Isode

Role Configuration: Cobalt & Harrier

Configuring Harrier (Isode's web based Military Messaging Client) to offer "Roles" to a User, using Cobalt (Isode's tool for provisioning users and roles in an LDAP directory).

Contents

Introduction

This guide describes how to configure Harrier (releases 3.0 and onwards) to offer 'Roles' to a User when logging in. The process described uses Harrier 3.0 together with the R18.0v5 releases of M-Switch, M-Box & M-Vault.

R18.0v5 or later Isode releases are required for Cobalt.

Prerequisites

This guide assumes you already have a working Harrier installation, such as the one installed as part of the Harrier Military Messaging Client evaluation available from *https://www.isode.com/evaluate/evaluate-email.html#harrier*.

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 access to the Self-Service Portal for 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. In addition to the server platforms listed, we support the use of Isode server products on Windows 10 for simple evaluations and demonstrations.

Isode supports the use of the latest versions of Google Chrome, Mozilla Firefox and Microsoft Edge browsers with the Harrier web client. Internet Explorer is not supported.

Product Download

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 Evaluation page.

Product Activation

The Cobalt installation process will lead to the Cobalt server running on port *8001* with access from a Web browser. The HTTP URL for accessing from a local system will be *https://localhost:8001*.

The server will bootstrap itself with an auto generated certificate to offer HTTPS services. The browsers will display the page as insecure and give an option to add security exception. You will be able to set it up with a certificate trusted by the browsers and issued by trusted *CA* later (see Section 2.2.2 of the Cobalt Administration Guide available from *https://www.isode.com/support/help.html*

Your first interaction with Cobalt will be Product Activation. Cobalt requires a valid Product Activation Key from Isode before it will run correctly. For instructions on applying for and requesting a Product Activation Key, see Section 2.1.1 of the Cobalt Administration Guide.

Configuration Changes

Harrier

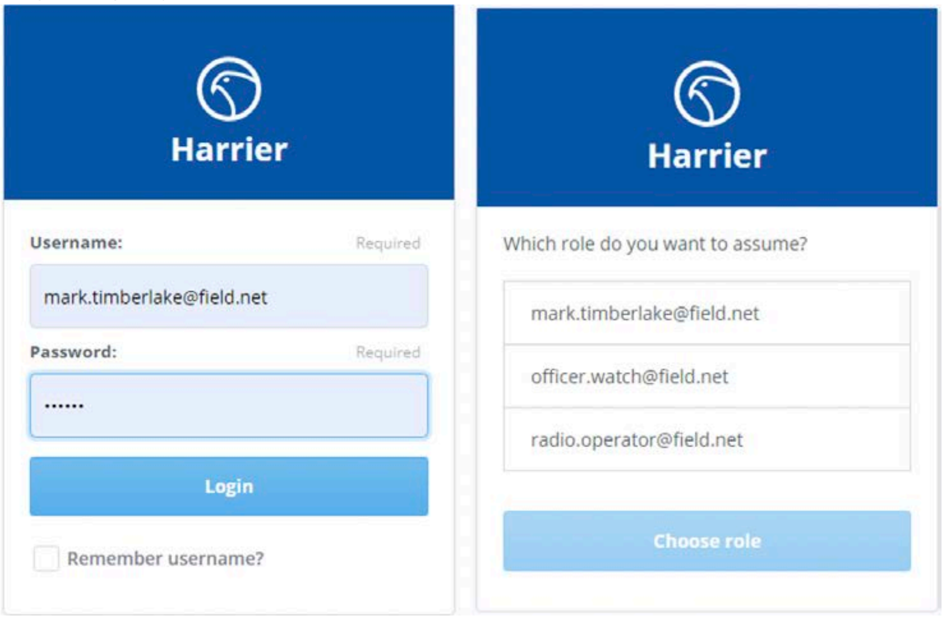
The following lines (in red) need to be added to the “harrier_web_conf.cml”file in the domain section. This file is located in “C:\Isode\Harrier\etc” on Windows systems and “/etc/isode/harrier/” on Linux systems.

```
    <domain name="field.net">
            <imap_url>imap://NEW-FIELD:143</imap_url>
            <smtp_url>smtp://NEW-FIELD:587</smtp_url>
            <ldap_url>ldap://NEW-FIELD:19389</ldap_url>
            <mode>military</mode>

<sio_catalog>$(harrier.dir.etc_or_share)/label_catalog.xml</sio_catalog>
            <sio_policy>$(harrier.dir.etc_or_share)/policy.xml</sio_policy>
<ldap_group_base_filter>(&amp;(objectclass=inetOrgRole)(roleOccupant=$(user.dn
)))</ldap_group_base_filter>
            <ldap_group_id_at>mail</ldap_group_id_at>
            <ldap_group_search>true</ldap_group_search>
            <ldap_group_base_dn>o=New FIELD</ldap_group_base_dn>
            <role_self>true</role_self>
        </domain>
```

The last tag (role_self) is optional, it allows the user to login as themselves as well as their roles, as shown in Image 1.

Image 1: Login Options



Username: Required

mark.timberlake@field.net

Password: Required

••••••

Which role do you want to assume?

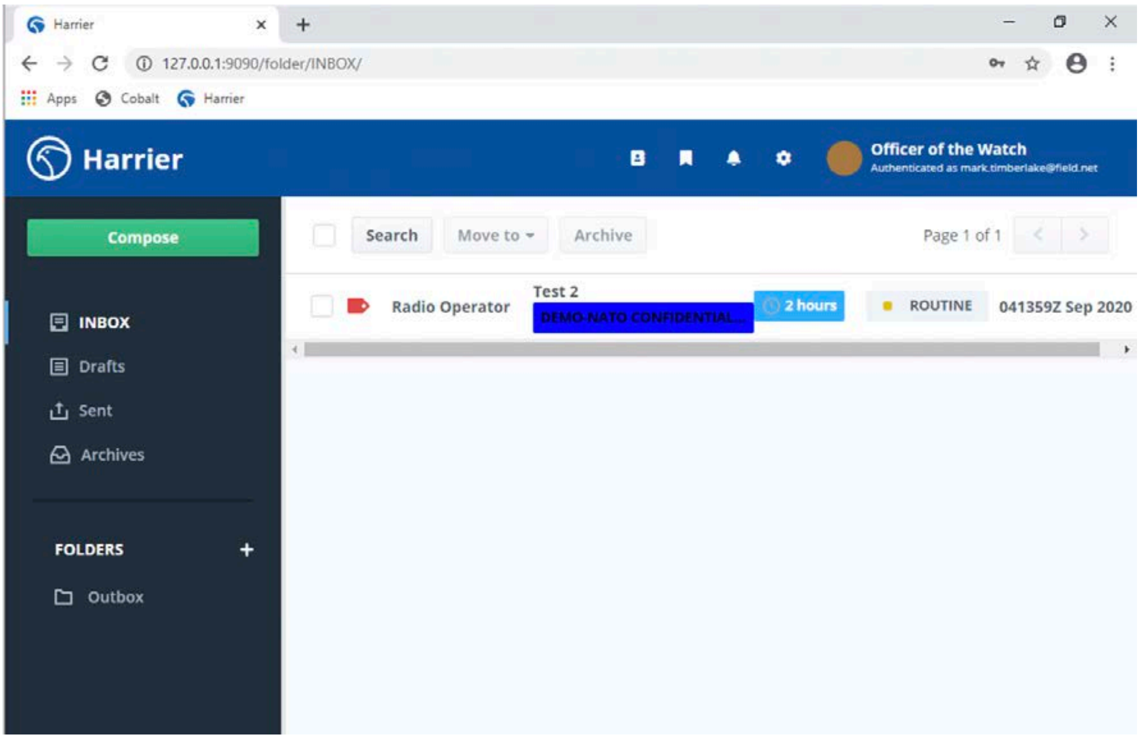
mark.timberlake@field.net

officer.watch@field.net

radio.operator@field.net

When logged in as a Role your initial screen will be similar to the that shown in Image 2.

IMAGE 2: Harrier Inbox



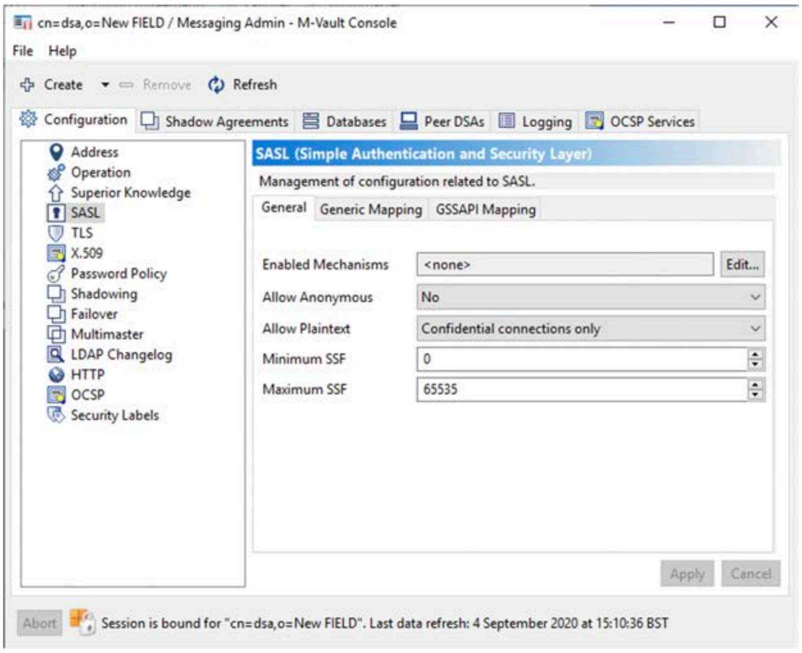
Officer of the Watch
Authenticated as mark.timberlake@field.net

Radio Operator	Test 2 DEMO NATO CONFIDENTIAL...	2 hours	ROUTINE	041359Z Sep 2020

M-Vault SASL Configuration

By default, M-Vault has no SASL configuration, but Harrier Web requires this for using Roles. So start M-Vault Console and navigate to the SASL Configuration (Image 3) then click on [**Edit**] next to the Enabled Mechanisms field.

Image 3: M-Vault Console SASL Configuration



SASL (Simple Authentication and Security Layer)

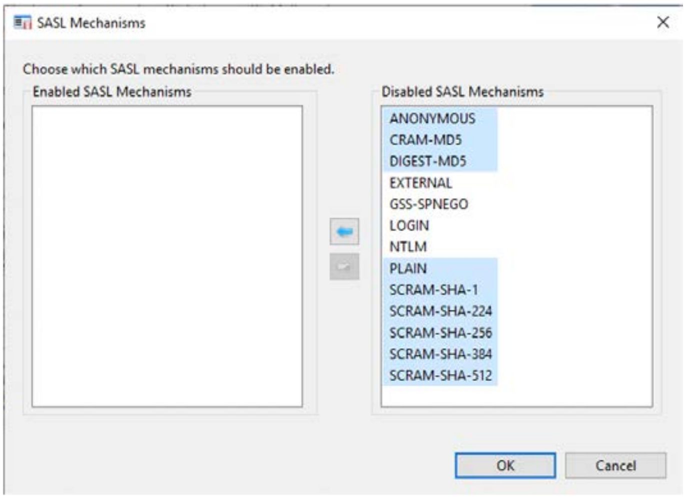
Management of configuration related to SASL.

Enabled Mechanisms	<none>
Allow Anonymous	No
Allow Plaintext	Confidential connections only
Minimum SSF	0
Maximum SSF	65535

Session is bound for "cn=dsa,o=New FIELD". Last data refresh: 4 September 2020 at 15:10:36 BST

From the right-hand pane (Image 4) select ANONYMOUS, CRAM-MD5, DIGEST-MD5, PLAIN and all the SCRAM-SHA-xxx mechanisms, then click the blue Left Arrow (Image 5).

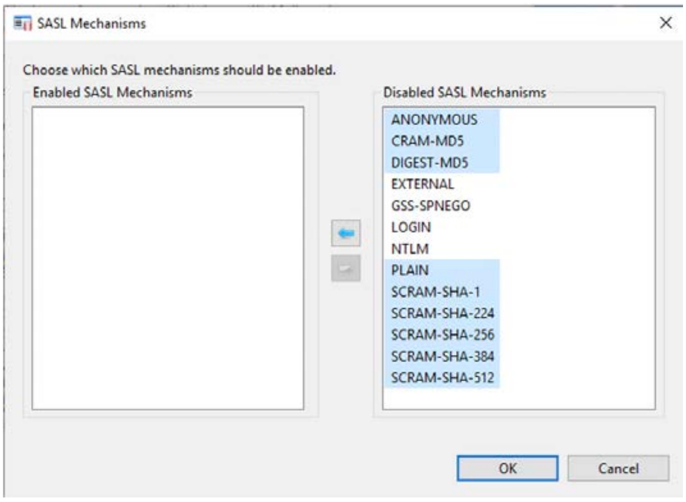
Image 4: Select Mechanisms



Choose which SASL mechanisms should be enabled.

ANONYMOUS
CRAM-MD5
DIGEST-MD5
EXTERNAL
GSS-SPNEGO
LOGIN
NTLM
PLAIN
SCRAM-SHA-1
SCRAM-SHA-224
SCRAM-SHA-256
SCRAM-SHA-384
SCRAM-SHA-512

Image 5: Confirm Mechanisms



Choose which SASL mechanisms should be enabled.

ANONYMOUS
CRAM-MD5
DIGEST-MD5
EXTERNAL
GSS-SPNEGO
LOGIN
NTLM
PLAIN
SCRAM-SHA-1
SCRAM-SHA-224
SCRAM-SHA-256
SCRAM-SHA-384
SCRAM-SHA-512

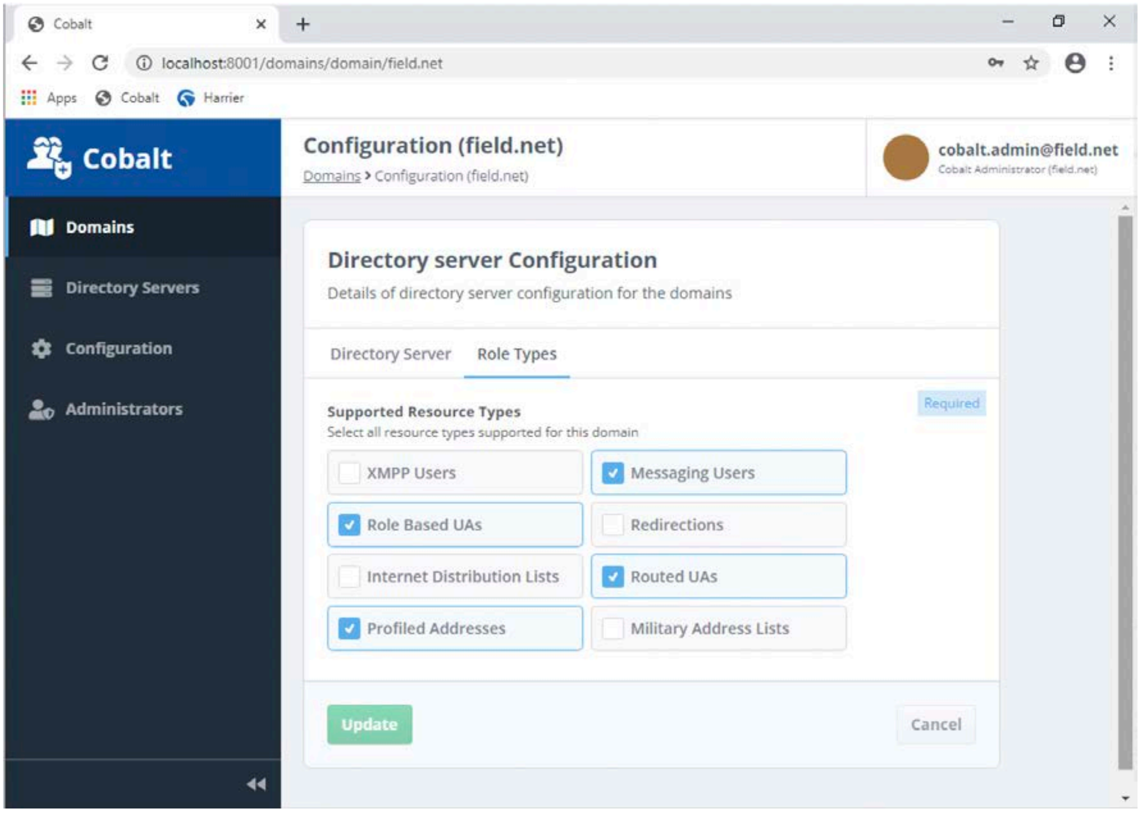
Now click [**OK**] to complete.

Back in the main M-Vault Console screen (as in Image 3) click on the now highlighted [**Apply**] button. This completes the M-Vault configuration but as a good measure it is probably best to restart the M-Vault Server.

Configuring Users and Roles in Cobalt

Login to Cobalt as Cobalt Administrator and ensure that the domain has as a minimum the following “Role Types”; “Messaging Users” and “Role Based UAs” available. You may, as in Image 6, want additional “Role Types”.

Image 6



Directory server Configuration

Details of directory server configuration for the domains

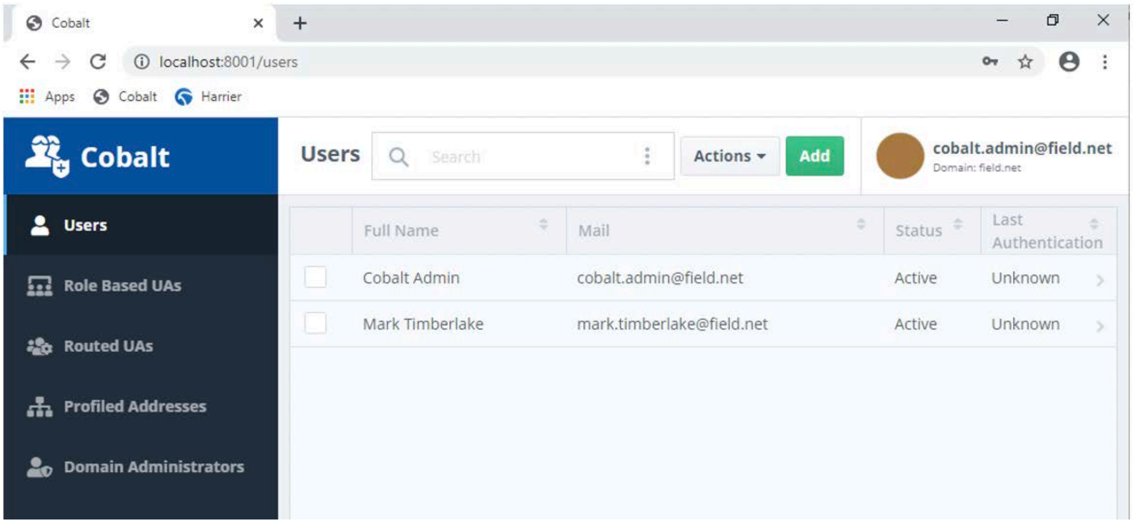
Supported Resource Types

Select all resource types supported for this domain

□ XMPP Users	☑ Messaging Users
☑ Role Based UAs	□ Redirections
□ Internet Distribution Lists	☑ Routed UAs
☑ Profiled Addresses	□ Military Address Lists

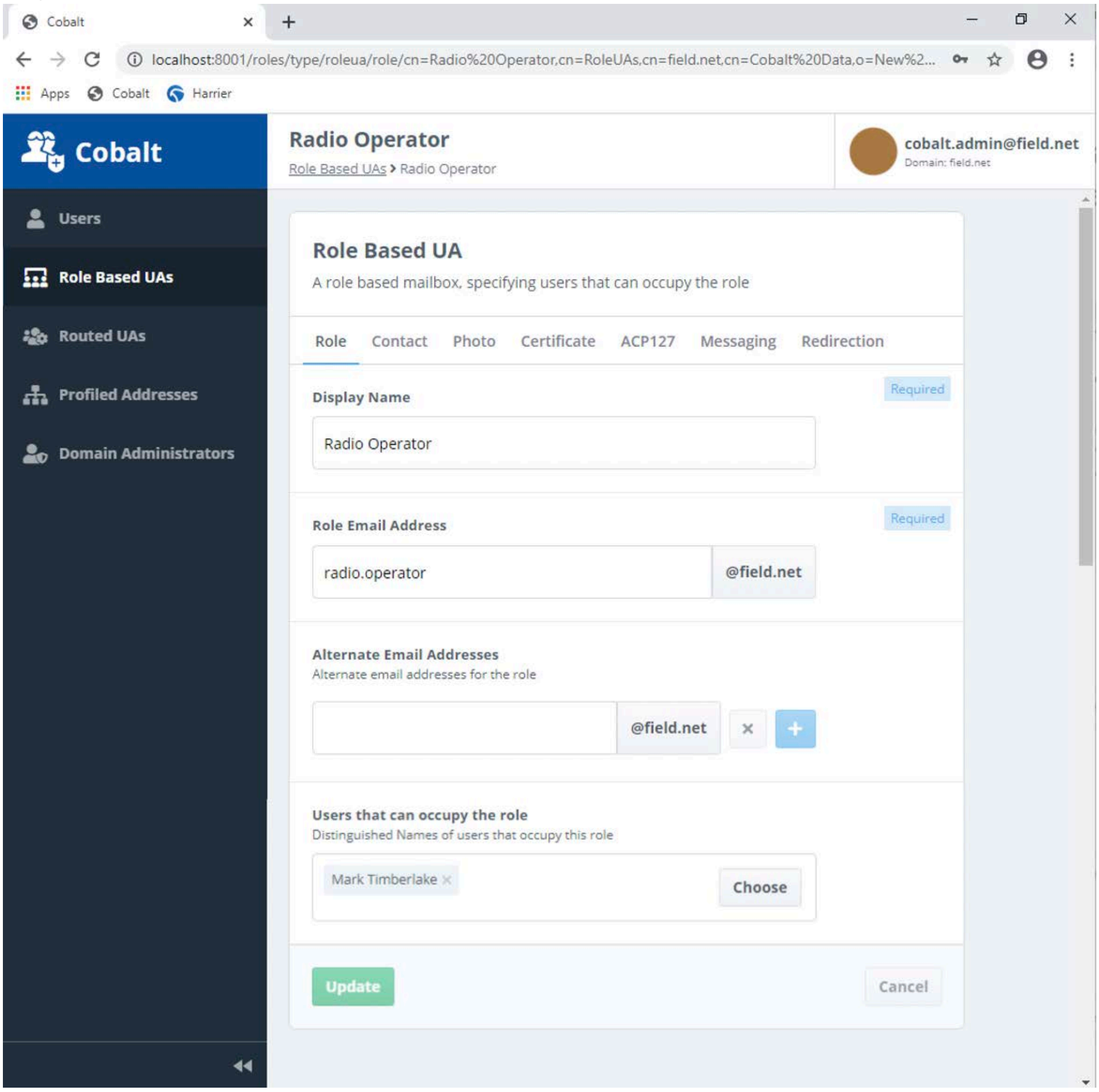
Logout as the Cobalt Administrator and login as an Administrator that has the rights to “Manage Everything” in the domain. Now create a User, in Image 7 this is the user “Mark Timberlake), then select [**Role Based UAs**] to create a Role (such as the Radio Operator role shown in Image 8.

Image 7



	Full Name	Mail	Status	Last Authentication
□	Cobalt Admin	cobalt.admin@field.net	Active	Unknown
□	Mark Timberlake	mark.timberlake@field.net	Active	Unknown

Image 8



Radio Operator

Role Based UAs > Radio Operator

Role Based UA

A role based mailbox, specifying users that can occupy the role

Display Name: Radio Operator

Role Email Address: radio.operator @field.net

Alternate Email Addresses

Alternate email addresses for the role

@field.net

Users that can occupy the role

Distinguished Names of users that occupy this role

Mark Timberlake ×

In the “Users that can occupy the role” field use the [Choose] button to select Users, multiple Users can be selected.

You are now ready to work with Cobalt.

What Next?

More information on Cobalt can be found on the Isode website at *https://www.isode.com/products/cobalt.html*.

Detailed configuration and operational information on Cobalt can be found in the Administration Guide available from the Isode website at *https://www.isode.com/support/help.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