HARRIERWEB-4.0

Harrier User Guide

Isode

Table of Contents

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

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

Isode software is © copyright Isode Limited 2002-2024, all rights reserved.

Isode software is a compilation of software of which Isode Limited is either the copyright holder or licensee.

Acquisition and use of this software and related materials for any purpose requires a written licence agreement from Isode Limited, or a written licence from an organization licensed by Isode Limited to grant such a licence.

This manual is © copyright Isode Limited 2024.

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 Users of Harrier as a Messaging Client using a standard web-browser interface for clients wishing to use Military Messaging or Internet Mail. Administrators who plan to configure Harrier Web, are recommended to read the Harrier Web Server Administration Guide.

3 Related publications

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

Volume	Title
SWADM	*M-Switch Administration 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
Input to the system	`cd newdir`
Cross references	see Section 2, “Readership”
Additional information to note, or a warning that the system could be damaged by certain actions.	Notes are additional information; cautions are warnings.

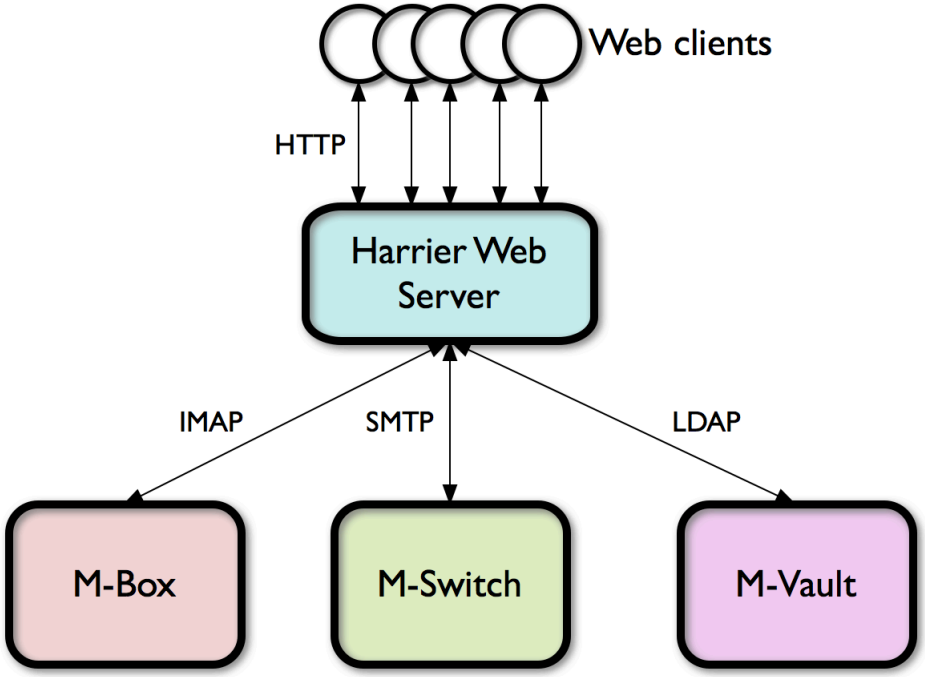
Chapter 1 Introduction to Harrier Web

This section introduces Harrier Web server and describes how the Web Browsers clients, Harrier Web Server and other Messaging Servers work together.

1.1 Overview

Harrier is Web messaging server, supporting both formal Military Message Handling and email. It provides a range of security and other capabilities for both MMHS and email. Harrier provides a zero-footprint web mail client that allows user and role-based access to mailboxes. 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 Getting Started

This section talks about how to connect to Harrier Web Server, and the different modes of operation available in Harrier.

2.1 Server Modes

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

2.1.1 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.

2.1.2 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.
- Message Type support with server side configuration of MMHS types catalogue.
- 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 2.1.3, “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.

2.1.3 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.

Chapter 3 Drafter-centric Review

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

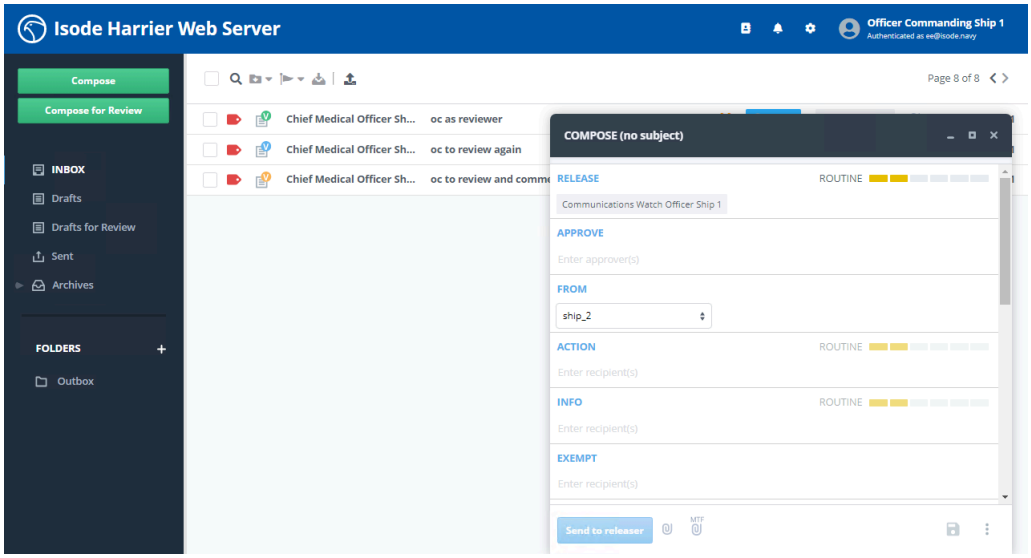
3.1 Drafter-centric Review

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. 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 3.1. Compose for Review window



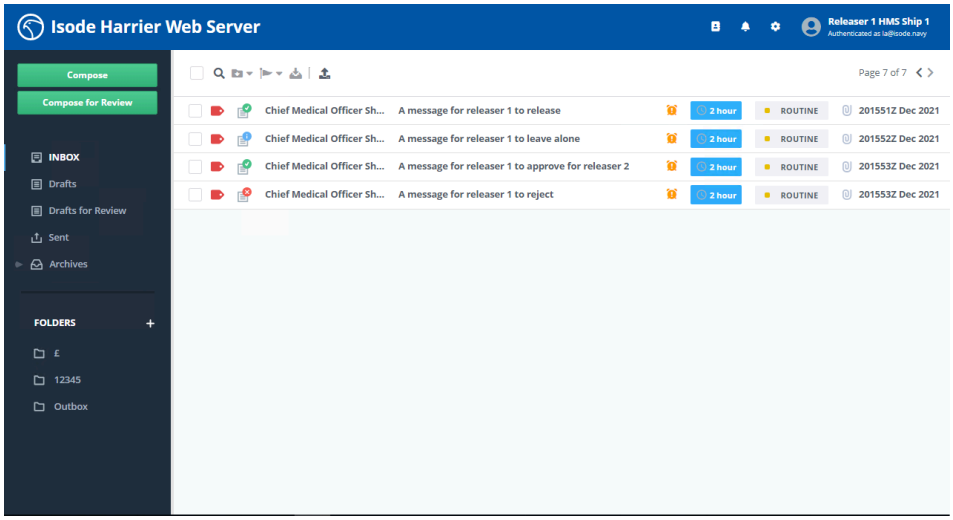
A Reviewer's message list contains icons to indicate which messages are "draft-for-review" messages, and whether they need to be reviewed, or have been reviewed already. The screenshot below has examples of 3 icons you may see on a Drafter-centric Review message.

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.

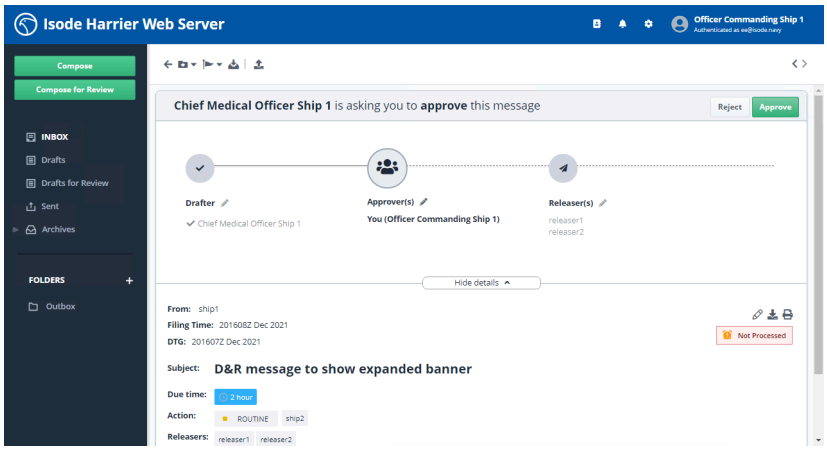
The yellow icon indicates a message that has been commented on.

Figure 3.2. Message list with examples of Drafter-centric Review icons



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

Figure 3.3. Message view with Drafter-centric Review related action buttons



Chapter 4 Draft And Release

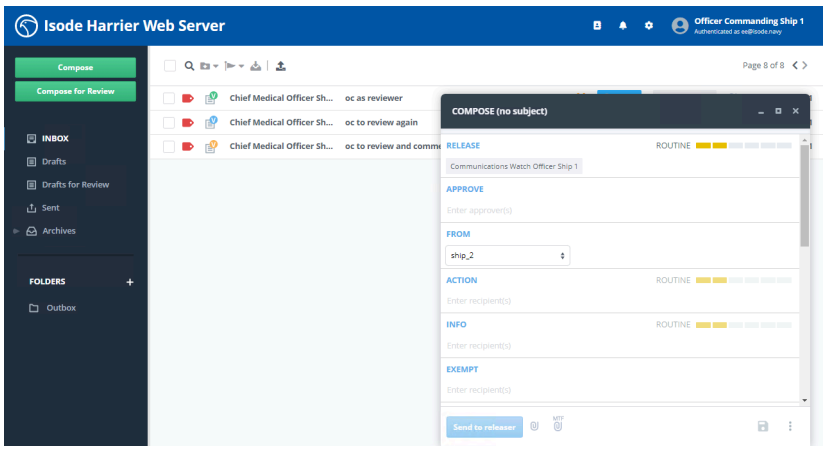
This section introduces Draft and Release and explains how this feature of Harrier is presented to the Harrier User.

4.1 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.

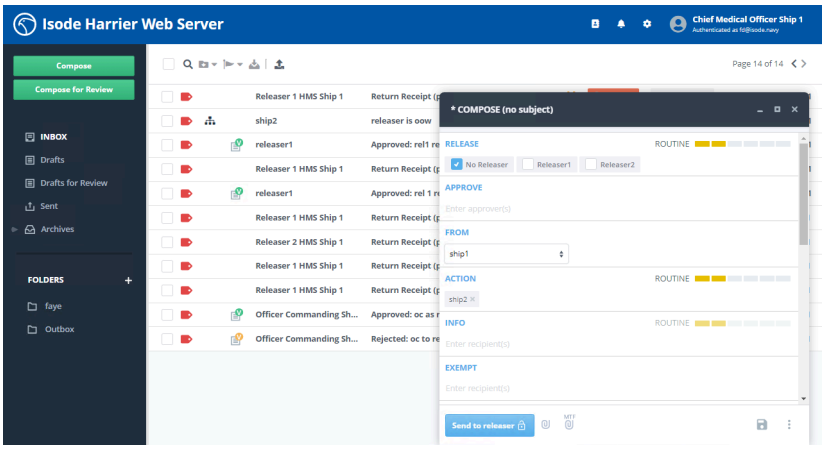
In Draft & Release mode, Drafters compose messages in the usual manner, but will see two extra fields in the Compose window: "Releaser" field and (optional) "Approver" field. Depending on policy, the Drafter may be forced to use a specific Releaser, or may be able to choose from a list of Releasers. 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 4.1. Compose Draft & Release message with required releaser



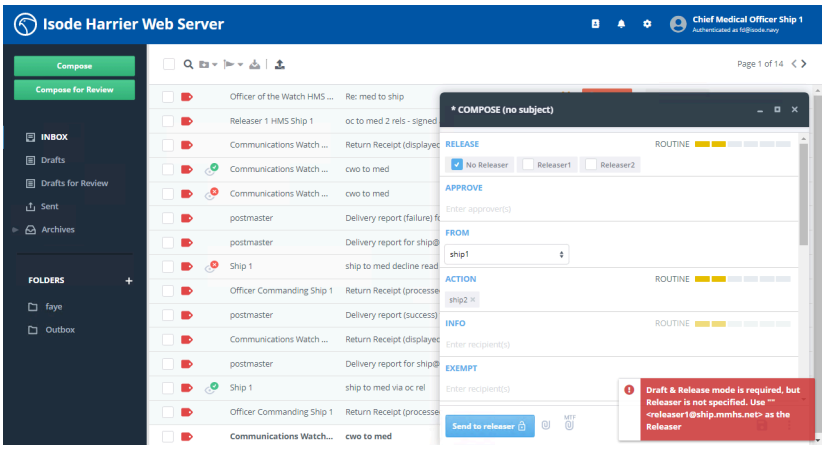
The following screenshot shows what the "Compose" screen may look like for a "From" organization which has multiple releasers configured, and a drafter who is configured to be able to draft and also to send direct in certain circumstances. The drafter may select from the releasers listed and can also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

Figure 4.2. Compose Draft & Release message with multiple releaser options



"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 4.3. Draft & Release message with required releaser



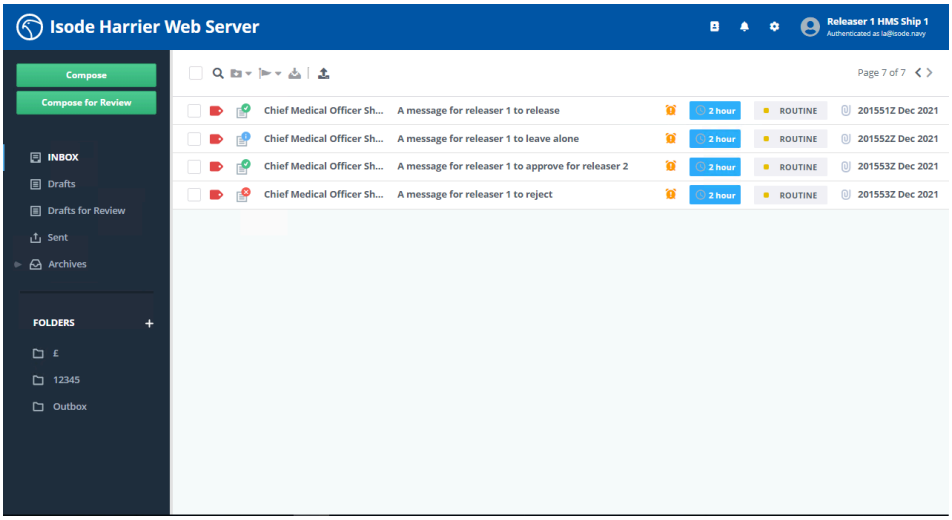
A Releaser's/Approver's message list contains icons to indicate which messages are "draft" messages, and whether they need to be approved, or have been approved already. The screenshot below has examples of 3 different icons you may see on a Draft & Release message.

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.

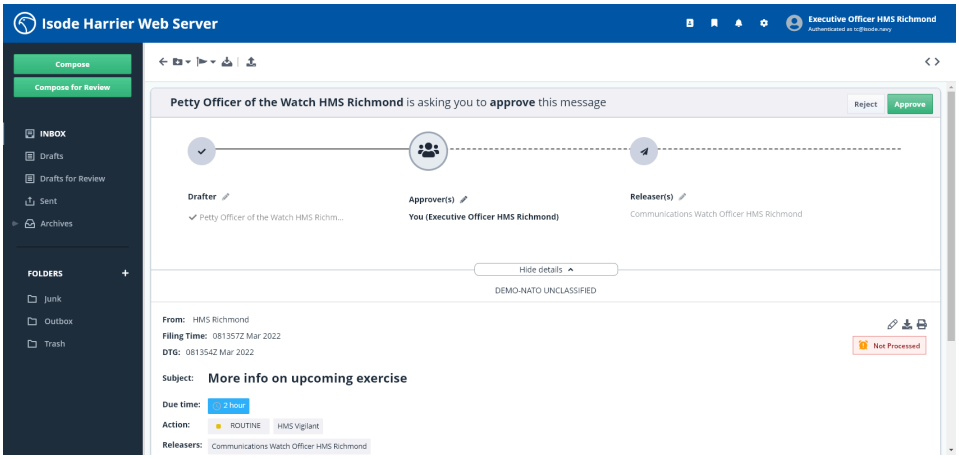
The red icon indicates a message that has been rejected.

Figure 4.4. Message list with examples of Draft & Release icons



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 4.5. Message view with Draft & Release related action buttons



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 certain criteria. For example all messages with a particular SIC code, all messages with FLASH precedence or all messages from particular senders.

4.1.1 Expected Behaviours

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

4.1.1.1 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.
- 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 instruction for approvers/releasers, in case they use a Mail User Agent different from Harrier.

- 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 messages which do not have a releaser.

4.1.1.2 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. 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.

4.1.1.3 Expected behaviour when releasing a message

- The to be released message is sent to the recipients specified by the drafter. It will include the list of releasers that approved it.
- The to be released message is copied into the releaser's "Sent" folder
- The corresponding Draft & Release message is marked as released, which is visible in the scan listing or in the message view.
- If drafter has requested confirmation of release, an MDN is sent to the drafter. This option is turned on by default.

4.1.1.4 Expected behaviour when rejecting a message

- A rejection message is sent to the drafter. It is similar to the Draft & Release message from which it was generated, but its first part contains the rejection note specified by approver/releaser.
- The rejection message is copied into the releaser's "Sent" folder.
- The Draft & Release message that was rejected is marked as rejected, which is visible in the scan listing or in the message view.

4.1.1.5 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 to suppress further MDNs from being generated. 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.

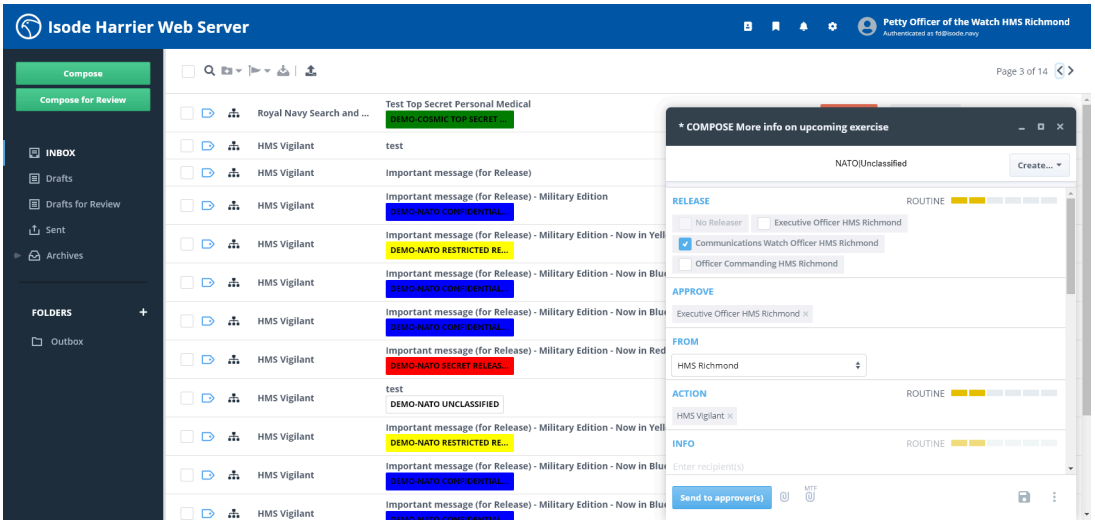
4.1.2 Using Draft & Release

The following sub-sections show examples of Draft & Release in use.

4.1.2.1 Sending and releasing a Draft & Release message

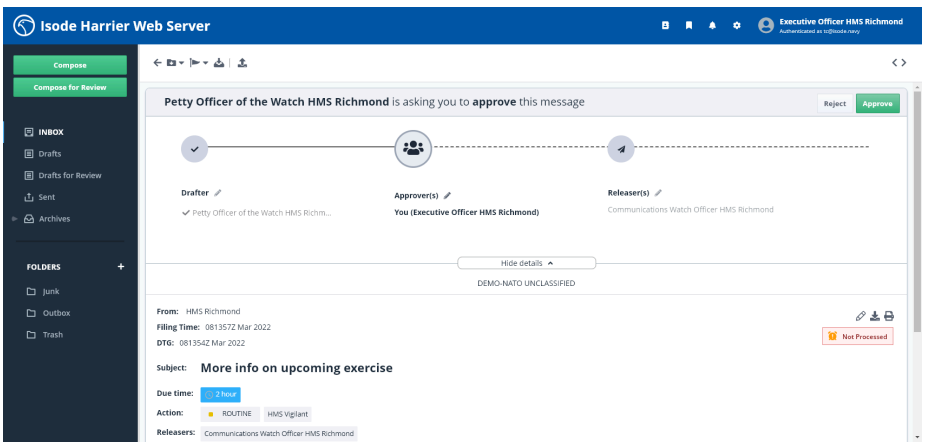
Allowed releasers will appear in a field in the compose box, where desired releasers can be selected with a mouse. There is another field for optional approvers. (Addressbook can be used for entering approvers, in the same way addressbook can be used for Action/ Info recipients.) If you add an approver you will see a **Send to approver** button as in the picture below. (If no approver is specified, you will see a button that says **Send to releaser**.)

Figure 4.6. Sending and Releasing a Draft & Release message - Compose



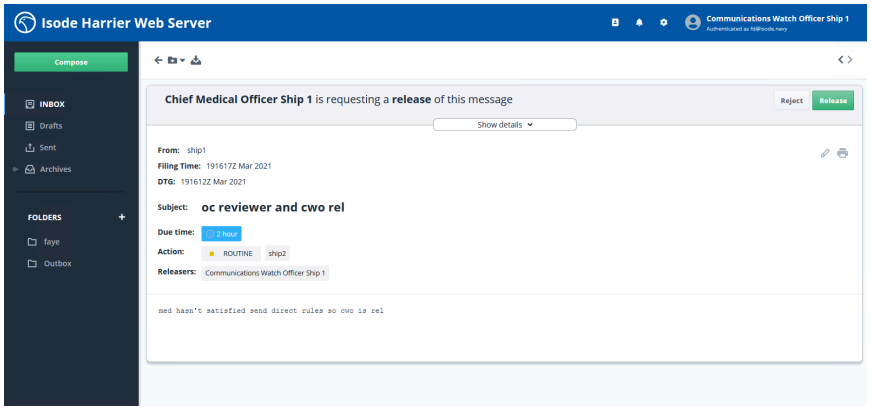
The message will be delivered to the first specified approver who can reject it or select "Approve" in order to pass on to the next approver/releaser

Figure 4.7. Sending and Releasing a Draft & Release message - Approve



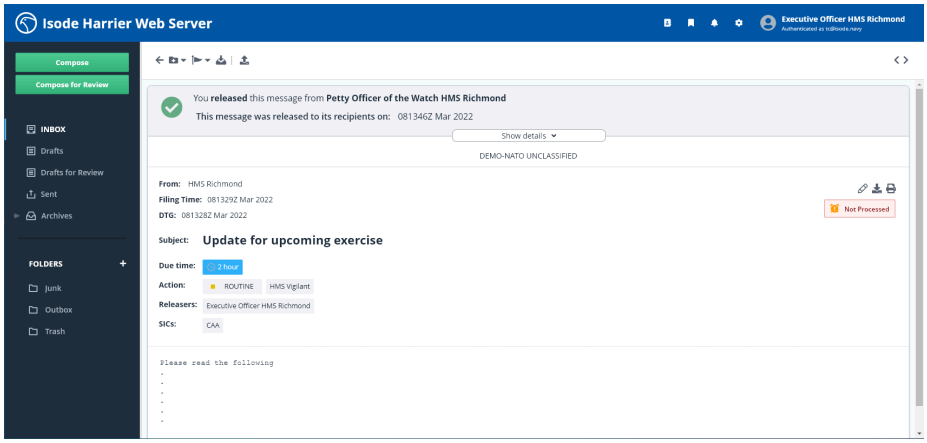
The last releaser may release the message if appropriate

Figure 4.8. Sending and Releasing a Draft & Release message - Release



Upon release, the message will update to inform the user that the message has been released to its recipients, and include a timestamp.

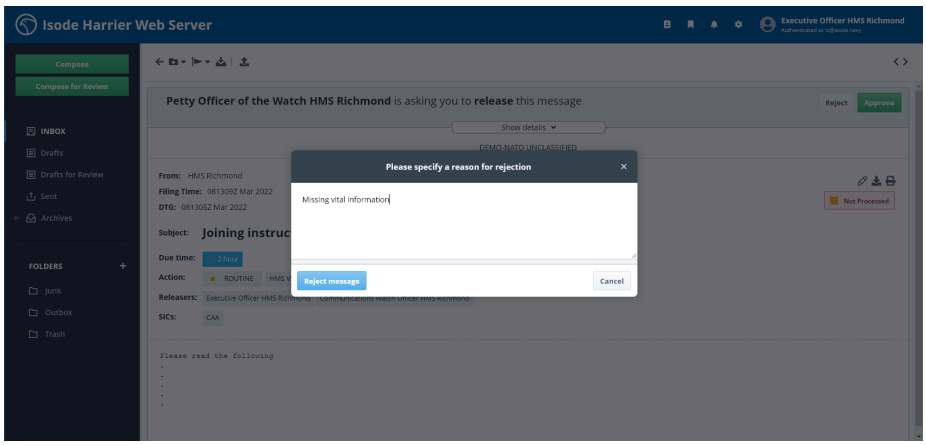
Figure 4.9. Sending and Releasing a Draft & Release message - Released



4.1.2.2 Rejecting a Draft & Release message

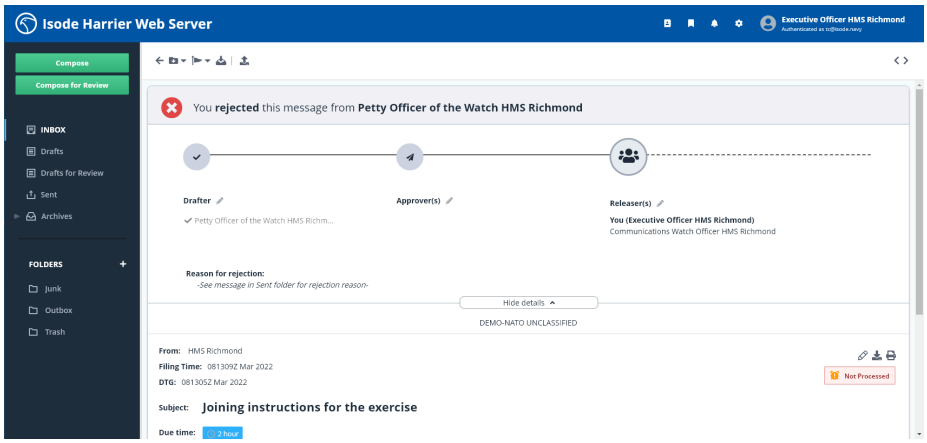
If an approver or a releaser decides to reject the Draft & Release message, they will be required to provide their reason for the rejection.

Figure 4.10. Rejecting a Draft & Release message - Rejection reason



Rejection of a message will result in a notification to the drafter with the reason specified as a part of the rejection message

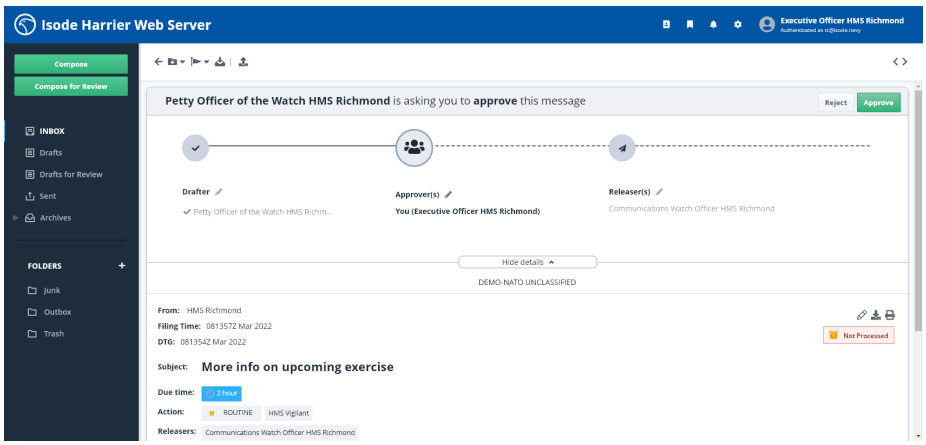
Figure 4.11. Rejecting a Draft & Release message - Rejection notification



4.1.2.3 Changing the Drafter, Approver(s) or Releaser(s)

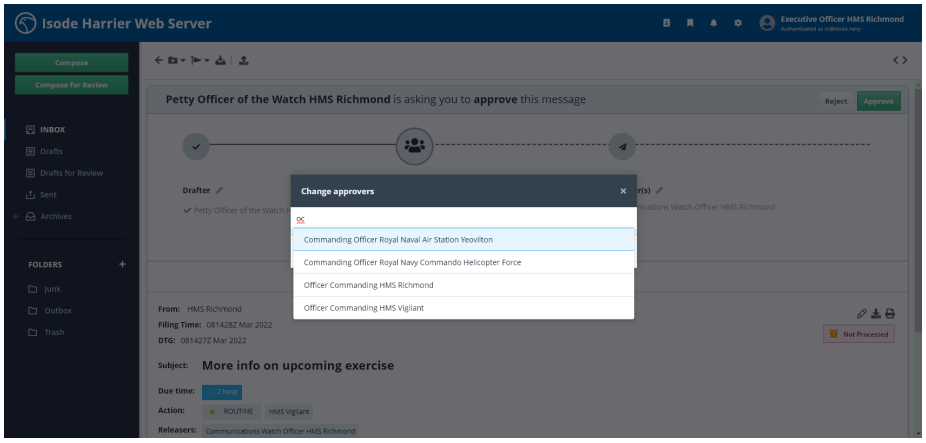
If there is no need to edit the message itself but you would like to change the drafter, approver(s) or releaser(s), you can do so by expanding the Draft & Release panel and clicking on the edit icon near the desired field.

Figure 4.12. Change Drafter / Approver / Releaser



Select one of the options and input the desired new address(es) when prompted.

Figure 4.13. Input new approver address



After applying changes the new approver/releaser will now receive the message for further review/approval. (Note that it is not possible to delete approvers/releasers who already approved the message.) If the edited message was not approved/rejected, it will be replaced by a new message with changed approver(s)/releaser(s)/drafter. If the

message was already rejected, a new message will be added to approver's/releaser's scan list for the current folder. This new message can now be actioned, i.e. approved or rejected.

You may also make changes to the approvers and releasers while editing the contents of the message. If you click on the edit icon, a compose box will appear and you can add and delete approvers and releasers here.

Chapter 5 Profiled Messages

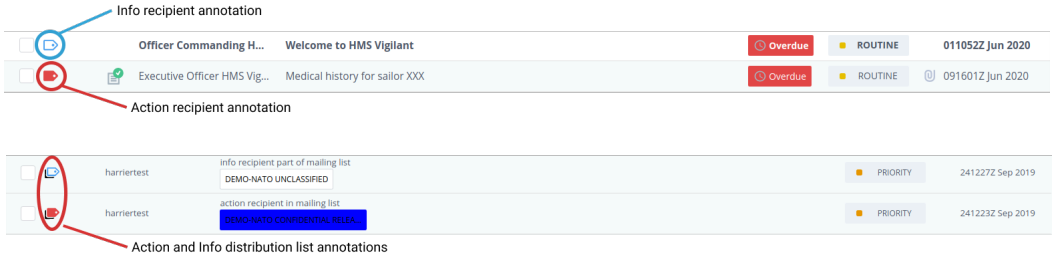
This section explains how Profiled Messages are presented to the User.

5.1 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. 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.

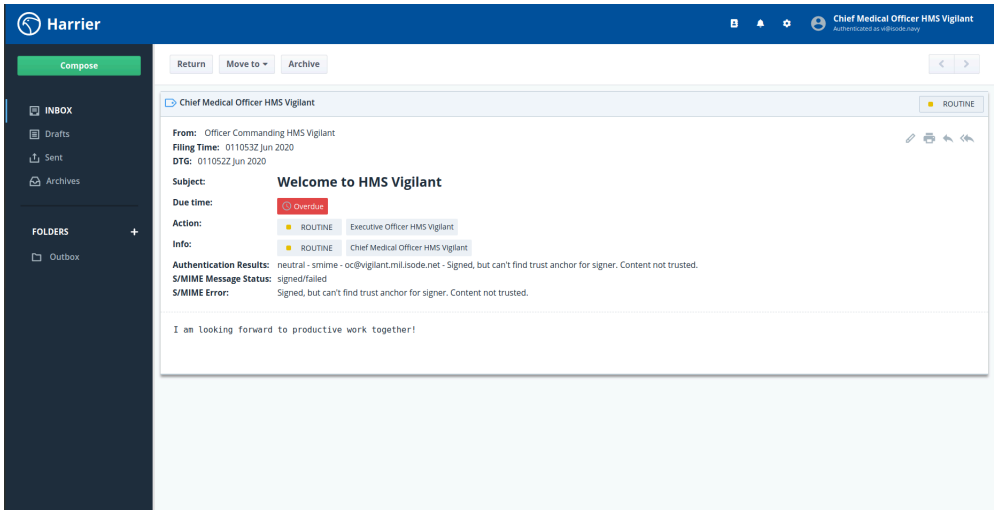
On the scan-list, the user can look at all of the messages and see the recipient type as an icon.

Figure 5.1. Scan-list view of recipient type bar



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 5.2. Message pane view of recipient type bar



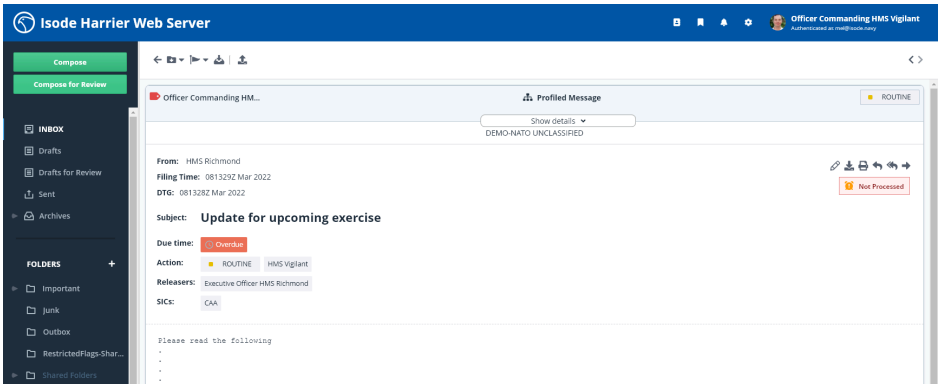
5.2 Display of profiled messages

Harrier Web supports profiled messages and their display. When a message has been through a profiler, the profiler distributes the message based on its various attributes. Harrier then presents that message to the users accordingly and passes on the profiled information. Results of this process are displayed in the message pane and the message is also marked as profiled in the scan-list.

Figure 5.3. Scan-list view of Profiled message

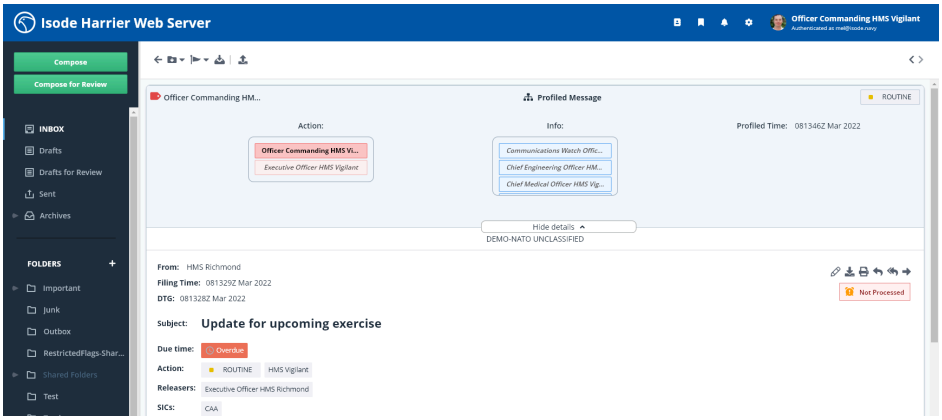
When viewing the message, the user is presented with a bar very similar to the one displayed when looking at the recipient type information. That bar contains details about the recipient type and the precedence of the message as well as it notifies the user that the message has been through a profiler.

Figure 5.4. Message pane view of a profiled message



When the user expands the bar, they can inspect in detail who the message was distributed to and when it was profiled. In addition to that, the user would be able to see who they received the message as based on the role they are logged in as.

Figure 5.5. Message pane view of a profiled message (expanded)



Chapter 6 S/MIME

This section talks about S/MIME related features.

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 or globally per user's domain.

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 or for the specific user; 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 user's LDAP entry contains the private key and corresponding certificate. Because of the last point, Harrier system administrator either needs to manage private keys/certificates for each user or needs to enable automatic CSR generation for users.

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 or for the specific user; 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 contains the private key and corresponding certificate. 4) each recipient's LDAP entry contains 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 $\rightarrow$ encrypt $\rightarrow$ 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) triple-wrap must be enabled for the domain; 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 contain the private key and corresponding certificate; 4) user must not have signing and/or encryption explicitly disabled; 5) each recipient's LDAP entry must contain 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

Harrier supports configuration when private keys/CSR are generated automatically. Generated CSRs can then be sent to a Certificate Authority for certificate generation or be processed with Sodium CA.

Provided CSR generation is enabled by Harrier system administrator, then whenever a user logs in, Harrier will check to see whether a valid certificate is configured for the user. If not, Harrier will generate a key pair and corresponding CSR. Harrier system administrator can access generated CSRs to issue certificates (using Sodium CA or by sending them to a third party Certificate Authority). Once the certificate is issued, when the user logs in, Harrier will import the certificate and private key into user's LDAP entry. Following this, the user will be able to sign and encrypt messages, and to receive encrypted messages from other users.

6.1.2.3 S/MIME verification/decryption

This happens automatically for all received messages. Harrier system administrator needs to configure correct Trust Anchors for this to work properly.

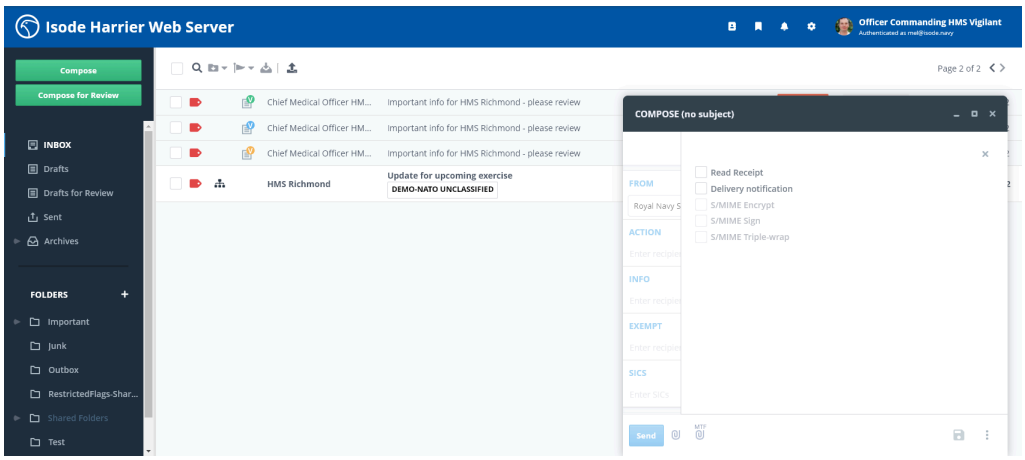
In order to be able to decrypt messages, Harrier needs to access user's private key stored in user's LDAP entry. This uses the same configuration that is needed for encryption. Note that decryption can be performed even if the certificate that corresponds to a private key is expired.

6.1.3 Expected Behaviours

The following sub-sections describe the various behaviours that are expected when performing S/MIME functionalities when sending messages.

Overall behaviour of when S/MIME has not been configured and/or a user has invalid certificates (be it revoked or expired) should not vary much and Harrier should resolve the cases in a similar manner. For example, when sending a message from a user/sender that does not have S/MIME configured and sending a message from a user/sender that has a revoked or expired certificate, are expected to have the same use case:

Figure 6.1. Composing with invalid or non-existent S/MIME configuration



- The user is presented with a standard compose form
- None of the S/MIME options are selected in the ‘More options’ menu in Compose
- All of the S/MIME options are disabled in the ‘More options’ menu in Compose
- User composes and sends a message as they will usually send a message
- Receiver gets the message and can see that the S/MIME status is empty.

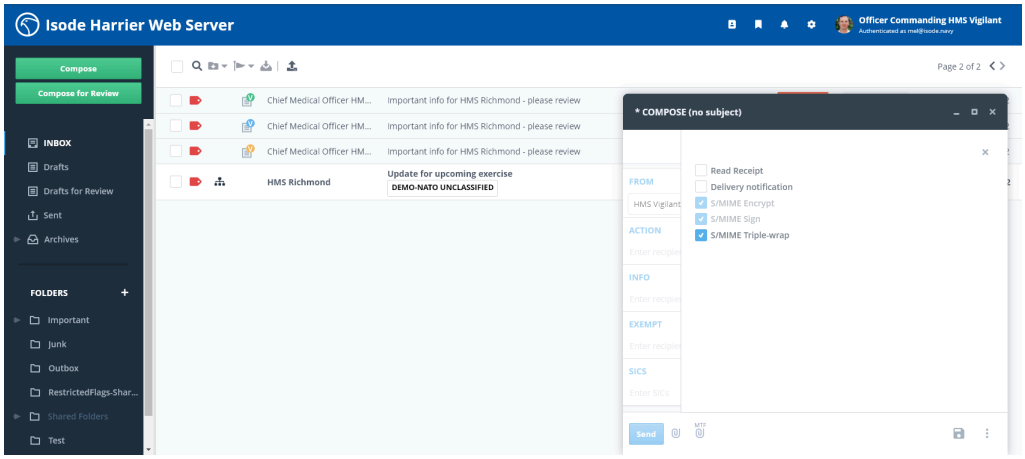
Note that Harrier is doing signature verification and decryption even if S/MIME signing and/or encryption is disabled.

Expected behaviour with the following optimal server configuration:

S/MIME Sign	S/MIME Encrypt	S/MIME Triple-wrap
true	true	true

1. Composing to an S/MIME enabled receiver from a sender that has a valid certificate/ private key

Figure 6.2. Composing a message having full valid S/MIME configuration



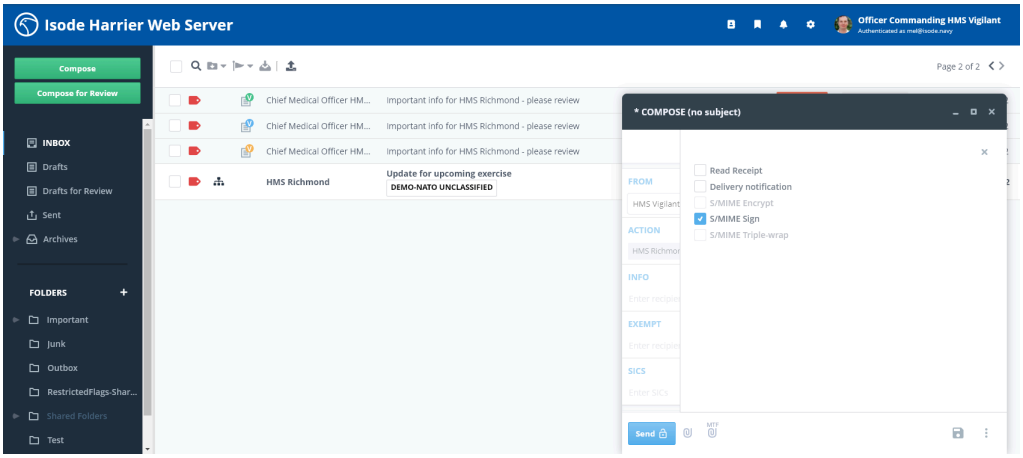
- The user will be presented with the compose window as usual
- The user will fill out the message form as intended
- The user will open ‘More options’ menu and see the three S/MIME options (triple-wrap selected by default, sign and encrypt selected and disabled)
- The user can also see if the message will be encrypted or triple-wrapped when looking at the 'Send' button. Next to the text of the button a lock icon will appear when S/

MIME is configured. The locked lock icon will appear when sending encrypted message and the unlocked lock icon will appear when sending just signed or non-S/MIME messages. When hovering over the button, the user will be presented with a text stating if the message will be encrypted or not.

- The user can either send the message as it is or change the S/MIME selected checkboxes by deselecting triple-wrap. This will enable all three checkboxes and the user can select what they would like to use.

2. Composing to an S/MIME disabled receiver (can't encrypt) from a sender that has a valid certificate/private key

Figure 6.3. Composing message to a recipient that has an invalid certificate



- The user will be presented with the compose window as usual
- The user will compose the message form as intended, including a recipient that doesn't have or is not allowed to use S/MIME (for example the receiver of the message would not have S/MIME configured, their certificates might have expired or been revoked or the recipient might not be found in the directory)
- The user will open 'More options' menu and observe that instead of having the three checkboxes selected like the previous case, this time only S/MIME sign is checked and the rest is not selected and disabled.
- The user can either send the message like this, which will result in an S/MIME signed message or can deselect the sign and send the message without any S/MIME options.

3. Composing to a group of people or many recipients and one of them cannot receive encrypted messages

- The expected behaviour would be the same as the case above. However, if there is a recipient in the group or the list of recipients that we are sending to that has S/MIME disabled, not configured or has invalid certificates, the message won't be allowed to be encrypted or triple-wrapped to any of the recipients.

4. Receiving an S/MIME message

- The recipient will receive the message as usual
- The recipient will open the message and operate on the message
- The recipient will be able to see the S/MIME Message Status as one of the headers of the message and observe if there are any errors or warnings due to failures in the procedure or configuration

6.1.4 Using S/MIME

The following sub-sections show examples of S/MIME in use.

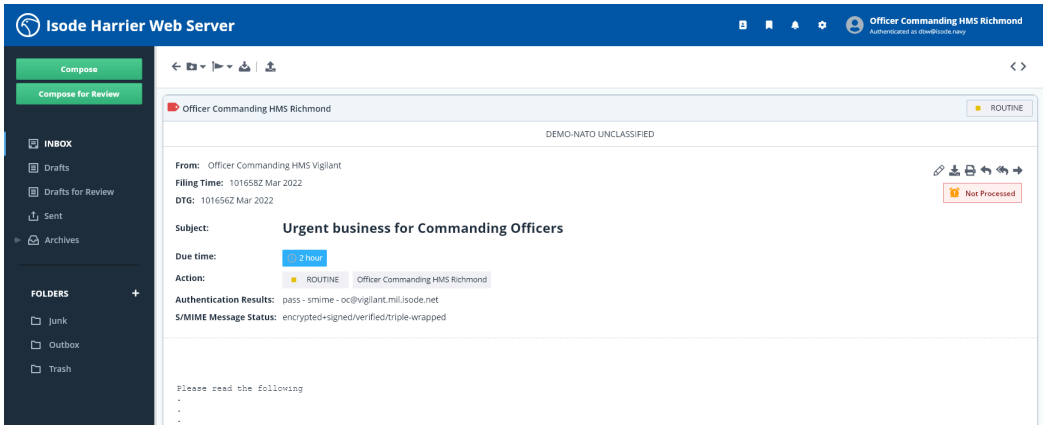
6.1.4.1 Sending an S/MIME message

S/MIME options will be present in the compose box and will appear in the ‘More options’ menu as checkboxes. Here you can modify and control how you want to send the message in terms of signing, encryption and triple-wrapping. Base on your configuration and the user you are logged in as/sending as, selected and/or disabled options may vary. If you add a recipient to the message with different S/MIME setup, some of the checkboxes may get unselected and disabled. If both you and the recipient have optimal S/MIME configuration (S/MIME enabled and valid certificates), all of the options should be selected and signing and encryption should be disabled until you deselect the triple-wrap option. After composing the message, it will be sent and the appropriate S/MIME operations will be executed on the message, depending on what was selected.

6.1.4.2 Receiving an S/MIME message

When the message is received the user can open it and look at the message. The S/MIME message status will show the S/MIME that was used and if it was decrypted/verified on the receiver’s side. If there are any issues, they will be displayed in the S/MIME Warning or Error headers in the message pane.

Figure 6.4. Message pane view of S/MIME status

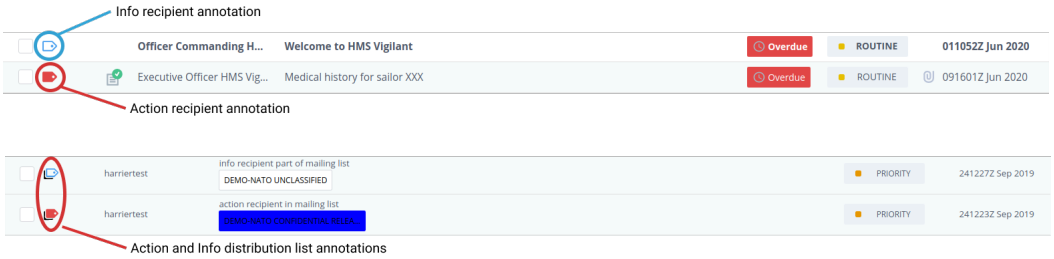


6.2 Recipient Type annotation

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 6.5. Scan-list view of recipient type bar



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 6.6. Message pane view of recipient type bar