

Setting up a Directory Server

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

Contents

Objectives	3
Using Isode Support	3
Preparation	4
Isode Products	4
Evaluation License File	Error! Bookmark not defined.
Terminology	5
Creating a Directory Server	7
Starting MVC	7
Setting a Bind Profile Passphrase	7
Creating a New Directory Server	7
Populating and Browsing a Directory using Sodium	10
Binding to a Directory Server	10
Bulk-loading entries from a sample LDIF file	11
Adding an Entry/Entries using Sodium	13
Modifying and Deleting an Entry	15
Searching	15
Isode's Web Applications for Directory	18
Installing Web Applications	18
Modifying the 'dsinterface.xml' file	18
Start Apache Tomcat	18
Using the Directory Service Interface (DSI) Packages	19
Understanding Templates	19
What Next?	23
Sample LDIF Files	23
Further Evaluations	23
Copyright	24

Objectives

The purpose of this guide is to introduce M-Vault to users new to Isode's servers and management tools. During this evaluation you will:

- Become familiar with the terminology of some of the major Directory concepts.
- Created a Directory Server using M-Vault Console.
- Bulk loaded data into the Directory from a sample LDIF file
- Added, modified and deleted entries in the directory.
- Activated and used Isode's web applications for Directory.

For the purposes of this evaluation we have assumed that this is a 'clean' installation of M-Vault. We'll interact with M-Vault using:

- M-Vault Console (MVC) M-Vault Console is a graphical user interface for managing M-Vault. It can be used to create and manage a Directory Service as well as to maintain operational information for the modification and extension of the Directory Service.
- Secure Open Data, Identity and User Manager (Sodium) is used to manage user information in the Directory (such as entries for people or organizational units). It allows you to manage user information on multiple Directory Servers across the network, bulk load & dump data, browse through the Directory & add, delete and modify entries.

Using Isode Support

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

Preparation

You should visit www.isode.com/products/supported-platforms.html to discover which operating systems are supported for Isode evaluations. Please note that in addition to the server platforms listed, we support the use of Isode servers on Windows 8, Windows 8.1 and Windows 10 for simple evaluations and demonstrations.

Isode Products

Product downloads are held in a password-protected section of the Isode website. If you have not already done so you should apply for a username/password by filling in the form located at www.isode.com/evaluate/evalrequest.html.

Products can be obtained by clicking on the links in the “Download Links” section of the Directory evaluation page (www.isode.com/evaluate/evaluate-directory.html).

Product Activation Key

Isode server products require a valid Product Activation Key from Isode before they will run correctly. Keys are issued by Isode Customer Services. If you haven't already been sent a Key when requesting access to the evaluation files, please send a message to request one to support@isode.com remembering to specify which Isode server products you need a Key for.

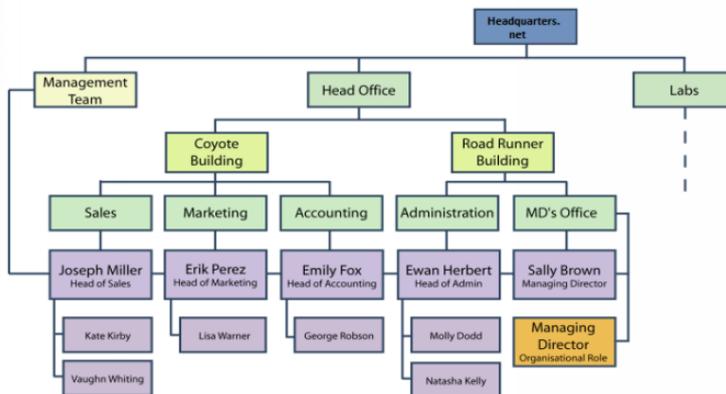
By default, the file you receive needs to be placed in `\Isode\etc\` (Windows) or `/etc/isode/` (Linux), renamed as 'license.dat'. You may have chosen an alternative installation directory when installing the software, in which case you will have to place the license file there.

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 (Image 1) 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.

Image 1: 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:

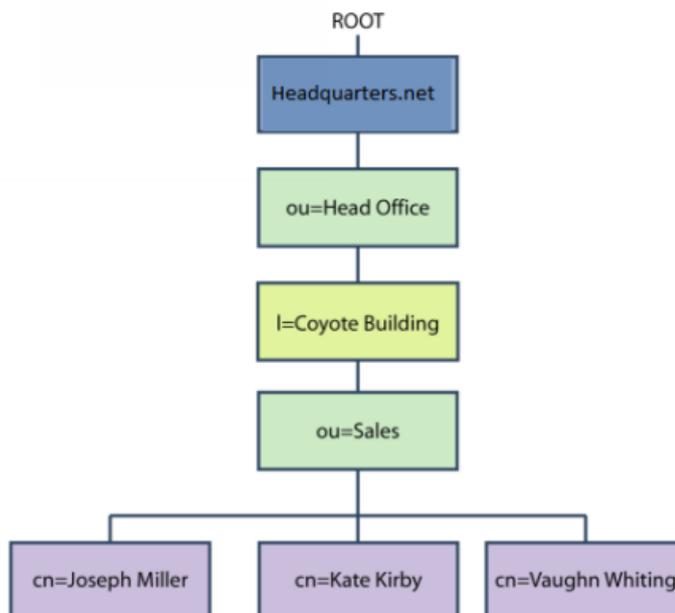
```
cn=Eric Perez
ou=Marketing
o=Acme
```

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 `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 Image 2 which shows the Directory Information Tree for the Sales department (an organizational unit) of Headquarters.net.

Image 2: 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`).

Creating a Directory Server

In this section we use M-Vault Console (MVC) to create a Directory Server for Acme; we then use MVC to start this Directory Server and open a connection to it. MVC is started differently on Windows and Solaris/Linux, but once started, the process, displays and commands are the same.

Starting MVC

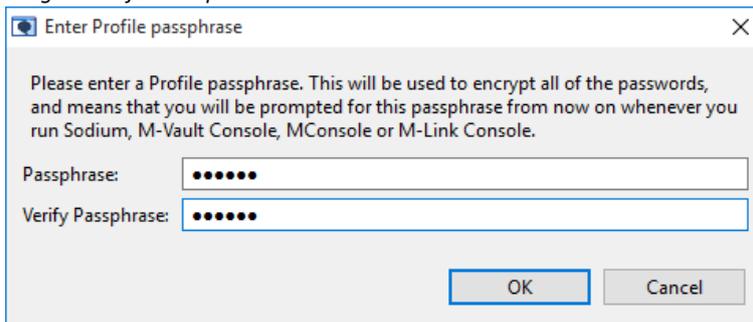
In Windows click “Start” and from the “Programs’ Menu, select 'Isode 16.6 / M-Vault Console'. In Linux execute the following command:

```
% /opt/isode/sbin/mvc
```

Setting a Bind Profile Passphrase

If this is the first time you've used any of the Isode management GUI tools, you will not yet have Isode profile settings saved and will be asked if you wish to encrypt your bind profile (Yes), then prompted to set and confirm a password for that profile (Image 3).

Image 3: Profile Passphrase



If you have already created an Isode bind profile as part of another evaluation, you will be prompted for your passphrase.

You must remember this passphrase as you will be asked to provide it every time you start MLC or any other Isode Management GUI.

Once you have created the profile, or entered your passphrase, click [OK] and MVC will launch.

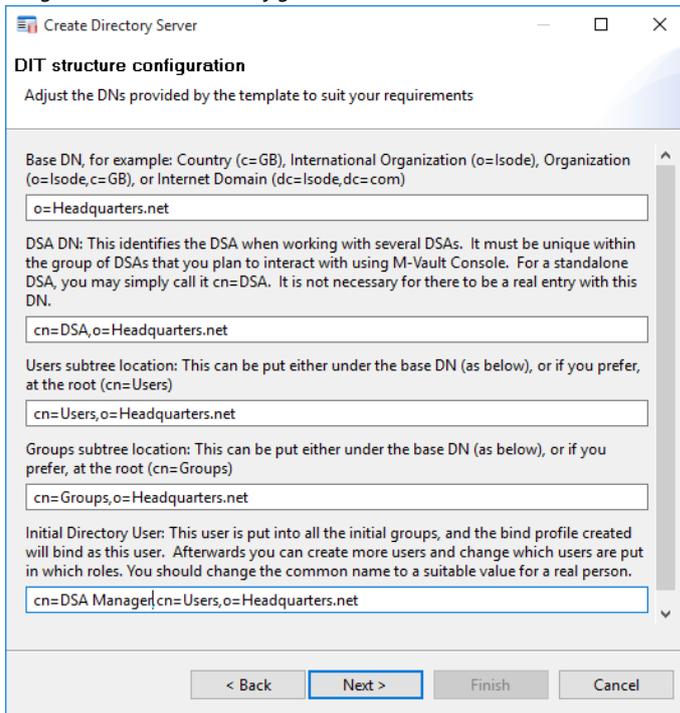
Creating a New Directory Server

In the following example we will be creating a standalone Directory Server which will represent the company Acme, illustrated in the Terminology Background section.

To create a new Directory Server, from the main MVC screen, select 'Create > New Directory Server'. Select the Default DSA Configuration template and click on [Next].

The Create New Directory Server screen will be displayed, together with default example values. In Image 4 the values match those we'll need in order to create the basis for our Headquarters.net example.

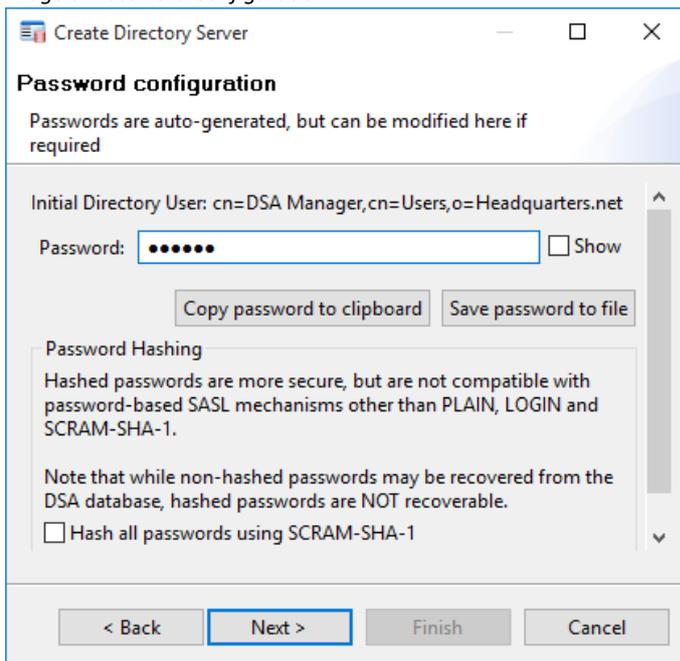
Image 4: DIT Structure Configuration



Fill in the values as shown in Image 4. Note the Base DN value has been changed from the default value to "o=Headquartersnet" and that the Initial Directory User has been changed from "Thomas Atkins" to "DSA Manager". Click on [Next].

Accept the default settings in the Access Control Rule Selection and Access Control Group Configuration screens and click [Next] in both instances. In the Password configuration screen (Image 5) ensure that you make a note of the auto-generated password or type in your own memorable password (this guide assumes use of the password 'secret'), then click [Next].

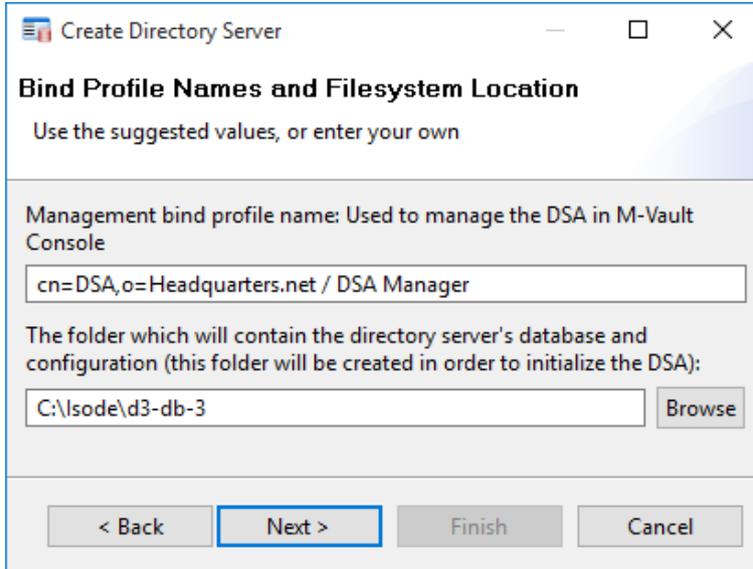
Image 5: Password Configuration



MVC will create and display Bind Profile Name and filesystem location for the Directory. Accept

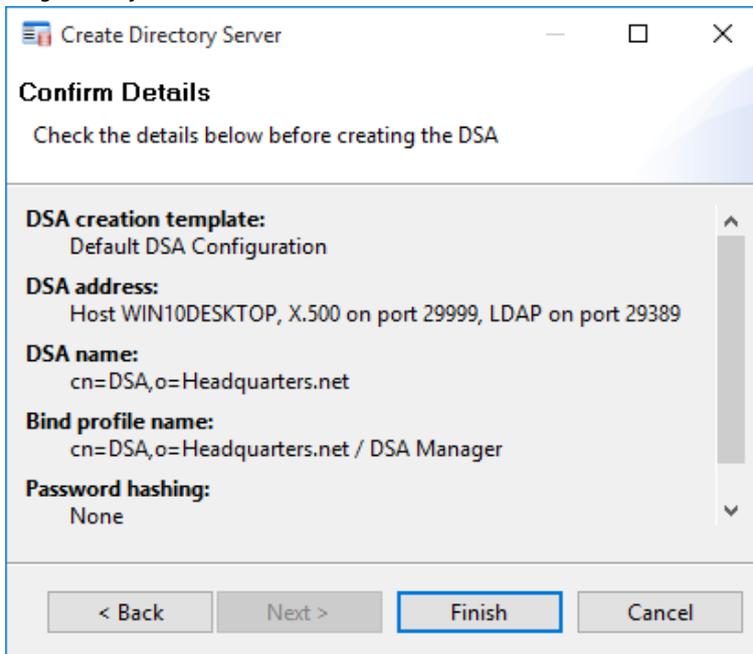
the defaults in the two fields (Image 6) and click [Next].

Image 6: Filesystem Location



On the next two screens, Address Configuration & Confirm Details (Image 7), accept the defaults, click [Finish] at the end and MVC will create and start your DSA.

Image 7: Confirm Details



For the purposes of this simple setup we're now finished with MVC however you can get a brief glimpse MVC features, by clicking [Yes] when asked if you want to connect to and manage the DSA.

Populating and Browsing a Directory using Sodium

Isode provides a Directory User Agent (DUA) called Sodium as part of M-Vault. 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.

Starting Sodium

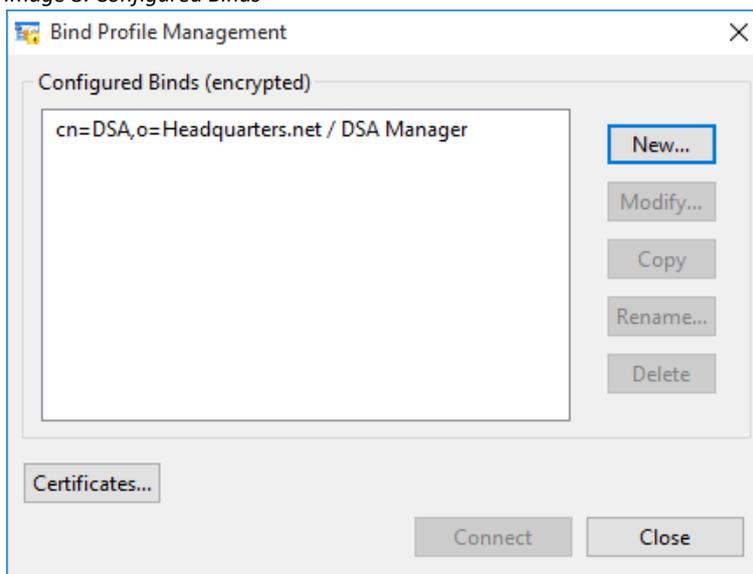
In Windows click 'Start' and from the 'Programs' menu, select 'Isode 16.6 > Sodium (Secure Open Data, Identity and User Manager)'. In Linux execute the following command:

```
% /opt/isode/bin/sodium
```

Binding to a Directory Server

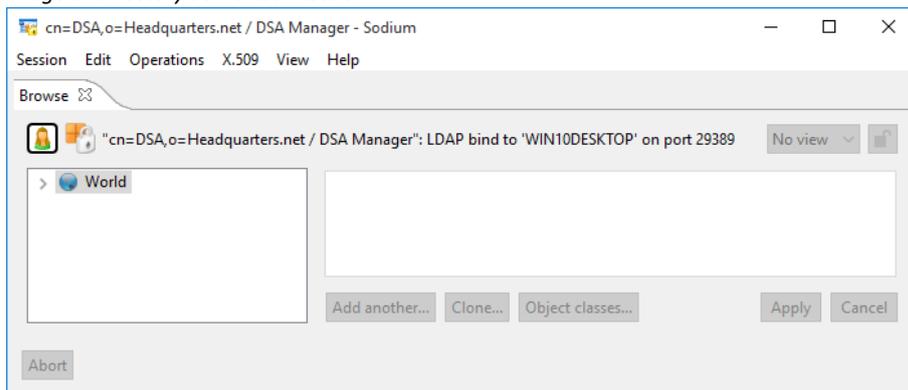
On startup, Sodium will ask you for the Bind Profile passphrase you set earlier and will then list your configured binds (Image 8). In our case, we have only one.

Image 8: 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 Acme so, make sure it is highlighted and click on **[Connect]**. You are now connected to the Directory Server and the initial World view is displayed (Image 9).

Image 9: Directory Server Connection

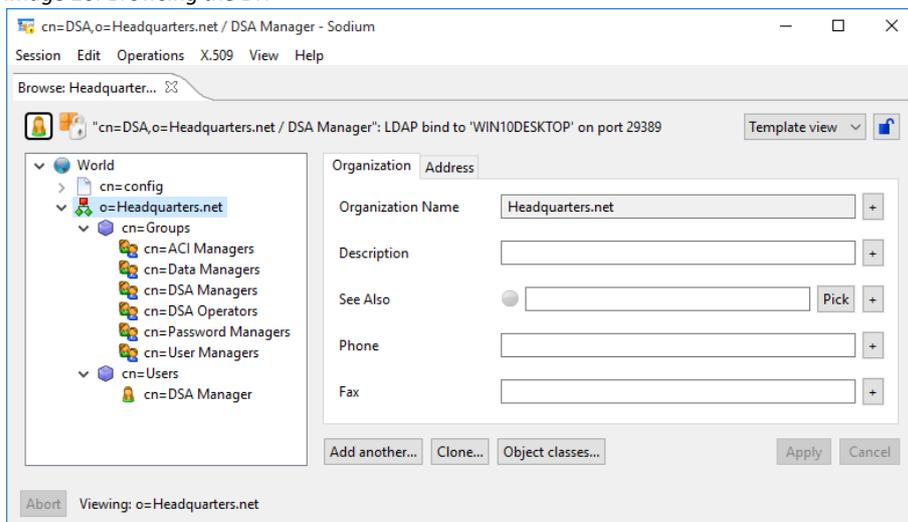


Bulk-loading entries from a sample LDIF file

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.

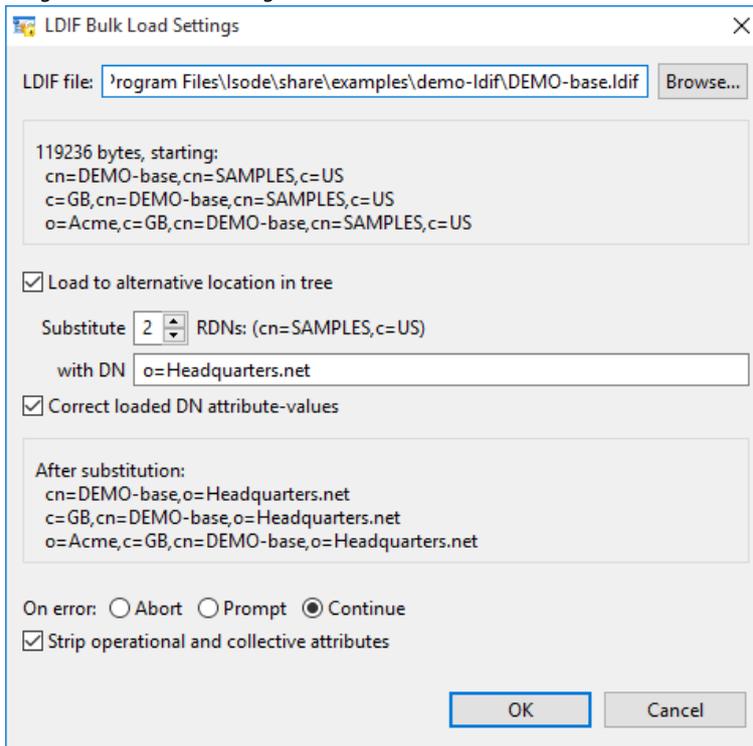
Data cannot be loaded directly under 'World' so firstly expand the tree to reveal the current entries in the DIT. Clicking on any entry in the DIT will cause Sodium to read the entry in the Directory Server and display the results in the right-hand pane (Image 10).

Image 10: Browsing the DIT



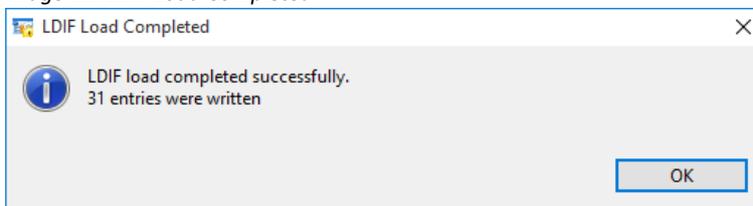
Make sure that you have the 'Headquarters.net' Entry selected and then select "Help > Load Demo Data" from the menu. Click [OK] after reading the information popup and you'll be presented with the LDIF Bulk Load Settings screen (Image 11).

Image 11: Bulk Load Settings



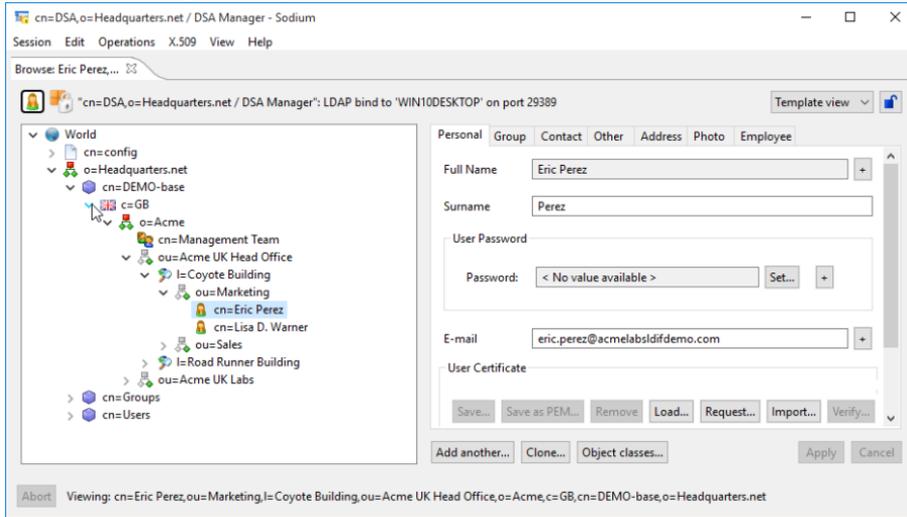
Accept these default settings and click on **[OK]** to proceed with the load, after which you'll get a Load Complete acknowledgement (Image 12).

Image 12: LDIF Load Completed



Clicking on **[OK]** will return you to the main Sodium screen and if you now expand the entries under Headquarters.net 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 (Image 13) will reveal the detail of that entry in the right-hand pane (grouped into tabbed views).

Image 13: Browsing the DIT (post bulk load)

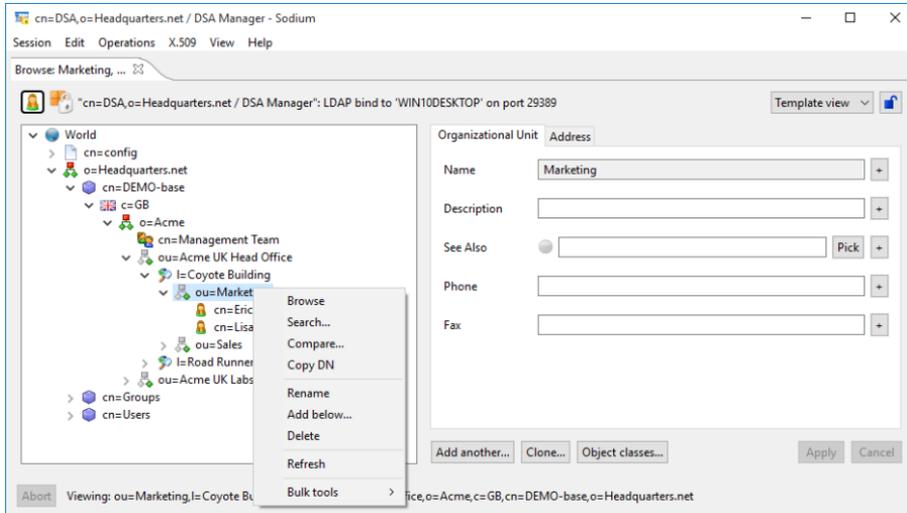


Adding an Entry/Entries using Sodium

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.

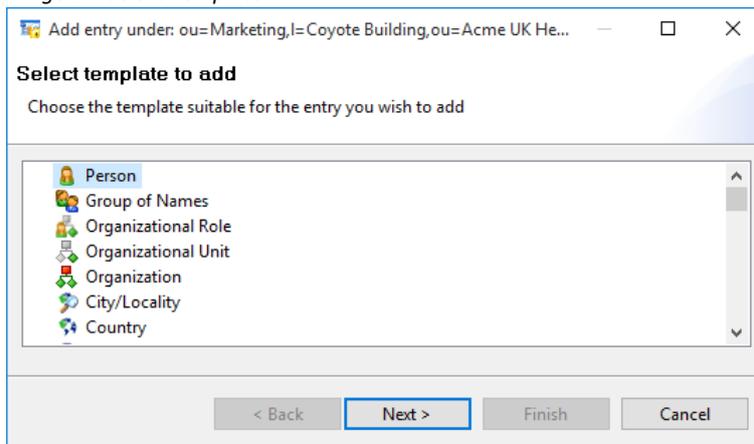
In this section we're going to add another staff member to the Marketing department. First, right-click on the "ou=Marketing" entry and select [Add Below] as in Image 14.

Image 14: Blah



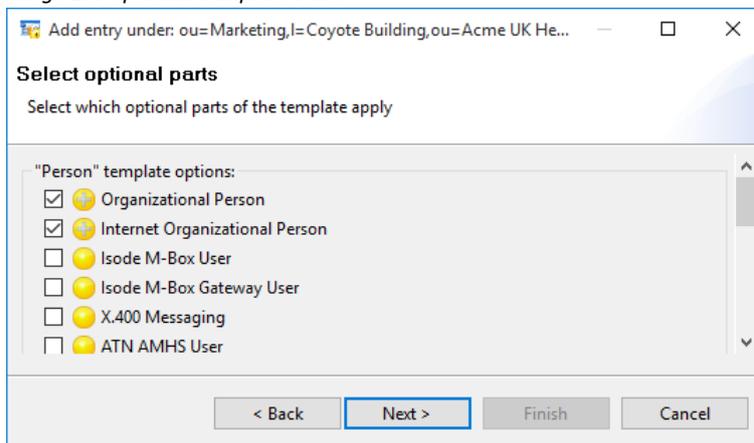
Select 'Person' from the Template list (Image 15).

Image 15: Select Template



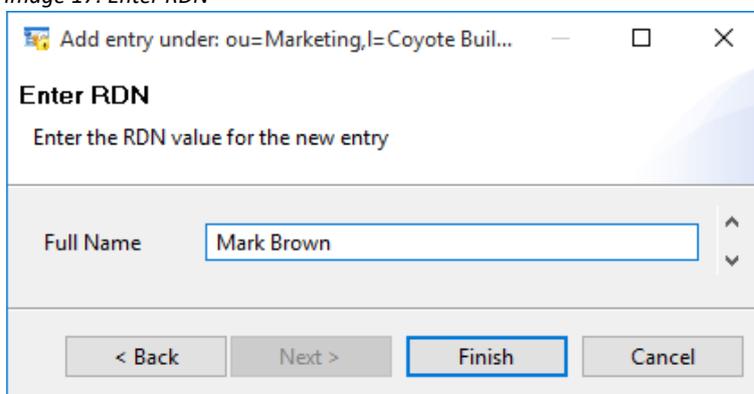
Next, select optional template parts: 'Organizational Person' and 'Internet Organizational Person' (Image 16).

Image 16: Optional Template Parts



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. Click [**Next**] and add the full name of the person being added to the directory (Image 17).

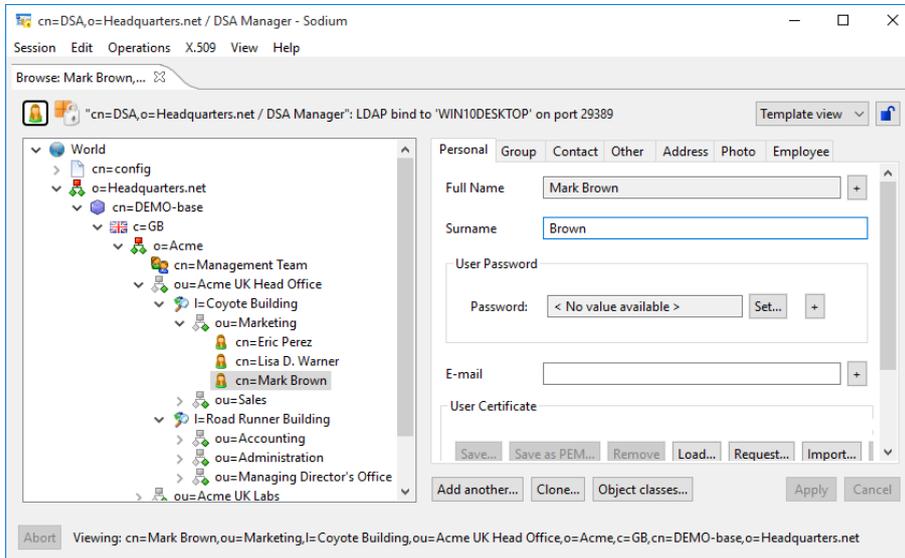
Image 17: Enter RDN



Finally click on [**Finish**] to add the entry. In most cases there will additional required attributes needed before the record can be committed (in this case it's Surname) and these will be highlighted. Add the required attribute of "Brown" and finish by clicking the [**Add**] button. You

can quickly add another entry of the same type by clicking the **[Add Another]** button at the bottom of the screen (Image 18).

Image 18: Browsing the DIT (post entry addition)



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.

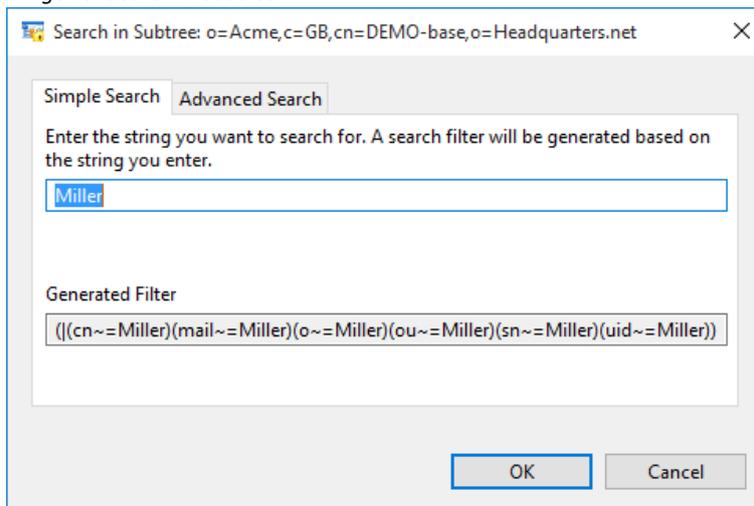
You can delete an entry from the DIT by right-clicking on it and selecting **[Delete]**. Please note that you cannot remove an entry with subordinate entries. In order to remove an entry and its subordinate entries you can use the menu item 'Bulk Tools / Delete Subtree' when right-clicking on an entry.

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.

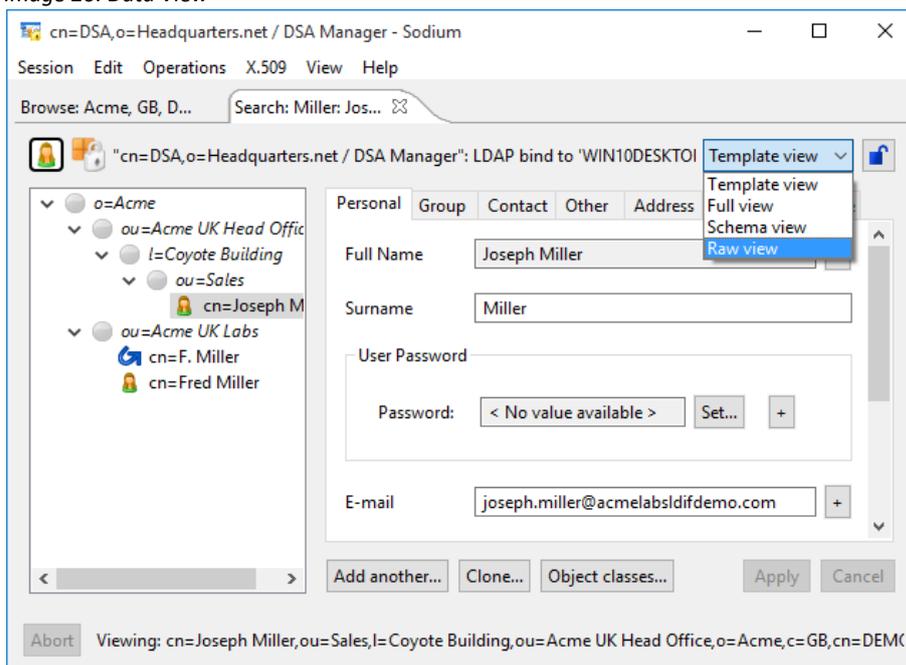
Try this operation with the `o=Acme` entry. Select '`o=Acme`' and bring up the search box. In this example we're going to search for entries containing 'Miller' (Image 19).

Image 19: Search in Subtree



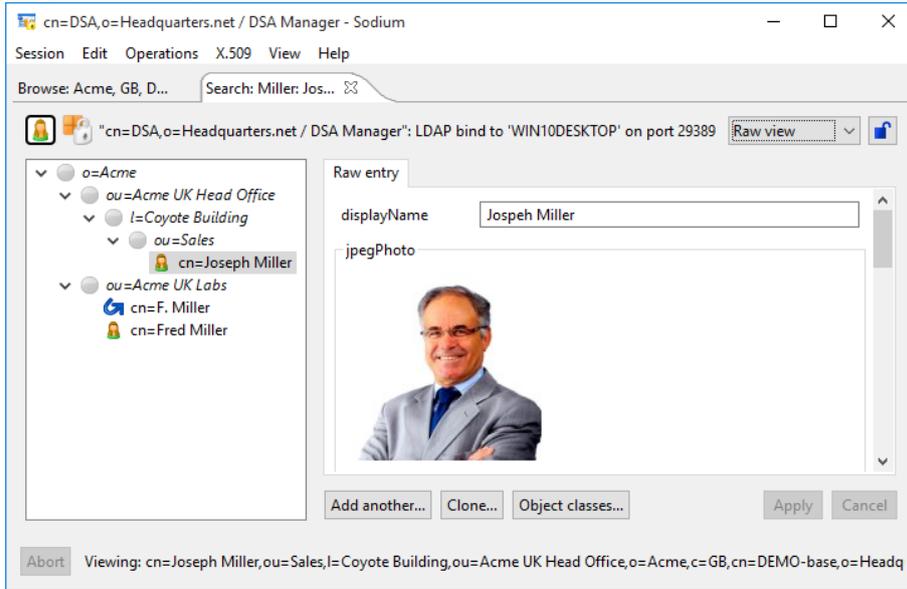
Click on [OK], and Sodium will return the results in a separate Tab, showing the entries that match the search request and their position in the DIT. Up to this point we've been viewing entries in Template mode. For a fuller view of the data you can switch to Raw view using the drop-down menu in the top right-hand corner (Image 20).

Image 20: Data View



In Image 21 we can see the Raw view of the entry for Joseph Miller.

Image 21: Raw Entry



Isode's Web Applications for Directory

In this final section we're going to install and examine the sample Directory Server Interface (DSI) applications that Isode ships with M-Vault. Isode's web applications for M-Vault are part of a larger suite of web based management tools which includes functionality for M-Link, M-Box and M-Switch. For information on other web applications, please consult the Web Applications Administration Guide available from www.isode.com/support/docs.html.

Isode ships an embedded Tomcat Server to assist with evaluations and this guide assumes use of that server. For real deployments Tomcat should be set up following the instructions in the Web Applications Administration Guide.

Installing Web Applications

In Windows, from the Programs menu select "Isode 16.6 > Isode Service Configuration". From the 'Actions' menu choose 'Install Isode Services' and tick the 'Isode Embedded Tomcat Server' option before clicking on [Finish]. From the Programs menu select 'Isode 16.3 > Web Applications Setup Utility' and follow the instructions in the setup wizard, answering Yes when asked if you wish to install the *.war files.

In Linux, execute the following command to set up the Isode web applications:

```
# /opt/isode/sbin/isode-tomcat-setup
```

Follow the instructions in the setup wizard, answering Yes when asked if you wish to install the *.war files.

Modifying the 'dsinterface.xml' file

In 'C:\Isode\etc' (/etc/isode on Linux) you'll find a dsinterface.xml.sample file. Rename this file dsinterface.xml and open it to edit. The changes you'll need to make to this file will depend on how you have set up your DSA, if you've followed this guide without alteration, the changes below (in red) will work.

```
<dsinterface_config>
<ldap_url>ldap://localhost:19389</ldap_url>
<ldap_bind_dn>cn=DSA Manager,cn-
Users,o=Headquarters.net</ldap_bind_dn>
<ldap_bind_pwd>secret</ldap_bind_pwd>
<ldap_bind_method>SIMPLE</ldap_bind_method>
<ldap_bind_id>DSA Manager</ldap_bind_id>
<dsa_config_dn>cn=core,cn=config</dsa_config_dn>
</dsinterface_config>
```

The ldap_bind_pwd is the password you set up for the DSA Manager.

Start Apache Tomcat

You can now start Tomcat via the Isode Service Configuration Tool, 'Isode 16.6 > Isode Service Configuration', on Windows and starting the isode.tomcat service or, on Linux by using:

```
# /init.d/isode-tomcat-start
```

Using the Directory Service Interface (DSI) Packages

The DSI packages can now be accessed via a browser at the following addresses:

- Directory Services Interface (Phonebook): <http://localhost:8080/dsinterface-phonebook>
- Directory Services Interface (Directory): <http://localhost:8080/dsinterface-directory>
- Directory Services Interface (Personal Information Administrator): <http://localhost:8080/dsinterface-pia>

On viewing, the scope and features of all three packages should be self-evident. You can log in as any of the users set up via your directory by using their email address and password. Please note that DSI applications require the use of a password on login. If passwords have not been set for the directory user you are logging on as, you can set one by editing the password field of the Personal tab within Sodium.

Image 22 shows the relevant details for the user Emily Fox' Note that you will need to set a password for Emily Fox before proceeding (in this case we've used "secret").

Image 22: Editing User Details

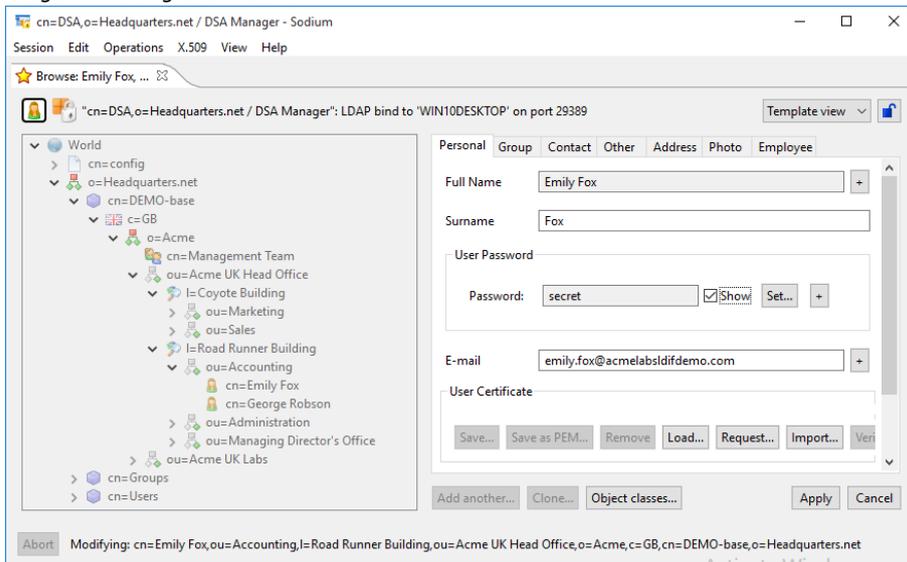


Image 23 shows the user Emily Fox logged into the Personal Information Administrator using the Username "emily.fox@acmelabslidifdemo.com" and the Password "secret".

Image 23: Directory Services Interface



Understanding Templates

Sodium displays entries that are read from the directory using one of a number of configured

templates. The template used is based on the objectclasses of the entry being read. If the objectclasses do not match any template, a raw template is provided. Templates are also used when adding a new entry to a directory.

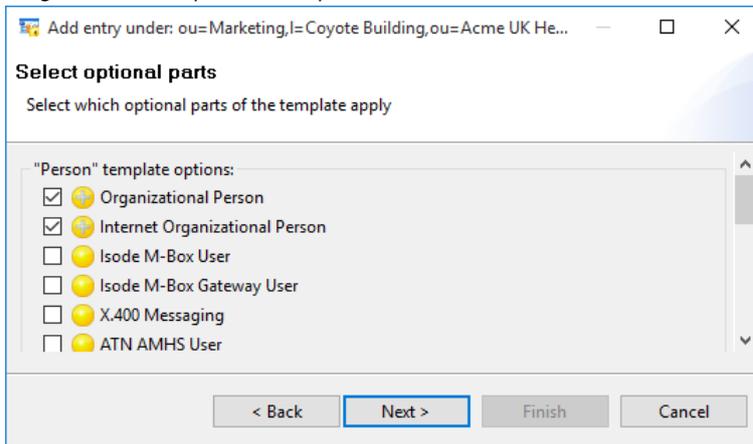
Templates are stored in an XML file (located at the (SHAREDIR)/sodium/templates.xml) which is read when Sodium starts. You can edit the templates file using any XML or text editor.

Each template in the XML file references a number of forms that are used by Sodium. In the example that follows we can see how the templates.xml file (Image 24) defines Sodium's choice of optional parts for the 'person' template (Image 25).

Image 24: Templates XML

```
<template rdn="cn" keyclass="person" label="Person" icon="person.png" >
  <form ref="person" />
  <form keyclass="organizationalPerson" ref="organizational-person" label="Organizational Person" />
  <form keyclass="inetOrgPerson" ref="inet-org-person" label="Internet Organizational Person" />
  <form keyclass="mboxUser" ref="mbox-user" label="Isode M-Box User" icon="mbox_user.png" />
  <form keyclass="mhsUser" ref="mhs-user" label="X.400 Messaging" />
  <form keyclass="atn-amhsUser" ref="atn-amhs-user" label="ATN AMHS User"/>
  <form keyclass="pkiUser" ref="pki-user" label="PKI User"/>
  <form keyclass="pkiCA" ref="pki-ca" label="PKI CA"/>
  <form ref="nis-posixAccount" keyclass="posixAccount" label="(NIS) POSIX Account" />
  <form ref="nis-shadowAccount" keyclass="shadowAccount" label="(NIS) POSIX Shadow Password" />
```

Image 25: Sodium "person" Template



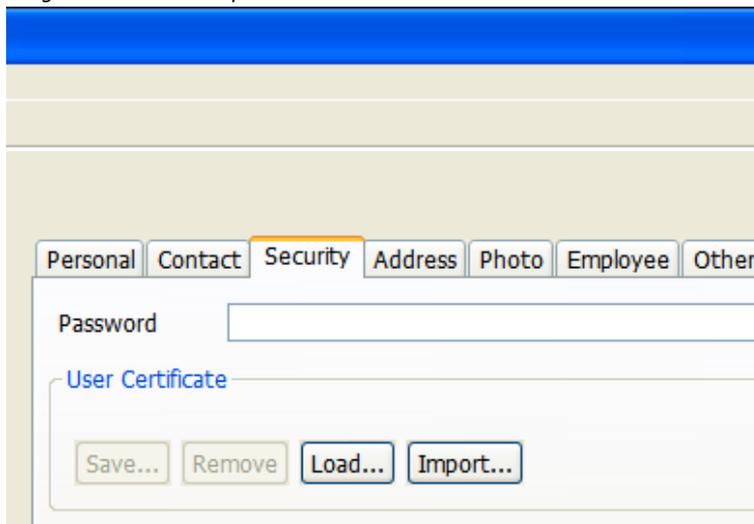
Each 'form' defines additional attributes for that entry, gathered into groups, displayed as tabs by sodium. In Image 26 'contact', 'photo' and 'security' named groups are defined for the 'Internet Organizational Person' optional part.

Image 26: Defining Named Groups

```
<form name="inet-org-person">
  <group label="Personal" >
    <editor label="Given Name" attrtype="givenName" />
    <editor label="Initials" attrtype="initials" />
    <editor label="Display Name" attrtype="displayName" />
    <editor label="Labelled URI" attrtype="labeledURI" />
  </group>
  <group label="Contact">
    <editor attrtype="homePhone" editor="string" label="Home Phone" />
    <editor attrtype="mobile" editor="string" label="Mobile" />
    <editor attrtype="pager" editor="string" label="Pager" />
    <editor attrtype="mail" editor="string" label="E-mail" />
  </group>
  <group label="Security">
    <editor attrtype="userCertificate" editor="certificate" label="User Certificate"/>
  </group>
  <group label="Address">
    <editor attrtype="homePostalAddress" label="Home Postal Address" />
  </group>
  <group label="Photo" >
    <editor attrtype="jpegPhoto" editor="jpeg" label="Photo" />
  </group>
  <group label="Employee">
    <editor label="Employee Number" attrtype="employeeNumber" />
    <editor label="Employee Type" attrtype="employeeType" />
    <editor label="Room Number" attrtype="roomNumber" />
    <editor label="Secretary" attrtype="secretary" />
    <editor label="Manager" attrtype="manager" />
    <editor label="Business Category" attrtype="businessCategory" />
    <editor label="Department Number" attrtype="departmentNumber" />
    <editor label="Organizational Unit" attrtype="ou" />
    <editor label="Organization" attrtype="o" />
  </group>
  <group label="Other">
    <editor label="X.500 Unique Identifier" attrtype="x500UniqueIdentifier" />
    <editor label="Car License" attrtype="carLicense" />
    <editor label="Preferred Language" attrtype="preferredLanguage" />
  </group>
</form>
```

These groups are displayed as tabs within Sodium (Image 27).

Image 27: Named Groups in Sodium



Multiple groups can use the same label. When a template uses forms that use multiple groups with the same label, the contents of the groups are merged together for that template. In this case the Contact tab contains additional fields defined by the Internet Organizational Person form.

Each <editor> element can have several attribute types. In the example below we have added the attribute type 'compulsory="yes"' to the 'mail' attribute type within the 'inet-org-person' form referenced above.

Image 28

```
<row><editor attrtype="mail" editor="string" label="E-mail" compulsory="yes" /></row>
```

Causing Sodium to flag 'mail' as a compulsory field when new entries of this type are added (Image 29).

Image 29

The screenshot shows a web form with several tabs: Personal, Contact, Security, Address, Photo, and Emp. The 'Contact' tab is active. Below the tabs are several input fields: Phone, Fax, Home Phone, Mobile, Pager, and E-mail. The 'E-mail' field has a red warning triangle icon next to it, indicating it is a compulsory field.

You can find out more about template structure and editing by reading the Sodium section of the M-Vault Administration Guide.

What Next?

More information on M-Vault's capabilities can be found from the main M-Vault product page on the Isode website at www.isode.com/products/m-vault.html.

Detailed configuration and operation information on M-Vault can be found in the M-Vault Administration Guide which is available for download in PDF format from www.isode.com/documentation/VAUADM.pdf.

Documentation for all Isode products can be found at www.isode.com/support/help.html.

Sample LDIF Files

During this evaluation guide we have looked at M-Vault and Sodium in the context of the 'Acme' sample LDIF file shipped with M-Vault. In addition to the Acme file, four other sample LDIFs are shipped with M-Vault covering aviation, military, PKI and NIS scenarios.

Like the Acme file, each of these can be loaded from the "Help>Load demo Data.." menu item. The bulk-load settings screen will default to the Acme data, clicking the Browse button will enable you to access the other data sets.

Other Evaluations

This guide is one of two relating to Isode's directory products:

- Setting up a Directory Server (this guide), and
- Synchronising Directories

For directory product evaluations outside of the scope of these guides, please contact us.

In addition to these guides, evaluations are also available for:

- Email Messaging (www.isode.com/evaluate/evaluate-email.html)
- XMPP Messaging (www.isode.com/evaluation/evaluate-xmpp.html)

Whitepapers

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

Copyright

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

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

Isode software is © copyright Isode Limited 2002-2018, All rights reserved.

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

This manual is © copyright Isode Limited 2018.