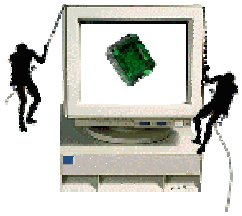


**EMERALD Development Project**

June 2001
Acknowledgments:

DARPA ITO
DARPA ISO

# EMERALD™ *Alert Management Interface*

http://www.sdl.sri.com/emerald/

System Design Laboratory

SRI International

Release Date: June 30, 2001

## User's Guide, Version 1.3



## EMERALD Development Team


EMERALD@sdl.sri.com

Steve Cheung (PI), Martin Fong, Ulf Lindqvist (PI), Phillip Porras (PD), Keith Skinner,
Alfonso Valdes (PI), Magnus Almgren, Mike Frandsen, Peter Neumann, Sandy Smith, Lynn Voss


# 1 Notice to Users

The *EMERALD Alert Management Interface* is a Java-based user interface for displaying EMERALD Security Incident Reports stored in either Postgres or Oracle databases. This component is dependent on the installation of the EMERALD database interface component, eDBMS. For more information on this component, and other EMERALD technologies, please visit the EMERALD Development Team web site at SRI International http://www.sdl.sri.com/emerald/.

# 2 Installation and Start

This section is intended as a checklist for the minimum steps required to start the EMERALD Alert Management Interface (eAMI).

## 2.1 Unix

1. Check the System Requirements for what additional components are needed to start eAMI in your Unix Environment.
2. Change to the root directory of the eAMI package.
3. Type `Run.AMI.Unix.csh` from the installation directory.

## 2.2 Windows

1. Run the self-extracting archive EM_AMI_WIN-1-3-1.exe from any Windows directory. This will automatically setup eAMI for your environment and place an icon on your desktop and also in your start menu.
2. **If you are Running Windows 95/98: You will need to Right-Click on the desktop EMERALD icon and increase the environment memory size to 1024.**
3. Click on the eAMI desktop icon to start eAMI.

# 3 System Requirements

The Windows release of the EMERALD Alert Management Interface will run on Windows 98, Windows NT, and Windows 2000.

## 3.1 Unix System Requirements

The EMERALD Alert Management Interface requires that JAVA JRE 1.2.2 must be installed on your system and accessible to the account from which you will run *eAMI*. Java 1.2.2 can be obtained from Sun Microsystems at

http://java.sun.com/products/jdk/1.2/jre/

## 3.2 eAMI Package Contents

All files included in the project are located inside one root directory. All paths used in the application are relative to this directory. Currently the following sub-directories are used:

- **com** – root for Java source and class files. In release version should be replaced by a single JAR file. *Important: before release all classes should be recompiled with ApplicationFrame.DEBUG set to false (see source code for details).*
- **img** – contains image files. Relative to com/sri/intruder/ui directory.
- **res** – contains localized messages and labels (like Emerald_de.properties). . Relative to com/sri/intruder/ui directory.
- **config** – contains configuration files. *Important: not all settings used for debug may be appropriate in release.*
- **docs** – contains documentation.
- **help** – will contain help files. May be replaced by a single JAR file.
- **lib** – contains JAR libraries used by application:

# 4 EMERALD Alert Management Interface

The EMERALD Alert Management Interface is a unique graphical user interface (GUI) for managing alerts produced by EMERALD sensors. Using this interface, an administrator can view individual alerts, manage incident handling reports, print reports, forward reports via e-mail, and view recommendations on responding to attacks. Administrators can also associate incident handling notes with each alert record to document information gathered during an investigation of the alert.

Alerts are displayed in the GUI in folders. There are two built-in system folders, Inbox and Trash, which are always present. A user may also define additional folders which contain alerts matching specific criteria. These additional folders contain subsets of the Inbox folder; that is, any alert in a user-defined folder also appears in the Inbox and may appear in more than one user-defined folder if it matches their criteria. Alerts in the Trash folder do not appear in the Inbox or in any of the user-defined folders. The Inbox

and Trash folders together contain all the alerts in the chosen database. Each user of the GUI has her or his own Trash folder, and alerts in one user's Inbox may appear in another user's Trash folder. Therefore, what one user puts in her or his Trash folder has no consequences for other users. However, if a user deletes an alert from the database, that alert will no longer be accessible by any user.

The GUI has three windows: the Alert window, the Sensor Status window, and the Help window. The functionality of each window is described below. A folder becomes the active folder when its icon is selected by clicking on it in the Folder panel in the Alert window.

When the eAMI is run, the Alert window is displayed and a dialog box pops up (Figure 2). This dialog box controls what alert database is opened and is described below.

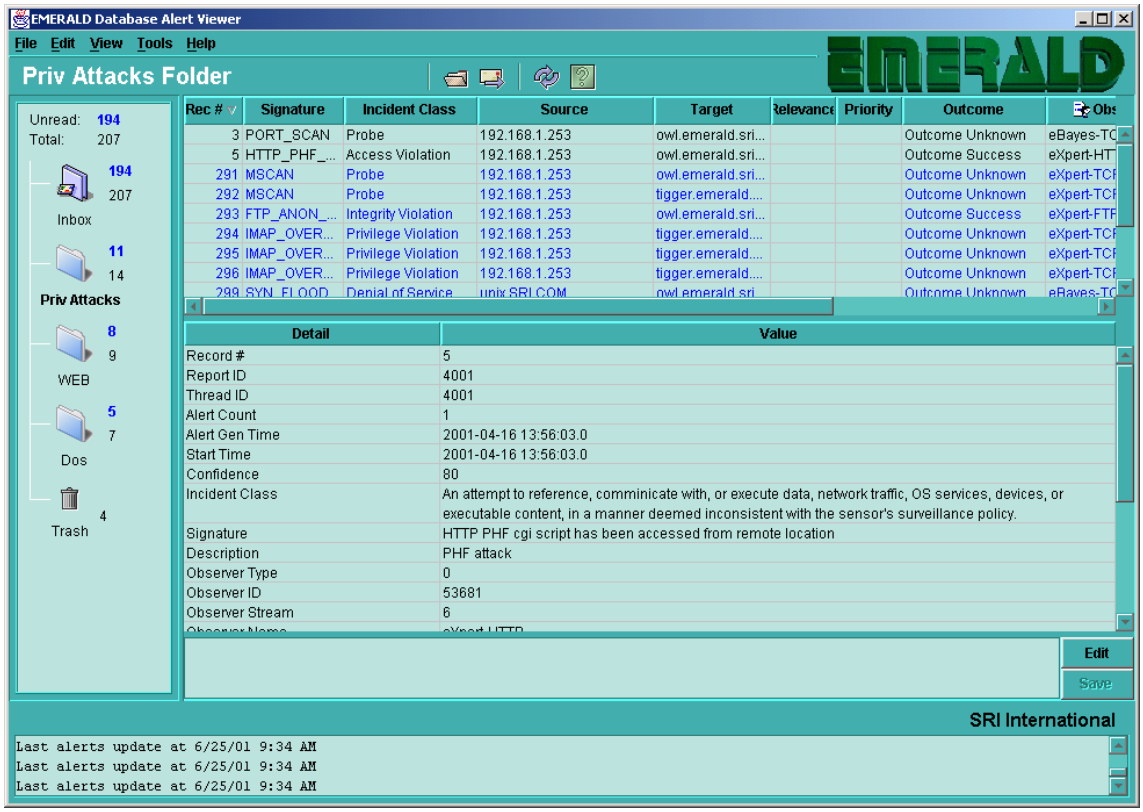
## 5 Alert window

The Alert window is the main window displayed most of the time during normal operation. It includes a pull-down menu bar and six panels: the Buttons panel, the Folder panel, the Table of Contents panel, the Details panel, the Administrative Notes panel, and a Status panel. The Buttons panel is the narrow panel above the top, just below the menu bar, containing four buttons. The Folder panel is the vertical panel on the left. On the right, the Table of Contents panel appears on the top, the Details panel below it, and the Administrative Notes panel below the Details panel. Across the bottom of the window is the Status panel.

In the upper left of the window, immediately below the menu bar, is displayed the name of the currently active folder, whose contents are listed in the Table of Contents panel. The active folder's name is also shown in bold type in the Folder panel.

The Alert window is shown in Figure 1. In this example, there are three user-defined folders, Priv Attacks, WEB, and Dos, in addition to the Inbox and Trash folders. The active folder is Priv Attacks, containing 11 unread alerts and 3 read alerts, or a total of 14. The alerts are sorted by their record number (Rec #) in the Table of Contents panel, where the first nine alerts are shown. The Details panel shows more information on record number 5. There are no notes shown in the Administrative Notes panel. The Status panel contains messages showing the times of the last alert updates.

**Figure 1. Alert window**




## 5.1 Menus

There are five pull-down menus: File, Edit, View, Tools, and Help.

### 5.1.1 File menu

The File menu contains the following options:

Open Connection…: This option opens a connection to a database of alerts. It pops up a dialog window for the user to select the database; an example of the dialog window is shown in Figure 2. The dialog window saves information from recently opened connections, enabling the user to select a database without re-entering all its information. In general, users will most often enter only their user name and password. Opening a connection to a database closes the connection to any previously open database.

**Figure 2. Open Connection… dialog window**


Close Connection: This option pops up a confirmation box. If the user confirms that s/he really wants to proceed, this closes the connection to the open alert database.

Folder: This option brings up a submenu with three options, New Folder…, Edit Folder…, and Delete Folder. (On a Windows system, this same submenu can be accessed by clicking on a folder in the Folder panel with the right mouse button.) User-defined folders are an organizational convenience; the content of a new, user-defined folder is always a subset of the Inbox folder. Note that the two system folders, Inbox and Trash, may not be deleted, and can be edited to only a limited extent.

> New Folder…: This option opens a dialog box allowing a new folder to be configured. The dialog box has three tabs, *Criteria*, *Options*, and *Location*.
>
> An alert appears in a user-defined folder (as well as in the Inbox) if it matches some criterion set by the user in the *Criteria* tab, shown in Figure 3. The criterion takes the form of an SQL clause, in which a database field name and value or set of values are specified. Further information on the field names and on structuring an SQL clause can be found elsewhere [XX: need ref].
>
> The *Options* tab, in Figure 4, lets the user name the folder and specify an audio file to be played when an alert arrives that matches that folder's criterion. The user can also specify a custom image file to use as that folder's icon in the Folder panel, and can choose to have new alerts in that folder automatically e-mailed to an address entered in this tab.
>
> The *Location* tab lets the user choose where (vertically) to display the new folder in the Folder panel.

**Figure 3. New/Edit Folder… dialog box: *Criteria* tab**

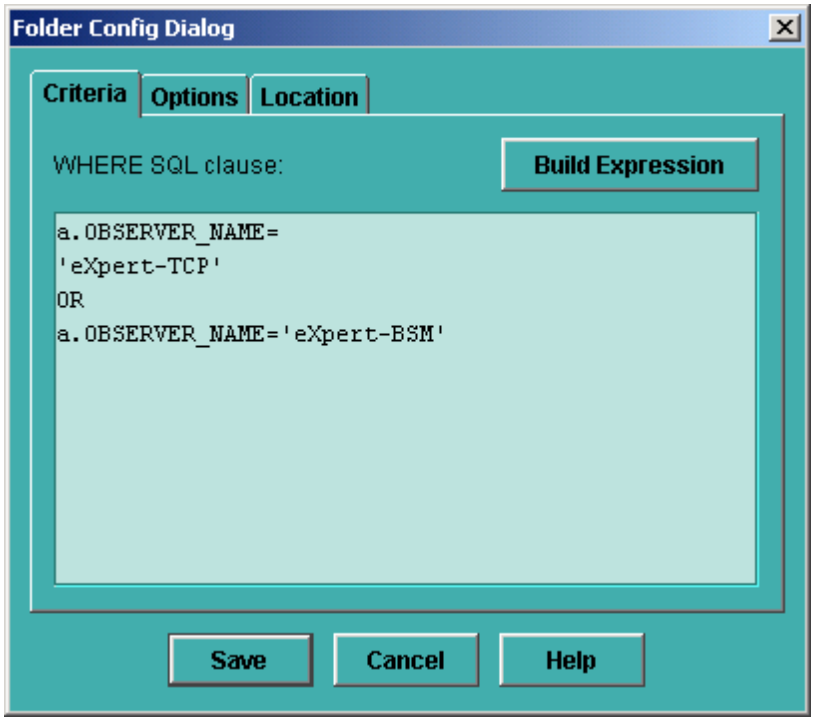
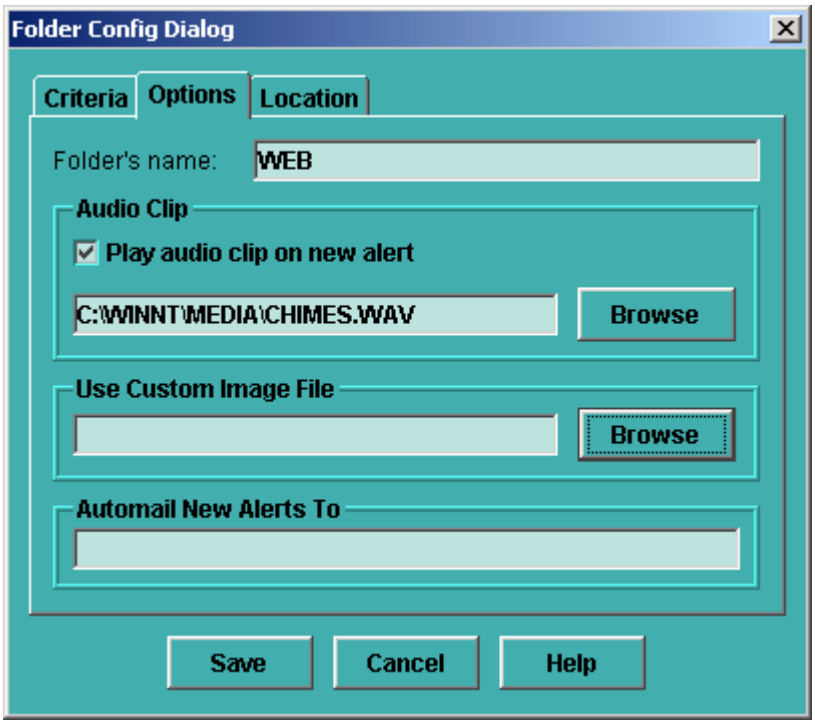



**Figure 4. New/Edit Folder… dialog box: *Options* tab**




Edit Folder…: This option opens a dialog box allowing the configuration of the folder being edited to be modified. The dialog box has three tabs, *Criteria*, *Options*, and *Location* and is the same as when New Folder… is

chosen. For the Inbox and Trash folders, only the *Location* tab is available.

An alert appears in a user-defined folder (as well as in the Inbox) if it matches some criterion set by the user in the *Criteria* tab. The criterion takes the form of an SQL clause, in which a database field name and value or set of values are specified. Further information on the field names and on structuring an SQL clause can be found elsewhere [XX: need ref].

The *Options* tab lets the user rename the folder and specify an audio file to be played when an alert arrives that matches that folder's criterion. The user can also specify a custom image file to use as that folder's icon in the Folder panel, and can choose to have new alerts in that folder automatically e-mailed to an address entered in this tab.

The *Location* tab lets the user organize the folders in the Folder panel by changing their vertical placement.

Delete Folder: This option can be used to delete any folder other than the two system folders, Inbox and Trash. A confirmation box appears when this option is selected.

Empty Trash Folder: This option deletes any alerts stored in the Trash folder from the database. If there are no alerts in the Trash folder, this option is disabled. Note that each user has her or his own Trash folder, which is local. Deleting the alerts by emptying the Trash folder will remove them from the database and they will no longer be accessible to any user.

Export to File…: This option saves alert records to an HTML file. It opens a configuration box in which the user can specify the name of a file to save alerts to. If the file already exists, a confirmation box will ask the user if s/he wants to write over the file or cancel. The user can also choose between exporting all the alerts in the active folder, or only selected alerts. The information saved includes all the information in the Details panel and the Administrative Notes panel for the saved alerts. The help button on the dialog box is not yet implemented.

E-mail Alerts…: This option sends an e-mail to the address specified in the dialog box which appears, with the specified subject line and additional message text if desired. The user may choose to mail all the alerts in the active folder or only selected alerts. All database fields that contain information about that alert are included in the e-mail, along with any administrative notes; this is equivalent to mailing the information in the Details panel and the Administrative Notes panel. The help button on the dialog box is not yet implemented.

Exit: This option closes the eAMI GUI.

### 5.1.2 Edit menu

The following options are available in the Edit menu:

Set Read: If there are one or more alerts selected in the Table of Contents panel and this option is chosen, the selected alerts are marked as read. The alerts

therefore will appear in black in the Table of Contents panel and not be included in the Unread messages count for the folder(s) in which the alerts appear.

Set Unread: If there are one or more alerts selected in the Table of Contents panel and this option is chosen, the selected alerts are marked as unread. The alerts therefore will appear in blue in the Table of Contents panel and will be included in the Unread messages count for the folder(s) in which the alerts appear.

Set Lock: If there are one or more alerts selected in the Table of Contents panel and this option is chosen, the selected alerts are "locked" for all users. A locked alert may not be directly deleted from the database. In order to delete a locked alert, a user must first unlock it and then delete it. This option is useful when several users are accessing the same database and a user wishes to protect alerts from accidental deletion. The locking user's name is associated with the alert; however, any user may unlock the alert.

Set Unlock: If there are one or more alerts selected in the Table of Contents panel and this option is chosen, the selected alerts are "unlocked" for all users. Unlocked alerts can be deleted in a single step.

Move To Trash: If there are one or more alerts selected in the Table of Contents panel and this option is chosen, the selected alerts are moved to the user's Trash folder. They are removed from the Inbox folder and any other folders in which they appear. Note that the Trash folder is local to each user; an alert may be in one user's Trash folder and in another user's Inbox.

Restore From Trash: If one or more alerts in the Trash folder are selected in the Table of Contents panel, this option will restore the selected alerts to the user's Inbox folder and to any other folders whose inclusion criteria they match. The alerts are removed from the Trash folder. Note that the Trash folder is local to each user; an alert may be in one user's Trash folder and in another user's Inbox.

Delete: If there are one or more alerts selected in the Table of Contents panel and this option is chosen, the selected alerts are completely removed from the database (and do not appear in the Trash folder). A confirmation box pops up when Delete is selected. An alert which is deleted is deleted for all users. An alert whose administrative notes are being edited may not be deleted, nor may a locked alert.

Clear database: This option deletes all alerts which are neither locked nor having their administrative notes being edited, from the database. It opens a confirmation box before proceeding.

### 5.1.3 View menu

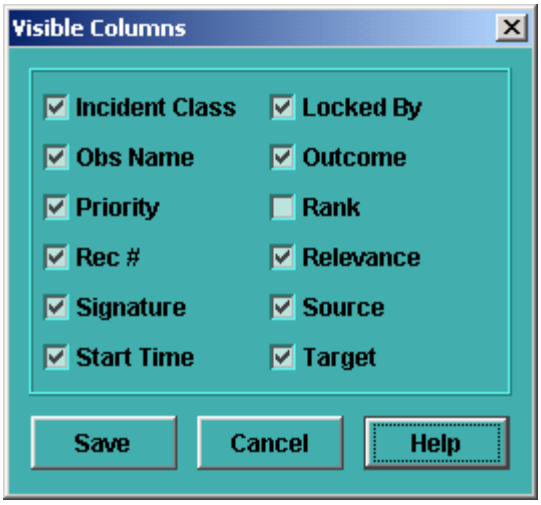
Available options are Sensor Status and Visible Columns.

Sensor Status: Selecting this option opens the Sensor Status window.

Visible Columns: Selecting this option displays the information columns which may be displayed in the Table of Contents panel. Those columns currently being displayed are marked with a check. A column may be shown or hidden by

toggling the check mark in this list. [XX: would be nice if I could cross-reference where the list of available columns and what they mean] Figure 5 shows the dialog box showing the available information columns. The help button in this dialog box is not yet implemented.

**Figure 5. View/Visible Columns checklist**




### 5.1.4 Tools menu

There are two options available, Update Alerts Table and Settings…

Update Alerts Table: This option accesses the database and updates the set of alerts and the status of EMERALD sensors connected to the system. The list of alerts in the eAMI is ordinarily updated on a schedule set in the *Update* tab in the Settings… dialog box. Choosing this menu option requests an additional, immediate update to the list.

Settings…: This option opens a dialog box shown in Figure 6. The dialog box contains four tabs: *Appearance*, *Format*, *Update*, and *Mail*.

The *Appearance* tab allows the user to change the color scheme of the application and localization information. The localization information is read in from a set of configuration files described elsewhere [XX: would be nice to have a reference]

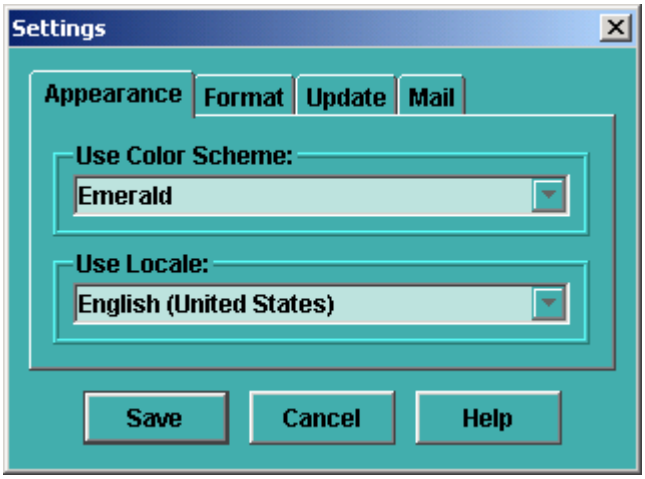
The *Format* tab allows customization of the time zone to be used in formatting dates. In addition, a check box on this tab controls whether IP addresses or their corresponding domain names are displayed, for example in the Table of Contents panel.

The *Update* tab affects the viewing of alerts. Using this tab, the user can control how often the list of alerts is updated, in milliseconds. The user can also choose to display only alerts created during the last given number of days; if the user enters 0 days, all alerts in the database will be shown.

The *Mail* tab contains information for e-mailing records. The information includes the address, host name, and user name to send the mail from.

This information is used when the E-mail Alerts option in the File menu is chosen.

**Figure 6. Tools/Settings dialog box**




### 5.1.5 Help menu

Available options are Help Topics and About….

Help Topics: This option brings up the Help window containing on-line documentation.

About…: This option shows the current EMERALD version number and copyright information, and the JVM version number.

## 5.2 Button panel

In the top center of the window, to the right of the active folder name, are four buttons: *Open connection*, *Send e-mail*, *Update data*, and *Help*.

The *Open connection* button has the same effect as selecting Open Connection… from the File menu. Before opening a connection to a database of alerts, it pops up a dialog window for the user to select the database, shown in Figure 2. The dialog window saves information from recently opened connections, enabling the user to select a database without re-entering all its information. In general, users will most often enter only their user name and password. Opening a connection to a database closes the connection to any previously open database.

The *Send e-mail* button has the same effect as the E-mail Alerts… option in the File menu. It sends e-mails to the address specified in the dialog box which appears, with the specified subject line and additional message text if desired. The user may choose to mail all the alerts in the active folder or only selected alerts. All database fields that contain information about that alert are included in the e-mail, as well as any administrative notes; this is equivalent to mailing the information in the Details panel and the Administrative Notes panel. The help button on the dialog box is not yet implemented.

The *Update data* button has the same effect as the Update Alerts Table option in the Tools menu. It accesses the database and updates the set of alerts and the status of EMERALD sensors connected to the system. The list of alerts in the eAMI is ordinarily updated on a schedule set in the *Update* tab in the Settings… dialog box. Clicking on this button requests an additional, immediate update to the list.

The *Help* button has the same effect as the Help Topics option in the Help window. It brings up the Help window containing on-line documentation.

## 5.3 Folder panel

The Folder panel displays the folders which can be used for managing alerts. The folders include two system folders, Inbox and Trash, as well as any user-defined folders. Clicking on a folder with the left mouse button opens that folder. When a folder is open, or active, its name changes to bold font and is displayed above the Folder panel and its contents are listed in the Table of Contents panel. On a Windows system, clicking on a folder's icon with the right mouse button brings up the same submenu as found on the main menu bar under File/Folder. The right mouse button does not have this functionality on a Unix system.

In Figure 1, there are three user-defined folders, Priv Attacks, WEB, and Dos, in addition to the two system folders. Priv Attacks is the active folder.

## 5.4 Table of Contents panel

This panel shows the alerts stored in the active folder. (The name of the active folder is displayed in the upper left of the Alert window, directly below the pull-down menu bar.) Alerts shown in blue are unread; black alerts have been selected and read. In Figure 1, the first two alerts have been read, and the seven others which are displayed are unread.

If a user selects an alert by clicking on it with the left mouse button, detailed information on the alert appears in the Details panel. On Windows systems, if the user selects an alert and then clicks the right mouse button, a copy of the Edit menu appears and those options may be applied to the selected alert.

Alerts can be moved to the Trash folder by selecting them in the Table of Contents panel and dragging them to the Trash folder icon in the Folder panel.

Information about the alerts is contained in a number of columns. The alerts may be sorted by any one column, into either ascending or descending order, by clicking on the heading of that column. The column currently being used for sorting, and the order of sorting, are indicated by a small vertical arrow to the right of the column name. In Figure 1, the alerts are being sorted in ascending order by record number, the leftmost column.

The column widths may be changed by clicking on the edge of a column heading and dragging it to the right or left. The columns may be reordered (left or right) by clicking on a column heading and dragging it to the left or right. It is also possible to hide selected columns, using View/Visible Columns on the pull-down menu bar. Scroll bars at the bottom and right edges of the Table of Contents panel allow viewing if the list of alerts and their information is too long or wide to be entirely displayed in the panel.

Descriptions of the information contained in each column can be found elsewhere [XX: ref].

## 5.5 Details panel

When an alert is selected by clicking on it in the Table of Contents panel, detailed information on that alert is displayed in the Details panel. This information takes the form of a list of field names, in the "Detail" column, with their values in the "Value" column. [XX: would be nice to reference field names described elsewhere] The relative widths of the two columns may be adjusted by clicking on and dragging the edge between the column headings. If more information is available than can be displayed in the panel, a scroll bar at the right edge of the panel allows vertical scrolling.

## 5.6 Administrative Notes panel

This panel allows the entry of textual notes relating to an alert which has been selected in the Table of Contents panel. The notes can be viewed by all users and appear in the Administrative Notes panel when the alert is selected. To add or modify a note, the user must click on the *Edit* button; this prevents any other user from modifying the notes for that alert at the same time. The notes will immediately become accessible to all users when the editing user clicks on the *Save* button, or selects another alert, or when the window becomes deactivated through selecting another window.

If an alert is being edited by one user, no other user can delete it.

## 5.7 Status panel

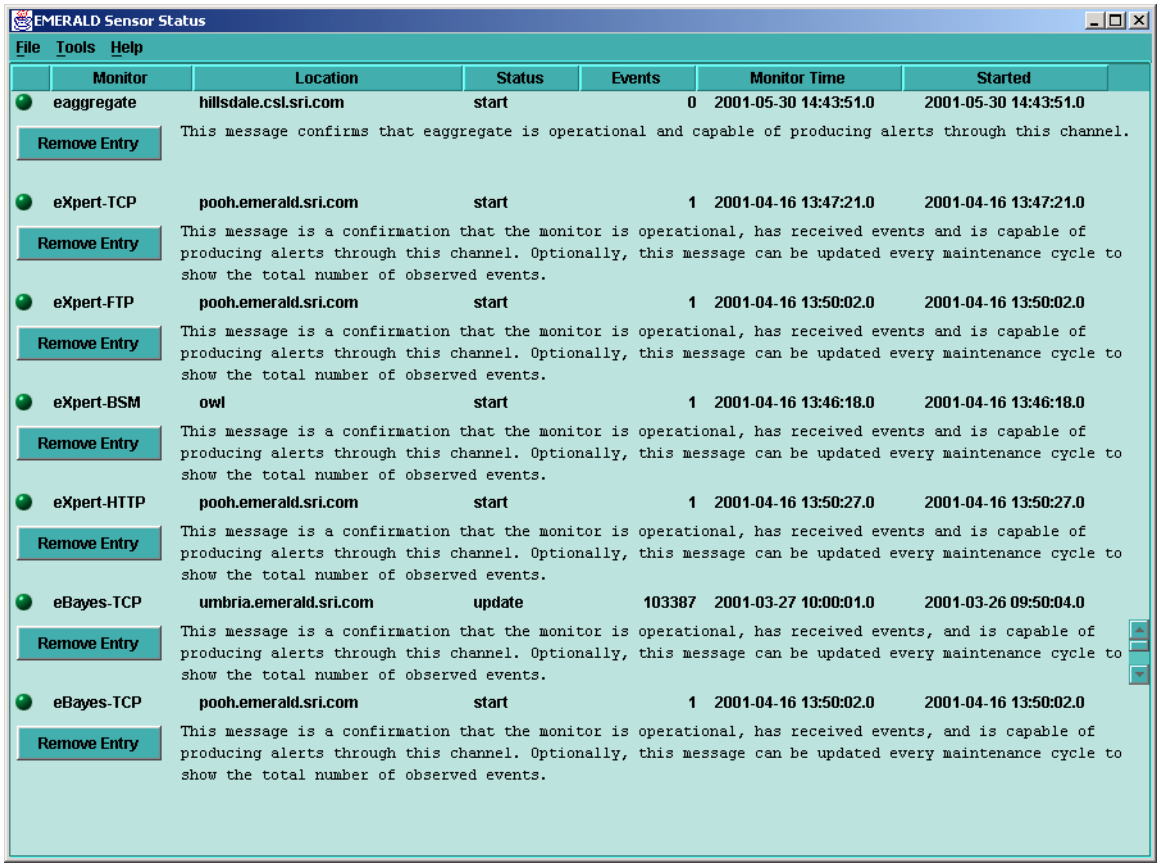
This panel contains informational messages such as the "last alerts update" messages in Figure 1. Possible messages include connection information, the time of the last alerts update, printing and e-mailing information, as well as certain kinds of errors.

If there are more messages than can be shown in this panel, a scroll bar at the right edge allows the most recent messages to be viewed. These are only the most recent messages, not all those received during a session while the eAMI is open.

# 6 Sensor Status window

The Sensor Status window shows EMERALD monitors that are connected to this system. An example of this window is shown in Figure 7. This window contains a pull-down menu bar and an information panel.

**Figure 7. Sensor Status window**




## 6.1 Menus

Menus available on the pull-down menu bar are File, Tools, and Help.

### 6.1.1 File menu

The File menu contains two options: MFILE_PRINT and Close.

> MFILE_PRINT sends the displayed sensor status information to the default installed printer, if one exists. If no printer is installed or properly configured, this option has no effect. [XX: is this true?] [XX: why is it called that, anyway? why not "Print" as it used to be?]
>
> Close closes the Sensor Status window.

### 6.1.2 Tools menu

This menu has a single option, Update Sensors Status. Ordinarily, the sensors send status signals to the database which appear in the Sensor Status window after the next automatic update. Selecting this option forces an immediate update to the sensor status information. It does not update the list of alerts.

### 6.1.3 Help menu

Available options are Help Topics and About….

Help Topics: This option brings up the Help window containing on-line documentation.

About…: This option shows the current EMERALD version number and copyright information, and the JVM version number.

## 6.2 Information panel

For each monitor, this panel displays the name, location, status, started time (time when the monitor came on-line), number of events since the started time, and monitor time (the clock time on the monitor. In the example in Figure 7, we note that all seven monitors are operational, as shown by the green balls in the leftmost column. These balls give a quick visual status check by displaying one of the following colors: green to indicate the sensor is active; amber to indicate that the sensor is late in reporting its status; yellow to indicate that it is very late and presumed not to be working; or red to indicate that the sensor has been shut down.

The *Remove Entry* buttons remove a sensor record from the database. Alerts may still be received from that sensor, but its status information will not be accessible. This is useful when a sensor has been shut down; when the sensor is re-started, it will have a new record in the database. The old record will remain and may be removed when it is no longer useful.

# 7 Help window

The Help window may be reached from either the Alert window or the Sensor Status window, by selecting Help/Help Topics on the menu bar. The Help window, shown in Figure 8, contains three panels. Along the top is a panel of four buttons. Below, the left or Navigation panel allows navigation of the help documentation, and the right or Text panel displays help text. The width of the Navigation and Text panels can be adjusted by clicking on and dragging the narrow border between the panels to the left or right.

## 7.1 Button panel

This panel contains four buttons. The *previous* and *next* buttons, marked with left and right arrows, permit navigation of previously viewed help sections, in the order in which they were viewed. The *print* button, labelled with an icon of a printer, opens a printer dialog window enabling the user to send [XX: something] to a printer. The *page setup* button, identified by an icon of a printer with a small setup button on the lower right, brings up a dialog box which lets the user control paper size and source, printing orientation, and margins, and select a printer. The setup information is only used when printing from the Help window. [XX: confirm]

## 7.2 Navigation panel

This panel has two tabs, for the *Table of Contents* and the *Help Index*.

The *Table of Contents* tab displays a table of contents of the on-line help documentation. Clicking on any section in the table of contents will display the corresponding text in the Text panel to the right. This is the tab shown in Figure 8.

The *Help Index* tab has two capabilities. First, the user can use the "Find" text box to search for a word which appears in the Table of Contents section headings. If the word is found, the text corresponding to that section will automatically be displayed in the Text panel. If the word occurs in more than one section heading, pressing the "enter" key will advance to the next section where the word was found. The second capability the *Help Index* tab offers is the ability to view the Table of Contents sections in alphabetical order. When the user clicks on a section, the corresponding text appears in the Text panel.

The section selected using either tab is highlighted in the Navigation panel.

## 7.3 Text panel

On-line help text for a section selected in either the *Table of Contents* tab or the *Help Index* tab is displayed in the Text panel, on the right.

If a word appears in the help text underlined and in a different color, the user may click on that word to jump to a section with more information on that concept.

A scroll bar appears at the right edge of the Text panel when the current text is too long to fit in the displayed panel.

**Figure 8. Help window**


# 8 Advanced Configuration

## 8.1 Overview

All information necessary to configure EMERALD project GUI is kept in a set of XML and text files located in `config` directory (relative to the root directory of installation). These files can be edited prior or during installation. Some information will be stored automatically on program's exit. The following table lists all the files currently used:

| *File* | *Content* | *Usage* |
|---|---|---|
| ***TableOfContent.xml*** | Describes data in TOC (upper table). | This file should be pre-configured according to the database schema. Part of information (columns width and order) will be saved on application's exit. |

| | | |
|---|---|---|
| ***DetailsPanel.xml*** | Describes data in details table (middle). | This file should be pre-configured according to the database schema. |
| ***NotesPanel.xml*** | Contains SQL queries used to update notes panel (bottom). | This file should be pre-configured according to the database schema. |
| ***SensorStatus.xml*** | Contains SQL queries used to update sensor status frame. | This file should be pre-configured according to the database schema. |
| ***Folders.xml*** | Contains information about folders with alerts. | System folders (inbox) must be present a installation time (and cannot be deleted o modified). User-defined folders will be store on application's exit. |
| ***System.xml*** | Lists available locales (English, German, etc.) | This file should be pre-configured at installation time. Later we may add some other information to this file. |
| ***EmeraldApp.properties*** | Contains current application's configuration information | All information stored in this file can be configured using GUI. However some reasonable default settings would be desirable. |
| ***ViewedIds.data*** | Contains list of alerts Ids viewed by local user. | This file creates and updates automatically and is not supposed to be edited. In the future we may remove this file and keep viewed alerts Ids in the database. |

## 8.2 TableOfContent.xml

| *Node* | *Description* | *Usage* |
|---|---|---|
| ***Query*** | Root node | |
| ***IdSource*** | Contains database column with unique Id for the selected row | Will be passed to queries to get detail information about selected row. Mandatory element. |
| ***From*** | Contains list of tables with possible aliases (FROM SQL clause). | Mandatory element. |

| | | |
|---|---|---|
| ***Where*** | May include part of WHERE SQL clause. *Important: selected Folder also contributed to WHERE clause.* | Optional element. |
| ***Delete*** | Contains SQL query to be executed to delete a single row with given Id. May call stored procedure. Must provide one parameter for Id to be deleted. | Used to delete a single row with given Id. Mandatory element. |
| ***Columns*** | Root for collection of query columns. | Mandatory element. |
| ***Column*** | Single column description (for both SQL query column and UI table column). | At least one Column must be present. |
| ***Source*** | Database source for this column. May include single table's column name or expression. | Mandatory element. |
| ***Title*** | UI table's column title. *Important: this is not a text, but Id of localized text stored in properties file.* | Mandatory element. |
| ***Type*** | Column's data type. Currently supported types:<br>• TEXT: for text and numerical<br>• DATE: for date (to be formatted).<br>• IP: for IP addresses (may be resolved to host names). | Mandatory element. List of supported types may be changed or extended in the future. |
| ***Format*** | Used for type DATE only. Contains reference to date format string as defined in java.text.SimpleDateFormat class. *Important :this is Id of localized format string stored in properties file.* | Mandatory element for type DATE. |
| ***Icon*** | May include name of the icon file to be used in the column's header. *Important: all names are relative to ApplicationFrame.class file. It is recommended to keep them in* ***img*** *sub-directory. Image files may be placed in JAR file along with CLASS files.* | Optional element. |
| ***Alignment*** | Contains text alignment for UI table's header: LEFT, CENTER, or RIGHT. | Optional element, default value is LEFT. |
| ***Sort*** | Contains sort order for this column: 1, 2, or none. Also contains ascending/descending attribute. | Optional element. Will be automatically |

| | | |
|---|---|---|
| | attribute. | updated as the user makes the selection. |
| ***Width*** | Contains column's width in UI table in pixels. | Optional element. Will be automatically updated as the user makes the selection. |
| ***Visible*** | Contains **true** for visible UI columns and **false** for hidden columns. | Optional element. Will be automatically updated as the user makes the selection. |

Example: given XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Query>
   <IdSource>a.ALERT_REPORT_ID</IdSource>
   <From>emerald_report a</From>
   <Where/>
   <Delete>delete from emerald_report where ALERT_REPORT_ID=?</Delete>
   <Columns>
      <Column>
         <Source>a.ALERT_START</Source>
         <Title>COLUMN_DATE</Title>
         <Type>DATE</Type>
         <Format>COLUMN_DATE_FORMAT</Format>
         <Sort asc="false">1</Sort>
         <Icon>img/date.gif</Icon>
         <Width>135</Width>
         <Alignment>Left</Alignment>
         <Visible>yes</Visible>
      </Column>
      <Column>
         <Source>a.ALERT_REPORT_ID</Source>
         <Title>ID</Title>
         <Width>110</Width>
         <Alignment>Left</Alignment>
```

```
            <Visible>yes</Visible>
        </Column>
        <Column>
            <Source>a.OBSERVER_NAME</Source>
            <Title>COLUMN_ATTACKER</Title>
            <Icon>img/attacker.gif</Icon>
            <Width>132</Width>
            <Alignment>Left</Alignment>
            <Visible>yes</Visible>
        </Column>
        <Column>
            <Source>a.OBSERVER_LOCATION</Source>
            <Title>COLUMN_LOCATION</Title>
            <Type>IP</Type>
            <Sort asc="true">2</Sort>
            <Width>183</Width>
            <Alignment>Left</Alignment>
            <Visible>yes</Visible>
        </Column>
        <Column>
            <Source>a.ALERT_COUNT</Source>
            <Title>COLUMN_COUNT</Title>
            <Width>145</Width>
            <Alignment>Left</Alignment>
            <Visible>yes</Visible>
        </Column>
    </Columns>
</Query>
```

This file will generate SQL query to update UI alerts table:

```
SELECT a.ALERT_REPORT_ID, a.ALERT_START, a.ALERT_REPORT_ID,
a.OBSERVER_NAME, a.OBSERVER_LOCATION, a.ALERT_COUNT FROM emerald_report
a ORDER BY a.ALERT_START DESC, a.OBSERVER_LOCATION ASC
```

## 8.3 DetailsPanel.xml

| *Node* | *Description* | *Usage* |
|---|---|---|
| ***Query*** | Root node | |
| ***IdSource*** | Contains database column with unique Id for the selected row. *Note: unlike TOC Alerts table, this query will bring up only one row with given Id.* | Will be passed to queriy to get detail information about selected row. Mandatory element. |
| ***From*** | Contains list of tables with possible aliases (FROM SQL clause). | Mandatory element. |
| ***Where*** | May include part of WHERE SQL clause. | Optional element. |
| ***Columns*** | Root for collection of query columns. | Mandatory element. |
| ***Column*** | Single column description (for both SQL query column and UI table column). *Note: unlike TOC Alerts table, every column in this query will be placed in a* ***row*** *of UI table.* | At least one Column must be present. |
| ***Source*** | Database source for this column. May include single table's column name or expression. | Mandatory element. |
| ***Title*** | UI table's column title. *Important: this is not a text, but Id of localized text stored in properties file.* | Mandatory element. |
| ***Type*** | Column's data type. Currently supported types:<br>• TEXT: for text and numerical<br>• DATE: for date (to be formatted).<br>• IP: for IP addresses (may be resolved to host names). | Mandatory element. List of supported types may be changed or extended in the future. |
| ***Format*** | Used for type DATE only. Contains reference to date format string as defined in java.text.SimpleDateFormat class. *Important :this is Id of localized format string stored in properties file.* | Mandatory element for type DATE. |

Example: given XML file:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Query>
```

```
  <IdSource>a.ALERT_REPORT_ID</IdSource>
  <From>emerald_report a</From>
  <Where>a.ALERT_REPORT_ID=?</Where>
- <Columns>
- <Column>
  <Source>a.ALERT_START</Source>
  <Title>DETAIL_START</Title>
  <Type>DATE</Type>
  <Format>COLUMN_DATE_FORMAT</Format>
  </Column>
- <Column>
  <Source>a.ALERT_END</Source>
  <Title>DETAIL_END</Title>
  <Type>DATE</Type>
  <Format>COLUMN_DATE_FORMAT</Format>
  </Column>
- <Column>
  <Source>a.OUTCOME_GENERIC</Source>
  <Title>DETAIL_SEVERITY</Title>
  </Column>
- <Column>
  <Source>a.ALERT_COUNT</Source>
  <Title>DETAIL_COUNT</Title>
  </Column>
- <Column>
  <Source>a.INCIDENT_CLASS</Source>
  <Title>DETAIL_CLASS</Title>
  </Column>
  </Columns>
  </Query>
```

This file will generate SQL query to update UI details table:

```
SELECT a.ALERT_REPORT_ID, a.ALERT_START, a.ALERT_END, a.OUTCOME_GENERIC,
a.ALERT_COUNT,    a.INCIDENT_CLASS    FROM    emerald_report    a    WHERE
a.ALERT_REPORT_ID=?
```

## 8.4 NotesPanel.xml

| *Node* | *Description* | *Usage* |
|---|---|---|
| ***Query*** | Root node | |
| ***Select*** | Contains SQL query to select note's text for given unique Id. Must provide one query parameter for Id. | Mandatory element. |
| ***Update*** | Contains SQL query to update note's text for given unique Id. Must provide two query parameters: for new text and for Id. | Mandatory element. |

Example XML file:

```
   <?xml version="1.0" encoding="UTF-8" ?>
- <Query>
  <Select>select INCIDENT_DESCRIPTION from emerald_report where
ALERT_REPORT_ID=?</Select>
  <Update>update emerald_report set INCIDENT_DESCRIPTION=? where
ALERT_REPORT_ID=?</Update>
  </Query>
```

## 8.5 Folders.xml

| *Node* | *Description* | *Usage* |
|---|---|---|
| ***Folders*** | Root node for collection of Folder nodes. | |
| ***Folder*** | Single Folder description. | At least one system Folder (Inbox) must be present. |
| ***Name*** | Folder's name to be used in UI panel. *Note: this name is typed by the user, so it is not localized*. | Mandatory element. |
| ***Type*** | Folder's type (integer). Currently supported:<br>• 1 – Inbox<br>• 10 – Custom (user created). | Mandatory element. |

| | | |
|---|---|---|
| ***Where*** | Part of SQL query, will be added to WHERE clause to select alerts belonging to this folder. | Mandatory element. |

Example XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Folders>
   <Folder>
      <Name>Inbox</Name>
      <Type>1</Type>
      <Where/>
   </Folder>
   <Folder>
      <Name>WEB</Name>
      <Type>10</Type>
      <Where>a.OBSERVER_NAME='eXpert-TCP'</Where>
   </Folder>
   <Folder>
      <Name>Priv Attacks</Name>
      <Type>10</Type>
      <Where>a.OBSERVER_LOCATION='pooh.emerald.sri.com'</Where>
   </Folder>
   <Folder>
      <Name>Dos</Name>
      <Type>10</Type>
      <Where>a.ALERT_COUNT &gt; 1</Where>
   </Folder>
</Folders>
```

## 8.6 System.xml

| *Node* | *Description* | *Usage* |
|---|---|---|
| ***System*** | Root node. | |
| ***Locales*** | Collection of Locale nodes supported by application | |

| | | |
|---|---|---|
| | application. | |
| ***Locale*** | Describes one supported Locale. Has no value and two attributes: Language and Country (see java.util.Locale documentation for details*). Note: each supported locale must have corresponding localized properties file. Property files must be located in* ***res*** *sub-directory relative to ApplicationFrame.class file. Property files may be placed in JAR file along with CLASS files. If some property is not found, default property from English-US locale will be used.* | At least one Locale must be present. |

Example XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<System>
   <Locales>
      <Locale Language="en" Country="US"/>
      <Locale Language="de" Country="DE"/>
      <Locale Language="fr" Country="FR"/>
   </Locales>
</System>
```

# 9 Internationalization

The following files contain localized text for the EMERALD AMI. These files are located in the installed directory under com/sri/intruder/ui/res.

Emerald.properties: Text for AMI controls, menu items, dialogs, alerts, table items, etc.

us_attack_long.properties: Text for translating numeric attack signatures in details panel.

us_attack_short.properties: Text for translating numeric attack signatures in alert panel.

us_incident_long.properties: Text for translating numeric incident class in details panel.

us_incident_short.properties: Text for translating numeric incident class in alert panel.

us_outcome.properties: Text for translating numeric outcome in details and alert panel.

us_SensorText.properties: Text for translating sensor status values in sensor window.

## To create a localized version of a property file (4 steps):

- Make a copy of an existing properties file.
- Modify the new file name by appending an underscore and the localized prefix (i.e. Emerald_de.properties and us_attack_long_de.properties for German).
- Localize the text (on the right side of the equal sign) in the new file.

Example: the English version of the Edit Menu is

MEDIT_EDIT=Edit
MEDIT_SET_READ=Set Read
MEDIT_SET_UNREAD=Set UnRead
MEDIT_LOCK=Set Lock
MEDIT_UNLOCK=Set Unlock
MEDIT_RESTORE=Restore from Trash
MEDIT_DELETE=Move to Trash

Example: what the German version of the Edit Menu might be

MEDIT_EDIT=Bearbeiten
MEDIT_SET_READ=Stellen Gelesen
MEDIT_SET_UNREAD=Stellen UnGelesen
MEDIT_LOCK=Stellen Sperre
MEDIT_UNLOCK=Stellen UnSperre
MEDIT_RESTORE= Restaurieren von Abfalleimer
MEDIT_DELETE=Beweigen zu Abfalleimer

- If this is a new country, modify Locales.xml in the com/config directory.

  This file contains one entry for each localized country.

  These entries appear in the Appearance panel of the Settings dialog.

# 10 Version Status

EMERALD Alert Management Interface, Version 1.3, June 2001. See the EMERALD software distribution web page http://www.sdl.sri.com/emerald/releases for further information regarding our follow-on release that will precede the expiration of this release.