HARRIERWEB-4.0

Harrier Web Server Administration Guide

Isode

Table of Contents

1 Software version

This guide is published in support of Isode Harrier Web R4.0. 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 Harrier Web, a server application which provides a web-browser interface for clients wishing to use Military Messaging or Internet Mail.

3 Related publications

A separate guide is published for Users of the Harrier client in order to send and receive messages. See the Harrier Web Server User's Guide.

Related topics are discussed in the volumes of the Isode documentation set for other servers which are listed below.

Volume	Title
SWADM	*M-Switch Administration Guide*
SWAAG	*M-Switch Advanced Administration Guide*
SWOPG	*M-Switch Operators Guide*
VAUADM	*M-Vault Administration Guide*
MBOXADM	*M-Box Administration Guide*

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	*isoentities*
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.

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
(BINDIR)	Programs run by users.	*C:\Program Files\Isode \Harrier\bin*	*/opt/isode/bin*
(CACHEDIR)	Cache files.	*C:\Isode\Harrier\cache*	*/var/cache/isode/harrier*
(CLIENTDIR)	Default Harrier client files	*C:\Program Files\Isode \Harrier\share\webapps \harrier*	*/opt/isode/share/webapps/ harrier*
(DATADIR)	Storing local data.	*C:\Isode\Harrier*	*/var/isode/harrier*
(ETCDIR)	System-specific configuration files.	*C:\Isode\Harrier\etc*	*/etc/isode/harrier*
(LIBDIR)	Libraries.	*C:\Program Files\Isode \Harrier\bin*	*/opt/isode/harrier/lib*
(LOGDIR)	Log files.	*C:\Isode\Harrier\log*	*/var/log/isode/harrier*
(SBINDIR)	Programs run by the system administrators.	*C:\Program Files\Isode \Harrier\bin*	*/opt/isode/sbin*
(SHAREDIR)	Configuration files that may be shared between systems. Common data and documentation files.	*C:\Program Files\Isode \Harrier\share*	*/opt/isode/share*
(TMPDIR)	Temporary files.	*C:\Isode\Harrier\tmp*	*/var/tmp/isode/harrier*

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: customer-service@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 licensing 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.

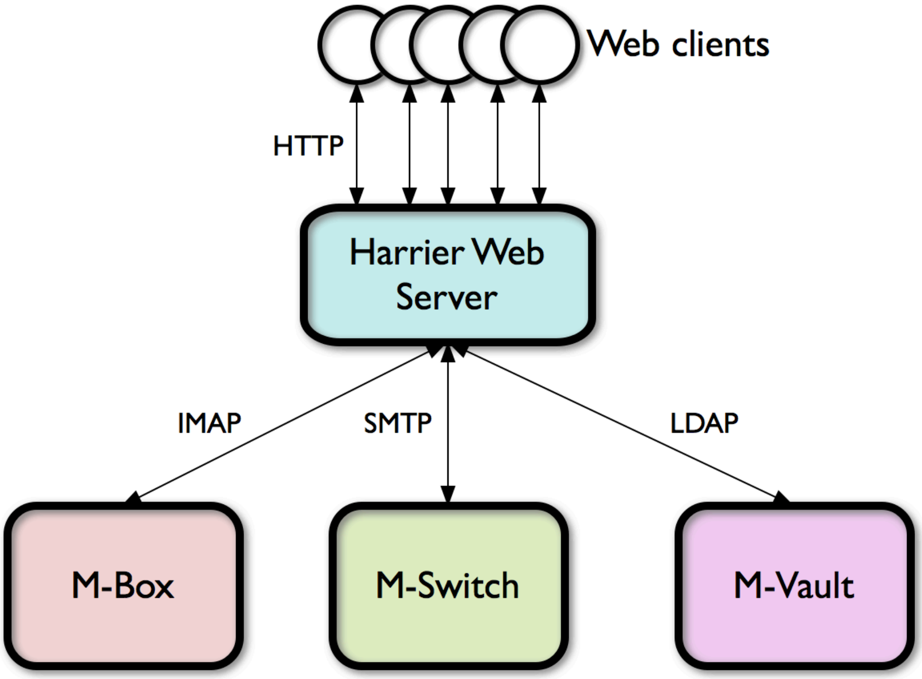
Chapter 1 Introduction to Harrier Web

This section introduces Harrier Web server and talks about how its configuration is stored.

1.1 Overview

The Isode Web Email server, Harrier, provides a zero-footprint web mail client that allows users to access email. Harrier Web Server uses standards-based technologies including HTTP, IMAP, SMTP and LDAP

Figure 1.1. Web clients accessing mail via Harrier Web Server



The Harrier Web Server establishes connections to IMAP, SMTP and LDAP servers on behalf of individual users, who need only supply a single set of login credentials in order to be able to send and read email, and to access an address book.

The Cobalt web application can be used for provisioning users, roles and organizations in an LDAP directory. In particular, Cobalt supports management of users, roles, organizations, distribution lists, per user S/MIME settings and per organization Draft & Release policies.

Chapter 2 Configuration

This section describes configuration of Harrier Web Server.

This section also provides basic information about services included in Harrier Web Server and describes how to start/stop Harrier Web Server services.

2.1 Configuration file

By default Harrier Web Server reads its configuration from *(ETCDIR)/ harrier_web_conf.xml*.

Config file used by Harrier instance can be changed using '-f' or '--config' option.

Harrier Manager application provides an easy and convenient way for editing configuration.

2.2 Runtime user

On UNIX systems, you should create a runtime user (for example using **useradd** on Linux) to be used for the Harrier Web Server. The name of this user is then set in the configuration file (see **Runtime user**).

2.3 Installing an Isode activation file

In order to create or start a Harrier instance on a host system, the activation file for the respective product is required.

Isode MAS web application manages activation keys on a host system. Each system hosting a product component will have its own set of activation files.

Alternatively, the activation file can be installed manually or generated using Section 2.7, “Product Activation Mode”.

Questions regarding licensing/activation should be directed to support@isode.com.

2.4 Starting and stopping Harrier

2.4.1 Harrier process

Harrier includes a single process isode.harrierwebserver. Subsequent references will use a shortened form "harrierwebserver". This section summarizes installation of Harrier service and how to start it on different platforms.

2.4.2 Starting/stopping Harrier on Linux

On Linux Harrier Web Server is managed as any regular daemon using systemd commands

- To start Harrier run: **sudo systemctl start harrier**
- To stop it run: **sudo systemctl stop harrier**
- To check if Harrier server is running: **sudo systemctl status harrier**

2.4.3 Starting/stopping Harrier on Windows

On Windows Harrier server process is installed as a Windows service. This process runs under the Local System account.

By default Harrier service is set for **Automatic start** at system startup.

In order to stop or start Harrier manually use standard Windows Services manager (You can also use Isode Service Manager if installed separately with other Isode packages).

2.5 Command Line

In addition to using the Manager application, it is possible to create/modify configuration by direct creation/modification of the XML configuration file.

To make it easier and safer Harrier provides command line options to operate on configuration

- **-f<file>, --config=<file>** Configuration file path
- **-r, --reset** Create clean configuration (back up pre-existing configuration)
- **-s<path>=<value>, --set=<path>=<value>** Set option
- **-u<path>, --unset=<path>** Unset option
- **-d<path>, --add=<path>** Add list option

# Enable TLS with default self-signed keypair

```
isode.harrierwebserver -s /tls/keyPair=default_keypair
```

# Create isode.com domain

```
isode.harrierwebserver -d /domainList -s /domainList/0/
selector=isode.com
```

# Setup Manager's credentials

```
isode.harrierwebserver -s /manager/user=admin -s /manager/
password=secret
```

2.6 Manager Application

The Manager application is a web-based tool for configuring and monitoring the Harrier server.

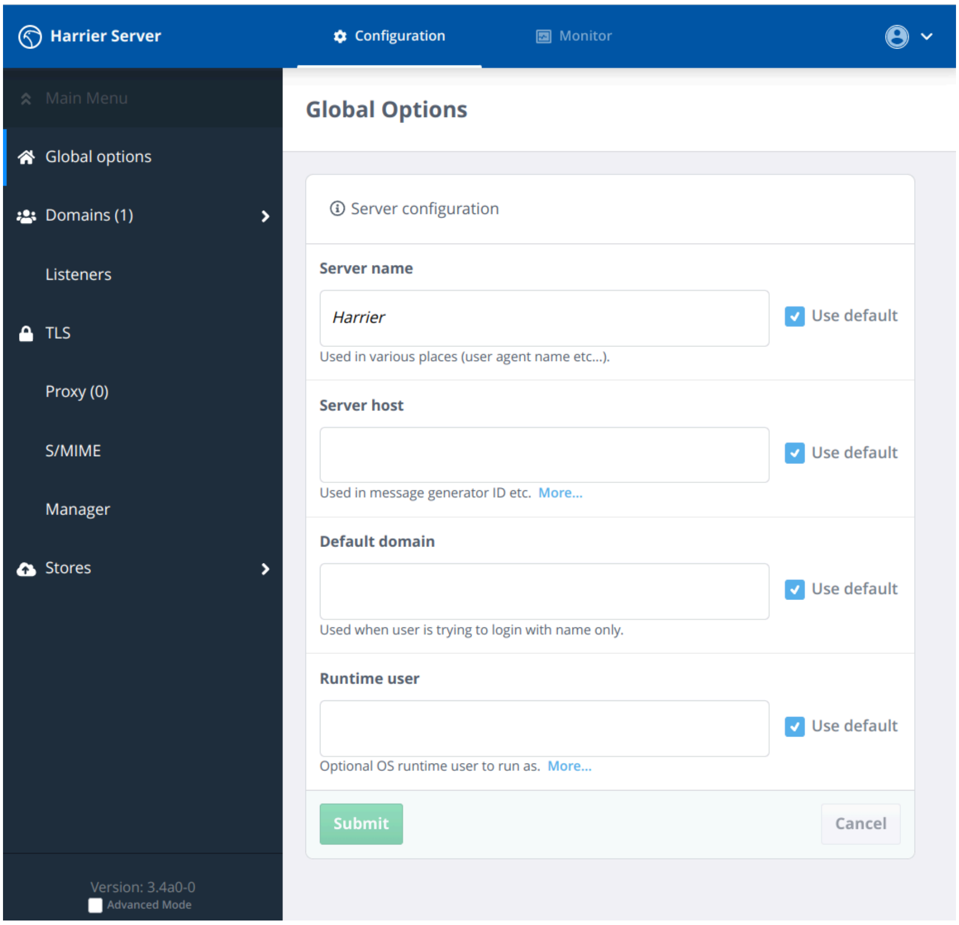
It is accessed by pointing a web browser at the URL `https://localhost:9095` (or the appropriate host and port if the server is not running on the local machine).

In order to prevent unauthorized access in the future, the Manager Application will always prompt for initial administrator's login name and password. These will be used for future authentication attempts.

> **Note:** The initial screen will display a warning about the insecure website because of the self signed certificate. You need to trust this in order to enable the Manager Application to be used.

Once the initial administrator's login name and password are set, and if Harrier is not yet activated externally using Messaging Activation Server, it will request for activation within Manager Application (see: Section 2.7, “Product Activation Mode”).

Figure 2.1. Configuration Options



Server name: *Harrier* ☑ Use default
Used in various places (user agent name etc...).

Server host: ☑ Use default
Used in message generator ID etc. More...

Default domain: ☑ Use default
Used when user is trying to login with name only.

Runtime user: ☑ Use default
Optional OS runtime user to run as. More...

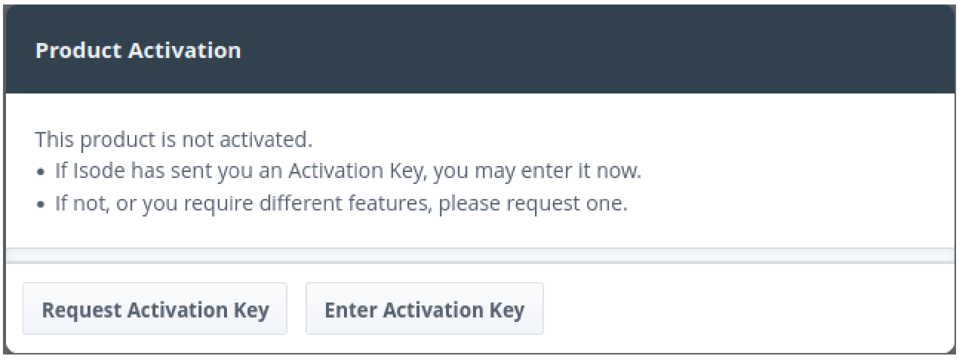
Currently Manager contains Configuration options described in Section 2.8, “Options” and simple "Monitor" page displaying various Harrier server information.

2.7 Product Activation Mode

The first time Harrier is started, it will require a product activation key to enable it to work. This screen will prompt for the details if the product has not yet been activated.

This starts with the dialog shown in Figure 2.2, “Product Activation stage 1”.

Figure 2.2. Product Activation stage 1



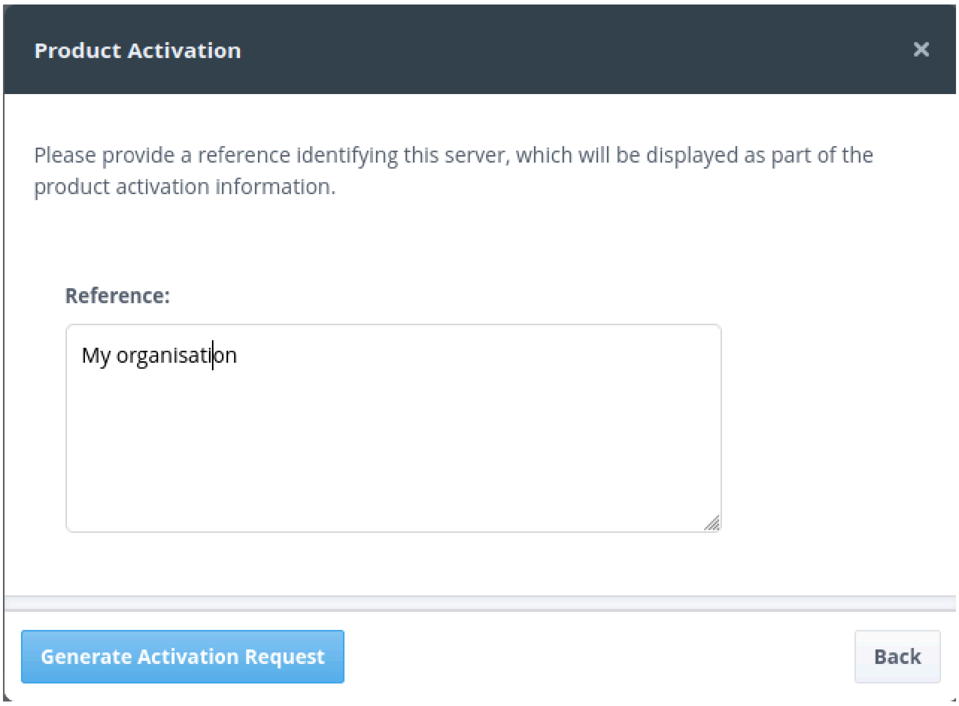
Product Activation

This product is not activated.

- If Isode has sent you an Activation Key, you may enter it now.
- If not, or you require different features, please request one.

At this point it is necessary to generate an activation request to send to the support address support@isode.com. This is shown in Figure 2.3, “Product Activation stage 2”.

Figure 2.3. Product Activation stage 2



Product Activation

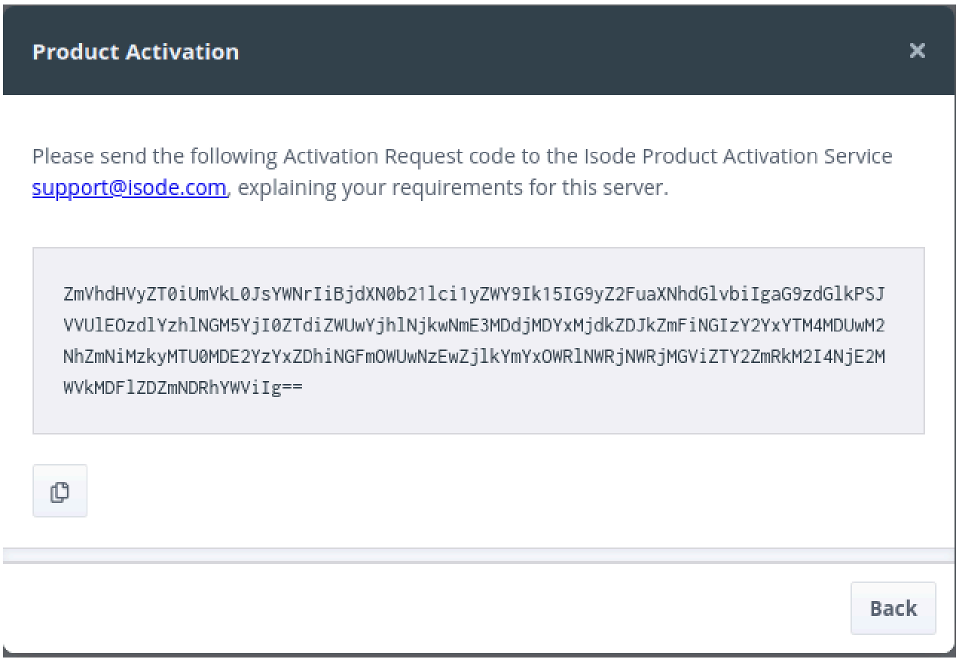
Please provide a reference identifying this server, which will be displayed as part of the product activation information.

Reference: My organisation

The reference should be filled in an then a request generated.

After the request is generated, it should be sent to the license address for a product activation to be issued.

Figure 2.4. Product Activation stage 3



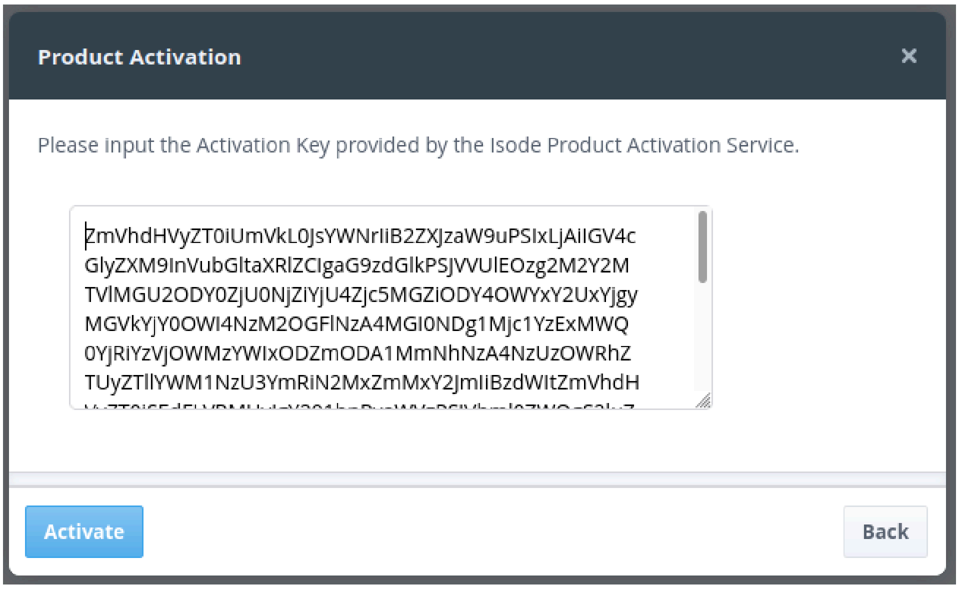
Please send the following Activation Request code to the Isode Product Activation Service support@isode.com, explaining your requirements for this server.

ZmVhdHVyZT0iUmVkL0JsYWNrIiBjdXN0b21lci1yZWY9Ik15IG9yZ2FuaXNhdGlvbiIgaG9zdGlkPSJ
VVUlEOzdlYzhlNGM5YjI0ZTdiZWUwYjhlNjkwNmE3MDdjMDYxMjdkZDJkZmFiNGIzY2YxYTM4MDUwM2
NhZmNiMzkyMTU0MDE2YzYxZDhiNGFmOWUwNzEwZjlkYmYxOWRlNWRjNWRjMGViZTY2ZmRkM2I4NjE2M
WVkMDFlZDZmNDRhYWViIg==

There is a button to copy the data to the clipboard ready for sending.

When the activation result is received from the license desk, it can be entered into the activation box, and the product activated as shown in Figure 2.5, “Product Activation stage 4”.

Figure 2.5. Product Activation stage 4



Please input the Activation Key provided by the Isode Product Activation Service.

ZmVhdHVyZT0iUmVkL0JsYWNrIiB2ZXJzaW9uPSIxLjAiIGV4c
GlyZXM9InVubGltaXRlZCIgaG9zdGlkPSJVVUlEOzg2M2Y2M
TVlMGU2ODY0ZjU0NjZiYjU4Zjc5MGZiODY4OWYxY2UxYjgy
MGVkYjY0OWI4NzM2OGFlNzA4MGI0NDg1Mjc1YzExMWQ
0YjRiYzVjOWMzYWIxODZmODA1MmNhNzA4NzUzOWRhZ
TUyZTllYWM1NzU3YmRiN2MxZmMxY2JmIiBzdWItZmVhdH

2.8 Options

This chapter describes configuration options available in the Manager application.

When using the Harrier Manager application, advanced options are not visible by default, unless the system administrator checks the "Advanced options" checkbox at the bottom left of the Management page.

2.8.1 Variables

Wherever file paths are specified inside the configuration file, you can use one of several pre-defined placeholders rather than entering an absolute file path. These all have the form `$(`*name*`)`. You can use these placeholders wherever a file path is expected in the configuration file.

Name	Description
`$(harrier.dir.client)`	(CLIENTDIR) file system placeholder
`$(harrier.dir.etc)`	(ETCDIR) file system placeholder
`$(harrier.dir.lib)`	(LIBDIR) file system placeholder
`$(harrier.dir.log)`	(LOGDIR) file system placeholder
`$(harrier.dir.share)`	(SHAREDIR) file system placeholder
`$(harrier.dir.tmp)`	(TMPDIR) file system placeholder
`$(harrier.dir.var)`	(DATADIR) file system placeholder
`$(harrier.dir.etc_or_share)`	First checks (ETCDIR) then (SHAREDIR)
`$(harrier.dir.app)`	Directory where Harrier Web Server executable is located
`$(harrier.dir.cfg)`	Directory where current configuration file is located

2.8.2 Global Options

The following are global options that control the configuration of the Harrier server.

Server name

Used in various places (user agent name etc...).

Default value: `Harrier`

Old (3.X) configuration: `<name>`

Server host

Specifies text to be used when generating a unique string used for the `message-id` header for messages that have been composed within Harrier. If this is not specified, then the a value is derived from the hostname in the URL that the user supplied to connect to Harrier. Setting this option avoids exposing this hostname in the message header.

A value for `host` is required when a self-signed certificate is to be generated for the Harrier Web Server (see **Key pair**).

Example value: `example.com`

Old (3.X) configuration: `<host>`

Default login domain

Specifies the default domain to be used when a user logs in with a username that does not contain a domain part (The default domain is being added to the username to determine fully qualified username - E.g. "user1" instead of "user1@example.com"). If specified, it must be a domain corresponding to an existing domain configuration. If this option is not specified, then the user must supply a domain when logging in.

Example value: `example.com`

Old (3.X) configuration: `<default_domain>`

Runtime user

Specifies the OS user that Harrier Web Server will run as. This option only applies on Linux systems. To use this option the server will need to be started as the root user: it will bind to any ports (which may include privileged ports) before dropping privileges to run as the specified runtime user.

Example value: `harrier`

Old (3.X) configuration: `<runtime_user>`

Shutdown watchdog [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

The shutdown watchdog allows to enforce server shutdown after specific timeout (period of graceful shutdown attempt).

0 - means watchdog disabled.

Notice: If set it should be longer than `HTTP/S and WS/S -> Shutdown timeout` options values.

Default value: `5s`

Old (3.X) configuration: `<shutdown_watchdog_timeout>`

Developer's mode [advanced]

Enables developer's mode - exposes experimental functionality. This option is intended for developers only and should not be used in production.

Default value: `Off`

Old (3.X) configuration: `<dev_mode>`

Stack tracing [advanced]

Enable server to log stack trace in case of crash (default true)

Default value: `On`

Old (3.X) configuration: `<stack_tracing>`

2.8.3 Domains

This section describes configuration options that are associated with specific user/role (like IMAP, SMTP and LDAP) - usually with domain.

Old (3.X) configuration: `<domains>`

Domain name or pattern

`Regular expression (case insensitive)` - See http://cplusplus.com/reference/regex/ECMAScript for more detailed information about regular expressions.

Specifies a domain name used to match the domain part of the username supplied by someone logging in to Harrier Web.

Example value: `example.com` matches any username that ends with `@example.com`

Old (3.X) configuration: `<domain name="" pattern="">`

Domain name is regular expression pattern [advanced]

Allows to define more advanced selector matching rules. The "Domain name or pattern" specifies an ECMAScript Regular Expression which is used to match the domain part of the username supplied by someone logging in to Harrier Web.

Default value: `Off`

Example value: `example\.(net|com)` matches any username that ends in either `@example.com` or `@example.net`

Old (3.X) configuration: `<domain name="" pattern="">`

Mode

Whether or not the server is running in one of military modes: "Military", "ACP 127" or "Internet" mode.

Options:

- `Military` **[default]**
- `ACP 127`
- `Internet`

Old (3.X) configuration: `<mode>`

Session timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Specifies the period of inactivity before web client sessions are terminated by the Harrier Web Server.

A value of `0` can be used to indicate that sessions should never be timed out.

Default value: `30min`

Old (3.X) configuration: `<session_timeout>`

Allowed attachment extensions [advanced]

List of ;-separated file extensions (without the leading ".") that are allowed when attaching files to composed messages. The default value is empty, i.e. all file extensions are allowed. This option is mutually exclusive with the "Disallowed attachment extensions" option.

Old (3.X) configuration: `<allowed_attachment_ext>`

LDAP authentication [advanced]

Enable LDAP based auth instead of IMAP based.

Default value: `Off`

Old (3.X) configuration: `<auth_ldap>`

Auto-save period

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Option allows to enable periodical saving of edited messages (0 means disabled).

It must be shorter than `Session timeout` to help ensure that if a user session is timed out while a composing a message, any changes to the message would already have been saved.

Default value: `5m`

Old (3.X) configuration: `<auto_save>`

Cleaning period [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

How often to perform internal cleaning (cache, expired certificates). 0 means disabled periodical cleaning process.

Default value: `5m`

Old (3.X) configuration: `<cleaning_period>`

Blocked content URI [advanced]

Replacement URIs used for resources that are blocked when remote content is disallowed (original URI may be added using $1 variable)). Default value is: /api/block?uri=$1 which blocks direct jump to the URI displaying HTML 403 error page (exposing blocked uri). To suppress exposing original URI you can use i.e. /api/block?uri=%3d%3d%20HIDDEN%20%3d%3d

Default value: `/api/block?uri=$1`

Old (3.X) configuration: `<content_blocked_uri>`

Disallowed attachment extensions [advanced]

List of ;-separated file extensions (without the leading ".") that are disallowed when attaching files to composed messages. The default value is empty, i.e. all file extensions are allowed. This option is mutually exclusive with the "Allowed attachment extensions" option.

Old (3.X) configuration: `<disallowed_attachment_ext>`

Require DSN by default in new messages [advanced]

Automatically request DSN for each message sent by the user.

Default value: `Off`

Old (3.X) configuration: `<dsn_require>`

Manage S/MIME Identities [advanced]

This option controls whether Harrier updates harrierSignIdentity attribute. PKCS#11-based (HSM) identities are typically managed by Cobalt, but Cobalt currently can't manage PKCS#12-based identities. Set this value to true if you either a) want to update identity information from Harrier R3.2 and/or b) want to use Harrier CSR generation feature with PKCS#12 identities.

Default value: `Off`

Old (3.X) configuration: `<manage_smime_identities>`

Max mailbox view size [advanced]

Maximum number of messages that can be viewed in any folder. This is only used when IMAP PARTIAL extension is also supported by the server.

Default value: `10000`

Old (3.X) configuration: `<max_mailbox_view>`

Message tracking [advanced]

Whether or not the server should track progress of messages based on received DSNs and MDNs.

Default value: `Off`

Old (3.X) configuration: `<message_tracking>`

Notify unread deletion

Option allows generation of MDNs for messages requesting MDN (e.g. Read Receipt) when a logged in user deletes (or moves to Trash) messages without reading them first.

This option should only be used in environments where senders are trusted.

Default value: `Off`

Old (3.X) configuration: `<notify_delete_before_read>`

Role auto-selection [advanced]

Enables implicit role selection when user can choose only one role.

Default value: `On`

Old (3.X) configuration: `<role_auto_selection>`

Role self

Enable adding login name to the list of roles.

Default value: `Off`

Old (3.X) configuration: `<role_self>`

Session sustain [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Sustain session after lost client websocket connection for given time to allow restoring connection in example in case of page reload. 0 means terminate session immediately.

Default value: `3s`

Old (3.X) configuration: `<session_sustain>`

2.8.3.1 Action thresholds

Defines action thresholds (act by) for messages with given precedence. Action thresholds are used in message sorting in absence of Reply-By header fields. They are also used to display remaining time for taking action on a particular message.

Old (3.X) configuration: `<act_by>`

Deferred

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expected act timing for 'Deferred' precedence.

Default value: `7d`

Routine

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expected act timing for 'Routine' precedence.

Default value: `3h`

Priority

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expected act timing for 'Priority' precedence.

Default value: `1h`

Immediate

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expected act timing for 'Immediate' precedence.

Default value: `15m`

Flash

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expected act timing for 'Flash' precedence.

Default value: `10m`

Override

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expected act timing for 'Override' precedence.

Default value: `5m`

2.8.3.2 ADatP-3 [advanced]

ADatP-3

Inline

Control how ADatP-3 attachments are handled when added to a message being composed. If true, the ADatP-3 body part is inserted as text/plain and not marked as attachment. If false, the ADatP-3 body part is inserted as a text/adatp-3 attachment.

Default value: `On`

Old (3.X) configuration: `<adatp3_inline>`

Script template

HTML template file with JavaScript fragment used when contacting the web application specified in the "adatp3_webforms_uri" option.

Default value: `default_adatp3`

Old (3.X) configuration: `<adatp3_script_template>`

Web forms URI

Control how ADatP-3 attachments are handled by specifying URI of a web application that is used for displaying and composing ADatP-3 attachments. Empty value means that default processing is used.

Old (3.X) configuration: `<adatp3_webforms_uri>`

2.8.3.3 Draft & release [advanced]

This section describes configuration options related to Draft & Release workflow support.

Optional releasers

This option includes an email address for which Draft & Release procedure is optional, i.e. the email address can send direct email messages, as well as draft messages that are subject to Draft & Release procedure. The email address appears in the "sender" attribute.

Draft & Release rules specified in the Harrier Server's configuration can be extended by setting the harrierDraftReleaseRules LDAP attribute in the domain's and/or organization's configuration entry. This LDAP attribute contains XML fragment with `release_policy_rule`, `exempted_address` and/or `optional_releaser` XML elements.

Default value: Empty - which means that no user (other than Releasers specified in Section 2.8.3.3.3, “Releaser addresses” or Section 2.8.3.3.2, “Release policy rules”) is exempt from the Draft & Release procedure.

Example value: `xo@example.org`

Old (3.X) configuration: `<optional_releaser>`

Require D&R

This option controls whether or not Draft & Release procedure is required for the domain. When it is required, this means that each message sent by any domain user needs to be approved for release by an authorized Releaser. When Draft & Release procedure is in effect, two extra fields appear in the Compose window: one for selected Reviewers (can be empty) and another one for selected Releasers. See Section 2.8.3.3.3, “Releaser addresses” for more details on the meaning of these fields and operations allowed.

If **Require D&R** is set to true and Releaser addresses option is also set, the email address(es) specified in that option will be used as Releaser(s) for all messages: the Releaser field in the Compose window will display the specified email address(es), and the user will be able to pick one of the Releasers, but will not be able to leave the Releaser field empty.

If **Require D&R** is set to true and no Releaser addresses option is set, the Releaser field remains empty and it needs to be entered manually.

If **Require D&R** is set to false and no Releaser addresses option is set, then Draft & Release procedure is disabled for the domain.

If **Require D&R** is set to false and Releaser addresses option is also set, the email address(es) specified in that option will be used as Releaser(s) for all messages (as above), plus an extra choice "No Releaser / Default Releaser" is given to the user.

Note, irrespective of the value of this option, the Draft & Release procedure is enabled if the Releaser addresses option is set.

Default value: `Off` - which means that the Draft & Release procedure is not used for the domain, unless the Releaser addresses option is also set.

Old (3.X) configuration: `<releaser_required>`

2.8.3.3.1 Exempted addresses

This option includes an email address exempted from Draft & Release.

Draft & Release rules specified in the Harrier's configuration can be extended by setting the harrierDraftReleaseRules LDAP attribute in the domain's and/or organization's configuration entry. This LDAP attribute contains XML fragment with `release_policy_rule`, `exempted_address` and/or `optional_releaser` XML elements.

Default value: Empty - which means that no user (other than Releasers specified in Section 2.8.3.3.3, “Releaser addresses” or Section 2.8.3.3.2, “Release policy rules”) is exempt from the Draft & Release procedure.

Example value: `co@example.org`

Old (3.X) configuration: `<exempted_address>`

Sender

Old (3.X) configuration: `<exempted_address>`

Precedence

Old (3.X) configuration: `<exempted_address precedence="">`

Label

Old (3.X) configuration: `<exempted_address label="">`

Subject indicator codes

Old (3.X) configuration: `<exempted_address sics="">`

Domain

Old (3.X) configuration: `<exempted_address domain="">`

2.8.3.3.2 Release policy rules

It is possible to specify Draft & Release configuration that will only apply to certain messages (e.g. messages with certain SICs, messages from certain senders or messages above certain priority). Releasers specified using such conditional rules can be selected in the Compose window, or the user can select "No releaser" if the releaser is optional or an exception rule applies.

Each conditional rule is defined using **Releaser** with following condition options. The order of conditional rules is important: the first matching rule applies to any sent message. (Or if none of them apply, the message is sent without Draft & Release.)

Each condition attribute must be true for the submitted message in order for the corresponding rule to be triggered. If multiple such conditions are specified, they all must be true for the rule to apply (i.e. they are ANDed), with the exception of "default", which is treated specially.

If no condition is specified, this option behaves the same way as the corresponding Releaser addresses option.

Example 1: `precedence="flash" sics="ZZZ;WWW" releaser="mir@example.com"`

This rule will use mir@example.com as the Releaser if the message has action precedence "flash" (or higher) AND contains one or more of SICs {"ZZZ", "WWW"}.

Example 2: `domain="example.net" sender="jengo@example.com" releaser="mir@example.com"`

This rule will use mir@example.com as the Releaser if the message is sent to any recipients in domain "example.net" and has From/Sender "jengo@example.com".

Draft & Release rules specified in the Harrier configuration can be extended by setting the harrierDraftReleaseRules LDAP attribute in domain's configuration entry. This LDAP attribute contains XML fragment with `release_policy_rule` and/or `exempted_address` XML elements.

By default rules list is empty, which means that the Draft & Release procedure is not used for the domain, unless the Releaser addresses option is also set.

Old (3.X) configuration: `<release_policy_rule>`

Name

Internal name of the rule.

Priority

The lower number the higher priority of the rule to be matched. (the order of rules of the same priority Is undefined)

Releaser

Email address of the releaser assigned to this rule.

Available only if: **Default releasers** is disabled.

Old (3.X) configuration: `<release_policy_rule>`

Default releasers

Used to reference the default set of releasers (all releasers specified with no conditions). The releaser value is ignored in this case.

Default value: `Off`

Example value: sics="AAA" default=On - All messages that contain SIC "AAA" will be releasable by the default set of Releasers.

Old (3.X) configuration: `<release_policy_rule default="">`

Sender

<optional-negate-char><email address>. Where <optional-negate-char> is the character "!". If optional-negate-char is absent and the message sent by the specified (role) email address, this rule will be triggered. If optional-negate-char is present and the message is not sent by the specified (role) email address, this rule will be triggered.

Example value: `alex@example.com` - All messages that were sent by alex@example.com will use associated Releaser.

Old (3.X) configuration: `<release_policy_rule sender="">`

From

<optional-negate-char><email address>. Where <optional-negate-char> is the character "!". If optional-negate-char is absent and the message contains the specified email address in the From header field, this rule will be triggered. If optional-negate-char is present and the message doesn't contain the specified email address in the From header field, this rule will be triggered. (Note that in the case of an Organizational email message, this will be the Organization email address, while "sender" would be the role that generated the email message.)

Example value: `!alex@example.com` - All messages that don't contain From alex@example.com will use associated Releaser.

Old (3.X) configuration: `<release_policy_rule from="">`

Prefer

Does this rule specify the preferred releaser?

Default value: `Off`

Old (3.X) configuration: `<release_policy_rule prefer="">`

Precedence

<optional-negate-char><number or a precedence keyword, such as `flash` or `override`>. Where <optional-negate-char> is the character "!". If optional-negate-char is absent, all messages with the action precedence which is the same or higher

than this value trigger this rule. If optional-negate-char is present, all messages with the action precedence which is the same or lower than this value trigger this rule.

Example value:

```
flash
```

```
!3
```

Old (3.X) configuration: `<release_policy_rule precedence="">`

Label

<optional-negate-char><selector>. Where <optional-negate-char> is the character "!". If optional-negate-char is absent and the message contains the specified Security Label, this rule will be triggered. If optional-negate-char is present and the message doesn't contain the specified Security Label, this rule will be triggered. It is also possible to specially handle messages with unrecognized/invalid or missing SIO-Label header field values using special ":missing" and ":unknown" selectors.

Example value:

```
NATO|Secret
```

```
:missing
```

Old (3.X) configuration: `<release_policy_rule label="">`

Subject indicator codes

<optional-negate-char><list of ;-separated SIC codes that trigger this rule>. Where <optional-negate-char> is the character "!". If optional-negate-char is absent, any of the SICs has to match for the rule to be triggered. If optional-negate-char is present, none of the SICs have to match for the rule to be triggered.

Example value:

```
AAA;BBB;CCC
```

```
!ZZZ;YYY
```

Old (3.X) configuration: `<release_policy_rule sics="">`

Domain

<optional-negate-char><email address>. Where <optional-negate-char> is the character "!". If optional-negate-char is absent and the message sent by the specified (role) email address, this rule will be triggered. If optional-negate-char is present and the message is not sent by the specified (role) email address, this rule will be triggered.

Example value: `isode.net`

Old (3.X) configuration: `<release_policy_rule domain="">`

2.8.3.3.3 Releaser addresses

This option specifies the email address of a Releaser that is used for releasing Draft & Release messages. When this option is set all messages sent by users in the domain will be subject to Draft & Release procedure, except for messages created by the Releaser or senders specified in Exempted addresses.

When Draft & Release procedure is in effect, two extra fields appear in the Compose window: one for selected Reviewers (can be empty) and another one for selected Releasers. The latter field allows one or more Releaser to be selected from the list of Releaser email addresses configured for the domain. Reviewer(s) will receive such messages in the order specified in the message. Each Reviewer can reject (return to Drafter with some comments), pass to the next Reviewer or Releaser, change

Reviewer(s), or take ownership of the message and become the Drafter (to be reviewed by remaining Reviewer(s) and Releaser(s)). Releaser(s) will receive such messages once they are approved by Reviewer(s) (if any), in the order specified in the message. Each Releaser can reject (return to Drafter), pass to the next Releaser (if not the last Releaser), release (send to the originally intended recipients. Only if the last Releaser), change Drafter (reassign authorship of the message to another Drafter), change Reviewer(s), change Releaser(s), or edit and send each individual message.

This option can be defined multiple times - than it specifies alternative Releasers that can be selected in the Compose window. Any one of them will be able to release messages.

Default value: Empty - which means that the Draft & Release procedure is not used for the domain, unless **Require D&R** is also enabled.

Old (3.X) configuration: `<releaser_address>`

Address

Email address of a Releaser.

Old (3.X) configuration: `<releaser_address>`

Prefer

Is this the preferred (default) releaser?

Default value: `Off`

Old (3.X) configuration: `<releaser_address prefer="">`

2.8.3.4 IMAP server

IMAP Server options defines how Harrier connects to IMAP server.

Primary URL

`IMAP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The primary IMAP server URL. A URL must start with either "imap://" or "imaps://" and be followed by the <host>:<port> - for example, "imaps://myserver.example.com:993". The typical port is 143 for "imap" and 993 for "imaps". The substring $(domain) will be replaced by the current domain configuration Selector value.

Default value: `imap://$(domain):143`

Old (3.X) configuration: `<imap_url>`

Backup URL

`IMAP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The backup IMAP server URL. A URL must start with either "imap://" or "imaps://" and be followed by the <host>:<port> - for example, "imaps://myserver.example.com:993". The typical port is 143 for "imap" and 993 for "imaps". The substring $(domain) will be replaced by the current domain configuration Selector value.

Old (3.X) configuration: `<imap_url>`

STARTTLS policy

Controls use or non use of STARTTLS.

Options:

- `License` **[default]** - Depending on license-activation - When TLS sub-feature is activated the default is `Opportunistic`, and `Suppress` otherwise.
- `Mandatory` - Always use STARTTLS, fail the connection if not advertised.
- `Opportunistic` - Try to use STARTTLS if advertised, but carry on regardless of STARTTLS success.
- `Suppress` - Never use STARTTLS, even if advertised.

Old (3.X) configuration: `<imap_starttls_policy>`

Trust anchors

Connections to the IMAP server using TLS, will fail unless the IMAP server's certificate can be verified against these trust anchors.

(see: Section 2.9, “Certificate Verification”)

Specifying this option forces Harrier Web Server to use `StartTLS` for all IMAP connections, and to require that the IMAP server provides a certificate which can be verified using this set of CA certificates.

Old (3.X) configuration: `<imap_server_trustanchors>`

Pinned certificates

If IMAP server certificate is not issued by any trusted CA pinned certificates allows to specify trustworthy certificates directly.

(see: Section 2.9, “Certificate Verification”)

Old (3.X) configuration: `<imap_server_pinned>`

Allow PLAIN over clear text [advanced]

Controls whether authentication using the PLAIN or the LOGIN SASL mechanisms can be used without TLS in IMAP.

Default value: `Off`

Old (3.X) configuration: `<imap_plain_over_cleartext>`

Keepalive interval [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

IMAP servers may be configured with an autologout timer, which will drop connections to clients (including Harrier Web Server) if there has been no IMAP activity for a certain time. This option can be used to make Harrier Web Server keep IMAP sessions alive. IMAP servers which are RFC3501 conformant will not use timeout values of less than thirty minutes, in which case a setting 29m (minutes) will prevent the IMAP session from being disconnected.

Note that the "Session timeout" option may be used to have HWS disconnect idle web client sessions, and may be a more appropriate way to control idle users.

Default value: `29m`

Old (3.X) configuration: `<imap_keepalive_interval>`

Reconnect interval [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Specifies how frequently Harrier Web Server should re-attempt to connect to an IMAP server after failed/lost connection to it.

Value `0` disables automatic re-bind.

Default value: `5s`

Old (3.X) configuration: `<imap_reconnect_interval>`

TLS SNI [advanced]

TLS Server Name Indication (SNI) extension value, in the format of a hostname. This is required by some IMAP servers to connect. In most cases this value should be the same as the host part of the "Primary URL". The default is empty, which means that TLS SNI extension shouldn't be used.

Old (3.X) configuration: `<imap_tls_sni>`

Administrative username [advanced]

Administrative username to use with SASL proxy authentication.

Old (3.X) configuration: `<imap_admin_user>`

Allow IMAP IDLE use [advanced]

Enable IMAP IDLE usage (if supported by server)

Default value: `On`

Old (3.X) configuration: `<imap_idle_support>`

Single fetch chunk size [advanced]

How many octets to request from IMAP server in a single FETCH when fetching large body parts. Larger values can make operations like forward as attachment quicker, but can make Harrier less responsive to user requests. Make this value larger on WiFi networks and smaller on slow links.

Default value: `64k`

Old (3.X) configuration: `<imap_single_fetch_chunk_size>`

Total fetch limit [advanced]

Restrict the total size of all images.

Default value: `1M`

Old (3.X) configuration: `<imap_total_fetch_limit>`

2.8.3.5 LDAP

LDAP access and how to find / store information

Validate attributes [advanced]

By default, all LDAP attribute names used in this file will be validated using the local directory schema, and if any unrecognised names are present then Harrier Web Server will not start. If the LDAP server is using a different schema then this option may be used to prevent this validation.

Default value: `On`

Old (3.X) configuration: `<ldap_validate_attributes>`

2.8.3.5.1 Server

LDAP Server options defines how Harrier connects to LDAP server.

Primary URL

`LDAP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The primary LDAP server URL. A URL must start with either "ldap://" or "ldaps://" and be followed by the <host>:<port> - for example, "ldap://myserver.example.com:19389". It may be empty. In such case directory services will not be available. The typical port is 389 for "ldap" and 636 for "ldaps". The substring $(domain) will be replaced by the current domain configuration Selector value.

Example value: `ldap://example.net:389`

Old (3.X) configuration: `<ldap_url>`

Backup URL

`LDAP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The backup LDAP server URL. A URL must start with either "ldap://" or "ldaps://" and be followed by the <host>:<port> - for example, "ldap://myserver.example.com:19389". It may be empty. In such case directory services will not be available. The typical port is 389 for "ldap" and 636 for "ldaps". The substring $(domain) will be replaced by the current domain configuration Selector value.

Example value: `ldap://backup.example.net:389`

Old (3.X) configuration: `<ldap_url>`

Trust anchors

Connections to the LDAP server using TLS, will fail unless the LDAP server's certificate can be verified against these trust anchors.

(see: Section 2.9, “Certificate Verification”)

Old (3.X) configuration: `<ldap_server_trustanchors>`

Pinned certificates

If LDAP server certificate is not issued by any trusted CA pinned certificates allows to specify trustworthy certificates directly.

(see: Section 2.9, “Certificate Verification”)

Old (3.X) configuration: `<ldap_server_pinned>`

Rebind interval [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Specifies how frequently Harrier Web Server should re-attempt to bind to an LDAP server after lost connection to it.

Value `0` disables automatic re-bind.

Default value: `5s`

Old (3.X) configuration: `<ldap_rebind_interval>`

SASL mechanisms [advanced]

Space separated list of SASL mechanisms (in order of preference) to be used when authenticating to the LDAP server. Mechanisms not supported by the server are ignored from the list. The remaining mechanisms are tried in order. The ANONYMOUS and EXTERNAL mechanisms are not supported by Harrier (LDAP client) so not allowed in this option. If not specified, the client code will try to use any SASL mechanisms supported by the server.

Default value: Not specified - negotiated with the server.

Old (3.X) configuration: `<ldap_sasl_mechs>`

SASL user name only ID [advanced]

Enable user name only id (without domain part) in SASL authentication (Some LDAP servers like Active Directory require that).

Default value: `Off`

Old (3.X) configuration: `<ldap_sasl_user_only_id>`

Cache expiration [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expiration time of cached data collected from LDAP directory. 0 means expiration disabled.

Default value: `10m`

Old (3.X) configuration: `<ldap_cache_expiration>`

2.8.3.5.2 Server auth

How Harrier binds to LDAP server. Currently anonymous bind, simple bind and SASL bind are supported.

DN

`LDAP distinguished name.`

Specifies LDAP DN used to enable simple bind to access local directory and organisational address book.

This option requires setting **Password** while **SASL ID** cannot be set at the same time.

Example value: `cn=user1,cn=users,o=example`

Old (3.X) configuration: `<ldap_auth_dn>`

SASL ID

Specifies SASL ID used to enable SASL ID based bind to access local directory and organisational address book.

This option requires setting **Password** while **DN** cannot be set at the same time.

Example value: `ldapuser@example.com`

Old (3.X) configuration: `<ldap_auth_sasl_id>`

Password

Specifies optional password used by simple bind or SASL ID based bind.

This option is required when **DN** or **SASL ID** is specified.

Old (3.X) configuration: `<ldap_auth_pwd>`

2.8.3.5.3 Address book

Address-book lookups are performed when a user enters part of an address and the application provides matching names/addresses - for example when entering recipient names in the compose window, or when searching the address book for contacts.

The options determine how Harrier should search the LDAP directory when performing address-book lookups.

Base DN

`LDAP distinguished name.`

This option specifies base DN in the directory for searches. Only entries below this DN will be considered when searching the addressbook.

Default value: Empty - the root DN

Example value: `ou=staff,c=us`

Old (3.X) configuration: `<ldap_addressbook_base_dn>`

Default search filter attributes

`Comma separated list of LDAP attribute names.`

Attributes used to search for address book entry using with given sub-string.

It is used only when the **Custom search filter** option is not defined and generates filter automatically for finding entries that have the searched string (represented by $1 variable) in any of attributes specified and limited to specific `cobaltObjectType` where:

`0` = User for local addressbook filter in `Internet` mode

`1` = Role for local addressbook filter in `Military/ACP 127` mode

`2` = Organisation for organisational addressbook filter

Default value: in `ACP 127` mode: `displayName,sn,givenName,plaNameACP127,CN`; in other modes: `displayName,sn,givenName,CN,mail,mailLocalAddress,mailRoutingAddress`

Old (3.X) configuration: `<ldap_addressbook_filter_ats>`

Custom search filter

`LDAP filter` - See https://www.rfc-editor.org/rfc/rfc4515.html.

This option specifies filter used when performing address book searches. The special string `$1` may be used in the filter string to indicate the user's search string.

If this option specified, the **Default search filter attributes** option is ignored.

Default value: Empty - which means that the search simply looks for matches in attributes as specified by the **Default search filter attributes** option.

Example value: `(&(mail=*)(cn=*$1))`

Old (3.X) configuration: `<ldap_addressbook_filter>`

Mail attributes

`Comma separated list of LDAP attribute names.`

Attributes used to find email addresses in users' entry.

The first attribute in the list will be used as the main user email address. Any other attributes are used to find alternate addresses for the user.

These values are used by Harrier when showing a user's messages, to indicate whether a message was addressed "to" (action) or "cc" (info) that user. The email values are also used when searching the address book (e.g. in order to be able to locate a user's photo or public certificate).

Note: that the first named attribute must be single valued.

Default value: `mail, mailLocalAddress`

Old (3.X) configuration: `<ldap_addressbook_mail_ats>`

Name attributes

`Comma separated list of LDAP attribute names.`

Attributes used to find user friendly user name in users' entry. Used both by logged in user and address book (first value found where attributes order search is preserved).

Default value:

`ACP 127` mode: "`plaNameACP127,displayName,CN`"

`Military` mode: "`displayName,plaNameACP127,CN`"

`Internet` mode: "`displayName,CN`"

Example value: `displayName,CN`

Old (3.X) configuration: `<ldap_addressbook_name_ats>`

Routing indicator attribute

`LDAP attribute name.`

Attribute used as an address hint in ACP-127 mode.

Default value: `rI`

Old (3.X) configuration: `<ldap_addressbook_routing_indicator_at>`

2.8.3.5.4 Org. address books

The domain may contain one or more `Organisational address books` used to search organisations (recipients) in `military`mode.

Each `Organisational address books` inherits by default all settings from local (Server, Server auth, Address book) and allows to redefine / overwrite differences. (In simple case organisational address book may be in the same directory but under distinct base DN or using different search filter for example). Yet it is flexible enough to use distinct directory, schema, and authentication (bind) details.

Old (3.X) configuration: `<ldap_orgs_addressbook>`

Name

Name which identifies this address book.

2.8.3.5.4.1 Server

Server access options.

Primary URL

`LDAP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The primary LDAP server URL. A URL must start with either "ldap://" or "ldaps://" and be followed by the <host>:<port> - for example, "ldap://myserver.example.com:19389". It may be empty. In such case directory services will not be available. The typical port is 389 for "ldap" and 636 for "ldaps". The substring $(domain) will be replaced by the current domain configuration Selector value.

Default value: Inherited from local **Primary URL**

Example value: `ldap://example.net:389`

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_url>`

Backup URL

`LDAP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The backup LDAP server URL. A URL must start with either "ldap://" or "ldaps://" and be followed by the <host>:<port> - for example, "ldap://myserver.example.com:19389". It may be empty. In such case directory services will not be available. The typical port is 389 for "ldap" and 636 for "ldaps". The substring $(domain) will be replaced by the current domain configuration Selector value.

Default value: Inherited from local **Backup URL**

Example value: `ldap://backup.example.net:389`

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_url>`

Trust anchors

Connections to the LDAP server using TLS, will fail unless the LDAP server's certificate can be verified against these trust anchors.

(see: Section 2.9, “Certificate Verification”)

Default value: Inherited from local **Trust anchors**

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_server_trustanchors>`

Pinned certificates

If LDAP server certificate is not issued by any trusted CA pinned certificates allows to specify trustworthy certificates directly.

(see: Section 2.9, “Certificate Verification”)

Default value: Inherited from local **Pinned certificates**

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_server_pinned>`

Rebind interval [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Specifies how frequently Harrier Web Server should re-attempt to bind to an LDAP server after lost connection to it.

Value `0` disables automatic re-bind.

Default value: Inherited from local **Rebind interval** [advanced]

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_rebind_interval>`

SASL mechanisms [advanced]

Space separated list of SASL mechanisms (in order of preference) to be used when authenticating to the LDAP server. Mechanisms not supported by the server are ignored from the list. The remaining mechanisms are tried in order. The ANONYMOUS and EXTERNAL mechanisms are not supported by Harrier (LDAP client) so not allowed in this option. If not specified, the client code will try to use any SASL mechanisms supported by the server.

Default value: Inherited from local **SASL mechanisms** [advanced]

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_sasl_mechs>`

SASL user name only ID [advanced]

Enable user name only id (without domain part) in SASL authentication (Some LDAP servers like Active Directory require that).

Default value: Inherited from local **SASL user name only ID** [advanced]

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_sasl_user_only_id>`

Cache expiration [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Expiration time of cached data collected from LDAP directory. 0 means expiration disabled.

Default value: Inherited from local **Cache expiration** [advanced]

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_cache_expiration>`

2.8.3.5.4.2 Server auth

How Harrier binds to LDAP server. Currently anonymous bind, simple bind and SASL bind are supported.

DN

`LDAP distinguished name.`

Optional simple bind DN for non-anonymous access.

Default value: Inherited from local **DN**

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_auth_dn>`

SASL ID

Optional SASL ID bind for non-anonymous access.

Default value: Inherited from local **SASL ID**

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_auth_sasl_id>`

Password

Optional bind password for non-anonymous access.

Default value: Inherited from local **Password**

Old (3.X) configuration: `<ldap_orgs_addressbook><ldap_auth_pwd>`

2.8.3.5.4.3 Address book

Address book

Base DN

`LDAP distinguished name.`

The address book search base DN. Empty value means root DN.

Default value: Inherited from local **Base DN**

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_addressbook_base_dn>`

Default search filter attributes

`Comma separated list of LDAP attribute names.`

Attributes searched for given sub-string. It is used only when the filter option is not defined.

Default value: Inherited from local **Default search filter attributes**

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_addressbook_filter_ats>`

Custom search filter

`LDAP filter` - See https://www.rfc-editor.org/rfc/rfc4515.html.

Defines custom search filter. If not defined it is being automatically constructed to find entries that have the searched string (represented by $1 variable) in any of attributes specified in "Mail attributes" and limited to specific cobaltObjectType: 0 = User for local addressbook filter in "Internet" mode 1 = Role for local addressbook filter in "Military"/"ACP 127" mode 2 = Organisation for organisational addressbook filter (defined under ldap_orgs_addressbook elements) for example: (&(mail=*)(cobaltObjectType=1)(|(displayName=*$1*)(sn=*$1*)(givenName=*$1*)(CN=*$1*)(mail=*$1*)(mailLocalAddress=*$1*)(mailRoutingAddress=*$1*))) By default it is not defined (aggregated from filter_ats).

Default value: Inherited from local **Custom search filter**

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_addressbook_filter>`

Mail attributes

`Comma separated list of LDAP attribute names.`

Attributes used to find users' email addresses.

The first attribute in the list will be used as the main user email address. Any other attributes are used to find alternate addresses for the user. These values are used by Harrier when showing a user's messages, to indicate whether a message was addressed "to" (action) or "cc" (info) that user. The email values are also used when searching the address book (e.g. in order to be able to locate a user's photo or public certificate).

Note: that the first named attribute must be single valued.

Default value: Inherited from local **Mail attributes**

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_addressbook_mail_ats>`

Name attributes

`Comma separated list of LDAP attribute names.`

User friendly user name attributes. Used both by logged in user and address book (first value found where attributes order search is preserved). The default in "ACP 127" mode is: "plaNameACP127,displayName,CN". The default in "Military" mode is: "displayName,plaNameACP127,CN". The default in "Internet" mode is: "displayName,CN".

Default value: Inherited from local **Name attributes**

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_addressbook_name_ats>`

Routing indicator attribute

`LDAP attribute name.`

ACP 127 specific address routing indicator. Attribute used as an address's hint in ACP-127 mode.

Default value: Inherited from local **Routing indicator attribute**

Old (3.X) configuration:
`<ldap_orgs_addressbook><ldap_addressbook_routing_indicator_at>`

2.8.3.5.5 Roles

Group entries used to define roles.

Use roles

Enable searching for role group entries where user is a member.

Default value: `On`

Old (3.X) configuration: `<ldap_group_search>`

Base DN

`LDAP distinguished name.`

The role groups search base DN. Empty value means root DN.

Available only if: Use roles is enabled.

Old (3.X) configuration: `<ldap_group_base_dn>`

Search filter

`LDAP filter` - See https://www.rfc-editor.org/rfc/rfc4515.html.

The role groups search filter.

Supports `$(user.mail)` variable substituted with main user email address and `$(user.dn)` variable representing user's DN.

Default value: `(&(objectclass=inetOrgRole)(roleOccupant= $(user.dn)))`

Example value:

POSIX group and members referenced via email adddreses:
`(&(objectclass=posixGroup)(memberUid=$(user.mail)))`

Example for group of name and members referenced via DNs:
`(&(objectclass=groupOfNames)(member=$(user.dn)))`

Available only if: Use roles is enabled.

Old (3.X) configuration: `<ldap_group_base_filter>`

ID attribute

`LDAP attribute name.`

The role ID attribute type.

Default value: `mail`

Available only if: Use roles is enabled.

Old (3.X) configuration: `<ldap_group_id_at>`

Name attributes

`Comma separated list of LDAP attribute names.`

Attributes used to find group name in role group entry (the first found is used).

Default value: `displayName,CN`

Available only if: Use roles is enabled.

Old (3.X) configuration: `<ldap_group_name_ats>`

2.8.3.5.6 Draft & release

Draft & Release configuration in LDAP.

Use LDAP configuration

Enable searching for Draft & Release configuration stored in LDAP.

Default value: `On`

Old (3.X) configuration: `<ldap_release_config_search>`

Role attribute

`LDAP attribute name.`

The Draft & Release role attribute type.

Default value: `harrierDraftReleaseRole`

Old (3.X) configuration: `<ldap_release_role_at>`

Search filter

`LDAP filter` - See https://www.rfc-editor.org/rfc/rfc4515.html.

LDAP filter for groups that contain Draft & Release related information. For example a PosixGroup containing all Releasers. Supports $(user.domain) variable substituted with domain of the main user email address.

Default value: `(&(objectclass=posixGroup)(|(memberUid=*@ $(user.domain))(harrierDraftReleaseRole=*)))`

Old (3.X) configuration: `<ldap_release_role_group_base_filter>`

Members emails attribute

`LDAP attribute name.`

Attribute that contains email addresses of members of a Draft & Release related group.

Default value: `memberUid`

Old (3.X) configuration: `<ldap_release_group_member_at>`

2.8.3.5.7 User

User specific information storage in the directory.

Mail attributes

`Comma separated list of LDAP attribute names.`

Attributes used to find users' email addresses.

The first attribute in the list will be used as the main user email address. Any other attributes are used to find alternate addresses for the user. These values are used by Harrier when showing a user's messages, to indicate whether a message was addressed "to" (action) or "cc" (info) that user.

Note that the first named attribute must be single valued.

Default value: `mail, mailLocalAddress`

Old (3.X) configuration: `<ldap_user_mail_ats>`

Name attributes

`Comma separated list of LDAP attribute names.`

Attributes which may contain alternate user friendly user name.

This is used both by logged in user and address book and also appears in the From header field of sent messages.

Default value: Empty - Means

`ACP 127` mode: `plaNameACP127,displayName,CN`

`Military` mode: `displayName,plaNameACP127,CN`

`Internet` mode: `displayName,CN`

Old (3.X) configuration: `<ldap_user_name_ats>`

Preferences attribute
`LDAP attribute name.`

The name of the attribute type in user entries that is used to store Harrier-client specific user preferences (JSON string).

See **Preferences object class**.

Default value: `harrierUserPreferences`

Old (3.X) configuration: `<ldap_user_prefs_at>`

Preferences object class
`LDAP object class.`

The ObjectClass value that must be present in a role's (or user's, if you don't use roles) own directory entry in order for Harrier Web Server to be able to save user preferences.

See **Preferences attribute**.

Default value: `isodeHarrierRole`

Old (3.X) configuration: `<ldap_user_prefs_oc>`

Labels attribute [advanced]
`LDAP attribute name.`

The name of the LDAP attribute type used to store user's custom labels catalog in XML format.

Default value: `harrierUserLabels`

Old (3.X) configuration: `<ldap_user_labels_at>`

Labels object class [advanced]
`LDAP object class.`

The ObjectClass value that must be present in a user's own directory entry in order for Harrier Web to be able to save user defined security labels.

Default value: `isodeHarrierRole`

Old (3.X) configuration: `<ldap_user_labels_oc>`

Groups attribute [advanced]
`LDAP attribute name.`

Attribute type used to store groups IDs in user entry.

Old (3.X) configuration: `<ldap_user_groups_at>`

2.8.3.5.8 Domain [advanced]

Domain configuration

Base DN
`LDAP distinguished name.`

The domain configuration entry search base DN. Empty value means root DN.

Old (3.X) configuration: `<ldap_domain_base_dn>`

2.8.3.6 Organisations

This section describes configuration options related to Organizational Messaging. Organizational Messaging allows logged in users to send email messages on behalf of organizations, for example as specific roles within organizations.

Allow send message as self

When Organisation Messaging is enabled by Addresses, this option is used to control whether a logged in user can send email messages with selected role address or just on behalf of the Organization.

Default value: `Off`

Old (3.X) configuration: `<org_allow_send_as_self>`

Organizational messaging LDAP configuration

Enable retrieval of Organizational Messaging configuration from LDAP.

Default value: `On`

Old (3.X) configuration: `<org_enable_org_messaging>`

2.8.3.6.1 Addresses

This option specifies list of an email addresses and associated display name that will be used as a From header field value in all emails sent by users of the domain, with the exception of outer From in Draft & Release messages.

If this option is not set or set to empty value and **Organizational messaging LDAP configuration** is set to false, Organizational Messaging is not enabled for the domain.

Administrators should use Cobalt to configure Organizations in LDAP, as that provides more flexibility.

By default the list is empty, which means that no domain-wide Organization is defined for the domain.

Old (3.X) configuration: `<org_address>`

Address

Email address

Name

Optional associated organisation name - when empty Harrier will try to get the name from corresponding directory entry (first LDAP user name attribute).

2.8.3.7 SIC

Subject Indicator Codes

Definitions file

Subject Indicator Codes definition XML file (Catalog).

Default value: `sample_sics`

Old (3.X) configuration: `<sics>`

Required

Specifies whether every message sent from Harrier requires at least one SIC code to be included.

Note that this option should only be used in the `Military` or `ACP 127` mode, as there is no way of entering SICs in the `Internet` mode.

Default value: `Off`

Old (3.X) configuration: `<sic_required>`

Maximum number

Specifies the maximum number of SICs that can be included in a message. The user will be prevented from sending a message if it contains more than the specified number of SICs.

The `0` value means no limit.

Old (3.X) configuration: `<sic_max>`

2.8.3.7.1 Rules

Rule for automatically inserting a Subject Indicator Code into a message being composed.

Code

(i.e.: "AAA", "ADA" ...)

Old (3.X) configuration: `<sic_rule>`

Label selector

Selector string for an ESS label. If this label matches the security label set on a message, then the associated Subject Indicator Code will be inserted into the message. (i.e.: "Demo|Cosmic Top Secret")

Old (3.X) configuration: `<sic_rule label="">`

Raw label

Alternative to label option with raw ESS label. If this label matches the security label set on a message, then the associated Subject Indicator Code will be inserted into the message.

Old (3.X) configuration: `<sic_rule raw_label="">`

Handling instructions

Substring that should appear in the Handling Instructions compose field for the associated Subject Indicator Code to be inserted into the message. (i.e.: "PERSONNEL")

Old (3.X) configuration: `<sic_rule handling_instructions="">`

2.8.3.8 SIO

Security Information Objects (SIO) are used to define security labels and policies for use in military messaging. The SIOs are defined in XML files. Security labels can be applied to messages, and the policies and security clearances are used to determine whether a message can be sent to a particular recipient.

Note that these options are ignored for `Internet` mode.

Labels catalog

Security labels catalog XML file.

When a user composes a message, this catalog is used to populate the list of available security labels presented to the user.

This option is ignored unless a policy has been configured (see **Policies**).

Old (3.X) configuration: `<sio_catalog>`

Policies

Security policy information XML files.

Used when interpreting security labels that are presented to the user, either when composing a message or when viewing a message that has been received.

Old (3.X) configuration: `<sio_policy>`

Clearances catalog

Security clearances catalog XML file.

Old (3.X) configuration: `<sio_clearances>`

Clearance check

Option controls whether the clearance check is performed on message send. Harrier will display a modal dialog if one or more recipients doesn't have clearance compatible with the currently selected security label.

Default value: `Off`

Old (3.X) configuration: `<sio_clearance_check>`

Clearance check failure is an error

Treat clearance check failure as an error when sending emails

Default value: `Off`

Old (3.X) configuration: `<sio_clearance_check_fail_is_error>`

Use STANAG 4778

Prefer STANAG 4778 Binding-Data over sio-label.

Default value: `Off`

Old (3.X) configuration: `<sio_use_tn1491>`

Demo succeeding label subject

Enable dev/test/demo hack which injects sample succeeding label (STANAG 4778) to composed messages on given subject. This is being used only when "Use STANAG 4778" is enabled and CWIX19 demo labels catalog and policy, and server working in London's time zone!!!

Default value: Empty - injection disabled.

Example value: samplesl

Available only if: **Use STANAG 4778** is enabled.

Old (3.X) configuration: `<demo_succeeding_label_subject>`

2.8.3.8.1 Clearance map

Allows to override user's clearance. Each map item describes which Clearance applies to a specific pattern of recipients.

Old (3.X) configuration: `<sio_clearance_map>`

Pattern

`Regular expression (case insensitive)` - See http://cplusplus.com/reference/regex/ECMAScript for more detailed information about regular expressions.

Pattern used to match recipient email address.

Example value:

User: "`alfa@example\.com`"

Domain: "`.*@example\.com`"

Name

The clearance item name as defined in the clearance catalog (for example: "DEMO-NATO SECRET")

Override

Off = use this clearance as default in case of lack clearance in user's directory entry
On = enforce using this clearance even if there is clearance in user's directory entry

Default value: `Off`

2.8.3.9 S/MIME

This section describes configuration options that can be used to control S/MIME. Harrier supports S/MIME signing of outgoing email, signature verification on incoming email, email encryption/decryption, as well as automatic issuance of user certificates.

Sign

This option controls whether or not by default, all messages sent by users of the domain will be S/MIME signed. This option can be overridden by setting the harrierSmimeSign LDAP attribute to TRUE in user's entry.

In order to be able to S/MIME sign email, Harrier server needs to have LDAP access configured for the domain, it needs to have read access to the userPKCS12 attribute in the user's LDAP entry (which contain PKCS#12 object encrypted with user's login password) and/or to have read access to harrierSignIdentity & userCertificate attributes in the role's LDAP entry (when HSM/PKCS#11 is used).

Default value: `Off` - which means that outgoing messages from the domain will not be S/MIME signed, unless explicitly enabled for a user account in LDAP.

Old (3.X) configuration: `<smime_sign>`

Sign policy

S/MIME signing policy that is applied to messages being sent in military modes. "Never" - Never S/MIME sign any messages being sent. "If Possible" - Attempt S/MIME signing messages if a non expired certificate exists for the role, but fall back to sending unsigned messages otherwise. "Always" - Always S/MIME sign messages. Fail to send messages if there is no unexpired certificate for the role.

Options:

- `Never` - Never S/MIME sign any messages being sent.
- `If possible` **[default]** - Attempt S/MIME signing messages if a non expired certificate exists for the role, but fall back to sending unsigned messages otherwise.
- `Always` - Always S/MIME sign messages. Fail to send messages if there is no unexpired certificate for the role.

Old (3.X) configuration: `<smime_sign_policy>`

Encrypt

This option controls whether or not by default, all messages sent by users of the domain will be S/MIME encrypted. This option can be overridden by setting the harrierSmimeEncrypt LDAP attribute to TRUE in user's entry. In order to be able to S/MIME encrypt an email message, Harrier server needs to have LDAP access configured for the domain, it needs to have read access to userPKCS12 attribute in user's LDAP entry (which contain PKCS#12 object encrypted with user's login password) or to have read access to harrierSignIdentity attribute in role's LDAP entry (when HSM/PKCS#11 is used), and each recipient of the message must have S/MIME certificate published in userCertificate attribute of her respective LDAP entry. Note that expired certificates and certificates that don't correspond to the current From email address (in userPKCS12/userCertificate) are ignored when deciding whether a particular user can send encrypted or receive encrypted email.

Default value: `Off` - which means that outgoing messages from the domain will not be S/MIME encrypted, unless explicitly enabled for a user account in LDAP.

Old (3.X) configuration: `<smime_encrypt>`

Encrypt policy

S/MIME encryption policy that is applied to messages being sent in military modes. "Never" - Never S/MIME encrypt any messages being sent. "Sign + Encrypt" - Sign and encrypt all messages being sent. "Triple Wrap" - Triple wrap all messages being sent.

Options:

- `Never` **[default]** - Never S/MIME encrypt any messages being sent.
- `Sign + encrypt` - Sign and encrypt all messages being sent.
- `Triple wrap` - Triple wrap all messages being sent.

Old (3.X) configuration: `<smime_encrypt_policy>`

Show unsigned messages

Whether or not unsigned S/MIME messages should be highlighted in Harrier Web.

Default value: `Off`

Encrypt algorithm [advanced]

Symmetric cipher used for encrypting S/MIME messages.

Default value: `aes-128-cbc`

Old (3.X) configuration: `<smime_encrypt_algorithm>`

Protect header

This option controls whether or not by default, headers of email messages are protected from changes in transit and disclosure to unintended readers. This is done by wrapping any to-be-signed/to-be-encrypted email message within message/rfc822 MIME body part in order to apply S/MIME security services to the message header fields. This procedure is described in RFC 5751, however it is not always implemented by common Email Clients. Administrator should set this option to false if compatibility with common Email clients such as Thunderbird or Apple Mail is required at the expense of less secure handling of S/MIME email messages.

This option can be overridden by setting harrierHeaderProtect LDAP attribute in user's entry. This option is ignored, unless S/MIME signing and/or encryption is also enabled for the user.

Default value: `On` - which means that header of outgoing messages from the domain will be S/MIME protected, unless explicitly disabled for a user account in LDAP.

Old (3.X) configuration: `<smime_protect_header>`

Triple wrap

This option controls whether or not by default, all messages sent by users of the domain will be S/MIME triple-wrapped, which means signed, then encrypted, then signed again. You can find more information about triple-wrap in RFC 2634. In order to be able to S/MIME triple-wrap an email message, Harrier server needs to have LDAP access configured for the domain, it needs to have read access to userPKCS12 attribute in user's LDAP entry (which contain PKCS#12 object encrypted with user's login password) or to have read access to harrierSignIdentity attribute in role's LDAP entry (when HSM/PKCS#11 is used), and each recipient of the message must have S/MIME certificate published in userCertificate attribute of her respective LDAP entry. Note that expired certificates and certificates that don't correspond to the current From email address (in userPKCS12/userCertificate) are ignored when deciding whether a particular user can send triple-wrapped or receive triple-wrapped email.

This option is automatically set to false if S/MIME signing and/or S/MIME encryption is explicitly disabled or not configured.

Default value: `Off` - which means that outgoing messages from the domain will not be S/MIME triple-wrapped.

Old (3.X) configuration: `<smime_triple_wrap>`

Auto decrypt [advanced]

Whether Harrier should perform automatic decryption of S/MIME encrypted messages.

Default value: `Off`

Old (3.X) configuration: `<smime_auto_decrypt>`

ESS security label [advanced]

Whether Harrier should embed ESS Security Labels in S/MIME SignedData instead of using SIO-Label header field.

Default value: `Off`

Old (3.X) configuration: `<smime_ess_sec_label>`

Certificate expiration warning period [advanced]

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Warning period before orignator certificate expiration.

Default value: `7d`

Old (3.X) configuration: `<smime_cert_expiration_warning_period>`

Auto generate CSRs

This option controls whether or not Certificate Signing Requests (CSR) are generated for users that don't have any valid S/MIME certificate in userPKCS12 attributes of their LDAP entries. If this option is enabled, S/MIME certificates corresponding to issued CSRs will also be uploaded to users' LDAP entries.

When this option is enabled for a domain, when a user logs in for the first time, CSR is generated in the **CSR auto-generation path** directory and the corresponding private key is saved in the **P12 auto-generation path** directory. At suitable intervals, a suitably privileged administrator should review pending CSRs, and either issue certificates for them (using a tool such as Sodium CA), or submit them to an external CA. Once certificates are generated and saved in the **CSR auto-generation path** directory, the subsequent login attempt by the user will update the PKCS#12 file to include the user's certificate and upload both PKCS#12 file and certificate to the userPKCS12 and userCertificate attributes (respectively) in user's LDAP entry. After that, the user will be able to S/MIME sign and/or encrypt her messages.

This option is ignored, unless S/MIME signing and/or encryption is also enabled for the user. When this option is set to true, both **CSR auto-generation path** and **P12 auto-generation path** must be set to non empty values.

Default value: `false` - which means that user S/MIME certificate requests will not automatically be generated.

Old (3.X) configuration: `<smime_auto_generate_csrs>`

Elliptic curve name [advanced]

S/MIME Elliptic Curve name to use for automatic generation of S/MIME private keys. The default value is "" which means that an RSA key pair should be generated instead. Use one of the curves listed in "openssl ecparam -list_curve"

Default value: Empty - which means that an RSA key pair should be generated instead. Use one of the curves listed in "`openssl ecparam -list_curve`"

Example value: `secp256k1`

Available only if: **Auto generate CSRs** is not empty.

Old (3.X) configuration: `<smime_ec_name>`

Key size [advanced]

S/MIME RSA key size (in bits) when S/MIME private keys are automatically generated.

This option is ignored when the **Elliptic curve name** [advanced] is set to a non empty value.

The `0` value means RSA default (2048 bits).

Default value: `2k`

Available only if: **Auto generate CSRs** is not empty.

Old (3.X) configuration: `<smime_key_size>`

CSR auto-generation path

`Folder Path` - You can use variables in the path.

Filesystem directory where S/MIME CSRs will be generated by Harrier Web Server and where the corresponding certificate (PEM) files should also be saved. (The directory must exist)

This option is ignored, unless S/MIME signing and/or encryption is also enabled for the user and **Auto generate CSRs** is enabled.

Default value: `$(harrier.dir.var)/csr`

Example value: `$(harrier.dir.var)/csr`

Available only if: **Auto generate CSRs** is not empty.

Old (3.X) configuration: `<smime_csr_path>`

P12 auto-generation path

`Folder Path` - You can use variables in the path.

Filesystem directory where S/MIME private keys and final PKCS#12 files (which also include the corresponding certificates and certificate chains) will be generated by Harrier Web Server. (The directory must exist)

This option is ignored, unless S/MIME signing and/or encryption is also enabled for the user and **Auto generate CSRs** is enabled.

Default value: `$(harrier.dir.var)/pkcs12`

Example value: `$(harrier.dir.var)/pkcs12`

Available only if: **Auto generate CSRs** is not empty.

Old (3.X) configuration: `<smime_pkcs12_path>`

2.8.3.10 SMTP server

SMTP server options defines how Harrier connects to SMTP server.

Primary URL

`SMTP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The primary SMTP server URL. A URL must start with "smtp://" and be followed by the <host>:<port> - for example, "smtp://myserver.example.com:587". The typical port is 587 for "smtp". The substring $(domain) will be replaced by the current domain configuration Selector value.

Default value: `smtp://$(domain):587`

Old (3.X) configuration: `<smtp_url>`

Backup URL

`SMTP/S URL` - Option supports `$(domain)` variable specified by current domain configuration **Domain name or pattern** value.

The backup SMTP server URL. A URL must start with "smtp://" and be followed by the <host>:<port> - for example, "smtp://myserver.example.com:587". The typical port is 587 for "smtp". The substring $(domain) will be replaced by the current domain configuration Selector value.

Old (3.X) configuration: `<smtp_url>`

STARTTLS policy

Controls use or non use of STARTTLS.

Options:

- `License` **[default]** - Depending on license-activation - When TLS sub-feature is activated the default is `Opportunistic`, and `Suppress` otherwise.
- `Mandatory` - Always use STARTTLS, fail the connection if not advertised.
- `Opportunistic` - Try to use STARTTLS if advertised, but carry on regardless of STARTTLS success.
- `Suppress` - Never use STARTTLS, even if advertised.

Old (3.X) configuration: `<smtp_starttls_policy>`

Trust anchors

Connections to the SMTP server using TLS, will fail unless the SMTP server's certificate can be verified against these trust anchors.

(see: Section 2.9, “Certificate Verification”)

Specifying this option forces Harrier Web Server to use `StartTLS` for all SMTP connections, and to require that the SMTP server provides a certificate which can be verified using this set of CA certificates.

Old (3.X) configuration: `<smtp_server_trustanchors>`

Pinned certificates

If SMTP server certificate is not issued by any trusted CA pinned certificates allows to specify trustworthy certificates directly.

(see: Section 2.9, “Certificate Verification”)

Old (3.X) configuration: `<smtp_server_pinned>`

Allow PLAIN over clear text [advanced]

Controls whether authentication using the PLAIN or the LOGIN SASL mechanisms can be used without TLS in SMTP.

Default value: `Off`

Old (3.X) configuration: `<smtp_plain_over_cleartext>`

TLS SNI [advanced]

TLS Server Name Indication (SNI) extension value, in the format of a hostname. This is required by some SMTP servers to connect. In most cases this value should be the same as the host part of the "Primary URL". The default is empty, which means that TLS SNI extension shouldn't be used.

Old (3.X) configuration: `<smtp_tls_sni>`

2.8.3.11 User interface

User interface

Allow active content [advanced]

Control whether there is any blocking of <script> or Javascript: URIs when displaying messages.

Default value: `On`

Old (3.X) configuration: `<ui_active_content>`

Preferences template [advanced]

Default user interface preferences (JSON file).

Default value: `default_user_prefs`

Old (3.X) configuration: `<user_preferences>`

Show processed flag

Whether or not Harrier should display processed/unprocessed status for messages.

Options:

- `Mode default` **[default]** - Depending on selected **Mode**

  in military modes: `On`

  in the `Internet` mode: `Off`
- `On`
- `Off`

Old (3.X) configuration: `<show_processed_flag>`

Limit charset

Specifies if composition of messages should restrict the user to a limited set of characters.

This option has no effect in the `Internet` mode.

Options:

- `No restriction` **[default]**
- `IA5` - 7-bit character encoding corresponding to International Reference Alphabet (IRA). See http://www.itu.int/rec/T-REC-T.50-199209-I/en/
- `ITA2` - 5-bit character encoding. See https://en.wikipedia.org/wiki/Bauddot_code#ITA2.

Old (3.X) configuration: `<limit_charset>`

Allow HTML editing in compose window

Whether or not Harrier should allow editing of message bodies as HTML (when true) or plain text (when false).

Default value: `Off`

Message display HTML template file path [advanced]

HTML template used for displaying content of messages.

Default value: `default_mail_display`

Old (3.X) configuration: `<message_display_template>`

Message print HTML template file path [advanced]

Option controls what appears on the message print tab and how message information is formatted. It contains path to the message print Twig template, which is basically HTML file with special control operators to control insertion of different fields from message, such as message subject, message recipients, S/MIME verification status or message content.

Default value: `default_mail_print`

Old (3.X) configuration: `<message_print_template>`

Military sort order

Whether or not the server should apply military sort order to INBOX in any of military modes. This option has no effect in the "Internet" mode.

Default value: `On`

Old (3.X) configuration: `<military_sort_order>`

Disallow message and folder deletion in military modes

Whether or not the server should allow message and folder deletion in any of military modes. This option has no effect in the "Internet" mode.

Default value: `Off`

Military time zone

The following option controls how date/time is shown in any of military modes. Allowed values are "zulu" (the default, all date/times are shown in UTC, e.g. "211701Z Dec 2021") or "server" (server local timezone, e.g. "211901H Dec 2021"). This option has no effect in the "Internet" mode.

Options:

- `Zulu` **[default]**
- `Server`

Old (3.X) configuration: `<military_timezone>`

Precedence set

Specifies which precedence values can be selected in Compose in military modes.

Options:

- `Mode default` **[default]** - Depending on selected **Mode**

  in the `Military` and `Internet` mode: `STANAG 4406`

  in the `ACP 127` mode: `ACP 127`
- `STANAG 4406` - all 6 precedence values are available.
- `ACP 127` - 4 precedence values are available: ROUTINE, PRIORITY, IMMEDIATE and FLASH.
- `ACP 127 + Emergency` - 4 "ACP 127" values + EMERGENCY (which is mapped to OVERRIDE).

Old (3.X) configuration: `<precedence_set>`

Print allowed

Option controls presence of the print button in message view. When enabled and the user presses the print button, Harrier would open a new message print tab in browser and would show message print dialog.

Default value: `On`

Old (3.X) configuration: `<print_allowed>`

2.8.4 Listeners

Listeners allows to define ports (and addresses in advanced mode) accepting incoming HTTP/S and WS/S requests.

Port

Default port to access HTTP/S and WS/S.

Default value: `9090`

Old (3.X) configuration: `<port>`

TLS mode

Default TLS mode. Specifies if HTTP+WS or HTTPS+WSS are acceptable.

Options:

- `HTTP only` - Accept incoming HTTP and WS requests only (Non TLS).
- `HTTP/S` **[default]** - Accept incoming HTTP and WS as well as HTTPS and WSS requests.
- `HTTP redirected to HTTPS` - Accept incoming HTTP and WS requests and redirects them to HTTPS or WSS respectively.
- `HTTPS only` - Accept incoming HTTPS and WSS requests only (TLS secured).

Available only if: **TLS feature** is activated and **Key pair** is set.

Listeners backlog [advanced]

The maximum length of the queue of pending connections. Default 0 means system default.

Old (3.X) configuration: `<listen_backlog>`

2.8.4.1 Addresses [advanced]

Accept incoming HTTP/S and WS/S requests on the specific address-and-port combinations.

Old (3.X) configuration: `<listen>`

Address (and port)

Listener address and optionally port. If only address is specified it uses defaut port number from "Port" option. The "::" address means unspecified (all) IPv6 and IPv4 addresses (for example [::]:9090 specifies listening on all addresses and port 9090).

TLS mode

TLS mode. Specifies if HTTP+WS or HTTPS+WSS are acceptable. If not specified defaut TLS mode is used.

Has the same values as **TLS mode**.

Available only if: **TLS feature** is activated and **Key pair** is set.

2.8.5 TLS

TLS support used by Web server (HTTPS/WSS)

Available only if: **TLS feature** is activated.

Key pair

This is used when serving over HTTPS if not specified HTTPS is disabled.

Chain certificates

Optional certificate chains. When the server performs a TLS handshake in response to an HTTPS/WSS connection, it sends a certificate chain consisting of its own "Certificate" and all of the "Chain certificates" which have been specified. The order of this option is significant: the first should be the issuer of a "Certificate", the next should be the issuer of that certificate, etc.

Available only if: **Key pair** is specified.

Old (3.X) configuration: `<ssl_chain_certificate>`

Private key size [advanced]

TLS key size (in bits) when TLS private key is automatically generated. The default value is 0 which means RSA default (2048 bits).

Default value: `2048`

Old (3.X) configuration: `<ssl_key_size>`

Cipher list [advanced]

Specifies list of allowed ciphers used by HTTP/S and WebSocket/S server connections.

The list should be in format as described in: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html

Default value: `DEFAULT`

Old (3.X) configuration: `<ssl_cipher_list>`

Diffie-Hellman parameters [advanced]

Specifies a file containing the Harrier Web server's Diffie-Hellman parameters. The file is in PEM format.

In order to perform a DH key exchange the server must use a DH group (DH parameters) and generate a DH key. The server will always generate a new DH key during the negotiation.

As generating DH parameters is extremely time consuming, Harrier Web server doesn't generate the parameters on the fly but uses pregenerated parameters. (A pregenerated DH group is installed as $(harrier.dir.share)/harrier.dhp) DH parameters can be reused, as the actual key is newly generated during the negotiation. The risk in reusing DH parameters is that an attacker may specialize on a very often used DH group. So a particular installation should periodically regenerate their own DH parameters.

In order to regenerate DH parameters, one can run OpenSSL's executable, for example on Linux:

```
% openssl dhparam 2048 > harrier.dhp
```

and upload it into "Other" object store.

Note that this is an advanced option and typically doesn't need to be changed. However system administrators should consider periodically regenerating DH parameters.

Default value: `default_dh`

Old (3.X) configuration: `<ssl_dh_params_path>`

2.8.6 HTTP/S [advanced]

HTTP/S settings

These options control the behaviour of the HTTP/S server which is used to serve static files (such as HTML, CSS, JavaScript, images, etc.) and to provide access to the API required by Harrier Client and Harrier Manager WEB applications.

Access-Control-Allow-Origin

Control for which origins can call JavaScript APIs on the website - default value of the Access-Control-Allow-Origin header field. Should be one of `*`, `null` or <origin> (e.g. "https://example.org"). Special value `$1` can be used as an <origin> constructed from the Host request header field. (The last option is useful if the Web Server serves multiple web domains.)

Default value: `$1`

Old (3.X) configuration: `<access_control_allow_origin>`

CSRF token timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

HTTP CSRF token timeout (0 means disabled - token will be fixed).

Default value: `1h`

Old (3.X) configuration: `<http_csrf_token_timeout>`

Keep alive

Enable HTTP keep-alive support.

Default value: `On`

Old (3.X) configuration: `<http_keep_alive>`

No cache enforcement

Enforce "Pragma: no-cache" in all HTTP responses.

Default value: `Off`

Old (3.X) configuration: `<http_no_cache>`

Open handshake timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

HTTP open handshake timeout (0 means disabled).

Default value: `5s`

Old (3.X) configuration: `<http_open_handshake_timeout>`

Pipeline queue

The length of optional pipeline queue (0 means disabled pipeline support)

Default value: `16`

Old (3.X) configuration: `<http_pipeline_queue_len>`

Read timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Allows to timeout whole request reading (0 means disabled) (should be large for slow links and large request like attachments).

Default value: `5m`

Old (3.X) configuration: `<http_read_timeout>`

Read chunk size

`Size` - Option value (Integer) may contain case insensitive k/m/g suffixes (1k = 1024 etc.).

Allows to setup reading buffer size. It influences partial reading timeout check frequency.

Default value: `16k`

Old (3.X) configuration: `<http_read_chunk_size>`

Read chunk timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Allows to timeout not advancing reading. (0 means disabled checking for partial read timeouts).

Default value: `0` - disabled as it is an expensive option.

Old (3.X) configuration: `<http_read_chunk_timeout>`

Upload size limit

HTTP upload size limit.

Default value: `10M`

Old (3.X) configuration: `<http_upload_size_limit>`

Write timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Timeout for sending response messages. (0 means disabled).

Default value: `5m`

Old (3.X) configuration: `<http_write_timeout>`

Shutdown timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Timeout for graceful HTTP connection shutdown. (0 means disabled) If set it should be shorter than "Shutdown watchdog timeout".

Default value: `3s`

Old (3.X) configuration: `<http_shutdown_timeout>`

2.8.6.1 Path map

Specifies the location in the local filesystem which can be used to resolve URLs from the client.

The default configuration contains a definition for `url="/"` which should not be modified.

`/data/mmhs-types.xml` is used to locate the catalog of MMHS types which are presented to the user when composing a message. The default location for this file is `$(harrier.dir.share)/webapps/harrier/data/mmhs-types.xml`

Old (3.X) configuration: `<http_map>`

URL path pattern

`Optional regular expression (case insensitive)` - The string is automatically converted into regular expression for example "/pub.lic/" is converted into "^/pub\.lic/(.*). If string starts with '^' it is not converted and assumed to be already a regular expression. See http://cplusplus.com/reference/regex/ECMAScript for more detailed information about regular expressions.

Requested URL pattern - Example: /public/ or ^/public/(.+)

Destination file path

Destination path.

Example value: $(harrier.dir.client)public/$1

No cache

Mark this file as not cacheable in HTTP response header.

Default value: `Off`

Process $(lng)

Enable $(lng) variable in the destination path processing. It's value depends on Accept-Language specification in HTTP request header (configurable via web browser langauage preferences).

Default value: `Off`

Authentication required

Authentication is required to access this file.

Default value: `Off`

2.8.7 WS/S [advanced]

WebSocket settings

Buffer size

Specifies the buffer size to be used for websocket connections.

Default value: `64K`

Old (3.X) configuration: `<ws_buffer_size>`

Compression

Enable permessage-deflate extension (compressed transmission).

Default value: `On`

Old (3.X) configuration: `<ws_deflate>`

Handshake timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Handshake timeout (0 means disabled).

Default value: `5s`

Old (3.X) configuration: `<ws_handshake_timeout>`

Inactivity timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Inactivity timeout triggers ping to check if client connection is alive and if there is no response connection is being closed. (0 means disabled).

Default value: `30s`

Old (3.X) configuration: `<ws_inactivity_timeout>`

Shutdown timeout

`Period` - Option value may be defined as a number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks. (i.e. 29m).

Websocket graceful shutdown timeout (0 means disabled) If set it should be shorter than shutdown_watchdog_timeout.

Default value: `3s`

Old (3.X) configuration: `<ws_shutdown_timeout>`

2.8.8 PKCS#11

PKCS#11 - Used by S/MIME. Note that for changes to any option in this section to have an effect, Harrier Server restart is required.

Module path

`File Path` - You can use variables in the path.

Path to the shared library that provides PKCS#11 interface to a software or hardware HSM. Setting this enables PKCS#11 initialization in S/MIME subsystem.

Old (3.X) configuration: `<pkcs11_module_path>`

PIN

HSM-specific PIN.

Old (3.X) configuration: `<pkcs11_pin>`

Initialization arguments

PKCS#11 specific initialization arguments.

Old (3.X) configuration: `<pkcs11_init_args>`

2.8.9 Proxy

Reverse proxy passing request to new URI and responses back to the client.

Old (3.X) configuration: `<proxy_map>`

Request path

`Optional regular expression (case insensitive)` - The string is automatically converted into regular expression for example "/pub.lic/" is converted into "^/pub\.lic/(.*). If string starts with '^' it is not converted and assumed to be already a regular expression. See http://cplusplus.com/reference/regex/ECMAScript for more detailed information about regular expressions.

Request path pattern.

Old (3.X) configuration: `<proxy_map pattern="">`

Destination URI

URI used in modified request (header and target). The response returned will be passed back to the original client. Regex capturing groups may be inserted into new URI via ${N} variables, where N is the number of capturing group.

Old (3.X) configuration: `<proxy_map uri="">`

2.8.10 S/MIME

This section contains options that can be used to control S/MIME.

Harrier supports S/MIME signing of outgoing email, signature verification on incoming email, email encryption/decryption, as well as automatic issuance of user certificates.

Most of the S/MIME related settings are configured per domain (See Section 2.8.3.9, “S/MIME”) but few of them must be the same for all domains so they are configured under top level element and treated as global option shared by all domains

OCSP/CRL check

Perform S/MIME OCSP/CRL checks when determining message signature status.

Default value: `On`

Old (3.X) configuration: `<smime_crl_check>`

Trusted certificates

Trusted certificates. For S/MIME signature verification, one or more trusted certificates (for trusted anchors) and zero or more "Intermediate certificates" can be specified. For verification to succeed, all trust anchors and intermediate certificates must be included.

Old (3.X) configuration: `<smime_trusted_certificate>`

Intermediate certificates

Intermediate certificates. For S/MIME signature verification, one or more trusted certificates (for trusted anchors) and zero or more "Intermediate certificates" can be specified. For verification to succeed, all trust anchors and intermediate certificates must be included.

Old (3.X) configuration: `<smime_intermediate_certificate>`

OCSP nonce [advanced]

If enabled, OCSP requests will be made with the nonce extension.

Default value: `Off`

Old (3.X) configuration: `<smime_ocsp_nonce>`

OCSP responder [advanced]

The filename of a DER-encoded certificate that will be trusted as a signer of OCSP responses.

Old (3.X) configuration: `<smime_ocsp_responder>`

OCSP URI [advanced]

Basic OCSP responder URI (http or https) that will be used for OCSP requests.

Old (3.X) configuration: `<smime_ocsp_uri>`

Avoid CRL URI [advanced]

If enabled then CRLs will not be retrieved from URIs in CRL or ARL Distribution Point extensions, or from freshestCRL extensions.

Default value: `Off`

Old (3.X) configuration: `<smime_avoid_crl_uri>`

Avoid OCSP URI [advanced]

If enabled then URIs from certificate extensions will not be used for OCSP.

Default value: `Off`

Old (3.X) configuration: `<smime_avoid_ocsp_uri>`

2.8.11 Manager

Manager application access settings.

Port

Port to access mananager application

Default value: `9095`

Login

Manager login (letters, numbers and symbols other than " ' & : < > @ and / are allowed).

Password

Manager password (no character restrictions).

2.8.12 Product Activation [advanced]

Product activation. (These options are read-only)

TLS feature

TLS feature is activated.

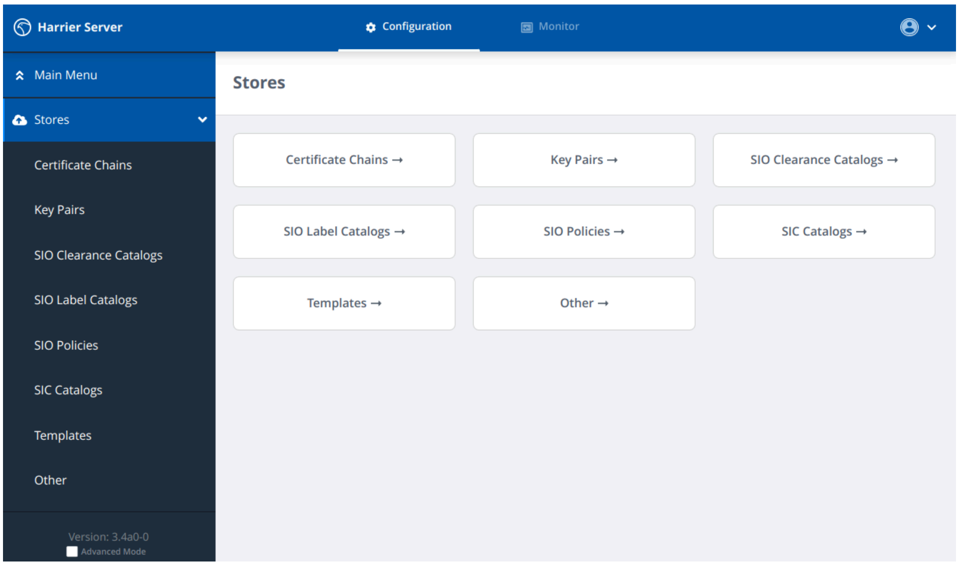
Encrypt feature

S/MIME encryption and decryption feature is activated.

2.8.13 Stores

There are a possible number of stores which the server has access to that provide a mechanism to keep slightly larger elements that the server may need.

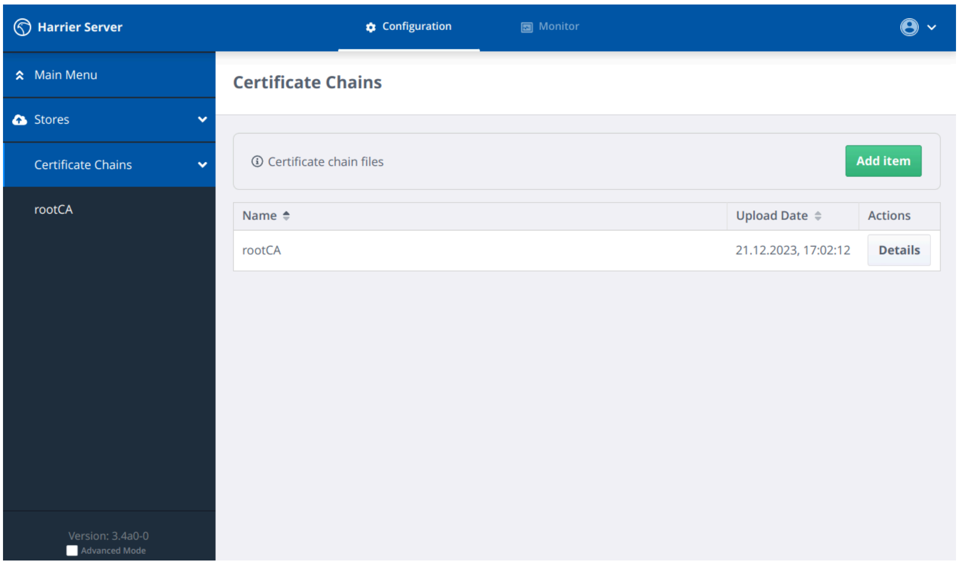
Figure 2.6. Stores Configuration Options



2.8.13.1 Certificate Chains

This is the storage of certificate chains which can be used as trust anchors, pinned certificates, etc.

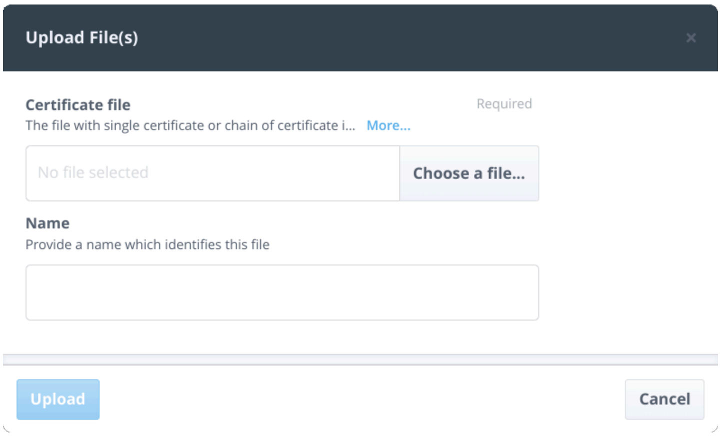
Figure 2.7. Certificate Chains Store Options



Name	Upload Date	Actions
rootCA	21.12.2023, 17:02:12	Details

New certificate chain entries can be added with the **Add Item** button.

Figure 2.8. Certificate Chain Upload Dialog



Certificate file Required

The file with single certificate or chain of certificate i... More...

No file selected

Name

Provide a name which identifies this file

Certificate file
: This will be the file containing the Certificate or Certificate Chain in PEM format.

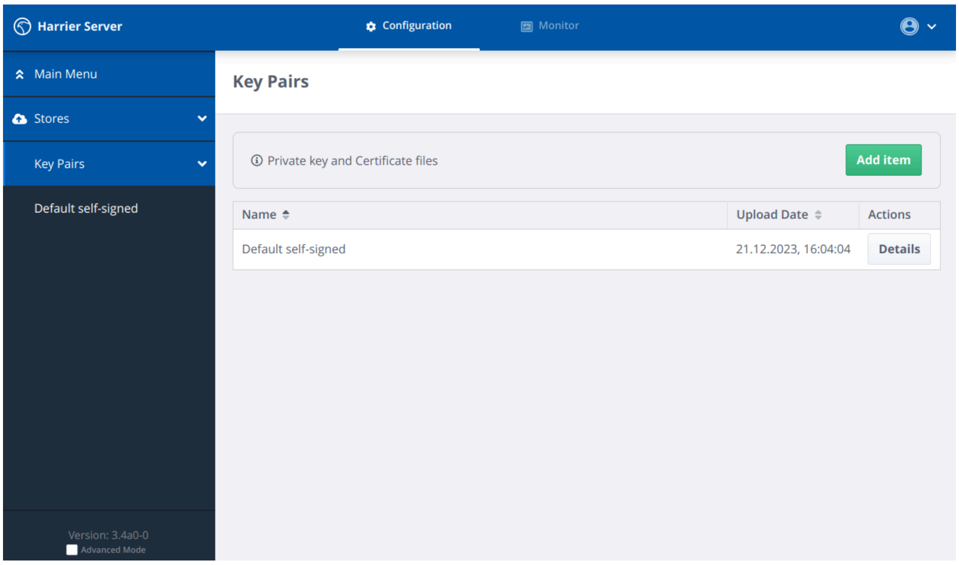
Name
: The Name of the entry. This must be without spaces or non-ascii characters to identify it. It must also be unique.

2.8.13.2 Key Pairs

This is the storage for bundle of private key, password and public key required. It is used to support TLS encryption of the Web server (HTTPS) as well as message encryption/ signing.

If only Harrier is activated with TLS support there will be always up-to-date self-signed certificate key pair which can be used for HTTPS.

Figure 2.9. Key Pair Store Options



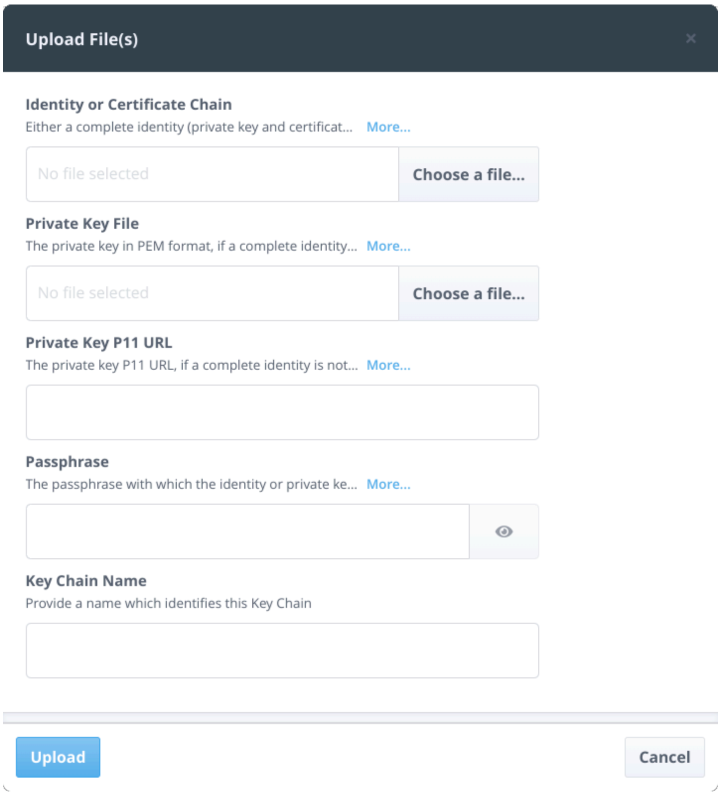
Key Pairs

ⓘ Private key and Certificate files

Name	Upload Date	Actions
Default self-signed	21.12.2023, 16:04:04	Details

New certificate chain entries can be added with the **Add Item** button.

Figure 2.10. Key Pair Upload Dialog



Upload File(s)

Identity or Certificate Chain
Either a complete identity (private key and certificat... More...

No file selected

Private Key File
The private key in PEM format, if a complete identity... More...

No file selected

Private Key P11 URL
The private key P11 URL, if a complete identity is not... More...

Passphrase
The passphrase with which the identity or private ke... More...

Key Chain Name
Provide a name which identifies this Key Chain

Identity or Certificate Chain
: Either a complete identity (private key and certificate chain) or a certificate chain, in PEM or P12 format.

Private Key File
: The private key in PEM format, if a complete identity is not being provided and the private key is not stored in a PKCS#11 token.

Private Key P11 URL
: The private key P11 URL, if a complete identity is not being provided and the private key is stored in a PKCS#11 token.

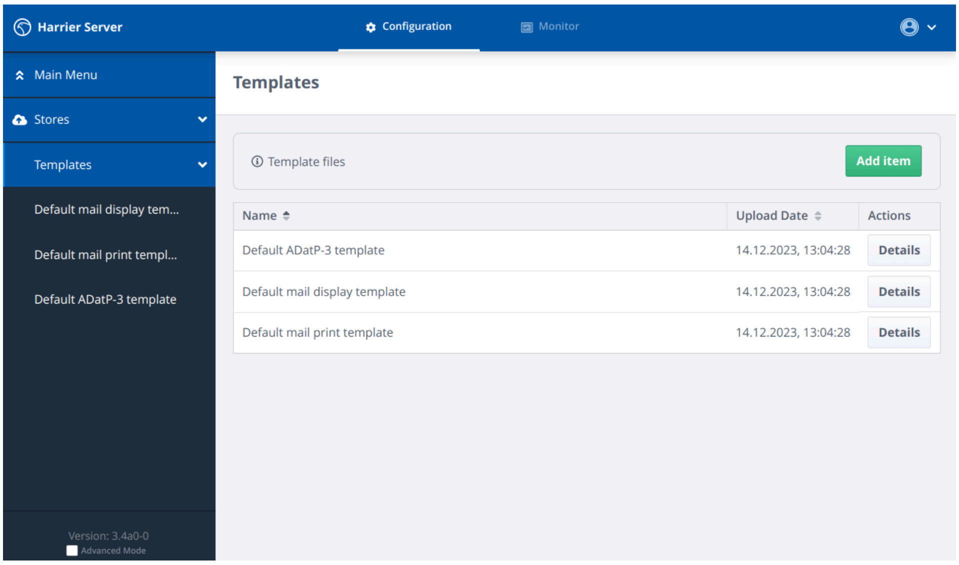
Passphrase
: The passphrase with which the identity or private key has been encrypted (if any).

Key Chain Name
: Provide a name which identifies this Key Chain. This must be without spaces or non-ascii characters to identify it. It must also be unique.

2.8.13.3 Other

There are also other (generic) stores which are used for specific purposes. All of them just keep files: SIO Clearance Catalogs, SIO Label Catalogs, SIO Policies, Templates, Others.

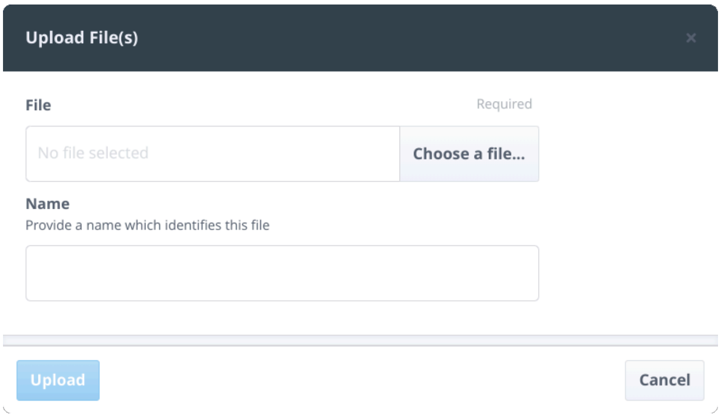
Figure 2.11. Templates Store Options



Name	Upload Date	Actions
Default ADatP-3 template	14.12.2023, 13:04:28	Details
Default mail display template	14.12.2023, 13:04:28	Details
Default mail print template	14.12.2023, 13:04:28	Details

New file entries can be added with the **Add Item** button.

Figure 2.12. File Upload Dialog



File

This will be the file which extension may be differently limited in each store.

Name

The Name of the file entry. This must be without spaces or non-ascii characters to identify it. It must also be unique.

2.9 Certificate Verification

A certificate which is presented as part of a TLS handshake is verified via a multi-stage process. The first stage takes place during the handshake itself, and checks (among other things) that the certificate has been signed by one of the Trust Anchors which have been configured for the current TLS context. Even if the certificate fails one or more of these checks, the TLS handshake may still complete successfully, with an encrypted TLS session being established.

Once the TLS handshake is complete, secondary checks are performed on the presented certificate, if the configuration of the domain or link requires a valid certificate. These are:

- If a Pinned Certificate is configured, the results of the first-stage verification are ignored and a direct comparison between this and the presented certificate is performed. If they match, the presented certificate is considered valid. If they do not match, the presented certificate is considered invalid. In either case, no further verification of the presented certificate is performed.

- A check of the result of the first-stage verification, described above. If this first-stage verification has failed, no further action is taken, and the certificate is considered invalid.
- If the appropriate checks described above succeed, the certificate is considered valid.

A certificate can contain multiple Subject Alternative Names, of varying types. When attempting to match a domain name, DNS name or hostname against these, a number of different comparisons are performed:

- A match against one of the certificate's DNS Names. This includes wildcard matching, so that a certificate with a DNS Name of `*.isode.com` would match `mary.isode.com`.
- If the certificate has no other Subject Alternative Names, a match against one of the certificate's Common Name values.

2.10 Trust Anchors

Trust Anchors are certificates which identify trusted signing entities. These are used by Harrier to verify that a chain of certificates (up to and including an end-entity certificate) received from another IMAP/SMTP/LDAP server or client is valid.

Most operating systems provide a built-in set of Trust Anchors which identify commercial Certification Authorities. The location and format of these is system-specific. By default, Harrier will make use of these Trust Anchors. Use of system Trust Anchors can be overridden via configuration of particular servers.

A set of private Trust Anchors may be specified as part of Harrier's configuration, across the whole installation. Use of private Trust Anchors is required when the end-entity certificates being presented have been signed by Certification Authorities whose CA certificates are not configured as part of the operating system.

2.11 Server Modes

Harrier Web Server can be configured to run in one of three separate server modes.

2.11.1 General Purpose ("Internet") Mode

Harrier can operate as a general purpose SMTP/IMAP client, providing a high performance easy to use Web interface to an IMAP/SMTP service. Harrier provides a useful set of general purpose email capabilities, but in addition will display any MMHS military headers (including security labels, message types, expires, reply-by, deliver-by etc.) that are present on received messages.

Internet mode is configured using the *mode* option in the configuration file. See **Mode**.

2.11.2 Military Mode

In Military mode, *To* and *CC* recipients are always labelled as *Action* and *Info* respectively.

Users are able to specify values for the following fields when composing a message:

- Priorities can be specified for Action and Information recipients
- Exempted recipients can be specified
- Zen Action and Zen Info recipients can be specified
- Security Label selection and display
- SIC (Subject Indicator Code) support with server side configuration of SIC catalogue. See **Definitions file**.
- Message Type support with server side configuration of MMHS types catalogue. See mmhs-types at Section 2.8.6.1, “Path map”.
- Time controls (Filing Time; DTG; Expires; Reply-By; Deliver-By)
- Handling and Message Instructions can be specified
- Line length and charset can be restricted (e.g. to interoperate with ACP 127 recipients). See Section 2.11.3, “ACP127”. The Server returns limits per recipient in response to ldap-address-book command. Client restricts charset/line length/ attachments in the compose window.

Other changes from internet mode:

- The "Junk" folder is not visible
- Priorities are displayed in the list of messages in a folder.
- All dates are displayed in DTG format
- Some IMAP keywords can't be set, such as TODO, Later, Work.
- By default, military sort order is used, unless disabled in configuration. Military sort order sorts first by the precedence, then by delivery date, then by message UID. See **Military sort order**

Military mode is configured using the *mode* option in the configuration file. See **Mode**.

2.11.3 ACP127

ACP127 mode is largely the same as *Military* mode, with some additional changes/ restrictions:

- Both in scan listing and Compose window addresses are presented as ACP 127 PLA (Plain Language Address) and RI (Routing Indicator) as "hints". SMTP addresses are hidden from the user.
- When composing a message lines are limited to 69 characters.
- When composing a message character set is restricted to ITA2 or IA5 (ASCII). The default is IA5.
- When composing a message attachments are disabled.
- Display names for senders and recipients are searched for in the LDAP directory.
- Forwarding is disallowed (as attachments are disallowed).
- DEFERRED and OVERRIDE priorities are not supported.

ACP127 mode is configured using the *mode* option in the configuration file. See **Mode**.

2.12 Logging

Harrier Web Server generates event and audit logs. When it starts, the server looks for the file *harrierlogging.xml* (first in *`(ETCDIR)`* and then *`(SHAREDIR)`*). If this file is found, it is used to determine where and what types of log records should be preserved.

The version of *(SHAREDIR)/harrierlogging.xml* provided by Isode will cause Harrier to generate event and audit log files in *(LOGDIR)*.

To modify the default logging settings for the Harrier Web Server application, you should do the following:

Copy the file *(SHAREDIR)/harrierlogging.xml* into *(ETCDIR)harrierlogging.xml*, and then use the Log Configuration tool to make changes to the file in *(ETCDIR)*.

On Windows, a shortcut to the Log Configuration Tool will have been set up in the Isode folder on your Start menu.

On Unix, run */opt/isode/sbin/logconfig*.

Once the GUI is running, open *(ETCDIR)harrierlogging.xml*. You will see a display of a number of predefined logging streams used by the Harrier Web Server, which can be modified as required.

2.13 Storing passwords

The *(ETCDIR)/harrier_web_conf.xml* file which configures how Harrier Web Server connects to other servers can contain passwords and other sensitive data.

These values will be obfuscated by the "servpass" facility, which means that while the server is able to decrypt and use them when necessary, there is no way for the user to obtain the original values; they should be treated as "write-only".

Once the Harrier Server performs encryption, the passwords and other sensitive data in the configuration file will no longer be stored in plain text, and will appear something like this:

```
<password>{spcrypt3}rnak0U/xxDw6W/P8lF+MN+f/
lUf0AK0C7Ln1vjDs8U7ZB2CyBQ==</password>
```

Chapter 3 Features

This section talks about certain features and how they are configured.

3.1 User and Role configuration/preferences in LDAP

Harrier Web Server relies on user specific information stored in LDAP in order to implement some features, such as Section 6.1.2.1, “S/MIME signing/encryption/triple-wrap” or Section 3.6, “Recipients Capability”.

In order to be able to use full functionality provided by Harrier, you must ensure all user entries have the **isodeHarrierUser** auxiliary object class. This is typically combined with the **person** or the **inetOrgPerson** structural object class.

If you use Roles, you must ensure all role entries have the **isodeHarrierRole** auxiliary object class. This is typically combined with the **inetOrgRole** structural object class.

3.2 Security Labels

Harrier Web Server supports security labels for messages as per RFC 7444 [https://www.rfc-editor.org/rfc/rfc7444.html]. When viewing a message that contains a security label, that label will be always shown to the user. When Harrier is suitably configured, then users will be able to select a security label to be applied to any message that they compose (*military* and *ACP127* modes only).

If a security policy and label catalog are configured (see the Section 2.8.3.8, “SIO”), then users will be able to select a label when composing a new message. The catalog contains the labels which will be presented to the user; the policy contains information about how each label should be displayed (name and colors). A sample policy and label catalog are provided in

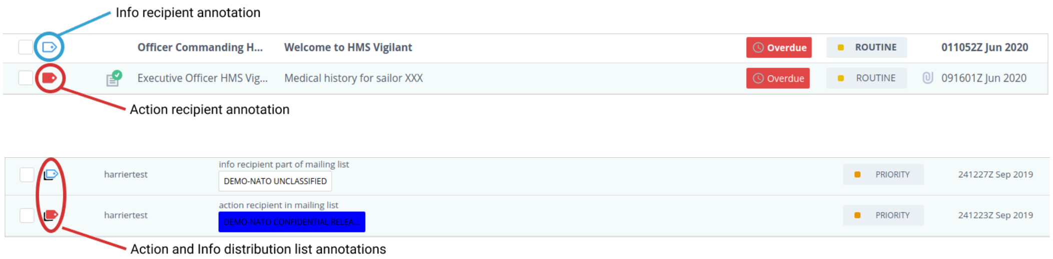
```
$(SHAREDIR)/policy.xml
$(SHAREDIR)/label_catalog.xml
```

3.3 Recipient Type annotation

Each message displayed by Harrier Web is annotated to show whether you are an *action* recipient (you need to do something about this message) or *info* recipient (this message is for your information). No icon will appear if the recipient is BCCed or in some uncommon cases. This feature enables the user to get a better understanding of which message needs action and which is just informative. The annotation can also help the user get a better understanding if the message was sent directly to them or they received it as part of a distribution list.

On the scan-list, the user can look at all of the messages and see the recipient type as an icon.

Figure 3.1. Scan-list view of recipient type bar


Info recipient annotation

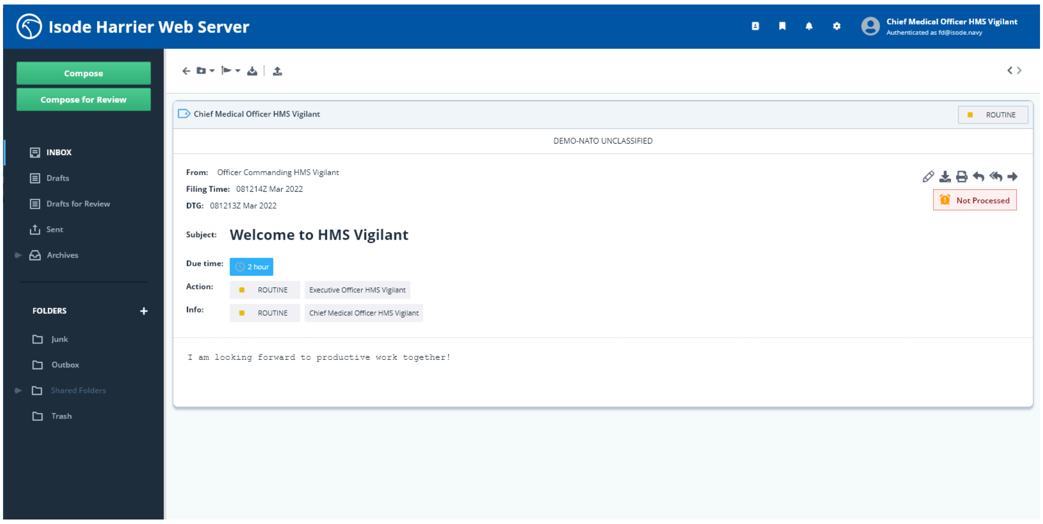
Action recipient annotation

Action and Info distribution list annotations

Officer Commanding H... | Welcome to HMS Vigilant | Overdue | ROUTINE | 011052Z Jun 2020
Executive Officer HMS Vig... | Medical history for sailor XXX | Overdue | ROUTINE | 091601Z Jun 2020
harriertest | info recipient part of mailing list | DEMO-NATO UNCLASSIFIED | PRIORITY | 241227Z Sep 2019
harriertest | action recipient in mailing list | PRIORITY | 241223Z Sep 2019

For example, if the user sees the action recipient annotation in the scan-list they would have to take action on the message. Whereas, if they see the info recipient annotation, they know that this is not as urgent on their side since the message serves more of an informative purpose. And if it is one of the action/info distribution annotations, that would mean that they have received the message as part of a mailing list. On the scan-list, the user can hover over the icon to get more information and on an opened message this is presented with more detail. On the message pane, this information is displayed in a bar at the top of the message.

Figure 3.2. Message pane view of recipient type bar



From: Officer Commanding HMS Vigilant
Filing Time: 081214Z Mar 2022
DTG: 081213Z Mar 2022
Subject: Welcome to HMS Vigilant
Due time: 2 hour
Action: ROUTINE Executive Officer HMS Vigilant
Info: ROUTINE Chief Medical Officer HMS Vigilant

```
I am looking forward to productive work together!
```

3.4 Profiled Messages

Harrier Web Server supports Profiled Messaging in which the messages are redistributed by M-Switch to a set of users depending on the content, and the rules of the Profiler configured in M-Switch.

3.5 Organizational Messaging

Harrier Web Server supports Organizational Messaging. Organizational Messaging allows users to send email messages on behalf of one or more organizations they are associated with, for example an Engineering Officer on a ship HMS Kent sending a message to HQ on behalf of HMS Kent.

Information about Organizations associated with a particular email domain can be provided in either Harrier configuration file and/or retrieved from the configured LDAP server. When storing Organizations in LDAP the mmhsOrganization object class is used.

3.6 Recipients Capability

When operating in *military* or *acp127* mode Harrier Web Server will check any limitations that apply to message recipients. When a user is composing a message they will see the enforced limits at the top of the message content. Invalid content will be highlighted to the user and they will be unable to send the message until this has been corrected.

Limits may be specified on any user entry in the directory which has the objectClass `isodeHarrierUser`, using the attributes described below.

3.6.1 Charset

Description: The charset option can be be set to either `ITA2` or `IA5`

Default value: -None-

Example: ITA2

LDAP attribute name: `harrierCharsetRestrictions`

3.6.2 Max Line Length

Description: The Max Line Length option can be set to any positive integer. Once set user will not be able to send messages with lines that exceed this length. Note that in *ACP127* mode, a default maximum line length of 69 is assumed.

Default value: -None-

Example: 80

LDAP attribute name: `harrierMaxTextPlainLineLength`

3.6.3 Attachments

Description: The attachment option is a boolean value to indicate if users can receive attachments. If it is set to `false` then users will not be able to send them attachments.

Default value: true

Example: false

LDAP attribute name: `harrierAllowAttachments`

3.7 Allowing remote content in HTML messages

External content, such as images, videos and CSS, is frequently used by spammers and attackers for tracking when an email message was read. By default, Harrier blocks external content in HTML messages. This doesn't apply to content generated by Harrier Web Server itself or to content embedded into HTML messages. When such external content is found, a button appears on the message, allowing the user to show remote content.

Once the user allows remote content for a specific message, Harrier Web Server remembers this decision by storing it on the IMAP server using $ShowRemoteContent IMAP keyword. Next time the user views the same message (using the same or different instance of Harrier Web Server), remote content will be shown automatically.

3.8 Message Search

Harrier Web Server supports search for messages that match a specific search criteria. For example, a user can search for messages sent or received by specific senders/ recipients, messages containing certain text in subject or body of the message, messages with a particular SIC, security label and/or of specific precedence.

3.9 Military Sort Order

Military sort order can be enabled in `military` and `acp127` modes. This is controlled by the `military_sort_order` option.

By default INBOX and other folders are sorted by the message arrival time, which is the time they were delivered (using SMTP) or uploaded to the corresponding IMAP folder. When military sort order is enabled, messages in INBOX are sorted so that they appear in the order that they should be actioned. This is done by sorting first on the message Action or Info precedence (see below), with highest precedence messages appearing first. When messages have the same precedence, they are sorted in order of "due time" (see below) so that messages with the soonest "due time" appear first. Messages with the same precedence and "due time" are sorted by arrival time.

The "Due time" for a message is calculated as the shortest time period of the following: a) time left till the Reply-By time (if any); b) time left till the Expires time (if any); c) default processing time as prescribed by the message precedence that applies to the logged in role. See the `act_by` option for more details.

Message precedence is calculated as follows:

1. If the logged in role is an Action recipient, then the Action precedence is used;
2. Otherwise, if the logged in role is an Info recipient, then the Info precedence is used;
3. Otherwise Harrier assumes that the message was received through a distribution list, so the Action precedence is used.

3.10 HSM (PKCS#11) support

Hardware security modules (HSMs) are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates. Harrier Web Server supports HSMs for managing of user/role/organization S/MIME private keys using PKCS#11 interface. See Section 2.8.8, “PKCS#11” for details of how to configure PKCS#11.

3.11 Integration with IRIS WebForms

Harrier Web Server supports close integration with Systematic IRIS WebForms for display and creation of MTF (Message Text Format) attachments.

In order to integrate IRIS WebForms into Harrier, 2 steps need to be completed:

1. Add a Section 2.8.9, “Proxy” entry with the **Request path** option having value `^\/iris\/(.*)` and the **Destination URI** option having the value `http://localhost/webforms/${1}` where http://localhost/webforms is the location of the IIS web server running in front of the IRIS WebForms, and "/iris/" is the URL prefix reserved on Harrier Web Server for IRIS specific forms and related documents.
2. To enable IRIS WebForms integration for a particular domain set the **Web forms URI** advanced option to `/iris/webforms.html`

Chapter 4 Drafter-centric Review

This section introduces Drafter-centric Review and explains how this feature of Harrier is presented to Harrier Users.

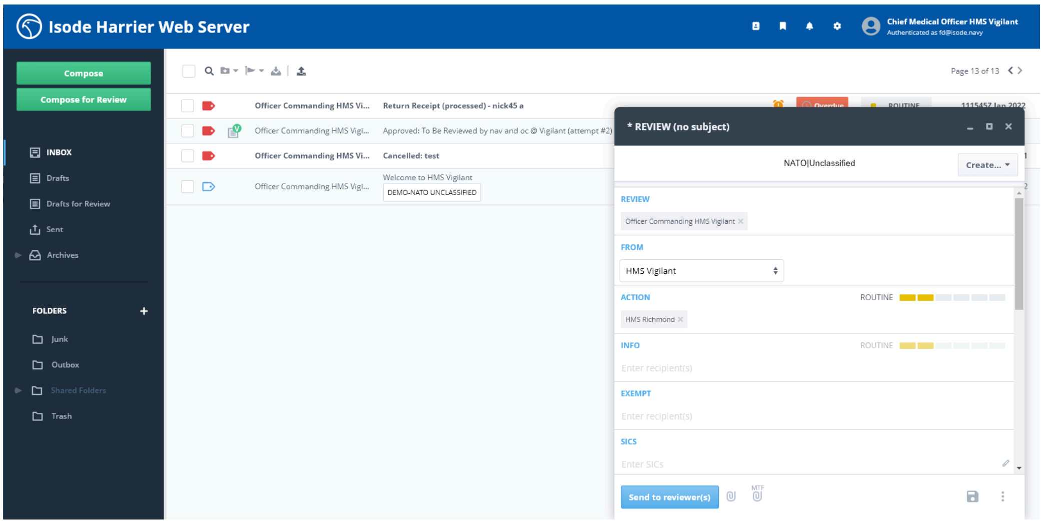
4.1 Drafter-centric Review

Drafter-centric Review is an optional process that allows outgoing messages to be reviewed by one or more reviewer before they are sent out to intended recipients or being subjected to Draft & Release process. Drafter-centric Review requires no Harrier server configuration. Any recipient can be specified as a reviewer.

Reviewers can approve a draft message, or make comments on it. The drafter does not need to wait for any reviewers to respond before sending the message, and does not need to make changes as a result of reviewer comments. If the drafter decides to change the message in response to reviewer comments, then the re-drafted message may be submitted without further review, or sent to reviewers again. The drafter can also cancel a message before sending it, which will notify reviewers that the message has been abandoned.

In Drafter-centric Review mode, Drafters compose messages in the usual manner, but will press "Compose for Review" instead of "Compose" button. The "Compose for Review" window is going to be almost identical to the regular Compose window, except that it will contain an extra "Reviewer" field.

Figure 4.1. Compose for Review window



Officer Commanding HMS Vi... Return Receipt (processed) - nick45 a

Officer Commanding HMS Vigi... Approved: To Be Reviewed by nav and oc @ Vigilant (attempt #2)

Officer Commanding HMS Vi... Cancelled: test

Officer Commanding HMS Vigi... Welcome to HMS Vigilant DEMO-NATO UNCLASSIFIED

* REVIEW (no subject)

NATO|Unclassified

REVIEW: Officer Commanding HMS Vigilant

FROM: HMS Vigilant

ACTION: ROUTINE — HMS Richmond

INFO: ROUTINE — Enter recipient(s)

EXEMPT: Enter recipient(s)

SICS: Enter SICs

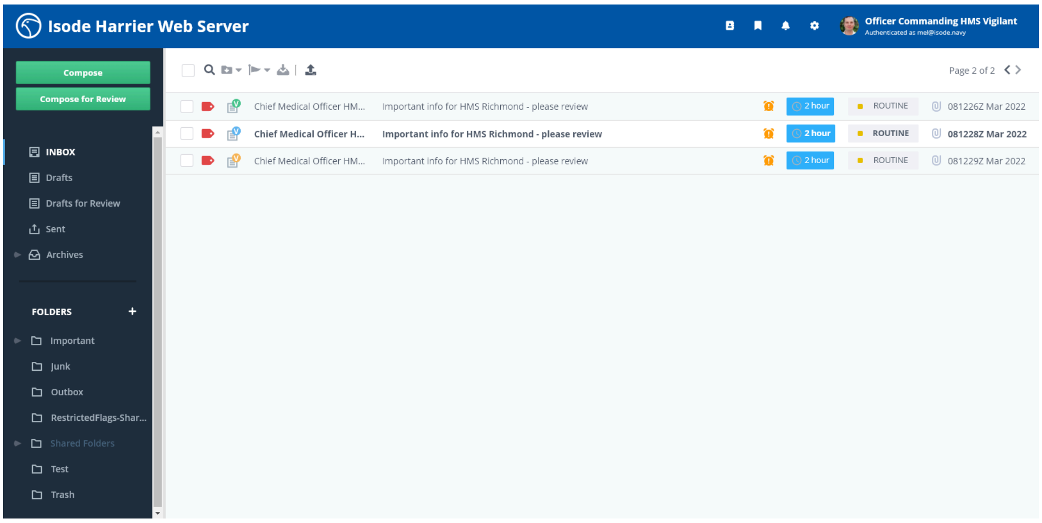
A Reviewer's message list contains icons to indicate which messages are "draft-for-review" messages, and whether they need to be reviewed, or have been reviewed already. The screenshot below has examples of 3 icons you may see on a Drafter-centric Review message.

The green icon with the letter "V" indicates that the message has been approved with no comments for the drafter.

The blue "info" icon indicates messages that have yet to be processed.

The yellow icon indicates a message that has been commented on.

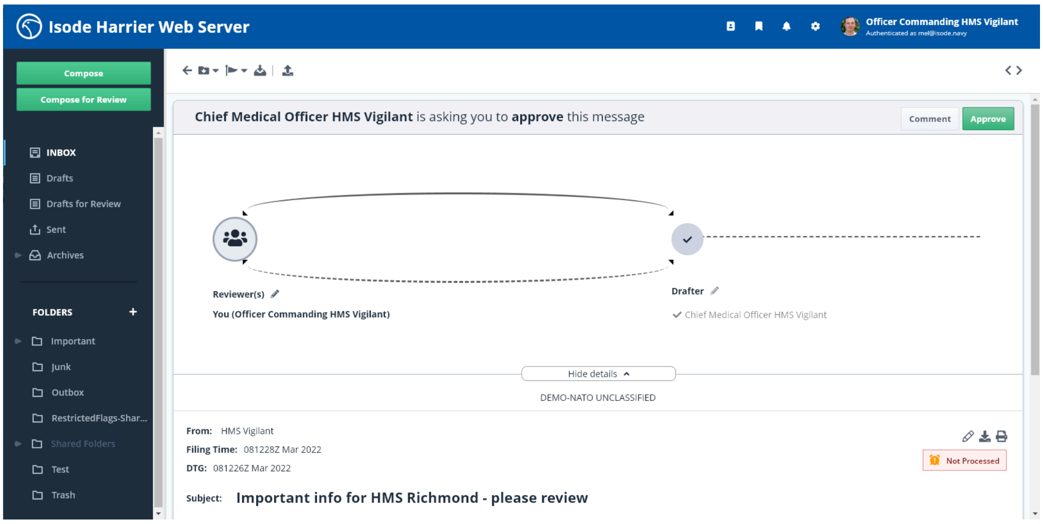
Figure 4.2. Message list with examples of Drafter-centric Review icons



Chief Medical Officer HM...	Important info for HMS Richmond - please review	2 hour	ROUTINE	081226Z Mar 2022
Chief Medical Officer H...	Important info for HMS Richmond - please review	2 hour	ROUTINE	081228Z Mar 2022
Chief Medical Officer HM...	Important info for HMS Richmond - please review	2 hour	ROUTINE	081229Z Mar 2022

Extra buttons are displayed in the message view to allow a Reviewer to comment on or approve the message.

Figure 4.3. Message view with Drafter-centric Review related action buttons



Chief Medical Officer HMS Vigilant is asking you to **approve** this message

Reviewer(s)
You (Officer Commanding HMS Vigilant)

Drafter
✓ Chief Medical Officer HMS Vigilant

DEMO-NATO UNCLASSIFIED

From: HMS Vigilant
Filing Time: 081228Z Mar 2022
DTG: 081226Z Mar 2022

Subject: Important info for HMS Richmond - please review

Chapter 5 Draft And Release

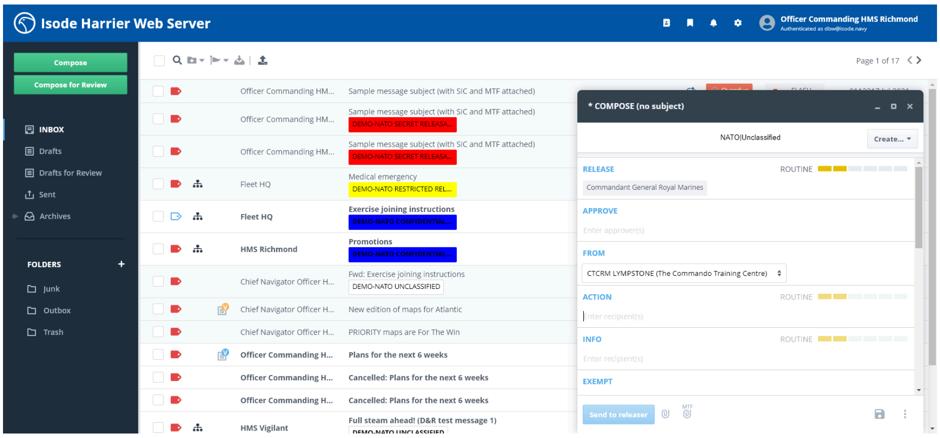
This section introduces Draft and Release and explains how this feature of Harrier is presented to Harrier Users.

5.1 Draft & Release

Draft & Release allows outgoing messages to be approved before they are sent out to intended recipients. When a Draft & Release policy has been configured, messages that are sent by any users who have not been designated as "exempted" will be sent to zero or more approvers, and then to one or more "releasers". Approvers and releasers are able to reject a message (in which case they can supply a reason for rejection), or to approve a message (in which case they can optionally edit the message before approving). A releaser can modify the list of approvers or releasers, or reassign the message to another drafter. The final releaser decides whether the message is released (sent) to the recipient(s) specified by the drafter. Messages which are rejected will be returned to the drafter, who can then choose to edit the message and re-submit, reassign editing to another drafter, or to abandon the attempt.

In Draft & Release mode, Drafters compose messages in the usual manner, but will see two extra fields in the Compose window: "Releaser" field and (optional) "Approver" field. Depending on policy, the Drafter may be forced to use a specific Releaser, or may be able to choose from a list of Releasers. The screenshot below shows an example of the "Compose" screen where the drafter is being required to use the releaser configured for this particular "From" organization

Figure 5.1. Compose Draft & Release message with required releaser



Officer Commanding HM...	Sample message subject (with SIC and MTF attached)
Officer Commanding HM...	Sample message subject (with SIC and MTF attached) DEMO-NATO SECRET RELEASA...
Officer Commanding HM...	Sample message subject (with SIC and MTF attached) DEMO-NATO SECRET RELEASA...
Fleet HQ	Medical emergency DEMO-NATO RESTRICTED REL...
Fleet HQ	Exercise joining instructions DEMO-NATO CONFIDENTIAL...
HMS Richmond	Promotions DEMO-NATO CONFIDENTIAL...
Chief Navigator Officer H...	Fwd: Exercise joining instructions DEMO-NATO UNCLASSIFIED
Chief Navigator Officer H...	New edition of maps for Atlantic
Chief Navigator Officer H...	PRIORITY maps are For The Win
Officer Commanding H...	Plans for the next 6 weeks
Officer Commanding H...	Cancelled: Plans for the next 6 weeks
Officer Commanding H...	Cancelled: Plans for the next 6 weeks
HMS Vigilant	Full steam ahead! (D&R test message 1) DEMO-NATO UNCLASSIFIED

* COMPOSE (no subject)

NATO|Unclassified

RELEASE ROUTINE: Commandant General Royal Marines

APPROVE: Enter approver(s)

FROM: CTCRM LYMPSTONE (The Commando Training Centre)

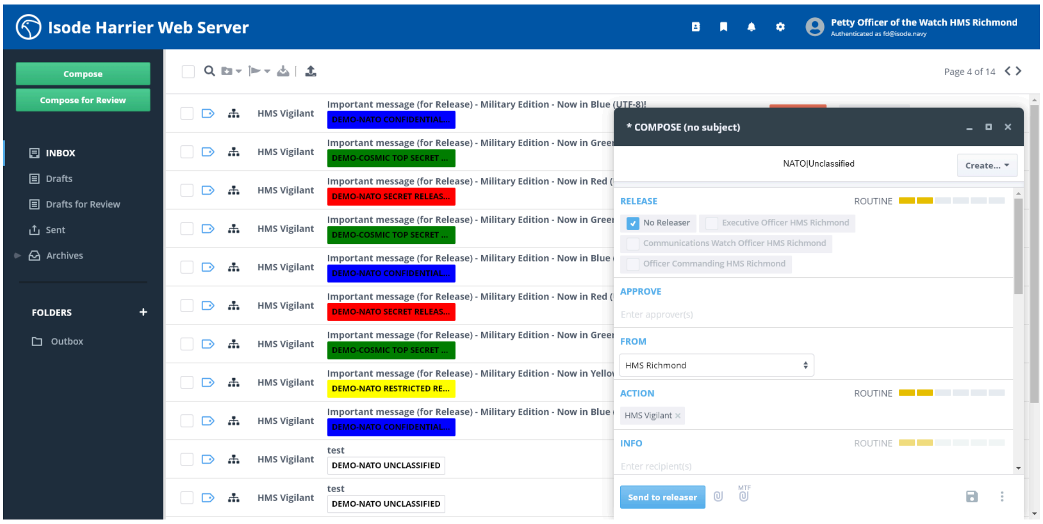
ACTION ROUTINE: Enter recipient(s)

INFO ROUTINE: Enter recipient(s)

EXEMPT

The following screenshot shows what the "Compose" screen may look like for a "From" organization which has multiple releasers configured, and a drafter who is configured to be able to draft and also to send direct in certain circumstances. The drafter may select from the releasers listed and can also choose "No Releaser".

Figure 5.2. Compose Draft & Release message with multiple releaser options



HMS Vigilant — Important message (for Release) - Military Edition - Now in Blue (UTF-8)! — DEMO-NATO CONFIDENTIAL...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Green — DEMO-COSMIC TOP SECRET ...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Red (— DEMO-NATO SECRET RELEAS...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Green — DEMO-COSMIC TOP SECRET ...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Blue (— DEMO-NATO CONFIDENTIAL...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Red (— DEMO-NATO SECRET RELEAS...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Green — DEMO-COSMIC TOP SECRET ...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Yellow — DEMO-NATO RESTRICTED RE...
HMS Vigilant — Important message (for Release) - Military Edition - Now in Blue (— DEMO-NATO CONFIDENTIAL...
HMS Vigilant — test — DEMO-NATO UNCLASSIFIED
HMS Vigilant — test — DEMO-NATO UNCLASSIFIED

* COMPOSE (no subject)

NATO|Unclassified — Create...

RELEASE — ROUTINE
☑ No Releaser
□ Executive Officer HMS Richmond
□ Communications Watch Officer HMS Richmond
□ Officer Commanding HMS Richmond

APPROVE: Enter approver(s)

FROM: HMS Richmond

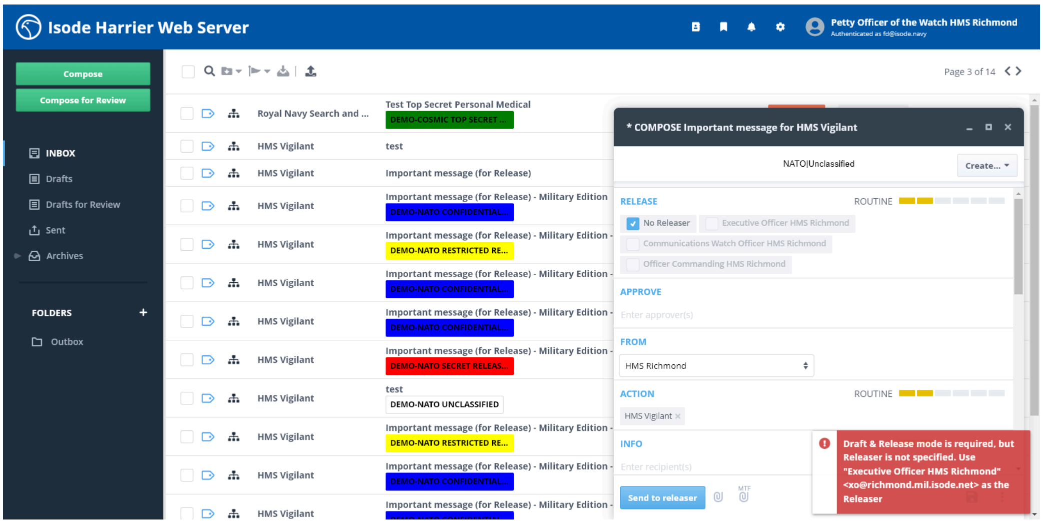
ACTION — ROUTINE: HMS Vigilant ×

INFO — ROUTINE: Enter recipient(s)

Send to releaser

"No Releaser" is only a valid option if the rules for sending directly have been followed. If any of the rules are contravened, Harrier will provide a prompt when the drafter tries to send, and suggest the use of the default releaser, as seen in the screenshot below.

Figure 5.3. Draft & Release message with required releaser



Royal Navy Search and ... — Test Top Secret Personal Medical — DEMO-COSMIC TOP SECRET ...
HMS Vigilant — test
HMS Vigilant — Important message (for Release)
HMS Vigilant — Important message (for Release) - Military Edition — DEMO-NATO CONFIDENTIAL...
HMS Vigilant — Important message (for Release) - Military Edition - — DEMO-NATO RESTRICTED RE...
HMS Vigilant — Important message (for Release) - Military Edition - — DEMO-NATO CONFIDENTIAL...
HMS Vigilant — Important message (for Release) - Military Edition - — DEMO-NATO CONFIDENTIAL...
HMS Vigilant — Important message (for Release) - Military Edition - — DEMO-NATO SECRET RELEAS...
HMS Vigilant — test — DEMO-NATO UNCLASSIFIED
HMS Vigilant — Important message (for Release) - Military Edition - — DEMO-NATO RESTRICTED RE...
HMS Vigilant — Important message (for Release) - Military Edition - — DEMO-NATO CONFIDENTIAL...
HMS Vigilant — Important message (for Release) - Military Edition -

* COMPOSE Important message for HMS Vigilant

NATO|Unclassified — Create...

RELEASE — ROUTINE
☑ No Releaser
□ Executive Officer HMS Richmond
□ Communications Watch Officer HMS Richmond
□ Officer Commanding HMS Richmond

APPROVE: Enter approver(s)

FROM: HMS Richmond

ACTION — ROUTINE: HMS Vigilant ×

INFO: Enter recipient(s)

Send to releaser

Draft & Release mode is required, but Releaser is not specified. Use "Executive Officer HMS Richmond" <xo@richmond.mil.isode.net> as the Releaser

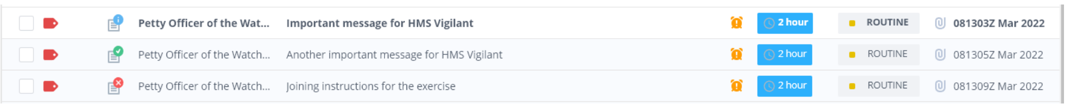
A Releaser's/Approver's message list contains icons to indicate which messages are "draft" messages, and whether they need to be approved, or have been approved already. The screenshot below has examples of 3 icons you may see on a Draft & Release message.

The green icon with a tick indicates that the message has completed its journey through Draft & Release and has been released to the recipients.

The blue "info" icon indicates messages that have yet to be processed.

The red icon indicates a message that has been rejected.

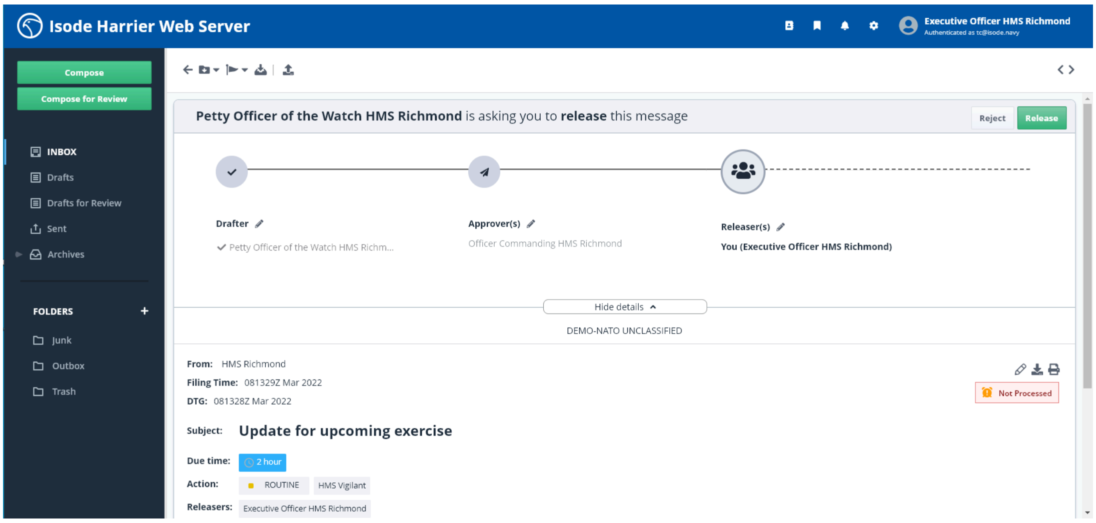
Figure 5.4. Message list with examples of Draft & Release icons



Petty Officer of the Wat...	Important message for HMS Vigilant	2 hour	ROUTINE	081303Z Mar 2022
Petty Officer of the Watch...	Another important message for HMS Vigilant	2 hour	ROUTINE	081305Z Mar 2022
Petty Officer of the Watch...	Joining instructions for the exercise	2 hour	ROUTINE	081309Z Mar 2022

Extra buttons are displayed in the message view to allow a Releaser / Approver to release/approve/reject the message. In order to change the drafter, approvers, or releasers the Releaser / Approver needs to expand the Draft & Release panel.

Figure 5.5. Message view with Draft & Release related action buttons



Petty Officer of the Watch HMS Richmond is asking you to **release** this message

Drafter: ✓ Petty Officer of the Watch HMS Richm...

Approver(s): Officer Commanding HMS Richmond

Releaser(s): You (Executive Officer HMS Richmond)

DEMO-NATO UNCLASSIFIED

From: HMS Richmond
Filing Time: 081329Z Mar 2022
DTG: 081328Z Mar 2022

Subject: Update for upcoming exercise

Due time: 2 hour
Action: ROUTINE HMS Vigilant
Releasers: Executive Officer HMS Richmond

In order to enable Draft & Release, the Harrier administrator should use Isode's User Provisioning tool Cobalt. See *Cobalt Administration Guide* for information on how to do this.

In Cobalt, the administrator can enable Draft & Release for certain domains, create Profiled Addresses for organizations, and add members to those organizations who can be configured as Drafters and/or Releasers. Rules for sending directly can also be configured here.

Note that, in order to have an organization as an Action or Info recipient, the administrator must also provide the profiler.json file with a rule that allows this. Information on the Profiler channel can be found in the *M-Switch Administration Guide*.

For advanced configurations, the Harrier administrator could directly edit the harrierDraftReleaseRules LDAP attribute in the organization's configuration entry. This attribute contains an XML document with `exempted_address`, `release_policy_rule`, `optional_releaser` and/or `exempted_address` XML elements. For example, the `exempted_address` option can be used to exclude some senders from the Draft & Release procedure.

Releasers can be configured to be conditional or unconditional. Unconditional Releasers are authorised to approve all messages sent. Conditional Releasers are responsible for approving messages that satisfy a certain criteria. For example all messages with a particular SIC code, all messages with FLASH precedence or all messages from particular senders. `release_policy_rule` option can be used to define one or more conditional or unconditional Releaser, or an exception condition when no releaser is required. `releaser_address` option is a simplified version of a `release_policy_rule` option, which can only define an unconditional releaser.

5.1.1 Expected Behaviours

The following sub-sections describe the various behaviours that are expected when performing actions on a Draft & Release message.

5.1.1.1 Expected behaviour when composing a message for release

- The user is presented with a standard compose form with additional fields for releasers and optional approvers.
- The user can pick one or more releaser from the list. If multiple are selected, their order is important.

- In some configurations the user can also pick "No Releaser" choice. This is only available when a conditional Draft and Release rule is configured.
- When the user sends a new message the Harrier Web Server constructs a message with the drafted message as a nested message. Harrier Web Server includes a hardcoded explanatory note with instructions for approvers/releasers, in case they use a Mail User Agent different from Harrier. (The generated message is multipart/mixed with the first body part being text/plain (containing the explanatory note) and the second part message/rfc822 with the message to be released inside it).
- The release and reject controls will be hidden from the drafter when they view the message in their Drafts, Sent or Trash folders.
- If Draft and Release is enabled and required, the Harrier server will disallow sending a message which does not have a releaser.

5.1.1.2 Expected behaviour when receiving and Draft and Release message for approval

- The scan list will indicate the message is for Draft and Release, and whether it has already been released or rejected.
- When the message is opened the user is presented with options to Approve or Reject, as well as options to change Drafter or edit the list of Approvers.
- The release and reject controls will be hidden once one of these actions has been chosen. The server also rejects multiple actions on the same Draft & Release message if they are performed simultaneously by different users.
- Users are not allowed to release their own messages. Release/Reject controls are also not shown in "Drafts", "Sent" and "Trash" folders.

5.1.1.3 Expected behaviour when releasing a message

- The inner (to be released) message includes a header field indicating one or more releaser.
- The inner message is sent to the specified recipients.
- The inner message is copied into the releaser's "Sent" folder
- An IMAP flag is added to the outer Draft & Release message to indicate that it has been released.
- If drafter has requested confirmation of release, an MDN is sent to the drafter. This option is turned on by default.

5.1.1.4 Expected behaviour when rejecting a message

- A rejection message is sent to the drafter. A multipart/mixed message with the first part being a rejection note and the second part being message/rfc822 with the original message.
- The rejection message is copied into the releaser's "Sent" folder.
- An IMAP flag is added to the outer Draft & Release message to indicate that it has been rejected.

5.1.1.5 Expected behaviour when a releaser edits a Draft & Release message

- If the drafter has requested confirmation of release, an MDN is sent to the drafter and the releaser's copy is marked with $MDNSent IMAP keyword. This option is turned on by default.
- The releaser takes ownership of the message, so the From header field of the edited message will be the releaser's email address.
- The releaser is able to edit the earlier drafted message.

- If the releaser who edited the message is not exempted from Draft & Release procedure, the edited message will include all releasers who haven't yet approved the message.
- A releaser can edit a Draft & Release message any number of times. A releaser can also edit a message that was already released or rejected. This allows for flexible workflow, for example to allow releaser to split a single message from a drafter into multiple independent pieces.
- An edited Draft & Release message can be saved to "Drafts" as any other draft message. No special handling occurs.

Chapter 6 S/MIME

This section describes sending and receiving signed/encrypted messages using S/MIME.

6.1 S/MIME

Harrier Web Server supports S/MIME signing, verification of signed messages, encryption/decryption as specified in RFC 5750, RFC 5751 and RFC 1847.

When S/MIME has been configured, it provides the user with a method to send and receive secure MIME messages. Depending on the server configuration and the sender/recipient certificates, a user can choose to sign, encrypt, sign and encrypt, triple-wrap a message or not use S/MIME at all. If S/MIME is not configured or a user's certificate is not valid, the user won’t be able to use partial or full functionality of the feature. Based on the setup and environment, some users may always need to send signed/encrypted/triple-wrapped messages or may never be able to send messages with a particular S/MIME option.

In an S/MIME configured environment, a sender would compose messages in the usual manner, but will have the option to enable S/MIME signing, encryption and triple-wrap by toggling the S/MIME checkboxes from the ‘More options’ menu in the Compose window. The following combinations of user options are available, if everything is enabled and the sender and recipients have valid certificates:

None	S/MIME Sign	S/MIME Encrypt	S/MIME Triple-wrap
x			
	x		
		x	
			x
	x	x	
	x		x
		x	x
	x	x	x

6.1.1 S/MIME Message Status

After the message has been delivered, the receiver can look at the message and see the S/MIME status. This shows irrespective of whether S/MIME signing and/or encryption is enabled for the logged in user. For example, if a signed and encrypted message was encrypted and signed and if the receiver was able to decrypt the message and verify the signature. The following options are most common:

<empty string>	Non S/MIME message
encrypted	S/MIME encrypted message. This doesn't convey whether or not the message was successfully decrypted.
encrypted+signed/failed	The message was both signed and encrypted. While decryption has succeeded, signature verification has failed. See **signed/failed**.
encrypted+signed/verified	The message was both signed and encrypted. The signature was verified (see **signed/verified**)

encrypted/failed	S/MIME encrypted message failed on decryption. The message might or might not contain other S/MIME messages inside.
signed	S/MIME signed message, but the signature was not yet verified
signed/failed	S/MIME signed message, but the signature failed to verify. This could be due to untrusted certificate authority(CA) or incomplete chain of certificates to a Trusted Anchor, expired or revoked signing certificate and broken signature due to message modification.
signed/verified	S/MIME signed message and the sender's signature was successfully verified, sender matches the From header field and the sender's certificate is trusted for signing.
encrypted+signed/verified/triple-wrapped	The message was signed, encrypted and then signed again. The two signatures were verified (see **signed/verified**)
unknown	S/MIME message, but it is neither signed, nor encrypted. Sometimes this is reported for corrupted S/MIME messages. This is also displayed for OpenPGP messages, which are not being handled for the time being.

If any of the failures above have occurred, the message will have an S/MIME Warning or Error displayed, explaining in a more comprehensive way what has gone wrong.

6.1.2 Configuration of S/MIME operations

6.1.2.1 S/MIME signing/encryption/triple-wrap

Signing and/or encryption can be enabled per user by setting harrierSmimeSign/harrierSmimeEncrypt LDAP attributes. It is also possible to just enable signing/encryption per domain, but setting harrierSmimeSign/harrierSmimeEncrypt will override it for a specific user. To enable signing for a domain use the **Sign** option. To enable encryption for a domain use the **Encrypt** option. To enable triple-wrap for a domain use the **Triple wrap** option. Note that setting harrierSmimeSign and/or harrierSmimeEncrypt LDAP attributes to FALSE for a user will also disable ability to send triple wrapped messages by that user.

When sending messages, it is possible to disable S/MIME signing/encryption/triple-wrap on per message basis. (It is not possible to enable signing/encryption/triple-wrap for a message, if it is disabled for the user.) A Harrier user can see whether S/MIME signing/encryption/triple-wrap is enabled by viewing message options in the Compose window.

Note that in order for S/MIME signing to be enabled by default, all of the following conditions must be met: 1) signing must be enabled for the domain (in domain configuration) or for the specific user (in LDAP); 2) the domain has LDAP configuration and all users can bind to Directory using the same username/password as used for IMAP login; 3) the logged in user's LDAP entry must have a userPKCS12 attribute, containing the private key and corresponding certificate, encrypted with the user's login password. Alternatively PKCS#11 configuration is present in the Harrier configuration file, the user's (or role's) LDAP entry has both a userCertificate attribute and a harrierSignIdentity attribute that describes how a particular user certificate related to a private key stored on an HSM. Because of the last point, you either need to upload an existing PKCS#12 object (encrypted with the user's login password) to the userPKCS12 attribute or you need to configure Harrier to automatically generate a CSR and key pair (see below), in order to be able to obtain a certificate for the user. (HSM/PKCS#11 private keys and certificates can be managed with Cobalt.)

Encryption for a message depends on sender's ability to encrypt, as well as the ability of each recipient to receive encrypted messages. In order to be able to encrypt a message, all of the following conditions must be met: 1) Harrier activation includes "encrypt" sub-feature; 2) encryption must be enabled for the domain (in domain configuration) or for the specific user (in LDAP); 3) the domain has LDAP configuration and all users can bind to Directory using the same username/password as used for IMAP login; 4) the logged in user's LDAP entry must have a userPKCS12 attribute, containing the private key and corresponding certificate, encrypted with the user's login password. Alternatively PKCS#11 configuration is present in the Harrier configuration file, the user's (or role's) LDAP entry has both a userCertificate attribute and a harrierSignIdentity attribute that describes how a particular user certificate related to a private key stored on an HSM. 5) each recipient's LDAP entry must contain userCertificate attribute (an unexpired certificate) that can be used to encrypt the message.

Triple-wrap is the process of sending a message that is signed then encrypted then wrapped in another signature. In order to do triple-wrap, the sender must have the necessary certificates (and corresponding private keys) for signing and encryption but it is not needed for the user to have signing and encryption enabled in the configuration. Triple-wrap for a message depends on sender's ability to triple-wrap (sign → encrypt → sign), as well as the ability of each recipient to receive encrypted messages. In order to be able to triple-wrap a message, all of the following conditions must be met: 1) Harrier activation includes "encrypt" sub-feature; 2) triple-wrap must be enabled for the domain (in domain configuration); 3) the domain has LDAP configuration and all users can bind to Directory using the same username/password as used for IMAP login; 4) the logged in user's LDAP entry must have a userPKCS12 attribute, containing the private key and corresponding certificate, encrypted with the user's login password. Alternatively PKCS#11 configuration is present in the Harrier configuration file, the user's (or role's) LDAP entry has both a userCertificate attribute and a harrierSignIdentity attribute that describes how a particular user certificate related to a private key stored on an HSM. 5) the user's LDAP entry must not have harrierSmimeSign and/or harrierSmimeEncrypt LDAP attributes set to FALSE; 6) each recipient's LDAP entry must contain userCertificate attribute (an unexpired certificate) that can be used to encrypt the message.

Note that when using S/MIME encryption together with Draft & Release procedure, Harrier needs to be able to encrypt the message to each recipient plus the selected Releaser(s) and Reviewer(s).

6.1.2.2 Automatic CSR generation/certificate import

In order to enable automatic private key and CSR generation with the subsequent installation of an issued certificate, you first need to enable S/MIME signing and/or encryption and second set the following 3 options: **Auto generate CSRs**, **CSR auto-generation path** and **P12 auto-generation path**

The **CSR auto-generation path** specifies filesystem directory where automatically generated S/MIME CSR files (and corresponding PEM files) will be written. The directory must exist.

The **P12 auto-generation path** specifies filesystem directory where automatically generated S/MIME PKCS#12 files (initially containing private key) will be written. The directory must also exist.

Provided these three options are set, then whenever a user logs in, Harrier will check to see whether a certificate is configured for the user. If not, Harrier will generate a key pair and corresponding CSR, which will be written to **CSR auto-generation path** and **P12 auto-generation path** respectively. (Note that the system administrator doesn't need access to the **P12 auto-generation path** directory.) The system administrator should review the **CSR auto-generation path** directory for CSR files (which are named using the user's canonical email address). These CSRs should be submitted to an appropriate Certificate Authority or be processed by a tool like Sodium CA, and once corresponding certificates have been issued, they should be placed in the **CSR auto-generation path** directory as PEM files. (Note that original CSR files must not be deleted, as they are used by Harrier.) Subsequently, when the user logs in, Harrier will import the certificate and private key as a userPKCS12 attribute value, and also import the certificate as the userCertificate value. Following this, the user will be able to sign and encrypt messages, and to receive encrypted messages from other users.

Note that when using S/MIME encryption in a configuration where users are allowed to assume various roles, the userPKCS12 attribute is read from the logged in user entry, while userCertificate attribute is read from role (recipient) entries. For example, let's consider a configuration where user user1@example.com is able to select one of 2 roles upon login: postmaster@example.net and support@example.net. In order for other senders to send encrypted messages to postmaster@example.net the postmaster@example.net's LDAP entry must contain certificate with postmaster@example.net email in the userCertificate attribute. Similarly for support@example.net. When S/MIME encryption is used together with the automatic CSR generation/certificate import feature, this means that postmaster@example.net's certificate will be imported into user1@example.com's LDAP entry. It needs to be manually copied to the postmaster@example.net entry.

6.1.2.3 S/MIME verification/decryption

This happens automatically for all received messages.

In order for S/MIME signature verification to work Harrier needs to be configured with Trust Anchors (the certificates of Certificate Authorities (CAs) which are trusted) as well as any other CA certificates that may be needed when building a certificate chain from a Trust Anchor to sender's end-entity certificates. List all Trust Anchors in **Trusted certificates** option. List all intermediate Certification Authorities in **Intermediate certificates** option.

In order to be able to decrypt messages, Harrier needs to access to user's private key stored in LDAP Directory in the userPKCS12 attribute. This uses the same configuration that is needed for encryption. Note that decryption can be performed even if the certificate that corresponds to a private key is expired.