Isode

R19.0 M-Vault Directory Server Evaluation Guide

Getting started with M-Vault, Isode's X.500/LDAP Directory Server.

Contents

Introduction

The purpose of this guide is to introduce M-Vault to readers new to Isode's servers and management tools. The guide will introduce some basic directory concepts in the context of the Isode product set. M-Vault Directory Server is one of a family of Directory and messaging products which comprises:

M-Switch SMTP (SMTP Message Transfer Agent)

M-Box (POP/IMAP Message Store)

M-Switch X.400 (X.400 Message Transfer Agent)

M-Store (X.400 Message Store)

M-Switch MIXER (message gateway providing conversion between X.400 and Internet email according to the MIXER specifications)

M-Switch Gateway (Email Messaging for low-bandwidth and/or high-latency networks)

Harrier (web based email client)

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

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

Objectives

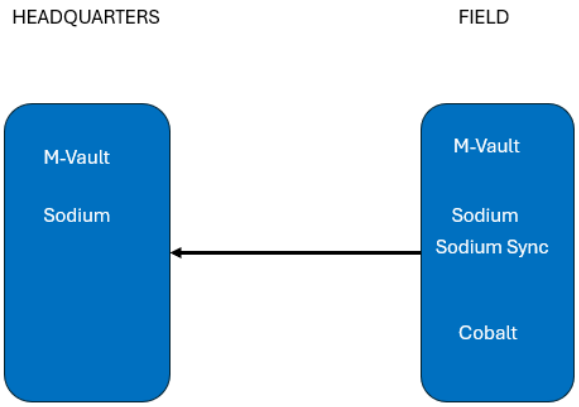
By the end of this guide you will have:

1. Become familiar with some directory terminology and concepts
2. Created a Directory Server using M-Vault Console.
3. Configured a Sodium CA
4. Configured M-Vault to support TLS with Certificates generated with Sodium CA
5. Added, modified and deleted directory entries using Sodium (Secure Open Data, Identity and User Manager)
6. Bulk loaded data into the Directory from a sample LDIF file
7. Created a Directory Server using Cobalt.
8. Added, modified and deleted entries in the directory using Cobalt
9. Synchronized directory data using Sodium Sync

Environment Overview

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

High Level Overview



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

Using Isode Support

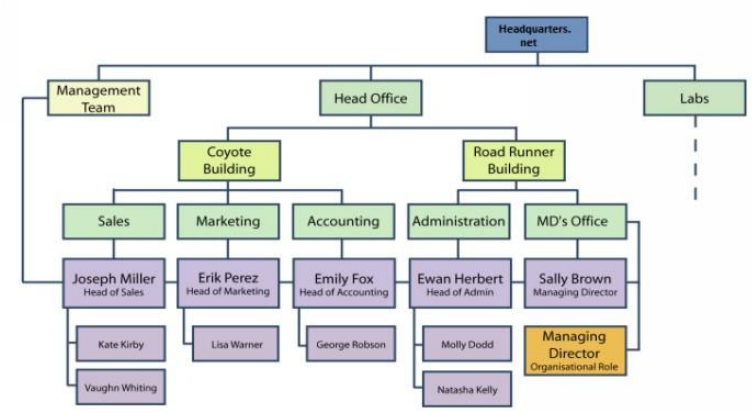
You will be given access to Isode support resources when carrying out your evaluation. Any queries you have during your evaluation should be sent to isode.support@isode.com. Please note that access to the Self-Service Portal for web-based ticket submission and tracking is not available to evaluators.

Terminology

This section describes some of the major Directory concepts that you will encounter in this evaluation. Feel free to skip this section if you are already familiar with Directories.

Prior to creating a new Directory Server, you need to decide what schema (data dictionary) you want to use and the structure of the Directory. One good way to plan this is to draw a chart of your company's structure, as this will be very similar to the structure of the Directory that you create. Shown below is part of such a chart for a fictional company, Headquarters.net. An LDIF file containing this 'Headquarters.net' dataset is one of the sample files shipped with M-Vault and later in this guide you'll load and work with this data.

Organizational Chart



In this organizational chart we can see entries for an organization (Headquarters.net), organizational units (Head Office, Labs, Sales, Marketing, etc.), locations (the two buildings), people, an organizational role (Managing Director) and a Group of Names (the Management Team).

The hierarchical structure of the information held in the Directory is called the Directory Information Tree (DIT). Most of the useful information, from the perspective of a user, is found at the lower levels of the DIT, while the top levels hold information that facilitates identification and navigation of entries across the hierarchy.

Each entry in the Directory (such as a person, organizational unit or organization) has attributes which contain information about it. An attribute consists of an attribute type and one or more values. An entry for Eric Perez contains attributes like:

```
telephoneNumber: 070 4166 2970

mail: eric.perez@acmelabsldifdemo.com
```

In this example, “telephoneNumber” and “mail” are attribute types, while “070 4166 2970” and "eric.perez@acmelabsldifdemo.com" are values for these attribute types.

Each entry must also have at least one attribute which is used to name the entry (naming attribute). This attribute forms the Relative Distinguished Name (RDN) for this entry. The examples below are all valid RDNs, where cn stands for the attribute type “commonName”, ou for “organizationalUnitName”, and o for “organizationName”:

```
cn=Eric Perez ou=Marketing o=Acme
```

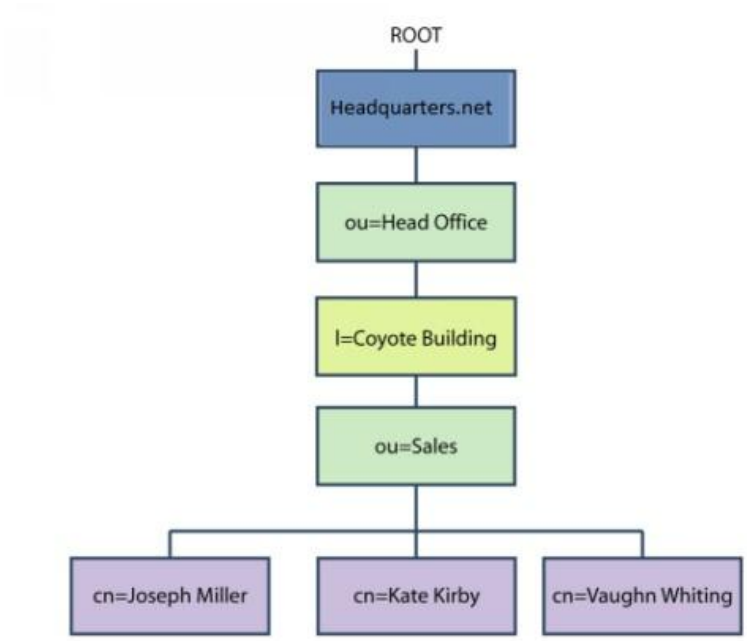
An entry can have more than one naming attribute, although usually only one is used. You may adopt a more complicated naming system, involving multiple naming attributes, to distinguish between large numbers of entries located at a single level of the DIT. For example, if there are two employees in the Marketing department called John Smith, you could use the userId (uid) attribute type to distinguish between them:

```
cn=John Smith+uid=jrs

cn=John Smith+uid=cbs
```

Each Directory entry also has a Distinguished Name (DN), which uniquely identifies the entry in the DIT. The DN is constructed by joining the RDNs of all the entries in the DIT at and above this entry, up to the root. For example, consider the image below which shows the Directory Information Tree for the Sales department (an organizational unit) of Headquarters.net.

Sales Department DIT



This chart shows the RDN of each level of the hierarchy. To construct the DN for the entry for Joseph Miller, join the RDNs of all entries at and above this entry up to the root. The chart above shows the required information. Therefore, the DN for the entry for Joseph Miller is:

```
cn=Joseph Miller, ou=Sales, l=Coyote Building, ou=Head Office,
o=Acme
```

The DN of an entry thus shows its position in the DIT as well as identifying it.

Note that the RDN of an entry must distinguish it from all other entries with the same parent, where a parent is the next level up in the DIT. This means that you cannot have two entries with the same RDN (e.g. cn=Joseph Miller) underneath the same parent (e.g. ou=Sales).

Preparing the Server Environment

These steps should be followed on two servers.

Naming the Servers

Make the first machine name : HQDSASERVER

Make the primary dns suffix for this server HEADQUARTERS.NET

Make the second machine name : FIELDDSASERVER

Make the primary dns suffix for this server FIELD.NET

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

Install the Isode Software

Follow the instructions in the release notes for the appropriate platform for the products.

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

Messaging Activation Server 1.1v1

M-Vault 19.0v21

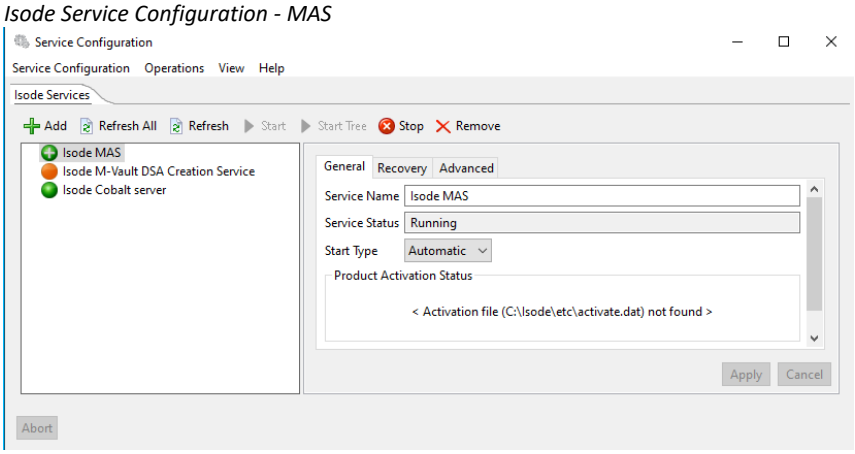
Cobalt-1.5v3

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

Activating the Isode Products

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

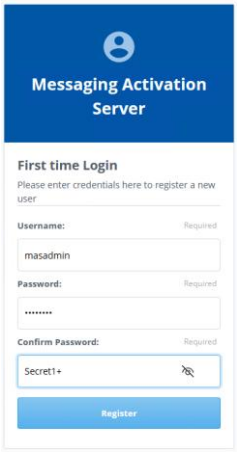
Isode Service Configuration - MAS



Browse to “https://localhost:9000”

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

MAS First Time Log in



In “Username” type “masadmin”

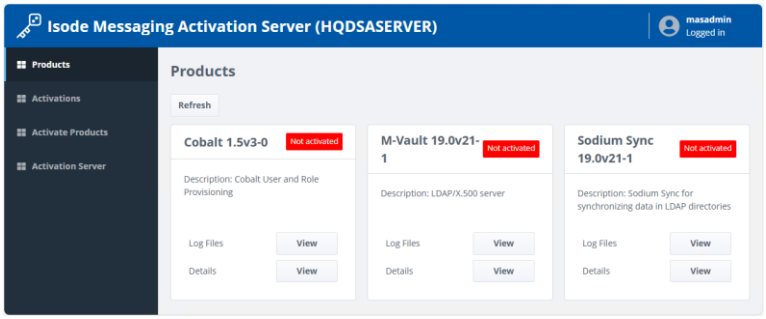
In “Password” type “Secret1+”

In “Confirm Password” type “Secret1+”

Press “Register”

You will be presented with a list of installed products.

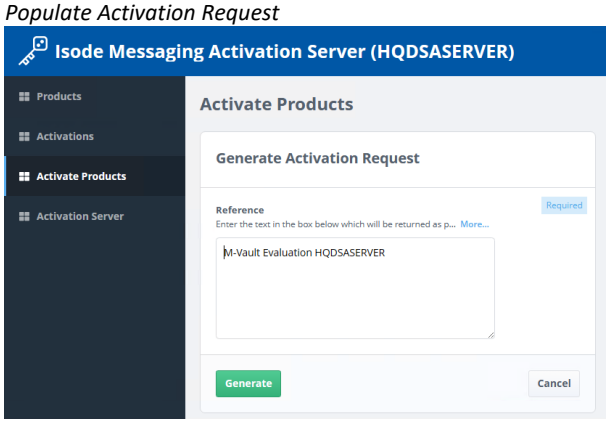
View installed Product List



Select “Activate Products”

In “Reference” type “M-Vault Evaluation HQDSASERVER” (or FIELDDSASERVER)

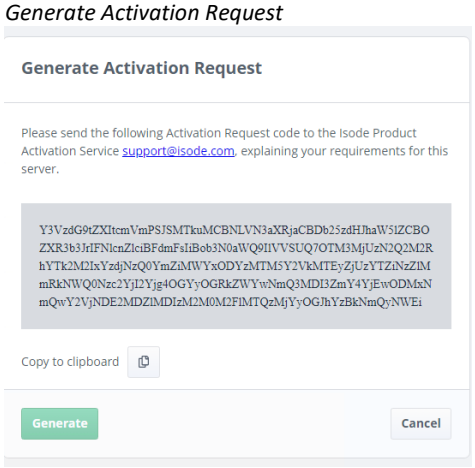
Populate Activation Request



Press “Generate”

Copy the activation request code to your clipboard.

Generate Activation Request



Send an email to Isode support asking for a Product Activation for M-Vault, Sodium Sync and Cobalt for a “R19.0 M-Vault Evaluation”. Include the activation request code.

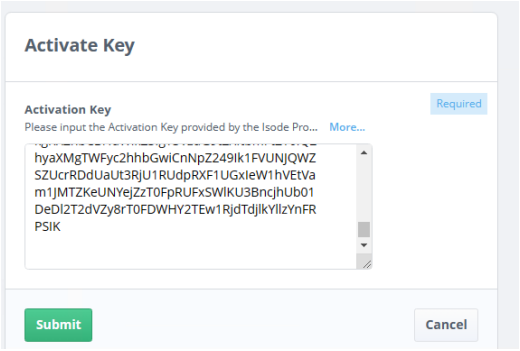
Isode support will supply a set of Product Activation keys.

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

Select “Activate Products”

Paste the keys into the “Reference” field.

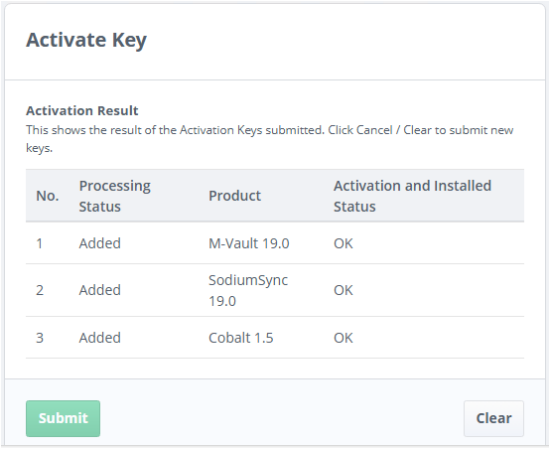
Submit Activation key



Press “Submit”.

You will be presented with an “Activation Result”

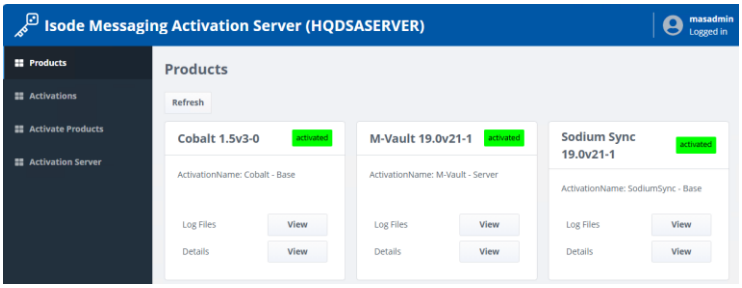
Activation result



Select “Products”

The products that have been activated should appear in green.

Activated Product List



Creating a Directory Server Using M-Vault Console

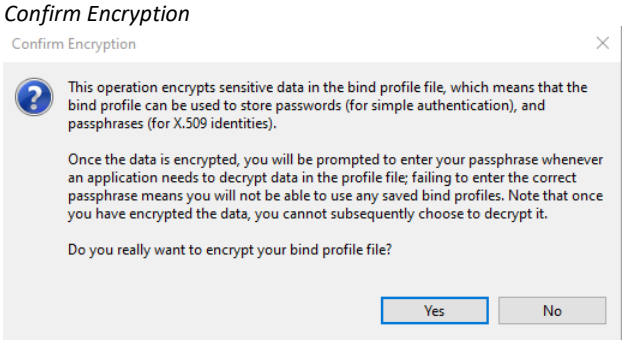
This part of the guide is written to be carried out on HQDSASERVER.

Create the DSA

Open the "M-Vault Console" from the Windows Start menu. On Linux execute the following command:

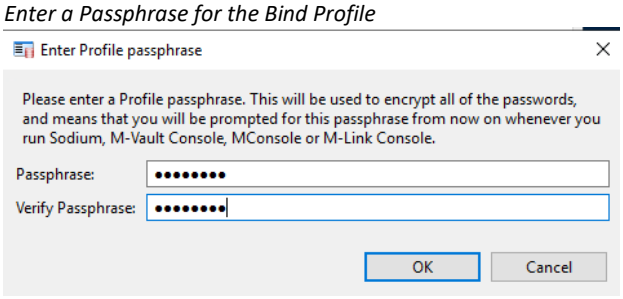
```
% /opt/isode/bin/mvc
```

Confirm Encryption



Click "Yes".

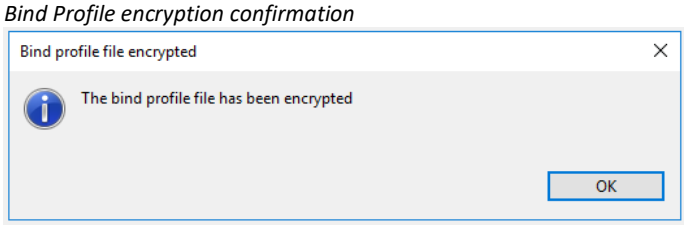
Enter a Passphrase for the Bind Profile



Enter and verify the password "Secret1+"

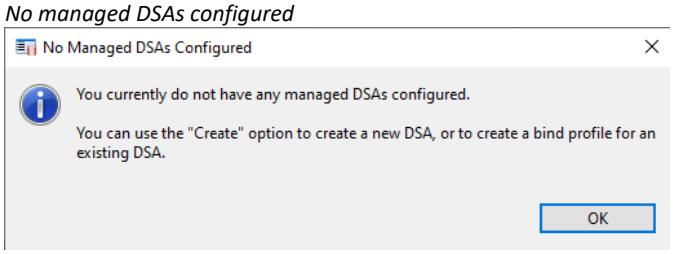
Click "OK".

Bind Profile encryption confirmation



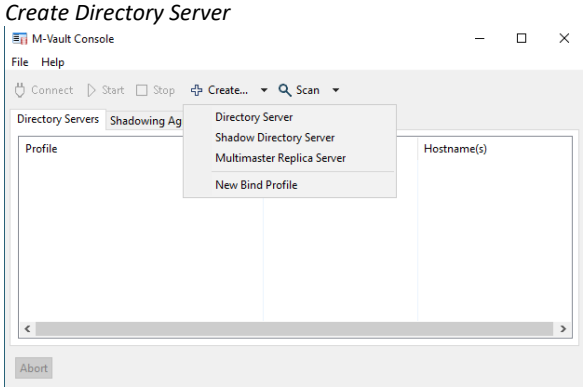
Click "OK".

No managed DSAs configured



Click “OK”.

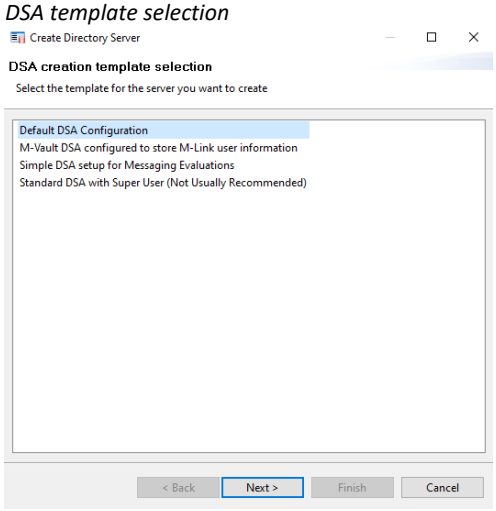
Create Directory Server



Select “Create” and then from the menu presented “Directory Server”

Click “OK”.

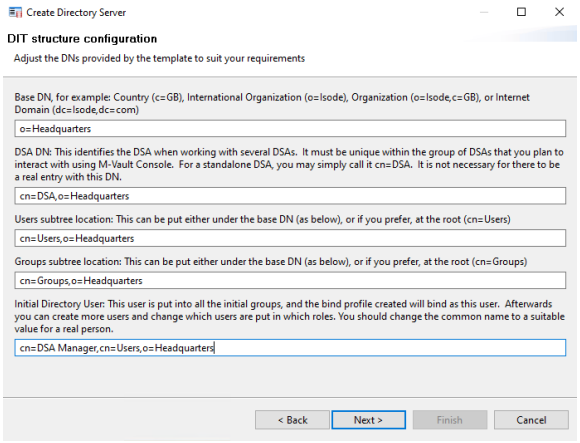
DSA template selection



Ensure “Default DSA Configuration” is selected.

Click “Next >”.

DIT structure configuration

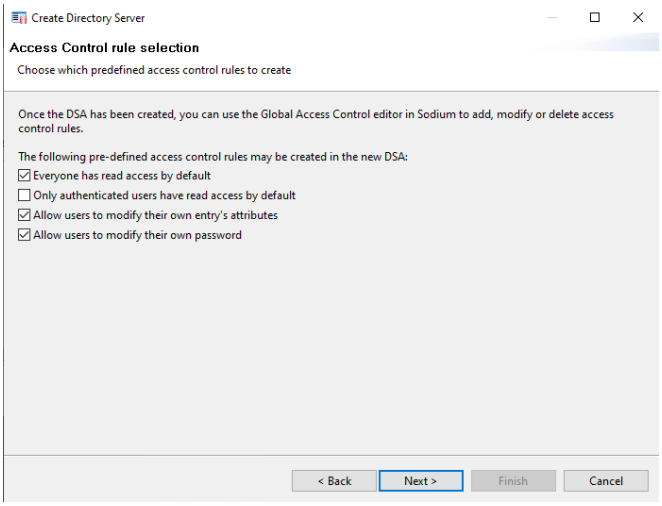


In the “Base DN” field type “o=Headquarters”

In “Initial Directory User” type “ cn=DSA Manager,cn=Users,o=Headquarters”

Click “Next >”.

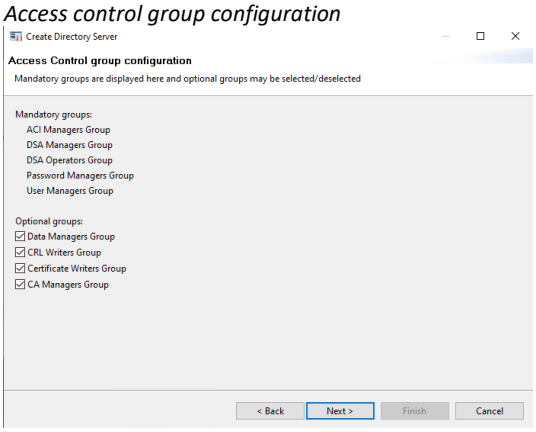
Access control rule selection



Leave the Defaults

Click “Next >”

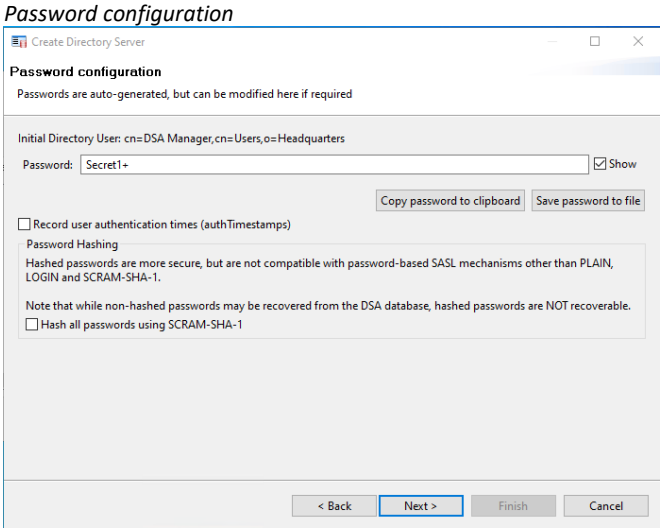
Access control group configuration



On “Access Control group configuration” ensure all optional groups are selected.

Click “Next >”

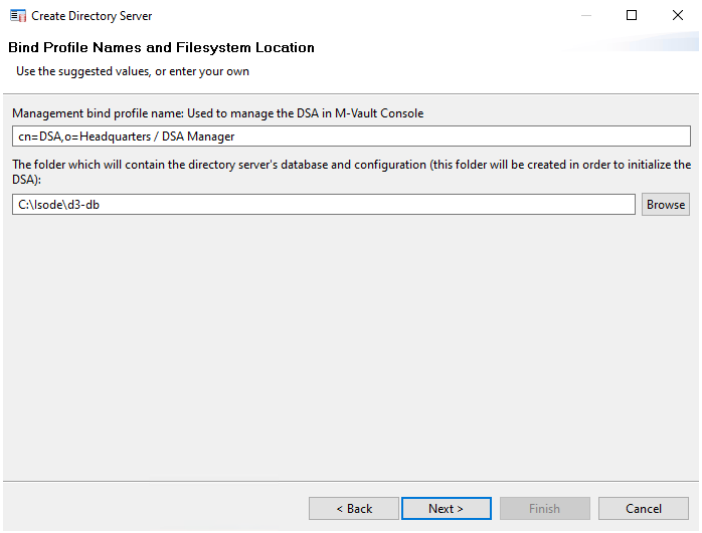
Password configuration



Provide a memorable password

Click “Next >”

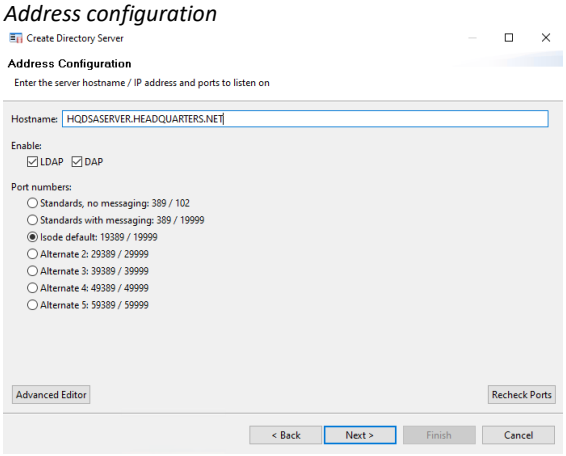
Bind Profile Names



Leave as default

Click “Next >”.

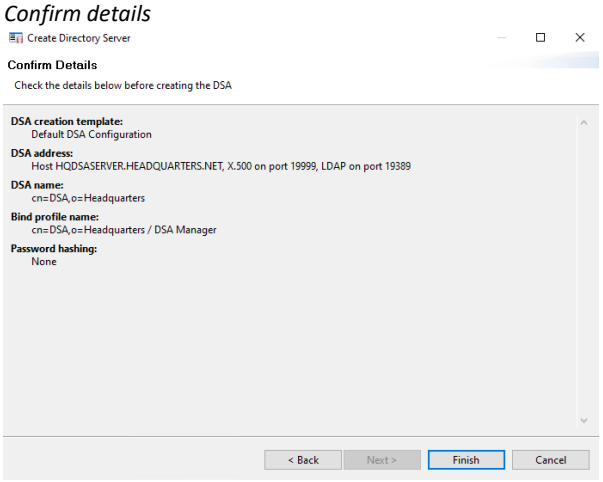
Address configuration



In “Hostname:” type “HQDSASERVER.HEADQUARTERS.NET”

Click “Next >”.

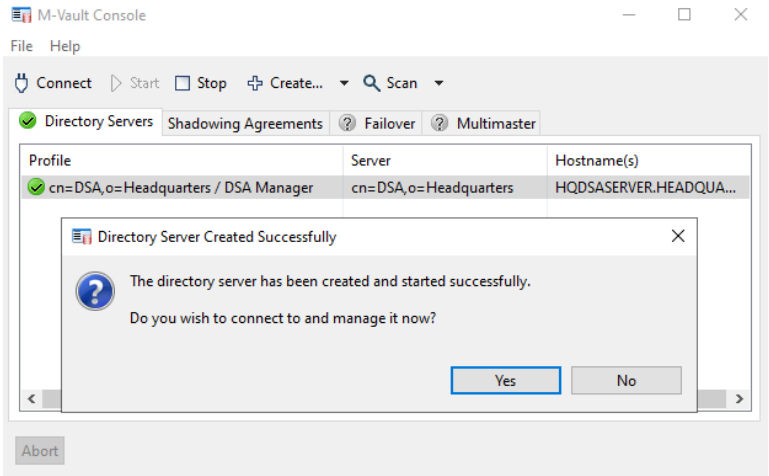
Confirm details



Click “Finish”.

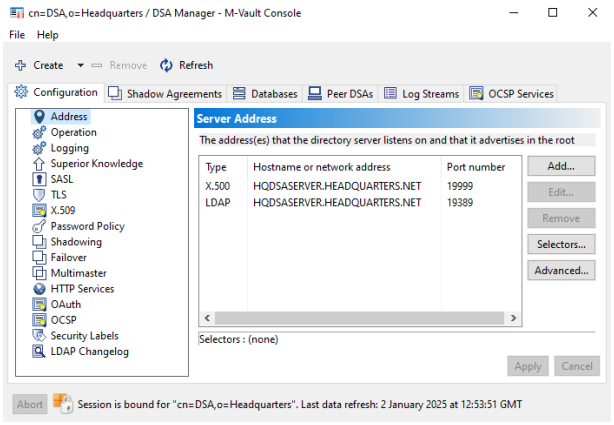
The DSA will be created and started.

DSA successfully created



Press “Yes”

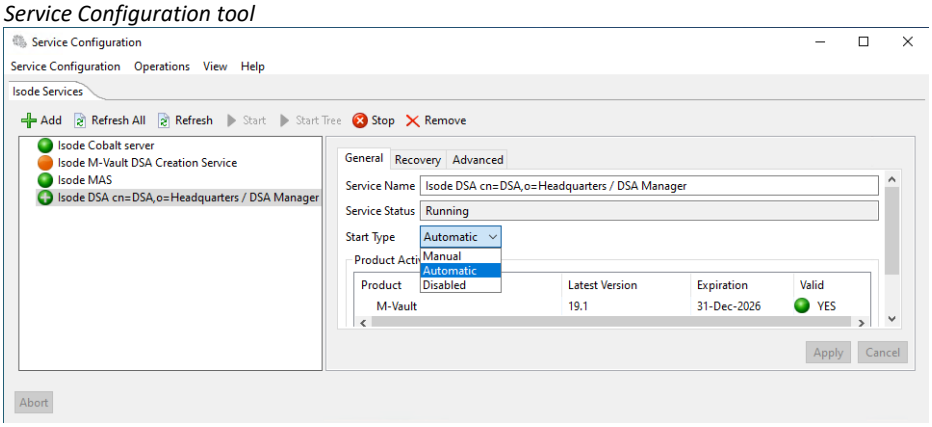
DSA configuration



It is sensible at this point to configure the dsa to start automatically with Windows.

Start the “Isode Service Configuration” tool from the Windows Start menu.

Service Configuration tool



Select the newly created DSA service in the left hand pane.

In the right-hand pane, select “Automatic” from “Start Type”

Press “Apply”

```
(Linux : systemctl enable isode-dsa@d3-db)
```

Create an Isode PKI

These steps explain how to create an Isode PKI to generate certificates.

You may skip this step if you already possess a PKI infrastructure.

Create the directory “c:\IsodeCerts”

```
(Linux:/var/isode/certs)
```

Open “Sodium CA” from the Windows start menu

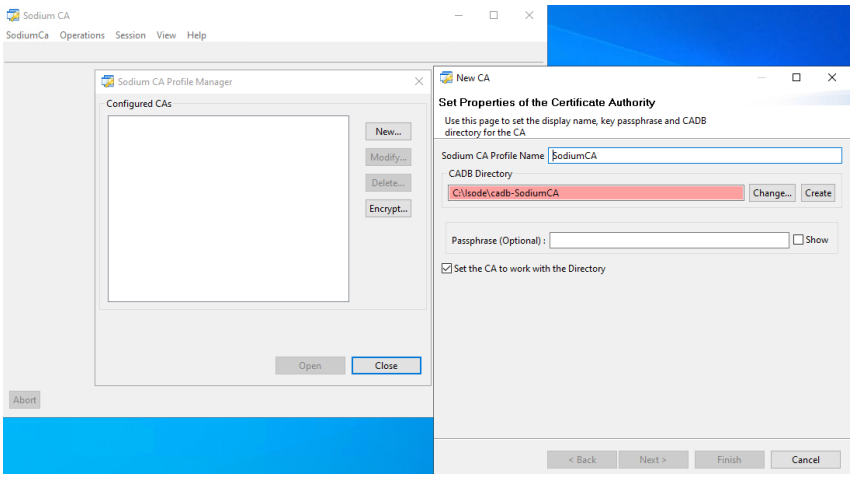
```
(Linux: %/opt/isode/sbin/sodiumca)
```

Click “New”

On “Set Properties of the Certificate Authority” leave Defaults

Click “Create”

create ca



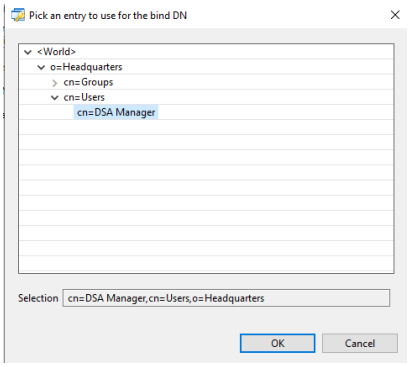
Click “Next >”

In “Hostname” type the fully qualified host name (“HQDSASERVER.HEADQUARTERS.NET”)

Click “Pick”

Browse to “cn=DSA Manager,cn=Users,o=Headquarters”

Pick CA Bind DN



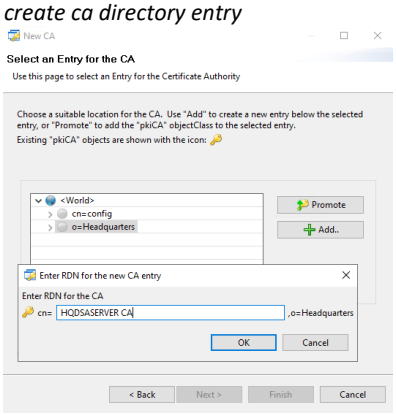
Click “OK”

Define bind password

In “Bind Password” type “Secret1+”

Click “Next >”

create ca directory entry



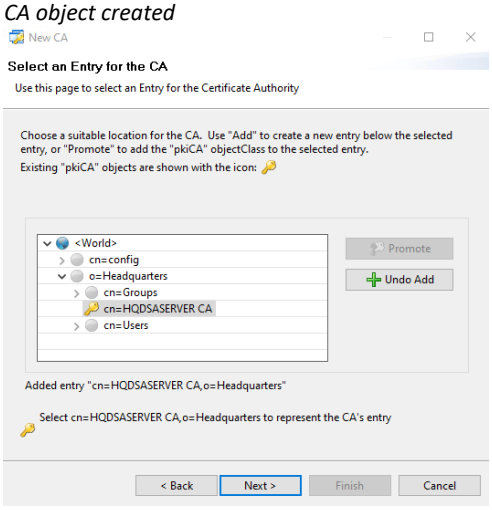
On “Select an Entry for the CA” browse to and select “o=Headquarters”

Click “Add”

On “Enter RDN for the new CA entry” type “HQDSASERVER CA”

Click “OK”

CA object created



Click “Next >”

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

Click “Next >”

On “Certificate Status Sharing” leave Defaults

Click “Next >”

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

Click “Next >”

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

Click “Next >”

On “Set Basic Constraints and KeyUsage Extension” leave defaults

Click “Next >”

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

generate self signed ca certificate

Leave the defaults.

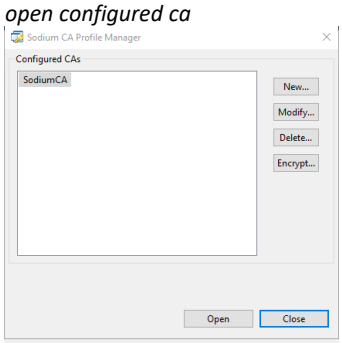
Click “Next >”

On “Root CA Certificate” leave Defaults

Click “Next >”

On “Finish CA Configuration” press “Finish”

open configured ca



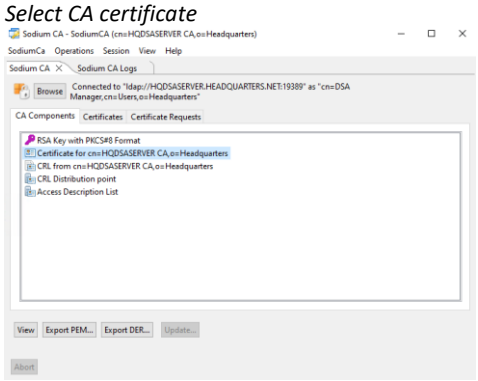
On ”Sodium CA Profile Manager” select “SodiumCA”

Click “Open”

In “Password” type “Secret1+”

Click “OK”

Select CA certificate



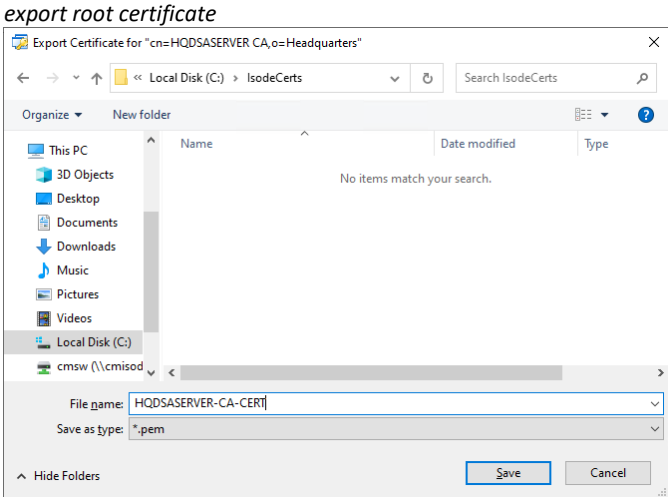
Select “Certificate for cn=HQDSASERVER, o=Headquarters”

Press “Export PEM ..”

On “Export Certificate for “cn=HQDSASERVER CA, o=Headquarters”, browse to “c:\IsodeCerts”

Change Filename to “HQDSASERVER-CA-CERT.pem”

export root certificate

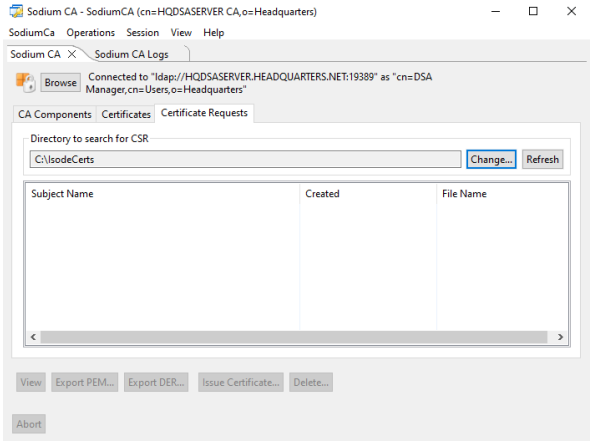


Press “Save”

On “Certificate for cn=HQDSASERVER CA,o=Messaging System” exported Click “OK”

Change to “Certificate Requests” tab

CSR directory changed

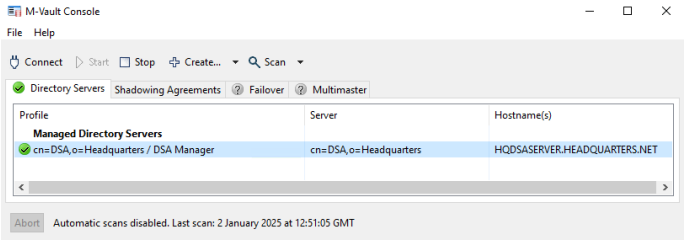


Change “Directory to Search for CSR” to “C:\IsodeCerts”

Configure M-Vault to Support TLS

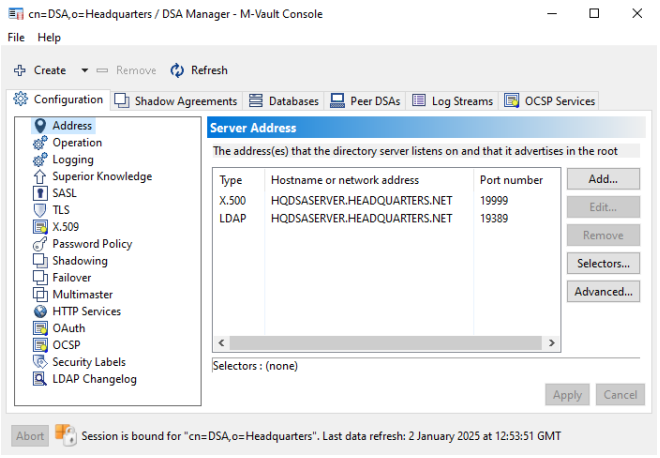
From the Windows Start menu, open “M-Vault console” and provide the password “Secret1+”

Populated M-Vault console



Double Click on the “Managed Directory server”

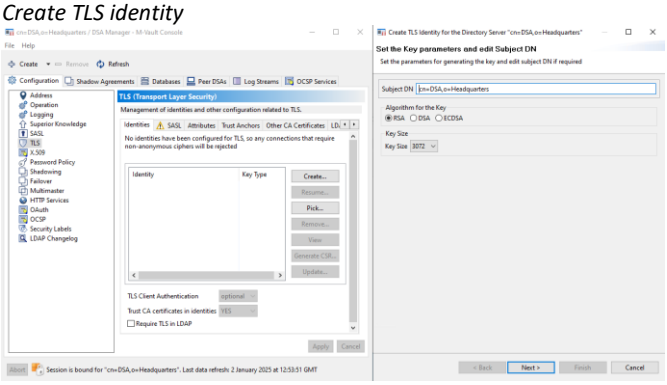
Directory configuration



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

On the “Identities” tab Press “Create”

Create TLS identity



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

Click “Next >”

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

Click “Next >”

On “Select X.509 Extensions”, leave defaults

Press “Next >”

On “Certificate Request Contents” leave defaults

Press “Next >”

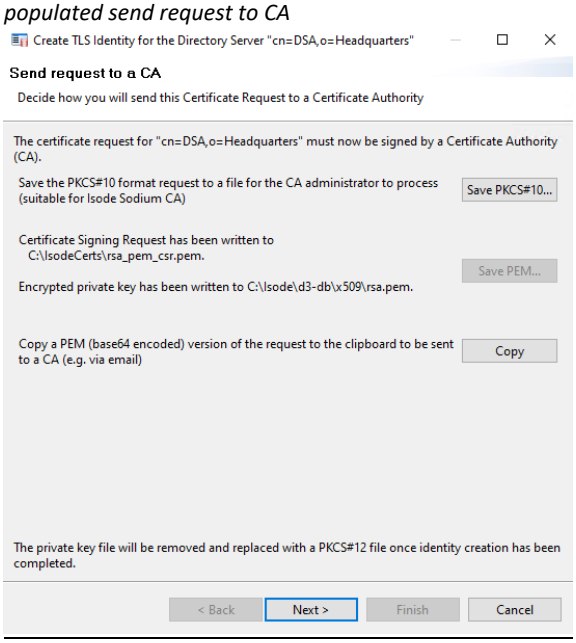
On “Send Request to a CA” press “Save PEM …”

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

Click “Select Folder”

Back on “Send Request to CA” leave defaults

populated send request to CA



Click “Next >”

In Sodium CA:

Change to “Certificate Requests” Tab

Press “Refresh”

Ensure that the Certificate request is selected

Click “Issue Certificate…”

On “Certificate Signing Request” leave defaults

Click “Next >”

On “Select and add Subject Alternative Names” leave defaults

Press “Next >”

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

Press “Next >”

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

Click “Next >”

On “Generated Certificate” press “Finish”

On “CSR Signed” Click “OK”.

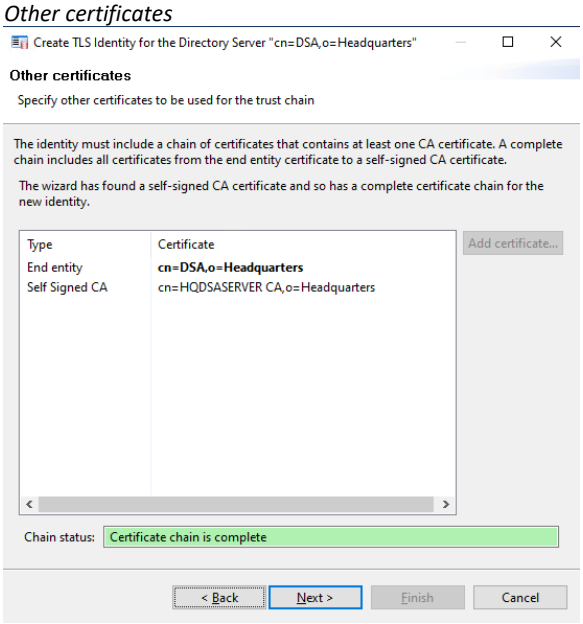
Back in in M-Vault Console:

Select “The CA has provided a certificate”

Click “Next >”

On “User Certificate” leave defaults
Click “Next >”

Other certificates



On “Other Certificates” leave defaults

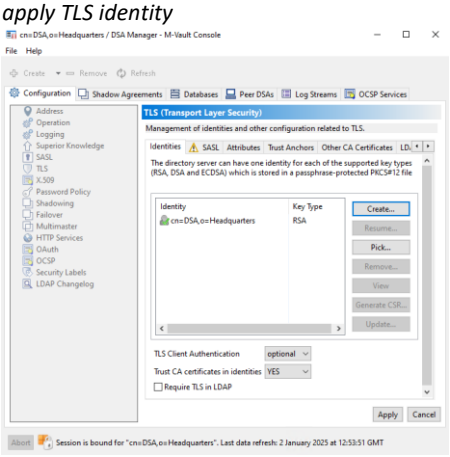
Click “Next >”

On “Finish directory servers Identity creation” leave defaults

Click “Finish”

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

apply TLS identity



On “Configuration” tab press “Apply”

Close “M-Vault Console”

Go to the “Isode Service Configuration” tool.

Select “Operations/Stop all”

Wait for the services to stop

Select “Operations/Start all”

Populating and Browsing a Directory using Sodium

Isode provides a Directory User Agent (DUA) called Sodium as part of the M-Vault installation. Sodium can be used to manage user information in a directory. In this section we're going to use Sodium to add some entries to the directory in pursuit of the DIT described in the section of this guide on Terminology.

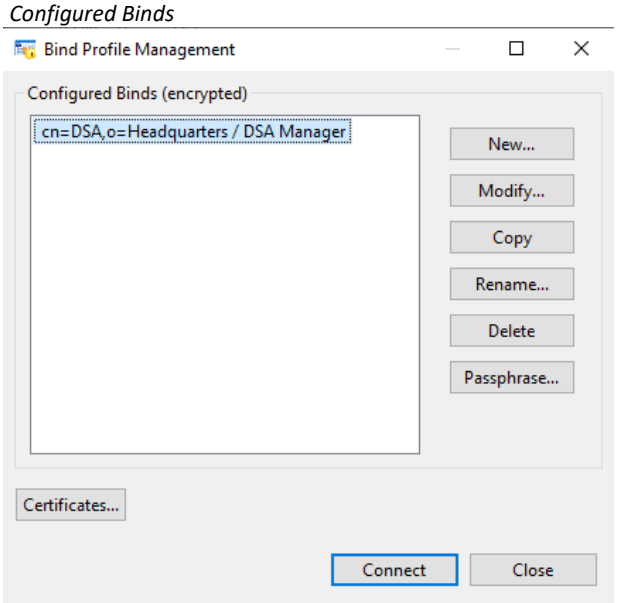
Sodium can be launched from the windows start menu.

```
(Linux: %/opt/isode/bin/sodium)
```

Binding to a Directory Server

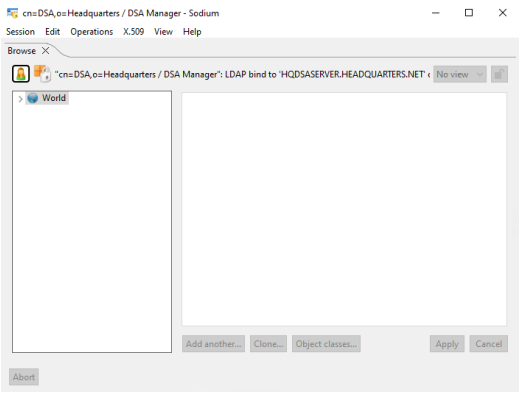
On startup, Sodium will ask you for the Bind Profile passphrase you set earlier and will then list your configured binds. In our case, we have only one.

Configured Binds



You can use the Bind Profile Management screen to modify a profile or copy it as a template for other connection configurations but we're simply going to connect to the directory. Ensure the bind profile is selected and press “Connect”.

Initial world view



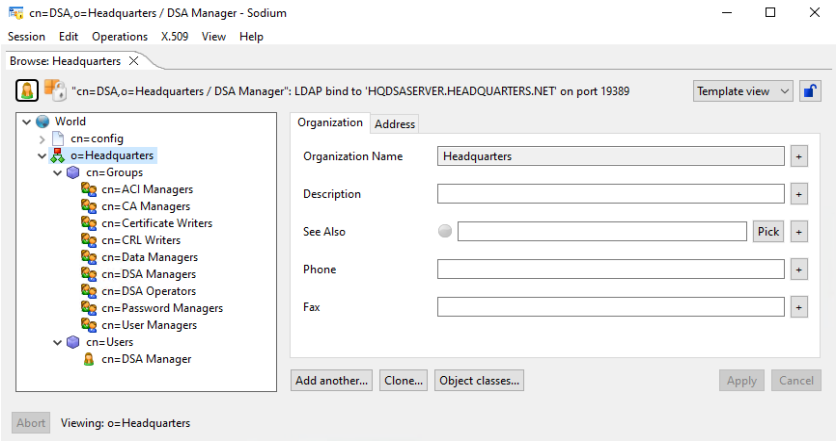
You are now connected to the Directory Server and the initial World view is displayed.

Bulk-loading entries from a sample LDIF file

M-Vault ships with a number of sample LDIF (LDAP Data Interchange Format) files. We're going to load the default Headquarters.net data. Normally when bulk-loading data you would use the “Bulk Tools” option in the Operations menu. The sample data sets are loaded from the Help menu.

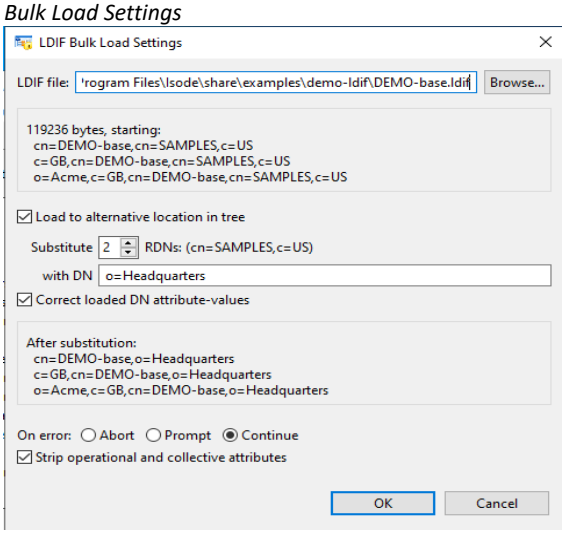
Data cannot be loaded directly under 'World' so firstly expand the tree to reveal the current entries in the DIT. Clicking on any entry in the DIT will cause Sodium to read the entry in the Directory Server and display the results in the right-hand pane.

Browsing the DIT



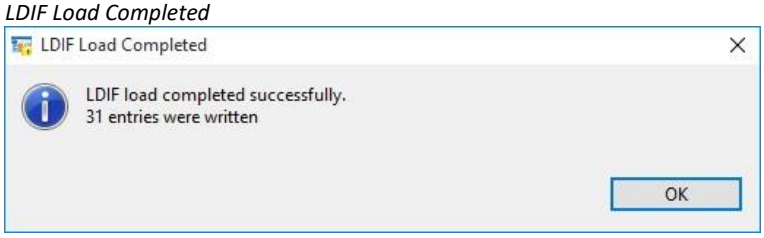
Make sure that you have the 'Headquarters” entry selected and then select “Help > Load Demo Data” from the menu. Click “OK” after reading the information popup and you'll be presented with the LDIF Bulk Load Settings screen.

Bulk Load Settings



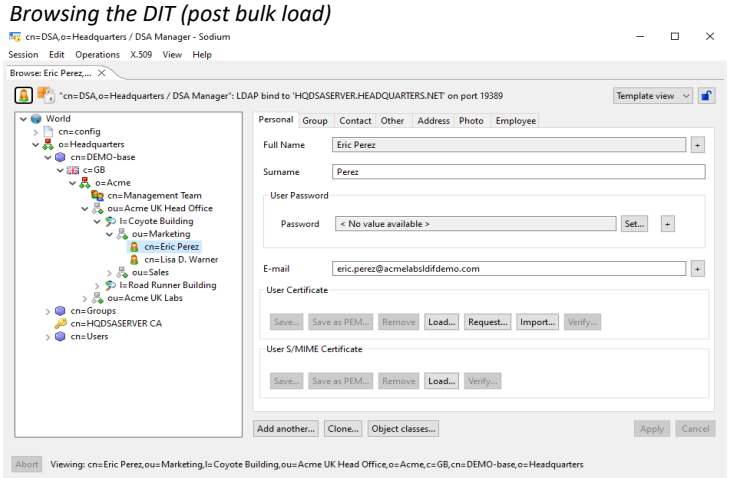
Accept these default settings by pressing “OK”.

LDIF Load Completed



Clicking on “OK” will return you to the main Sodium screen and if you now expand the entries under “Headquarters” you'll see that the sample data set has been loaded and now reflects the organizational diagram which we part examined in an earlier section. Clicking on any of the entries will reveal the detail of that entry in the right-hand pane (grouped into tabbed views).

Browsing the DIT (post bulk load)

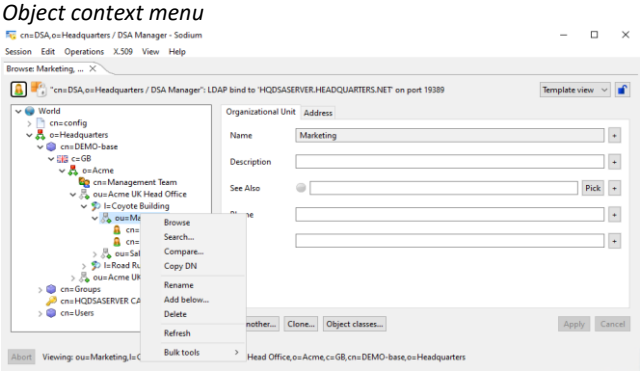


Adding an Entry/Entries using Sodium

As we have seen, the left-hand pane of the Sodium interface shows a hierarchical tree view of the directory. Right-clicking on an entry in the DIT allows you, amongst other things, to add entries below the one you have selected.

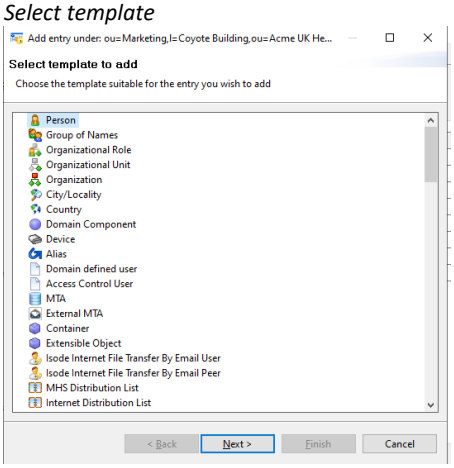
In this section we're going to add another staff member to the Marketing department.

Object context menu



Right click on the "ou=Marketing" entry and select “Add Below”

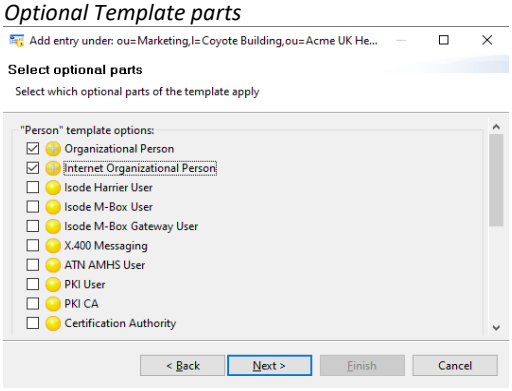
Select template



Select 'Person' from the Template list.

Press “Next >”

Optional Template parts



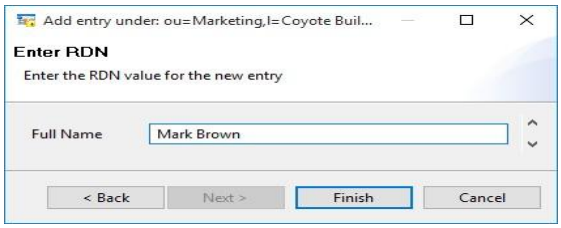
Select optional template parts: 'Organizational Person' and 'Internet Organizational Person'.

Note that some of these templates have linked dependencies, so when clicking on 'Internet

Organizational Person', Sodium will automatically include the required Organizational Person template

Press “Next >”

Enter RDN

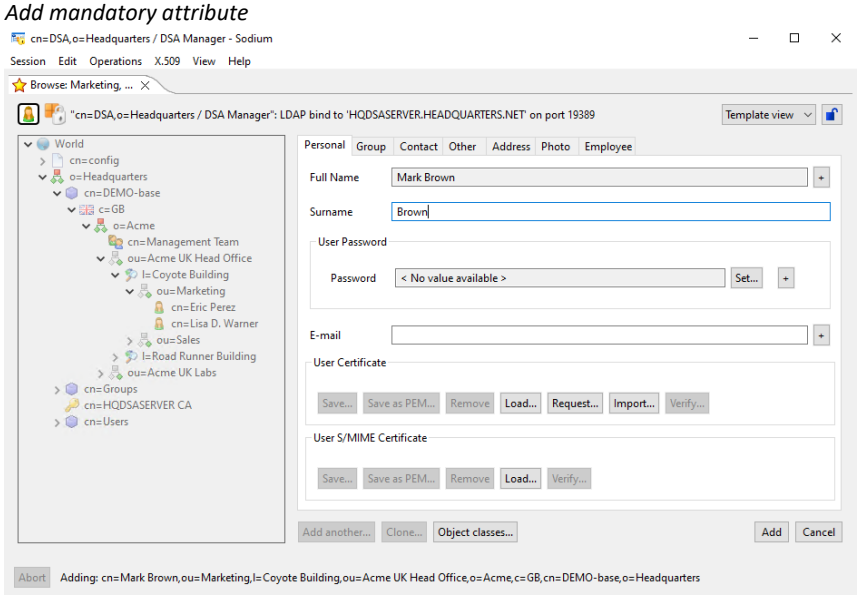


Add the full name of the person being added to the directory.

Click “Finish”

In most cases there will additional mandatory attributes needed before the record can be committed (in this case it's Surname) and these will be highlighted.

Add mandatory attribute



Type the required attribute of "Brown".

Press “Add”

It is possible to quickly add another entry of the same type by clicking “Add Another”

For later use, add an additional object “Cobalt Data” of type “Container below “o=Headquarters”

Modifying and Deleting an Entry

You can modify any entry in the tree by clicking on it and using the entry detail tabs displayed to the right. If you change any of the values for the entry, Sodium will enable an Apply button which, when clicked, will cause Sodium to attempt to modify the directory entry with the changes.

You can delete an entry from the DIT by right-clicking on it and pressing “Delete” Please note that you cannot remove an entry with subordinate entries. In order to remove an entry and its subordinate entries you can use the menu item 'Bulk Tools / Delete Subtree 'when right-clicking on an entry.

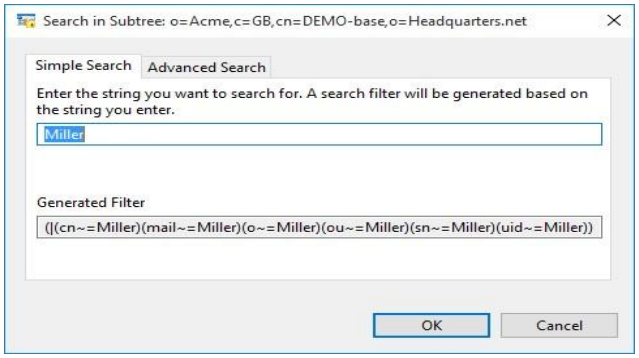
Searching

You can search the DIT by right-clicking on an entry and selecting 'Search' from the pop-up menu or by clicking on an entry and selecting 'Operations / Search' from the main toolbar. In both cases a search will be performed on all entries below the currently selected one.

Try this operation with the o=Acme entry. Select 'o=Acme' and bring up the search box.

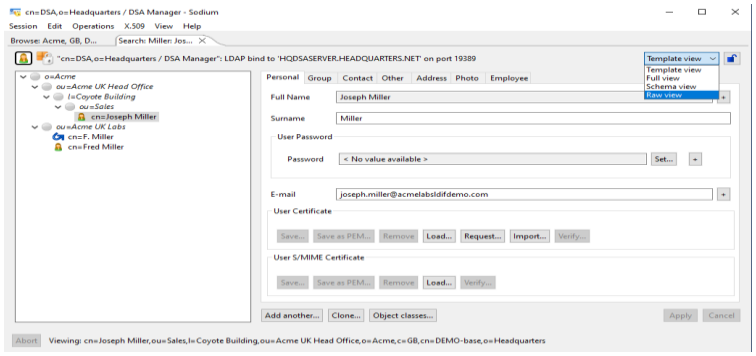
In this example we're going to search for entries containing 'Miller'

Search in Subtree



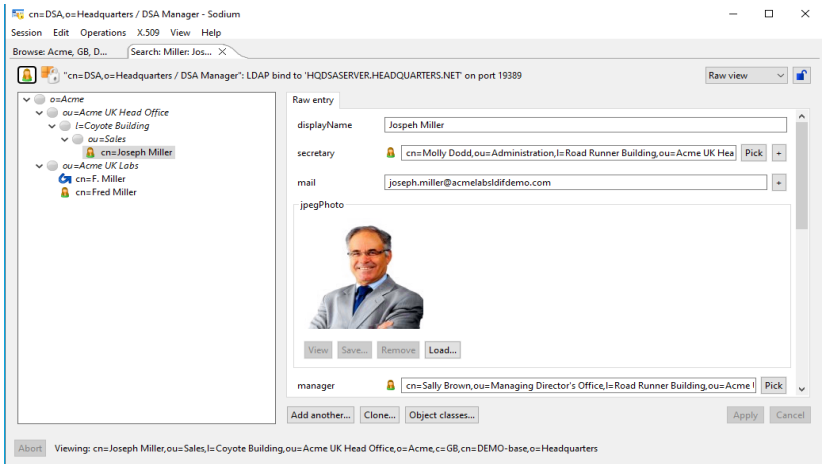
Click “OK” and Sodium will return the results in a separate Tab, showing the entries that match the search request and their position in the DIT. Up to this point we've been viewing entries in Template mode.

Search results



For a fuller view of the data you can switch to Raw view using the drop-down menu in the top right-hand corner:

Raw view



Creating a Directory Server Using Cobalt

This part of the guide is written to be carried out on FIELDDSASERVER.

It is possible to create a directory using the Cobalt web application. Cobalt can then be used to manage certain aspects of the DIT.

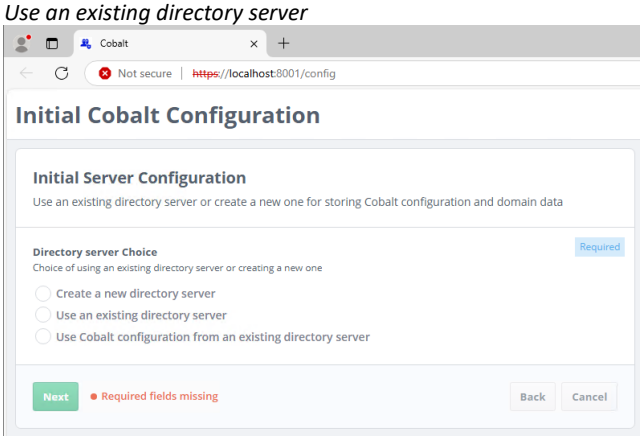
Start the "Isode M-Vault DSA Creation Service"

Initial Cobalt Configuration.

Browse to "https://localhost:8001"

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

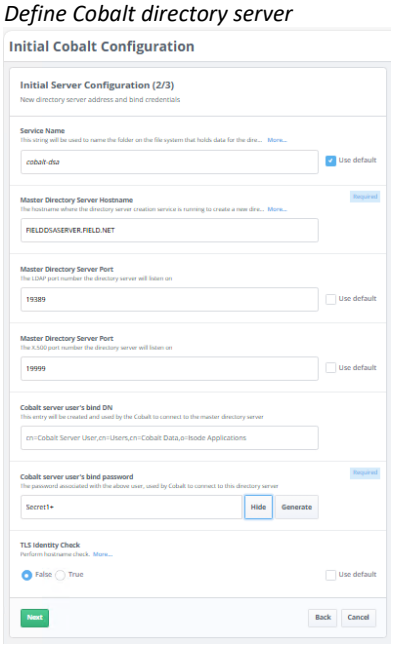
Use an existing directory server



On "Initial Server Configuration" select "Create a new directory server"

Press "Next"

Define Cobalt directory server



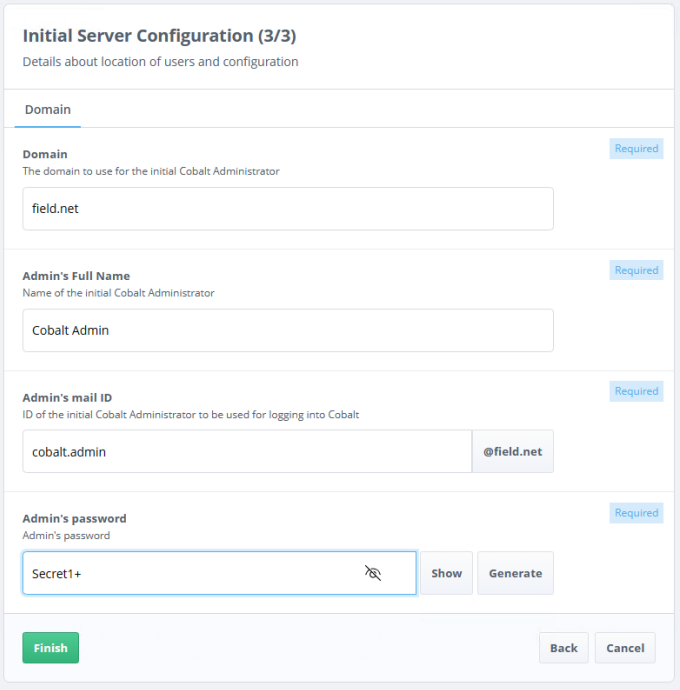
Ensure the "Master Directory Server Hostname" correctly references your server

Set "TLS Identity Check" to "False"

Type the “Cobalt server user’s bind password”

Press “Next”

Define Cobalt domain



Set the “Domain” to be “field.net”

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

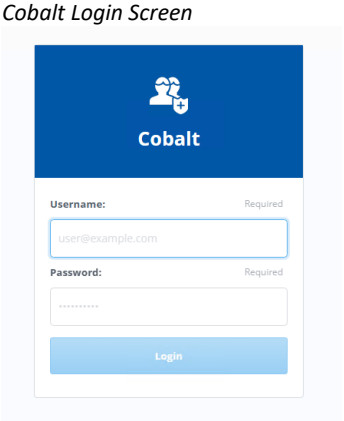
We will use “Cobalt Admin”

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

Click “Finish”.

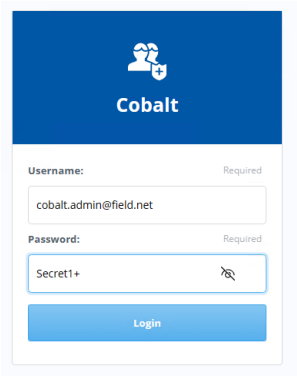
You will be presented with the Cobalt login screen.

Cobalt Login Screen



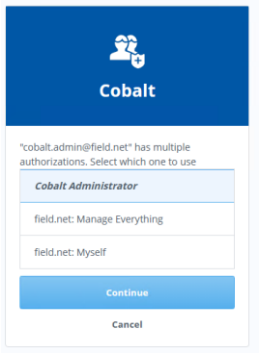
Enter the Cobalt Admin Email address and password

Cobalt login credentials



Click “Login”.

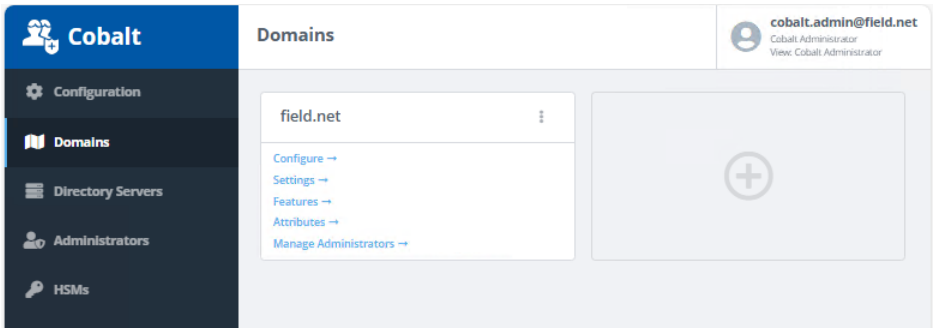
Cobalt Role Selection



Select “Cobalt Administrator” role.

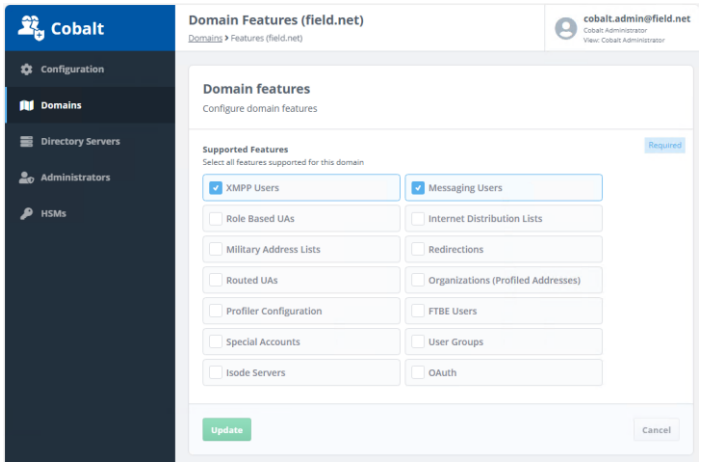
Click “Continue”.

Cobalt domains



Press “Features”

Domain Features

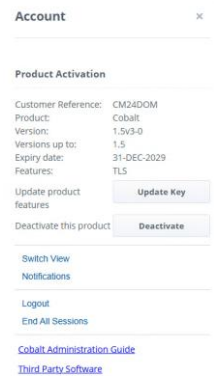


Note the range of features that can be provided by Cobalt.

Add Directory Objects

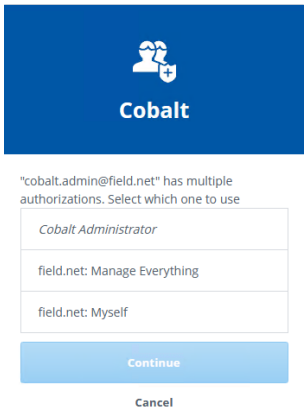
We will switch to the “field.net: Manage Everything” Role. Click on “cobalt.admin@field.net” in the top right corner.

Cobalt change role



Click “Switch View”.

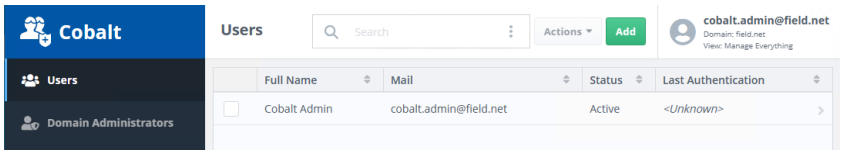
Switch view



Select “field.net: Manage Everything”

Click “Continue”.

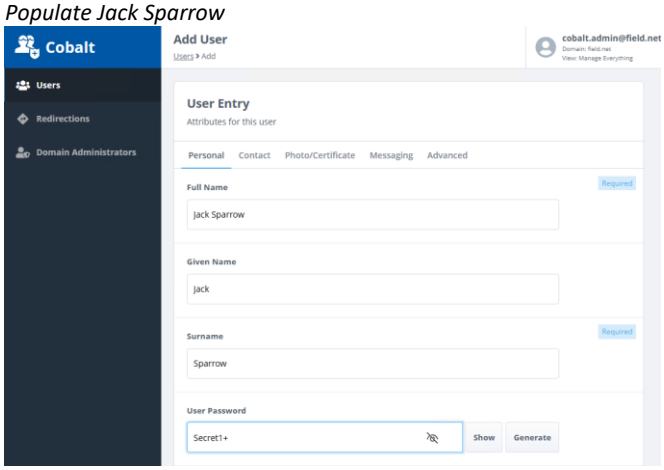
Field.net users



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

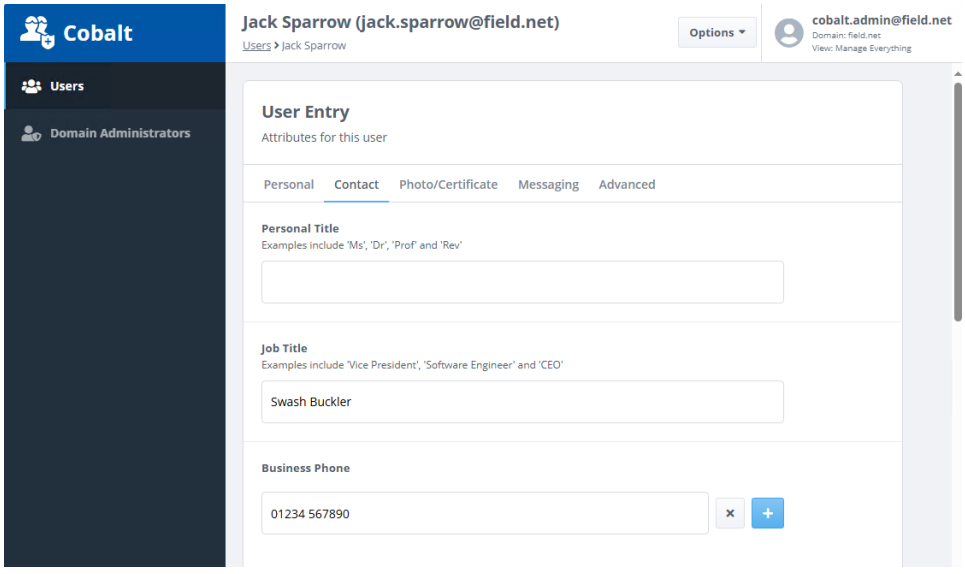
Populate details for "Jack Sparrow", starting with his name. Give Jack a password. You may want to add a wide variety of user information via this dialogue. This information may also include picture or certificate information. Please feel free to explore the tabs available to see the information that could be stored.

Populate Jack Sparrow



Change to the "Contact" tab.

Cobalt Contact tab



In the "Job Title" field, type a job title

In the "Business Phone" field, type a telephone number

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

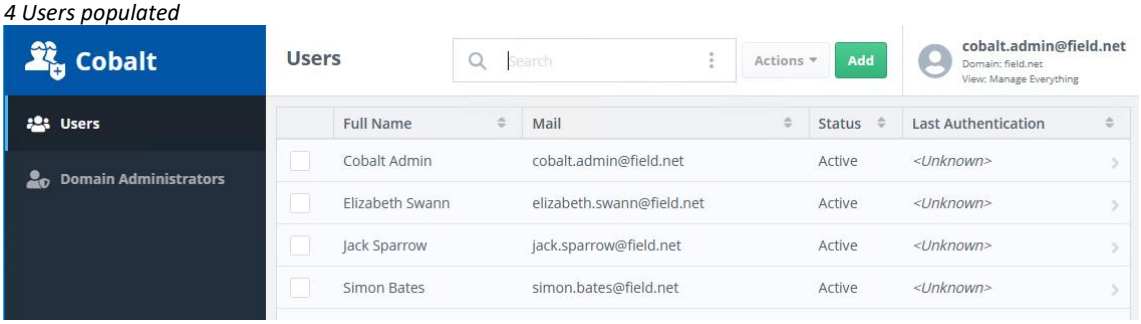
Note that "Jack Sparrow" has been added to the directory

Repeat the above steps to add the additional two objects from the table below:

Display Name	Internet Address
Jack Sparrow	jack.sparrow@field.net
Elizabeth Swann	elizabeth.swann@field.net
Simon Bates	simon.bates@field.net

You should now have 4 users populated

4 Users populated

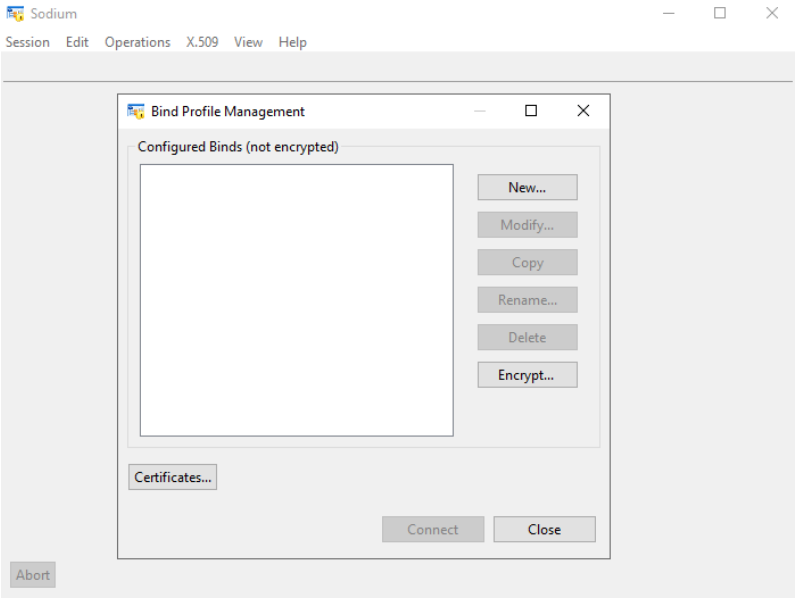


Locate Cobalt data in the Directory

Create a Bind Profile

Launch “Sodium” from the Windows Start Menu

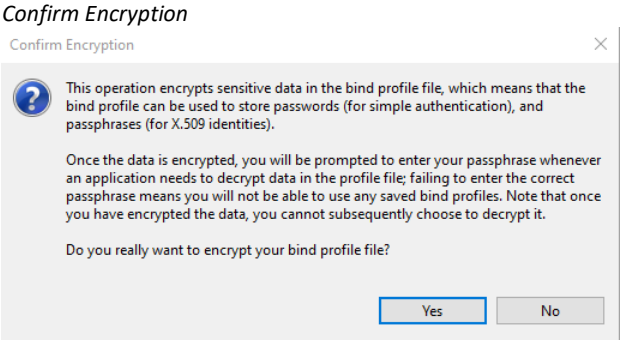
Sodium bind manager



Note that no Binds are configured and that the bind profile isn’t encrypted.

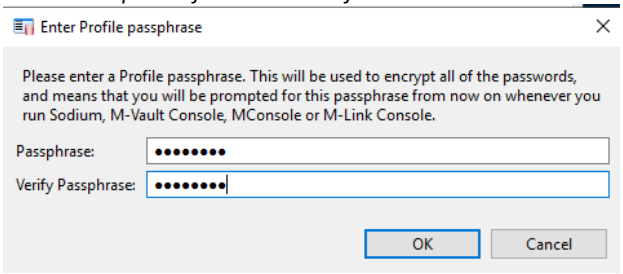
Press “Encrypt …”

Confirm Encryption



Click “Yes”.

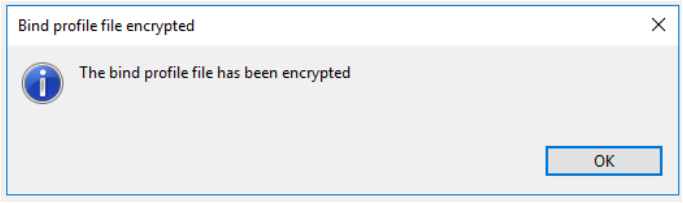
Enter a Passphrase for the Bind Profile



Enter and verify the password “Secret1+”

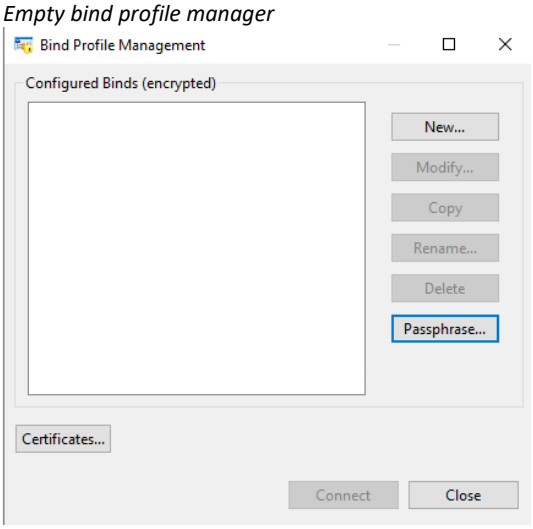
Click “OK”.

Bind Profile encryption confirmation



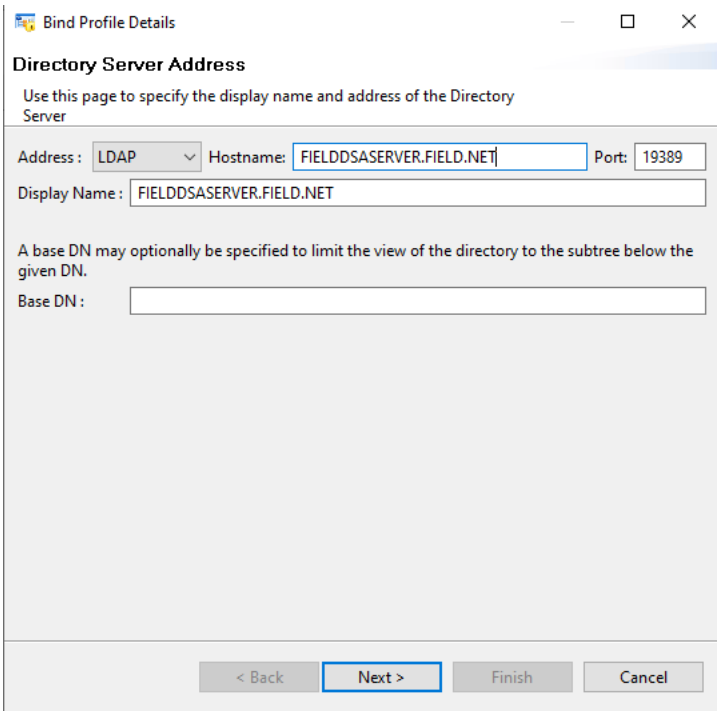
Click “OK”

Empty bind profile manager



Press “New ...”

Provide dsa server address

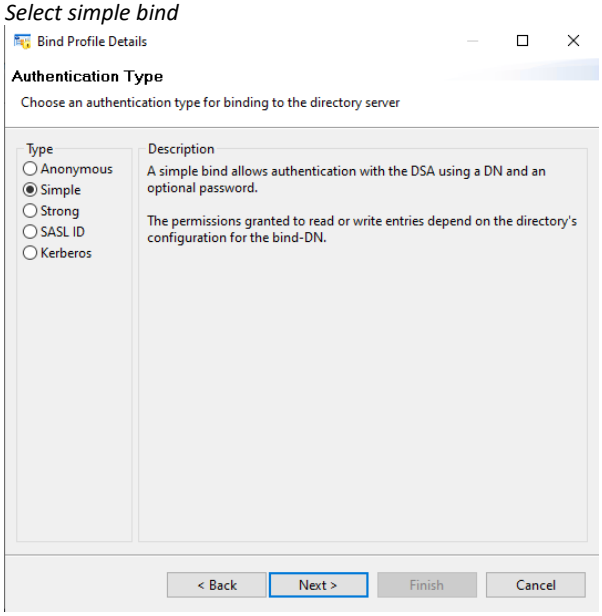


Select “LDAP” from the “Address” dropdown

In “Hostname” type “FIELDDSASERVER.FIELD.NET”

Press “Next >”

Select simple bind



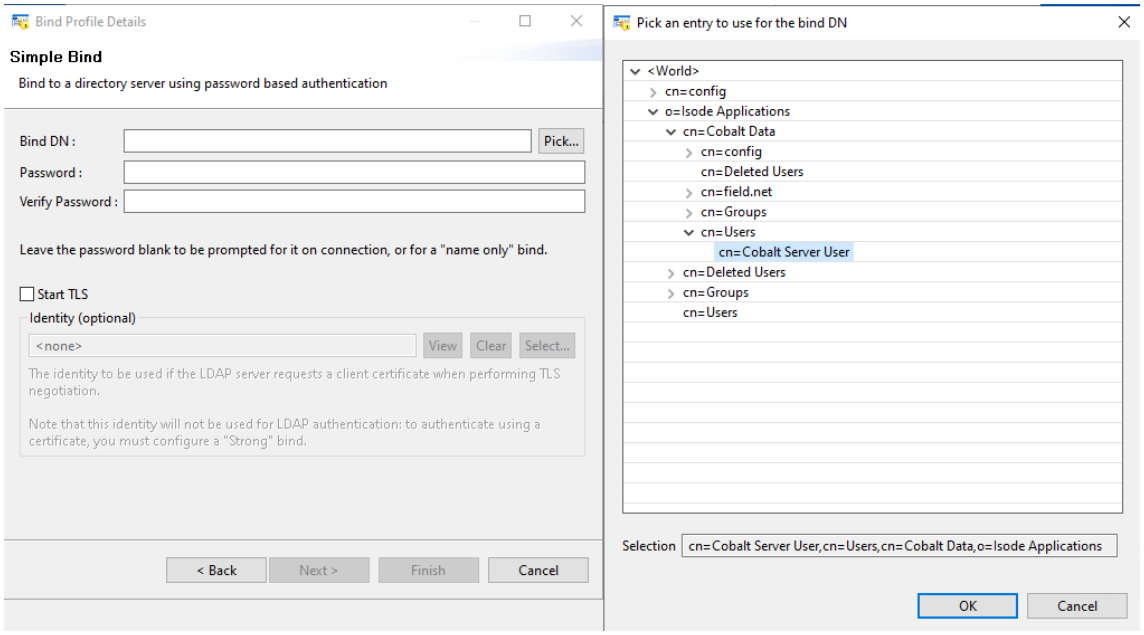
Select “Simple”

Press “Next >”

On “Simple Bind” press “Pick …”

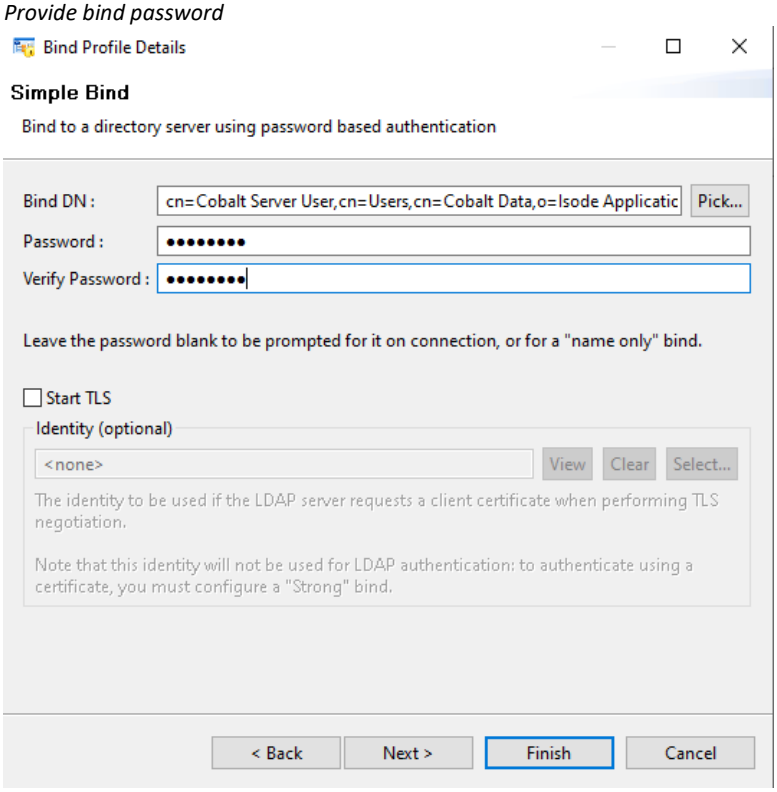
Browse to and Select “cn=Cobalt Server User,cn=Users,cn=Cobalt Data,o=Isode Applications”

Select bind dn



Press “OK”

Provide bind password



In “Password” and “Verify Password” type “Secret1+”

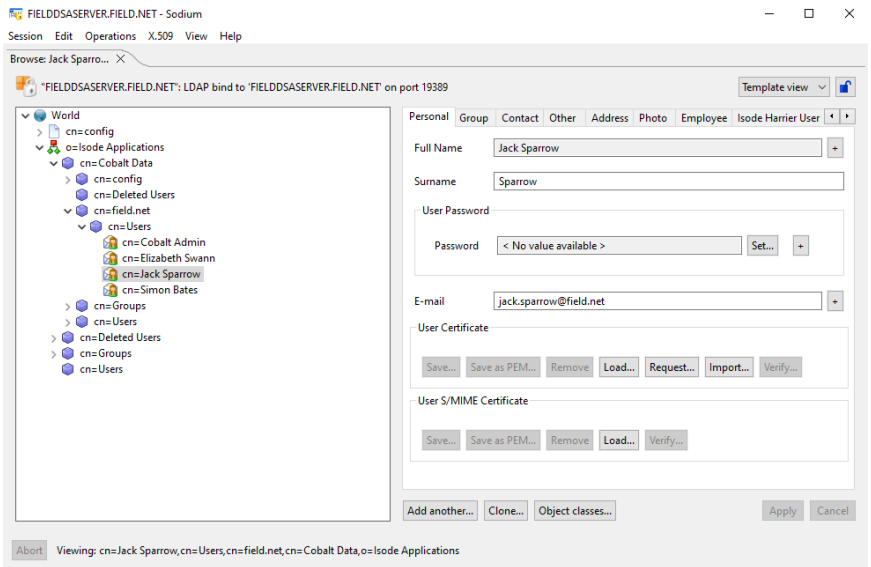
Press “Finish”

Locate the Cobalt Data using Sodium

Open Sodium using the bind profile just created.

Browse to the object “Jack Sparrow” which has the dn “cn=Jack Sparrow,cn=Users,cn=field.net,cn=Cobalt Data,o=Isode Applications”

Jack Sparrow cobalt object



Note the three users added via Cobalt and attributes of the Jack Sparrow User.

Synchronising the Directories Using Sodium Sync

Sodium Sync Overview

Sodium Sync provides a mechanism to copy a set of data from a source Directory Server to a target Directory Server, and to ensure that the target remains up to date by performing regular updates to take account of any subsequent changes in the source Directory Server.

Synchronization occurs in one direction only: whilst changes, additions and deletions made to data held on the source Directory Server will be copied to the target. Any local changes made to data in the target Directory Server will not be copied back to the source, and will normally be lost when the next synchronization operation takes place.

In particular Sodium Sync is designed to be able to handle synchronization from non-Isode DSAs (for example Active Directory) to Isode's M-Vault. Sodium Sync has a number of features to make it easier to deal with translation between directories which are not completely compatible with one another.

When configuring the synchronization operation, Sodium requires that you specify: the base of a subtree in the source Directory from which entries will be copied, the location of the entry in the target Directory that will form the base of the copied subtree; any existing entries under this base entry on the target will be deleted.

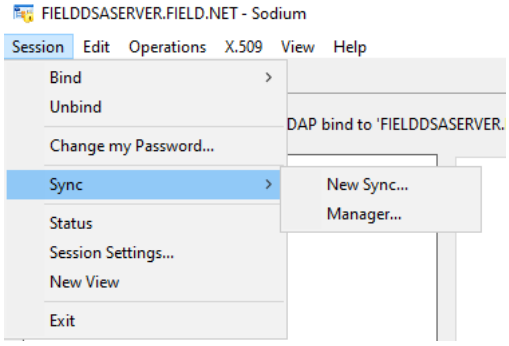
Sodium Sync will automatically rename entries if the source and target base DNs are different, and it is possible to synchronize between two separate subtrees on the same Directory.

Running a Simple Sync (M-Vault to M-Vault)

In this example we will configure a simple synchronization between two M-Vault directories (hqdsaserver and Fielddsaserver) using Sodium Sync.

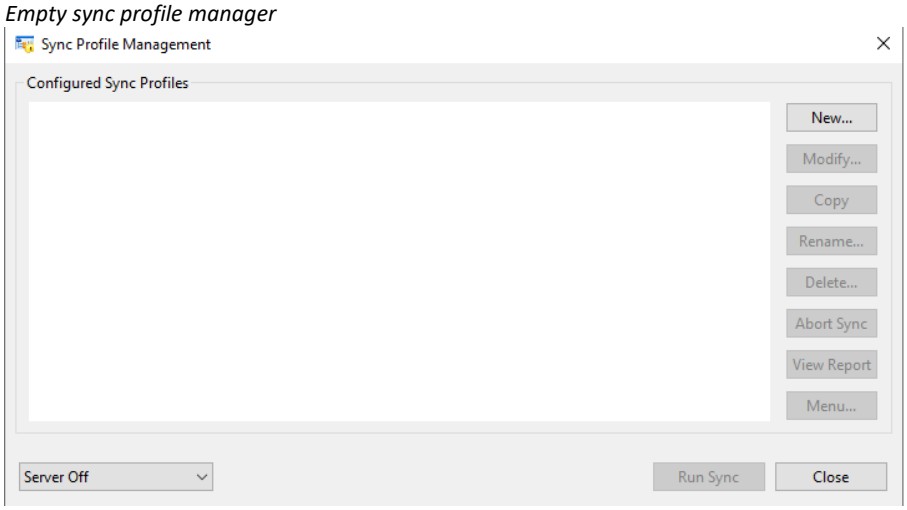
Open Sodium on the fielddsaserver.

Sodium sync menu



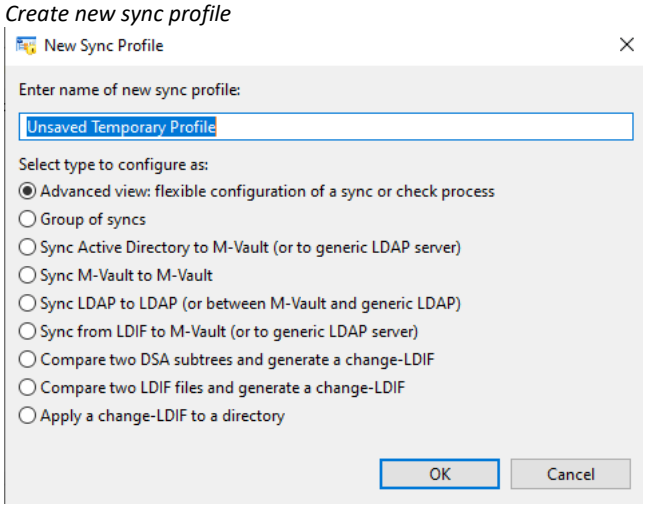
Select “Manager” from the “Session/Sync” menu.

Empty sync profile manager



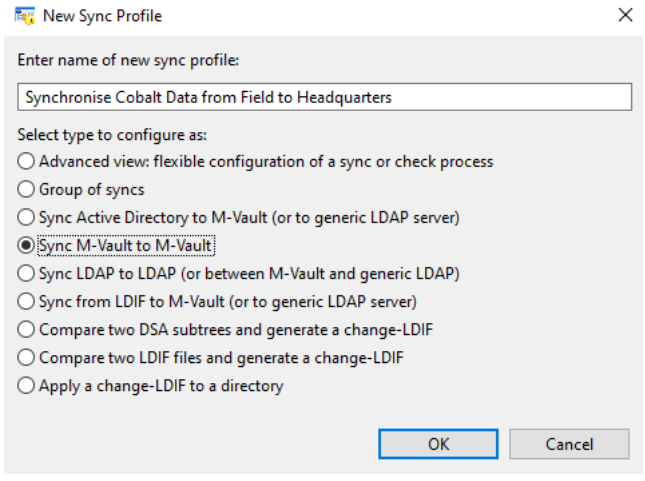
Press “New”

Create new sync profile



Select “Sync M-Vault to M-Vault”

Name sync profile

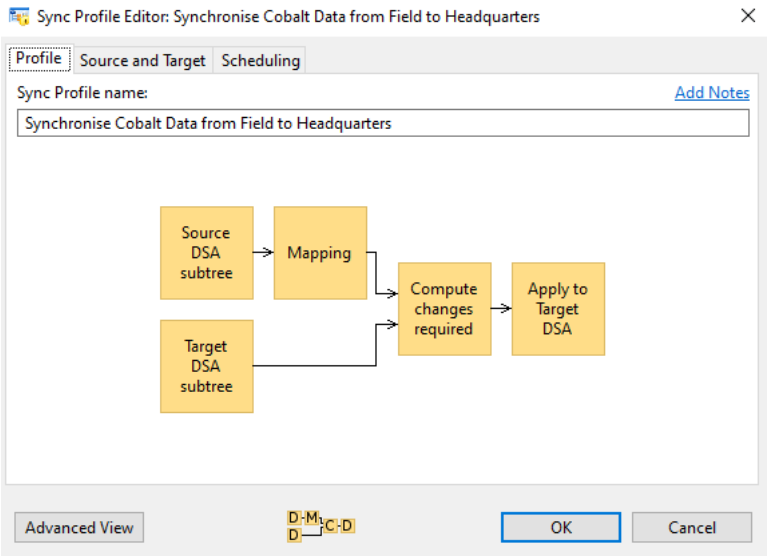


Give the profile a meaningful name.

Press “OK”

The “Sync Profile Editor” is displayed.

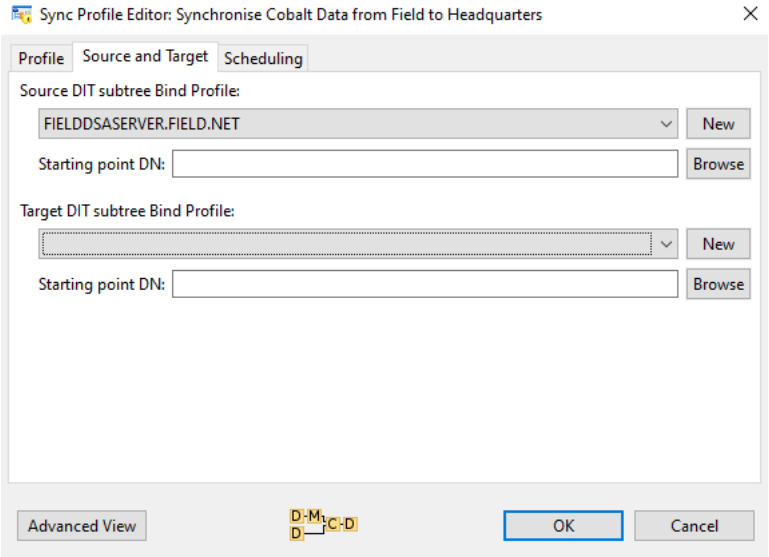
Sync profile editor



The flow diagram shown in the editor illustrates the flow of data during the synchronization process. In this case source DSA subtree entries are read, then mapped, and glue entries added if required. This is then compared to the target DSA subtree to find what changes need to be made, which are finally applied to the target DSA.

Select “Source and Target” tab.

Source and target

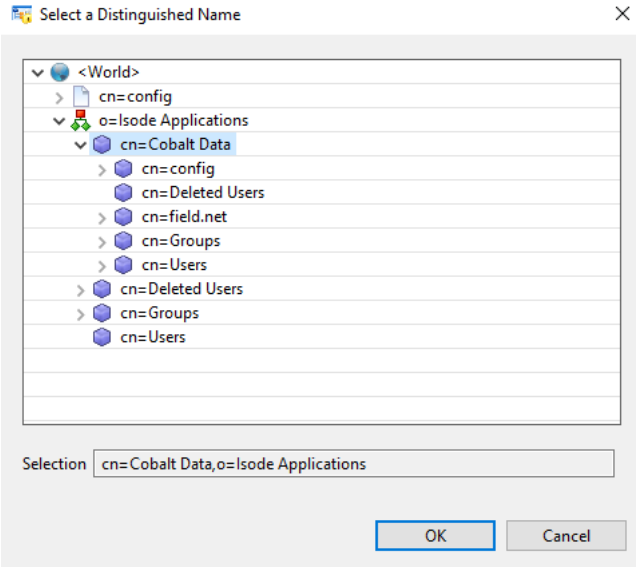


For “Source DIT subtree Bind Profile” select “FIELDDSASERVER.FIELD.NET

Select “Browse” for the “Starting point DN” for the Source DIT.

Browse to and select the object “cn=Cobalt Data,o=Isode Applications”

Select Cobalt data object

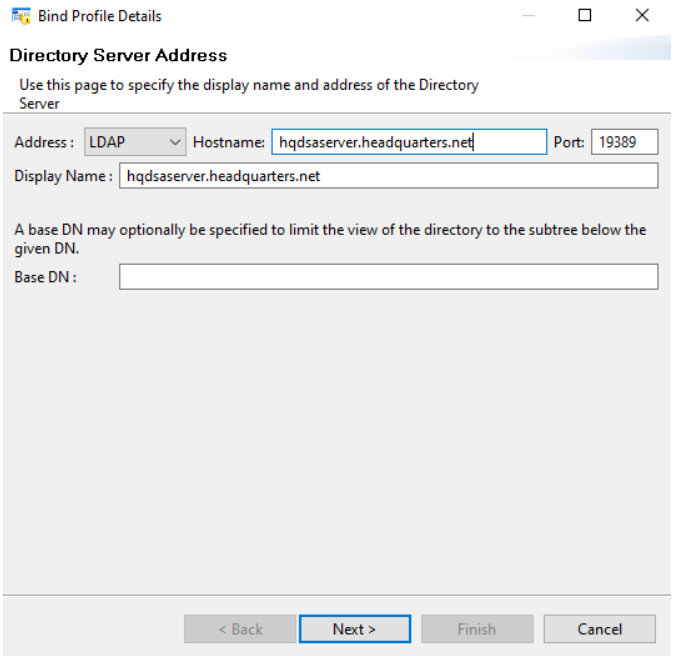


Press “OK”

Press “New” for the “Target DIT subtree Bind Profile”

Provide connection details to the headquarters DSA

Define target dsa address

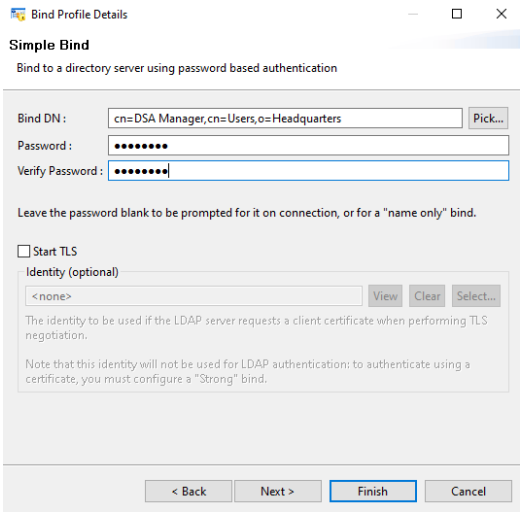


Press “Next >”

On “Authentication Type” Select “Simple”

Press “Next >”

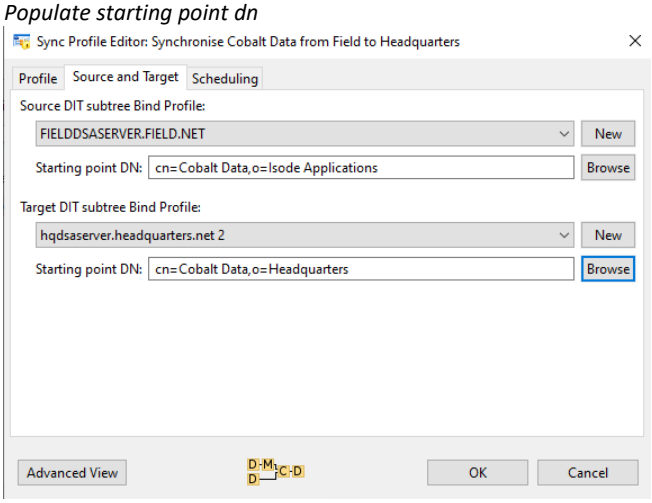
Simple bind details



Populate the “Bind DN” and “Password” Field.

Press “Finish”

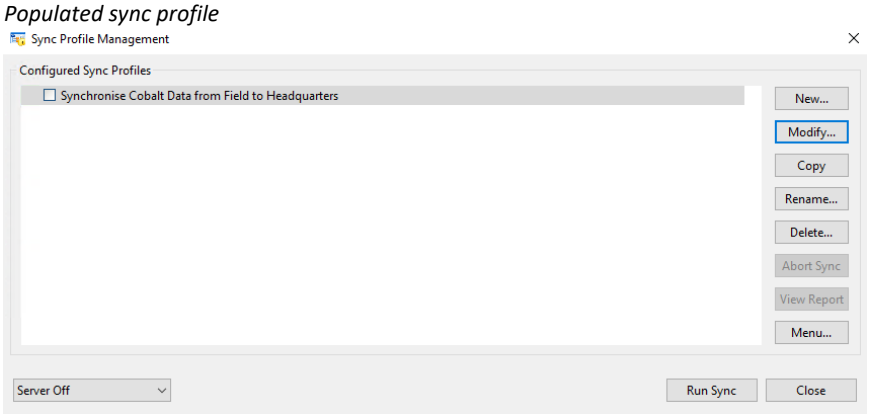
Populate starting point dn



Populate the “Starting point DN” for the target as “cn=Cobalt Data,o=Headquarters”

Press “OK”

Populated sync profile



Filtering using Attributes

The “Advanced View” in the Sync Profile Editor exposes the full functionality of Sodium Sync. We're going to make a number of changes using capabilities exposed by this view.

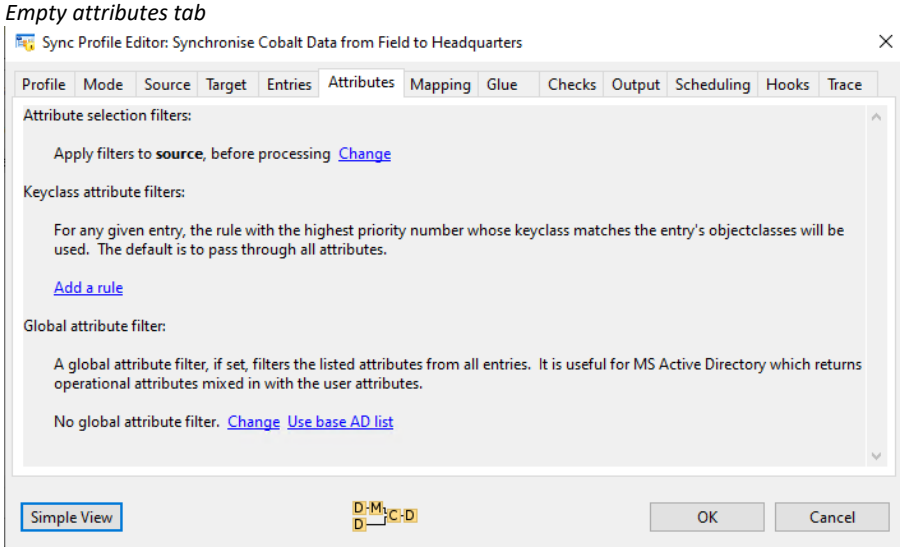
With the New Sync profile selected, press “Modify”

Press “Advanced View”

We're going to exclude from our sync all business telephone numbers by creating a rule.

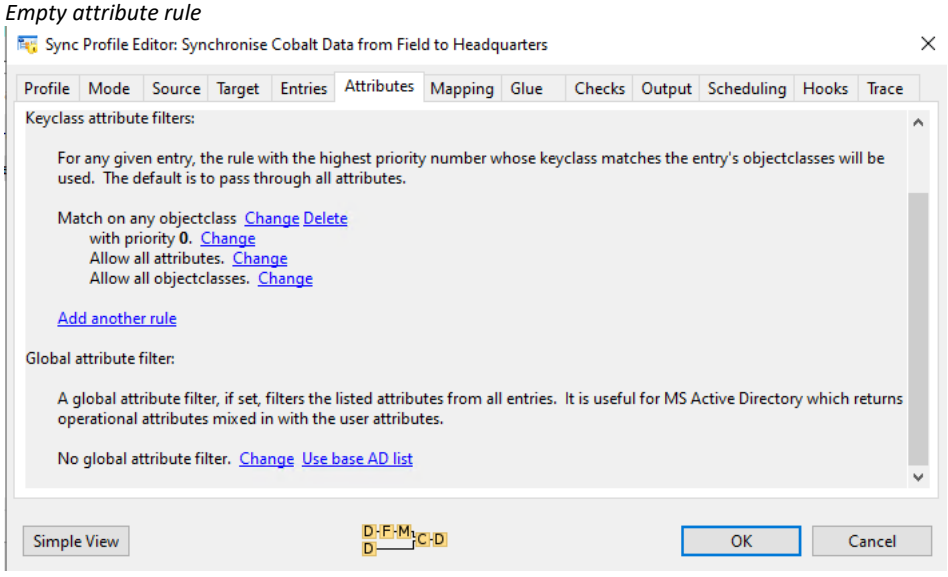
Select the “attributes” tab.

Empty attributes tab



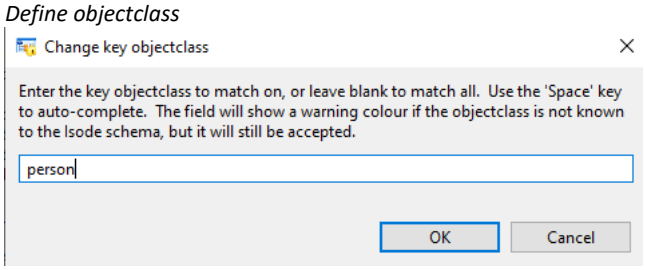
Click on “Add Rule”

Empty attribute rule



Select “Change” next to “Match on any objectclass”

Define objectclass

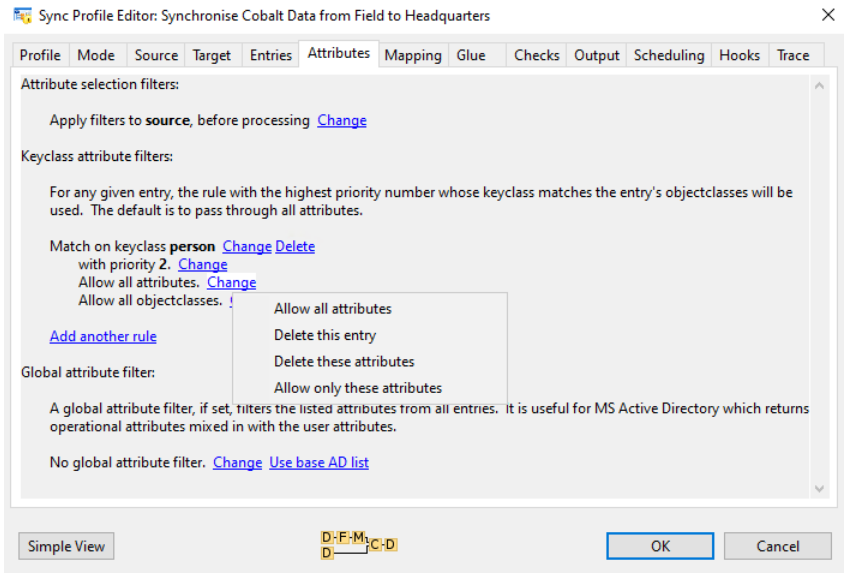


In the “Change key objectclass” pop-up, type "person"

Press “OK”

Next to “Allow all attributes”, click on “Change”

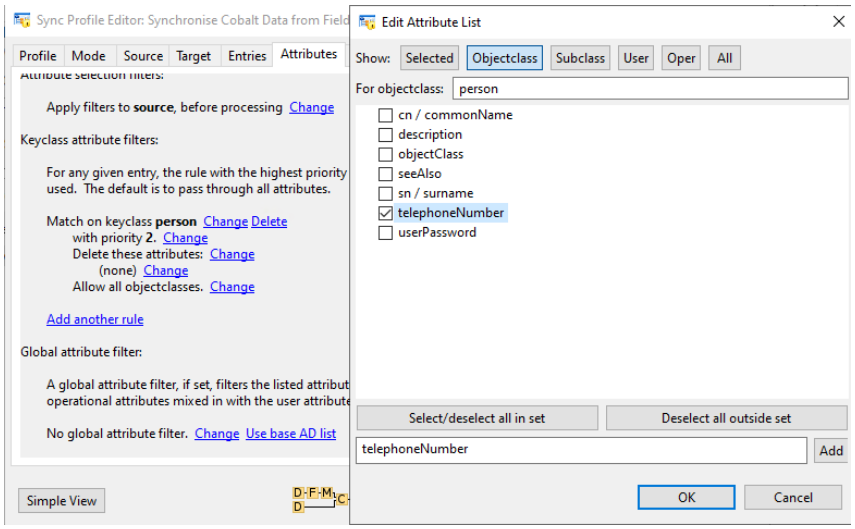
Change context menu



Click on “Delete these attributes”

Click on “Change” next to “(none)”

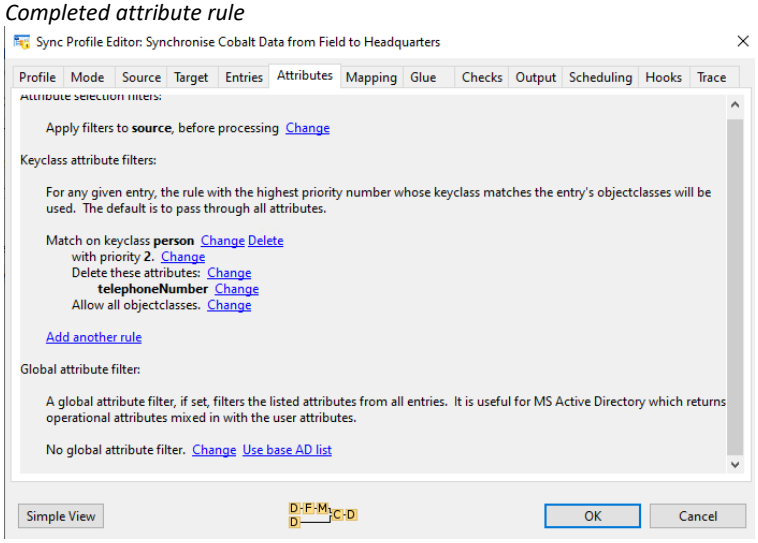
Select attributes



In the Edit Attribute List screen, select “telephoneNumber”

Press “OK”

Completed attribute rule



Press “OK”

Running a Manual Sync

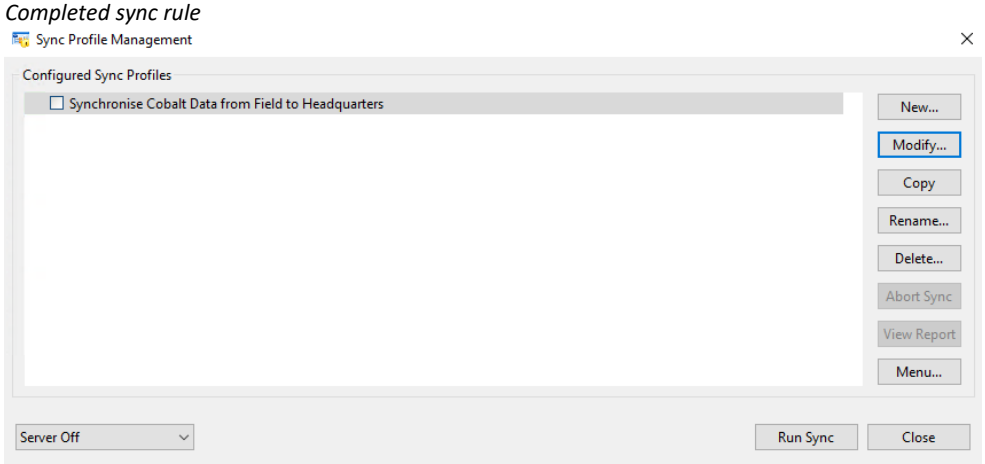
You've now set up a Sync Profile that will:

- Scan all entries below cn=Cobalt Data,o=Isode Applications in the “Field” source directory.
- Filter our source directory to exclude the telephoneNumber attribute from the Person objectclass
- Copy the resulting data into the “Headquarters” target directory starting at cn=Cobalt Data,o=Headquarters.

Now you need to run the Sync, which we'll do manually.

Switch to the Sync Profile Management screen

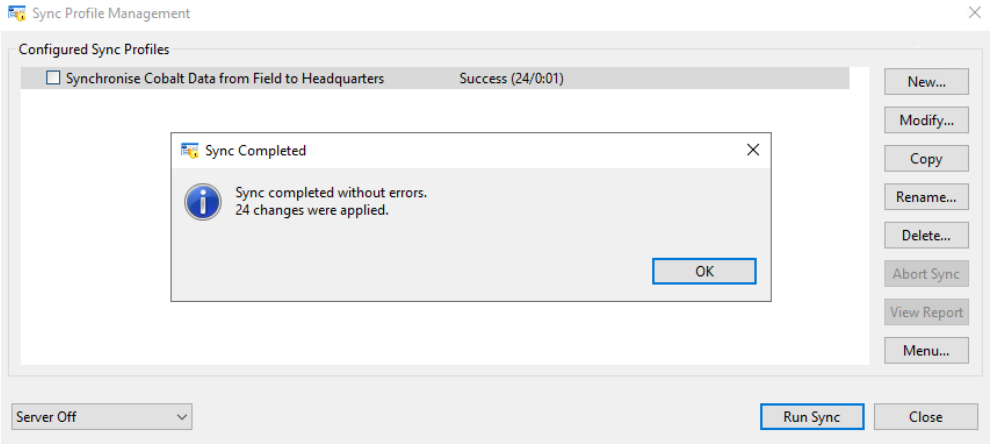
Completed sync rule



Select the Sync “Synchronise Cobalt Data from Field to Headquarters”

Press “Run Sync”

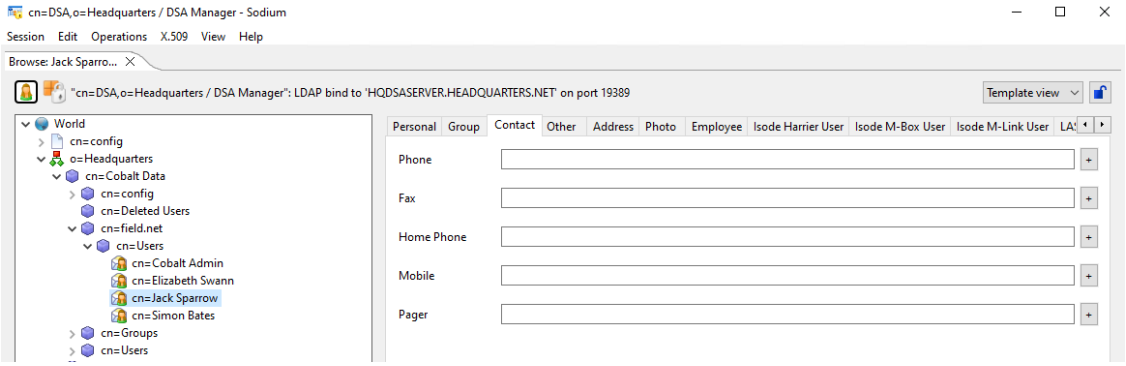
Sync completed



Note that the data was successfully synchronised.

On the HQ server, use Sodium to browse to the object "cn=Jack Sparrow,cn=Users,cn=field.net,cn=Cobalt Data,o=Headquarters"

Jack Sparrow at headquarters



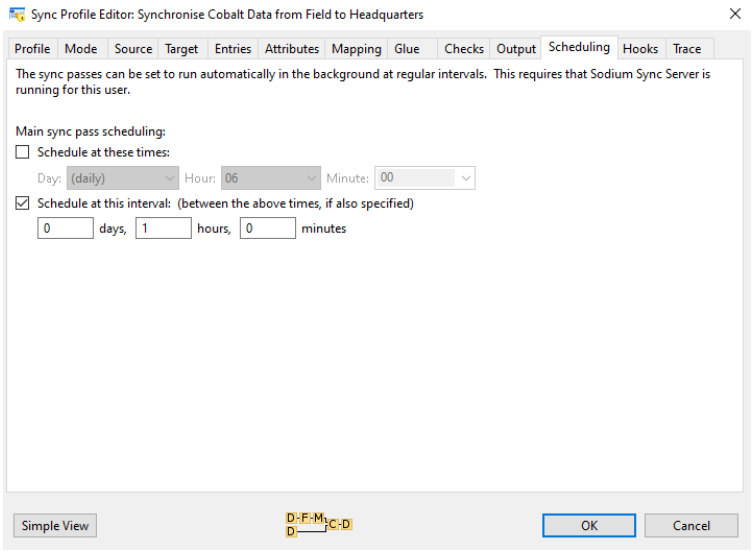
Note that this copy of the Jack Sparrow object doesn't contain a telephone number.

Running an Automatic Sync

To run syncs automatically at regular scheduled intervals, you must start the Sync Server. This is a background process that runs continuously, even over system reboots, and which runs the scheduled syncs without needing to have the Sodium GUI application running.

Sync schedules can be set up using the "Scheduling" tab in "Advanced" view:

Scheduling tab

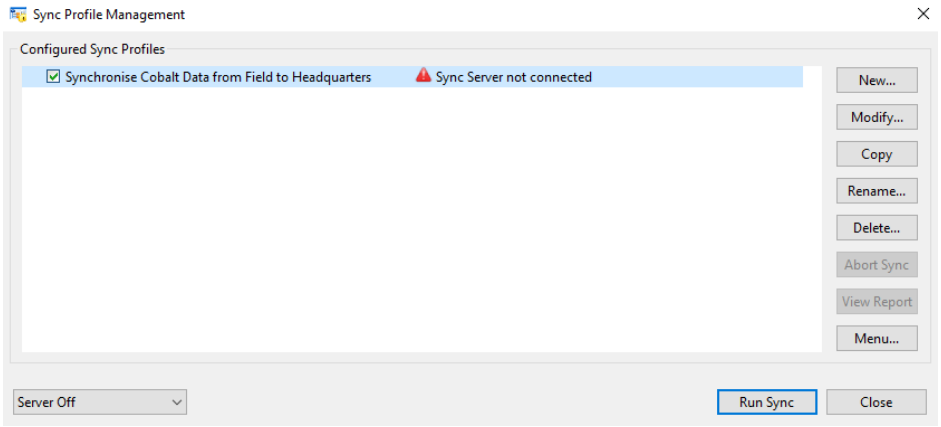


Check “Schedule at this interval ...”

Press “OK”

When the Sync Server is not running, scheduled syncs are displayed in the Sync Profile Management window with an error triangle to warn that the server is not running:

Sync server not connected



For information on setting up the Sync Server, see the Chapter on "Configuring Sodium Sync Server" in the M-Vault Administration Guide.