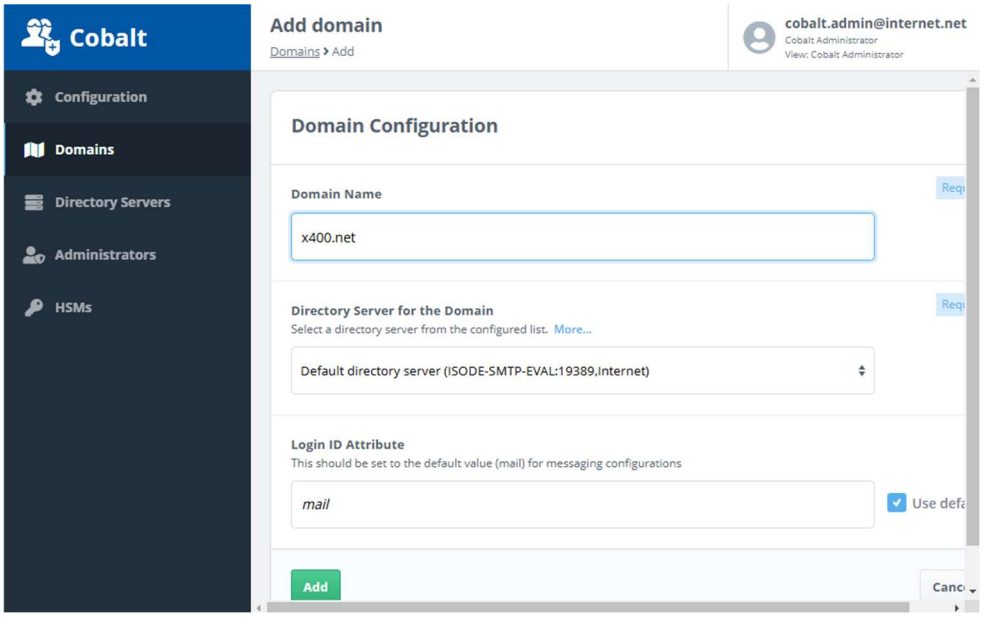
Login to Cobalt as the Cobalt Administrator

Cobalt Administrator Login.



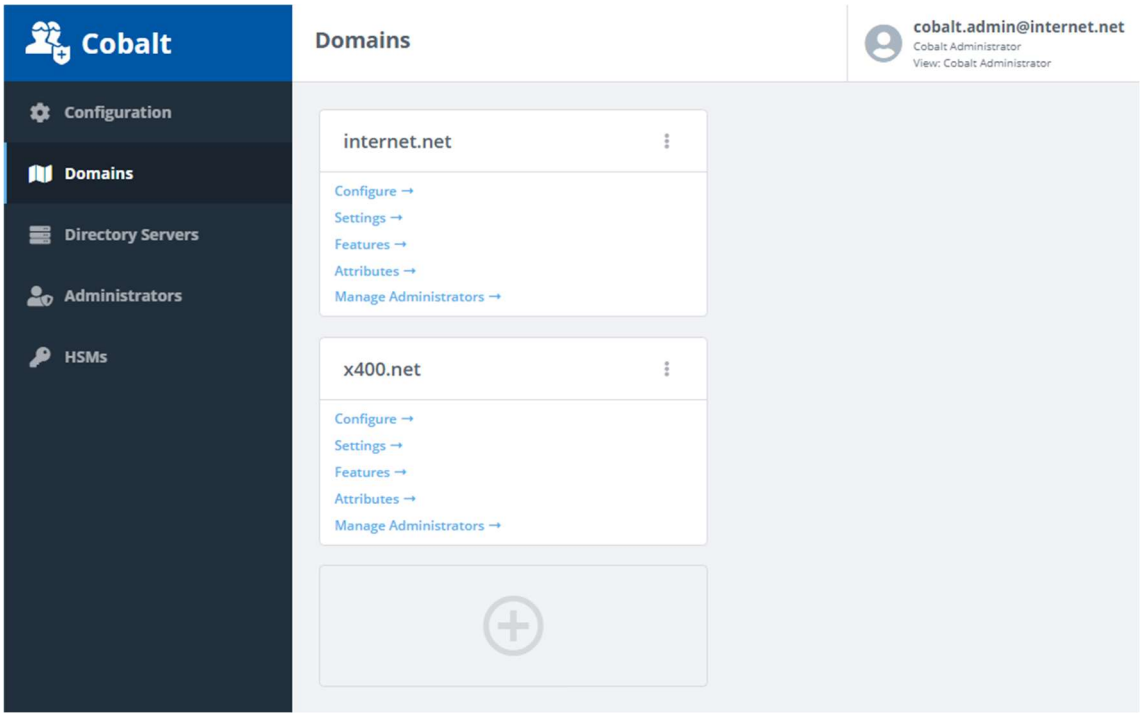
Then from the "Domains" Menu Click "+".

Cobalt Domain Add.



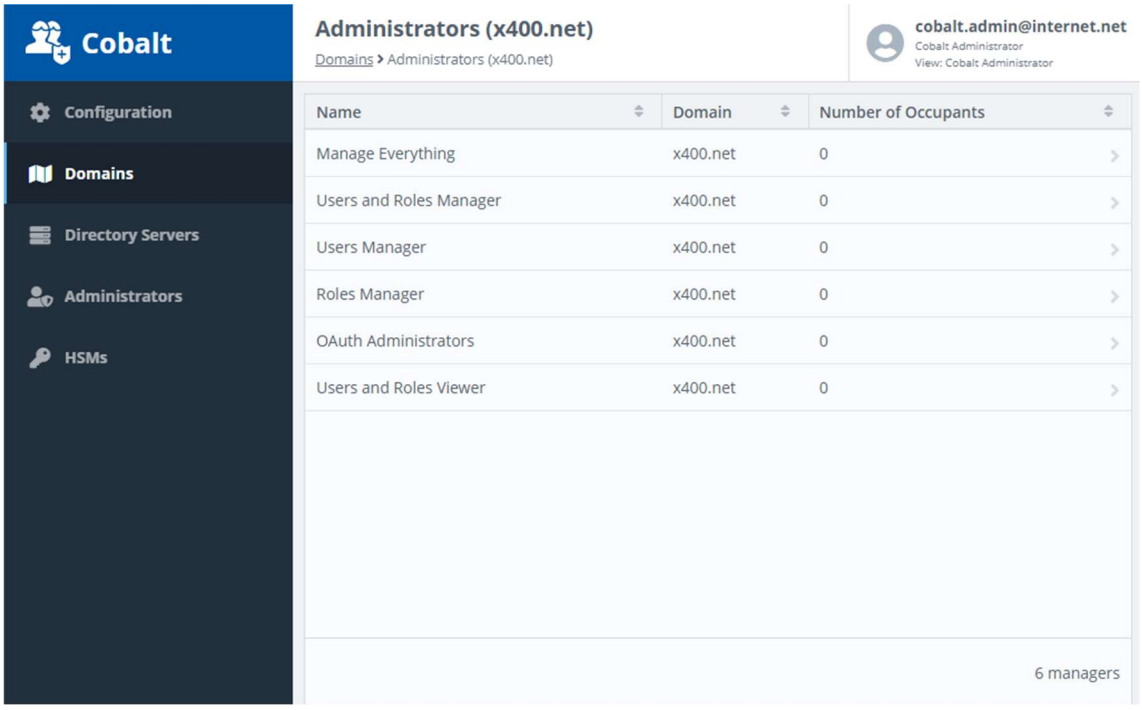
Enter the External Domain (x400.net) in this example. Click Add.

Cobalt Domain Add.



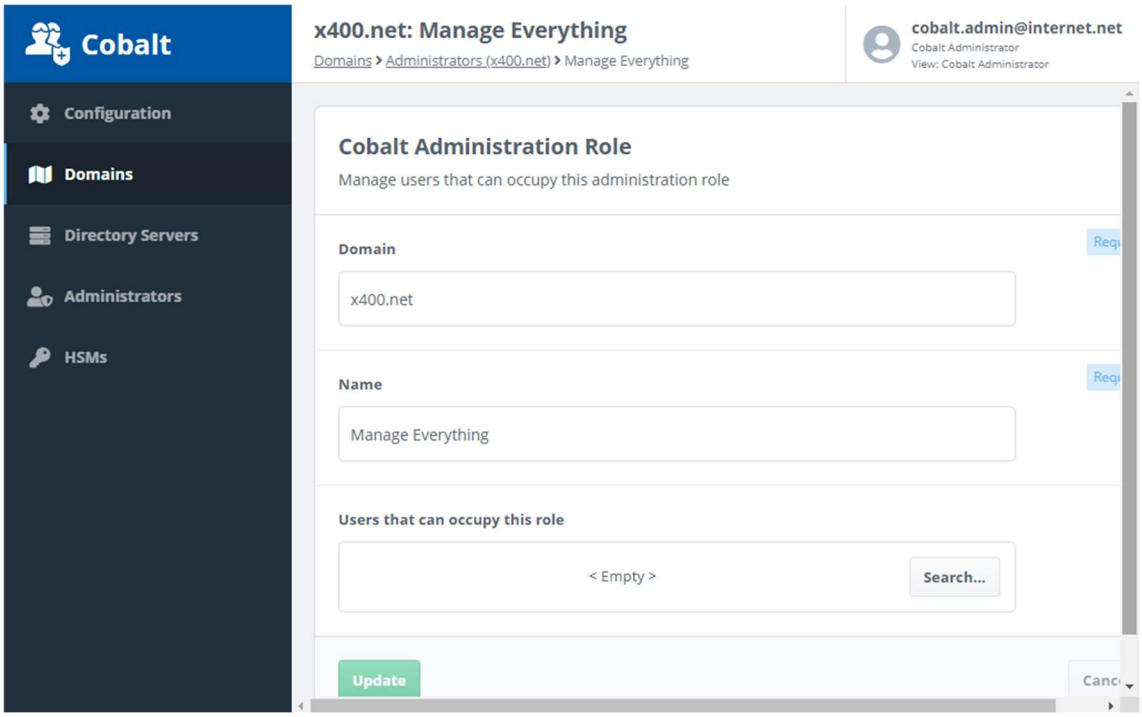
Click “Manage Administrators”.

Cobalt Domain Add.



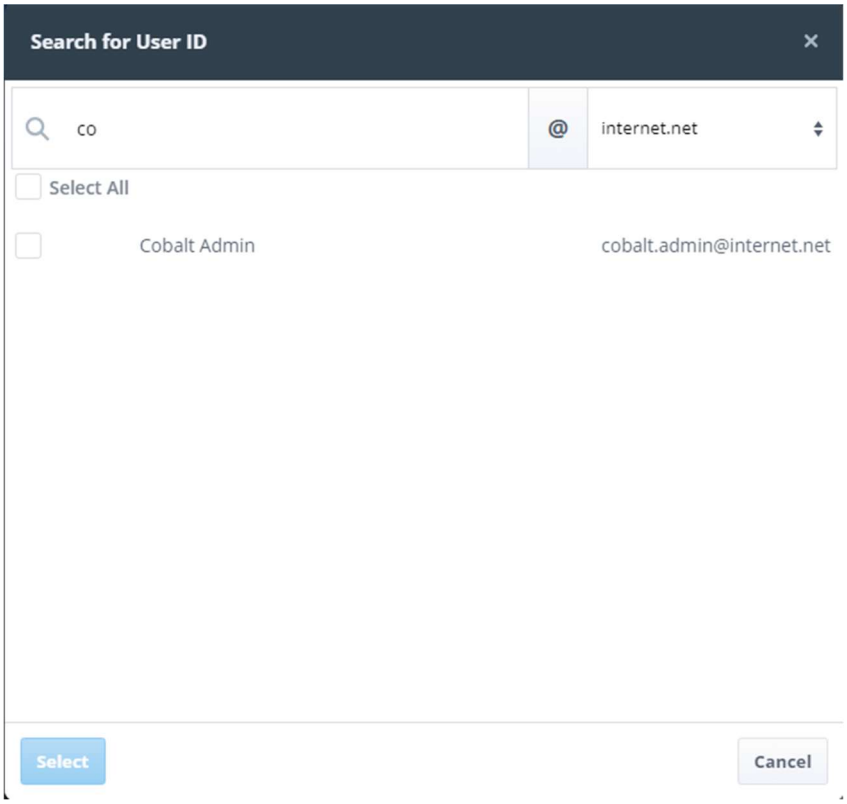
Select “Manage Everything”.

Cobalt Domain Add.



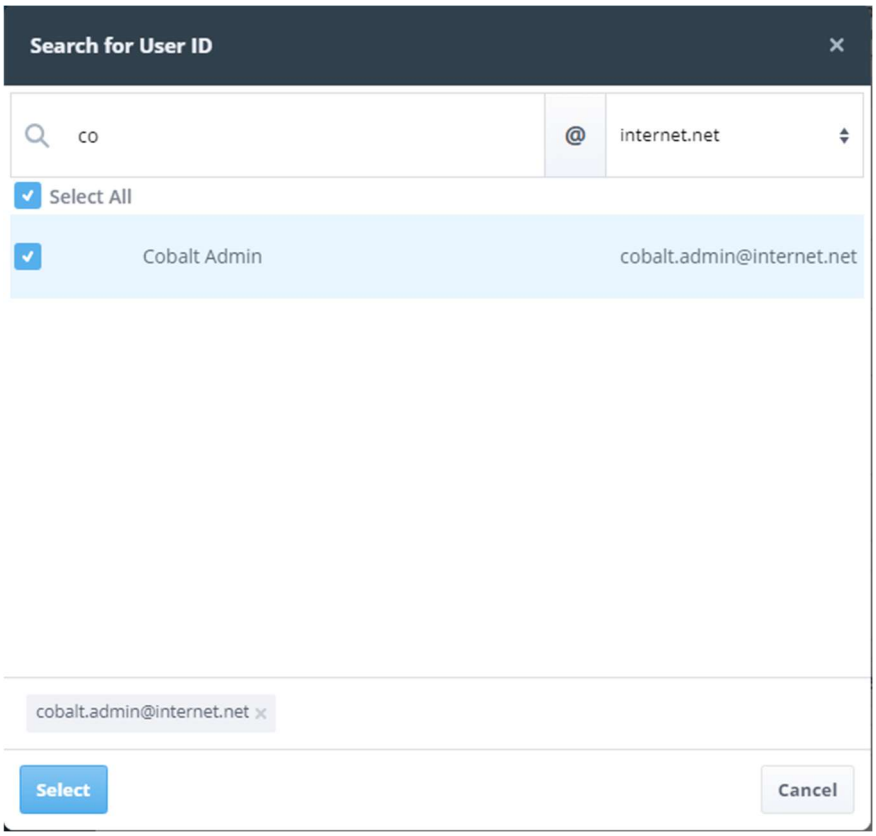
Click “Search”.

Cobalt Domain Add.



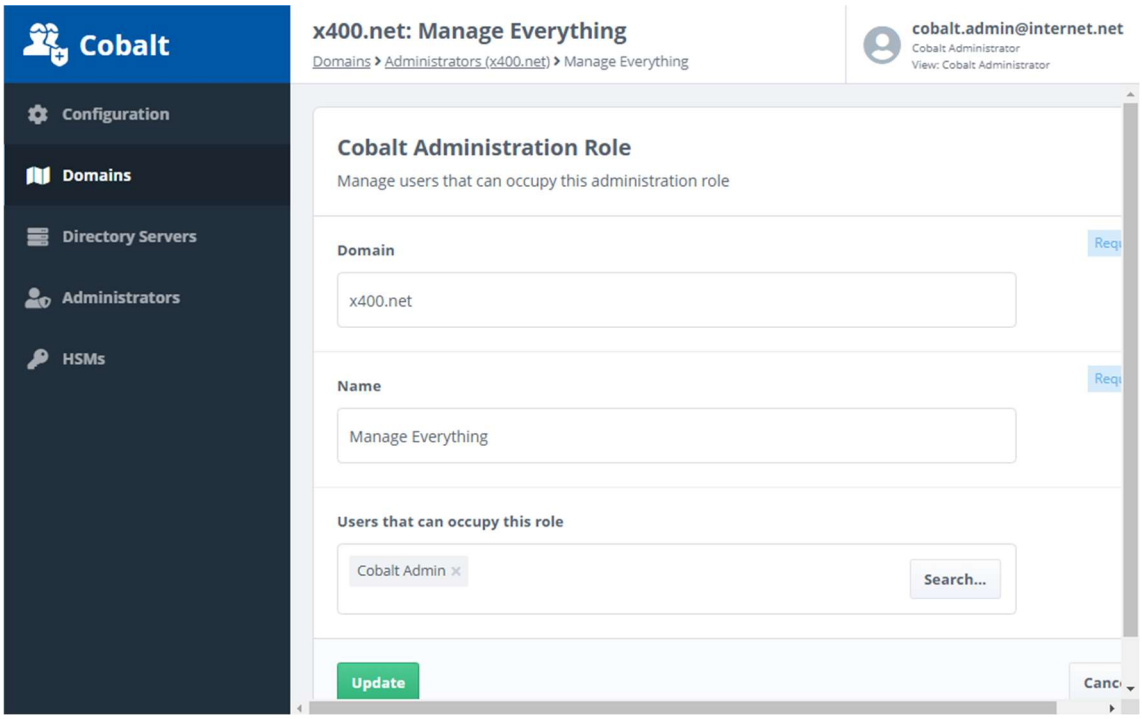
From the drop down menu on the top right select “internet.net” and start typing “co…” and the entry “Cobalt Admin” will display.

Cobalt Domain Add.



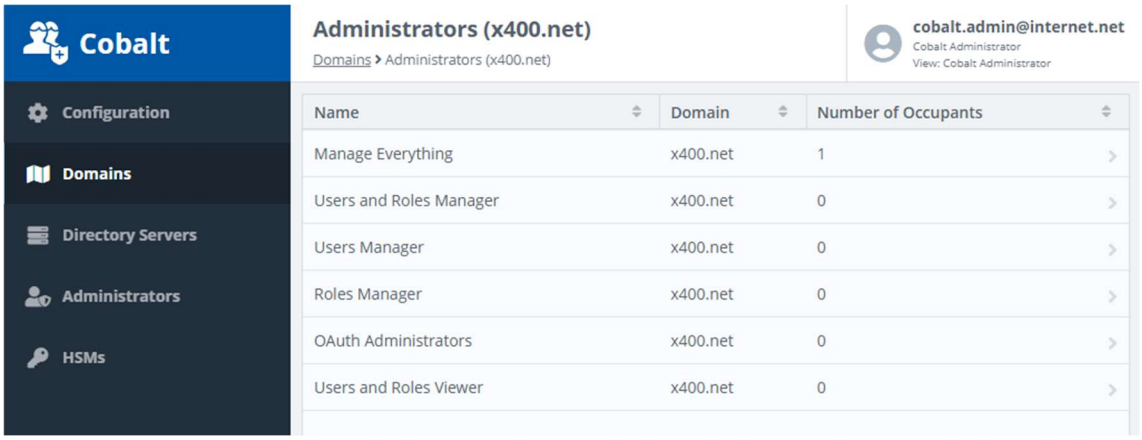
Select it and the Click “Select”.

Cobalt Domain Add.



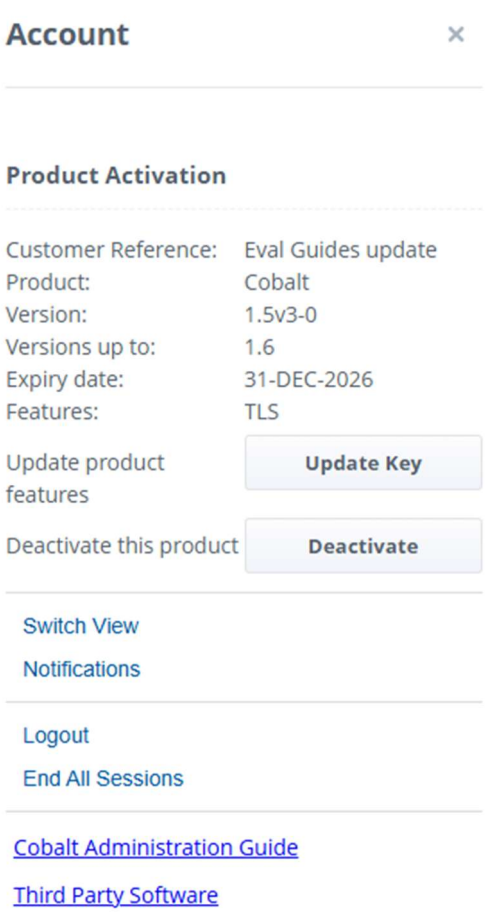
Click “Update”.

Cobalt Domain Add.



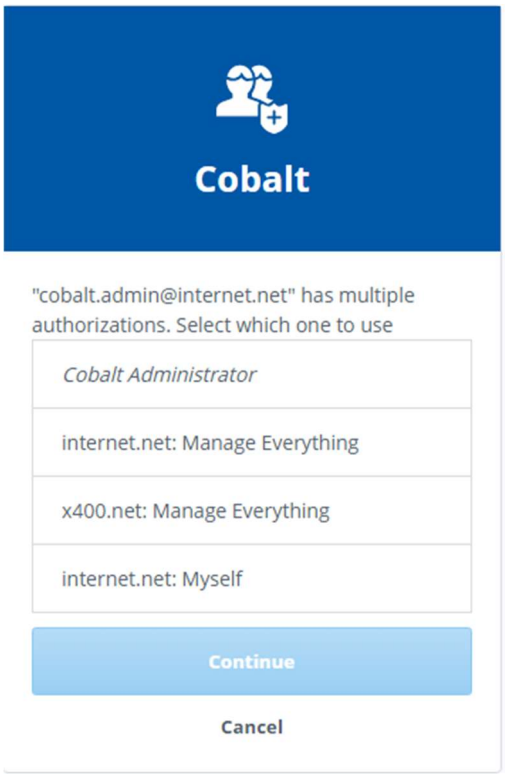
Click on the Username Box in the Top Right.

Cobalt External Domain Users Add.



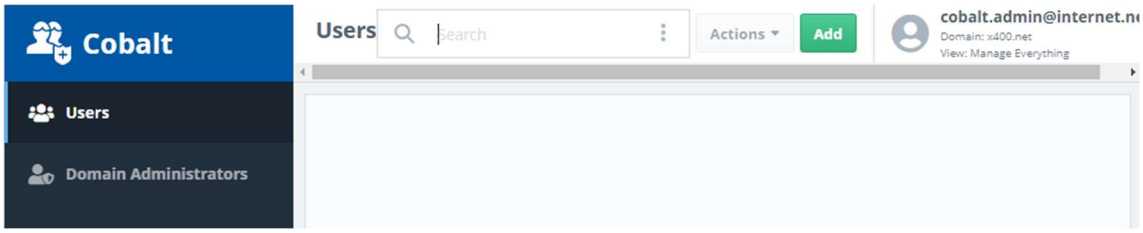
Select “Switch View”.

Cobalt External Domain Users Add.



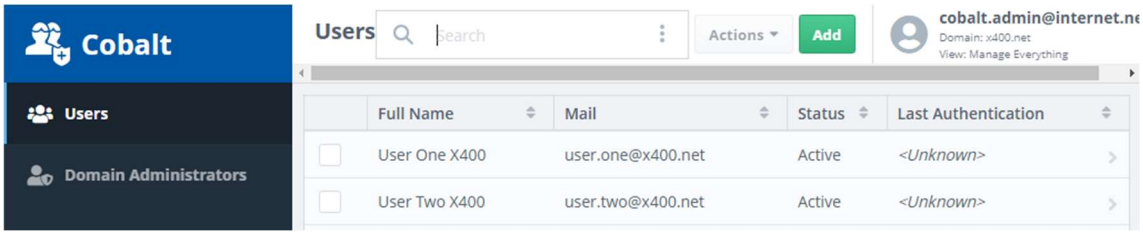
Select “x400.net: Manage Everything”. Click “Continue”.

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.

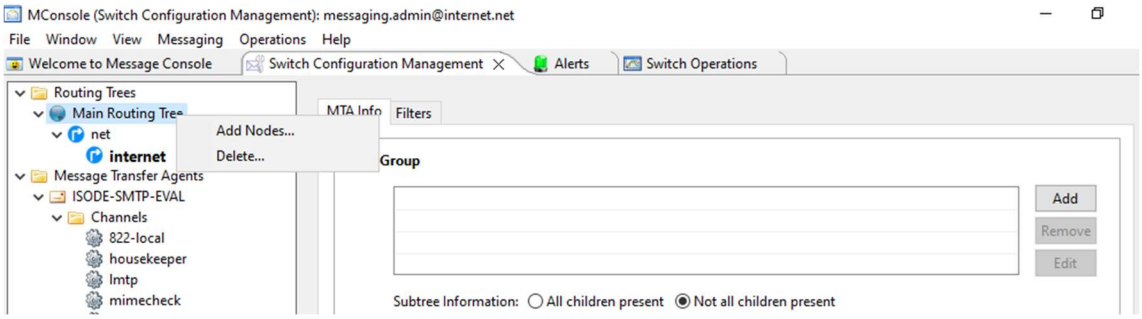


You have now added the External Users and can now go to M-Console to Configure the Routing and External MTA.

Adding and Configuring the External Domain in M-Console

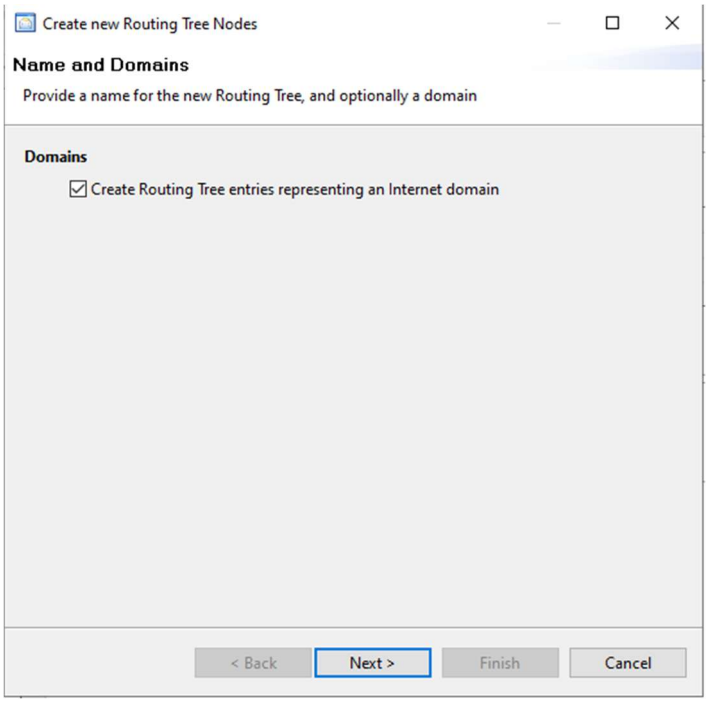
From M-Console Switch Configuration Management.

M-Console Configure Routing Tree Entry.



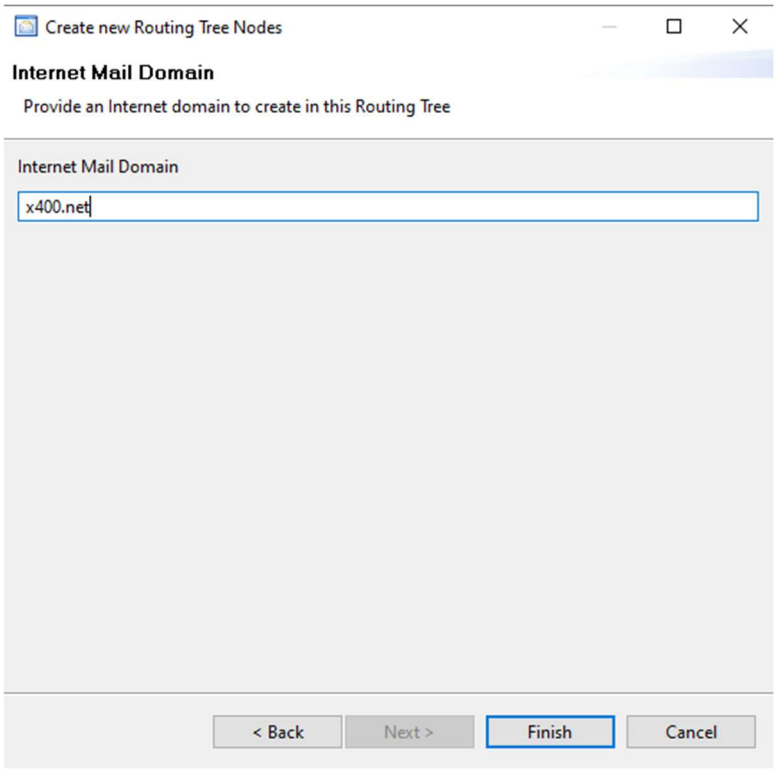
Right Click on the “Main Routing Treee”, Click “Add Nodes…”

M-Console Configure Routing Tree Entry.



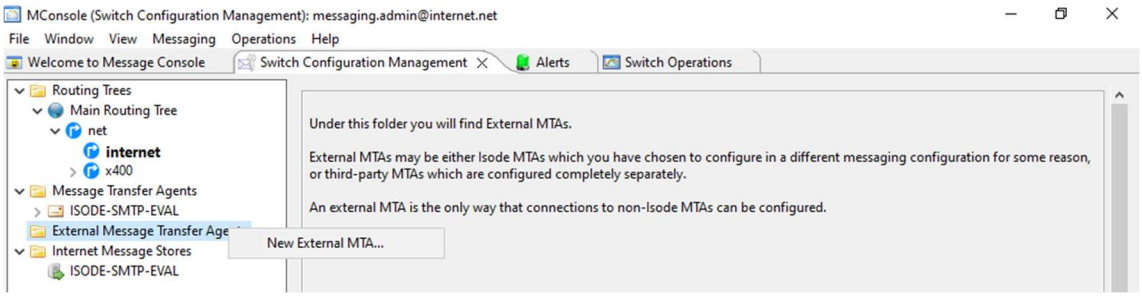
Click “Next>”.

M-Console Configure Routing Tree Entry.



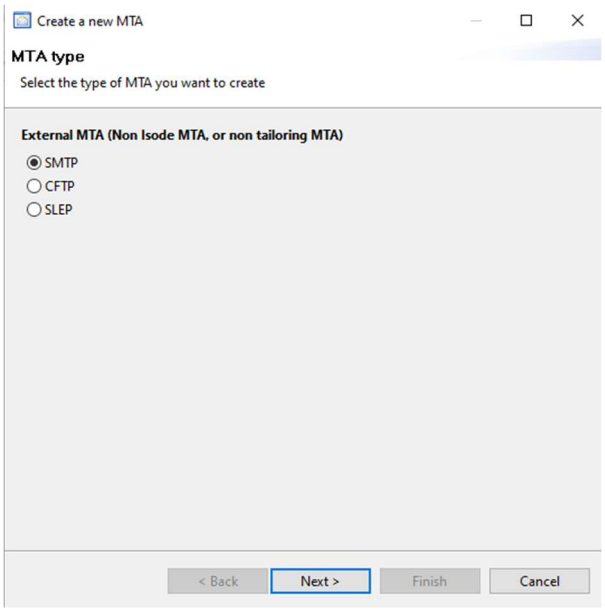
Enter “x400.net”, Click “Finish”.

M-Console Configure External MTA.



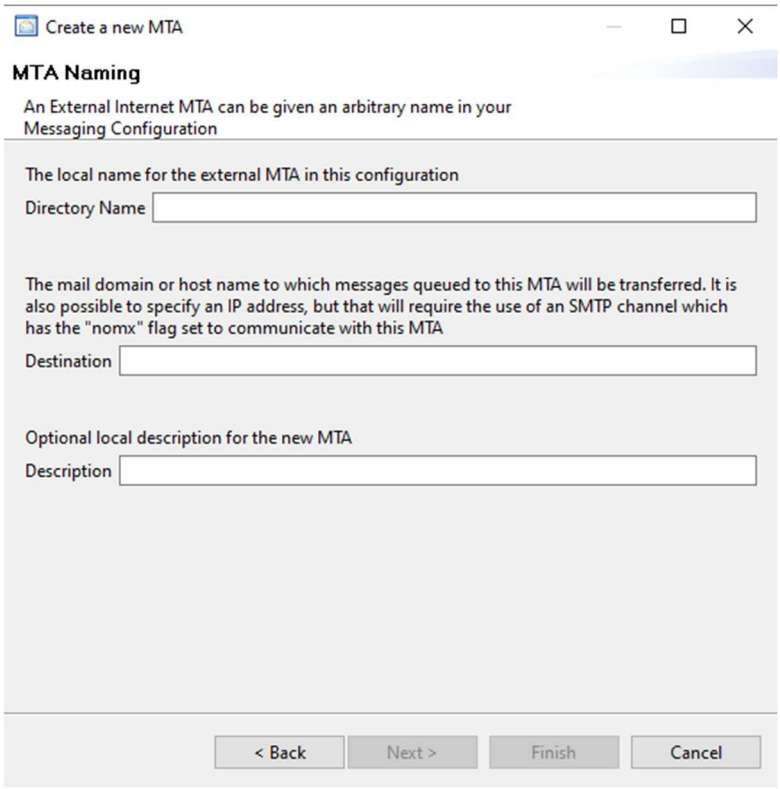
Eight Click on “External Message Transfer Agents”, Click “New External MTA…”.

M-Console Configure External MTA.



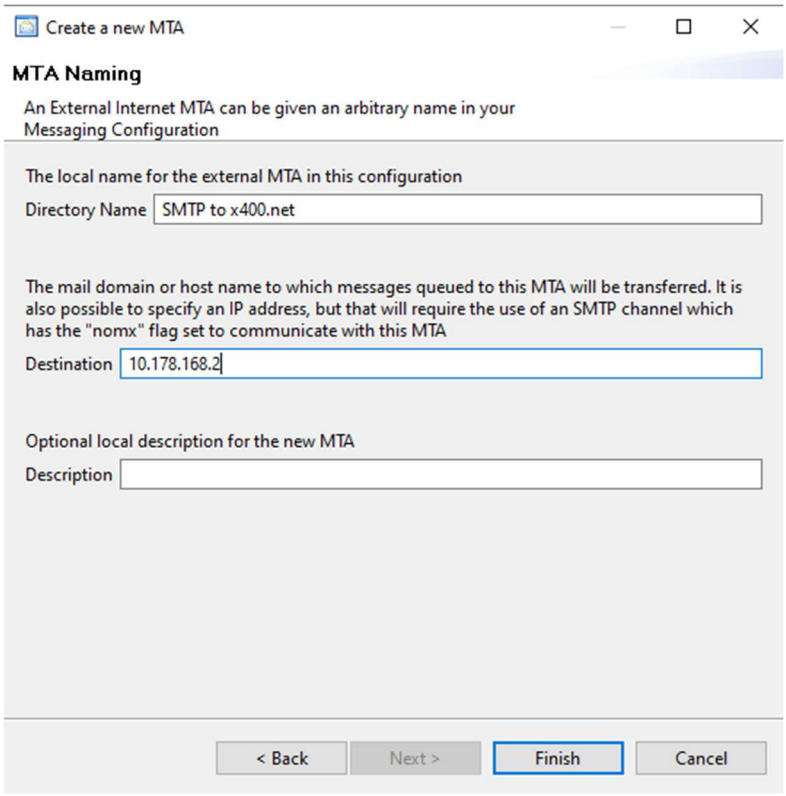
Select “SMTP, Click “Next>”.

M-Console Configure External MTA.



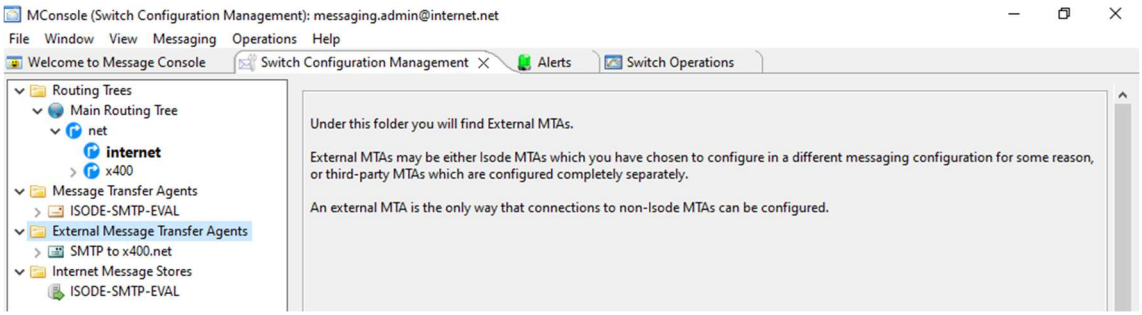
Enter a friendly name for the “Directory Name” and the hostname or IP Address of where that MTA is.

M-Console Configure External MTA.



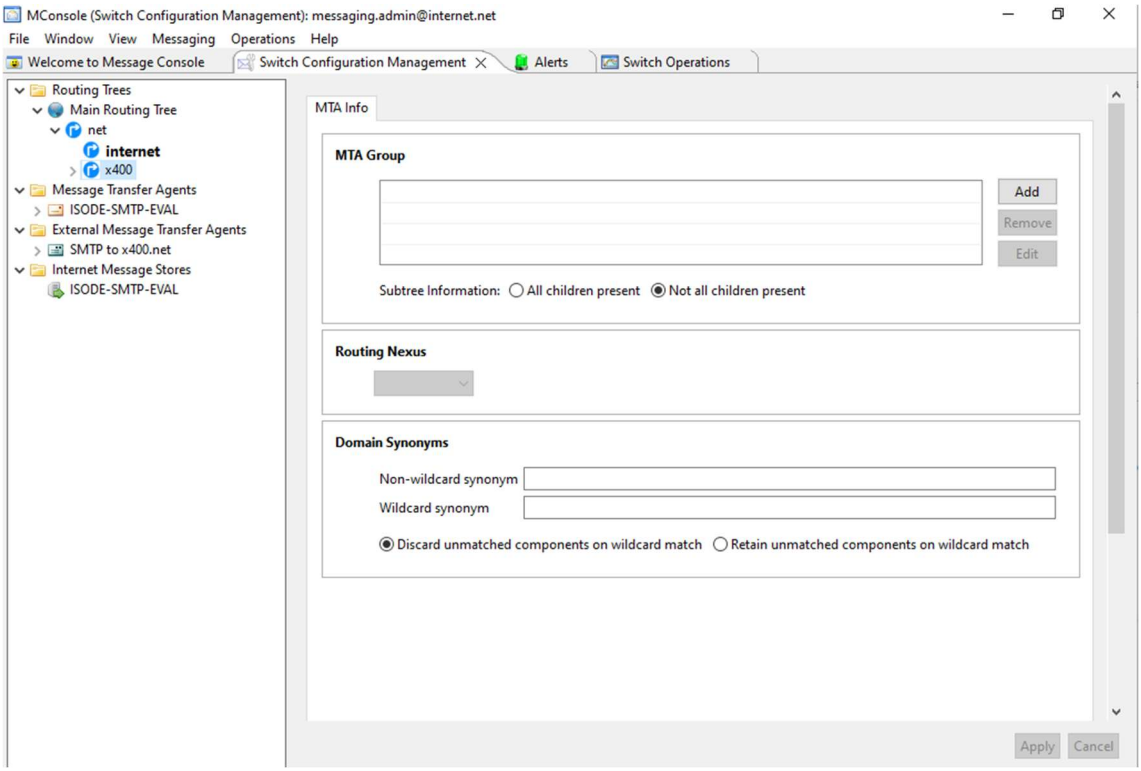
Click “Finish”.

M-Console Configure External MTA.



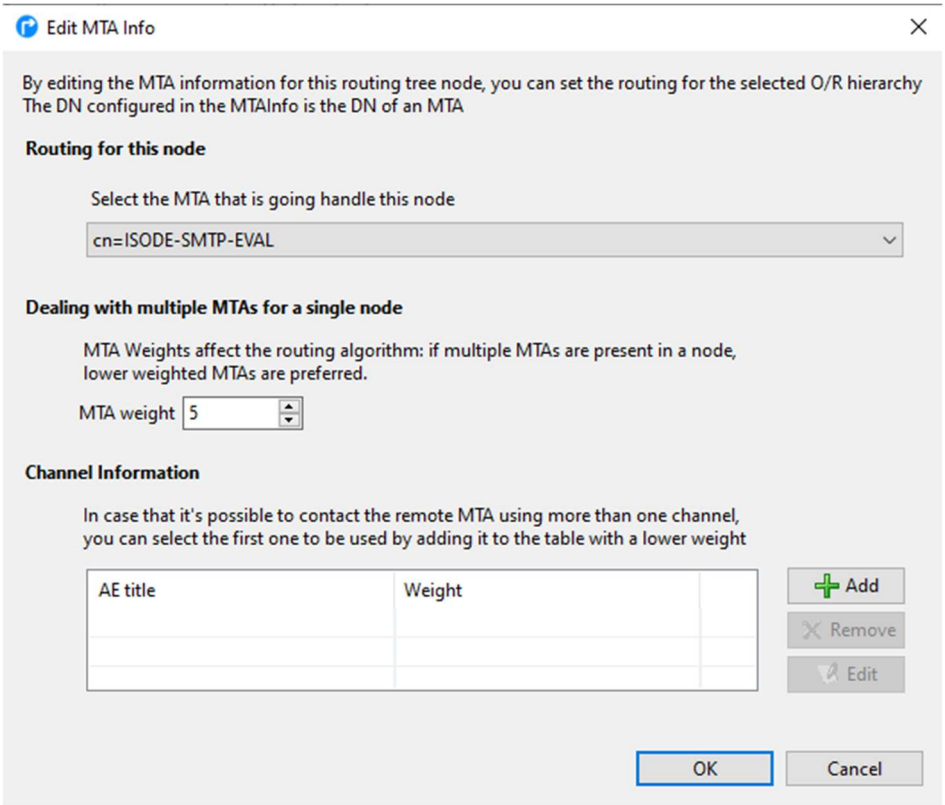
Select the “x400” entry on the “Main Routing Tree”.

M-Console Configure External MTA.



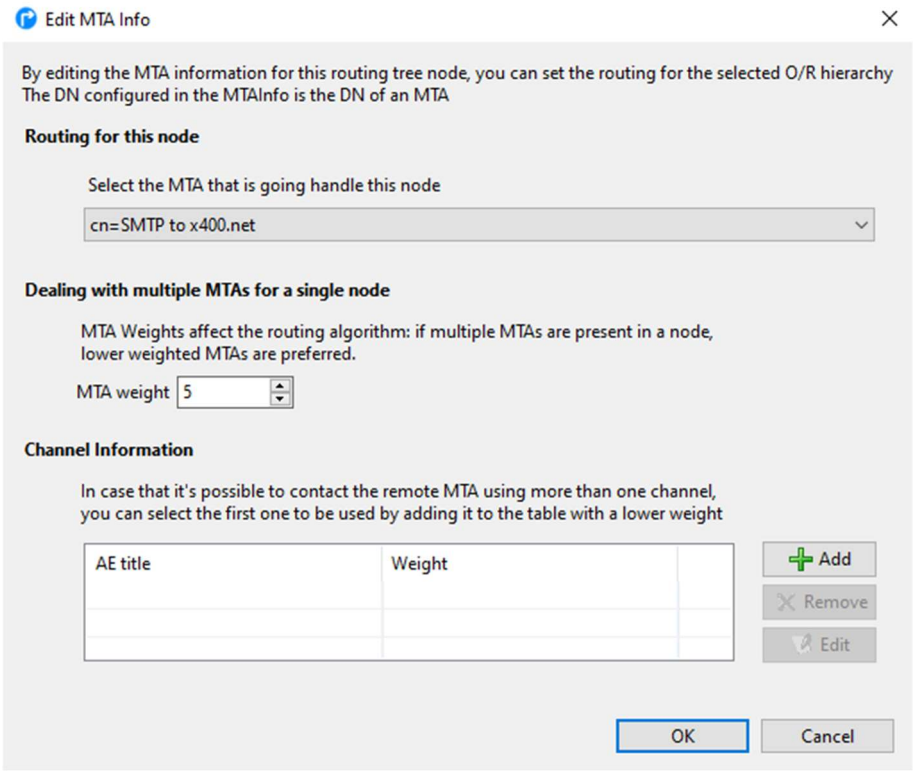
Click “Add”.

M-Console Configure External MTA.



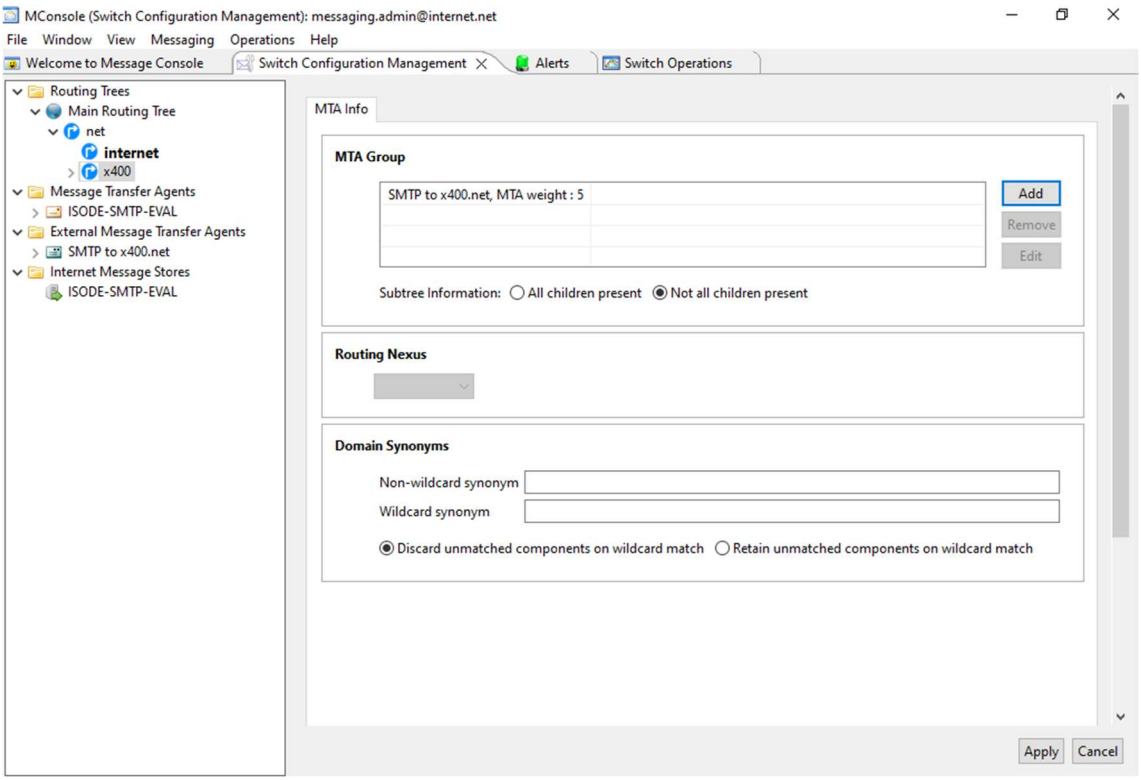
Change the”Routing for this node” to your newly created External MTA from the Drop Down.

M-Console Configure External MTA.



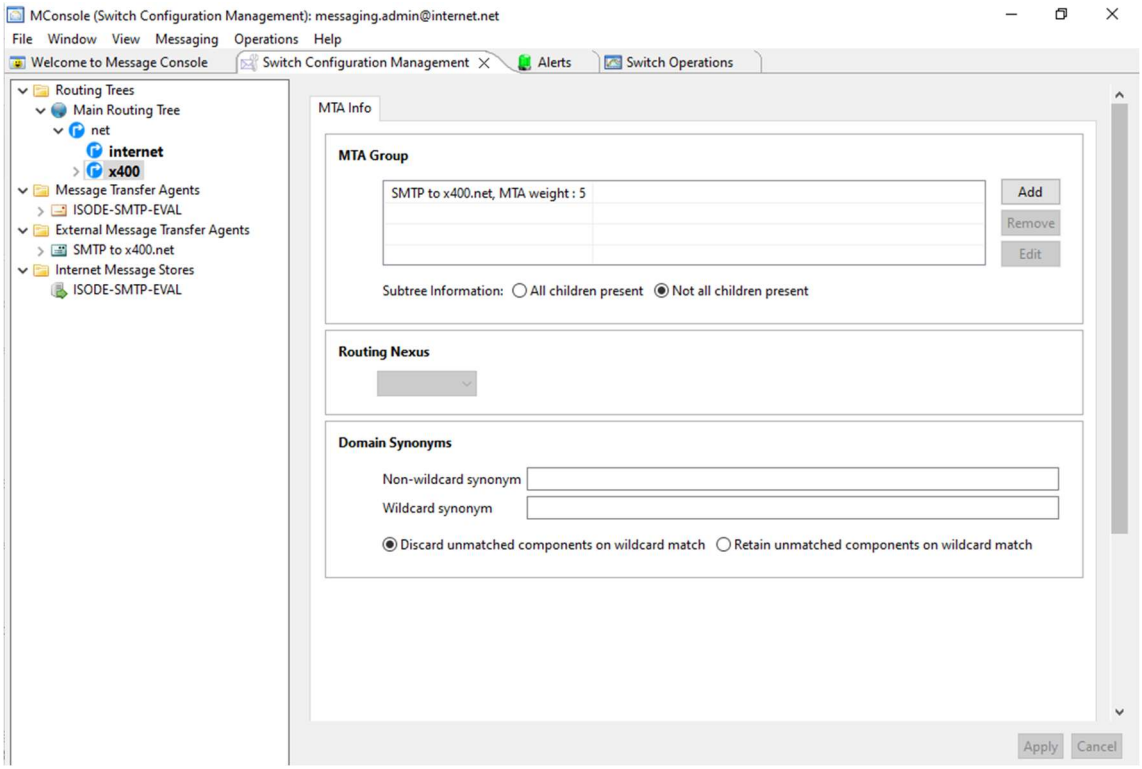
Click “OK”.

M-Console Configure External MTA.



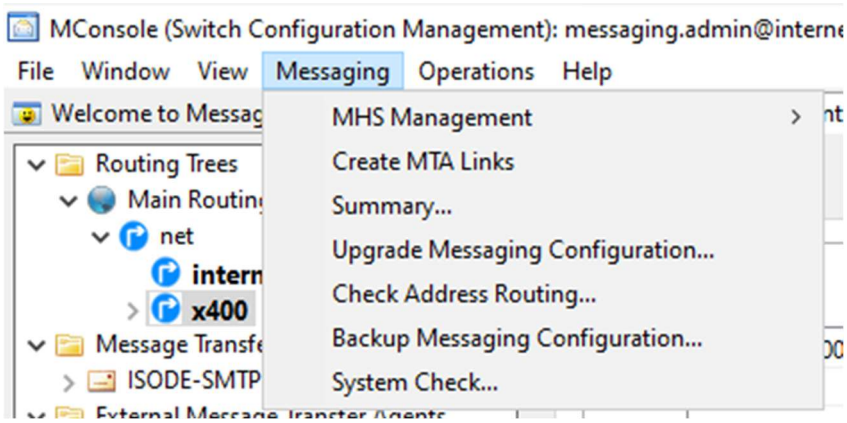
Click “Apply”.

M-Console Configure External MTA.



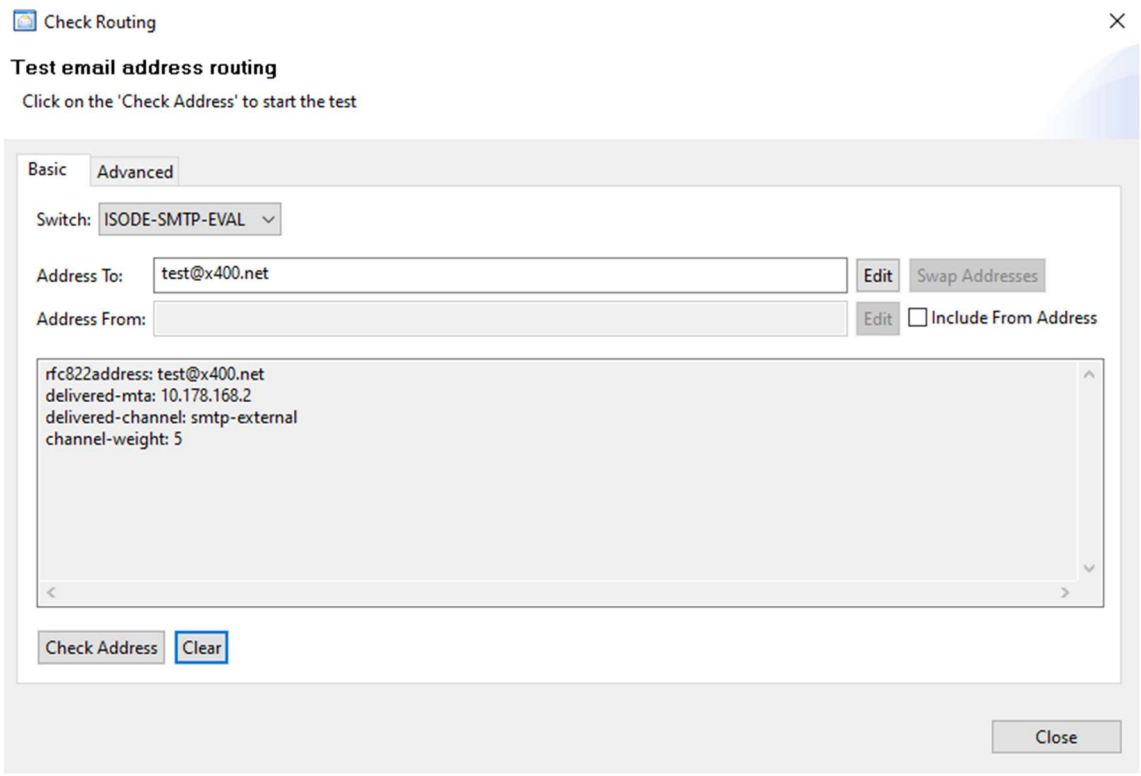
Now we need to check the Routing is working. From the very top Menu Right Click on "Messaging".

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