



EAGLE GLINT

OPERATOR Manual



Reference : EAGLE / MAN-EAGLE-OPERATOR
Version : 1.0
Date : 19/03/09
State : Draft

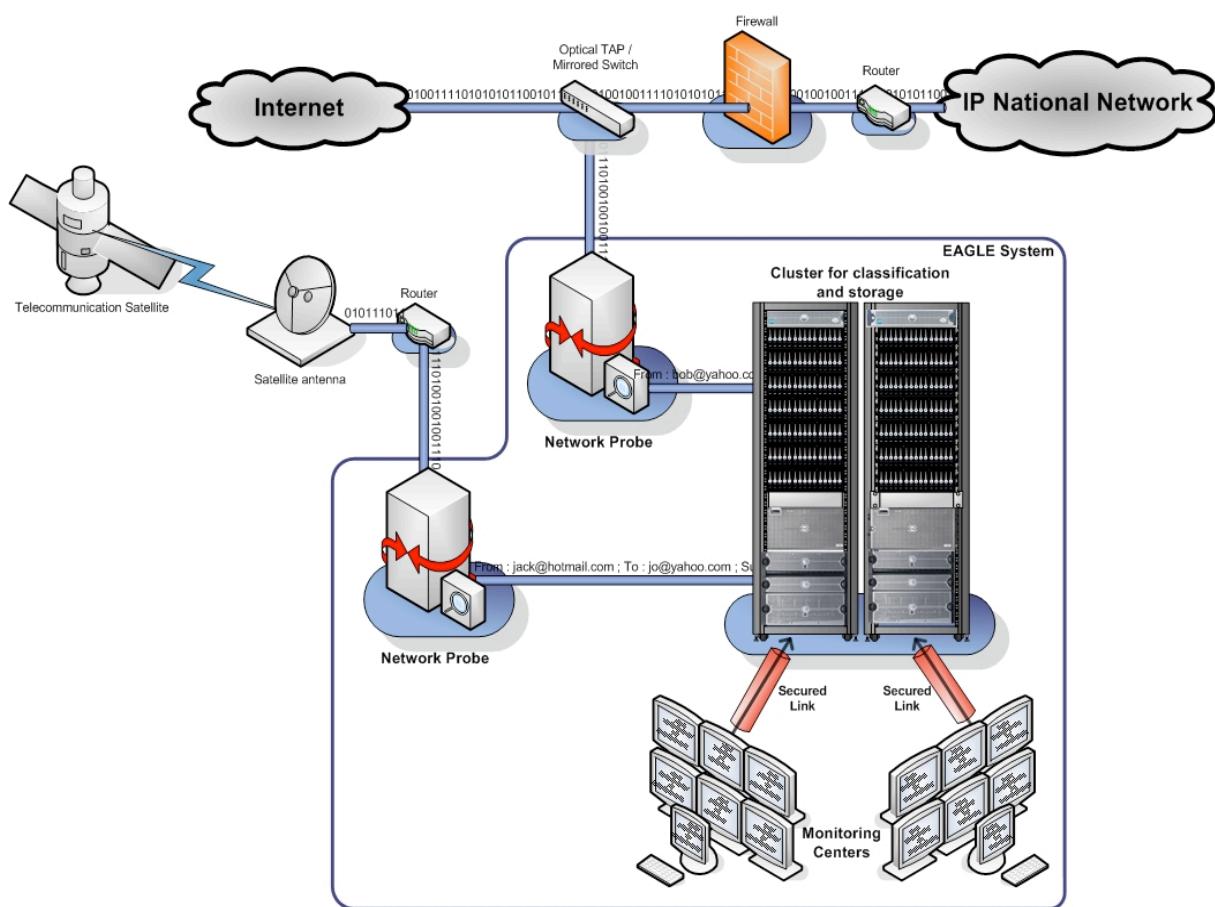
1. INTRODUCTION	4
1.1. Concept.....	4
1.2. Features	5
1.3. Components and Terminology of the MMI.....	7
2. MENUS DESCRIPTION	9
2.1. Home (WEL)	10
2.2. New Interception Manager (NIM)	11
2.2.1. Search Directives Tab	12
2.2.2. Pre-classified interception Tabs	13
2.2.3. Search Function	15
2.2.4. Filter Function.....	18
2.2.5. Graph+ (only for OC).....	20
2.2.6. Suspects (only for OC)	23
2.2.7. No-Interest popup	25
2.2.8. Warnings popup	27
2.3. Personal Information Management (PIM).....	28
3. INTERCEPTIONS ANALYSIS.....	30
3.1. Methodology	30
3.2. Components and Terminology of an Interception.....	31
3.2.1. Technical Data	33
3.2.2. Technical Specific Data.....	35
3.2.3. Extra Data.....	35
3.2.4. Relevance note	37
3.2.5. Transcription	39
3.3. Categories of Interception	41

3.3.1.	Mail	41
3.3.2.	VoIP	42
3.3.3.	Chat	42
3.3.4.	Http	43
3.3.5.	Search Engine.....	43
3.3.6.	Transfer	43
4.	FREQUENTLY ASKED QUESTIONS (FAQ)	45
4.1.	Firefox Messages	45
4.1.1.	Secure Connection Failed.....	45
4.1.2.	Offline Mode	48
4.2.	EAGLE Messages.....	49
4.2.1.	Interception locked by someone else.....	49
4.2.2.	At least 2 suspects are needed, sorry	51
4.2.3.	Too many nodes.....	52
4.2.4.	Cannot retrieve mail	53
4.2.5.	Cannot change password	54
4.3.	Cases Study	55
4.3.1.	Junk e-mail	55
4.3.2.	e-Newsletters, Alerts	57
4.3.3.	Notifications	58
4.3.4.	Placeholder in a message	61
5.	GLOSSARY.....	62

1. INTRODUCTION

1.1. CONCEPT

EAGLE core technology by AMESYS is designed to help Law Enforcement Agencies and Intelligence organization to reduce crime levels, to protect from terrorism threats and to identify new incoming security danger.



EAGLE Interception System can be decomposed in distinct parts:

- The Probe capturing the traffic
- The Data Centre for classification and storage
- The Monitoring Centres

1.2. FEATURES

EAGLE system will retrieve the complete protocol information from the Call Data Record (CDR) and all the attached documents for the following network protocols:

➤ ***Mail***

- SMTP
- POP3
- IMAP

➤ ***Webmails***

- Yahoo! Mail Classic and Yahoo! Mail v2
- Hotmail v1 and v2
- Gmail

➤ ***VoIP***

- SIP / RTP audio conversation
- MGCP audio conversation
- H.323 audio conversation

➤ ***Chat***

- MSN Chat
- Yahoo! Chat
- AOL Chat
- Paltalk

➤ ***Http***

➤ ***Search Engines***

- Google
- MSN Search

EAGLE GLINT - OPERATOR MANUAL

- Yahoo!

➤ ***Transfers***

- FTP
- Telnet

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

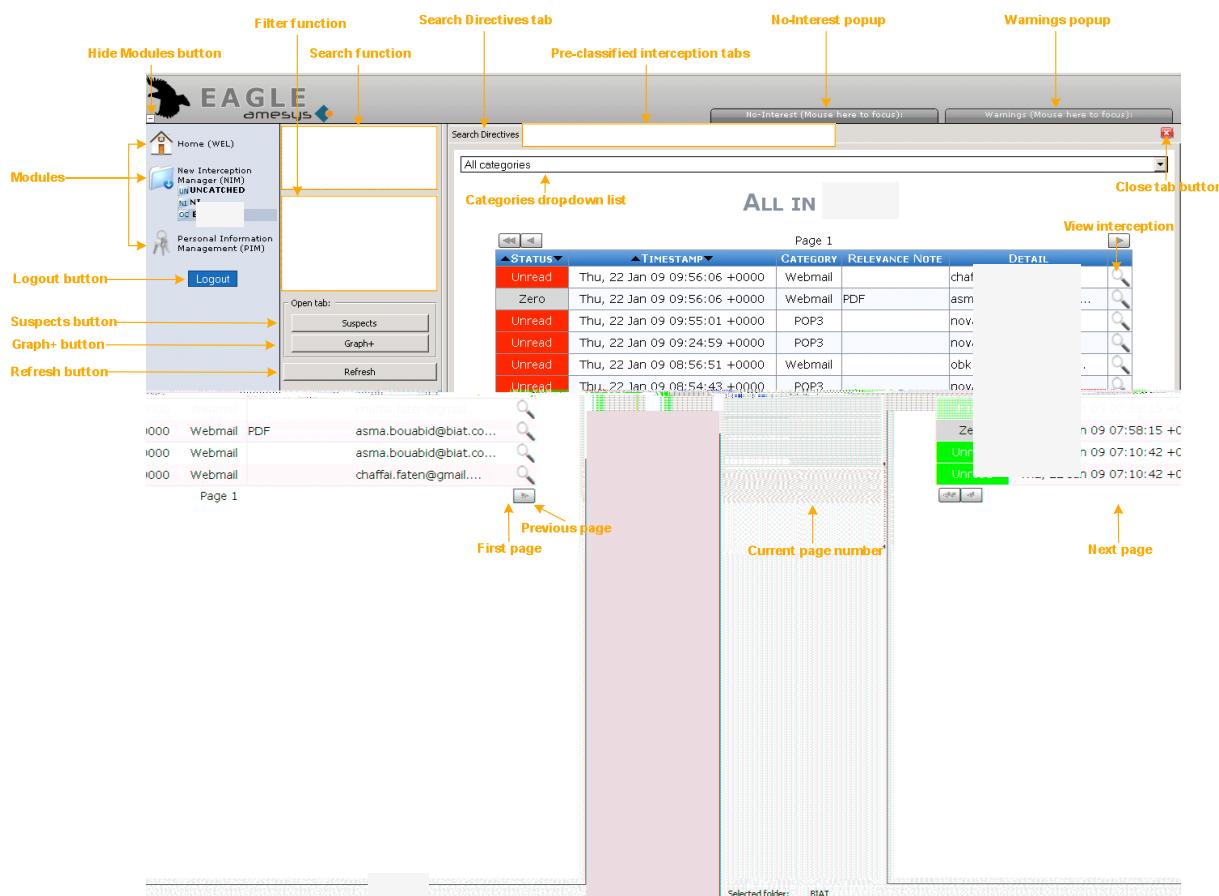
Page 6/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

1.3. COMPONENTS AND TERMINOLOGY OF THE MMI

The EAGLE's Man-Machine Interface (MMI) is made of a logo, a toolbar including three modules and a workspace changing according to the selected module. The diagram below illustrates the components and the terminology used by the MMI:



In addition, various Status message can be displayed. Their colour follows a convention:

- *Green*: requested action is successful

- *Yellow*: you missed an action

EAGLE GLINT - OPERATOR MANUAL

At least 2 suspects are needed, sorry.

- *Red:* unsuccessful action or specific attention is required

Cannot change password

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

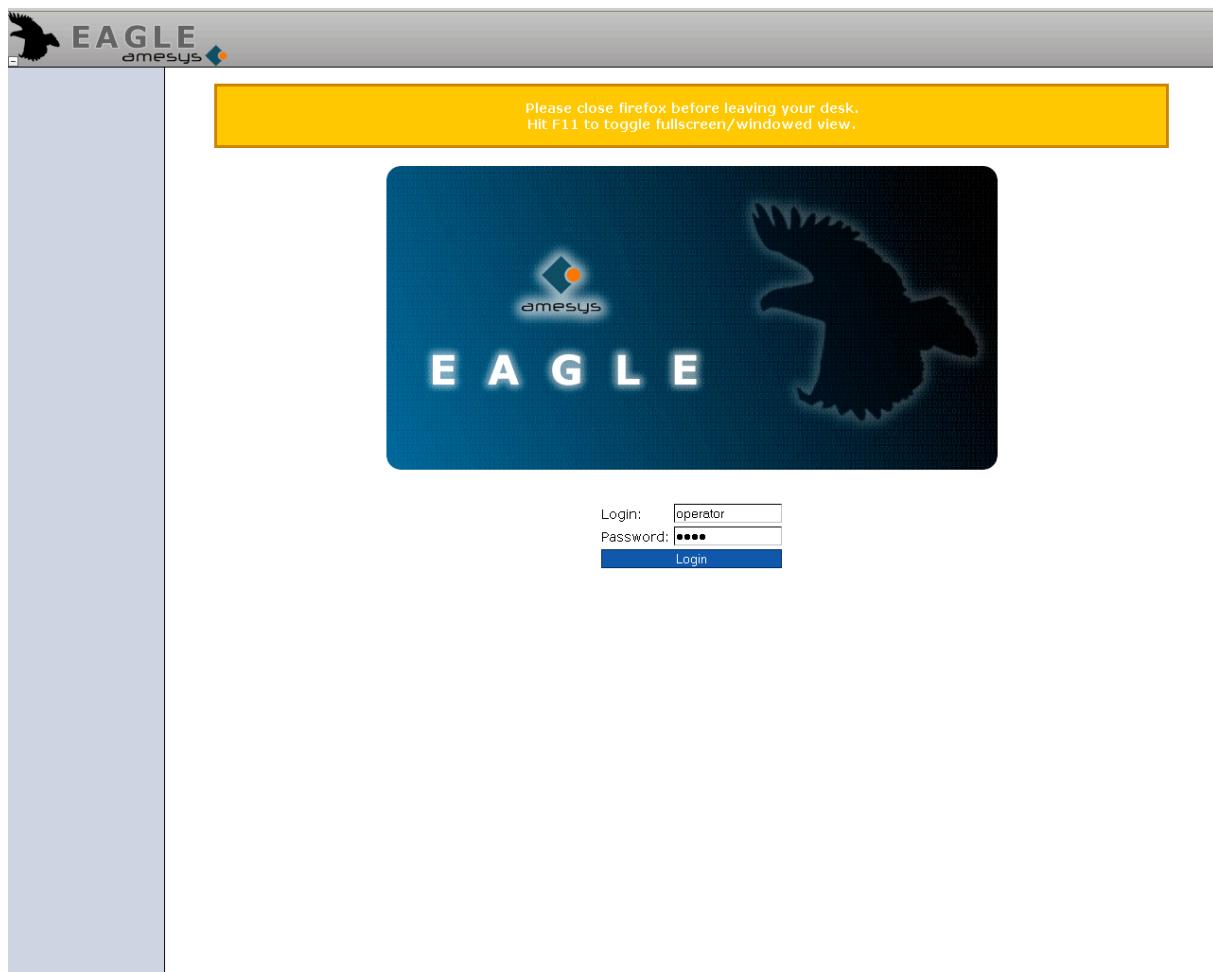
Page 8/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

2. MENUS DESCRIPTION

When you switch-on your computer or launches Mozilla Firefox by clicking on its icon, the window shown below appears:



Enter your login and password, and click the "Login" button to access to the EAGLE's MMI.

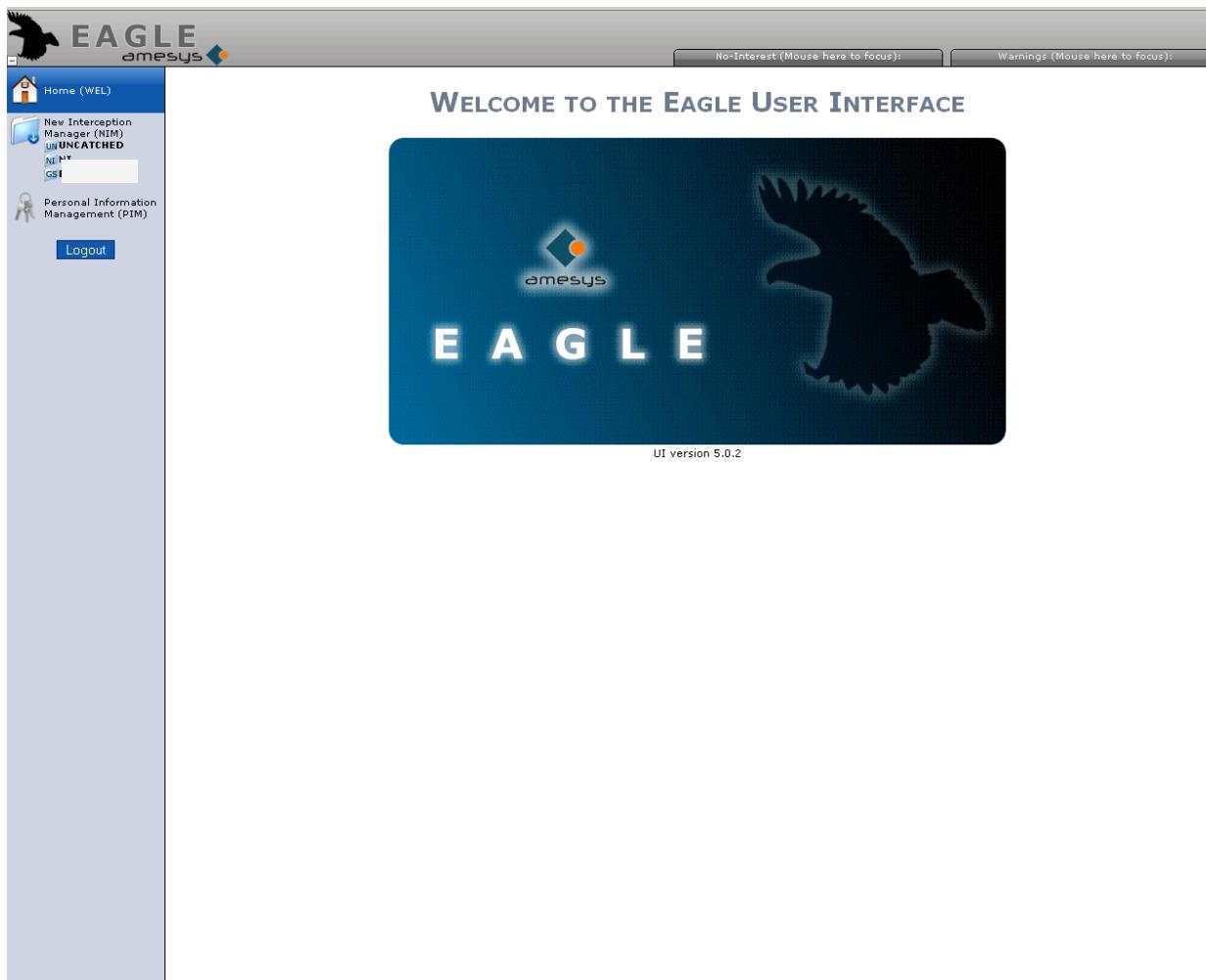
i *To display more content on the screen, EAGLE's MMI use Full Screen mode. Full Screen mode condenses the Firefox's Toolbars into one small toolbar. To disable Full Screen mode, simply press F11 as indicated on the yellow information message.*

EAGLE GLINT - OPERATOR MANUAL



2.1. HOME (WEL)

The “Home (WEL)” module displays the logo of the EAGLE system and the current version of the MMI.



Click on the “Logout” button to close your access to the MMI and then close Firefox and shutdown your computer.



2.2. NEW INTERCEPTION MANAGER (NIM)

The “New Interception Manager (NIM)” module contains the different Process Folders (OC, GS, NI or Uncatched) allocated to you by your Superuser.

TIMESTAMP	NOTE
06/10/08 11:07:10	please identify every employee from this bank



Once you have selected a Process Folder, you can hide the modules by clicking on the button, to enlarge your workspace.

2.2.1. Search Directives Tab

The “Search Directives” tab list chronologically the orders coming from the Superuser for each Process Folder. They include a “Note” and the “Timestamp” (date and time) of its emission.

TIMESTAMP	NOTE
06/10/08 11:07:10	

 Check regularly the “Search Directives” to be up-to-date of the Superuser’s orders.

2.2.2. Pre-classified interception Tabs

The pre-classified interception tabs, "All", "All\Http" (all interceptions except Http), "Mail", "VoIP", "Chat", "Search Engine", "Http" and "Transfer" list the interceptions by category.

STATUS	TIMESTAMP	CATEGORY	RELEVANCE NOTE	DETAIL
Zero	Mon, 10 Nov 08 11:53:53 +0000	Webmail	no interest	elys
Poor	Mon, 10 Nov 08 11:04:34 +0000	Webmail		moi
Zero	Mon, 10 Nov 08 10:18:29 +0000	Webmail	empty	bac
Zero	Mon, 10 Nov 08 10:17:18 +0000	Webmail	empty	bac
Zero	Mon, 10 Nov 08 09:10:01 +0000	Webmail	empty	
Zero	Mon, 10 Nov 08 09:07:49 +0000	Webmail	empty	ska
Zero	Mon, 10 Nov 08 08:07:07 +0000	Webmail	empty	
Zero	Sun, 09 Nov 08 21:10:03 +0000	Webmail	empty	moi
Zero	Sun, 09 Nov 08 20:51:36 +0000	Webmail	empty	moi
Zero	Sun, 09 Nov 08 07:40:31 +0000	Webmail	empty	ghr
Poor	Sun, 09 Nov 08 07:03:32 +0000	POP3	empty	trin

Some of the tabs have a drop-down list to refine the selection as described in the table below:

All	All\Http	Mail	VoIP	Transfer
All categories Webmail POP3 SMTP IMAP VoIP/SIG VoIP/RTP VoIP Chat Http FTP Telnet Search Engine	All categories Webmail POP3 SMTP IMAP VoIP/SIG VoIP/RTP VoIP Chat FTP Telnet Search Engine	All categories IMAP POP3 SMTP Webmail	All categories VoIP/SIG VoIP/RTP VoIP	All categories Telnet FTP

EAGLE GLINT - OPERATOR MANUAL



The pre-classified interception tabs cannot be closed!!!

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 14/66

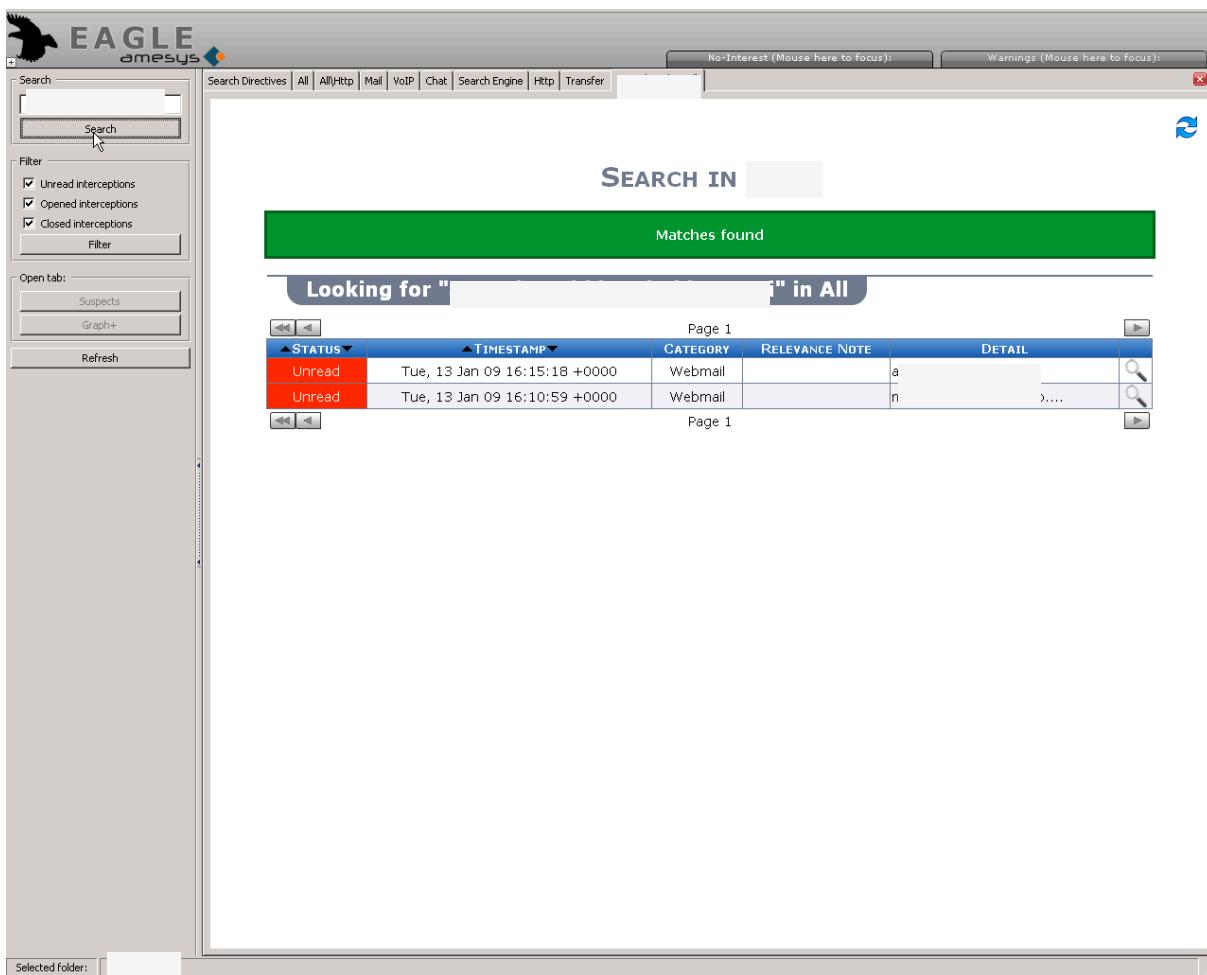


This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

2.2.3. Search Function

The “Search” function is a text search engine that can help you to minimize the time required to find valuable information, and the amount of interceptions which must be consulted.

Once a search is done, automatically, a new tab will be created as shown below, allowing you to work on it or to refine your search. When finish, click on the Close tab button  to close a Search result tab.



The screenshot shows the EAGLE Glint software interface. On the left, there's a sidebar with a search bar, filter options (Unread, Opened, Closed), and tabs for Suspects and Graph+. A 'Refresh' button is also present. The main area is titled 'SEARCH IN' and displays a table of search results. The table has columns for STATUS, TIMESTAMP, CATEGORY, RELEVANCE NOTE, and DETAIL. Two rows are visible, both labeled 'Unread' and timestamped 'Tue, 13 Jan 09 16:15:18 +0000'. The 'CATEGORY' column shows 'Webmail' and 'RELEVANCE NOTE' shows 'a' and 'n'. The 'DETAIL' column contains a truncated note '....'. At the bottom of the table, it says 'Page 1'.



The “Search” function uses a list of common words that are not indexed such as for example “of”, “the”, “is” and so on.

EAGLE GLINT - OPERATOR MANUAL

The Search Query identify the desired concept that one or more email, attachment or chat may contain and is expressed as a set of words and operators such as:

➤ **AND**

term1 AND term2

Use the AND operator to search for interceptions that contain at least one occurrence of each of the query terms.

For example, to obtain all the interceptions that contain the terms blue and black and red, issue the following query:

blue AND black AND red

➤ **OR**

term1 OR term2

Use the OR operator to search for interceptions that contain at least one occurrence of any of the query terms.

For example, to obtain all the interceptions that contain the term blue or the term black, issue the following query:

blue OR black

➤ **NOT**

term1 NOT term2

Use the NOT operator to search for interceptions that contain one query term and not another.

For example, to obtain the interceptions that contain the term blue but not the term black, issue the following query:

blue NOT black

➤ **EQUIV**

term1=ter

m2

Use the EQUIV operator to specify an acceptable substitution for a word in a query.

The following example returns all interceptions that contain either the phrase “blue is a colour” or “black is a colour”:

blue=black is a colour

2.2.4. Filter Function

An interception can have various statuses:

- “Unread” until any operator open it for the first time
- “Opened” when it has been opened but does not have “Relevance note”
- “Closed” when any operator attributes to it “Relevance note” (Zero, Poor, Good or Very good).

With the “Filter” function, you can filter interceptions according to their current status. For example, below are displayed only “Opened” and “Closed” interceptions.

The screenshot shows the EAGLE amesys software interface. On the left, there is a sidebar with a search bar, a 'Filter' section containing checkboxes for 'Unread interceptions', 'Opened interceptions' (which is checked), and 'Closed interceptions' (which is also checked), and a 'Filter' button. Below this are tabs for 'Suspects' and 'Graph+'. A 'Refresh' button is also present. The main area is titled 'ALL IN' and displays a table of search results. The table has columns for STATUS, TIMESTAMP, CATEGORY, RELEVANCE NOTE, and DETAIL. The results show several entries: Opened at Thu, 22 Jan 09 15:08:19 +0000, Opened at Thu, 22 Jan 09 14:27:18 +0000, Opened at Thu, 22 Jan 09 13:45:42 +0000, Opened at Thu, 22 Jan 09 10:34:47 +0000, Opened at Thu, 22 Jan 09 10:11:55 +0000, Zeroed at Thu, 22 Jan 09 09:56:06 +0000, and Zeroed at Thu, 22 Jan 09 07:58:15 +0000. The 'RELEVANCE NOTE' column for the zeroed entries contains 'PDF'. The 'DETAIL' column for the zeroed entries contains 'fr'. The table is labeled 'Page 1' at the bottom right. At the very bottom of the interface, there is a footer bar with the text 'Selected folder: []'.

EAGLE GLINT - OPERATOR MANUAL

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 19/66

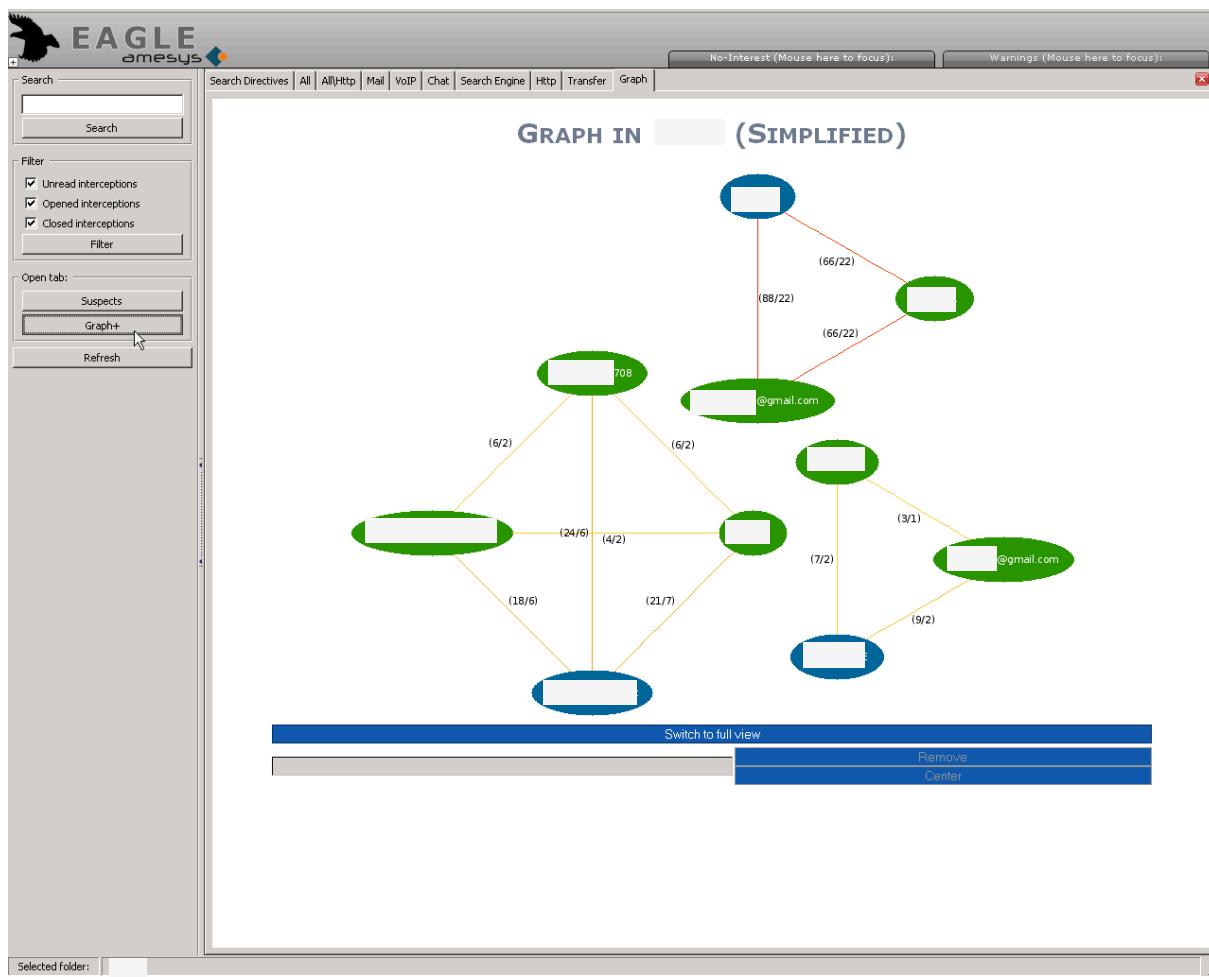


This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

2.2.5. Graph+ (only for OC)

In the case of an “Open Case” (OC) Process Folder, EAGLE system creates a “Graph+” chart automatically, using information from every interception. The “Graph+” is a graphical tool designed to display and to analyze the intelligence relating to an investigation in a visual form. It supports you in your analysis, helping to navigate through large networks of data and discover underlying interconnections quickly.

Click the “Graph+” button. A new tab called “Graph” appears:



When finish, click on the Close tab button to close a “Graph” tab.

EAGLE GLINT - OPERATOR MANUAL

From the Graph+, you can:

- Center the chart on a particular ID or suspect by clicking on it and then on the "Center" button.
- Remove an uninteresting node by clicking on it and then on the "Remove" button. The "Switch to full view" button allows you to display every node, even the previously removed ones.

The colour of the nodes follows a convention:

Colour	Description	Example
Green	IDs from automatic extract	
Blue	Suspects	
Grey	Removed IDs	

By clicking on a Suspect node, you can access to the Suspect information's:

EAGLE GLINT - OPERATOR MANUAL

The screenshot shows the EAGLE Glint software interface. At the top, there's a navigation bar with links like 'Search Directives', 'All', 'AllHttp', 'Mail', 'VoIP', 'Chat', 'Search Engine', 'Http', 'Transfer', and 'Graph'. Below the navigation bar, the word 'SUSPECT' is displayed in large letters. Underneath 'SUSPECT', there are several sections: 'General informations', 'ID+', 'KEYRING', 'NAME_ALIAS', 'SURNAME', and 'ID-'. The 'General informations' section contains fields for Nickname, Real firstname, Real name, Primary Language, and Priority. The 'ID+' section contains two 'MAIL' entries with 'EMAIL_ADDR' fields. The 'KEYRING', 'NAME_ALIAS', and 'SURNAME' sections are currently empty. The 'ID-' section is also empty.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 22/66

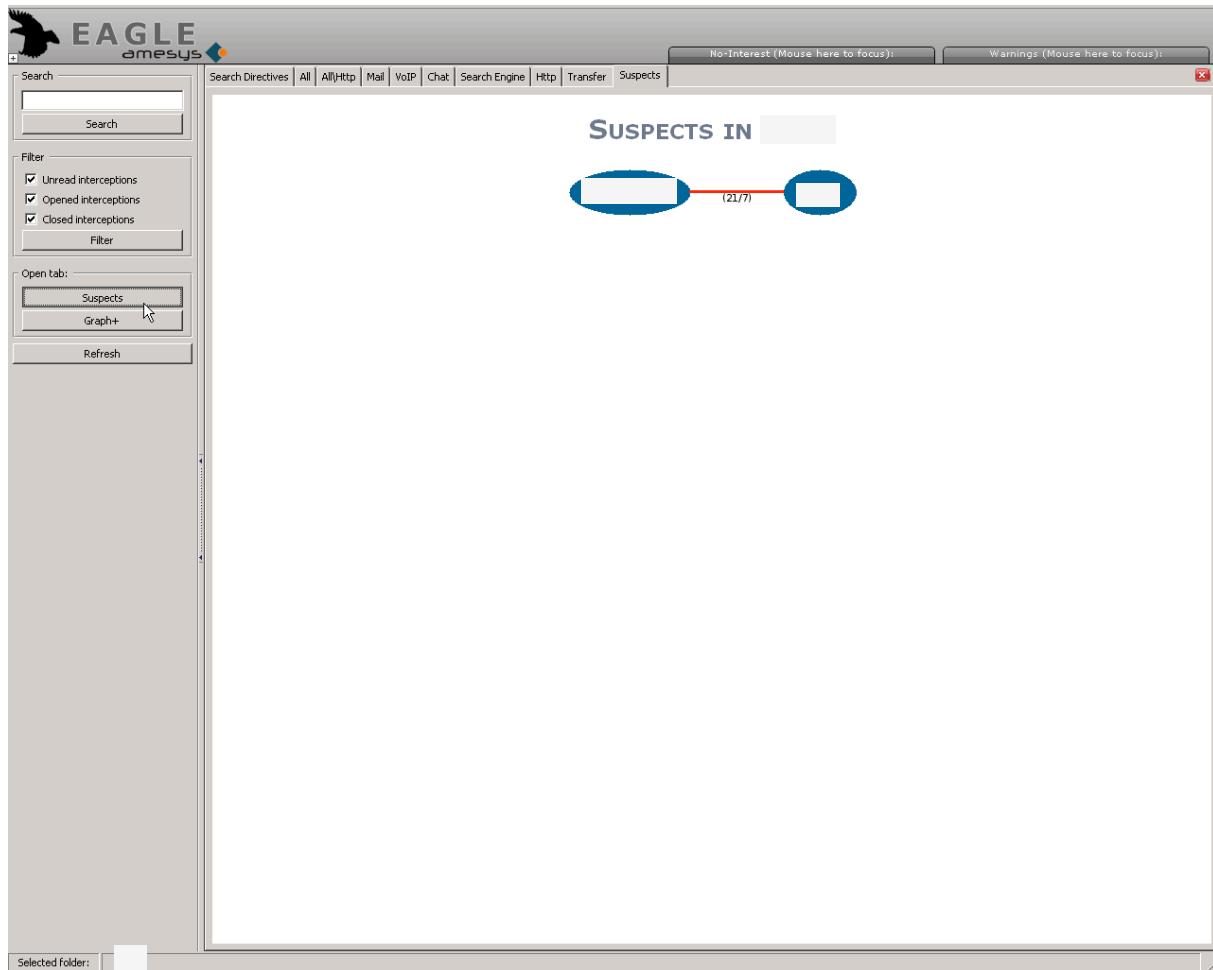
This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.



2.2.6. Suspects (only for OC)

In the case of an “Open Case” (OC) Process Folder, you can directly visualize only connections between suspects.

Click on the “Suspects” button. A new tab called “Suspects” appears as shown on the picture below:



When finish, click on the Close tab button to close a “Suspects” tab.

EAGLE GLINT - OPERATOR MANUAL

As for the Graph+, by clicking on the link between suspects, you can directly visualize their communications:

The screenshot shows the EAGLE GLINT software interface. On the left, there is a sidebar with a search bar, filter options (Unread, Opened, Closed interceptions), and tabs for Suspects and Graph+. The main area is titled "Link between suspect" and displays a table of communication logs. The columns are STATUS, TIMESTAMP, CATEGORY, RELEVANCE NOTE, and DETAIL. All entries are Unread, timestamped on Thu, 22 Jan 09, and categorized as POP3. The DETAIL column shows ".com..." followed by a magnifying glass icon. At the bottom of the table, it says "Page 1".

STATUS	TIMESTAMP	CATEGORY	RELEVANCE NOTE	DETAIL
Unread	Thu, 22 Jan 09 10:50:44 +0000	POP3		:.com...
Unread	Thu, 22 Jan 09 10:50:44 +0000	POP3		:.com...
Unread	Thu, 22 Jan 09 10:50:44 +0000	POP3		:.com...
Unread	Thu, 22 Jan 09 10:40:51 +0000	POP3		:.com...
Unread	Thu, 22 Jan 09 10:40:51 +0000	POP3		:.com...
Unread	Thu, 22 Jan 09 10:40:51 +0000	POP3		:.com...
Unread	Thu, 22 Jan 09 10:40:51 +0000	POP3		:.com...

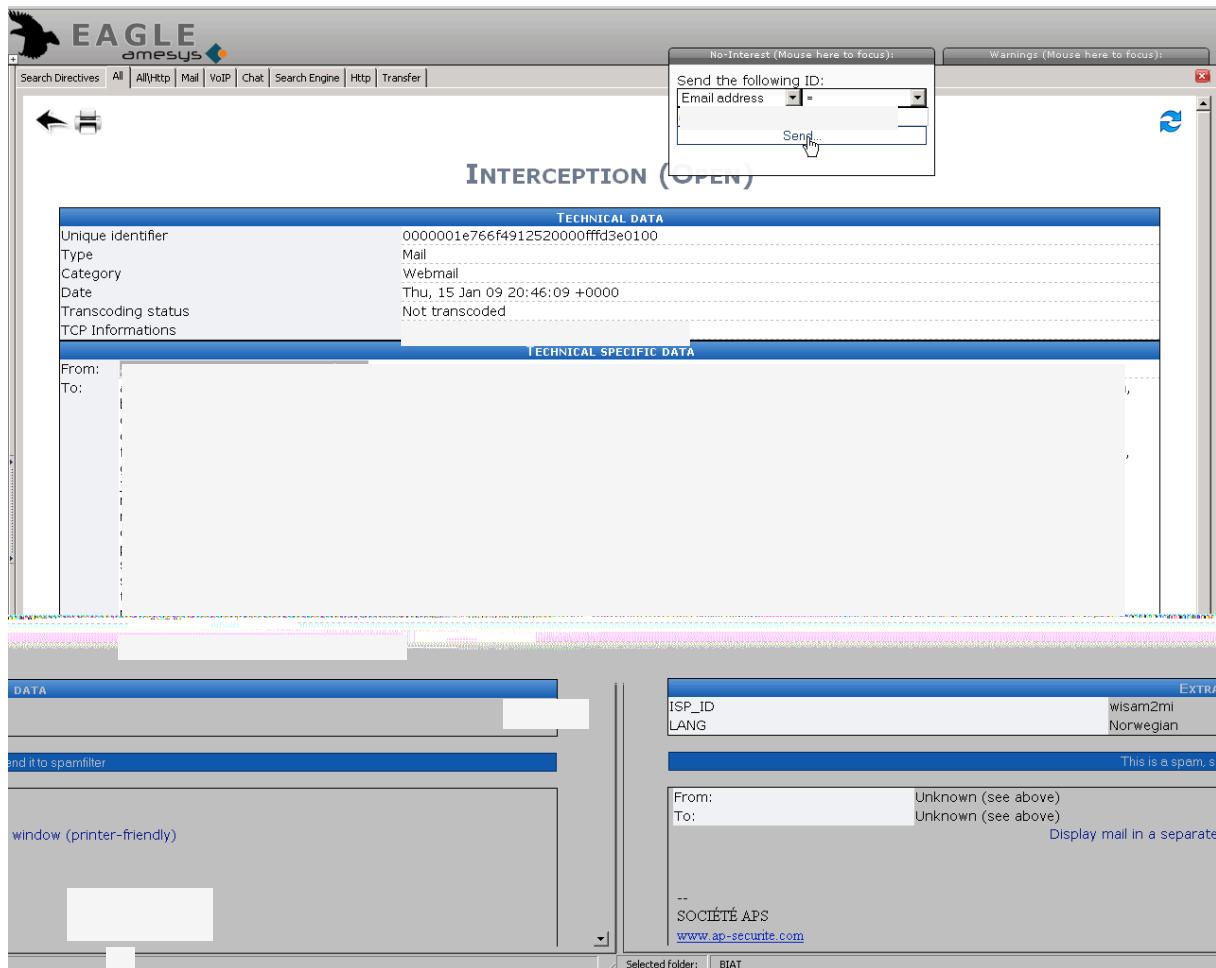
When finish, click on the Close tab button to close a "Link" tab.

2.2.7. No-Interest popup

At any time, you can report uninteresting IDs to your Superuser through the “No-Interest” popup.

Move the mouse over the “No-Interest (*Mouse here to focus*)” title at the top of the workspace to display the popup window.

From the drop-down lists, select respectively the type of ID (email address, Phone number or ISP account), the operator (=, BEGINS_WITH or ENDS_WITH) and type the appropriate ID in the text box.



Click the “Send ...” button to send your suggestion to the Superuser. A confirmation message is displayed:

EAGLE GLINT - OPERATOR MANUAL

ID has been sent

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 26/66

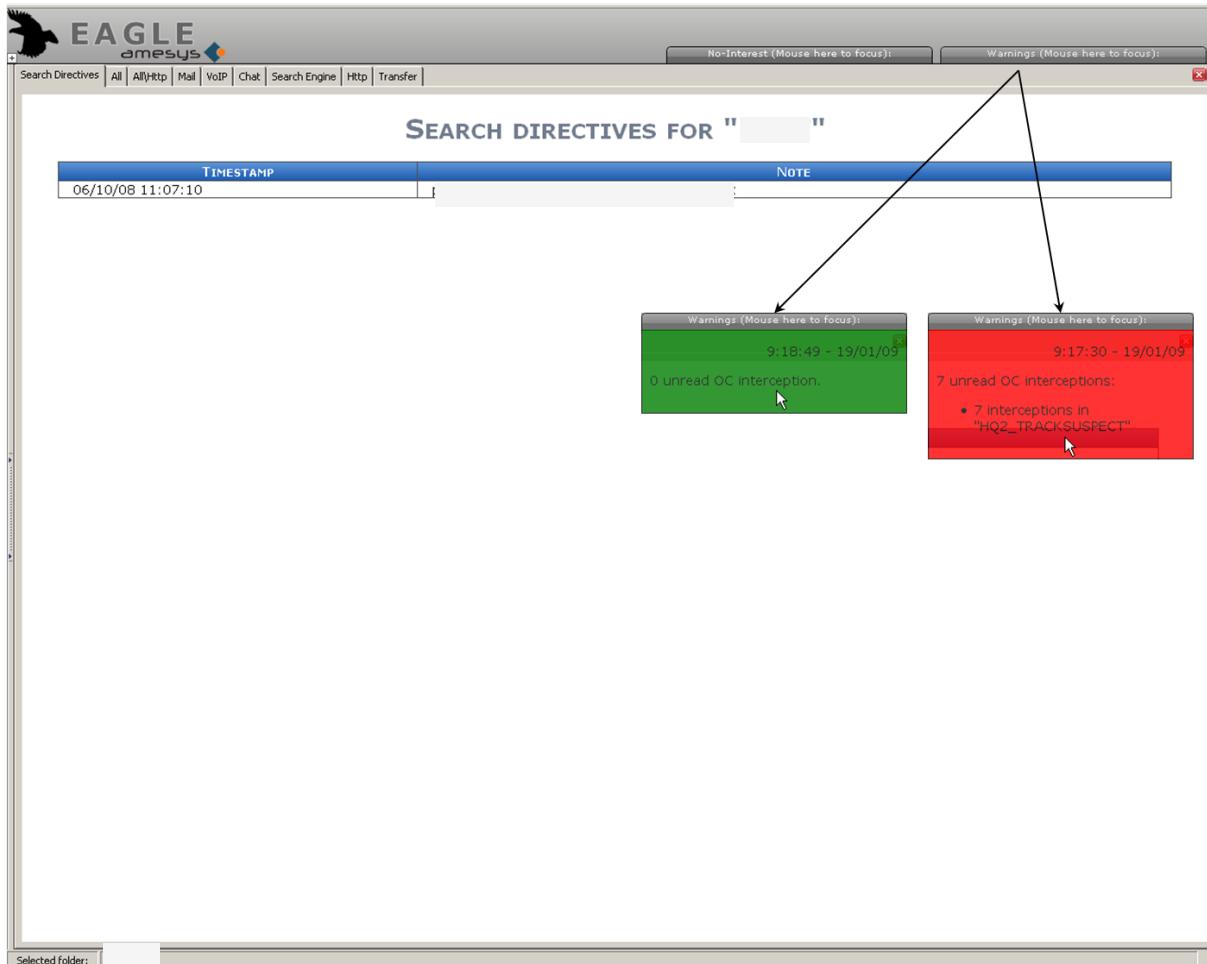


This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

amesys

2.2.8. Warnings popup

The “*Warnings*” popup window is an information area alerting you when at least one new interception is available in any of your OC Process Folders.



In addition, a window is regularly displayed:





2.3. PERSONAL INFORMATION MANAGEMENT (PIM)

The “*Personal Information Management (PIM)*” module permits to the logged Operator to change his password to access to the EAGLE’s MMI.

In the two text boxes, enter the password you would like to start using. Entering the password twice helps to make sure that you typed your new password correctly. Click the “*Change password*” button to confirm your changes.

The screenshot shows the EAGLE MMI interface. At the top, there's a header with the EAGLE logo and navigation buttons for 'No-Interest' and 'Warnings'. The main content area is titled 'PERSONAL INFORMATION MANAGEMENT (PIM)'. Below the title is a button labeled 'Change my password'. On the left, there's a sidebar with icons for 'Home (WEL)', 'New Interception Manager (NIM)' (which has 'UNCATCHED' written over it), and 'Personal Information Management (PIM)'. The 'Personal Information Management (PIM)' icon is highlighted with a blue border. At the bottom of the sidebar are 'Logout' and 'Logout' buttons.

EAGLE GLINT - OPERATOR MANUAL

Now that your logon password has been changed, you must use your new password to log on to EAGLE's MMI from this point forward.



Changing your logon password regularly is a good habit to help keep your access secure.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

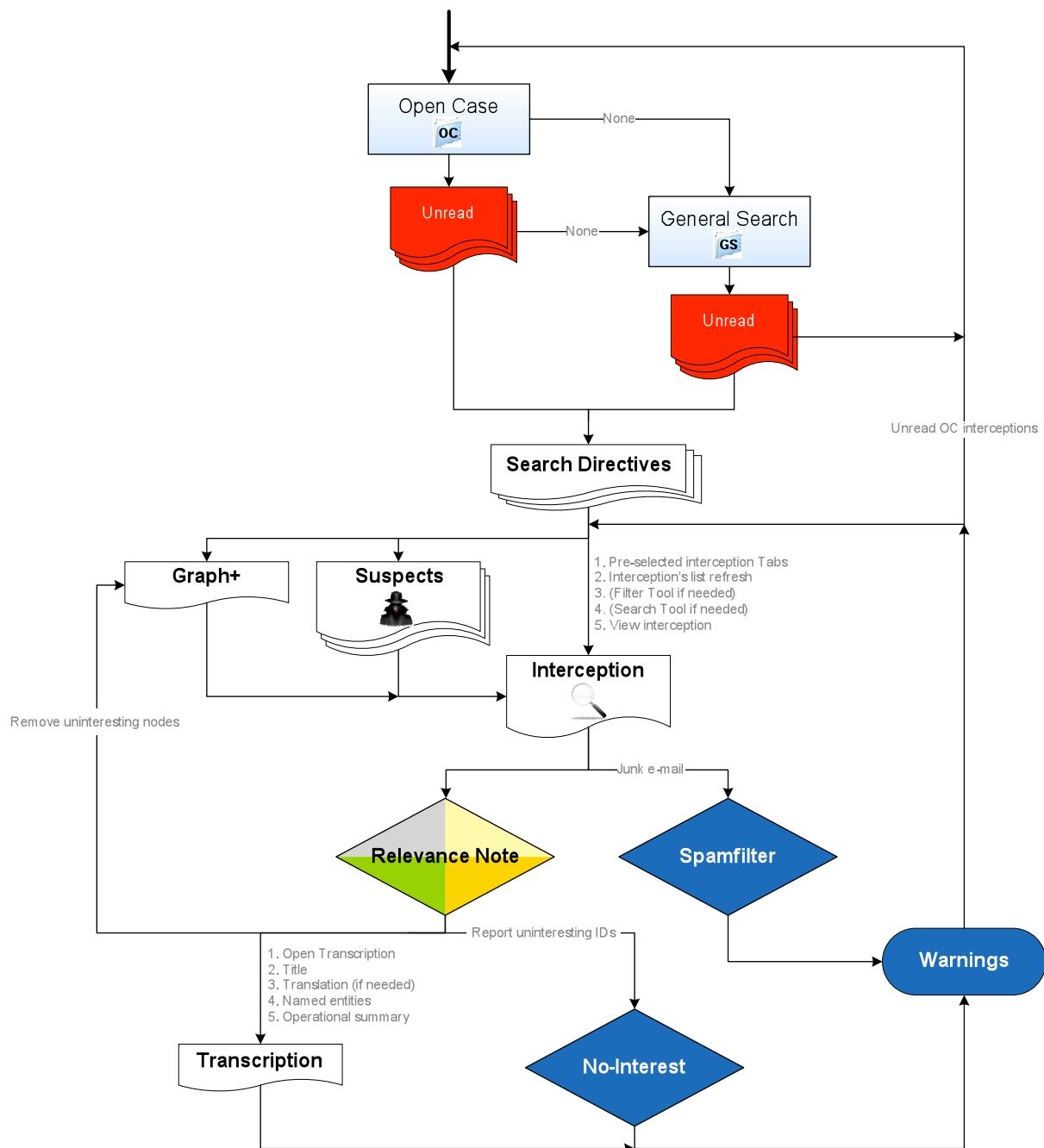
Page 29/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

3. INTERCEPTIONS ANALYSIS

3.1. METHODOLOGY



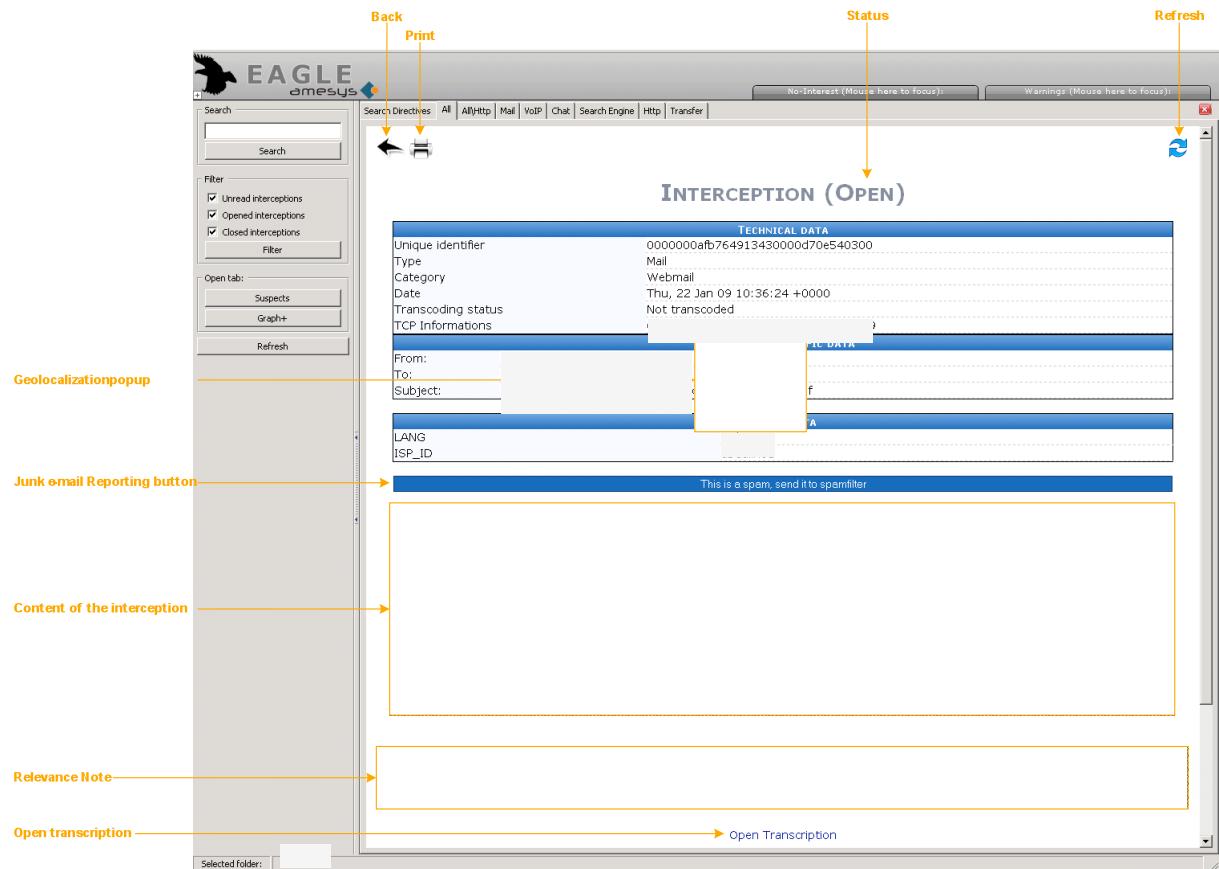
3.2. COMPONENTS AND TERMINOLOGY OF AN INTERCEPTION

The interception view is made of:

- A toolbar including three buttons (Back, Print and Refresh)
- The “*TECHNICAL DATA*” table
- The “*TECHNICAL SPECIFIC DATA*” table (changing according to the category of the interception)
- The “*EXTRA DATA*” table(optional)
- The “*This is a spam, send it to spamfilter*” button for Junk e-mail Reporting
- The content of the interception (changing according to the category of the interception)
- The “*Relevance Note*” made of a text box and four buttons for ranking.

The diagram below illustrates the components and the terminology used in this view:

EAGLE GLINT - OPERATOR MANUAL



Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 32/66

This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.



3.2.1. Technical Data

Every interception will have a “*TECHNICAL DATA*” table as the one shown below:

TECHNICAL DATA	
Unique identifier	0000000afb7649131000001703600300
Type	Mail
Category	POP3
Date	Thu, 22 Jan 09 10:50:44 +0000
Transcoding status	Not transcoded
TCP Informations	

➤ ***Unique identifier***

a unique hexadecimal number which is assigned by EAGLE to identify an interception

➤ ***Type and Category***

Classification of the interception

➤ ***Date***

Accurate date and time of the interception expressed in UTC (Coordinated Universal Time) time standard.

➤ ***Transcoding status***

Only VoIP communications need Transcoding.

➤ ***TCP Informations***

xx.xxx.250.1 00	:	110	-	xx.xxx.121.1 27	:	1142
From				To		
IP address		Port		IP address		Port

In addition, by moving the mouse over every IP address, a Geolocalization popup window appears with the accurate coordinates:

TECHNICAL DATA	
Unique identifier	0000000afb7649131000001703600300
Type	Mail
Category	POP3
Date	Thu, 22 Jan 09 10:50:44 +0000
Transcoding status	Not transcoded
TCP Informations	



EAGLE GLINT - OPERATOR MANUAL

TECHNICAL DATA	
Unique identifier	0000002ca1e04820030000cdf0b0000
Type	Mail
Category	POP3
Date	Wed, 17 Dec 08 21:47:24 +0000
Transcoding status	Not transcoded
TCP Informations	



Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 34/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

EAGLE GLINT - OPERATOR MANUAL

3.2.2. Technical Specific Data

Every interception will have a "*TECHNICAL SPECIFIC DATA*" table but the fields can be different:

Technical Specific Data		
Caller	:	
Callee	:	
Call duration	16m16s	
End status	COMPLETED	

For further details, please see the paragraphs dedicated to each category of interceptions.

3.2.3. Extra Data

For every interception, EAGLE system extract automatically some interesting data from the content itself such as email address, telephone number and ISP ID.

The result appears in the “*EXTRA DATA*” table:

The extra data supports you in your analysis, helping to report every interesting IDs for improvement of further interception.

EAGLE GLINT - OPERATOR MANUAL

Moreover, in the case of an Open Case Process Folder, "EXTRA DATA" are used in "Graph+" to discover underlying interconnections quickly.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 36/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

3.2.4. Relevance note

The “Relevance note” tool is located at the end of each interception page and is made of an “Header” text box and four “Ranking” buttons as shown on the picture below:



As Operator, you must associate an individual evaluation to each interception including a concise, clear and complete title and a content ranking based on the “Search Directives” criteria:

-	Zero	Junk content
	Poor	Communication not related to the Search Directives
	Good	Communication related to the Search Directives
	Very Good	Content is top importance
+		

Thus, it makes possible for the Superuser to quickly select the interceptions he is likely to want to see.

Note that each time you attribute a “Relevance note” to an interception, the interception tables of each pre-classified tabs are updated:

▲ STATUS ▼	▲ TIMESTAMP ▼	CATEGORY	RELEVANCE NOTE	DETAIL	...	🔍
Good	Thu, 22 Jan 09 16:50:30 +0000	POP3	Conference		...	🔍
Zero	Thu, 22 Jan 09 15:08:19 +0000	Webmail	Advertising		...	🔍
Zero	Thu, 22 Jan 09 15:08:19 +0000	Webmail	Chat		...	🔍
Zero	Thu, 22 Jan 09 14:27:22 +0000	Webmail	Advertising		...	🔍
Zero	Thu, 22 Jan 09 14:15:06 +0000	Webmail	Empty		...	🔍
Very Good	Thu, 22 Jan 09 10:34:51 +0000	Webmail	Names		...	🔍
Zero	Thu, 22 Jan 09 09:56:06 +0000	Webmail	PDF		...	🔍
Zero	Thu, 22 Jan 09 07:58:15 +0000	Webmail	PDF		...	🔍



Always fill in first the Header then click one of the Ranking buttons because when ranking is chosen, you:

EAGLE GLINT - OPERATOR MANUAL

- *cannot go back to fill the Header*
- *cannot modify your ranking.*

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 38/66

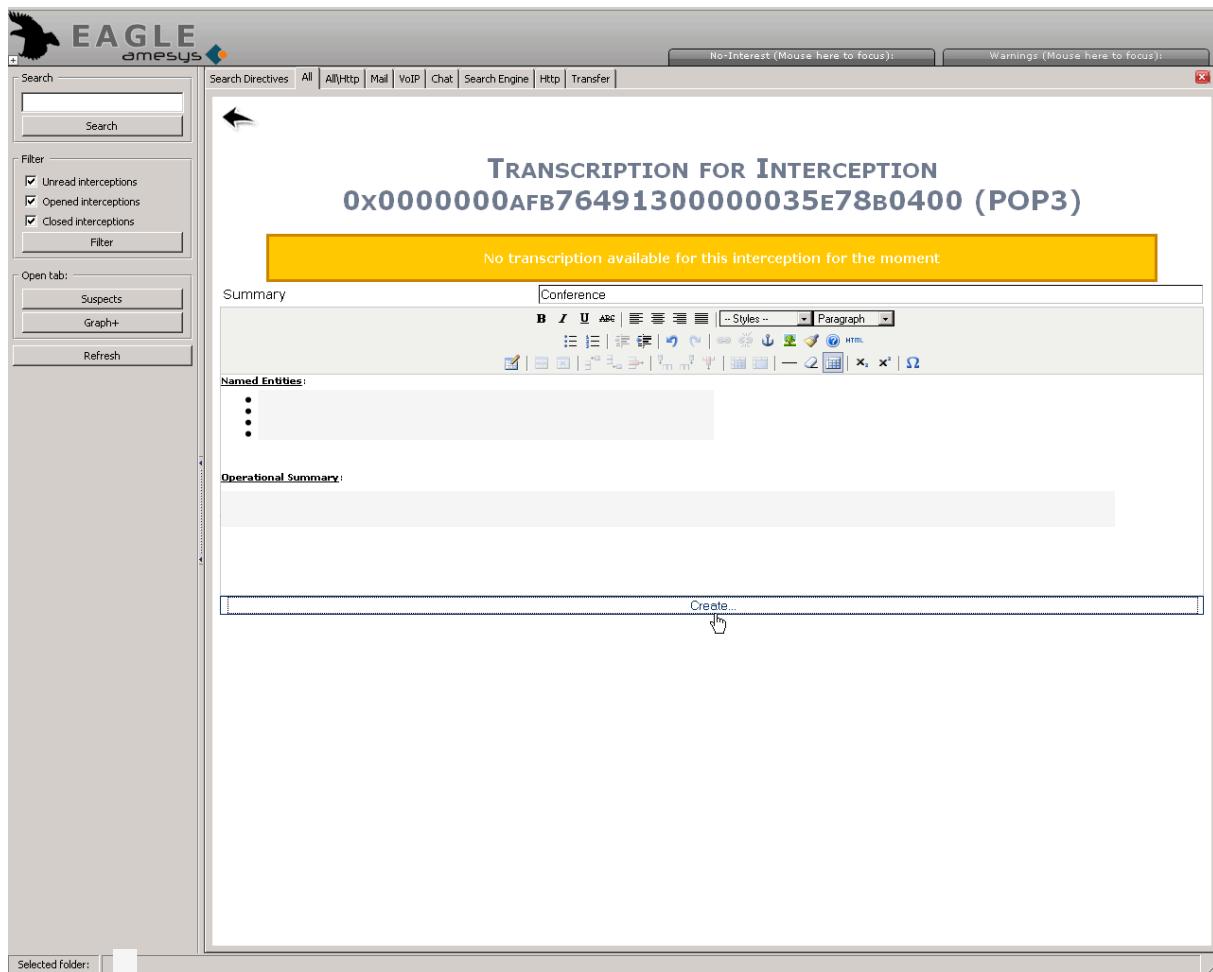


This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

3.2.5. Transcription

You must associate to each interception ranked as "Good" or "Very Good" a transcription.

Click on the "Open Transcription" link at the end of each interception page. A "Transcription" page opens, similar to the one below:



A typical transcription includes:

- A list of "Named Entities" such as names, geographic places ...
- A complete "Translation" of any written text or a complete transcription and translation (if needed) of any voice communication

EAGLE GLINT - OPERATOR MANUAL

- A short summary of content (answers to Who, What, When with no details or parenthesis).

At any time, a transcription can be modified. When finished, click the "Create ..." button.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 40/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

3.3. CATEGORIES OF INTERCEPTION

3.3.1. Mail

Below is a typical “*TECHNICAL SPECIFIC DATA*” table in the case of a Mail interception:

TECHNICAL SPECIFIC DATA	
From:	
To:	
Subject:	New Year Greeting

Attachment(s)

PDF
Adobe .pdf

From: | > To: | Subject: | Date: Thu, 22 Jan 2009 11:42:58 +0100 (CET)
[Display mail in a separate window \(printer-friendly\)](#)

Cher(e)

;

;

;

;

;

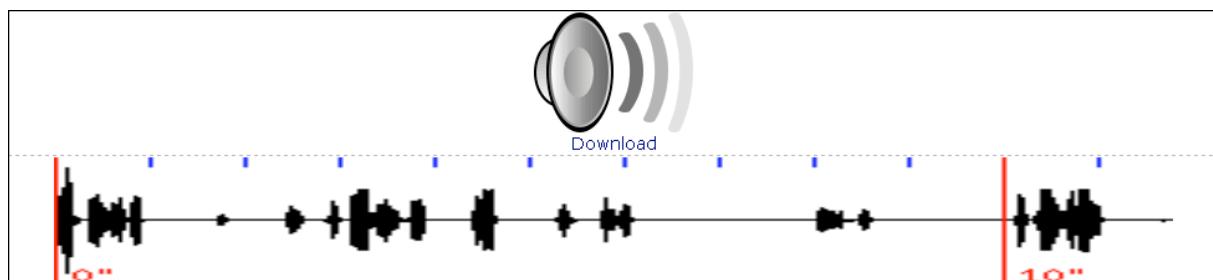
*

EAGLE GLINT - OPERATOR MANUAL

3.3.2. VoIP

Below is a typical “*TECHNICAL SPECIFIC DATA*” table in the case of a VoIP interception:

TECHNICAL SPECIFIC DATA	
Caller	
Callee	
Call duration	16m16s
End status	COMPLETED



3.3.3. Chat

Below is a typical “*TECHNICAL SPECIFIC DATA*” table in the case of a Chat interception:

TECHNICAL SPECIFIC DATA	
Login	
Participants	

CONTACTS	CHAT
	[Sat, 15 Nov 08 22:09:38 +0000] no again [Sat, 15 Nov 08 22:09:40 +0000] ok [Sat, 15 Nov 08 22:09:41 +0000] ill go too [Sat, 15 Nov 08 22:09:55 +0000] ok maybe tomorrow or later [Sat, 15 Nov 08 22:10:03 +0000] if i finished earlier [Sat, 15 Nov 08 22:10:04 +0000] ok [Sat, 15 Nov 08 22:10:12 +0000]

3.3.4. Http

Below is a typical “*TECHNICAL SPECIFIC DATA*” table in the case of a Http interception:

TECHNICAL SPECIFIC DATA	
Request #0	
Server URI	

3.3.5. Search Engine

Below is a typical “*TECHNICAL SPECIFIC DATA*” table in the case of a Search Engine interception:

TECHNICAL SPECIFIC DATA	
Request #0	
Query	

3.3.6. Transfer

Below is a typical “*TECHNICAL SPECIFIC DATA*” table in the case of a Transfer interception:

TECHNICAL SPECIFIC DATA	
Login	
Password	
Filename	/Nero Web/Int_AllFiles.info
Filesize (bytes)	614
Filename	/Nero Web/Nero 7.vinf
Filesize (bytes)	2116
Filename	/Nero Web/Nero 7/Cab/Int_AllFiles.info
Filesize (bytes)	123472
Filename	/Nero Web/Nero 7/Int_AllFiles.info
Filesize (bytes)	2202
Filename	/Nero Web/Nero 7/Redist/Config/Int_AllFiles.info
Filesize (bytes)	79
Filename	/Nero Web/Nero 7/Redist/DirectX/Int_AllFiles.info
Filesize (bytes)	533
Filename	/Nero Web/Nero 7/Redist/Int_AllFiles.info
Filesize (bytes)	396
Filename	/Nero Web/Nero 7/Setup/Int_AllFiles.info
Filesize (bytes)	1764
Filename	/Nero Web/Nero 7/Setup/fminf.fml
Filesize (bytes)	85
Filename	/Nero Web/Patches/Int_AllFiles.info

EAGLE GLINT - OPERATOR MANUAL

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 44/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

4. FREQUENTLY ASKED QUESTIONS (FAQ)

4.1. FIREFOX MESSAGES

4.1.1. Secure Connection Failed

Firefox uses certificates on secure websites (those that start with *https:*) to ensure that your information is being sent to the intended recipient and can't be read by eavesdroppers. To keep you secure, Firefox will warn you if there's a problem with a site's certificate. EAGLE site is legitimate; you can tell Firefox to bypass these warnings.

On the warning page, click "*Or you can add an exception...*".



Click "Add Exception...".

EAGLE GLINT - OPERATOR MANUAL



Secure Connection Failed

172.17.0.150 uses an invalid security certificate.

The certificate is not trusted because it is self signed.
The certificate is only valid for localhost.
The certificate expired on 14/02/2008 18:52.

(Error code: sec_error_expired_issuer_certificate)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

[Get me out of here!](#) [Add Exception...](#)

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

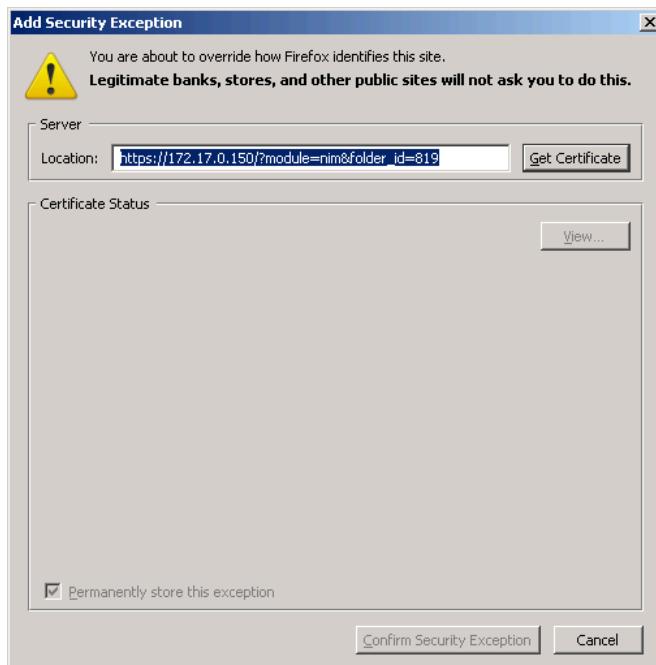
Page 46/66

This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

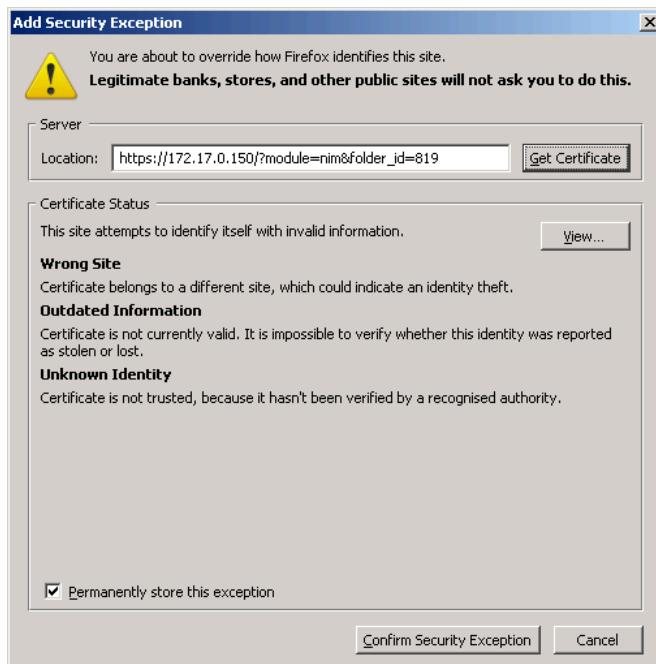


EAGLE GLINT - OPERATOR MANUAL

The “Add Security Exception” dialog will appear.



Click “Get Certificate”.



Click “Confirm Security Exception”.

“Confirm

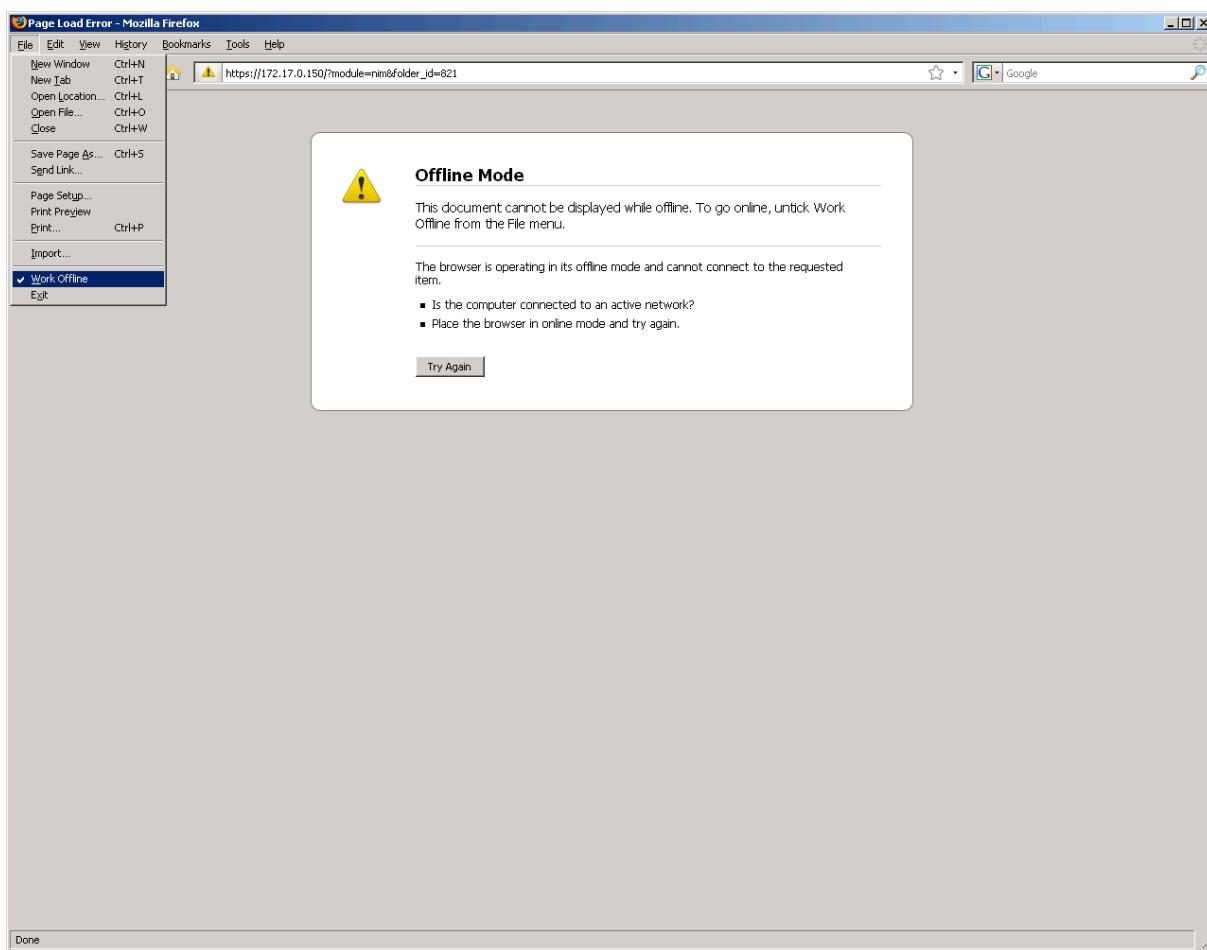
Security

Exception”.

4.1.2. Offline Mode

Firefox has an offline mode where it does not try to use the Internet. If your Firefox is in offline mode, it will show “*Offline mode*” message when you try to use EAGLE’s MMI.

To turn off offline mode, open the “File” menu. If there is a check mark beside “*Work Offline*”, click “*Work Offline*” to remove the check mark. If there's no check mark, Firefox is not in offline mode.



4.2. EAGLE MESSAGES

4.2.1. Interception locked by someone else

When an interception is opened for the first time by an Operator (you or somebody else), its current Status is changed for "Open" and a mechanism, called Lock, is applied for enforcing limits on its access. This is done to avoid concurrency ranking of an interception.

The screenshot shows the EAGLE interface with the title 'INTERCEPTION (OPEN)'. The page displays technical data such as Unique identifier (0000002cae04820000000f6d50e0000), Type (Http), Category (Http), Date (Wed, 07 Jan 09 16:00:55 +0000), and Transcoding status (TCP Informations). A yellow banner at the bottom states 'Interception locked by someone else'. Below the banner is a link 'Open Transcription'.

Then, the owner of the Lock become the "owner" of the interception and all other operators will have a read-only access until the Lock will be released. This will be done when the owner of the Lock will rank the interception.

EAGLE GLINT - OPERATOR MANUAL



Via his MMI, the Superuser can know who is the owner of a Lock.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

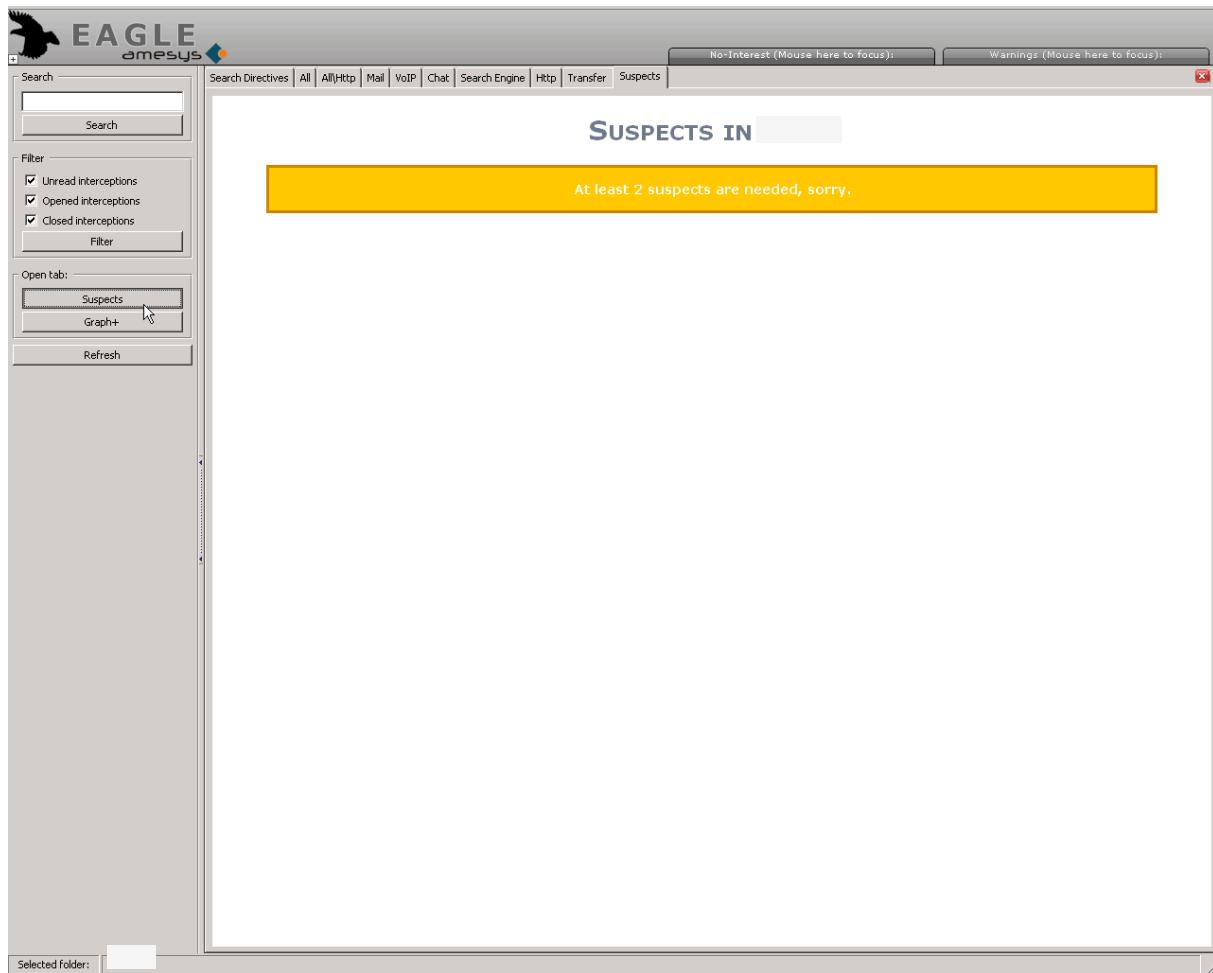
Page 50/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

4.2.2. At least 2 suspects are needed, sorry

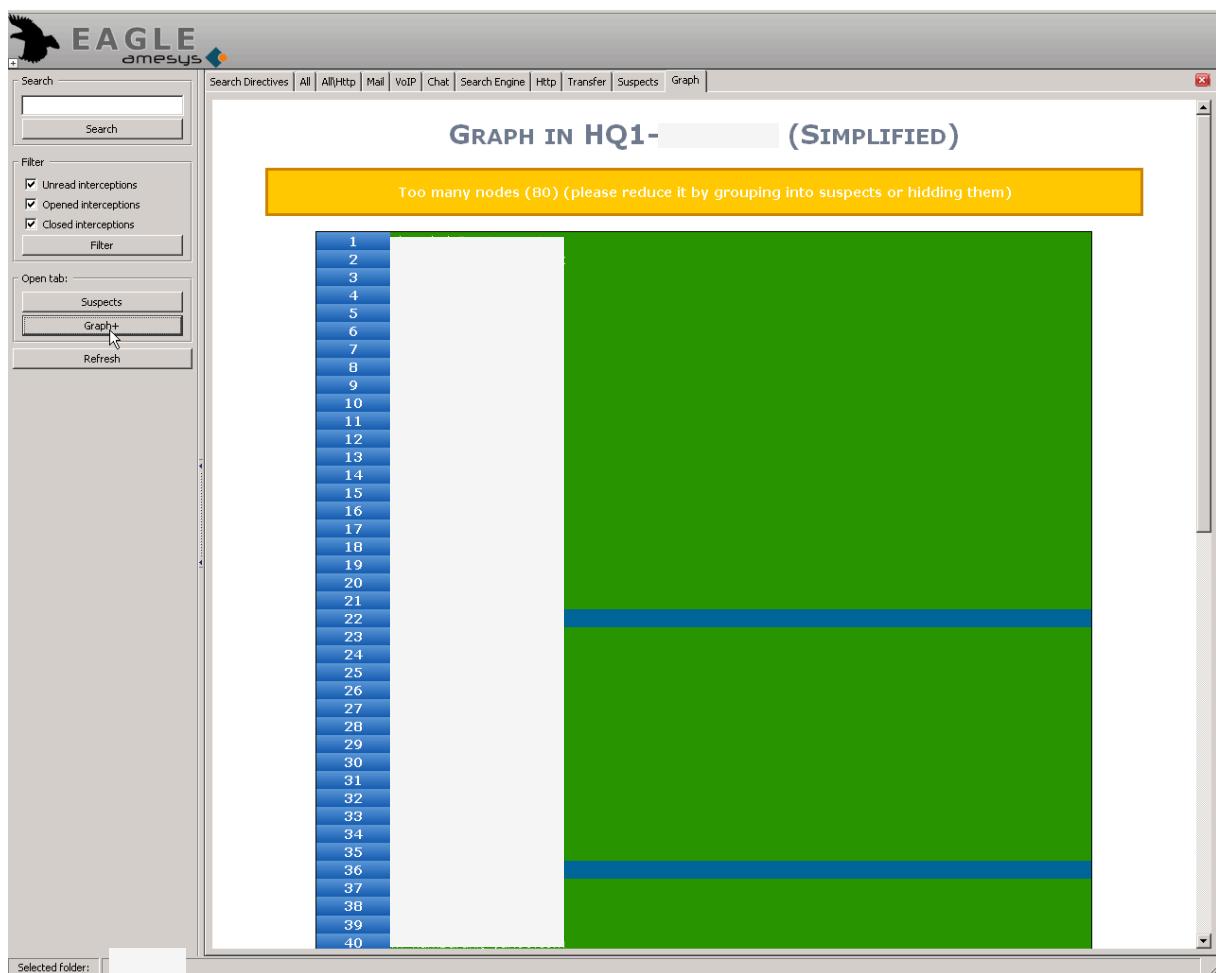
The “Suspects” tab displays only connections between suspects. You obtain the “*At least 2 suspects are needed, sorry*” message when one or fewer Suspects are linked to your current OC Process Folder: this is normal.



If you report new IDs through the “*Named Entities*” of your “*Transcription*”, your Superuser will create new Suspects and linked them to your OC Process Folder. Then, when at least two Suspects will be linked on it, you will be able to use the “*Suspects*” tab.

EAGLE GLINT - OPERATOR MANUAL

4.2.3. Too many nodes



Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 52/66

This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.



EAGLE GLINT - OPERATOR MANUAL

4.2.4. Cannot retrieve mail

Please alert your Superuser as soon as possible.

The screenshot shows a software window titled "INTERCEPTION (OPEN)". The window has several sections:

- Technical Data:**

Unique identifier	0000000afb764913370000e15c330400
Type	Mail
Category	Webmail
Date	Thu, 22 Jan 09 15:00:50 +0000
Transcoding status	Not transcoded
TCP Informations	[redacted]
- Technical Specific Data:**

From:	:
To:	:
Subject:	:
- Extra Data:**

LANG	[redacted]
ISP_ID	[redacted]

This is a spam, send it to spamfilter
- Relevance note:**

Very Good	Good	Poor	Zero
-----------	------	------	------
- Actions:**

Open Transcription

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 53/66

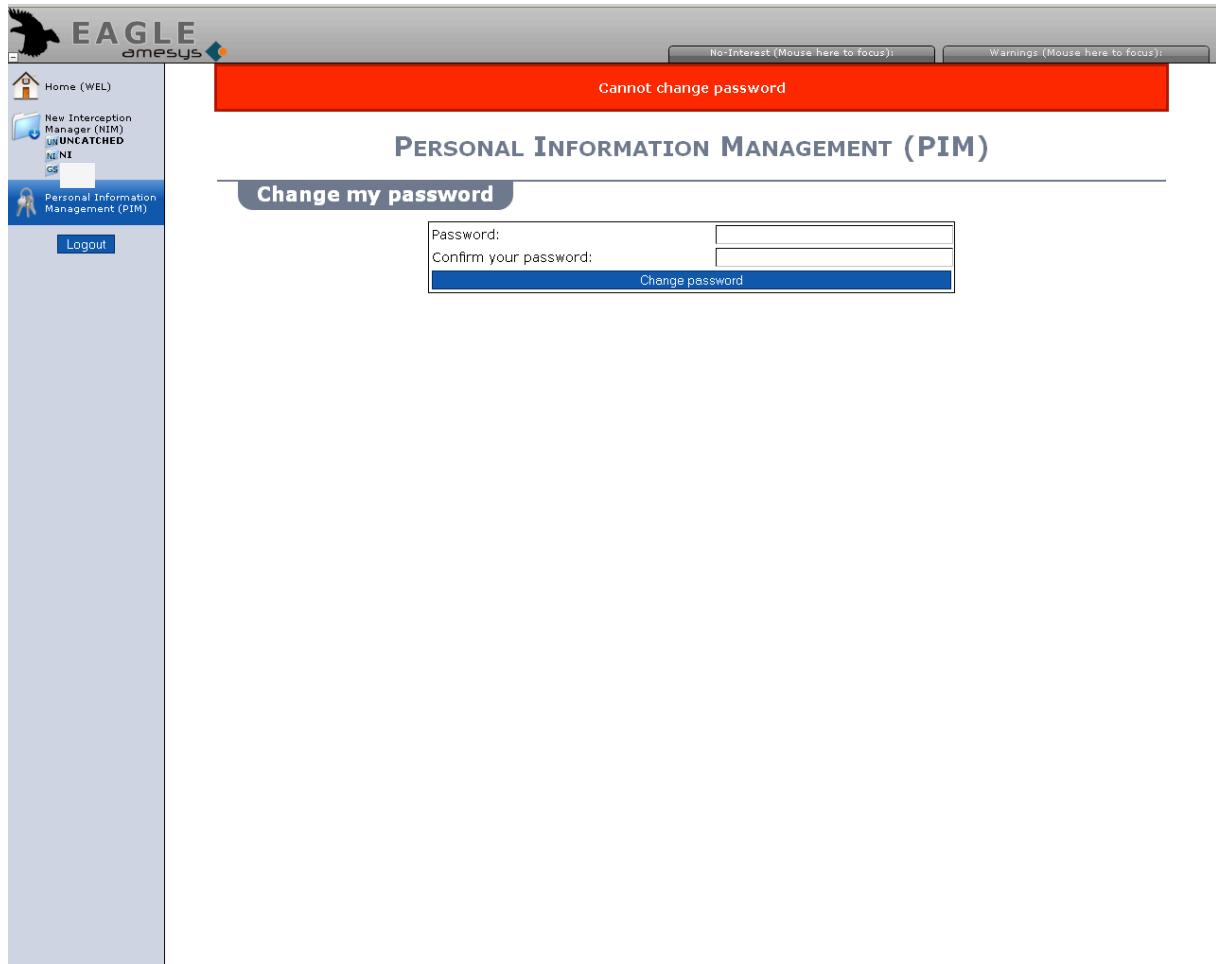


This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

amesys

4.2.5. Cannot change password

When you set a password, you must always type the password twice to confirm it. You did this, but the two passwords you typed do not match.



Just type carefully the password twice again.

4.3. CASES STUDY

4.3.1. Junk e-mail

E-mail spams, also known as Junk e-mails, are identical messages sent to numerous recipients by e-mail. Below is an example of spam:

From: [redacted]
To: [redacted]
Subject: Play with 555 Euro of Royal Club Casino's money!
Date: Sat, 24 Jan 2009 20:16:34 +0900
[Display mail in a separate window \(printer-friendly\)](#)

Play with 555€ of Royal Club Casino's money!

Yes indeed, Royal Club Casino is giving away its money and today it's your turn to get some. Open an account with Royal Club and you can receive up to 555€ free! So this is how it works:

First deposit: 300% bonus worth up to 300€
Second deposit: 100% bonus worth up to 100€
Third deposit: 155% bonus worth up to 155€

Not only will you receive this royal bonus, but you will also get the widest choice of realistic and exciting games available on the market, including slots, video poker, roulette and blackjack.

<http://www.realwavecasino.com/>

Get the Royal treatment you deserve!

EAGLE has its own e-mail spam filtering based on content-matching rules which are applied to determine whether an email is “**spam**” or “**ham**” (non-spam messages). Most rules are based on regular expressions that are matched against the body or header fields of the message. Usually a message will only be considered as spam if it matches multiple criteria.

EAGLE’s spamfilter tries to reinforce its own rules. Typically, when you attribute a “*Relevance note*” you feed example of ham (useful) mails to the spamfilter:

Mail successfully sent to the hamfilter

And when you click on the “*This is spam, send it to spamfilter*” button, you feed example of spam mails.

Mail successfully sent to the spamfilter

EAGLE GLINT - OPERATOR MANUAL

Then the spamfilter can learn the difference between the two.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 56/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

EAGLE GLINT - OPERATOR MANUAL

4.3.2. e-Newsletters, Alerts ...

Do not confused junk e-mail with a solicited mail such as e-Newsletters or the Google Alert below to which it is necessary to subscribe.

From: Google Alerts <googlealerts-noreply@google.com>
To:
Subject: Google Alert - BP SHARE PRICE
Date: Mon, 19 Jan 2009 16:11:54 +0000
[Display mail in a separate window \(printer-friendly\)](#)

Google News Alert for: BP SHARE PRICE

[FTSE up on comods but RBS blunts bank bailout boon](#)
guardian.co.uk - UK
Heavyweight energy stocks added most points to the index as the **price** of crude steadied around \$36 a barrel. BG Group, **BP** and Royal Dutch Shell gained ...
[See all stories on this topic](#)

[Four of My Favorite Stocks](#)
Seeking Alpha - New York,NY,USA
I own stock in each of these companies and have never sold a **share**. I look to add to my positions when I think the **prices** are cheap.
[See all stories on this topic](#)

[New £200bn bailout for UK banks](#)
This is Money - UK
The method of gambling on **share price** falls was widely blamed for a series of slumps in banks' **share prices** last summer and autumn, most notably at HBOS ...
[See all stories on this topic](#)

[Alliance Meet Alaska](#)
Alaskajournal.com - Anchorage,AK,USA
Speakers at this year's event include senior executives with the major North Slope producing

Nevertheless, emails such as e-Newsletters or Alerts can often, but not always, be reported to your Superuser as not-Interesting e-mails. As counterexample, consider the following e-Newsletter from a specialized website:

From:
To:
Subject: Gulf in the Media News Alert - December 18, 2008
Date: Thu, 18 Dec 2008 13:42:52 +0400
[Display mail in a separate window \(printer-friendly\)](#)

 For details of these and other stories on the Gulf, log on to
www.gulfinthemedia.com

Top Headlines December 18, 2008

 Bahrain arrests group suspected of planning attack

A group planning a terrorist attack in the Gulf state of Bahrain has been arrested, the state security authority said in a statement on Wednesday ...

 Bush touts relations with Pakistan, Saudi Arabia

President George W. Bush said on Wednesday he is leaving to his successor a stronger anti-terrorism partnership with Pakistan and Saudi

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 57/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

4.3.3. Notifications

The original SMTP mail service provides limited mechanisms for tracking a sent message, and none for verifying that it has been delivered or read. It requires that each mail server must either deliver it onward or return a failure notice (Bounce message), but both software bugs and system failures can cause messages to be lost. To remedy this, Delivery Status Notifications (DSN also called Delivery receipts) and Message Disposition Notifications (MDN also called Return receipts) are used.

Errors can occur at multiple places in mail delivery. A sender may sometimes receive a bounce message from the sender's mail server, and other times from a recipient's mail server. That happens because when a server accepts a message for delivery, at the same time it takes the burden to send a DSN in case the delivery fails.

There are many reasons why an e-mail may bounce. One reason is if the recipient address is misspelled, or simply does not exist on the receiving system. This is a user unknown condition. Other reasons include resource exhaustion, such as a full disk, or the rejection of the message due to spam filters. In addition, there are MUAs that allow users to bounce a message on demand.

Bounce messages in SMTP are sent with the envelope sender address <>, known as the “*null sender address*”. They are frequently sent with a “*From*” header address of MAILER-DAEMON at the recipient site.

TECHNICAL SPECIFIC DATA	
From:	<>
To:	
Subject:	failure notice
TECHNICAL SPECIFIC DATA	
From:	
To:	
Subject:	Warning: could not send message for past 4 hours

EAGLE GLINT - OPERATOR MANUAL

Typically, a bounce message will contain several pieces of information to help the original sender in understanding the reason his message was not delivered:

- The date and time the message was bounced,
- The identity of the mail server that bounced it,
- The reason that it was bounced (e.g. user unknown or mailbox full),
- The headers of the bounced message,
- Some or all of the content of the bounced message.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 59/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

EAGLE GLINT - OPERATOR MANUAL

Below are different examples of notifications:

From: [REDACTED]
To: [REDACTED]
Subject: failure notice
Date: 3 Sep 2008 10:54:08 -0000

[Display mail in a separate window \(printer-friendly\)](#)

Hi. This is the gmail-send

From: Unknown (see above)
To: Unknown (see above)

[Display mail in a separate window \(printer-friendly\)](#)

From: [REDACTED]
To: [REDACTED]
Subject: Unknown (see above)

This is an automatically generated Delivery Status Notification

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 60/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

4.3.4. Placeholder in a message

To protect your privacy from junk e-mail senders, some e-mail client such as Microsoft Office Outlook are configured by default to block image downloads from the Internet. Then, a blocked image appears as a  placeholder indicating an image can't be displayed.



The screenshot shows an email message with the following details:

From: Unknown (see above)
To: Unknown (see above)
Date: January 22, 2009
Subject: Make 20% Yields from Our Vegetable Economy
Author: By Tom Dyson
Text Preview: Traders called it the "Greenspan Put."
Text Content: During the 1980s and 1990s, the Federal Reserve adopted an unofficial "bailout" policy. Whenever a crisis occurred, Fed Chairman Alan Greenspan would cut interest rates and inject billions of dollars of extra credit into the system. This "re-juiced" the markets, making them rise again.
Text Footer: Traders buy put options to protect themselves from catastrophe. Put options are like insurance. With the Greenspan Put in place, traders felt comfortable
Image Placeholder: A large empty rectangular box with a small placeholder icon in the top-left corner, indicating where an image was blocked.

5. GLOSSARY

ADSL	Asymmetric Digital Subscriber Line Data communications Technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.
Bounce message	An automated electronic mail message from a mail system informing the sender of another message about a delivery problem. The original message is said to have bounced.
DSN	Delivery Status Notification See Bounce message.
e-Newsletter	A regularly distributed publication via email, generally about one main topic that is of interest to its subscribers.
FTP	File Transfer Protocol Internet standard protocol used to transfer data from one computer to another through a network such as the Internet.
GS	General Search Category of EAGLE Process Folder, dedicated to unidentified target or broad group.
H.323	H.323 is an ITU-T Recommendation that defines the protocols to provide audio-visual communication sessions on any packet network. It is widely deployed worldwide by service providers and enterprises for both voice and video services over Internet Protocol (IP) networks.
Ham	Non-spam message.
HTTP	Hypertext Transfer Protocol Internet standard protocol used for retrieving inter-linked text documents (hypertext) via the Internet.
IMAP	Internet Message Access Protocol Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
IP address	Internet Protocol address Numerical identification (logical address) that is assigned to devices participating in a computer network using the Internet Protocol for communication between its nodes.
ISP	Internet Service Provider

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 62/66



EAGLE GLINT - OPERATOR MANUAL

Company that offers to its customers access to the Internet.

MGCP

Media Gateway Control Protocol

Signalling and call control protocol used within a distributed Voice over IP system.

MIME

Multipurpose Internet Mail Extensions

Internet standard that extends the format of e-mail to support: Text in character sets other than ASCII, Non-text attachments, Message bodies with multiple parts and Header information in non-ASCII character sets.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 63/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

EAGLE GLINT - OPERATOR MANUAL

MMI	Man-Machine Interface Aggregate of means by which the users interact with the EAGLE system.
MUA	Mail User Agent also known as E-mail client Front-end computer program used to manage e-mail.
NDN	Non-Delivery Notification See Bounce message.
NDR	Non-Delivery Report/Receipt See Bounce message.
NI	Not-Interesting EAGLE Process Folder, dedicated to targets identified as uninteresting.
NIM	New Interception Manager EAGLE Module containing the different Process Folders allocated to the Operator by a Superuser.
OC	Open Case Category of EAGLE Process Folder, dedicated to well-known and identified target.
Paltalk	Paltalk is an internet chat service for text, voice and video chatting. The Paltalk Messenger program is only available to users of Microsoft Windows.
PIM	Personal Information Management EAGLE Module permitting to the logged user (Operator or Superuser) to change his password to access to the Eagle User Interface.
POP3	Post Office Protocol version 3 Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
Protocol	Convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints.
Proxy server	Server (a computer system or an application program) that forwards the requests of its clients to other servers.
Remailer	Server that receives messages with embedded instructions on where to send them next, and which forwards them without revealing where they originally came from.
RTP	Real-time Transport Protocol

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 64/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

EAGLE GLINT - OPERATOR MANUAL

Internet standard protocol used for audio and video Transmission over the Internet.

SIP

Session Initiation Protocol

Signalling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet.

SMTP

Simple Mail Transfer Protocol

Internet standard protocol used for e-mail Transmission over the Internet.

Reference: EAGLE / MAN-EAGLE-OPERATOR

Version 1.0 — 19/03/09

Page 65/66



This document is AMESYS property. It cannot be copied nor communicated to a third party without AMESYS written authorization.

EAGLE GLINT - OPERATOR MANUAL

SPAM

Also known as **junk e-mail**

Unsolicited identical messages sent to numerous recipients.

TCP

Transmission Control Protocol

One of the cores Internet standard protocols, providing reliable, ordered delivery of a stream of bytes from one program on one computer to another program on another computer.

Transcoding

The direct digital-to-digital conversion of one encoding to another.

UN

Uncatched

EAGLE Process Folder, dedicated to interceptions that correspond to no rules of interceptions.

URI

Uniform Resource Identifier

Compact string of characters used to identify or name a resource on the Internet. The main purpose of this identification is to enable interaction with representations of the resource over a network, typically the World Wide Web (WWW).

VoIP

Voice over Internet Protocol

Family of transmission Technologies used for Voice Communications over the Internet.

Webmail

Also known as **Web-based mail**

Email service intended to be primarily accessed via a web browser, as opposed to through an email client, such as Microsoft Outlook or Mozilla's Thunderbird. Very popular webmail providers include Gmail, Yahoo! Mail, Hotmail and AOL.