

ICON-TOPO-2.0

Icon-Topo Administration Guide

Isode

Table of Contents

Chapter 1	Overview.....	1
	This chapter introduces the Isode Icon-Topo giving an overview of its main features and components.	
Chapter 2	Directory And Configuration.....	4
	This chapter explains in more detail how Icon-Topo configuration is held in the Directory and how configuration works.	
Chapter 3	Getting Started.....	6
	This chapter explains the steps required to get the Isode Icon-Topo Configuration Server up and running with basic operator access.	
Chapter 4	Configuration Server.....	11
	This chapter describes the Isode Icon-Topo Configuration Server describing the Web based User Interface features, and lists the configuration options available.	
Chapter 5	Update Server.....	37
	This chapter describes the Isode Icon-Topo Update Server listing the configuration options available.	

Isode 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 2002-2023, 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 2023.

1 Software version

This guide is published in support of Isode Icon-Topo 2.0. It may also be pertinent to later releases. Please consult the release notes for further details.

2 Readership

This guide is intended for administrators who plan to configure and manage the Isode Icon-Topo.

3 How to use this guide

You are advised to read through [Chapter 1, Overview](#), before you start to set up your messaging system.

4 Typographical conventions

The text of this manual uses different typefaces to identify different types of objects, such as file names and input to the system. The typeface conventions are shown in the table below.

Object	Example
File and directory names	<i>isoentities</i>
Program and macro names	mkpasswd
Input to the system	cd newdir
Cross references	see Section 5, “File system place holders”
Additional information to note, or a warning that the system could be damaged by certain actions.	Notes are additional information; cautions are warnings.

Arrows are used to indicate options from the menu system that should be selected in sequence.

For example, **File** → **New** means to select the **File** menu and then select the **New** option from it.

5 File system place holders

Where directory names are given in the text, they are often place holders for the names of actual directories where particular files are stored. The actual directory names used depend on how the software is built and installed. All of these directories can be changed by configuration.

Certain configuration files are searched for first in (*ETCDIR*) and then (*SHAREDIR*), so local copies can override shared information.

The actual directories vary, depending on whether the platform is Windows or UNIX.

Name	Place holder for the directory used to store...	Windows (default)	UNIX
(<i>ETCDIR</i>)	System-specific configuration files.	<i>C:\Isode\etc\topo</i>	<i>/etc/isode/topo</i>
(<i>SHAREDIR</i>)	Configuration files that may be shared between systems.	<i>C:\Program Files\Isode\topo\share</i>	<i>/opt/isode/topo/share</i>
(<i>BINDIR</i>)	Programs run by users.	<i>C:\Program Files\Isode\topo\bin</i>	<i>/opt/isode/topo/bin</i>
(<i>SBINDIR</i>)	Programs run by the system administrators.	<i>C:\Program Files\Isode\topo\bin</i>	<i>/opt/isode/topo/sbin</i>
(<i>EXECDIR</i>)	Programs run by other programs.	<i>C:\Program Files\Isode\topo\bin</i>	<i>/opt/isode/topo/libexec</i>
(<i>LIBDIR</i>)	Libraries.	<i>C:\Program Files\Isode\topo\bin</i>	<i>/opt/isode/topo/lib</i>
(<i>LOGDIR</i>)	Log files.	<i>C:\Isode\topo\log</i>	<i>/var/isode/topo/log</i>
(<i>DSADIR</i>)	The Directory Server's configuration.	<i>C:\Isode\d3-db</i>	<i>/var/isode/d3-db</i>

6 Support queries and bug reporting

A number of email addresses are available for contacting Isode. Please use the address relevant to the content of your message.

- For all account-related inquiries and issues: support@isode.com. If customers are unsure of which list to use then they should send to this list. The list is monitored daily, and all messages will be responded to.
- For all product activation related issues: support@isode.com.
- For all technical inquiries and problem reports, including documentation issues from customers with support contracts: support@isode.com. Customers should include relevant contact details in initial calls to speed processing. Messages which are continuations of an existing call should include the call ID in the subject line. Customers without support contracts should not use this address.
- For all sales inquiries and similar communication: sales@isode.com.

Bug reports on software releases are welcomed. These may be sent by any means, but electronic mail to the support address listed above is preferred. Please send proposed fixes with the reports if possible. Any reports will be acknowledged, but further action is not guaranteed. Any changes resulting from bug reports may be included in future releases.

Isode sends release announcements and other information to the Isode News email list, which can be subscribed to from the address: <http://www.isode.com/company/subscribe.html>

7 Export Controls

Many Isode products use TLS (Transport Layer Security) to encrypt data in transit. This means that these products are subject to UK Export Controls.

For some countries (at the time of shipping this release, these comprise all EU countries, United States of America, Canada, Australia, New Zealand, Switzerland, Norway, Japan), these Export Controls can be handled by administrative process as part of evaluation or purchase. For other countries, a special Export License is required. This can be applied for only in context of a purchase order for those Isode products.

You must ensure that you comply with these Export Controls where applicable, i.e. if you are licensing or re-selling Isode products.

The TLS feature of Isode products is enabled by a TLS Product Activation feature. This feature may be turned off, and Isode products without this TLS feature are not export controlled. This can be helpful to support evaluation of Isode products in countries that need a special export license.

Isode products are used to administer sensitive data and so Isode strongly recommends that all operational deployments of Isode products use the export-controlled TLS feature.

All Isode Software is subject to a license agreement and your attention is also called to the export terms of your Isode license.

Chapter 1 Overview

This chapter introduces the Isode Icon-Topo giving an overview of its main features and components.

1.1 What is Icon-Topo

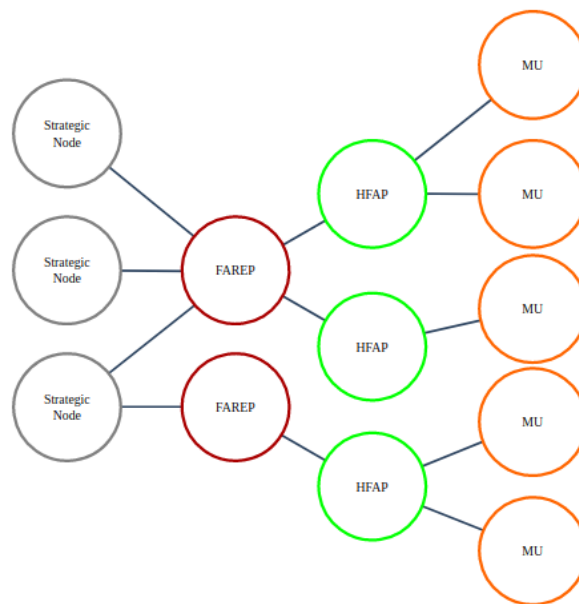
Icon-Topo provides control of Mobile Units (e.g., planes or ships) moving between HF transmitters, and ensuring that configuration of applications and HF systems is updated to support this movement.

Single Hop HF transmission gives a circle of (best) coverage of a few thousand miles. To extend this range, multiple ground stations with separations of typically thousands of miles are used. Mobile Units will move between transmitters. There is a need to modify application routing configuration so that communication works seamlessly. A number of entities need to change configuration in a coordinated manner. The goal of Icon Topo is to achieve this.

There are three types of entity involved:

- Mobile Unit (MU). This is something moving around with HF Communication. An MU is typically a ship or an aircraft.
- HF Access Point (HFAP). This is a ground station that is transmitting and receiving HF. This may include broadcast HF.
- Fixed Application Routing Entry Point (FAREP). This is a node to which entities that are not aware of MU location send messages. The FAREP will send messages to the MU through the correct HFAP.

Figure 1.1. MU/HFAP/FAREP Architecture



When Mobile Units (typically ships and planes) using HF communication move, it is often needed to change ground stations. Optimal communication over HF uses application level protocols, so this re-rerouting needs to happen at the application level. Solving this problem is the target of Isode's Icon-Topo product

Icon-Topo has two types of ground systems to support Mobile Units (MUs):

- HF Access Points (HFAP). These are sites that will transmit/broadcast HF.
- Fixed Access Routing Entry Points (FAREP). These are systems, possibly co-located with HFAPs, that fixed systems route to. Systems external to the FAREP can send traffic for an MU to the FAREP, without needing to know the location of the MU or the HFAP used.

Messages and XMPP traffic can be sent to a FAREP, and it will be correctly routed to the right MU. An Icon-Topo operator can assign an MU to a new HFAP. Icon-Topo will change application routing configuration of FAREP, HFAPs and MU to reflect this change. This allows operators to assign MUs to FAREPs and manage underlying ALE and HF systems.

Configuration of MUs/HFAPs/FAREPs is stored in a replicated LDAP/X.500 directory. Servers on shore use multi-master replication, so updates can be applied at any node. Incremental directory replication (Isode Sodium Sync product) with transfer by messaging over HF keeps the MU directory synchronized.

A key problem that Icon-Topo needs to address is that all routing changes need to happen at once, but propagation of directory updates over HF may take some time. Icon-Topo handles this by providing a scheduling layer over the directory, so that the changes are always made in context of the time they are to be applied. So, an operator may schedule a series of MU movements at times in the future. This information gets replicated ahead of the time that the changes need to be applied.

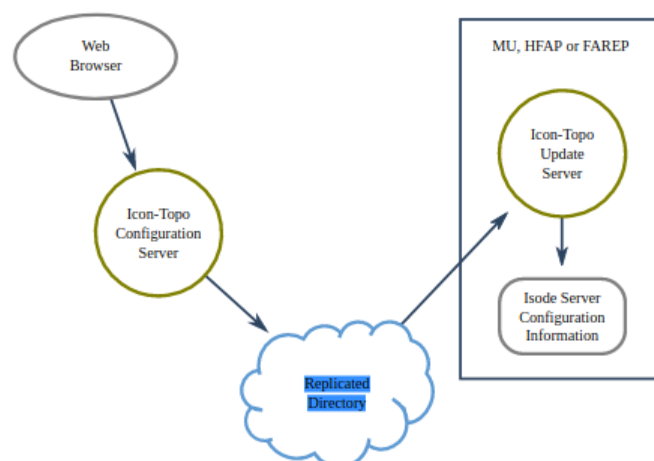
1.1 Topo Components

Topo comprises two server components:

- Configuration Server which acts as a Web Server allowing Administrators and Operators to update the Topo configuration using a web browser.
- Update Server which reads the Topo configuration and updates the appropriate Isode server application.

The following diagram shows how the Icon-Topo components interwork.

Figure 1.2. Topo Components



1.2 Use Of Directory

Icon-Topo holds information on MUs, HFAPs and FAREPs in the Directory which is replicated to all of the nodes using the information. MUs have read-only access to the Directory. This means that all Directory updates are done on shore.

The Icon-Topo information in the directory may be managed from any shore system (HFAP or FAREP) using a Web Browser to access Icon-Topo Configuration Server, which provides the operator experience and writes all information to the directory. This UI can also be used on an MU to view the Icon-Topo configuration (read only).

On every Icon-Topo managed node (MU, HFAP, FAREP), there is an Icon-Topo Update server that reads information from the directory. This process generates configuration information for all of the Isode servers running on the node. Configuration is updated in line with changes to the directory. In this manner, Icon-Topo provides centralized configuration management of all of the Icon-Topo managed nodes

1.2.1 User and Role Provisioning

The same directory also holds user and role provisioning information, which is also replicated to all nodes. This fully replicated directory allows rapid addressing of all users, irrespective of intervening HF links.

Cobalt is run on a shore system (HFAP or FAREP) to update users and roles. Cobalt may also be run on MUs (read only) to view user information. Directory information about users, accounts and roles is available on all nodes. White pages information on all users is used by products such as Harrier for address lookup.

The directory may also replicate in white pages information from external directories, so that users with addresses external to the Icon-Topo managed system can be addressed from HF nodes.

Isode servers running on Icon-Topo managed nodes will be able to use account information to authenticate users and control delivery of messages to local users.

Chapter 2 Directory And Configuration

This chapter explains in more detail how Icon-Topo configuration is held in the Directory and how configuration works.

2.1 Scheduling of configuration changes

It is desirable that some changes happen at the same time on each node, noting that in some cases described later, that order of change is important. This means that changes are coordinated relative to a fixed time.

Directory replication to MUs relies on HF communication, where there may be delays. The Icon-Topo architecture allows for this by scheduling all Icon-Topo changes. Each change to Icon-Topo has a scheduled time. An Icon-Topo network has a specified “freeze time”, which is the shortest time ahead of the current time for which a change can be scheduled. This time is set to a value that will give a high probability that the change can be replicated to all relevant MUs within that time. The Icon-Topo approach can recover from “lost” schedules, but this may require manual intervention, where the lost schedule has caused communication breakage. Scheduling changes as far into the future as possible will maximize resilience.

Scheduled changes are held in the directory, using an information framework to represent scheduled changes. The high level picture is that the DIT contains the current Icon-Topo values and a list of changes scheduled for future dates. The “freeze time” ensures that future changes within that time frame are stable.

Shortly after a scheduled change time, a designated FAREP node will merge the historical change into the current DIT, so that the DIT reflects current status and future changes only. These changes are replicated to all nodes.

Having changes arriving close together has potential to cause problems, which is addressed by a “minimum schedule interval” that specifies the shortest time between scheduled updates. This will generally lead to changes being batched at intervals, with this time being the minimum interval.

2.2 Mapping DIT to Configuration

Information held in the Icon-Topo part of the DIT represents the configuration of each Icon-Topo managed node, plus a series of scheduled changes to that configuration.

For an Icon-Topo managed node (FAREP, HFAP or MU), the configuration of each Isode server on the node can be derived from this DIT information. The key processing done by an Icon-Topo Update server is to derive the configuration information for the local node. For some Isode servers this represents the complete core configuration. Some aspects of the configuration may be modified locally to the node. For some servers, additional local configuration is essential for full operation.

A new Icon-Topo node is created in the DIT using the Icon-Topo Configuration Server. Then the Icon-Topo Update server on the node will be pointed at the deployed Icon-Topo directory. For an MU, it is expected that the MU will have fast IP access to shore for initial

setup. The Icon-Topo Update server will then create initial configurations for the Isode applications.

Icon-Topo Update server will then keep the configuration aligned to the DIT. Where there is an upcoming change scheduled, Icon-Topo Update server will compare the current configuration to the one derived from the DIT. In normal operation, these are expected to be the same. A difference implies that some updates have been missed (or partially missed), and Icon-Topo Update Server will immediately align configuration to the current DIT. Icon-Topo Update Server will also check that there are no schedules in the past, which implies a missed directory update.

2.3 Replicating Configuration Information

Each Icon-Topo managed node (MU, HFAP, FAREP) runs an M-Vault server, which contains the Icon-Topo configuration information and White Pages / Account information.

Directory replication on shore (all HFAPs and FAREPs) is done with M-Vault multi-master replication of all information. This enables data modification from any shore node.

Replication to MUs is done using Sodium Sync incremental replication over email, to share a subset of this information needed by each MU. This is expected to be all the provisioned users and roles, plus information from Icon-Topo necessary for the MU. This provides an up to date read-only copy of the relevant data in each MU

2.4 Information Held in the Directory for Icon-Topo

The information held in the directory represents the “global” information for each node. This information can be represented in the directory using straightforward schema. It provides data, including:

- General information for each node
- Protocol information for fast links (XMPP, SMTP, X.400 P1, ACP 127 over TCP) between HFAPs and FAREPs
- Management of ALE and Fixed Frequency networks
- Geographic location for HFAPs and MUs, with direction of travel for MUs. The key function of this data is to correctly configure application routing, so that communication between MU and shore continues as topology changes

Chapter 3 Getting Started

This chapter explains the steps required to get the Isode Icon-Topo Configuration Server up and running with basic operator access.

3.1 M-Vault DSA

You need to create an M-Vault DSA to hold the Icon-Topo database. This DSA is also used for authenticating users of the Web UI. This DSA needs a user which will be used by the Icon-Topo processes to access the data.

Decide where in the DIT the Icon-Topo database should reside. This is set by the directory name of the root entry. This is set in the config file as `<root>`. In the example below.

3.2 Topo Configuration Overview

The main Icon-Topo is in `$(ETCDIR)/topo/topoboot.xml`. Using a text editor create the file: for example:

```
<topoboot>
  <db-dsa>
    <ldaphost>ldap://localhost:19389/</ldaphost>
    <root>topoDBName=Topo DB,o=Isode,o=messaging</root>
    <sasluser>topo.admin@hardie.isode.net</sasluser>
    <password>secret</password>
    <saslmech>SCRAM-SHA-1</saslmech>
  </db-dsa>
</topoboot>
```

This file is divided into sections. Each section relates to a different aspect of the configuration.

3.2.1 Icon-Topo DB Connection

The `<db-dsa>` section configures the connection to the DSA which holds the Icon-Topo Database. It is common to both the Configuration Server and the Update Server.

ldaphost

contains the value of the LDAP URL for the server.

root

is the DN of the root entry for the Icon-Topo Database.

sasluser

is the SASL ID of the chosen user. Alternatively, *userdn* can be set to the DN of the user, in which case an LDAP simple bind is performed rather than a SASL bind.

Note: This user needs to be a suitably privileged user/role with write access to the icon-topo portion of the DIT.

password

is the user's password. This can be protected using *servpass*. See [Section 4.4, "Configuration of Passwords"](#) for a further explanation and example of *servpass* configuration and usage.

saslmech

This specifies the SASL mechanism to be used when authenticating to the DSA. It is optional. If not specified, one of the mechanisms offered by the DSA will be used.

usetls

If specified, the server will enable TLS to the DSA. This can be used for confidentiality, and is strongly advised if a plain-text password mechanism is to be used.

With no value specified, the client does not pass an identity to the DSA. No value should be specified as `<usetls/>`. To understand how to specify an identity to be passed, e.g. for use with EXTERNAL, see the section on TLS configuration below.

3.3 Topo Configuration Root

The database information is held in an area of the Directory Information Tree (DIT). The root entry for this area needs to be created. If the database area is to have its own access control, the root entry will need to be created manually by a suitably privileged user. The database access user should not have privileges to do this.

If this is not the case, then the root entry can be created using a suitable Directory Administration tool such as Isode's Sodium GUI tool.

Note: that if a new root naming context is created for Icon-Topo, it should be created as an administrative area.

Alternatively the root entry can be created using the following command in a shell:

```
$(BINDIR)/toposendop -e $(SHAREDIR)/topo/root-create.json
```

3.4 Adding The Topo Schema

The Icon-Topo database holds information about the Icon-Topo database schema in the DIT. This needs to be loaded using this command prior to running the Icon-Topo servers:

```
$(BINDIR)/toposendop -e $(SHAREDIR)/topo/schema-update.json
```

This command is also used to update the schema.

3.5 Create Topo run time user

On linux it is important to create a run time user `icontopo` under which the the Icon-Topo services run. Failure to do this means the Icon-Topo service will fail to start, or that they run with unnecessary root privileges.

The user can be created with the following command:

```
useradd icontopo
```

3.6 Create and Start Service

3.6.1 Windows

The Icon-Topo Services are created when the Icon-Topo packages are installed.

To Start, Stop or Modify the Icon-Topo Services, you can use the Windows Service Manager. Alternatively the M-Switch package can be installed and the Isode Service Manager used to start the `topo.web` Service.

The two Windows Services are:

- Icon-Topo Configuration Service
- Icon-Topo Update Service

3.6.2 Linux

3.6.2.1 Configuration Server

Run this command to register the configuration server with `systemd`. By default the service will be started when the system starts:

```
$(SBINDIR)/icon-topo-config-systemd.sh enable
```

This is a wrapper round this command:

```
systemctl start
```

3.6.2.2 Update Server

Run this command to register the update server with `systemd`. By default the service will be started when the system starts:

```
$(SBINDIR)/icon-topo-update-systemd.sh enable
```

3.6.2.3 Using systemd

Once the above commands have run, they appear as systemd services:

```
systemctl list-unit-files --type=service |grep topo
icon-topo-config.service          enabled disabled
icon-topo-update.service         enabled disabled
```

The services can then be started using the systemctl command

```
systemctl start icon-topo-config
```

```
systemctl start icon-topo-update
```

The status of the services can be checked using:

```
systemctl status icon-topo-config
```

```
systemctl status icon-topo-update
```

3.7 Web Access to the Configuration Server

You should now be able to use a browser to access the database, using:

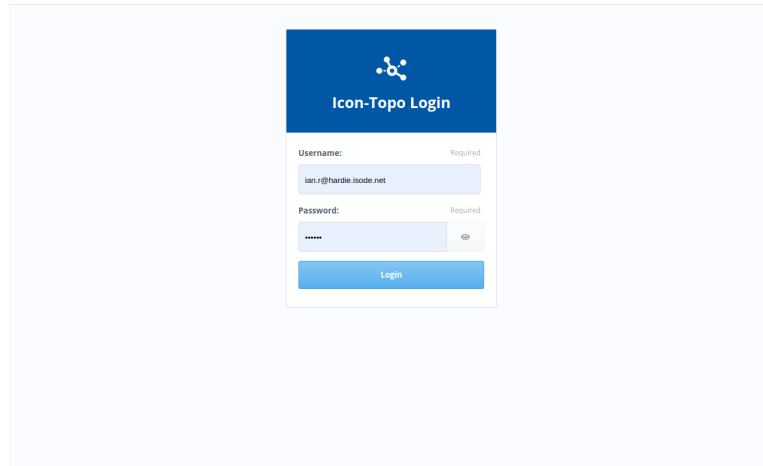
```
https://<hostname>:17000
```

Until the web server's TLS identity has been established, the server will generate a self-signed identity. You will need to permit your browser to accept this. To see how a proper identity can be established, see the section on TLS configuration below.

If you are unable to connect, check the Icon-Topo event log in \$(LOGDIR) for any errors which might give an indication of the problem.

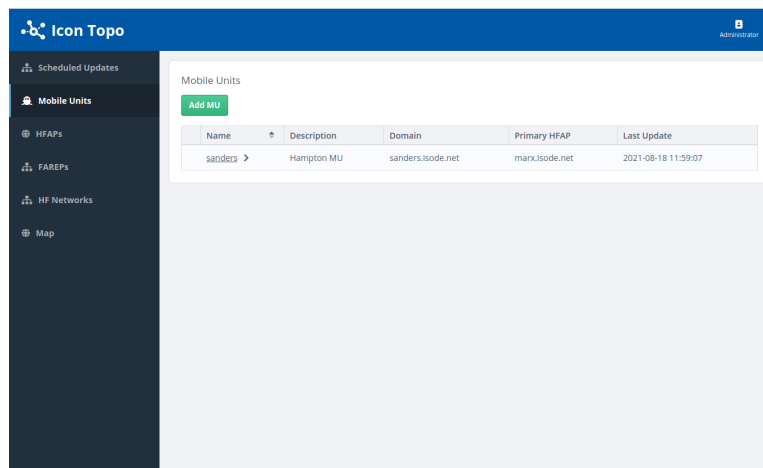
Note: By default, any user with a valid SASL authentication can now run the Icon-Topo configuration UI.

The following shows the basic login screen.

Figure 3.1. Icon-Topo Basic Login Screen

The login screen features a blue header with the Icon-Topo logo and the text "Icon-Topo Login". Below the header is a form with two input fields: "Username:" and "Password:". The "Username:" field contains the text "ian.r@hardie.isode.net". The "Password:" field is masked with dots. To the right of each field is a "Required" label. Below the form is a blue "Login" button.

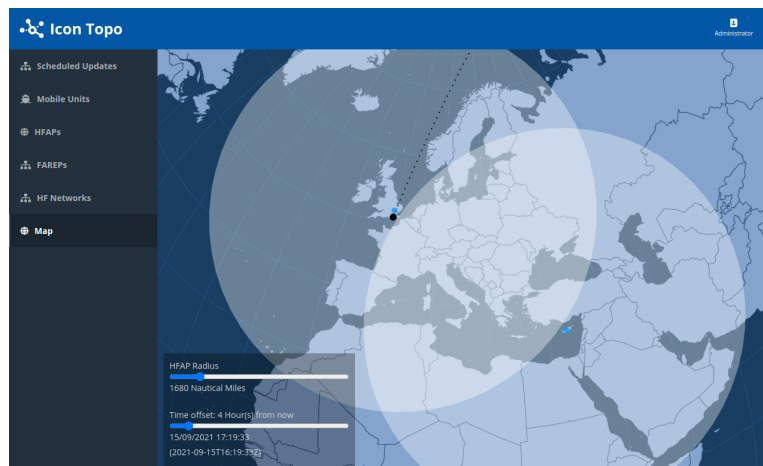
The following shows the initial screen after login.

Figure 3.2. Icon-Topo Initial Screen

The initial screen shows a dashboard with a left sidebar and a main content area. The sidebar includes "Scheduled Updates", "Mobile Units", "HFAPs", "FAREPs", "HF Networks", and "Map". The main content area displays a table of Mobile Units.

Name	Description	Domain	Primary HFAP	Last Update
sanders >	Hampton MU	sanders.isode.net	marx.isode.net	2021-08-18 11:59:07

The following shows the map view.

Figure 3.3. Icon-Topo Map View

Chapter 4 Configuration Server

This chapter describes the Isode Icon-Topo Configuration Server describing the Web based User Interface features, and lists the configuration options available.

4.1 Icon-Topo Configuration Server

Icon-Topo has management and operator interfaces allowing the product to be deployed and managed. This chapter describes how these can be used. These interfaces use a standard web browser to access the configuration server. The Configuration Server itself is configured using the `topboot.xml` configurations file which was introduced in [Chapter 3, Getting Started](#).

The complete set of Configuration Server and General configuration options available are listed here. See [Chapter 5, Update Server](#) for the configuration options available for the Update Server.

4.2 Using the Configuration Service

The Icon Topo Configuration Server's Web UI allows the viewing and managing the Icon-Topo entities.

The UI is accessed using a standard web browser, and has several views which may appear slightly differently depending on the user's authorization level (see below)

There is also a Left Hand Navigation panel with more links. These will take the user to:

- FAREPs – View all FAREPs. Admins can Add New or modify existing FAREPs from this page.
- HFAPs – View all HFAPs which have been added to the configuration server. Administrators can also add new HFAPs or modify existing HFAPs from this page.
- HF Networks - View all the HF Networks which have been added to the configuration server. Administrators can also add new or modify existing HF Networks from this page.
- Mobile Units – View all Mobile Units which have been added to the configuration server. Administrators can also add new MUs or modify existing MUs from this page.
- Scheduled Updates - View all the scheduled updates that are configured.
- Map – View and interact with all MUs, HFAPs and Scheduled Updates. MUs and HFAPs must have been configured with a position (see [Section 4.2.2.3, “HFAP Position: ”](#)) to become visible on the map screen.

Views are available to both Operator and Administrator roles (see [Section 4.5, “Access Control”](#)). A "Read Only" role is also available. The user's role may affect the way that information is shown, or the ability of the user to make modifications: see the descriptions of the individual views below.

4.2.1 FAREPs (Fixed Application Routing Entry Points)

All FAREPs which have been added to the Configuration Server will be listed here.

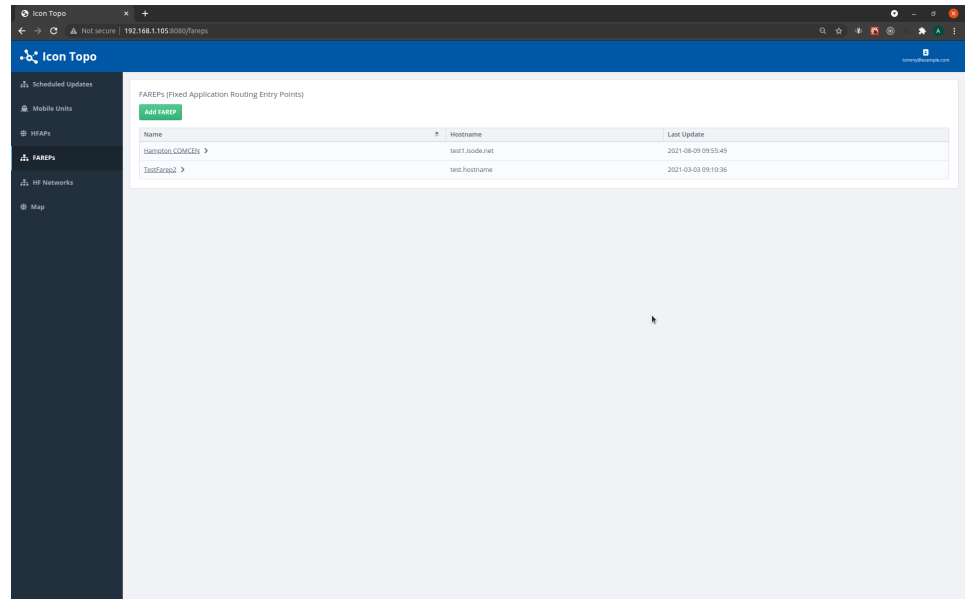
If the logged in user is an Administrator, then there will also be a button labelled “Add FAREP” which allows adding more FAREPs to the Configuration Server.

All users will also be able to see more information by clicking on the name of the FAREP in the table.

An Administrator will also be able to modify a FAREP’s details by clicking on the name and editing the details form. (see [Section 4.2.1.2, “FAREP Details Form:”](#))

The following screenshot shows the FAREP listing screen.

Figure 4.1. This screen shows all the configured FAREPs

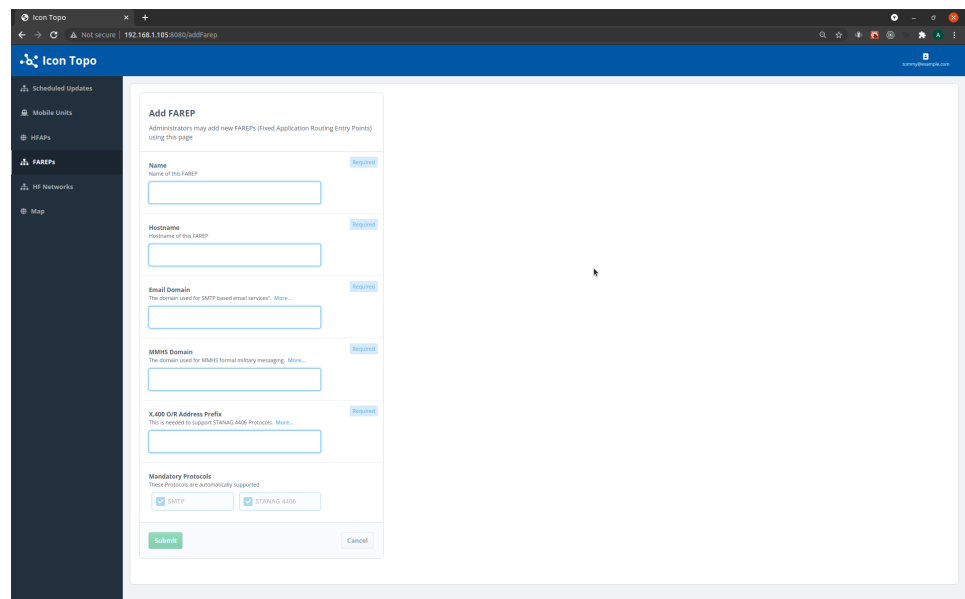


4.2.1.1 Adding FAREPs

To add the FAREP, complete all relevant fields. All Mandatory Protocols are preselected by default.

The following screenshot shows how to add a FAREP.

Figure 4.2. Administrators use this form to add a FAREP



Name

The name of this FAREP

Hostname

The hostname of this FAREP.

Email Domain

Enter the SMTP domain for this FAREP

MMHS Domain

Enter the SMTP domain for this FAREP when using formal messaging

X.400 O/R Address Prefix

Enter the X.400 O/R Address Prefix which is to be routed to this FAREP when using STANAG 4406.

Protocols

Two read only checkboxes which list the mandatory protocols for the FAREP.

Configure XMPP

If any Mobile Units are to support XMPP, XMPP should be enabled. The XMPP Port must be set to a value which is unique among the FAREPs, HFAPs and MUs.

Once all required fields have been populated, the green “Submit” button will become active. Click this button to save the FAREP. Details may be edited later by the Administrator by clicking on the newly created FAREP which will appear in the FAREPs list page.

Note: In order to add a Mobile Unit, there must be at least 1 HFAP and 1 FAREP to select from the list, and so both the Add HFAP and Add FAREP forms must be completed before adding any Mobile Units.

4.2.1.2 FAREP Details Form:

The following screenshot shows how to view and edit FAREPs.

Figure 4.3. Administrators use this form to view and edit FAREPs

The screenshot displays the 'View / Modify FAREP' form in a web browser. The form is titled 'View / Modify FAREP' and includes a sub-header: 'Administrators may modify the current FAREP (fixed application Routing Entry Point) using this page.' The form fields are as follows:

- Name:** Name of this FAREP. Value: Hampton COMCEN.
- Hostname:** Hostname of this FAREP. Value: 10011.1000@net. Label: Required.
- Email Domain:** The domain used for SMTP based email services. More... Value: 10011.1000.com. Label: Required.
- MMHS Domain:** The domain used for MMHS formal military messaging. More... Value: 10011.1000@. Label: Required.
- X.400 O/R Address Prefix:** This is needed to support STANAG 4406 Protocols. More... Value: 0019602. Label: Required.
- Mandatory Protocols:** These Protocols are automatically supported.
 - SMTP
 - STANAG 4406

At the bottom of the form, there is a green 'Submit' button, a 'Delete...' button, and a 'Cancel' button.

Edit FAREPs by clicking on the name in the FAREPs list page. The form itself is identical to the “Add FAREP” page, except that there will already be configuration populated in the fields. Edit by changing these fields as required and clicking “Submit”.

Once all the required fields are completed, the green “Submit” button is enabled. Click on this button to save the FAREP.

Administrators may also delete this FAREP by clicking the “Delete” button or “Cancel” current changes.

4.2.2 HFAPs (High Frequency Access Points)

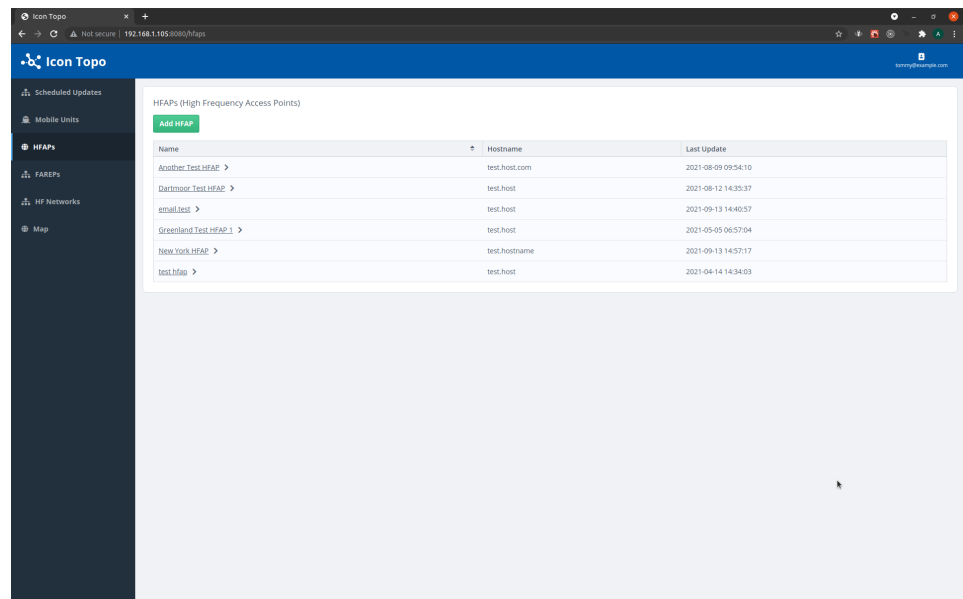
All HFAPs which have been added to the Configuration Server will be listed here.

If the logged in user is an Administrator, then there will also be a button labelled “Add HFAP” which allows adding more HFAPs to the Configuration Server.

All users will also be able to see more information by clicking on the name of the HFAP in the table. An Administrator will also be able to modify HFAPs’ details by clicking on the name and editing the details form. (see [Section 4.2.2.2, “HFAP Details”](#))

The following screenshot shows how to view HFAPs.

Figure 4.4. Administrators use this form to view HFAPs



If no HFAPs appear on this page, then an Administrator must create them, using the “Add HFAP” button, and completing the form. (See [Figure 4.5, “Administrators use this form to add HFAPs”](#)).

4.2.2.1 Add HFAP form:

Note: For HF Networks to appear in the Current HF Networks field, they must be added to the Configuration Server before this HFAP. (See [Figure 4.10, “Use this form to add an HF Network”](#)).

To add the HFAP, complete all relevant fields. As with adding MUs, the STANAG5066 address must be unique to this entity, and all Mandatory Protocols are preselected by default.

The following screenshot shows how to add HFAPs.

Figure 4.5. Administrators use this form to add HFAPs

Add HFAP

Administrators may add a new HFAP (High Frequency Access Point) using this page

Name Required
Name of this HFAP

STANAG5066 Address Required
Enter the STANAG5066 Address

Current HF Networks Required
Changes will be applied when hitting 'Submit' or reverted with 'Cancel'.
There are no Networks associated with this HFAP

Add an HF Network
Select an HF Network

Hostname Required
Enter a valid hostname of this HFAP

Email Domain Required
The domain used for SMTP based email services". [More...](#)

MMHS Domain Required
The domain used for MMHS formal military messaging. [More...](#)

X.400 O/R Address Prefix Required
This is needed to support STANAG 4406 Protocols. [More...](#)

Mandatory Protocols
These Protocols are automatically supported

SMTP STANAG 4406
 ACP 142/S4406E ACP 142/MULE

Protocols
You may select more messaging protocols if required

CFTP ACP 127

Submit **Cancel**

Name

The name of this HFAP

STANAG5066 Address

The address to use for the 5066 Server. The STANAG5066 address must be unique to this entity,

Primary HF Network

The primary HF Network to which this HFAP is connected.

Hostname

The hostname of this HFAP.

Email Domain

Enter the SMTP domain for this HFAP

X.400 O/R Address Prefix

Enter the X.400 O/R Address Prefix which is to be routed to this HFAP when using STANAG 4406.

Mandatory Protocols

Four read only checkboxes which list the mandatory protocols for the HFAP.

Protocols

Two checkboxes which allow optional protocols (CFTP and ACP 127) to be set for the HFAP. If ACP 127 is selected, ACP 127 Broadcast Circuit name(s) must be added. Currently, CFTP is not supported.

ACP127 Broadcast Circuit

The HFAP communicates with MUs using ACP 127 Broadcast Circuits. This entry is used to configure the names of the ACP 127 Broadcast Circuits which are configured in the M-Switch server.

Configure XMPP

If any Mobile Units are to support XMPP, XMPP should be enabled. The XMPP Port must be set to a value which is unique among the FAREPs, HFAPs and MUs.

Once all required fields have been populated, the green “Submit” button is enabled. Click this button to save the HFAP. Details may be edited later by the Administrator by clicking on the newly created HFAP which will appear in the HFAPs list page.

4.2.2.2 HFAP Details

Edit HFAPs by clicking on the name in the HFAPs list page. The form itself is identical to the “Add HFAP” page, except that there will already be configuration populated in the fields. Edit by changing these fields as required and clicking “Submit”.

4.2.2.2.1 Tab Navigation

Beneath the title, which displays the HFAP’s name and short description of the current page, the user is presented with 2 tabs which can be used to navigate between the HFAP’s configuration Details and Position:

- View Details – All the current HFAP’s configuration can be accessed and modified here (Administrators only).
- Position – The HFAP’s Position (Longitude and Latitude) can be modified here. (Administrators only). See [Section 4.2.2.3, “HFAP Position: ”](#)

The following screenshots show how to edit HFAPs (split into two for convenience).

Figure 4.6. Administrators use this form to edit HFAPs

Icon Topo

- Scheduled Updates
- Mobile Units
- HFAPs**
- FAREPs
- HF Networks
- Map

Dartmoor Test HFAP

View or modify details and position

View Details Position

View / Modify HFAP

Administrators may modify the current HFAP (High Frequency Access Point)

Name
Name of this HFAP
Dartmoor Test HFAP

STANAG5066 Address Required
Enter the STANAG5066 Address
1.1.32.4

Current HF Networks Required
Changes will be applied when hitting 'Submit' or reverted with 'Cancel'.

Name	Description	
network-1000	test-1000	X
test 10	test test	X

Add an HF Network
Select an HF Network

Figure 4.7. Administrators use this form to edit HFAPs

The screenshot shows a web-based configuration form for editing HFAPs. On the left is a dark sidebar with navigation links: 'FAREPs', 'HF Networks', and 'Map'. The main content area is a light-colored form with the following sections:

- Hostname** (Required): Text input field containing 'test.host'.
- Email Domain** (Required): Text input field containing 'test.email'. Subtext: 'The domain used for SMTP based email services'. [More...](#)
- MMHS Domain** (Required): Text input field containing 'test.mmhs'. Subtext: 'The domain used for MMHS formal military messaging'. [More...](#)
- X.400 O/R Address Prefix** (Required): Text input field containing '/o=test/'. Subtext: 'This is needed to support STANAG 4406 Protocols'. [More...](#)
- Mandatory Protocols**: Subtext: 'These Protocols are automatically supported'. Contains four checked checkboxes: SMTP, STANAG 4406, ACP 142/S4406E, and ACP 142/MULE.
- Protocols**: Subtext: 'You may select more messaging protocols if required'. Contains two checkboxes: CFTP (checked) and ACP 127 (unchecked).

At the bottom of the form are three buttons: 'Submit' (green), 'Delete...' (grey), and 'Cancel' (grey).

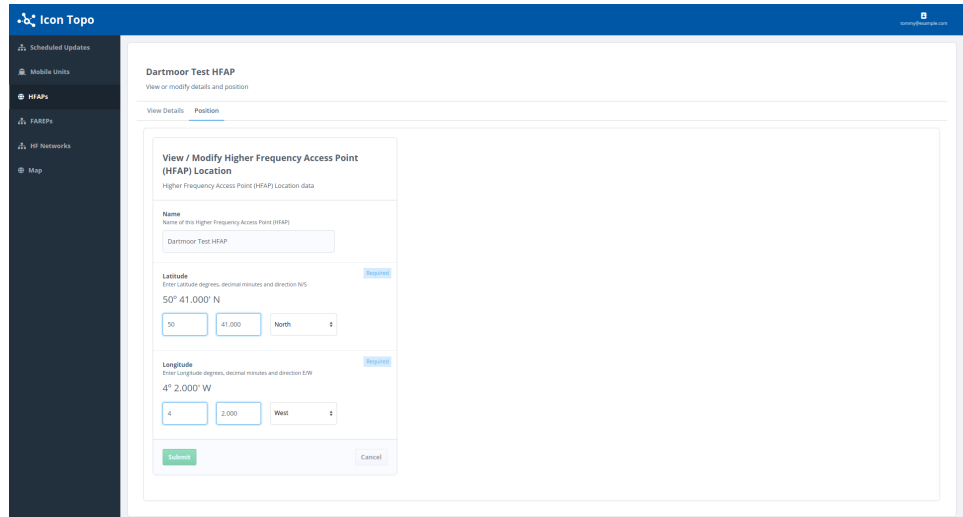
Note: If the name of the HFAP is incorrect, then the HFAP must be deleted and added again with the correct name.

4.2.2.3 HFAP Position:

The Position tab allows users to view the current HFAP location in Latitude and Longitude. The format: Degrees and Decimal Minutes in the same way as the positions of Mobile Units. An administrator may add or edit the location using this form.

The following screenshot shows how to edit the position of an HFAP.

Figure 4.8. Administrators use this form to edit the HFAP's position



Once an HFAP has a position entered, then it should appear in the Map screen.

4.2.3 HF Networks

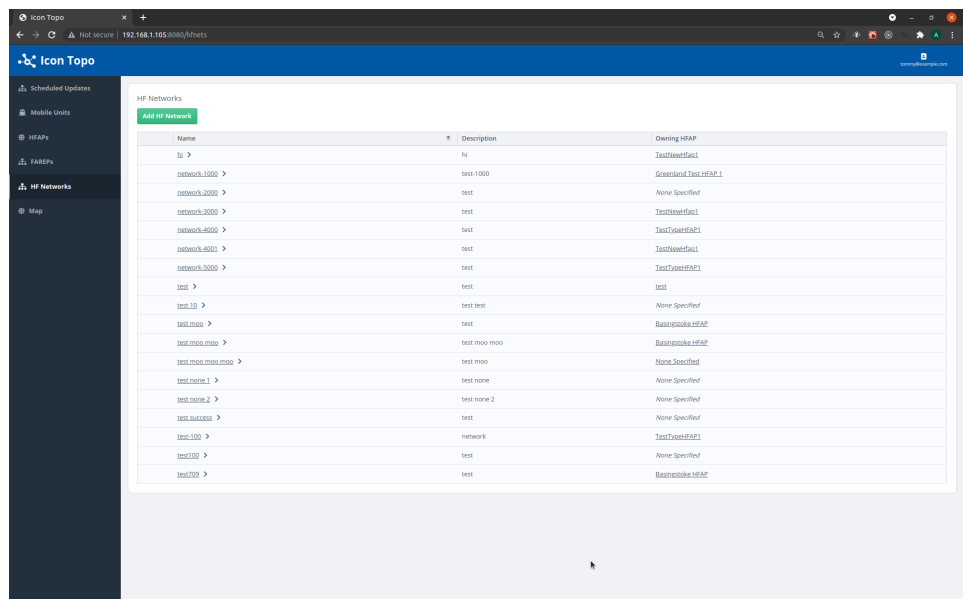
All HF Networks which have been added to the Configuration Server will be listed here.

If the logged in user is an Administrator, then there will also be a button labelled “Add HF Network” which allows adding more HF Networks to the Configuration Server.

All users will also be able to see more information by clicking on the name of the HF Network in the table. An Administrator will also be able to modify an HF Network’s details by clicking on the name and editing the details form. (see [Section 4.2.3.2, “HF Network Details”](#))

The following screenshot shows how to view HF Networks.

Figure 4.9. Viewing of configured HF Networks



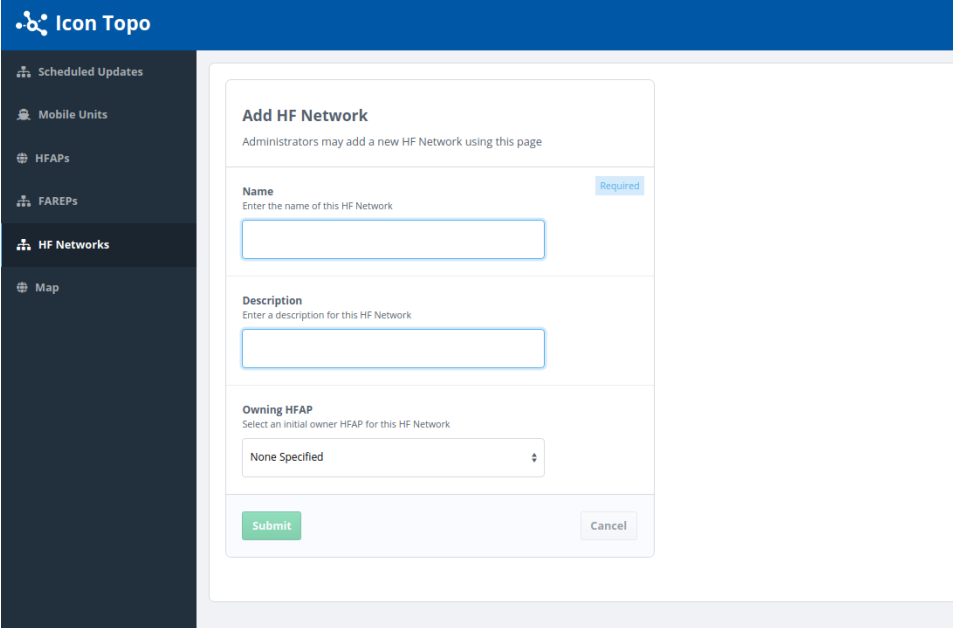
4.2.3.1 Add HF Network

To add an HF Network, complete all relevant fields. Note that only HFAPs which have been added to the Configuration Server already will be selectable in the “Owning HFAP” field.

For creation only the “Name” field is required, so an Administrator could press Submit to create the HF Network once the Name field is complete. (“Description” and “Owning HFAP” can be completed later if required).

The following screenshot shows how to add an HF Network.

Figure 4.10. Use this form to add an HF Network



The screenshot shows the 'Add HF Network' form in the Icon Topo interface. The form is titled 'Add HF Network' and includes the following fields:

- Name**: A text input field with a 'Required' label. The placeholder text is 'Enter the name of this HF Network'.
- Description**: A text input field with a placeholder text of 'Enter a description for this HF Network'.
- Owning HFAP**: A dropdown menu with the placeholder text 'Select an initial owner HFAP for this HF Network' and the current selection 'None Specified'.

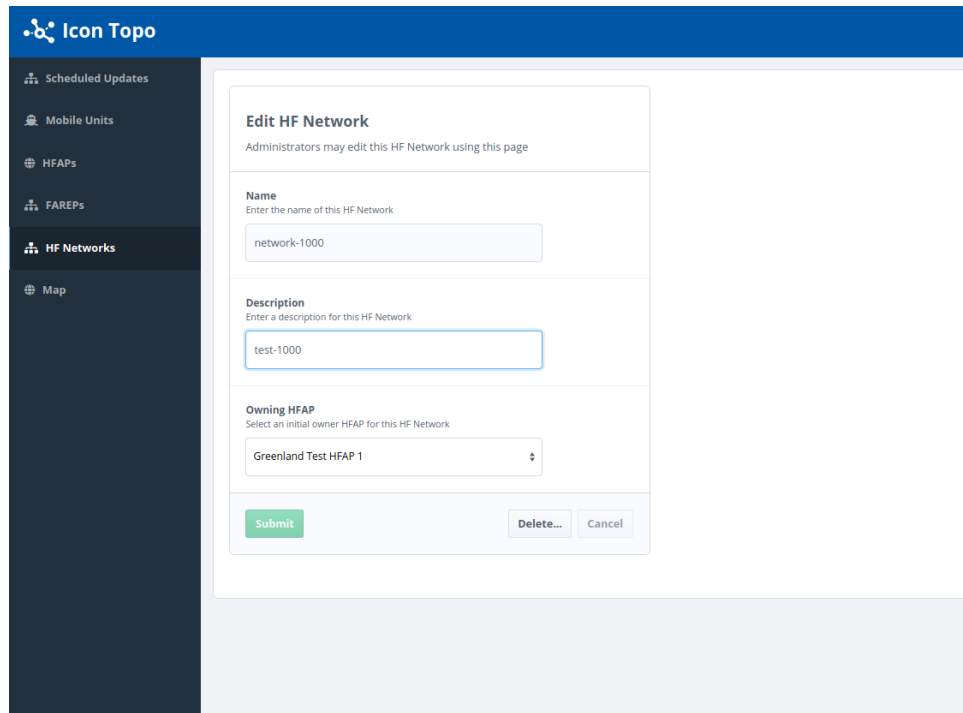
At the bottom of the form, there are two buttons: 'Submit' (green) and 'Cancel' (grey).

4.2.3.2 HF Network Details

Edit HF Networks by clicking on the name in the HF Networks list page. Edit by changing these fields as required and clicking “Submit”. (Administrator only).

The following screenshot shows how to edit HF Networks.

Figure 4.11. Administrators use this form to edit HF Networks

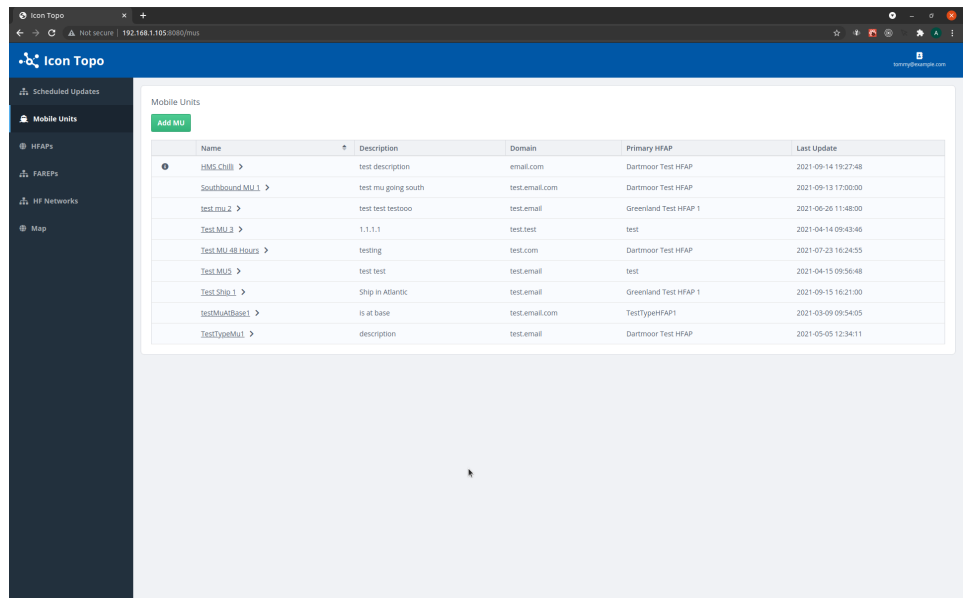


4.2.4 Mobile Units

All Mobile Units which have been added to the Configuration Server will be listed here. If the logged in user is an Administrator, then there will also be a button labelled “Add MU” which allows adding more MUs to the Configuration Server.

The following screenshot shows the list of Mobile Units.

Figure 4.12. Mobile Units list page when viewed by an administrator.



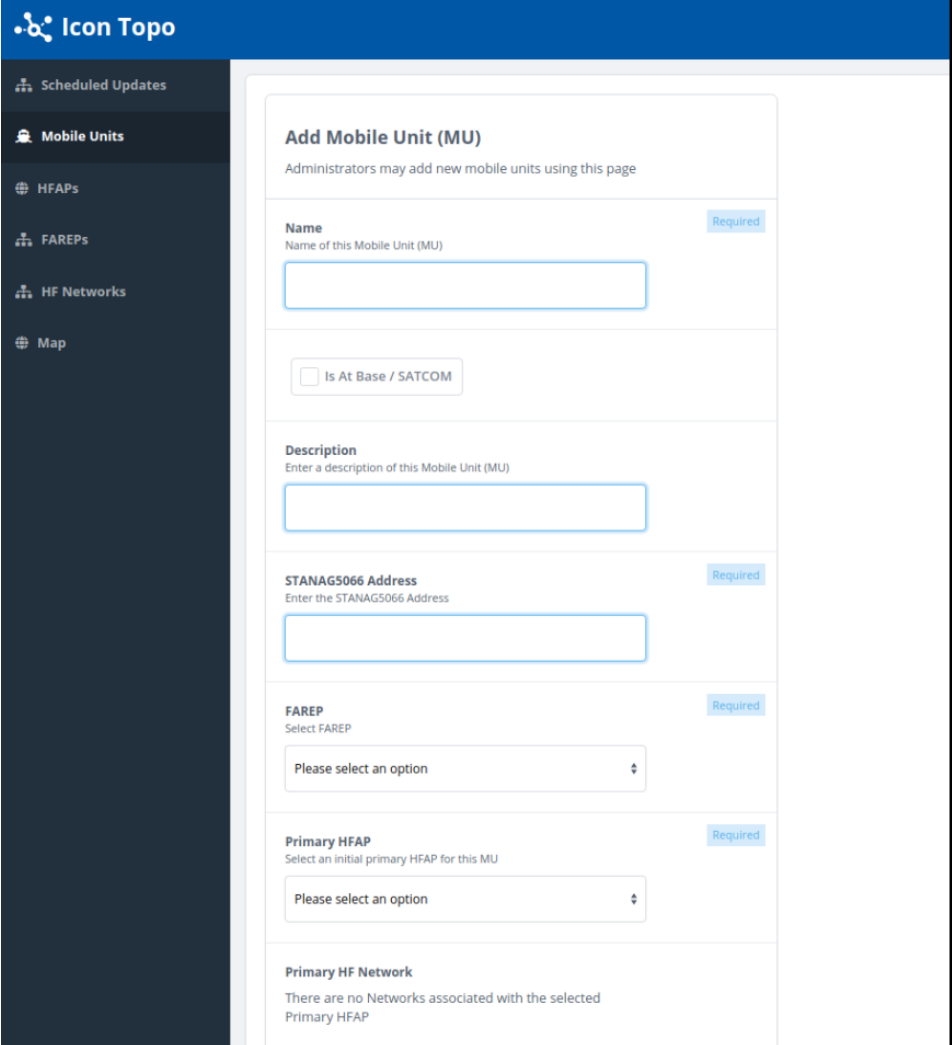
All users will also be able to see more information by clicking on the name of the Mobile Unit in the table. An Administrator will also be able to modify Mobile Units’ details by clicking on the name and editing the details form. (see [Section 4.2.4.3, “Mobile Unit Details”](#))

4.2.4.1 Add Mobile Unit

Note: HFAPs and FAREPs must have already been added to the Configuration Server in order to be selectable when completing this form.

The following screenshots show how to add Mobile Units (split into 2 for convenience).

Figure 4.13. Administrators use this form to add Mobile Units (top half)



The screenshot displays the 'Add Mobile Unit (MU)' form within the Icon Topo application. The interface features a dark blue header with the 'Icon Topo' logo and a left-hand navigation menu. The main content area is white and contains the following form fields:

- Name:** A text input field with a 'Required' label. The placeholder text is 'Name of this Mobile Unit (MU)'.
- Is At Base / SATCOM:** A checkbox.
- Description:** A text input field with a placeholder text 'Enter a description of this Mobile Unit (MU)'.
- STANAG5066 Address:** A text input field with a 'Required' label. The placeholder text is 'Enter the STANAG5066 Address'.
- FAREP:** A dropdown menu with a 'Required' label. The placeholder text is 'Please select an option'.
- Primary HFAP:** A dropdown menu with a 'Required' label. The placeholder text is 'Please select an option'.
- Primary HF Network:** A section with the text 'There are no Networks associated with the selected Primary HFAP'.

Figure 4.14. Administrators use this form to add Mobile Units (bottom half)

The screenshot shows the bottom half of a configuration form for adding Mobile Units. On the left is a dark sidebar with navigation options: Mobile Units, HFAPs, FAREPs, HF Networks, and Map. The main form area contains the following sections:

- Associated HFAPs** (Required): A section titled "Choose HFAPs associated with this MU" with six checkboxes: Another Test HFAP, Dartmoor Test HFAP, email.test, Greenland Test HFAP 1, New York HFAP, and test hfap.
- Email Domain** (Required): A text input field with the description "The domain used for SMTP based email services".
- MMHS Domain** (Required): A text input field with the description "The domain used for MMHS formal military messaging".
- X.400 O/R Address Prefix** (Required): A text input field with the description "This is needed to support STANAG 4406 Protocols".
- Base Address** (Required): A text input field with the description "The IP address or hostname of the system on which Icon-Topo and the applications are running".
- Mobile Unit is running Icon-Topo**: A checked checkbox.
- Mandatory Protocols**: A section titled "These Protocols are automatically supported" with four checked checkboxes: SMTP, STANAG 4406, ACP 142/S4406E, and ACP 142/MULE.
- Protocols**: A section titled "You may select more messaging protocols if required" with two unchecked checkboxes: CFTP and ACP 127.

At the bottom of the form are three buttons: a green "Submit" button, a "Back" button (left arrow), and a "Cancel" button.

To add the Mobile Unit, complete all relevant fields. The STANAG5066 address must be unique to this entity, and the “Mobile Unit is Running Icon topo” option is selected by default which means that four mandatory Protocols are preselected.

Primary HFAP the Mobile Unit is connected to, its associated FAREPs, host domain name and messaging protocols. An Administrator is allowed to reconfigure these values. For a more detailed explanation of each of these parameters, see the text description located under the label for each field. All users can read these parameters, but only Administrators may change them.

Name

The name of this Mobile Unit

Is at Base/SATCOM

Check the box if the Mobile Unit is at base or has other access to fast (non HF) networking

Description

A textual description of this Mobile Unit.

STANAG5066 Address

The address to use for the 5066 Server. The STANAG5066 address must be unique to this entity,

FAREP

The name of the FAREP to which this MU is connected.

Primary HFAP

Select the FAREP from the configured list to and from which this Mobile Unit sends and receives messages

Primary HF Network

The primary HF Network to which this MU is connected. Is overridden if the At Base/Satcom checkbox is ticked.

Associated HFAPs

Each configured HFAP can be set as associated to this Mobile Unit

Email Domain

Enter the SMTP domain for this Mobile Unit

MMHS Domain

Enter the SMTP domain for this Mobile Unit when using formal messaging

X.400 O/R Address Prefix

Enter the X.400 O/R Address Prefix which is to be routed to this Mobile Unit when using STANAG 4406.

Base Address

Enter the IP address of the system running Icon-Topo on the Mobile Unit.

Mobile Unit is Running Topo

Checkbox to be ticked if Icon-Topo is running on this Mobile Unit. This option is selected as true by default which means that four mandatory Protocols are preselected

Protocols

Two checkboxes which allow optional protocols (CFTP and ACP127) to be set for the Mobile Unit.

ACP127 RI

The MUs Routing Indicator must be set here if ACP 127 is enabled as a protocol.

ACP127 Broadcast Circuits

If the MU can receive over ACP 127, this can be set to specify which Broadcast Circuit or Circuits at the Primary HFAP are to be used for sending to the MU. If not specified, then any of the HFAPs Broadcast Circuits may be used.

Configure XMPP

If the Mobile Unit is to support XMPP, XMPP should be enabled. The XMPP Domain should be set to the MUs XMPP domain. The XMPP Port must be set to a value which is unique among the FAREPs, HFAPs and MUs.

Complete the form as required and click “Submit” to add the Mobile Unit.

4.2.4.2 Mobile Unit Schedule Update

Clicking on a Mobile Unit (either by name, or from the map screen) takes the user to a more detailed view of a particular Mobile Unit and its configuration – opening with the Mobile Unit’s Scheduled Updates Tab as in [Figure 4.15, “Administrators use this form to Schedule Updates to Mobile Units ”](#).

4.2.4.2.1 Tab Navigation

Beneath the title, which displays the Mobile Unit’s name and a short description of the current page, the user should be presented with three tabs which can be used to navigate between the Mobile Units:

- Scheduled Updates – This is the main area for scheduling updates. Note only those with Operator or Administrator access will be presented with the Scheduled Updates form
- Details – All the current Mobile Unit’s configuration can be accessed and modified here (Administrators only). See [Section 4.2.4.3, “Mobile Unit Details ”](#).

- Position – A Mobile Unit’s Course, Heading, and Position (Longitude and Latitude) can be modified here. (Administrators only). See [Section 4.2.4.4, “Mobile Unit Position”](#).

The following screenshot shows how to schedule updates to Mobile Units.

Figure 4.15. Administrators use this form to Schedule Updates to Mobile Units

The screenshot shows the 'Scheduled Updates' page for the mobile unit 'HMS Chillii'. The page has a dark sidebar with navigation options: Scheduled Updates, Mobile Units, HFAPs, FAREPs, HF Networks, and Map. The main content area is titled 'HMS Chillii' and includes a sub-header 'Schedule updates and view or modify details and position'. Below this, there are tabs for 'Scheduled Updates', 'Details', and 'Position'. The 'Scheduled Updates' tab is active, showing a table of current updates:

HFAP	Network	When	Cancel
Greenland Test HFAP 1	tu	2021-09-18 10:17:00Z (44 hours from now)	REMOVE
Dartmoor Test HFAP	network-1000	2021-09-19 10:18:00Z (3 days from now)	REMOVE

Below the table is a section titled 'Schedule an update to Primary HFAP'. It contains the following fields:

- Primary HFAP:** A dropdown menu with 'Dartmoor Test HFAP' selected.
- Primary HF Network:** A dropdown menu with 'network-1000' selected.
- Date/Time for Update:** A date and time picker showing '2021-09-16T11:38:29.177Z'.

At the bottom of the form are 'Submit' and 'Cancel' buttons.

4.2.4.2.2 Schedule an update to Primary HFAP

To use the Schedule Update form, the user simply needs to select the Primary HFAP which the Mobile Unit should switch to, the Primary HF Network which should be used at the time of the switch (if different), as well as a date and time for the update.

When the Operator is happy with the selections, then click Submit. Cancel should restore the default selections in case of any error.

A Green success notification should appear at the bottom of the screen if the update was scheduled successfully. A red error notification appears if there was a problem. Note that the Date/Time for Update must be sufficiently ahead of the present time or you’ll see a “Freeze time” error indicating that the time required to configure the change is not far enough in the future to guarantee the change can be propagated amongst all the entities in time. If this occurs, simply select a new time and try again.

4.2.4.3 Mobile Unit Details

The Mobile Unit Details screen comprises all the necessary configuration required for a Mobile Unit. This includes the Primary HFAP the Mobile Unit is connected to, its associated FAREPs, host domain name and messaging protocols. An Administrator is allowed to reconfigure these values. For a more detailed explanation of each of these parameters, see the text description located under the label for each field. All users can read these parameters, but only Administrators may change them.

The following screenshot shows how to configure the parameters of Mobile Units.

Figure 4.16. Administrators use this form to configure Mobile Units' parameters

The screenshot shows a web browser window with the URL `192.168.1.155:8080/mux/HM9N3DCM1`. The page title is "HMS Chilli" and it is part of the "Icon Topo" application. The left sidebar contains navigation options: "Scheduled Updates", "Mobile Units", "HFAPs", "FAREPs", "HF Networks", and "Map". The main content area is titled "View / Modify Mobile Unit" and includes the following fields:

- Name:** HMS Chilli
- Description:** text description
- STANAG566 Address:** 1.1.1.3 (Required)
- FAREP:** TextFarep2 (Required)
- Primary HFAP:** Outdoor Test HFAP (Required)
- Primary HF Network:** (Required)

To make changes to any of these parameters in the Mobile Units' Details page (as an Administrator) simply update any of the form's fields and click submit.

Administrators may also delete the Mobile Unit from this page. A confirmation dialogue will appear first to make sure they are happy to proceed with the deletion.

Cancel simply clears any modifications made to the Mobile Unit since it was last submitted.

This form is identical to the Add MUs page, except that when adding a new MU, all these fields will need to be filled in by the Administrator.

4.2.4.4 Mobile Unit Position

The last tab of the Mobile Units' Tab Navigation will take the user to a page showing the Mobile Unit's last reported position, course and heading. An Administrator may also use this page to update any of these fields.

The following screenshot shows how to update the position of Mobile Units.

Figure 4.17. Administrators use this form to update the position of Mobile Units

The screenshot shows a web browser window with the URL `192.168.1.105:8080/mcu/HMS%20CHIEF`. The page title is 'Icon Topo' and the user is logged in as 'Using HF'. The main content area is titled 'View / Modify Mobile Unit Course or Location' for 'Mobile Unit Location data'. The form contains the following fields:

- Name:** HMS CHIEF
- Last Update:** 2021-08-13 04:28:13 (Help)
- Course:** 00 (Help)
- Speed:** 200 (Help)
- Latitude:** 41° 0.740' N (Help)
- Longitude:** 59° 59.185' W (Help)

At the bottom of the form are 'Submit' and 'Cancel' buttons.

Course

The Mobile Unit's heading in degrees

Speed

The Mobile Unit's speed in knots

Latitude and Longitude

Displayed and edited in degrees and decimal minutes.

Submit reports any updates. Cancel clears them to the previous state. If any errors in the fields are present then an error message appears explaining what the problem is, and the Submit button will be disabled.

The Submit button is enabled automatically if any valid changes to the form have been made, and all required fields have been filled.

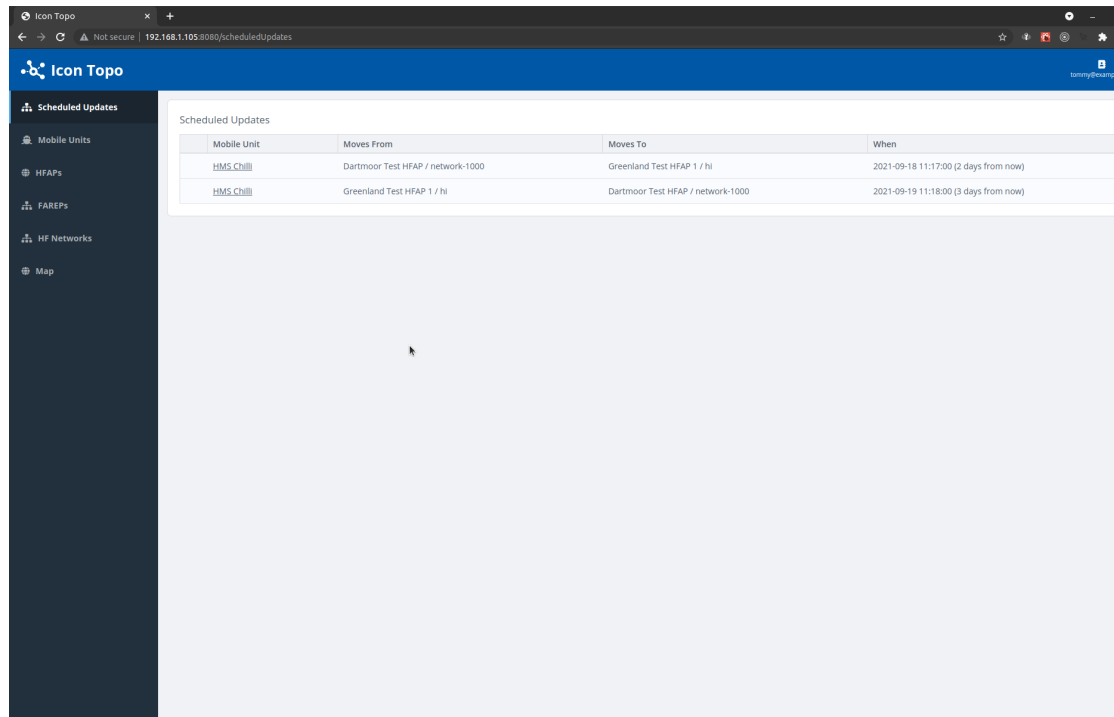
4.2.5 Scheduled Updates Page

The main purpose of Icon Topo is to view and schedule updates to Mobile Unit's Primary HFAP or Network, so when you login to Icon Topo, by default, a list of all upcoming scheduled updates (if any) will appear.

From this page the user can click on the Mobile Unit name in the table to view for more details or make changes to its scheduled updates.

The following screenshot shows the initial screen of the Configuration Service.

Figure 4.18. Configuration Service Initial Screen



4.2.6 Icon Topo Map

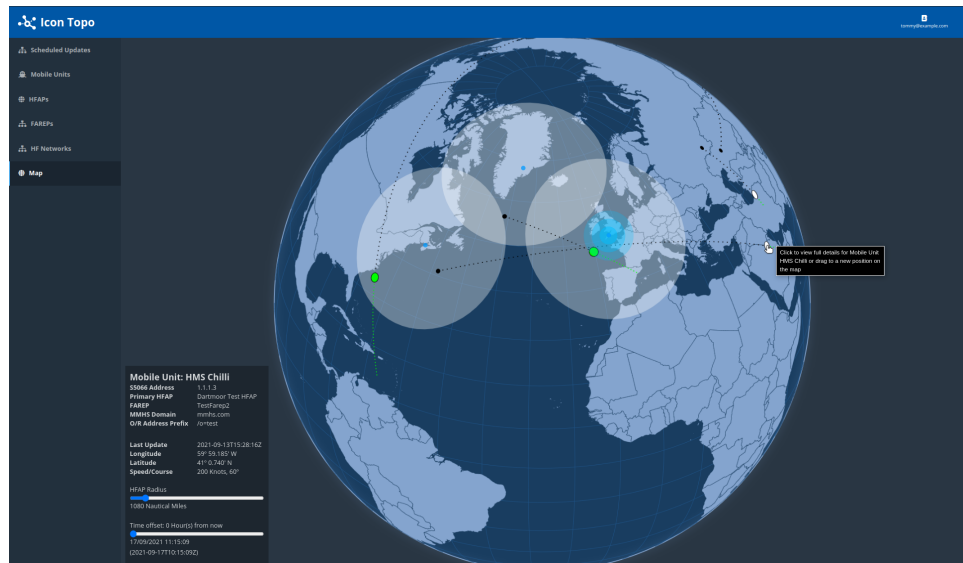
The Map View is accessible from the “Map” option in the Left hand navigation panel.

It can be useful to view all configured Mobile Units and their linked primary HFAPs via this screen, and also allows Operators and Administrators to Schedule Updates.

Administrators may also move Mobile Units.

The following screenshot shows the initial Map View.

Figure 4.19. This shows the Initial Map View



4.2.6.1 Navigating the map:

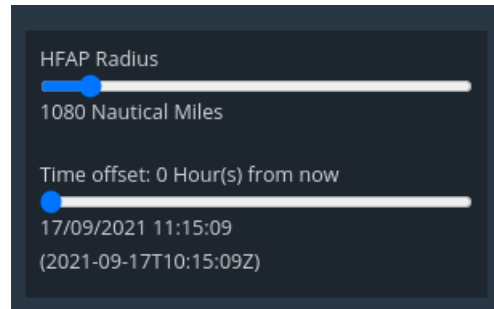
The map view consists of a diagram of the globe. This can be moved around by clicking and dragging any part of the map. The mouse scroll wheel can also be used to zoom in and

out of the map. Changes to the view of the globe will be saved if the user navigates away from the page, or even closes the application.

In the bottom left of the map view there is an info panel as shown in [Figure 4.20, “Map Info Panel”](#). This shows details of any entity currently under the mouse pointer. It also has sliders allowing users to modify the HFAP Radius, and the current time. Sliding the current time slider to the right will adjust the currently viewed time. So Mobile Units will appear to move according to their last reported speed and heading.

The following screenshot shows the Map Info Panel.

Figure 4.20. Map Info Panel



Map Key:

Visible entities are represented by various coloured dots and circles. This key explains what these entities are.

The **small blue circle** represents the location of an HFAP. Any HFAP added to the Configuration Server and which has a Position added by an administrator will be visible on the map. Its area of coverage is represented by the transparent white circle surrounding the blue circle.

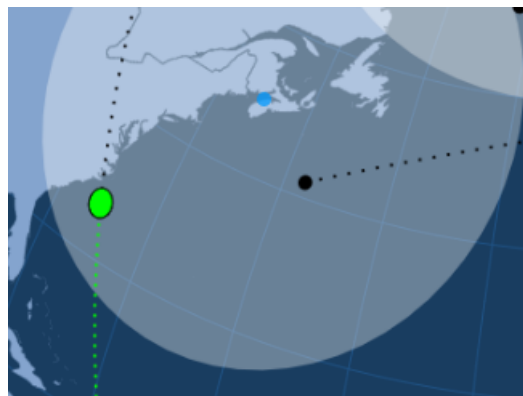
The **green circle** represents the estimated current location of a Mobile Unit. Any Mobile Unit added to the configuration server which has a position, course and speed added by an administrator will be visible on the map. Mobile Units may also appear as white circles if it is currently outside the coverage area of an HFAP.

The **smaller black dot** represents the last reported position of a Mobile unit. With the black dotted line coming away from the black dot representing the last reported direction of the Mobile Unit.

4.2.6.3 Using the Map View

The following screenshot shows the Mobile Unit and HFAP positions.

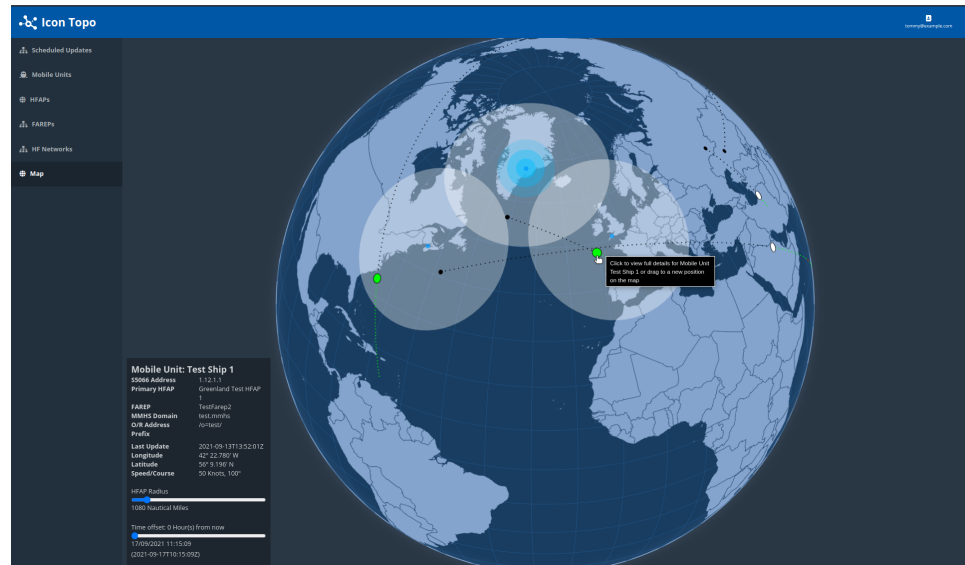
Figure 4.21. Mobile Unit and HFAP positions



When hovering the large green or white dot of a Mobile Unit, the map will display animated blue circles locating its current Primary HFAP.

The following screenshot shows the HFAP and MU connection.

Figure 4.22. HFAP connected to MU



Also note that when using the Time Offset slider in the bottom left of the Map display, the estimated current position of the Mobile Unit should move according to its last reported Speed and Heading.

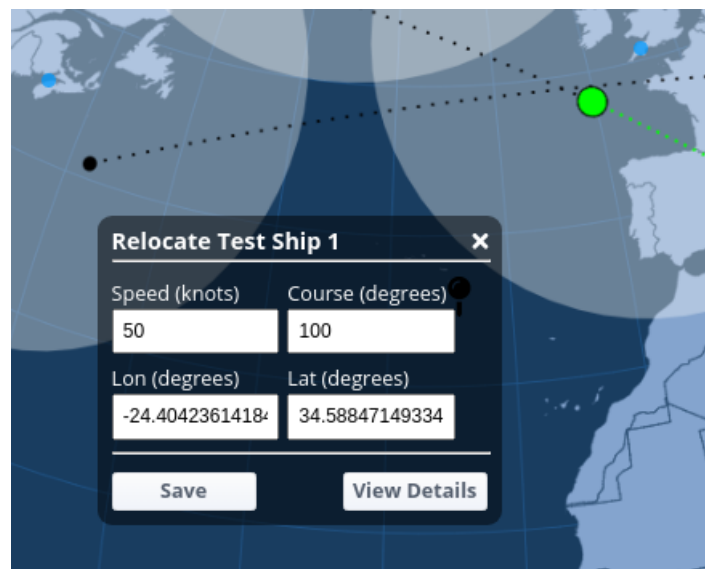
Using the Map View to Move Mobile Unit (Administrator only)

An administrator may use the map to update a Mobile Unit’s last known position, speed or heading.

To do this, ensure that the Offset Time Slider is set to show the current time (ie the slider position is fully dragged to the left). Then click and drag on the Mobile Unit. A pin should appear representing where the Mobile Unit wants to be moved to. Let go of the mouse on the desired location on the map. A “Relocate Mobile Unit” dialogue box will then appear:

The following screenshot shows how to relocate the MU from the Map.

Figure 4.23. Relocate Mobile Unit dialogue box



In the box make any adjustments required for Speed, Course Longitude or Latitude then click Save. Another button allowing the user to go straight to the Mobile Unit's Details page is also available if any other configuration changes are needed.

Once saved the Mobile Unit should reappear at the desired location with its new heading.

4.2.6.4 Using the Map View to Schedule Updates (Operators or Administrators only)

An Operator or Administrator may use the map to aid in scheduling updates to Mobile Units' primary HFAP or HF Network.

1. Find the Mobile Unit on the map.
2. Use the Offset Time slider in the bottom right to forward time and notice and use the map to see when the Mobile Unit arrives inside the radius of the HFAP it needs to switch to.
3. Click on the Mobile Unit and the Mobile Unit's scheduled updates form will appear.
4. Check that the new Primary HFAP and the time of the scheduled update are correct, make any amendments as necessary, and then click submit.
5. The update will be scheduled for the time set. Note that you may only schedule updates for up to 48 hours in the future from the map screen – but this time can be extended to any point in the future from the form itself.

4.3 Server Configuration

The main Icon-Topo configuration file is in `$(ETCDIR)/topo/topoboot.xml`. A minimal example was provided earlier in this chapter. This section describes the full set of configuration options available.

The `topoboot.xml` file contains the configuration for the Icon-Topo processes running on the system i.e. Configuration Server and Update Server.

General options and Configuration options for the Configuration Server follow in this chapter. Configuration options for the Update server are in [Section 5.1, "Update Server Overview"](#).

`topoboot.xml` is an XML file with the outermost element being `<topoboot>`. There are some elements within this, and also subsections with their own elements. These are expressed here as paths.

A more complete example Icon-Topo configuration file is provided below.

4.3.1 Example Topo Configuration File

The following is a more complete example `topoboot.xml` which configures both the Configuration Server and the Update Server

```
<topoboot>
  <servpass:info service="isode.topo"/>
  <db-dsa>
    <ldaphost>ldap://localhost:19389/</ldaphost>
    <root>topoDBName=Topo DB,o=topo</root>
    <sasluser>topo-administrator@example.com</sasluser>
```

```

    <password servpass:encrypt="true">secret</password>
    <saslmech>SCRAM-SHA-1</saslmech>
</db-dsa>
<web>
  <rebaser/>
</web>
<update>
  <switch>
    <mtadname>cn=HFAP/Stornoway,cn=farep,o=messaging</mtadname>
    <ldaphost>ldap://localhost:19389/</ldaphost>
    <sasluser>pp@macmini.local</sasluser>
    <password servpass:encrypt="true">secret</password>
  </switch>
</update>
</topoboot>

```

Note that although the password fields are flagged for encryption, they are not encrypted in this case. On the system where the servpass server isode.topo is set up, the boot file can have its passwords encrypted as described in [Section 4.4, “Configuration of Passwords”](#)

4.3.2 General Configuration

This section describes General Configuration options.

Servpass

/topoboot/servpass:info

Servpass is a mechanism for giving protection to passwords in configuration files. This identifies the servpass information to use.

General

/topoboot/ident

The string used to identify this Icon-Topo instance.

/topoboot/db-schema-file

The name of the file holding the schema information for the database, if this is not the standard file.

4.3.2.1 Icon-Topo DB DSA Connection

/topoboot/dsa-db/ldaphost

The LDAP URL for the DSA

/topoboot/dsa-db/root

The DN of the root entry for the database.

/topoboot/dsa-db/sasluser

The SASL ID to use for access to the DSA. (Overrides */topoboot/dsa-db/root*).

/topoboot/dsa-db/saslmech

The SASL mechanism to use. This must match a mechanism supported by the DSA. If not specified, the LDAP client will select a mechanism from those the DSA supports.

/topoboot/dsa-db/password

The password to use for access. This can be qualified with the attribute value `servpass:encrypt="true"`.

/topoboot/dsa-db/usetsls

If specified, the server will enable TLS to the DSA. This can be used for confidentiality, and is strongly advised if a plain-text password mechanism is to be used.

With no value specified, the client does not pass an identity to the DSA. No value should be specified as `<usetls/>`. To understand how to specify an identity to be passed, e.g. for use with EXTERNAL, see the section on TLS configuration below.

4.3.2.2 TLS Configuration

When fully configured, TLS keys and certificates, including trusted certificates, are held in a security database file. Its default location is `$(ETCDIR)/topo/topo.secdb`. The related parameters are:

/topoboot/security/security-pw

The password for the security database. This is mandatory. As for other passwords, it can be protected using `servpass` by adding to the XML element the attribute `servpass:encrypt="true"`.

/topoboot/security/security-db

The pathname to the security database file, overriding the default pathname. If a relative pathname, it is relative to `$(ETCDIR)`.

At present, the only way of providing a full TLS identity is by loading a PKCS#12 file containing the private key and certificates. The procedure is as follows:

1. Create the folder `$(ETCDIR)/topo/tls`
2. Copy the PKCS#12 file into this folder, naming it `rsa.p12`
3. If the PKCS#12 file needs a passphrase for access, put the value in a file called `rsa.p12.pphr`
4. Set */topoboot/security/security-pw* to a suitable value.
5. Restart the Configuration Server. All being well, the PKCS#12 information will have been loaded and will be used by the web-server interface.
6. When complete, you may delete the folder and its contents.

If you wish the client connections to the DSA to use the loaded identity, use `<usetls>default</usetls>` in the */topoboot/dsa-db* section, or the equivalent items for the update server.

4.3.3 Configuration Server Configuration

This section describes all the configuration options available for the Configuration Server. For Update Server configuration options, see [Section 5.1, "Update Server Overview"](#).

Configuration Server

/topoboot/web/port

Overrides the default port number for the server.

/topoboot/web/source-dir

Overrides the default location of the client files.

/topoboot/web/poll-interval

Overrides the default interval (10s) for checking for updates to the database from other servers.

/topoboot/web/rebaser

If present enables the configuration server to do 'rebasing' of the data.

4.4 Configuration of Passwords

The Icon-Topo configuration file holds passwords used to authenticate to other Isode servers such as M-Vault. To avoid holding such passwords in the clear, the Isode servpass mechanism is used.

It is currently necessary to use command line tools when setting up the `topoboot.xml` file with encrypted passwords. The steps to follow are described below.

- Create the Service Key for the `isode.topo` service. You will need to perform this operation as `root` on Unix platforms.

```
[root@hardie /]# spassmgt set isode.topo root
Passphrase: 1234567890abcABC
Re-enter: 1234567890abcABC
```

The final parameter in the command line above specifies the userid under which the `isode.topo` daemons will run on Unix. Choose a memorable passphrase, which must include a mixture of upper- and lower-case letters and digits.

- You then need to obtain a verifier for the service:

```
[root@hardie /]# spassmgt get isode.topo
AlsuJCfnoNUo
```

- Edit this verifier into your `topoboot.xml` file (the example file shown above already contains this):

```
<servpass:info service="isode.topo" verifier="AlsuJCfnoNUo"/>
```

- Configure the SOM password(s) in the `topoboot.xml` file in the clear:

```
<password servpass:encrypt="true">secret</password>
```

- Then encrypt the passwords held in `topoboot.xml` as follows:

```
spasscrypt -e -x topoboot.xml
```


4.5 Access Control

Different users can be given different access rights. There are four levels:

- Read only: no updates are permitted
- Operator: can update some attributes
- Administrator: can update all attributes and can create and delete entities
- Superuser: can update overall database attributes

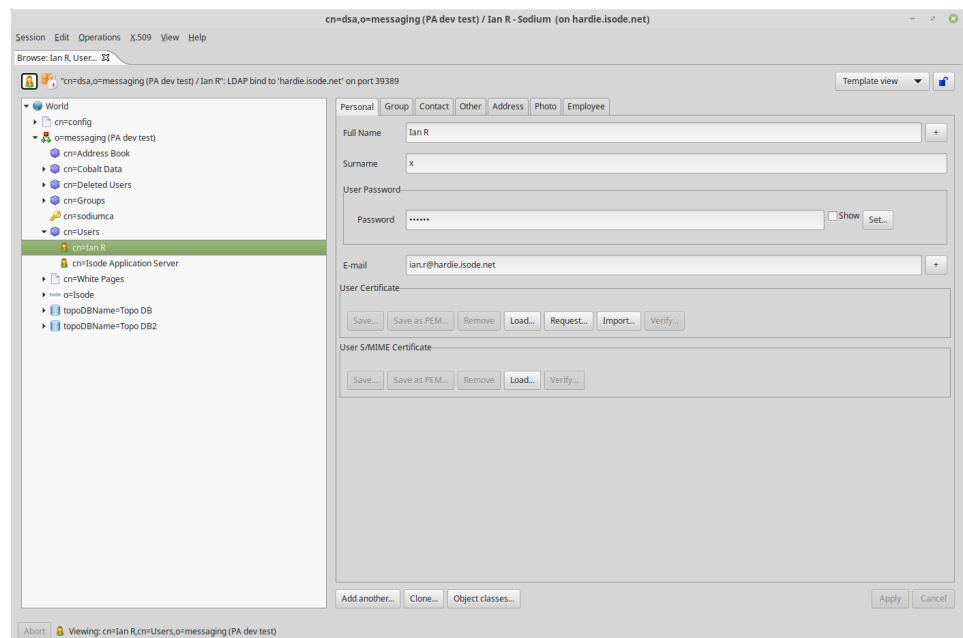
Currently, access control is set by having the DN of the users as one of the values of an attribute in the root entry. There are four such attributes, corresponding to the four access levels. If all of these attributes are absent, then no access control is imposed.

To be able to test this, you need to create several users. Currently the simplest way of managing the access control is to use Sodium.

- Bind to the DSA as the DB user, to ensure that you have modify access to the root entry.
- Find the entry for a given user, and 'copy' the DN value using right-click on the selected entry.
- Find the root entry for the DB.
- Paste the DN value into the appropriate attribute. The Template view has these. Operators are inserted in the `topoUpdateUser` attribute. The other attributes are appropriately named.

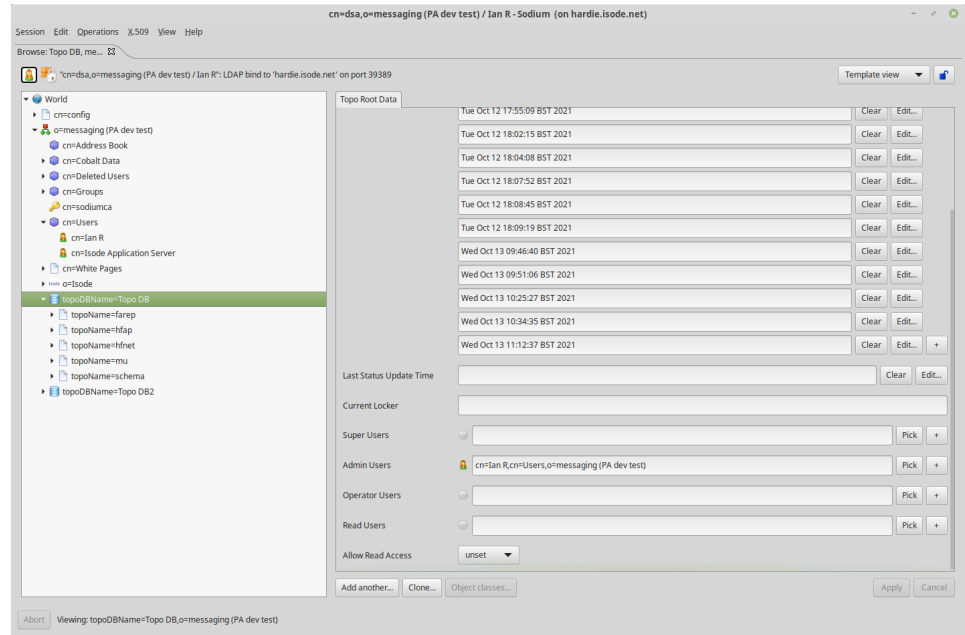
The following screenshot shows Sodium selecting a User to be given suitable ACI.

Figure 4.24. Sodium Selecting Icon-Topo Users



The following screenshot shows Sodium adding the User selected in the previous screenshot above, to the attribute `topoAdminUser` in order to be given suitable ACI.

Figure 4.25. Assign Admin Rights to Icon-Topo User



cn=Ian R,cn=Users,o=messaging (PA dev test)

Chapter 5 Update Server

This chapter describes the Isode Icon-Topo Update Server listing the configuration options available.

5.1 Update Server Overview

The Icon-Topo Update Server is responsible for taking scheduled updates from the Icon-Topo database and updating the appropriate Isode server configuration. Currently M-Switch and M-Link can be managed.

A single Icon-Topo Update Server manages a single M-Switch server and a single M-Link server. The Update Server would normally be located at the same site as the servers which it manages.

5.1.1 Messaging Routing

The messaging services have a general routing architecture. The basic model is that every FAREP can route messages to any MU. MUs and HFAPs perform limited routing, and make use of FAREPs to provide general MU to MU routing. See [Figure 1.1, "MU/HFAP/FAREP Architecture"](#) for the Messaging architecture.

5.1.1.1 Connections

Routing is dependent on connections that are configured. The following connections are configured:

- Every MU is reached via an HFAP for access over HF.
- Every MU is associated with a FAREP. When the MU is reached by 'fast' protocols, e.g. via SATMCOM, the MU is reached via its FAREP rather than an HFAP.
- Every FAREP is connected to every HFAP, and every HFAP is connected to all other HFAPs. This enables traffic for any MU to be sent directly to the correct current HFAP or FAREP
- If two MUs are reached by the same HFAP, then traffic will be passed via that HFAP.

The complete interconnectedness of the FAREPs and HFAPs is needed for MU to MU communication via the shore. When the MU can be reached, e.g. via SATCOM, it is reached via its FAREP.

Not shown in [Figure 1.1, "MU/HFAP/FAREP Architecture"](#) is one of the HFAPs receiving traffic for MUs from two FAREPs.

5.1.1.2 Messaging Routing Architecture

Routing for each of the types of node is as follows:

- HFAP:
 - Each connected MU is routed over the appropriate HF Network,
 - Traffic for an MU reached by another HFAP is sent to that HFAP.
 - Traffic for an MU which is reached via SATCOM is sent to the MU's FAREP.
 - All other traffic is sent to a FAREP.
- MU

- If the MU is reached via HF, all traffic is routed to its primary HFAP.
- If the MU is reached via SATCOM, all traffic is routed to its FAREP.
- FAREP
 - Each MU reached via HF is routed to the primary HFAP.
 - Each MU reached via SATCOM is routed directly if this FAREP is its primary.
 - Each MU reached via SATCOM is routed to its primary FAREP if this FAREP is not its primary.
 - All other traffic falls back to default routing. This routing is configured in the application outside of Icon-Topo

5.2 Overview of Configuring the Update Server

Configuration of a deployment of Isode servers by Icon-Topo is held in 3 places:

topoboot.xml

The main Icon-Topo config file as introduced in [Section 3.2, “Topo Configuration Overview”](#).

An HFAP or MU require the use of an Icon-5066 server, or servers. These need to be configured in *topoboot.xml* as described below.

Application Configuration

In this version of Icon-Topo is able to reflect changes in the location of `Mobile Units` in the M-Link configuration held internally in the server itself and in the M-Switch configuration held in M-Vault. In the future, other Isode applications will be able to be updated.

Each application will need some configuration, not made using Icon-Topo, for it to work within the control of Icon-Topo. However, those parts of the application's configuration which are managed by Icon-Topo should not be altered through the application's own configuration interface.

Icon-Topo Configuration

The Icon-Topo Configuration Server is updated using the Browser User Interface as described in [Section 4.2, “Using the Configuration Service”](#). This is held in M-Vault, which can be the same as that holding the Application Configuration or a separate DSA.

5.3 General Configuration of the Update Server

The Update Server shares with the Configuration Server these parts of *topoboot.xml*:

- The top-level items: `/topoboot/ident` (required), `/topoboot/db-sechema-file` and `/topoboot/servpass:info`,
- The `/topoboot/db-dsa` section. This is required.
- Any `/topoboot/security` section.

The configuration items specific to the Update Server are in the section */topoboot/update* section. This contains these items:

type

One of *farep*, *hfap* or *mu* corresponding to the type of the node the update server is controlling

name

The name of the node in the Icon-Topo database.

There is a sub-section for the STANAG 5066 servers and a sub-section for each application.

5.3.1 STANAG 5066 Server Configuration

A Mobile Unit will have one S5066 server which is used for communication with HFAPs. Which HF-net this accesses will depend upon the current primary HFAP and the network at that site.

An HFAP will have one or more HF-Nets for communication with Mobile Units. Each will be fixed in normal operation.

A FAREP does not have S5066 servers.

The local S5066 servers are configured using items in the */topoboot/update/s5066* section. This contains a */topoboot/update/s5066/server* section for each S5066 server. These section can contain the following items:

name

A name for the S5066 server

hfnet

The name of the HF-net to which this server connects. This is required for an S5066 server in an HFAP.

hostname

The hostname to be used to connect to the S5066 server. An IP address can also be used. This is required.

port

The number of the TCP port to be used for the server. If omitted, the value 5066 is assumed.

shore

This item is used for a Mobile Unit to indicate which S5066 server is used for the shore traffic. The value is not used, and this can be entered as *<shore/>*

local

This item is used for an HFAP to indicate that this S5066 server is used for Icon-Topo controlled use. The value is not used, and this can be entered as *<local/>*

There may be S5066 servers which are not directly used by the Icon-Topo system. At an HFAP, there should be one S5066 server for each HF-net in the Icon-Topo configuration for that HFAP. You must ensure that the names match.

The M-Switch configuration also contains S5066 server configuration information. These servers are associated with the Icon-Topo configuration by using the hostname and port number. It is therefore important to ensure that the hostname, in particular, is used in the same form in each place.

5.4 M-Switch and the Update Server

This section describes the configuration requirements for M-Switch if it is to be used with Icon-Topo. It also describes how Icon-Topo is to be configured to work with M-Switch

Mconsole indicates which items in the configuration have been created by Icon-Topo.

5.4.1 M-Switch Configuration

The type of messaging configuration and MTA needed to work with Icon-Topo is 'military'. This will provide the different facilities required.

5.4.1.1 S5066 Servers

An HFAP will need one S5066 server for each HF-net to be used for Icon-Topo protocols. Each server should have a hostname and port number which match an entry in the *topoboot.xml* configuration. The S5066 server will then be used to communicate over the corresponding HF-net.

If an HFAP's M-Switch configuration has S5066 servers not used for Icon-Topo controlled routes, these should be included in the */topoboot/update/s5066* section and marked with the flag *<local/>*. This is so that the Update Server can correlate all the S5066 servers between the M-Switch configuration and its configuration.

An MU will need one S5066 server for communication with the shore. Its hostname and port should match those in the 'shore' S5066 server in *topoboot.xml*

A FAREP does not use S5066 and so requires no such servers.

5.4.1.2 ACP 142 Configuration

The Icon-Topo managed use of ACP 142 splits the traffic, so that the traffic using MULE - SMTP content over ACP 142 - and that using STANAG 4406E - X400 content over ACP 142. This is done by using a different S5066 end point called a SAP. The result of this is that M-Switch needs a separate ACP142 channel for MULE and for S4406E for each HF-net it supports. An HFAP with three HF-nets will need a total of six ACP 142 channels.

First create the required S5066 servers - one for each HF-net. Then create the required ACP 142 channels by cloning. It is suggested that the names given to the channels should be of the form:

```
acp142-s4406e-<hfnetid>
acp142-mule-<hfnetid>
```

1. Clone the *acp142* channel for the first S4406E channel, named, e.g., *acp142-s4406e-hfnet1*
2. Change this to use S5066, and set the S5066 server and other information.
3. Clone this new channel for the first MULE channel, e.g. *acp142-mule-hfnet1*.
4. For this MULE channel, in the AC142 advanced tab change the S5066 SAP to use to the value 7. In the main Advanced tab, edit the content out value to remove the X400 content types (those not starting '822').

5. For the S4406E channel, remove from the content out value the SMTP content types - those with names starting '822').
6. For an HFAP with more than one HF-net, clone both the first s4406e and mule channels for each additional HF-net (e.g. as *acp142-x4406e-hfnet2* and *acp142-mule-hfnet2* etc.).
7. In each of these, change the S5066 server to be used to be that for the appropriate HF-net. Other values remain the same.
8. You are advised to delete the original *acp142* channel.

5.4.1.3 ACP 127 Configuration

Icon-Topo can control the use of ACP 127 Broadcast from an HFAP. This is used, in particular, to send to Mobile Units which do not support ACP 142.

An HFAP can have more than one ACP 127 Broadcast circuit. Icon-Topo controls which circuit is to be used for a MU by assigning the MU's Routing Indicator to that circuit. It is also possible for the MU to be reached by several such broadcast circuits, with the selection of which is used being made on some other basis, such as the security label on the message.

The broadcast circuits are set up as described in the M-Switch manual. Then the names chosen for these circuits should be set in the HFAP's configuration in Icon-Topo.

It is also possible to send ACP127 traffic between HFAPs. This enables traffic between MUs which only support ACP 127 to be transferred without tunnelling in SMTP or X400. Once the external MTA for the peer HFAP has been created by Icon-Topo, create an *acp127* channel in this external MTA, and then the corresponding circuit for the *acp127* channel.

5.4.1.4 Routing Configuration

Icon-Topo creates the required routing configuration for the addresses associated with MUs, HFAPs and FAREPs in the Icon-Topo Database. Mconsole indicates that Icon-Topo manages these configuration items.

Addresses external to the FAREP, HFAP and MU network need to be explicitly configured. In an HFAP or MU Icon-Topo will create a routing nexus called *Default*. For a MU, this sends external traffic down the correct route, depending upon the MU's current state. For an HFAP, the default route sends to the FAREPs for outward routing. The simplest way of handling external routing in these systems is to configure the Routing Tree Root to send using this Default nexus. You may chose, however, not to do this and restrict routing to the Default nexus to known, valid address spaces.

In a FAREP, external addresses need to be manually configured for their routing. This depends upon the local circumstances. It might be the case that the FAREPs also function as gateways to different external networks. This should use the inter-FAREP external MTAs which are created by Icon-Topo.

5.4.2 Update Server Configuration for M-Switch

The Update Server needs to be configured:

- to connect to the DSA where the M-Switch configuration is held, in order to make changes to that configuration
- to connect to the M-Switch Queue Manager, to inform the running system that changes have been made, and to re-route any queued messages affected by these changes.

The configuration is held in the section */topoboot/update/switch*:

/topoboot/update/switch/mtadname

This is the directory name of the Switch in the configuration DSA. It should match the value of *<mtadname>* in the *mtaboot.xml* file for the M-Switch.

/topoboot/update/switch/ldaphost

The LDAP URL for the DSA containing the M-Switch configuration. The host and port should match those used in *mtaboot.xml*.

/topoboot/update/switch/sasluser

The SASL ID to use to bind to the DSA. If not specified, the value of */topoboot/db-dsa/sasluser* will be used.

/topoboot/update/switch/password

This is the password for the bind. It can be encrypted as for other password values. If not set, the value of */topoboot/db-dsa/password* will be used.

/topoboot/update/switch/saslmech

The SASL mechanism to use. If not specified, then a mechanism offered by the DSA will be used.

/topoboot/update/switch/usetls

Configures the use of TLS with the DSA. See */topoboot/db-dsa/usetls* for more details.

/topoboot/update/switch/qmgrhost

The hostname for the Queue Manager

/topoboot/update/switch/qmgrport

The port number for the Queue Manager. If omitted, the default port of 18001 is assumed.

/topoboot/update/switch/qmgruser

The SASL ID used for connecting to the Queue Manager. If this is omitted, then the SASL ID used for the configuration DSA is used.

/topoboot/update/switch/qmgrpassword

The password for used accessing the Queue Manager. It can be encrypted as for other password values. If omitted, the password used when accessing the configuration DSA is used.

/topoboot/update/switch/qmgrusetls

Configures the use of TLS with the Queue Manager. See */topoboot/db-dsa/usetls* for how more details.

5.5 M-Link and the Update Server

M-Link servers are used to communicate XMPP traffic between external XMPP domains and M-Link servers on Mobile Units. M-Link MU Gateway is required to support the necessary protocols. XMPP domains which are may be associated with a FAREP or HFAP are not associated with this XMPP network.

HFAPs communicate with MUs using the SIS Layer Extension Protocol (SLEP) over STANAG 5066 for HF connections.

FAREPs and HFAPs communicate with each other uses X2X links. When using SATCOM or another fast link, the MU and its associated FAREP also use X2X links. An M-Link server requires that it listens on a unique TCP port for each X2X peer M-Link server. With Icon-Topo, this is achieved by each M-Link connecting to its peers by calling its configured XMPP port, and listening on the XMPP port of each of its peers.

Traffic from an MU to external domains is sent via the M-Link server at its associated FAREP. This is the external access point for the MU's XMPP domain. Current limitations mean that only standard server-to-server protocols can be used with external domains.

Not all MUs are required to support XMPP. However, unless there are no MUs which support it, XMPP support needs to be enabled in all FAREPs and HFAPs.

5.5.1 M-Link Configuration

The M-Link Administration Guide has details on the configuration for and by Icon-Topo in "Appendix A - Integration with Icon-Topo". There you will find how to:

- Enable the interface which Icon-Topo will use to update the M-link configuration.
- Obtain the Access Token needed for the Update Server to be allowed to perform the updates.

5.5.2 Update Server Configuration for M-Link

The Update Server configuration for M-Link is held in a section `/topoboot/update/mlink`:

`/topoboot/update/mlink/url`

The full URL for the Update Server to send updates to M-Link. This will normally have this value with the appropriate hostname:

```
https://hostname:5221/api/topo
```

`/topoboot/update/mlink/access-token`

The string access token obtained from M-Link.

`/topoboot/update/mlink/file`

This enables debugging of the information sent from the Update Server to M-Link. If a filename is specified, the JSON for each operation is appended to this single file, with a date/time stamp. If the filename is a relative path, then this is taken relative to the logging directory. If the value is empty, specified by `<file> </file>`, then each JSON block is written to a separate file in the logging directory.

If this is specified, `/topoboot/update/mlink/url` need not be specified, and no attempt will be made to update M-Link.

5.6 Update Server Configuration Options Example topoboot.xml

An example configuration file is provided below, and is also provided in the installed pkgs for reference

```
<topoboot>
<db-dsa>
<ldaphost>ldap://localhost:39389/</ldaphost>
<root>topoDBName=Topo DB,o=Isode,o=messaging</root>
<sasluser>topo.admin@hardie.isode.net</sasluser>
<password>secret</password>
<saslmech>SCRAM-SHA-1</saslmech>
</db-dsa>
<web>
<rebaser/>
</web>
<update>
<type>hfap</type>
<!-- NB this value must match the HFAP name
```

```

in the Topo configuration -->
<name>hardie.isode.net</name>

<!-- S5066 Servers -->
<s5066>
<server>
<name>NorthernEurope</name>
<!-- This value must match the name of a local HF-Net -->
<hfnet>NorthernEurope</hfnet>
<hostname>hardie2.isode.net</hostname>
<port>5067</port>
</server>
<server>
<name>SoutheastEngland</name>
<!-- This value must match the name of a local HF-Net -->
<hfnet>SoutheastEngland</hfnet>
<!-- NB these values must match the 5066 Server
in the M-Switch config -->
<hostname>hardie.isode.net</hostname>
<port>5066</port>
</server>
</s5066>

<!-- M-Switch Configuration -->
<switch>
<!-- NB this value must match the MTA DN in mtaboot.xml -->
<mtadname>cn=hardie.isode.net,cn=Messaging Configuration,
o=Isode,o=messaging</mtadname>
<ldaphost>ldap://localhost:39389/</ldaphost>
<sasluser>topo.admin@hardie.isode.net</sasluser>
<password>secret</password>
<qmgrhost>hardie.isode.net</qmgrhost>
<qmgruser>topo.admin@hardie.isode.net</qmgruser>
<qmgrpassword>secret</qmgrpassword>
<qmgrmech>SCRAM-SHA-1</qmgrmech>
</switch>

<!-- M-Link Configuration -->
<mlink>
<file></file>
<url>https://localhost:5221/api/topo</url>
<access-token>fC+zhYpksr+vWrbtJ4qU0vyjyUWxb7yUdXGH</access-token>
</mlink>
</update>
</topoboot>

```