HARRIERWEB-17.0

Harrier Web Server Administration Guide

Isode

Table of Contents

1 Software version

This guide is published in support of Isode Harrier Web R17.0. 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

Related topics are discussed in the volumes of the Isode documentation set listed below.

Volume	Title
SWADM-17.0	*M-Switch Administration Guide*
VAUADM-17.0	*M-Vault Administration Guide*
MBOXADM-17.0	*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
(ETCDIR)	System-specific configuration files.	*C:\Isode\etc*	*/etc/isode*
(SHAREDIR)	Configuration files that may be shared between systems.	*C:\Program Files\Isode\share*	*/opt/isode/share*
(BINDIR)	Programs run by users.	*C:\Program Files\Isode\bin*	*/opt/isode/bin*
(SBINDIR)	Programs run by the system administrators.	*C:\Program Files\Isode\bin*	*/opt/isode/sbin*
(EXECDIR)	Programs run by other programs; for example, M-Switch channel programs.	*C:\Program Files\Isode\bin*	*/opt/isode/libexec*
(LIBDIR)	Libraries.	*C:\Program Files\Isode\bin*	*/opt/isode/lib*
(DATADIR)	Storing local data.	*C:\Isode*	*/var/isode*
(LOGDIR)	Log files.	*C:\Isode\log*	*/var/isode/log*

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: license@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 protocols and algorithms to encrypt data on connections. If you license the higher grade encryption (HGE) Isode products they are subject to UK Export controls.

You must ensure that you comply with these controls where applicable, i.e. if you are licensing or re-selling Isode products outside the Community with the HGE option selected.

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

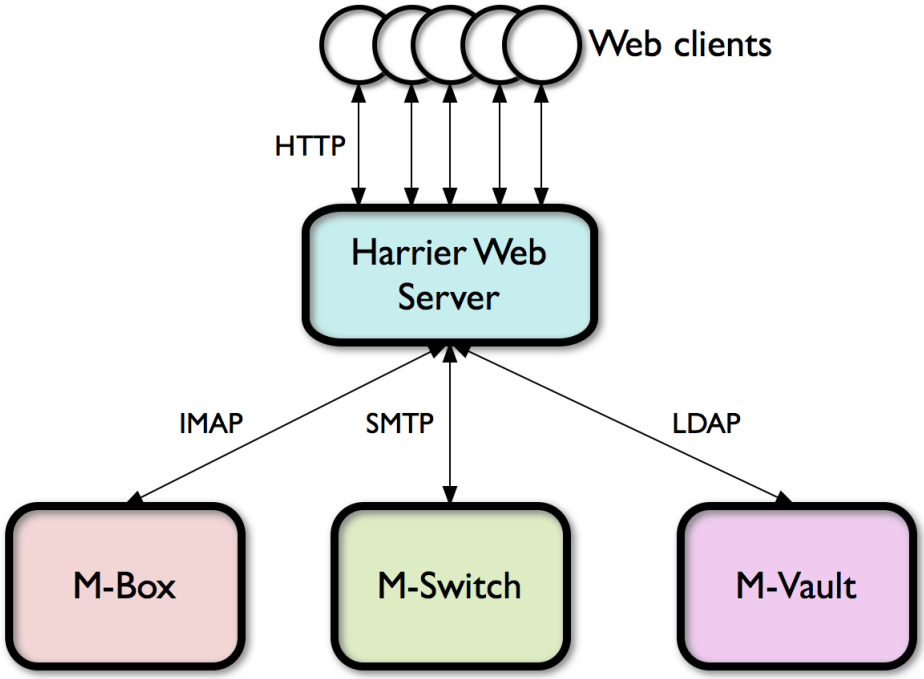
Chapter 1 Introduction to Harrier Web

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.

Chapter 2 Harrier Server Configuration

This section provides a detailed description of Harrier server configuration options.

Harrier Web Server reads its configuation from an XML file located in *(ETCDIR)/harrier_web_conf.xml*. This chapter describes the options that are available in the configuration file and how to make changes to them so that the Harrier Web Server will use them.

2.1 Initial configuration

This section describes initial configuration of Harrier Web Server. Please read this section to find out about all configuration steps required before starting Harrier Web Server for the first time.

This section also provides basic information about services included in Harrier Web Server and describes how to start/stop Harrier Web Server services once the initial configuration is complete.

2.1.1 Harrier Web Server configuration file

Harrier Web Server reads its configuration from *(ETCDIR)/harrier_web_conf.xml*. A sample configuration file is provided in *(ETCDIR)/harrier_web_conf.xml.sample*. It may be useful to use the contents of this file as a starting point, by copying it to *(ETCDIR)/harrier_web_conf.xml* and then editing it before starting the Harrier Web Server.

2.1.2 Harrier Web Server 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 Section 2.4.3.5, “Runtime User”).

2.2 Installing an Isode license file

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

Where Harrier and, if used, M-Vault Server are to be ran on the same host system, all relevant licenses are provided by Isode in single file. This file needs to be copied to *(ETCDIR)/license.dat* on the host system. Otherwise, each system hosting a product component will each have their own license file.

Questions regarding licensing should be directed to licensing@isode.com.

2.3 Starting and stopping Harrier

2.3.1 Harrier processes

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.

2.3.2 Starting/stopping Harrier on Linux

This section is specific to Linux.

An example startup/shutdown script, *(SBINDIR)/harrier_web_server*, is included in the M-Box package which contains Harrier.

The script can start, stop and query all of the Harrier services: `isode.harrierwebserver`.

- To start Harrier run **/opt/isode/sbin/harrier_web_server start**
- To stop it run **/opt/isode/sbin/harrier_web_server stop**
- To check which Harrier services are running: **/opt/isode/sbin/harrier_web_server status**

2.3.3 Installing Harrier on Windows

On Windows each Harrier process is installed as a Windows service. These processes run under the Local System account.

Once you have installed an Harrier license and created a proper *(ETCDIR)\harrier_web_conf.xml* file, you can use the **Isode Service Configuration** tool in the **Isode** program group to install Harrier services. (Note, this will require Java to be installed). Select the menu **Operations->Create Service->M-BOX->Isode Web Harrier Server** Alternatively you can run

```
(SBINDIR)\mbox.exe -f harrier.xml install
```

from a command line.

In either case you will need Administrator's permissions to run the correspondonding command, i.e. by starting the commands with "Run as administrator".

2.3.4 Starting/stopping Harrier on Windows

By default Harrier services are set to **Manual start**, i.e. they need to be started manually. Change this to "Automatic Start" if you need them to be started automatically at system startup.

It is also possible to start installed Harrier services from the command line using *(SBINDIR)\mbox.exe -f harrier.xml* utility.

In order to start Harrier run

```
(SBINDIR)\mbox.exe -f harrier.xml start
```

In order to stop it run

```
(SBINDIR)\mbox.exe -f harrier.xml stop
```

To check which Harrier services are are installed and running:

```
(SBINDIR)\mbox.exe -f harrier.xml status
```

2.4 Server configuration options

The Harrier Web Server configuration file *(ETCDIR)/harrier_web_conf.xml* contains an XML document. The top level XML element is `harrier`. Each configuration option is represented as an XML element.

2.4.1 Configuration file structure

The configuration file has general options located in elements under the root element. As well as general options, other tags contain groups of options:

- The `<domains>` element contains information about the domains which are supported by the Harrier Web Server.

2.4.2 Configuration file 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
`$(isode.dir.etc)`	(ETCDIR) file system placeholder
`$(isode.dir.var)`	(DATADIR) file system placeholder
`$(isode.dir.share)`	(SHAREDIR) file system placeholder
`$(isode.dir.etc_or_share)`	First checks (ETCDIR) then (SHAREDIR)
`$(harrier.dir.app)`	Directory where Harrier Web Server executable is located

2.4.3 General Options

This section describes configuration options that can be configured directly under the root level element harrier

2.4.3.1 servpass:info

Description: the service name to be used to identify the *servpass* key that is used to obfuscate sensitive data in this file. This option is empty by default, which means that sensitive data will not be obfuscated.

The value in this option will be used by the `spasscrypt` utility to obfuscate fields in the file which have been identified as sensitive. See Section 2.8, “Obfuscation of passwords”.

Default value: -None-

XML element name: `servpass:info`

Parent XML element: top level `<harrier>`

Example: `<servpass:info service="isode.harrier"/>`

2.4.3.2 Listen Addresses

Description: The `port` option can be used to specify that the server should listen for incoming HTTP/WS requests using the specified port on all available network addresses. The `listen` option provides more fine-grained control over which network addresses/ports should be used.

The HTTPS/WSS acceptance is defined separately (See Section 2.4.5.2, “Listen Addresses”).

If only address is specified it uses port number from `port` option..

Default value: "::" which means all IPv6 and IPv4 addresses

XML element name: `listen`

Parent XML element: top level `<harrier>`

Example:

```
<!-- listen on 127.0.0.1 interface and port as defined in port option -->
<listen>127.0.0.1</listen>
<!-- listen on 192.168.0.100 interface and port 9999 -->
<listen>192.168.0.100:9999</listen>
<!-- listen on IPv6 localhost interface and port as defined in port option -->
<listen>::1</listen>
<!-- listen on IPv6 fe80::9ada:8bdb:9871:6d1b interface and port 9999 -->
<listen>[fe80::9ada:8bdb:9871:6d1b]:9999</listen>
```

2.4.3.3 Host

Description: 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 Section 2.4.5.4, “Key”).

Default value: -None-

XML element name: `host`

Parent XML element: top level `<harrier>`

Example: `<host>example.com</host>`

2.4.3.4 Port

Description: Specifies the port that Harrier Web Server will listen on for incoming HTTP connections

Default value: 9090

XML element name: `port`

Parent XML element: top level `<harrier>`

Example: `<port>9009</port>`

2.4.3.5 Runtime User

Description: 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. Harrier Web Server is also able to bind to a privileged port before dropping user privileges.

Default value: -None-

XML element name: `runtime_user`

Parent XML element: top level `<harrier>`

Example: `<runtime_user>harrier</runtime_user>`

2.4.3.6 Websocket buffer size

Description: Specifies the buffer size to be used for websocket connections. This setting is reserved for use by Isode.

Default value: 64K

XML element name: `ws_buffer_size`

Parent XML element: top level `<harrier>`

Example: `<ws_buffer_size>64K</ws_buffer_size>`

2.4.3.7 Default Domain

Description: Specifies default domain name which allows to login with user name only (The default domain is being added to name to determine full user login).

Default value: -None-

XML element name: `default_domain`

Parent XML element: top level `<harrier>`

Example: `<default_domain>example.com</default_domain>`

2.4.4 HTTP server

This section describes configuration options used to control/override the behaviour of Harrier Web Server when acting as an HTTP server. Specifically, the `<http_map>` may be used to alter the path used to locate resources that may be used by the client, as described below.

2.4.4.1 URL mapping

Description: Specifies the location in the local filesystem which can be used to resolve URLs from the client. This option takes following parameters:

- `url` specifies a URL (or the start of a URL) in the client's request
- `pattern` used instead of `url` in more complex cases and specifies a URL regular expression pattern in the client's request
- `path` specifies the path on the local filesystem to be used to resolve the specified URL.

The default configuration contains a definition for `url="/"` which should not be modified. Other urls that may be modified are:

- `/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 `$(isode.dir.share)/webapps/harrier/data/mmhs-types.xml`

XML element name: `http_map`

Parent XML element: top level `<harrier>`

Example:
```
<http_map url="/data/mmhs-types.xml"
path="/usr/local/my-mmhs-types.xml"/>
```

2.4.5 SSL

This section describes configuration options relating to SSL configuration for incoming HTTPS connections. SSL configuration for outgoing IMAP, SMTP and LDAP connections is configured in the domains section (see Section 2.5, “Domains”).

2.4.5.1 Port

Description: Specifies the port that the server will listen on for incoming HTTPS connections

Default value: 9443

XML element name: `ssl_port`

Parent XML element: top level `<harrier>`

Example: `<ssl_port>9003</ssl_port>`

2.4.5.2 Listen Addresses

Description: The `ssl_port` option can be used to specify that the server should listen for incoming HTTPS/WSS requests using the specified port on all available network addresses. The `ssl_listen` option provides more fine-grained control over which network addresses/ports should be used.

The HTTP/WS acceptance is defined separately (See Section 2.4.3.2, “Listen Addresses”).

If only address is specified it uses port number from `ssl_port` option..

Default value: "::" which means all IPv6 and IPv4 addresses

XML element name: `ssl_listen`

Parent XML element: top level `<harrier>`

Example:

```
<!-- listen on 127.0.0.1 interface and port as defined in ssl_port option -->
<listen>127.0.0.1</listen>
<!-- listen on 192.168.0.100 interface and port 9443 -->
<listen>192.168.0.100:9443</listen>
<!-- listen on IPv6 localhost interface and port as defined in ssl_port option -->
<listen>::1</listen>
<!-- listen on IPv6 fe80::9ada:8bdb:9871:6d1b interface and port 9443 -->
<listen>[fe80::9ada:8bdb:9871:6d1b]:9443</listen>
```

2.4.5.3 Certificate

Description: Specifies the full path to a file containing the Harrier Web server's own TLS certificate. This certificate will be sent by the server to any client connecting using HTTPS, and may be used by the client browser to confirm the server's identity when negotiating secure communication.

The certificate format must be in PEM or PKCS#12 format. The format is determined from the file extension, which is "pem" and "p12" respectively.

The value "$(harrier.tlscert)" can be used to reference the default certificate. It expands to "$(isode.dir.etc)harriercert.pem". This option is ignored if the value of the `ssl_key` XML option is a PKCS#12 file, in which case the PKCS#12 file is assumed to contain both the private key and the corresponding certificate.

Default value: -None-

XML element name: `ssl_certificate`

Parent XML element: top level `<harrier>`

Example:
`<ssl_certificate>$(isode.dir.etc)harrier-cert.pem</ssl_certificate>`

2.4.5.4 Key

Description: specifies the full path to a file containing the private key belonging to the server TLS certificate.

If this option is not set or empty the HTTPS support is disabled and other related options are ignored.

The private key must be in PEM or PKCS#12 format. The format is determined from the file extension, which is "pem" and "p12" respectively.

The value "$(harrier.tlskey)" can be used to reference the default private key. It expands to "$(isode.dir.etc)harrierkey.pem", if the file exists, otherwise it expands to "$(isode.dir.etc)harrier.p12".

If `host` is defined, and `ssl_key` is set to $(harrier.tlskey) but the PCKS#12 file identified by $(harrier.tlskey) does not exist, then the Harrier Web Server will generate a self signed certificate and key, and store them in $(harrier.tlskey), and then update the configuration

file with the passphrase for the generate PKCS#12 file. The passphrase will be obfuscated using servpass if that has been configured.

Default value: -None-

XML element name: `ssl_key`

Parent XML element: top level `<harrier>`

Example: `<ssl_key>$(isode.dir.etc)harrier-key.pem</ssl_key>`

2.4.5.5 Password

Description: Specifies the password used to decrypt the server's private key. This option is empty by default, which means that the private key is not protected by any password.

The value in this option should be encrypted using the `servpass` utility (see Section 2.8, “Obfuscation of passwords”.

Default value: -None-

XML element name: `ssl_password`

Parent XML element: top level `<harrier>`

Example: `<ssl_password servpass:encrypt="true">secret</ssl_password>`

2.4.5.6 Certificate Chain

Description: Specifies the path of the file containing the CA certificates (in PEM format) that will be appended to the Harrier Web Server's own certificate to form a certificate chain that is sent to clients when they attempt a connection using HTTPS. This can be empty if no CA certificates are to be included in the certificate chain.

Default value: -None-

XML element name: `ssl_chain_certificate`

Parent XML element: top level `<harrier>`

Example:
`<ssl_chain_certificate>$(isode.dir.etc)cert-chain.pem</ssl_chain_certificate>`

2.4.5.7 Cipher List

Description: 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

XML element name: `ssl_cipher_list`

Parent XML element: top level `<harrier>`

Example: `<ssl_cipher_list>3DES</ssl_cipher_list>`

2.4.5.8 TLS Diffie-Hellman parameters

Description: Specifies the full path to 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 $(isode.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 > /etc/isode/harrier.dhp
```

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: $(isode.dir.etc_or_share)/harrier.dhp

XML element name: `ssl_dh_params_path`

Parent XML element: top level `<harrier>`

Example:
`<ssl_dh_params_path>$(isode.dir.etc_or_share)/harrier.dhp</ssl_dh_params_path>`

2.4.5.9 Redirect HTTP

Description: This option provides a means to prevent non HTTPS access, by forcing all HTTP accesses to redirect to the HTTPS port (using HTTP 301 response).

This option is ignored if SSL Key is not set (see: Section 2.4.5.4, “Key”)

Default value: false

XML element name: `ssl_redirect_http`

Parent XML element: top level `<harrier>`

Example: `<ssl_redirect_http>true</ssl_redirect_http>`

2.4.5.10 Key Size

Description: Specifies SSL key size (in bits) when SSL private key is automatically generated.

Default value: 0 which means RSA default (2048 bits)

XML element name: `ssl_key_size`

Parent XML element: top level `<harrier>`

Example: `<ssl_key_size>2048</ssl_key_size>`

2.4.6 Global S/MIME settings

Most of the S/MIME related settings are configured per domain (See Section 2.5.15, “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

2.4.6.1 Trusted Anchors

Description: Specifies in separate elements one or more trusted certificates (Trusted Anchors) used for S/MIME signature verification.

Each element must contain path to a DER or PEM encoded certificate.

For verification to succeed, all trust anchors and intermediate certificates must be included.

XML element name: `smime_trusted_certificate`

Parent XML element: top level `<harrier>`

Example:
`<smime_trusted_certificate>/path/to/file.der</smime_trusted_certificate>`

2.4.6.2 Intermediate Certificates

Description: Specifies in separate elements intermediate certificates used for S/MIME signature verification.

Each element must contain path to a DER or PEM encoded certificate.

For verification to succeed, all trust anchors and intermediate certificates must be included.

XML element name: `smime_intermediate_certificate`

Parent XML element: top level `<harrier>`

Example:
`<smime_intermediate_certificate>/path/to/anotherfile.der</smime_intermediate_certificate>`

2.5 Domains

This section describes options that can be configured under the domains element

The domains contains one or more `<domain>` elements, each of which describes distinct set of configuration options (like IMAP, SMTP and LDAP) for a specific user group (usually associated with internet mail domain).

Here is an example `<domain>` entry. The individual elements are described below:

```
<domain name="example.com">
  <imap_url>imap.example.com:143</imap_url>
  <imap_server_trustanchors>
    $(isode.dir.etc)trusted-ca-cert.pem
  </imap_server_trustanchors>

  <smtp_url>smtp.example.com:587</smtp_url>
  <smtp_server_trustanchors>
```

```
      $(isode.dir.etc)trusted-ca-cert.pem
    </smtp_server_trustanchors>

    <ldap_url>ldap.example.com:19389</ldap_url>
    <ldap_server_trustanchors>
      $(isode.dir.etc)trusted-ca-cert.pem
    </ldap_server_trustanchors>

    <ldap_sasl_mechs>SCRAM-SHA-1</ldap_sasl_mechs>

    <ldap_user_mail_ats>mail,mailLocalAddress</ldap_user_mail_ats>
    <ldap_user_name_ats>displayName,CN</ldap_user_name_ats>
    <ldap_user_prefs_oc>isodeHarrierUser</ldap_user_prefs_oc>
    <ldap_user_prefs_at>harrierUserPreferences</ldap_user_prefs_at>

    <ldap_addressbook_base_dn>
      ou=users,c=us
    </ldap_addressbook_base_dn>
  </domain>
```

2.5.1 Name

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

- `<domain name="example.com">` matches any username that ends with `@example.com`.

Default value: -None-

XML attribute name: `name`

Parent XML element: `<domain>`

Example: `<domain name="example.com">`

2.5.2 Pattern

Description: Replacement for `name` attribute allowing to define more advanced matching rules. Specifies an ECMAScript Regular Expression which is used to match the domain part of the username supplied by someone logging in to Harrier Web. For example:

- `<domain pattern="example\.(net|com)">` matches any username that ends in either `@example.com` or `@example.net`

See ECMAScript syntax documentation [http://cplusplus.com/reference/regex/ECMAScript/] for more detailed information about regular expressions.

Default value: -None-

XML attribute name: `pattern`

Parent XML element: `<domain>`

Example: `<domain pattern="example\.(net|com)">`

2.5.3 Limit Charset

Description: Specifies if composition of messages should restrict the user to a limited set of characters. This option has no effect in `internet` mode. Valid options are:

- `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.

Default value: empty (no restriction)

XML element name: `limit_charset`

Parent XML element: `<domain>`

Example: `<limit_charset>IA5</limit_charset>`

2.5.4 Military Sort Order

Description: Specifies if the Inbox should be sorted using the military sort order algorithm. This option has no effect in `internet` mode.

Default value: false

XML element name: `military_sort_order`

Parent XML element: `<domain>`

Example: `<military_sort_order>true</military_sort_order>`

2.5.5 Mode

Description: Specifies the mode Harrier will operate in. Can be either `internet`, `military` or `acp127`. See Section 2.6, “Server Modes” for more info.

Default value: military

XML element name: `mode`

Parent XML element: `<domain>`

Example: `<mode>internet</mode>`

2.5.6 Session Timeout

Description: 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.

The value may be defined as number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks.

Default value: 30min

XML element name: `session_timeout`

Parent XML element: `<domain>`

Example: `<session_timeout>30min</session_timeout>`

2.5.7 User Preferences

Description: Specifies the path for default user preferences. This setting is reserved for use by Isode.

Default value: -None-

XML element name: `user_preferences`

Parent XML element: `<domain>`

Example: `<user_preferences/>`

2.5.8 Automatic Saving

Description: 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.

The value may be defined as number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks.

Default value: 5m

XML element name: `auto_save`

Parent XML element: `<domain>`

Example: `<auto_save>5m</auto_save>`

2.5.9 Acting Thresholds

Description: Defines acting thresholds (act by) for messages with given precedence (so defines multiple pairs of precedence and period specified as attributes) - They are used in message sorting as a replacement for reply_by specification.

The precedence is specified as a number or corresponding name: DEFERRED=0, ROUTINE=1, PRIORITY=2, IMMEDIATE=3, FLASH=4, OVERRIDE=5

The period may be defined as number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks.

Default value: -Empty-

XML element name: `act_by`

Parent XML element: `<domain>`

Example:

```
<act_by precedence="5" period="5m" />
<act_by precedence="4" period="10m" />
<act_by precedence="3" period="15m" />
<act_by precedence="2" period="1h" />
<act_by precedence="1" period="3h" />
<act_by precedence="0" period="7d" />
```

2.5.10 IMAP

This section describes options related to IMAP service access and usage.

2.5.10.1 Host and Port

Description: Specifies the host and port of the IMAP server for this domain.

Default value: -None-

XML element name: `imap_url`

Parent XML element: `<domain>`

Example: `<imap_url>imap.example.com:143</imap_url>`

2.5.10.2 Keep Alive Interval

Description: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 of imap_keepalive_interval of 1740 (i.e. 29 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.

The value may be defined as number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks.

Default value: 29min

XML element name: `imap_keepalive_interval`

Parent XML element: `<domain>`

Example: `<imap_keepalive_interval>5m</imap_keepalive_interval>`

2.5.10.3 Re-connect Interval

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

The value may be defined as number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks.

Value 0 disables automatic re-bind.

Default value: 5s

XML element name: `imap_reconnect_interval`

Parent XML element: `<domain>`

Example: `<imap_reconnect_interval>5s</imap_reconnect_interval>`

2.5.10.4 Server Pinned Certificates

Description: Each <imap_server_pinned> element should contain the path to a file containing an X.509 certificate (in PEM format). Any number of pinned certificates (or none) may be specified. If any pinned certificates are specified then <imap_server_trustanchors> will be ignored, and the connection to the IMAP server will fail unless it responds to a TLS connection by sending an end-entity (EE) certificate which matches one of the pinned certificates.

Default value: -None-

XML element name: `imap_server_pinned`

Parent XML element: `<domain>`

Example:
`<imap_server_pinned>$(isode.dir.etc)remote.imap.pem</imap_server_pinned>`

2.5.10.5 Server Trust Anchors

Description: Specifies the path to a file that contains one or more CA certificates (in PEM format). Specifying this option forces Harrier Web 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.

This option is ignored if any values for <imap_server_pinned> are present.

Default value: -None-

XML element name: `imap_server_trustanchors`

Parent XML element: `<domain>`

Example:
`<imap_server_trustanchors>$(isode.dir.etc)imap.pem</imap_server_trustanchors>`

2.5.10.6 SASL PLAIN/LOGIN Usage

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

Default value: off

XML element name: `imap_plain_over_cleartext`

Parent XML element: `<domain>`

Example: `<imap_plain_over_cleartext>on</imap_plain_over_cleartext>`

2.5.10.7 STARTTLS Usage Policy

Description: Controls use or non use of STARTTLS. It can have one of the following 3 values: "mandatory" (always use STARTTLS, fail the connection if not advertised), "opportunistic" (try to use STARTTLS if advertised, but carry on regardless of STARTTLS success) and "suppress" (never use STARTTLS, even if advertised).

Default value: opportunistic

XML element name: `imap_starttls_policy`

Parent XML element: `<domain>`

Example: `<imap_starttls_policy>opportunistic</imap_starttls_policy>`

2.5.11 LDAP

This section describes options related to LDAP service connection and usage.

2.5.11.1 Host and Port

Description: Specifies the host and port of the LDAP server for this domain.

Default value: -None-

XML element name: `ldap_url`

Parent XML element: `<domain>`

Example: `<ldap_url>ldap.example.com:19389</ldap_url>`

2.5.11.2 Re-bind Interval

Description: Specifies how frequently Harrier Web Server should re-attempt to connect to an LDAP server after losing connection to it.

The value may be defined as number of seconds or number with unit: s/sec/seconds, m/min/minutes, h/hours, d/days, w/weeks.

Value 0 disables automatic re-bind.

Default value: 5s

XML element name: `ldap_rebind_interval`

Parent XML element: `<domain>`

Example: `<ldap_rebind_interval>5s</ldap_rebind_interval>`

2.5.11.3 SASL Mechanisms

Description: a 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 or the client are ignored from the list. The remaining mechanisms are tried in order. If this option is not specified (or specified with an empty value), then Harrier Web will use the first of the SASL mechanisms it recognises from those advertised by the LDAP server.

Default value: -None-

XML element name: `ldap_sasl_mechs`

Parent XML element: `<domain>`

Example: `<ldap_sasl_mechs>SCRAM-SHA-1</ldap_sasl_mechs>`

2.5.11.4 Server Pinned Certificates

Description: Each <ldap_server_pinned> element should contain the path to a file containing an X.509 certificate (in PEM format). Any number of pinned certificates (or none) may be specified. If any pinned certificates are specified then <ldap_server_trustanchors> will be ignored, and the connection to the LDAP server will fail unless it responds to a TLS connection by sending an end-entity (EE) certificate which matches one of the pinned certificates.

Default value: -None-

XML element name: `ldap_server_pinned`

Parent XML element: `<domain>`

Example:
`<ldap_server_pinned>$(isode.dir.etc)remote.ldap.pem</ldap_server_pinned>`

2.5.11.5 Server Trust Anchor

Description: Specifies the path to a file that contains one or more CA certificates (in PEM format). Specifying this option forces Harrier Web to use `StartTLS` for all LDAP connections, and to require that the LDAP server provides a certificate which can be verified using this set of CA certificates.

This option is ignored if any values for <ldap_server_pinned> are present.

Default value: -None-

XML element name: `ldap_server_trustanchors`

Parent XML element: `<domain>`

Example:
```
<ldap_server_trustanchors>$(isode.dir.etc)ldap.pem</ldap_server_trustanchors>
```

2.5.11.6 User Mail Attributes

Description: Comma-separated list of attributes which can be 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: mail,mailLocalAddress

XML element name: `ldap_user_mail_ats`

Parent XML element: `<domain>`

Example:
```
<ldap_user_mail_ats>mail,mailLocalAddress</ldap_user_mail_ats>
```

2.5.11.7 Custom User Mail Search Filter

Description: In certain cases the Harrier Web Server needs to locate a user's directory entry based on that user's email address - for example when displaying the user's picture on received messages, or obtain the user's certificate for validating the message signature. By default, Harrier Web Server will perform an ldap search using the filter generated. If the `<ldap_user_mail_filter>` option is specified, then this filter will be used instead.

Note that if the search results in more than one matching entry, then it is considered to have failed (e.g. no user picture will be displayed).

The LDAP search filter (see https://tools.ietf.org/search/rfc4515) is being used with `<ldap_addressbook_base_dn>` and special `$1` variable for searched user's email address.

Default value: empty, which means that the search filter will be generated to looks for matches in attributes specified by the `<ldap_user_mail_ats>` option (|(<first attribute>)(<second attribute>)...)(.

XML element name: `ldap_user_mail_filter`

Parent XML element: `<domain>`

Example:
```
<ldap_user_mail_filter>(|(mail=$1)(mailLocalAddress=$1))</ldap_user_mail_filter>
```

2.5.11.8 User Name Attributes

Description: This option provides a way to specify attributes which may contain alternate user friendly user name (used both by logged in user and address book) Value of this attribute also appears in the From header field of sent messages.

Default value: in ACP 127 mode: "plaNameACP127,displayName,CN", in military mode: "displayName,plaNameACP127,CN", in internet mode: "displayName,CN".

XML element name: `ldap_user_name_ats`

Parent XML element: `<domain>`

Example: `<ldap_user_name_ats>displayName,CN</ldap_user_name_ats>`

2.5.11.9 User Preferences Object Class

Description: this is 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 preferences. See Section 2.5.11.10, “User Preferences Attribute”.

Default value: isodeHarrierUser

XML element name: `ldap_user_prefs_oc`

Parent XML element: `<domain>`

Example: `<ldap_user_prefs_oc>isodeHarrierUser</ldap_user_prefs_oc>`

2.5.11.10 User Preferences Attribute

Description: this option specifies the directory attribute in user entries that is used to store Harrier-specific user preferences for a Harrier user (see Section 2.5.11.9, “User Preferences Object Class”.

Default value: harrierUserPreferences

XML element name: `ldap_user_prefs_at`

Parent XML element: `<domain>`

Example:
`<ldap_user_prefs_at>harrierUserPreferences</ldap_user_prefs_at>`

2.5.11.11 User Routing Indicator Attribute

Description: Attribute used as a user addresse's hint in ACP-127 mode.

Default value: rI

XML element name: `ldap_user_routing_indicator_at`

Parent XML element: `<domain>`

Example:
`<ldap_user_routing_indicator_at>rI</ldap_user_routing_indicator_at>`

2.5.11.12 Attributes Validation

Description: 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: true

XML element name: `ldap_validate_attributes`

Parent XML element: `<domain>`

Example: `<ldap_validate_attributes>false</ldap_validate_attributes>`

2.5.12 LDAP Address Book configuration

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 Web should search the LDAP directory when performing address-book lookups.

2.5.12.1 Base DN

Description: 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 (i.e. the root DN)

XML element name: `ldap_addressbook_base_dn`

Parent XML element: `<domain>`

Example:
```
<ldap_addressbook_base_dn>ou=staff,c=us</ldap_addressbook_base_dn>
```

2.5.12.2 Search Filter Attributes

Description: This option contains a list of attributes which will be searched . This option is used if `<filter>` is not specified. See Section 2.5.12.3, “Custom Search Filter”.

Default value: in ACP127 mode `displayName,sn,givenName,plaNameACP127,CN`; in other modes `displayName,sn,givenName,CN,mail,mailLocalAddress,mailRoutingAddress`.

XML element name: `ldap_addressbook_filter_ats`

Parent XML element: `<domain>`

Example:
```
<ldap_addressbook_filter_ats>cn,givenname,sn,mail</ldap_addressbook_filter_ats>
```

2.5.12.3 Custom Search Filter

Description: This option may be used to specify an LDAP search filter (see https://tools.ietf.org/search/rfc4515) that should be used when performing address book searches. The special string `$1` may be used in the filter string to indicate the user's seach string.

If this option is supplied, then the `<ats>` option is ignored (see Section 2.5.12.2, “Search Filter Attributes”).

Default value: empty, which means that the search simply looks for matches in attributes as specified by the `<ats>` option.

XML element name: `ldap_addressbook_filter`

Parent XML element: `<domain>`

Example:
```
<ldap_addressbook_filter>(&(mail=*)(cn=*$1))</ldap_addressbook_filter>
```

2.5.13 Security Labels

This section describes configuration options used to control how security labels are presented to the user in the web browser. Note that these options are ignored for *internet* mode.

2.5.13.1 Catalog

Description: Specifies the full file path of a security label catalog. 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 Section 2.5.13.2, “Policy”).

Default value: -None-

XML element name: `sio_catalog`

Parent XML element: `<domain>`

Example:
```
<sio_catalog>$(isode.dir.etc_or_share)label_catalog.xml</sio_catalog>
```

2.5.13.2 Policy

Description: Specifies the full file path of the security policy file to be 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.

Default value: -None-

XML element name: `sio_policy`

Parent XML element: `<domain>`

Example: `<sio_policy>$(isode.dir.etc_or_share)policy.xml</sio_policy>`

2.5.14 Subject Indicator Codes

This section describes configuration options used to control subject indicator codes support.

2.5.14.1 Catalog

Description: Specifies the full file path of a subject indicator codes catalog.

Default value: $(isode.dir.etc_or_share)/sic_catalog.xml

XML element name: `sics`

Parent XML element: `<domain>`

Example: `<sics>$$(isode.dir.etc_or_share)/sic_catalog.xml</sics>`

2.5.15 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.

2.5.15.1 Encrypt outgoing email by default

Description: 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) and each recipient of the message must have S/MIME certificate published in userCertificate attribute of her respective LDAP entry.

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

XML element name: `smime_encrypt`

Parent XML element: `<domain>`

Example: `<smime_encrypt>true</smime_encrypt>`

2.5.15.2 Encryption algorithm

Description: Specifies symmetric cipher used for encrypting S/MIME messages.

Default value: aes-256-cbc

XML element name: `smime_encrypt_algorithm`

Parent XML element: `<domain>`

Example:
`<smime_encrypt_algorithm>aes-128-cbc</smime_encrypt_algorithm>`

2.5.15.3 Sign outgoing email by default

Description: 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.

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

XML element name: `smime_sign`

Parent XML element: `<domain>`

Example: `<smime_sign>true</smime_sign>`

2.5.15.4 Protect message header when signing and/or encrypting outgoing email

Description: 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 commone 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: true, which means that header of outgoing messages from the domain will be S/MIME protected, unless explicitly disabled for a user account in LDAP.

XML element name: `smime_protect_header`

Parent XML element: `<domain>`

Example: `<smime_protect_header>false</smime_protect_header>`

2.5.15.5 Automatically generate user's S/MIME certificate requests

Description: 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 `smime_csr_path` directory and the corresponding private key is saved in the `smime_pkcs12_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 `smime_csr_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 `smime_csr_path` and `smime_pkcs12_path` must be set to non empty values.

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

XML element name: `smime_auto_generate_csrs`

Parent XML element: `<domain>`

Example: `<smime_auto_generate_csrs>true</smime_auto_generate_csrs>`

2.5.15.6 CSR and Certificate location path

Description: This option specifies the filesystem directory where S/MIME CSRs will be generated by Harrier Web Server and where the corresponding certificate (PEM) files should also be saved. This option is ignored, unless S/MIME signing and/or encryption is also enabled for the user and `smime_auto_generate_csrs` is enabled.

Default value: -None-

XML element name: `smime_csr_path`

Parent XML element: `<domain>`

Example: `<smime_csr_path>/etc/isode/smime/csr</smime_csr_path>`

2.5.15.7 PKCS#12 location path

Description: This option specifies the 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. This option is ignored, unless S/MIME signing and/or encryption is also enabled for the user and `smime_auto_generate_csrs` is enabled.

Default value: -None-

XML element name: `smime_pkcs12_path`

Parent XML element: `<domain>`

Example:
`<smime_pkcs12_path>/etc/isode/smime/pkcs12</smime_pkcs12_path>`

2.5.15.8 Key Size

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

Default value: 0 which means RSA default (2048 bits)

XML element name: `smime_key_size`

Parent XML element: `<domain>`

Example: `<smime_key_size>2048</smime_key_size>`

2.5.16 SMTP

This section describes options related to SMTP service connection and usage.

2.5.16.1 Host and Port

Description: Specifies the host and port of the SMTP server for this domain.

Default value: -None-

XML element name: `smtp_url`

Parent XML element: `<domain>`

Example: `<smtp_url>smtp.example.com:587</smtp_url>`

2.5.16.2 Server Pinned Certificates

Description: Each <smtp_server_pinned> element should contain the path to a file containing an X.509 certificate (in PEM format). Any number of pinned certificates (or none) may be specified. If any pinned certificates are specified then <smtp_server_trustanchors> will be ignored, and the connection to the SMTP server will fail unless it responds to a TLS connection by sending an end-entity (EE) certificate which matches one of the pinned certificates.

Default value: -None-

XML element name: `smtp_server_pinned`

Parent XML element: `<domain>`

Example:
`<smtp_server_pinned>$(isode.dir.etc)remote.smtp.pem</smtp_server_pinned>`

2.5.16.3 Server Trust Anchor

Description: Specifies the path to a file that contains one or more CA certificates (in PEM format). Specifying this option forces Harrier Web 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.

This option is ignored if any values for <smtp_server_pinned> are present.

Default value: -None-

XML element name: `smtp_server_trustanchors`

Parent XML element: `<domain>`

Example:
`<smtp_server_trustanchors>$(isode.dir.etc)smtp.pem</smtp_server_trustanchors>`

2.5.16.4 SASL PLAIN/LOGIN Usage

Description: Controls whether SASL PLAIN and SASL LOGIN can be used without TLS in SMTP.

Default value: off

XML element name: `smtp_plain_over_cleartext`

Parent XML element: `<domain>`

Example: `<smtp_plain_over_cleartext>on</smtp_plain_over_cleartext>`

2.5.16.5 STARTTLS Usage Policy

Description: Controls use or non use of STARTTLS. It can have one of the following 3 values: "mandatory" (always use STARTTLS, fail the connection if not advertised), "opportunistic" (try to use STARTTLS if advertised, but carry on regardless of STARTTLS success) and "suppress" (never use STARTTLS, even if advertised).

Default value: opportunistic

XML element name: `smtp_starttls_policy`

Parent XML element: `<domain>`

Example: `<smtp_starttls_policy>opportunistic</smtp_starttls_policy>`

2.5.17 Draft and release

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

2.5.17.1 Releaser Address

Description: 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_address`. When Draft & Release procedure is in effect, an extra field with all configured Releaser email addresses is shown in the Compose window. Releaser(s) will receive all messages and can reject (return to Drafter), release (send to the originally intended recipients) or edit and send each individual message.

This option can appear multiple times. If this option appears multiple times 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 `releaser_required` is also set to "on" or "true".

XML element name: `releaser_address`

Parent XML element: `<domain>`

Example: `<releaser_address>releaser@example.org</releaser_address>`

2.5.17.2 Enable Draft & Release procedure

Description: This option enables Draft & Release procedure for the domain, which 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, an extra field for the Releaser(s)

email address(es) is shown in the Compose window. Releaser(s) will receive all messages and can reject (return to Drafter), release (send to the originally intended recipients) edit and send each individual message.

If `releaser_address` 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 that option is not specified, the field remains empty and it needs to be entered manually.

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

Default value: off, which means that the Draft & Release procedure is not used for the domain, unless the `releaser_address` option is also set.

XML element name: `releaser_required`

Parent XML element: `<domain>`

Example: `<releaser_required>on</releaser_required>`

2.5.17.3 Conditional Draft & Release

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 "default releaser" and one will be selected automatically on Send.

Each conditional rule is defined using `release_policy_rule` XML option with some attributes (see below). 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 XML attribute specifies condition that 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 "inverse", which is treated specially.

Supported conditions are defined below:

a) sics=<list of ;-separated SIC codes that trigger this rule>. Any of the SICs has to match. **Example:** `<release_policy_rule sics="AAA;BBB;CCC">steve@example.com</release_policy_rule>`

b) precedence=<number or a precedence keyword, such as 'flash' or 'override'>. All messages with the action precedence which is the same or higher than this value trigger this rule. **Example:** `<release_policy_rule precedence="flash">nick@example.com</release_policy_rule>`

c) domain=<destination domain>. If any of the message recipients is in the specified domain, this rule is triggered. Note, that only a single domain can be specified in a single rule. **Example:** `<release_policy_rule domain="isode.net">alex@example.com</release_policy_rule>`

d) sender=<email address>. A message with From or Sender header field containing the specified email address will trigger this rule. **Example:** `<release_policy_rule sender="alex@example.com">damy@example.com</release_policy_rule>` All messages that contain From/Sender alex@example.com will use damy@example.com as the Releaser.

e) inverse=<any text>. Used to inverse (logical NOT) all conditions. This is useful to specify rules which apply if domain or list of SICs is not in the list. **Example:** `<release_policy_rule domain="example.com" inverse="yes">alex@example.com</release_policy_rule>` All messages that contain at least one recipient NOT in @example.com will use alex@example.com as the Releaser.

More complicated example 1: `<release_policy_rule precedence="flash" sics="ZZZ;WWW">mir@example.com</release_policy_rule>` 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"}.

More complicated example 2: `<release_policy_rule domain="example.net" sender="jengo@example.com">mir@example.com</release_policy_rule>` 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".

Default value: empty, which means that the Draft & Release procedure is not used for the domain, unless the `releaser_address` option is also set.

XML element name: `release_policy_rule`

Parent XML element: `<domain>`

2.5.17.4 Addresses Exempt from Draft & Release procedure

Description: This option includes an email address exempted from Draft & Release. This option can appear multiple times.

Default value: empty, which means that no user (other than Releasers specified in `releaser_address` or `release_policy_rule`) is exempt from the Draft & Release procedure.

XML element name: `exempted_address`

Parent XML element: `<domain>`

Example: `<exempted_address>co@example.org</exempted_address>`

2.5.18 Organizational Messaging

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.

2.5.18.1 Organizational From Address

Description: This option specifies the email address that will be used as the 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, Organizational Messaging is not enabled for the domain.

Default value: empty, which means that the Organizational Messaging procedure is not used for the domain.

XML element name: `org_address`

Parent XML element: `<domain>`

Example: `<org_address>support@example.org</org_address>`

2.5.18.2 Organizational Address Friendly Name

Description: This option specifies the friendly name that would appear together with the `org_address` in the From header field value. This option is ignored if `org_address` is not set.

Default value: empty.

XML element name: `org_name`

Parent XML element: `<domain>`

Example: `<org_name>Customer Support</org_name>`

2.5.18.3 Allow sending as self when Organizational Messaging is enabled

Description: When Organisation Messaging is enabled by `org_address`, this option is used to control whether a logged in user can send email messages from himself/herself or just on behalf of the Organization.

Default value: false.

XML element name: `org_allow_send_as_self`

Parent XML element: `<domain>`

Example: `<org_allow_send_as_self>true</org_allow_send_as_self>`

2.6 Server Modes

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

2.6.1 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 Section 2.5.5, “Mode”.

2.6.2 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 Section 2.5.14, “Subject Indicator Codes”.

- Message Type support with server side configuration of MMHS types catalogue. See mmhs-types at Section 2.4.4.1, “URL mapping”.
- 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 2.6.3, “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 Section 2.5.4, “Military Sort Order”

Military mode is configured using the *mode* option in the configuration file. See Section 2.5.5, “Mode”.

2.6.3 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 Section 2.5.5, “Mode”.

2.7 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.

2.8 Obfuscation of passwords

The *(ETCDIR)/harrier_web_conf.xml* file which configures how Harrier Web Server connects to other servers can contain passwords. These can be obfuscated using the Service Key facility. To do this:

- The `servpass` option must be specified in the configuration file. See Section 2.4.3.1, "servpass:info". For example:

  ```
  <servpass:info service="isode.harrier"/>
  ```

- Any `password` field containing a password to be obfuscated should Fields containing passwords should have a `servpass:encrypt` attribute:

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

- Create a service password using the command line tool *(SBINDIR)/spassmgt*:

  ```
  % spassmgt set isode.harrier
  ```

  The tool will prompt for a passphrase (16 characters minimum, and must contain at least three out of uppercase, lowercase, numeric digits and punctuation).

  On Unix systems, you need to run this command as whatever userid the Harrier Web Server process is using (see Section 2.1.2, "Harrier Web Server runtime user").

- Encrypt the passwords in your config file, using the *(SBINDIR)/spasscrypt* command-line tool:

  ```
  % spasscrypt -e -s isode.harrier
  -x /etc/isode/harrier_web_conf.xml
  Passphrase:
  Re-enter:
  ```

Once the `spasscrypt` tool has been executed, the passwords in the configuration file will no longer be stored in plain text, and will appear something like this:

```
<password servpass:encrypt="true">
{spcrypt2}Qly6XR/iQhKSHREM+JwT30HJygO/WwQMWFg </password>
```

Chapter 3 Features

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

3.1 Security Labels

Harrier Web Server supports security labels for messages as per RFC7444 [https://tools.ieft.org/html/rfc7444]. 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 2.5.13, “Security Labels”), 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
```

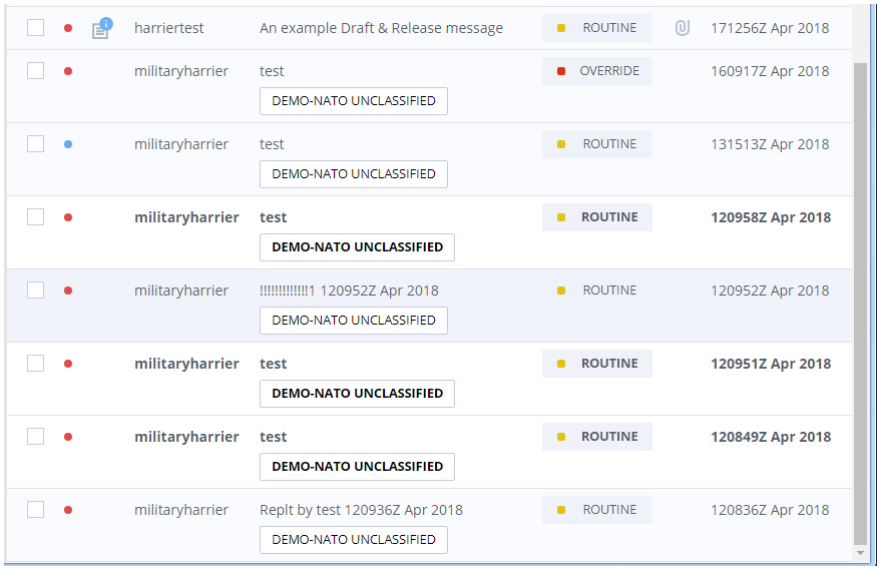
3.2 Draft & Release

Draft & Release allows outgoing messages to be reviewed before they are sent out to intended recipients. When a Draft & Release policy has been configured, messages that are sent by any users who are designated as "drafters" will appear in the INBOX of a designated "releaser". A releaser can review each draft message, and can choose either to approve ("release"), reject the it, or edit the message and then submit it. Messages which are released are 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, or to abandon the attempt.

In Draft & Release mode, Drafters compose messages in the usual manner, but will see an extra "Releaser" field in the Compose window. Depending on policy, the Drafter may be forced to use a specific Releaser, or may be able to choose from a list of Releasers.

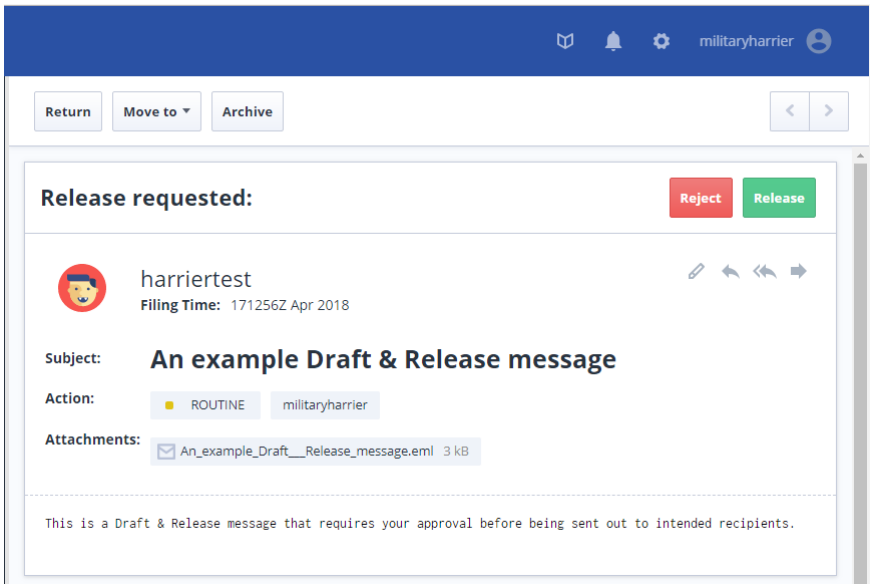
A Releaser's message list contains icons to indicate which messages are "draft" messages, and whether they need to be reviewed, or have been reviewed already.

Figure 3.1. Message list with an unprocessed Draft & Release message



They also have extra buttons for release/reject in the message view.

Figure 3.2. Message view with Draft & Release related action buttons



In order to enable Draft & Release, the Harrier administrator needs to specify `releaser_address` value(s) and/or `release_policy_rule` value(s). `exempted_address` option can be used to exclude some senders from Draft & Release procedure.

`releaser_address` option is used to define one or more unconditional Releasers, i.e. a Releaser authorised to review all messages sent. `release_policy_rule` option is used to define one or more conditional Releasers, i.e. Releasers responsible for reviewing messages that satisfy certain criteria, for example all messages with a particular SIC code, all messages with FLASH precedence or all messages from particular senders.

3.3 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.

3.3.1 S/MIME signing/encryption

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 use the following option under the corresponding <domain> XML element: `<smime_sign>true</smime_sign>` To enable encryption use the following option under the corresponding <domain> XML element: `<smime_encrypt>true</smime_encrypt>`

When sending messages, it is possible to disable S/MIME signing/encryption on per message basis. (It is not possible to enable signing/encryption for a message, if it is disabled for the user.) A Harrier user can see whether S/MIME signing/encryption 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 XML configuration) or for the specific user (in LDAP); 2) the domain has LDAP configured and all users can bind to Directory using the same username/password as used for IMAP login; 3) the user's LDAP entry must have a userPKCS12 attribute, containing the private key and corresponding certificate, encrypted with the user's login password. 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.

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) encryption must be enabled for the domain (in XML configuration) or for the specific user (in LDAP); 2) the domain has LDAP configured and all users can bind to Directory using the same username/password as used for IMAP login; 3) the user's LDAP entry must have a userPKCS12 attribute, containing the private key and corresponding certificate, encrypted with the user's login password. 4) each recipient's LDAP entry must contain userCertificate attribute 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.

3.3.2 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:

```
<smime_auto_generate_csrs>on</smime_auto_generate_csrs>
<smime_csr_path>$(isode.dir.var)csr</smime_csr_path>
<smime_pkcs12_path>$(isode.dir.var)pkcs12</smime_pkcs12_path>
```

`smime_csr_path` specifies filesystem directory where automatically generated S/MIME CSR files (and corresponding PEM files) will be written. The directory must exist.

`smime_pkcs12_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 <smime_csr_path> and <smime_pkcs12_path> respectively. (Note that the system administrator doesn't need access to the <smime_pkcs12_path> directory.) The system administrator should review the <smime_csr_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, and once corresponding certificates have been issued, they should be placed in the <smime_csr_path> directory as PEM files. 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.

3.3.3 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 end-entity certificates. List all Trust Anchors in `smime_trusted_certificate` XML elements under the top level `harrier` element. List all intermediate Certification Authorities in `smime_intermediate_certificate`.

In order to be able to decrypt messages, Harrier needs to access to user's private key stored in LDAP Directory. This uses the same configuration that is needed for encryption.

3.4 Organizational Messaging

Harrier Web Server supports Organizational Messaging. Organizational Messaging allows users to send email messages on behalf of their organizations, for example an Engineering Officer on a ship HMS Kent sending a message to HQ on behalf of HMS Kent.

3.5 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.

3.5.1 Charset

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

Default value: -None-

Example: ITA2

LDAP attribute name: `harrierCharsetRestrictions`

3.5.2 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`

3.5.3 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`

3.6 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.

3.7 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 mailboxes are sorted by the arrival time, which is the time they were delivered (using SMTP) or uploaded to the corresponding mailbox. When military sort order is enabled, messages in the 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 (depending on whether the recipient is an Action or Info recipient), 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 user. See the `act_by` option for more details.