IRISnGEN® v7 User Guide



© 2006 Teltronics, Inc. All rights reserved.

IRISnGEN® v7 User Guide

This document is the copyright of Teltronics, Inc. and is intended for exclusive use of Teltronics customers. All rights reserved. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. NO part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Teltronics, Inc.

The material in this document has been carefully reviewed; however, Teltronics, Inc. does not guarantee it to be free of all errors or omissions and reserves the right to make corrections, changes, updates, or revisions to the information contained herein.

IRISnGEN, IRISnGEN Traffic System, Site Event Buffer, SEB, Site Event Buffer Enterprise Agent, SEBea, Site Event Buffer II, SEB II, NET-PATH, NET-PATHm, and NET-PATH Plus are all trademarks of Teltronics, Inc.

Other than those held by Teltronics, Inc., any other brand or product names referenced in this guide are trademarks or registered trademarks of their respective holders and are used here for informational purposes only.

Teltronics, Inc.
2150 Whitfield Industrial Way
Sarasota, Florida 34243-4046 USA

Visit our web site at www.teltronics.com

Part Number: 610-0000-0493 Rev. G (Jan/07)

Table of Contents

Preface

Overview of IRISnGEN ..... i-xii
The IRISnGEN Architecture ..... i-xii
Extended Hierarchy ..... i-xiv

Getting Started

IRISnGEN Main Window 1-1
Shortcut Bar 1-3
Tree View Pane 1-4
- Expanding the Hierarchy Structure 1-5
- Tree Order 1-5

Navigating the Tree View 1-5
- Using the Tree View Menus 1-6
- Creating Shortcuts for Tree View Objects 1-7

Edit Pane 1-7
- Data Tables 1-7
- Editing Data in the Edit Pane 1-7
- Validating and Saving Data in the Edit Pane 1-8

Menu Bar 1-8
Toolbar 1-8
Mass Edit 1-10
Using the Navigator Tool 1-12
Navigation Bar 1-13
Database Command Buttons 1-14
- Clear 1-14
- Retrieve 1-14
- Copy 1-14
- Accept 1-14
- Delete 1-15
- Close 1-15

Customers, Sites, Hosts, and Remote Agents

Overview 2-1
Customers 2-1
- User Fields Tab 2-5
- Filters and Forwarding Tab 2-7
- Comments Tab 2-10
- Contacts Tab 2-11

Site 2-12
- Time Zone & Daylight Saving Tab 2-14

Host 2-15
- Host-Equipment Tab 2-17
- Polling Tab 2-19
- Thresholds and Correlations Tab 2-20
- SNMP Settings Tab 2-21
- Users Tab 2-22



SEBea/ NET-PATH Remote Agent Tab 2-23
SEBea/NET-PATH Database Utilities 2-27
Telnet Download Utility 2-28
Communicating with the remote agent via Telnet 2-30
SNMP Download Utility 2-30
Devices & Hosts Tab 2-32
Editing the Network Properties dialog 2-33
Establishing access to the remote subnet 2-35
Editing the Modem Properties dialog 2-37
Enhanced Action Delivery Tab 2-38
Layouts Tab 2-39
Last Status Tab 2-40
SEB II Remote Agent Tab 2-41
Foreign Remote Agent Tab 2-44

IRIS Administration

Overview 3-1
Alarm Colors 3-1
Communications 3-2
Communication Operations 3-2
Modem Types 3-3
Port Groups 3-4
Ports 3-7
Day/Night Forward Selectors 3-9
Day/Night Mode 3-10
Enhanced Authentication 3-10
Importing System and Security Tokens 3-11
Deleting System and Security Tokens 3-14
Enabling Enhanced Authentication in the Remote Agent 3-15
Assigning a Security Token to a Remote Agent User 3-16
Unlocking a Security Token 3-17
Remote Agent Access 3-17
Remote Agent User Access 3-18
Non-Protocol Access 3-18
Multiple Challenge Response 3-19
Protocol Access 3-20
Scheduler Access 3-20
Network Downloads 3-20
PPP Connections Using Enhanced Authentication 3-20
Processing Applications 3-23
System Parameters 3-24
User Defined Fields 3-24
Defining Values of User-Defined Fields 3-26
User Groups 3-26
Users 3-27
Zip Codes 3-28

IRIS Tools

Active Forward Selectors 4-1
Inserting Forward Selectors 4-2
Active Timed Filters 4-3
Inserting New Active Timed Filters 4-4
Alarm Report Queue 4-5
Generating Alarm Reports Manually 4-8



Automated Site Management 4-9
Selector Tab 4-9
Selector Results Tab 4-12
Bad Data 4-15
Viewing Bad Data 4-15
Resubmit Bad Data for Processing 4-18
Bad Data Detail 4-19
Bad Data Events List 4-20
Communication Queue 4-22
Communication Queue Detail 4-24
Deleted Alarms 4-27
Poll Schedule 4-28
Reports 4-29
Alarm Report Schedules 4-29
Alarm Report Selectors 4-30
Alarm Report Sets 4-33
Alarm Reports 4-34
Report Target Set 4-35
Traffic Report 4-36
Traffic Report Schedule 4-37
Traffic Report Selectors 4-38
Traffic Report Sets 4-40
Traffic Reports 4-41
Custom Reports 4-42
Traffic Report Formats 4-42
Scheduled Forward Selectors 4-43
Scheduled Timed Filters 4-44
Traffic Report Queue 4-45

IRISnGEN Libraries

Alarms 5-1
Correlations 5-2
Inter Host Correlations 5-2
Single Host Correlation 5-3
....5-4
Passing event variables to triggered events 5-4
Escalation Groups 5-7
Filters 5-9
Filter Actions 5-9
Filter Schedules 5-10
Filter Sets 5-11
Keyword Filter Sets 5-12
Regular Expression Filter Sets 5-13
Regular Expression Characters 5-14
Severity Filter Sets 5-17
String Filter Sets 5-18
Forwarding 5-19
Email 5-20
Faxes 5-21
Forward Schedules 5-22
Forward Selectors 5-23
Forward Sets 5-24
Pagers/Pager Services 5-26
Creating and Editing Pager Records 5-27



Print 5-28
SNMP Targets 5-29
SNMP Viewer Monitoring 5-31
Sending a test trap 5-32
Messages 5-33
Keyword Templates 5-34
Message Libraries 5-36
Creating and Editing Message Library Alarm Entries 5-37
Special 5-38
Superscripts 5-38
Thresholds 5-40
Stage 1 (Before Minimum Reached) 5-40
Stage 2 (Between Minimum and Maximum) 5-40
Stage 3 (After Maximum Reached) 5-41
Contact 5-42
Contact Types 5-42
Contacts 5-43
Assigning Contacts 5-45
Adding Comments 5-46
Equipment Libraries 5-46
Equipment 5-47
Deleting an Equipment Record 5-48
Duplicating an Equipment Record 5-49
Where Used 5-50
Equipment Actions 5-50
Deleting an Equipment Action Record 5-51
Duplicating an Equipment Action Record. 5-52
Equipment Icons 5-52
Deleting an Icon Record 5-53
Duplicating an Icon Record 5-53
Where Used 5-54
Equipment Types 5-54
Deleting an Equipment Type Record 5-55
Duplicating an Equipment Type Record 5-56
Where Used 5-57
Multi Media 5-57
Extended Hierarchy 5-59
Inserting and Renaming Nodes 5-60
Deleting Nodes and Objects 5-61
Attaching Objects 5-61
Adding and Deleting Contacts for Hierarchies 5-62
Dragging and Dropping Nodes and Objects 5-62
Moving several items within a hierarchy 5-63
Cutting and Pasting Nodes and Objects 5-64
Duplicating Hierarchies 5-64
Holidays 5-65
Host Types 5-65
Remote Agent Type 5-67
Dialout Override 5-68



Remote Agent Libraries

Overview 6-1
Device Libraries 6-2
Battery Device Library 6-3
Contact Device Library 6-4
DC Voltage Device Library 6-5
Memory Device Library 6-8
Modem Device Library 6-9
The Caller ID tab 6-12
Network Device Library 6-14
Power Device Library 6-16
Commercial Power Lost - Controlled Shut Down 6-16
Commercial Power Lost - Abnormal Power Down 6-17
Relay Device Library 6-17
Serial Port Device Library 6-19
System Device Library 6-23
Temperature Device Library 6-24
User Interface Device Library 6-25
Event Libraries Menu 6-27
Action Libraries 6-28
Buzzer Action Tab 6-29
Fax Action 6-30
Fax Device Connection Tab 6-31
LCD Action 6-33
LED Action Tab 6-34
Pager Action 6-35
Pager Device Connection Tab 6-36
Relay Action 6-38
Report Action 6-40
Report Action Device Connection Tab 6-41
Script Action 6-43
SNMP Action 6-44
SNMP Device Connection 6-47
Store Action 6-48
Terminal Action 6-49
Triggered Event Action 6-50
Action Group 6-51
Action Window Libraries 6-52
Action Window 6-52
Time Zone and Daylight Saving 6-54
Correlation Libraries 6-55
Correlation Tab 6-56
Correlation Actions 6-58
Correlation Groups 6-59
Event Detection Libraries 6-60
Record Definition 6-61
Pre-Processing 6-70
Post- Processing 6-72
Event Detection Groups 6-73
Event Matches 6-74
Event Match (Data) Tab 6-74
Trigger Words Tab 6-76
Sample Trigger Words 6-77



Variable Extraction Table 6-77
Event Match (SNMP) Tab..... 6-80
Event Match (Fixed) Tab 6-83
Event Match Group 6-84
Expect 6-85
Expect Groups 6-86
File Types 6-87
Filter 6-88
Filter Groups 6-89
Fixed Event 6-90
Fixed Event Groups 6-91
Holiday Libraries 6-92
Layouts 6-93
More About Layouts 6-97
Polling Layouts 6-97
Report Layouts 6-97
SEBII Protocol Layouts 6-97
Layout Groups 6-97
Script 6-98
Script Groups 6-99
SNMP Layouts 6-99
Tasks 6-100
Task Groups 6-102
Threshold 6-103
Threshold Action 6-106
Threshold Group 6-107
Host Libraries 6-108
Event Matches Tab 6-109
Host Library Group 6-110
Model Libraries 6-111
Security Libraries 6-112
Remote Agent Passwords 6-112
Access Groups 6-113
Adding Commands to the Data Table 6-115
Users 6-116
User Groups 6-118
Security Assignments 6-118
Template Libraries 6-120

Remote Agent Manager

Accessing Remote Agent Manager 7-1
Tree View 7-3
Displaying and Hiding the Tree View Pane 7-3
Task Detail Pane 7-4
History Detail Pane 7-4
Status Bar 7-5
Remote Agent Manager lists 7-5
Remote Agent Manager Active Toolbar 7-6
Remote Agent Manager Toolbar 7-6
SEBea/NET-PATH Toolbar 7-6
SEB II Toolbar 7-7
Foreign Agent Toolbar 7-7
Port Select 7-7
Connecting/Disconnecting from the Remote Agent 7-7



SEBea/NET-PATH Remote Agent Manager Functions 7-8
Effective Information 7-8
Get Status 7-9
Expanding and Collapsing the Status Fields 7-9
Polling 7-10
Transparency 7-13
SEBea/NET-PATHSEBea/NET-PATH Normal Transparency 7-14
Host Normal Transparency 7-14
Passive Transparency 7-14
Active Bridge Transparency 7-15
Override Terminal Type 7-16
Using Command Line Interface Commands 7-16
Transparency Window Toolbar 7-17
Ending transparency 7-17
Opening a file 7-17
Capturing to a Log File 7-18
Copying and Pasting Text 7-18
Sending Host Login Information 7-19
Sending Host Password 7-19
Sending Break 7-19
Turning on Local Echo 7-19
Viewing Transparency Status 7-20
Send Database 7-20
Send Application 7-22
Send Database and Application 7-23
Send Operating System 7-23
Send Loader 7-24
Send Date and Time 7-25
Get and View Database 7-26
Send and Retrieve Files 7-26
Lock and Unlock the Remote Agent 7-28
SEB II Remote Agent Manager Functions 7-28
Edit Remote Agent Database 7-28
Effective Information 7-29
Get Status 7-30
Remote Agent Status: General Tab 7-30
Remote Agent Status: Port Tab 7-32
Remote Agent Status: Miscellaneous Tab 7-33
Polling 7-35
Polling Password Options 7-36
Transparency 7-37
Going Transparent with a Host Device 7-39
Get Database 7-39
Save As Dialog 7-40
Edit Dialog 7-41
Used Dialog 7-41
View Dialog 7-41
Send Database and ASP 7-42
Remote Agent Send Database and ASP Dialog 7-43
Send Date and Time 7-43
Foreign Agent Remote Agent Manager Functions 7-44
Effective Information 7-44
Transparency 7-45
Going Transparent with a Host Device 7-45



SEB II Database Manager

Trigger Words Table (TW) 8-4
Trigger Sequences (TS) 8-6
Trigger Messages Table (TM) 8-9
Fixed Event Table (FE) 8-10
Fixed Event Sequence Table (FS) 8-13
Fixed Message Table (FM) 8-16
Action Window Table (AW) 8-17
Phone Number Table (PN) 8-18
Port Parameters Table (PP) 8-20
System Parameters Table (SP) 8-22
Compression Translation Table (CT) 8-25
Security Table (SE) 8-26
External Modem (EM) 8-28

Monitoring Data

List Viewer 9-2
Configuration 9-3
- Selectivity 9-3
- Refresh Time 9-5
- Speed Buttons 9-5
- Grid Lines Horizontal/Vertical 9-5
- Save Setting 9-6
- Exit 9-6

Alarm 9-6
- Alarm Status Open/Closed 9-6
- View Detail 9-7
- View Attachment 9-8
- Forward Alarms 9-8
- Choosing a Format When Forwarding Alarms via E-mail 9-9
- Changing the E-mail Subject Line Text for Forwarded Alarms . 9-9
- Selecting a Style for HTML Alarm Reports 9-10
- Escalate Alarms 9-10
- Dispatch Alarms 9-11
- Adding Comments to Alarms 9-11
- Ticket Alarms 9-11
- Export Alarms 9-12
- Remove Alarms 9-12
- Ignore Alarms 9-12
- Access List Viewer History 9-14
- Go Transparent 9-14

Batch Status 9-15
History Viewer 9-17
Customizing the History Viewer Display 9-19
Add a New Alarm 9-19
View Menu 9-20
- Server Time 9-20

Toolbar, Status Bar, Shortcut Bar 9-20
Map Viewer 9-21
Map Viewer Window 9-23
- Using Equipment Explorer with Map Viewer 9-24

Map Viewer Pop-up Menu 9-25
Address Lookup 9-26



Map Selectivity 9-27
Map Settings 9-31
Equipment Explorer 9-32
Launching Equipment Explorer 9-32
Using Navigation Buttons 9-32
Changing Equipment Explorer Selectivity 9-33
Programming Equipment Explorer Settings 9-35
Changing Modes 9-36
Sample Mode Views 9-36
Displaying Several View Windows at Once 9-37
Site View 9-37
Changing Selectivity 9-38
Changing Settings 9-38
Equipment View 9-39
Detail View 9-40
Get Status 9-41
Event View 9-41
Action View 9-43
History View 9-44
Remote Agent View 9-45
Icons and Colors 9-47
Event List Viewer 9-47
Event History Viewer 9-48

Polling

SEBea and NET-PATH 10-1
BeforeYou Begin Polling the SEBea or NET-PATH 10-1
File Types 10-2
Store Actions 10-2
Layouts 10-3
Users 10-4
Access Groups 10-5
Polling Methods for SEBea and NET-PATH 10-6
Manual Polling SEBea and NET-PATH 10-6
Scheduled Polling SEBea and NET-PATH 10-6
Command Line Polling SEBea and NET-PATH 10-6
Using the NDPOLL Command 10-7
Using the DPOLL Command 10-7
Remote Agent Manager Polling SEBea and NET-PATH 10-7
SEB II 10-12
Polling Password Options 10-13
Manual Poll 10-14
SEBea and NET-PATH Polling - Quick Setup 10-14
Security Setup (for command line polling, only) 10-14
Host setup 10-15
Remote Agent Setup 10-15
Storage Setup 10-15
Manual Polling (not RA Manager) 10-15
Troubleshooting Tips 10-16

Generic Output

Overview 11-1
Implementation 11-1
Generic output fields from Export table 11-2



Program Parameters 11-3
Configuration File 11-3
Configuration File Examples 11-4
BOR and EOR Configuration 11-5
Output Directory 11-6

Index



Preface

Teltronics Inc. designed its Remote Maintenance product line so that you, the service provider, can offer best-in-class maintenance services to your customers. Whether your customers are internal to your company or represent thousands of different companies, the Remote Maintenance product line lets you run your maintenance business the way you want.

A Remote Maintenance system consists of four major components: a management information system at a central location, a remote monitoring device, the Public Switched Telephone Network, and the Multi-Drop Alarm Delivery and Control System.

- Management information system at your maintenance center—The IRISnGEN® system is our foremost events management software. The IRISnGEN system collects fault and performance data from thousands of remote customers and manages this information in an efficient and customer-responsive way. With the IRISnGEN system, you have a system you can tailor to the way you run your business. We do not force you to mold your business to fit our product, rather our flexible product adapts to your way of doing business. The IRISnGEN system lets you build a database that reflects your customer's organization. All the information you need about your customer, the customer equipment, received events, and what to do about them, is only a mouse-click away.
- Remote agent devices—The Site Event Buffer Enterprise Agent® (SEBea®), Site Event Buffer-II® (SEB II®), NET-PATH®, and NET-PATHm™ monitors your customer's telecom, computer, and office automation products for faults and events that reflect the health and performance of these mission-critical systems. In this document, we refer to these monitored systems as remote agents. The configurable remote agent is a powerful tool that lets you offer monitoring and maintenance services for all of your customer equipment.
- Public Switched Telephone Network—the most connected and reliable network in the world. When you are dealing with thousands of customers scattered across continents, the PSTN is the only real choice for getting maintenance information from the hosts to the maintenance center. IRISnGEN and the remote agent use the potential of this network to its fullest to ensure reliable, error-free data communication.
- Multi-Drop Alarm Delivery and Control System—Customers can monitor and control equipment at several sites distributed throughout their data network. The sites connect to IRISnGEN via a fiber optic loop and several radio links (remote sites). SEBea remote agents located at the various sites can gather information from such devices as telemetry units already situated at these sites. The SEBea remote agents connect to IRISnGEN using a half-duplex multi-drop network. The Multi-Drop System incorporates all the functions of IRISnGEN and SEBea remote agents, including downloads, transparency, and polling, are available via modems or through a network. The Multi-Drop Alarm Delivery and Control System is only available to customers licensed to use the Multi-Drop application.



Overview of IRISnGEN

The IRISnGEN system provides enhanced service and maintenance capabilities by automatically collecting and analyzing event information. IRISnGEN does this using software modules, special remote agent devices, easy-to-use relational databases, and event message libraries. You can use the IRISnGEN system to notify you automatically when it detects critical event conditions in a host data stream. They use this system to retrieve minor event messages stored in your remote agent using a process known as polling. You can also use IRISnGEN to monitor and control equipment located throughout your network.

Remote agents can detect events and status-changes generated by the host equipment attached to the remote agent's contact sensors and control ports, and then deliver these events to the IRISnGEN system. The IRISnGEN system acknowledges the event, identifies the calling site, and stores the event information in a database. The event-processing engine retrieves the event and compares the data to user-defined filter information associated with the host equipment that generated the event. The IRISnGEN system compares them to threshold boundaries. Based on the comparison, the IRISnGEN system takes action, such as sending the event to a text or graphical viewer, storing or reporting an event, or issuing an action command (for Multi-Drop users), such as checking fuel levels in storage tanks, or changing channels on a radio.

The IRISnGEN system compares the event text to a message library, applies plain-English translations, and determines the event's severity. It then displays the event on a View window or the Map Viewer (for Multi-Drop users) showing a geographical view of all the customer's sites. From a View window, technicians can immediately access all information about the alarm event, the customer's equipment and contacts, and what corrective action to take. From a View window, or Map Viewer, a single keystroke invokes a connection to the equipment host for further problem analysis and troubleshooting.

Other actions the IRISnGEN system can take: storing the event in a history file, deleting, e-mailing, faxing, or printing it, or sending the event to pagers. The IRISnGEN system can also forward events and collect data from your legacy back-office systems, further integrating events management with your business.

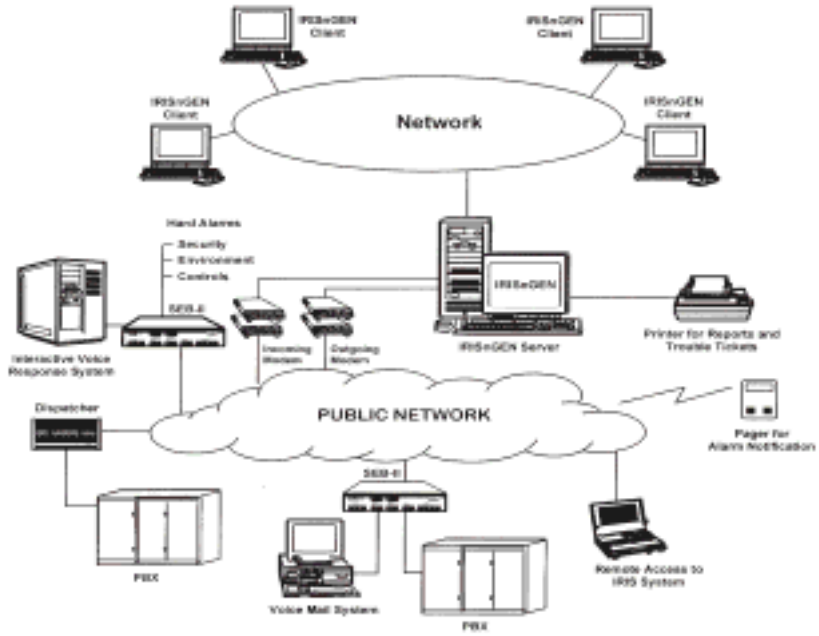
The IRISnGEN system performs event correlation and supports event escalation. Event correlation, which checks for the occurrence of multiple events within a defined time, reduces the number of nuisance events, thus making your technicians more efficient. Events that occur and clear before they become real problems can be routed to a history file, bypassing the Viewer. Event escalation ensures that no critical event ever goes unresolved. You can configure the IRISnGEN system for a variety of escalation scenarios based on the customer, site, severity, or status (new, open, and closed). For example, critical events not addressed in ten minutes may alert a supervisor at another viewer. When the problem remains unresolved for thirty minutes, the system can fax or email events from a critical-care customer to the customer's site. The combinations are almost limitless.

The IRISnGEN Architecture

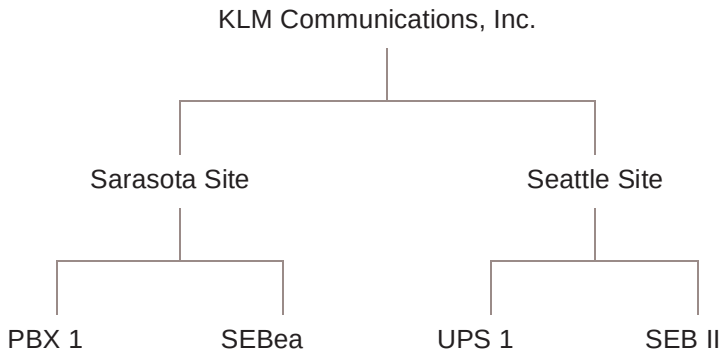
The IRISnGEN system is a client-server application suite that operates with Windows NT Server and the Microsoft SQL Server database engine. It is a multi-tasking, multi-user system capable of supporting thousands of monitoring devices, millions of events, and hundreds of client connections. All of the benefits of a Windows NT operating system are available, such as system back-ups, RAID, NTFS security, and Microsoft Outlook Client. The system architecture is modular and flexible to accommodate modifications or the addition of new features as required by the marketplace. The number of remote monitored sites supported by the IRISnGEN system is limited only by hardware capacity and throughput considerations. You can access the IRISnGEN system via the customer's LAN, dial-in access, and via Internet and Intranet using standard web browsers. The IRISnGEN client application operates on personal computers running Windows 98, 2000, XP, or NT



Workstation. These client PCs gain access to the IRISnGEN server via a network connection.



The IRISnGEN database is a three-tiered hierarchy structure defining customers, sites belonging to customers, and all host devices belonging to sites. Host devices are further defined as hosts and remote agents that monitor the hosts. For example, the SEBea and SEB II remote agents monitor host devices, such as PBXs, UPS systems, and data networks, to name a few.



Sample Hierarchy

You can build the customer database from the top down. That is, you first create a customer record, then add a site record that references the customer record, and then add a remote agent record that references a site record. Finally you create a host record that references a remote agent and site record.

You can configure each node of the customer hierarchy to streamline database entry. For example, you can create an alarm filter set and message library for a given host type, such as a specific PBX. You can then assign these two tables to the PBX host type record, rather than to each host record. If you have hundreds of sites for a given host type, you can maintain just two tables to support all of these sites.

Extended Hierarchy

If your business requires a more complex database structure than the standard database for an IRISnGEN system, you can define your own hierarchy with the Extended Hierarchy function. Extended Hierarchy lets you create unlimited logical groupings of customers, sites, or host types that conform to your organizational structure and how you run your business. For more information, see “Extended Hierarchy” on page 5-59.



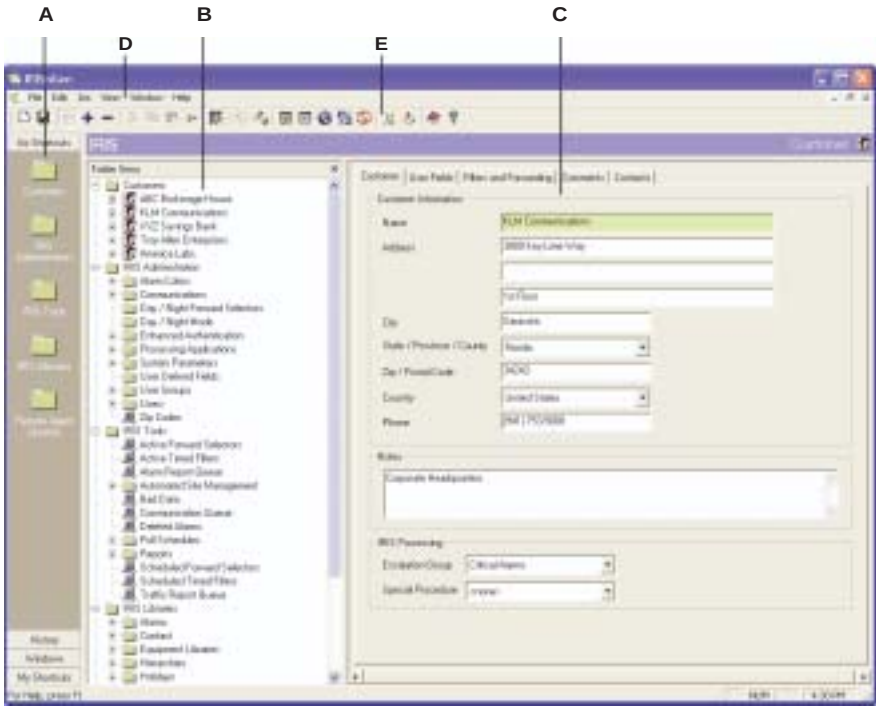
1

Getting Started

If you are new to IRISnGEN, this chapter is an important one to read. It explains the basic skills you need to work with IRISnGEN. You may want to return to this chapter often as a reference. It provides the information you need to manage your applications and files easily and efficiently.

IRISnGEN Main Window

The main IRISnGEN window has three panes, a toolbar, and a menu bar. The left pane is the shortcut bar. Use it to store system standards and user-defined shortcuts. The second pane is a tree view, similar to the folder system in Outlook. The tree shows the IRISnGEN database structure and its related elements in the database. The third pane is the Edit Pane. It displays data that you can format in several ways depending on the item selected from the tree. Other standard Windows elements, such as toolbars, menus, accelerator keys, keyboard and mouse navigation, and left and right mouse button clicking are also used.



A The *Shortcut Bar* lets you quickly open the files and folders you use most often.
B The *Tree View* pane displays the IRISnGEN database hierarchy. You can select folders and files from the tree view to edit the database.
C The *Edit* pane displays the file data that you can configure and save in your IRISnGEN database.
D The *menu bar* displays a list of options you can choose within IRISnGEN.
E The *tool bar* gives quick access to IRISnGEN features.

IRISnGEN Main Window

Shortcut Bar

The shortcut bar displays at the far left of the IRISnGEN window. It contains icons that represent system-defined and user-defined shortcuts to the files and folders displayed in the tree view and edit windows. A shortcut is a quick way to open a frequently used file or folder without searching for its installed location. Selecting the shortcut bar icon shifts the current tree to the icon's defined position and triggers all actions that occur when you click on its target location.



The shortcut bar contains four views:

- **Iris Shortcuts** displays the five root folders in the tree view.
- **History** displays all the folders and files accessed since you logged into IRISnGEN.
- **Windows** displays a list of all the files and folders currently in use.
- **My Shortcuts** displays a list of all shortcuts you created for yourself. The icons displayed in this view remain and display each time you log into IRISnGEN.

Click any of the views to display the list for that view.

To add your own shortcut

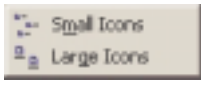
Do one of the following:

- Click any item in the tree view and drag it to the My Shortcuts area of the shortcut bar.
- Right-click any object in the tree view and then select Create Shortcut from the pop-up menu.

The shortcut appears in the My Shortcuts area of the shortcut bar with the same name as the object you selected in the tree view.

To change the shortcut bar's icon size

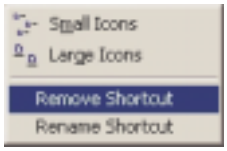
1 Right-click inside the shortcut bar area.



2 Choose either small icons or large icons from the pop-up menu options.

To remove or rename a shortcut

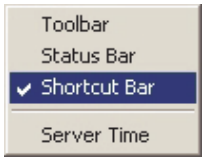
1 Right-click the icon you wish to remove or rename.



2 Select an option from the pop-up menu options.

To display or hide the shortcut bar

- Choose **View** > **Shortcut Bar**.

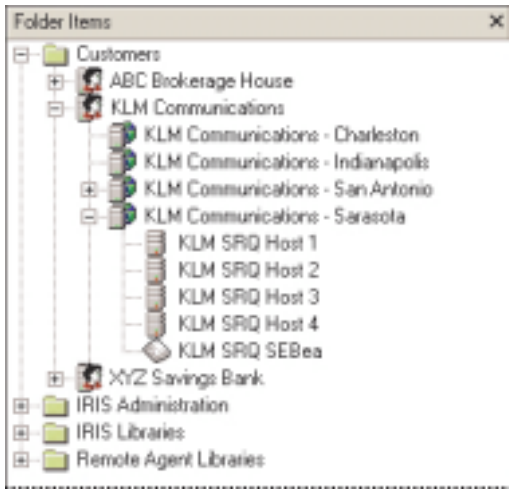


A checkmark appears beside the menu item, indicating the shortcut bar is active.

- To hide the shortcut bar, clear the Shortcut Bar menu option. The checkmark disappears and the shortcut bar is hidden.

Tree View Pane

The second (center) pane on the IRISnGEN main screen is the Tree View. The Tree View pane displays folders and icons similar to Outlook or the navigation window within Windows Explorer.



The Tree View pane shows the structure of the IRISnGEN hierarchy. The Tree View structure begins at the upper left with the Tree View root, the first folder on the list. Tree View displays four root folders. They include:

- **Customers** display all defined customers in your IRISnGEN system. Each customer folder expands to display the sites assigned to the associated customer. Each site expands to show remote agents that and hosts assigned to the site.
- **IRIS Administration** provides access to the database tables that control most of the server operations, including system parameters, communications, day/night forward selectors, poll schedules, processing applications, users, and user groups.
- **IRIS Libraries** contains all objects that support the event processing definitions for the IRISnGEN server.
- **Remote Agent Libraries** contains the database tables for SEBea remote agents. This is where you configure SEBea settings.

Expanding the Hierarchy Structure

You can control the level of hierarchy information shown in the tree view. Use the commands on the tree menu to expand and collapse the hierarchy shown. When you expand a folder, the names of the sub-folders in that folder display in the tree. You can expand the sub-folders as well.

As you expand each sub-folder, you will see object icons, such as Customers, Hosts, Sites, Modems, and Remote Agent icons. These icons can help you identify the item's category.

To expand and collapse the tree view

- Click ⊞ (plus sign) next to any item in the tree View to expand and display objects under that category.
- Click ⊟ (minus sign) to collapse the tree at that item.

Tree Order

The system software defines folder order. The system displays in alphabetical order those user data elements in the tree. For example, it displays customers, remote agents, and filter sets.

Navigating the Tree View

You can move around the tree view using the keyboard.

Use	To
Up Arrow	Move up the tree one object at a time.
Down Arrow	Move down the tree one object at a time.
Page Up	Move up one full screen.
Page Down	Move down one full screen full.



You can use the following keyboard shortcuts to perform an action.

Use	To
Insert	Add the menu item defined for the right mouse button.
Delete	Delete the menu item defined for the right mouse button.
Ctrl+C	Copy the selected item to the clipboard. You can paste it later.
Ctrl+V	Paste. The following rules apply when using paste. When the pasted item is the same type as the currently selected item (Customer, Filter Set, etc.) the system adds a copy to the tree at the current level, following the rules for adding a new item. When the pasted item is different, the system processes it using built-in drag and drop rules for the selected tree item. For example, when you paste a contact on a customer, the system adds the pasted contact to that customer's contact reference list.
Ctrl+X	Cut. Places the selected item in the clipboard buffer. You can then paste the information elsewhere.

Using the Tree View Menus

You can use the tree view menus and to give IRISnGEN instructions about what you want to do.

A menu displays a list of available commands. Tree view menus display when you right-click objects in the tree view pane. The menu is unique for each object in the system; however most menus include: ADD, DELETE, CUT, COPY, PASTE, and CREATE SHORTCUT.

To display the menu for a tree view object

1. Move the mouse over any tree view object.
2. Click the right mouse button.

To execute a menu command

1. Move the mouse pointer over the menu command you wish execute.
2. Click either mouse button.



Creating Shortcuts for Tree View Objects

A shortcut is a quick and easy way to access an object in the tree view without the need to click on every object in the tree structure. You may wish to create shortcuts to the objects you use most often. The shortcut appears in the My Shortcuts area of the shortcut bar. Clicking the icon for the shortcut opens the object immediately.

To create a shortcut

1. Right-click any object in the tree view. A menu appears.
2. Select **Create Shortcut** from the menu.

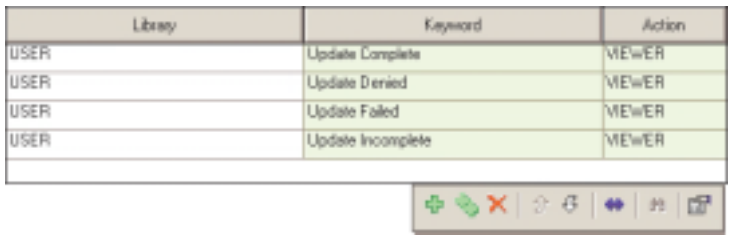
The shortcut appears in the My Shortcuts area of the shortcut bar, using the same name as the object in the tree view.

Edit Pane

The edit pane displays on the far right of the IRISnGEN Window. It displays data that you can configure in several ways, depending on the object you select from the tree. When you select a tree object, the edit pane displays a folder tab view (or property page) logically grouped in a series of separate displays. Simply click a tab to view its attributes. You can also use the keyboard combinations CTRL+TAB, CTRL+PAGE UP, AND CTRL+PAGE DOWN) to switch between tabs.

Data Tables

Data tables appear within the folder tabs that display in the edit pane. Data tables list multiple items in table format (rows and columns). Each column in a data table may be an edit box, list, radio button, checkbox, or duration control. The following shows an example of a data table.



Add or delete entries in the data table using the keyboard or the mini toolbar (shown below) located in the bottom-right of the data table. The toolbar becomes available as soon as you click inside any data table.

Editing Data in the Edit Pane

You must have permission rights to edit objects that display in the Edit Pane. If you experience difficulty editing, contact your system administrator.

When you have permission to do so, standard Windows editing keys are available for all editors. You can copy (Ctrl +C) and paste (Ctrl+V) between fields, and standard keyboard shortcuts for display elements are available. For example, pressing the Tab key moves your cursor to the next field.

Hold down the Control key and click the Object Viewer on the toolbar in any data window to display a selection list. The List choices vary depending on the content of the data table you view. Common selections include Folder and Name. Select Folder to navigate to the folder containing the highlighted object in the current data table. Select Name to navigate to the specific item. When you select Name, the result is the same as if you use Object Viewer to select a single item in the data table.

Validating and Saving Data in the Edit Pane

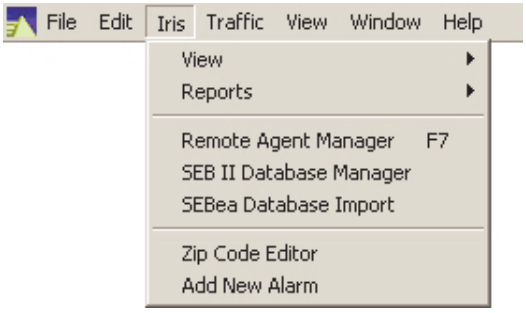
The Save icon ( ) appears shaded until you have pending changes to the Edit pane. As you make changes, the Save icon becomes active, as does the Revert toolbar button ( ). Click the Revert button to cancel your changes and return the previous display.

When you click on another item in the tree view before saving your work, the prompts you to save your changes before continuing. If any of the required fields are incomplete, the system displays a message in the status bar and the field background highlights. You must correct any incomplete field before you can continue. As you enter the correct data in a field, be sure to click outside that field before saving your record. This will signal IRISnGEN that you are no longer in input mode and will allow you to save your record.

When all required fields are present and the system finds no database validation errors, IRISnGEN saves the data in the its database and updates the status bar with a message indicating success.

Menu Bar

Select command options from the lists listed at the top of the window.



To select a command

- Click a menu from the menu bar, and then click the command.



Note *The options available on each menu may differ depending on the type of remote agent you are using.*

Toolbar

The toolbar icons represent the actions you can apply to elements within the IRISnGEN software. As you select items in the Tree View, the toolbar may change to reflect actions appropriate for the items you selected.

The following diagram shows a typical toolbar.



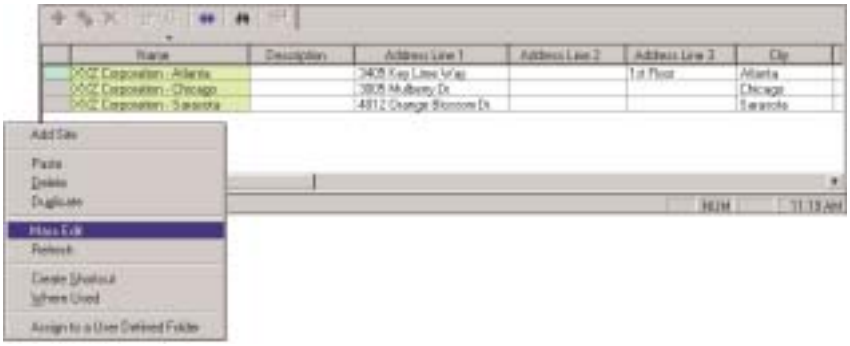
Icon	Name	Keyboard Equivalent	Description
	New	Ctrl + N	Create a new shortcut.
	Save	Ctrl + S	Save the selected item to the database. Messages display in the status bar area.
	Toggle	None	Toggle to display the Shortcut window. The button grays when you toggle to hide the pane.
	Expand	None	Expand the tree view.
	Collapse	None	Collapse the tree view.
	Cut	Ctrl+X	Remove the selected item and place the contents in the clipboard buffer. You can then paste the information elsewhere.
	Copy	Ctrl+C	Copy the selected item into the clipboard buffer. You can then paste the information elsewhere.
	Paste	Ctrl+V	Paste the contents of the clipboard. When the pasted item is the same type as the currently selected item (customer, filter set, etc.) the system adds a copy to the tree at the current level. When the pasted item is different, the system processes it using built-in drag and drop rules for the selected tree item.
	Revert	None	Abandon your changes. The system displays all the original data for the selected item.
	Navigator	None	Display the Navigator screen. Use Navigator to search for a system record. You can then click the result of your search to go directly to the record.
	Remote Agent Manager	None	Display the Remote Agent Manager window. The button appears gray until you select a remote agent device from the tree view pane, or when a host connects to an agent.
	Manage SEB II Databases	None	Display the SEB Database Manager dialog. Use it to retrieve and edit a database. The button appears gray until you select the SEB II remote agent device from the tree view pane.
	List Viewer	None	Display the Alarms List Viewer window.



	History Viewer	None	Display the Alarm History Viewer window.
	Geographical Viewer/Map Viewer	None	Display the Geographical Viewer/ Map Viewer window. Map Viewer is only available for licensed Multi-Drop users.
	Equipment Explorer	None	Display the Equipment Explorer window (for licensed Multi-Drop users, only).
	Bad Data	None	Display the Bad Data query window.
	Communication Queue	None	Display the Communication Queue window.
	Reports Queue	None	Displays the Alarm Reports Queue window.
	Help	None	Display the help system for the IRISnGEN application.
	About	None	Display system information.

Mass Edit

The Mass Edit function lets you view and edit details of multiple objects all at once. You can also search and replace characters. For example, you may need to change a telephone number for a technician in several customer records. When you select the Mass Edit option at the customer folder level, details about all customers in that folder displays in a data table. You can then view or edit the details in the table.



To use Mass Edit

1. Right-click a folder in the tree view.



Note *The Mass Edit menu option is available at most folders that contain other objects. (Examples include the Customers, Communications Operations, Poll Schedules, Modem Types, Port Groups, and User Groups folders).*

2. From the tree view pop-up menu, select Mass Edit.
3. A data table displays details about all objects in the folder you selected.
4. View or Edit the fields displayed in the table.



Note *You cannot add or delete records with Mass Edit. Add or delete records from the tree view using the pop-up menu.*

To search and replace with Mass Edit

1. From the Mass Edit Data Table window, choose the Find and Replace button.
2. A Find and Replace dialog appears. The following describes the fields in the Find and Replace Dialog.

Field	What to Enter
Find What	Enter the characters you wish to find
Replace With	Enter the characters you want to replace the found text.
Search	Choose a search option from the list. Choices are By Rows or By Columns.
Match Case	Select this checkbox to find only words that have the same case as those entered in the Find What field. Do not select this checkbox if you want to find both uppercase and lowercase versions of a word.
Find entire cells only	Select this checkbox to search cells for an exact match of the characters you enter in the Find What field. It will not find cells that contain additional characters.
Search Every Column	Select this checkbox to search every column in the data table for the characters you enter in the Find What field. Do not select this checkbox if you want to search a specific column.

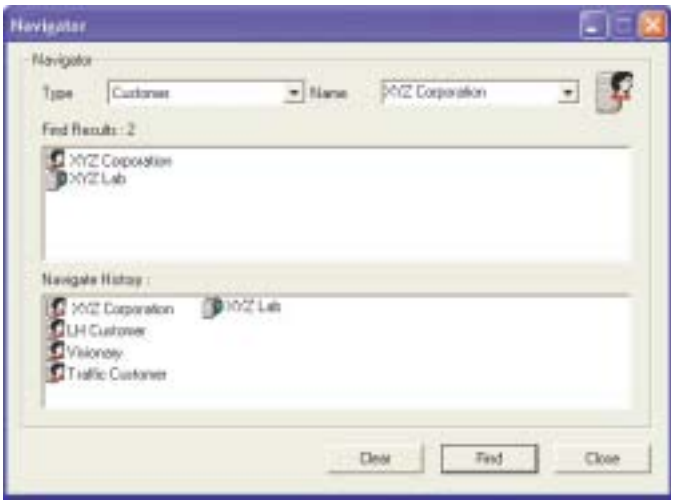
3 When you are satisfied with your search criteria, click the ***Find*** button.
- To replace the highlighted occurrence of the found characters, choose the ***Replace*** button.
- To replace all occurrences of the found characters, choose ***Replace All***.
- Choose ***Close*** to return to the Mass Edit data table.



Note *Replacement text must be a valid entry for the data table field; otherwise, the system will not save your changes.*

Using the Navigator Tool

Use the Navigator toolbar button ( ) to quickly search and find system records or objects. Search for a record type (for example, Customers0; then, select names from list based your type selection. Your search results display in the Find Results field. Click a result to navigate to it.



The following list describes the fields in the Navigator window:

Field	What to Enter
Type	Select an object type from the list.
Name	Select a name from the list for the type you selected.
Find Results	Displays the results of your query when you press the Find button. Click a result displayed in this area to go to that object.
Navigate History	Displays all objects you navigate to during a session. Click on any object in the Navigate History box to return to its location.
Clear	Click the Clear button to empty the Navigate History box.
Find	Click the Find button to begin the search based on the selections you make in the Type and Name fields.
Close	Click the Close button to exit the Navigator window.

Navigation Bar

Some screens feature the navigation bar, shown below. Click a button on the bar to scroll through the records.



From left to right, these buttons perform the following functions:

- go to beginning of the database (first entry)
- go previous entry
- go to next entry
- go to the end of the database (last entry)

To save the changes

1 Click **No** to return to database entry screen.

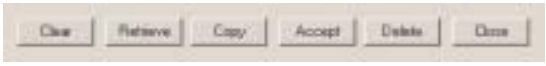
2 Click **Accept**, **Update**, or **Save**. You may now exit as normal.

To abandon your changes

- Click **Yes** to remove the prompt box and to close the database entry screen.

Database Command Buttons

The following command buttons appear on select SEB II windows in the IRISnGEN system that let you view, create, and edit database records.



Clear

Clear all records from cache memory and all the on-screen entry fields. This command only affects the display. It does not change anything in your database. Click **Retrieve** to browse the records after clearing them.

If you have any unsaved changes, the system will prompt you to save them before clearing your data from the screen. If you want to abandon your changes, click Yes. If you want to return and save the changes, click Accept; then, click No.

Retrieve

Retrieve the database records that match your search criteria.

Once your retrieve your records, you can use the navigation bar to move through your records (the navigation bar is unavailable until you click Retrieve). IRISnGEN does not automatically retrieve the records, since very large database retrievals can take a long time. IRISnGEN puts you in control by prompting you want to look at the existing records, or to add new records without retrieving old records.

You can use the various text fields in the dialog box as search fields. If you leave all records in the dialog box blank and click Retrieve, the system retrieves all records in the database.

To retrieve selected records, complete any field on the screen by typing in your selection or, from lists, choose a selection from the menu. Once you have entered your search criteria, click Retrieve. This retrieves only those records that match the information you have entered. You can use the *%* wildcard in the searchable fields. For example, type “N%” in the field and click Retrieve, when you want to display all records in a certain field that start with the letter *N*.



Note *Do not use square brackets as search criteria (for example, [FE01]). To search for an item containing square brackets, use the percent sign in place of the square brackets (for example: %FE01%).*

Copy

Copy the on-screen database information to a new record. This places the system into insert mode. Be sure to change the Name field of the record before clicking Accept.

Accept

Accept the changes you have made to the database record. Until you click Accept, the system will not save your changes. This is a non-reversible procedure.

Delete

Delete the selected database record. This is a non-reversible procedure.

Close

Close the database record that you have open and exits the current window.

If you have neglected to save your changes (by clicking Accept), the system prompts you to save it before closing the record. If you want to abandon your changes, answer **Yes**. If you want to return and save the changes, answer **No**.



Note



2

Customers, Sites, Hosts, and Remote Agents

Overview

The IRISnGEN database contains a three-tiered hierarchy for defining customers records, sites, hosts and remote agent records. Customers are at the top level and represent the customers in your IRISnGEN database. Sites are at the second level. Sites are the physical locations of your host devices. A customer can have many sites. Hosts and Remote Agents are at the third level. Hosts are the devices that your IRISnGEN system monitors, such as PBX and UPS systems, and data networks, to name a few. A site can contain many hosts. Remote agents monitor the host devices. For example, the SEBea, SEB II, and NET-PATH are remote agents that monitor host PBX devices. The following figure shows a typical hierarchy.



Sample Hierarchy

Build a customer database using customer libraries. Click the customer folder to create and save customer records. Next, add site records that references the customer records. Finally, add the remote agent and host records that reference the site records.

Customers

Customer records define the customers in the IRISnGEN database. For single-company operations, customers can be individual departments, such as Marketing, Administration, etc. For service providers, customers are companies, such as ABC Brokerage House, KLM Communications, etc.

Customer records are the top level of the IRISnGEN database hierarchy. Use these records to store specific customer information, such as name and address, alarm filtering definitions, escalation procedures, contact names, and forward sets and selectors.

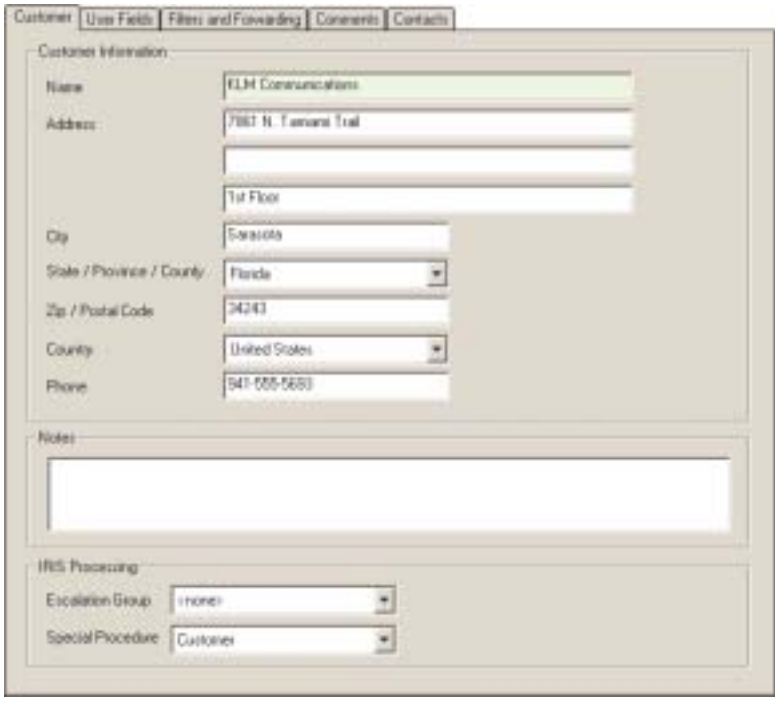
Customer record information is stored on five record tabs:

- Customer
- User Fields
- Filters and Forwarding
- Comments
- Contacts

Use these tabs to identify and define each customer in your IRISnGEN system. Tab information is covered throughout this chapter.

To create a customer record

1 Right-click the **Customers** folder in the tree view; then, select **Add Customer**. The system opens the Customer tab.



2 Type the basic customer information under the Customer Information section.



Note *Use the following format for Canadian Postal Codes: XXX XXX, where X represents any number or letter in the postal code. Include a space after the third character.*

3 Type descriptions, comments, or hypertext in the optional **Notes** field (up to 256 characters. The notes can be revised at any time.

4 Select the escalation group and special procedure from their respective lists under the IRIS Processing section. Selecting an escalation group allows customers to escalate alarms.

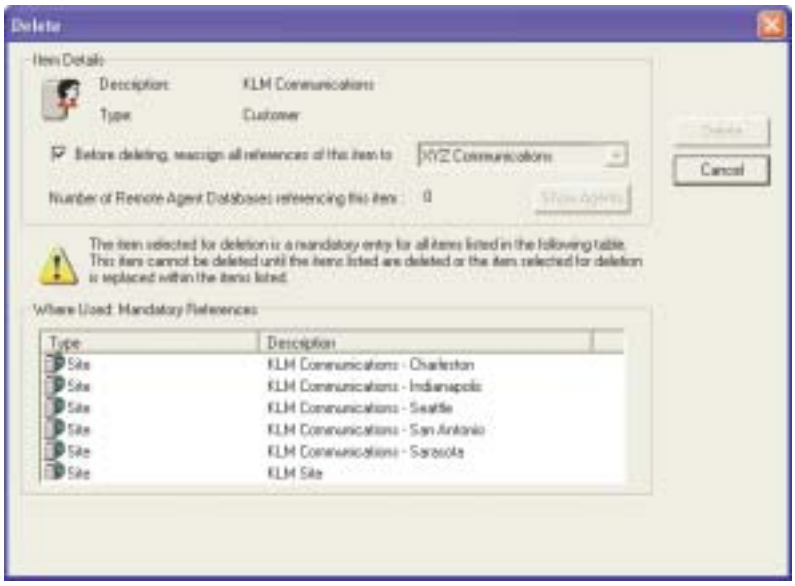
5 Select a special procedure from the **Special Procedure** list. The special procedure is the text that can be added to the alarm.



To delete a customer record

Caution *Before deleting a record, the IRISnGEN verifies that no sites or hosts reference this customer. If you have sites and hosts that reference this customer, you can reassign them to another customer before deleting the record.*

1 Right-click the **Customers** folder in the tree view; then, select **Delete**. The Delete window opens. This window lists the customer and all associates sites and hosts.



2 Make a selection:

To	Click
Reassign any sites or hosts to another customer.	The **Before deleting, reassign all references of this item to** box, then select a customer from the list. All sites and hosts are reassigned and the current customer is deleted.
Delete a customer.	***Delete***. ***Note*** *If you do not want to associate sites and hosts with another customer, manually delete them before deleting the customer.*

To duplicate a customer record

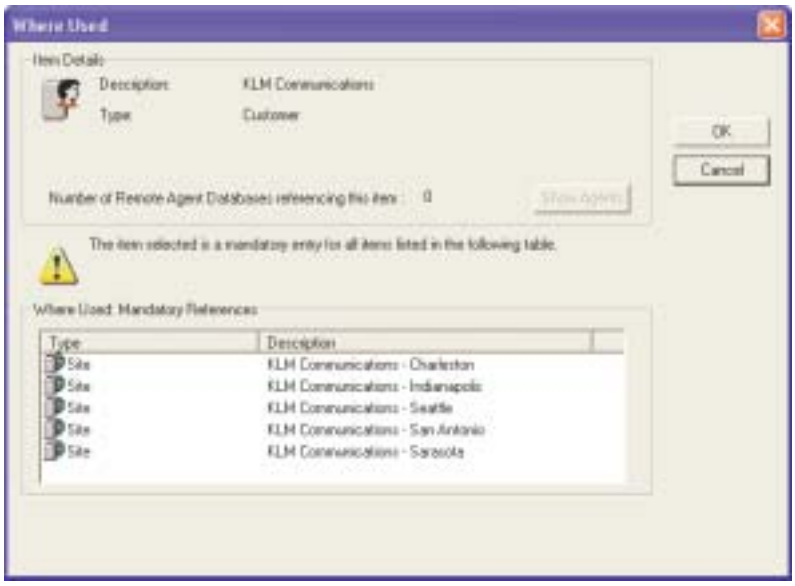
1. Right-click the **Customers** folder in the tree view; then, select **Duplicate**.
2. The customer record is displayed with "Copy" in the **Name** field.
3. Change the name of the customer and any additional customer information, including the information on the other four tabs.
4. Click ***OK*** to save the changes.



Caution *The site and host records assigned to the customer are not duplicated. They must be duplicated individually.*

To identify sites assigned to a customer

1. Right-click a customer name in the tree view; then, select **Where Used**. The Where Used dialog opens.



2. Double-click a site to display the site record.
3. Edit the record if necessary.
4. Click ***OK*** to save the changes.

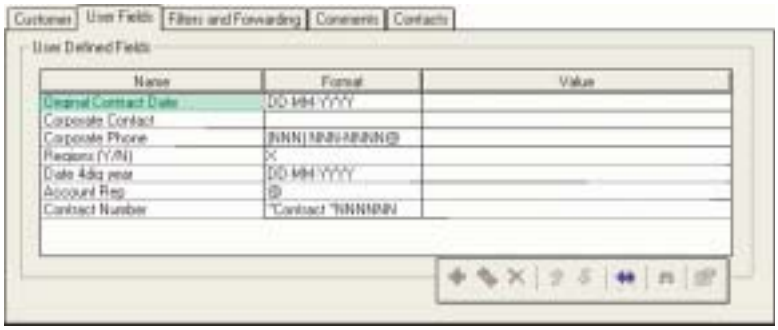


User Fields Tab

You can add an unlimited number of fields to customers, sites, and host records. User Defined Fields are listed under the User Fields tab for that customer, site, or host. Each User Defined Field is unique to each record. For example, User Defined Fields added to a Customer records only appear in Customer records. They do not appear in Site or Host records. A User Defined Field added to a Site record does not appear in the Customer or Host record, etc.

To define new fields for a customer record

1 Choose **IRIS Administration > User-Defined Fields**; then, select one of the three data tables.



2 Click the ✚ button to insert a table row.

3 Type a name of the field in the **Field Name** column. The maximum length is 255 characters.

4 Type a format for each user field in the **Format** field (optional). You can type up to 255 characters. The table on page 2-6 shows valid format characters.

Character	Definition
_ (underscore)	Any single character
A	Any single alphabetic character a-z and A-Z
U	Any single uppercase alphabetic character A-Z
L	Any single lowercase alphabetic character a-z
N	Any single whole number 0-9
@	Remaining characters at the end of a format to represent any number of additional characters.
B	Boolean T/F
X	Yes/No Y/N
0 (zero)	Any number or numbers.
YYYY	Any year with century
YY	Any year without century
MM	Any Month 01 to 12
DD	Any Day 01 to 31
HH	Any Hour 00 to 23
mm	Any Minute 00 to 59
ss	Any Second 00 to 59
"text	Any case-sensitive literal text within quotations (e.g. "Contract" would require the word Contract in the Value field for the Customer, Site or Host User Fields tab).
Special Marker characters	: . + - ( ) , [ ] ; { } ! # $ % ^ & * = | < > ? Space



The following characters are interpreted as literal characters.

Examples

Examples of data supported by format characters are:

Format: MM/DD/YY

- Supported data: 03/30/02
- Unsupported data: 03-30-02

Format: UULLLLNN

- Supported data: FLabcd97
- Unsupported data: flabcd97

Format: AAA mm:ss

- Supported data: Fla 12:45
- Unsupported data: Fla12:45

Format: "Contract Num": NNNNNN @

- Supported data: Contract Num: 123456 Any text
- Unsupported data: contract num- 123456 Any text

To change the name of an existing user-defined field for customer record

1. Highlight the **Name** field.
2. Type a new name (255 characters max).
3. Click ***Save***.

To add or change a value for a user-defined field

1. Click the **User Fields** tab at any customer, site, or host record.
2. Type a value for the field names that display in the Value column. Access to this field is restricted by the Format field. If the Format field is blank, data entry is free-form.
3. Click ***Save***.

Filters and Forwarding Tab

Use the Filters and Forwarding tab to group filter and forwarding instructions into a unique collection for a specific customer, site, or host.

The filter and forwarding instructions added to a customer also apply to the sites and host assigned to that customer. You can add additional filter and forwarding instructions at the site and host levels. However, filter and forwarding instructions added for the site only apply to that site and its assigned hosts. Other sites assigned to the customer are not affected.

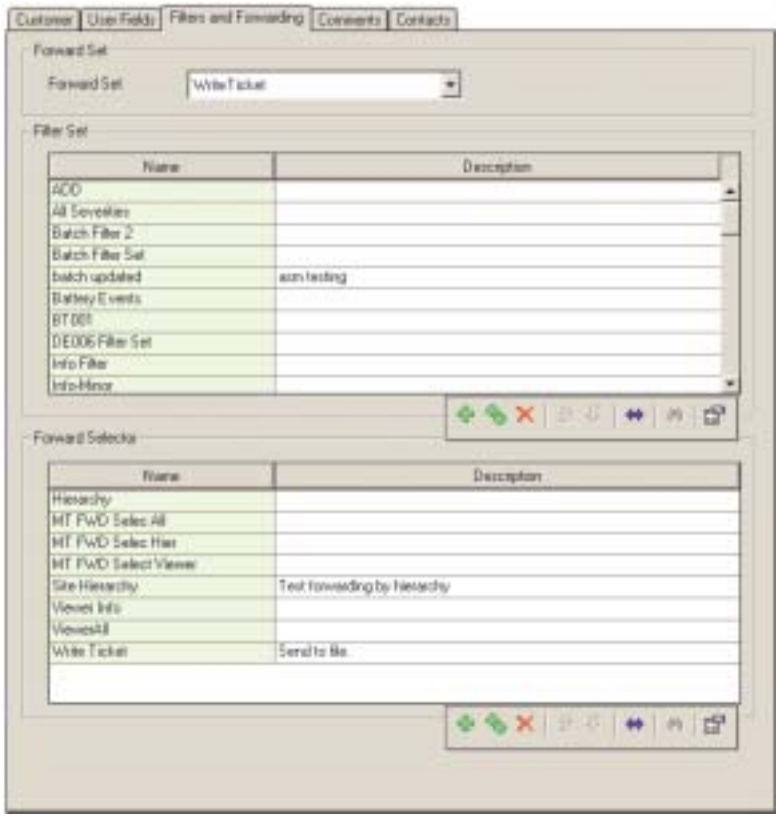
The same rule applies when adding filter and forwarding instructions at the host level. The instructions only apply to that host. No other hosts assigned to that site are affected.



Note *When adding filter sets and forward selectors, click anywhere inside the Filter Set or Forward Selector table to activate the data table toolbar. Use this toolbar to add or delete items.*

To create a filters and forwarding record

1 Select the **Filters and Forwarding** tab from a customer, site, or host record.



2 Complete the fields. The list on page 2-9 describes the fields on the Filters and Forwarding tab.



Field	Definition
Forward Sets	Forward sets tell the system where to send a copy of the alarm information. Select a forward set from the list to define how the alarm is forwarded. You can forward alarms to one or more printers or tables, email addresses, fax machines, and/or pagers. Forward sets only work when they are referenced in the forward selectors (see 'Forward Sets', page 5-24.
Filter Sets	To assign filter sets, select a filter set from the list. You can assign one or more filter sets to a customer, site, or host. The IRISnGEN system acts on each filter independently. When a filter set is selected, IRISnGEN automatically completes the Description field with the description entered when the filter set was created (see 'Filter Sets', page 5-11).
Forward Selectors	Forward selectors tell the system the type of information the system will send. Select a forward selector from the list. You can assign one or more forward selectors to a host. The system acts on each selector independently. When you select a forward selector, the system automatically completes the Description field with the description entered when the forward selector was created (see 'Forward Selectors', page 5-23).

3 Save your Filter and Forwarding record.

Comments Tab

Add comments to the customer, site, and host records when you need to add information that will help manage a specific customer, site, or host. You can also add hyperlinks.

The comments assigned to a customer, site, or host record cannot be modified or deleted. They are aged out according to the user-defined number of days in the System Parameter. The comments can be viewed in the database record for the customer, site, or host and in the Alarm Detail.

To add comments

1 Select the **Comments** tab for a customer, site, or host.



2 Type any comments in the **New Comment** text box; then, click ***Add***. IRISnGEN displays your comment with a timestamp in the Comments display area at the top of the window.

3 Select a duration for the comment.

Date	Click the down arrow to display the calendar. Select a date from the calendar. IRISnGEN will purge the comment on that date.
Days	Type the number of days that IRISnGEN will keep the comment. It will purge the comment after the last day.
Infinite	Select this radio button to keep the comment. IRISnGEN will not purge the comment.



Note *Timed comments do not support hypertext.*



Contacts Tab

A contact is the customer representative that is called for matters regarding a customer. Contact names and telephone numbers can be included in the customer, site, and host records.

To add a contact

1 Click the **Contacts** tab for a customer, site, or host.



2 Click to insert a blank row in the table.

3 Select a contact name from the list in the **Name** column. Contacts are created in the IRIS Libraries folder and include the Order number and the Telephone number.

4 Click in the **Order** field and change the order of the contacts. Entering 1 in this field defines this contact as a primary contact. Only primary contacts appear in the Alarm Detail reports. You can designate more than one primary contact.

5 Repeat steps 2 and 3 as needed.

6 Save the changes.

To remove a contact

1 Under the Contacts tab, highlight a contact from the table.

2 Click

3 Repeat steps 1 and 2 for each contact, as needed.

4 Exit from this window by selecting another object.

Site

Sites are the second level of the IRISnGEN database hierarchy. Use Site records to store specific site information, such as location, alarm filtering definitions, forward sets and selectors, and time zone information.

Site record information can be viewed on six tabs:

- Site
- User Fields
- Filters and Forwarding
- Comments
- Contacts
- Time Zone & Daylight Saving

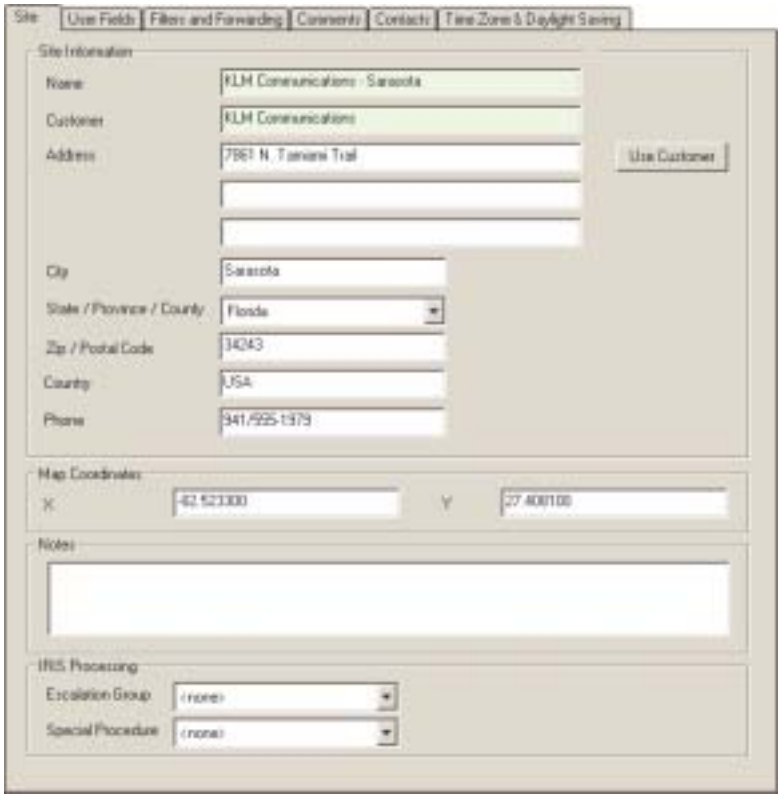
Use these tabs to identify and define each site. The procedures for using the User Fields, Filters and Forwarding, Comments, and Contact tabs are the same as those described in the Customer section (see 2-7). Please refer to those sections when editing these tabs and fields. The Time Zone & Daylight Saving tab is discussed below.



Note *Create your Customer record before your Site record. Also, define the Filter Set, Escalation Group, Special Procedure, and Contact records in the database BEFORE creating your Site record.*

To create a site record

1 Right-click a customer name in the tree view and select **Add Site**. The system displays the Site tab. Notice that the Site information, notes and IRIS Processing sections are the same as the customer Tab, see ’To create a customer record’, page 2-2.



The IRISnGEN system automatically completes the fields under the Map Coordinate section based on the zip code entered in the Zip Code field. The numbers in these fields are the X and Y coordinates locating the site on a map of the United States used by the Geographic Viewer. If these fields are not filled automatically, it is possible that the zip code is not in the system's database. Enter another zip code from the same city until the X and Y coordinates are filled, or contact Teltronics for an updated zip code list.

2 Click the ***Save*** button on the toolbar.

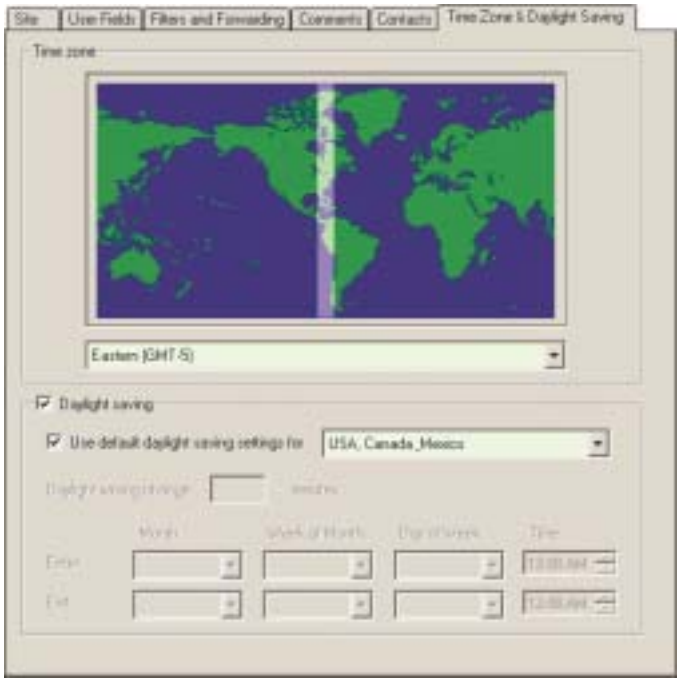
3 Complete and save the information on the fields on the other five tabs to add the site record.

Time Zone & Daylight Saving Tab

Use the Time Zone and Daylight Saving tab to select the appropriate time zones and daylight saving data for the site. System security controls access this page and its fields. The Time Zone & Daylight Saving tab is available only in Site records.

To create a time zone and daylight saving record

1 Click the **Time Zone & Daylight Saving** tab.



2 Select the time zone from the list just below the map.

3 Select the **Daylight saving** checkbox to apply daylight savings time.

- To use default daylight savings settings, select the **Use default daylight savings** box; then, select a region(s) from the list.
- To customize the daylight savings settings, clear the **Use default daylight savings** checkbox; then complete the fields below.

4 Click the ***Save*** button on the toolbar.



Host

A host is a device that attaches to a remote agent and monitors a customer site. Any device attached to the remote agent is considered host. For example, the Teltronics 20-20 PBX is a host device. Port 0 on the SEB II is also considered a host device. The SEBea/NET-PATH monitors the host for alarms and then sends them to IRISnGEN for processing.

Host records are the third-level of the IRISnGEN database hierarchy. Use these records to store specific host information, such as message libraries, alarm filtering definitions, polling, and threshold data.

Host information is stored on nine tabs:

- Host
- Equipment (for use with Multi-Drop Alarm Delivery and Control System, only)
- User Fields
- Filters and Forwarding
- Comments
- Contacts
- Polling
- Threshold and Correlations
- SNMP Settings (for use with SEBea/NET-PATH remote agents, only)
- Users (for use with SEBea/NET-PATH remote agents, only)

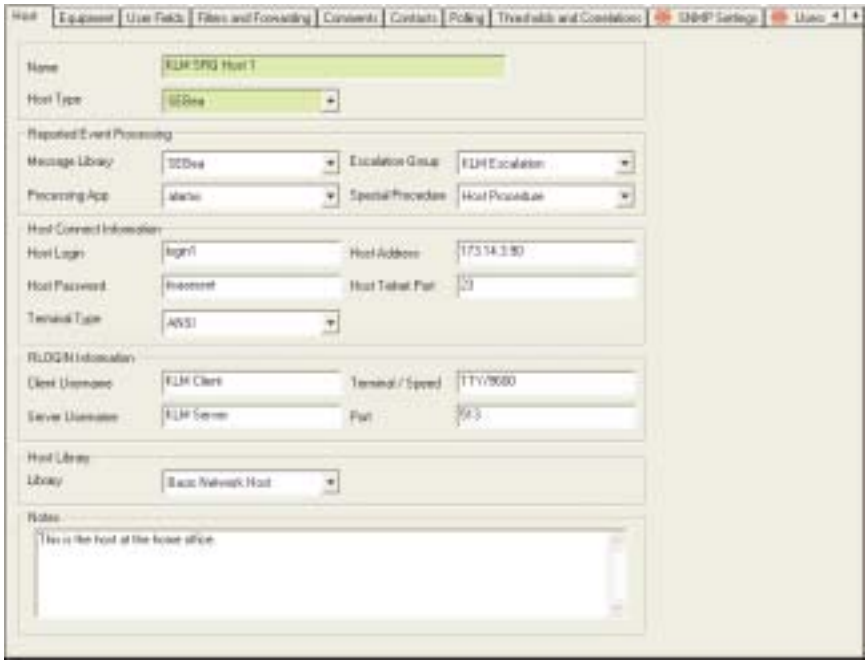
Use these tabs to identify and define each host in the IRISnGEN system. The procedures for using the User Fields, Filters and Forwarding, Comments, and Contact tabs are the same as those discussed in the Customer section earlier in the chapter, refer to those sections when editing these fields.



Warning *Create the Customer, Site, Host Type, and Message Library records before creating Host records. For hosts attached to SEBea and NET-PATH remote agents, create the Host Library record before creating the Host records.*

To create a host record

1 Right-click a site name in the tree view and select **Add Host**. The Host tab opens.



2 Type the host name in the **Name** field; then, select the type from the **Host Type** list. The host name can be any series of numbers and letters, up to forty characters. The selected host type may have a Message Library or Host Library assigned that determines behavior of the host to which it is assigned.

3 Select how to process reported events.

- From the **Message Library** list, select the messages the system expects to receive and process from the host device.
- From the **Processing App** list, select the special instructions application that the system uses to process incoming data.



Note *If you do not select an application, IRISnGEN will send the data to the Bad Data File.*

- From the **Escalation Group** list, select a group to define when alarms move to the next escalation level and the actions IRISnGEN takes when the escalation occurs.
- From the **Special Procedure** list, select the special procedures text that IRISnGEN will add to an alarm. Select **<NONE>** if you do not want to add text to an alarm.

4 Select the host connection information, if needed.

- Type the login name in the **Host Login** field to gain access to the host device. Some host devices for example, a PBX require a login name.
- Type the login password in the **Host Password** field.
- Type the IP address in **Host Address** field.
- Type the Telnet address in the **Host Telnet Port** field.
- Select a terminal type from the **Terminal Type** list.



5 Fill in the RLOGIN Information fields, if needed.
- Type user name that requests the RLOGIN session in the **Client Username** field.
- Type the name that the server uses to execute the command on the server in the **Server Username** field.
- Type the terminal type and speed used to connect to the remote host in **Terminal/Speed** field.
- Type the port number this is dedicated to RLOGIN communications in the **Port** field. The default for this field is 513.

6 Select a library from the **Library** list, found in the Host Library section. IRISnGEN only uses host reporting through SEBea/NET-PATH remote agent devices. The selected host library determines the behavior of the SEBea/NET-PATH.

7 Type a description or comments in the **Notes** field. This field is optional. Use it to provide additional information about the host. Its maximum size is 256 characters. You can also insert hyperlinks in this field. Its information does not expire (age out).

8 Click the ***Save*** button on the toolbar.

9 Complete the fields on the other tabs.

Host-Equipment Tab

The Host-Equipment tab is for users licensed for Teltronics' Multi-Drop Delivery and Control System. License holders can monitor hosts for events and can control equipment attached to the host. For example, an encoder is attached to the SEBea/NET-PATH and it has three pieces of equipment attached to it: a radio, a horn alarm and a temperature sensor. It is possible to monitor the encoder (the host), and its attached equipment. Each piece of equipment can have one or more control elements attached and each control element can be monitored independently of the others.

Equipment and control elements

Define the host device on the Host tab; then, use the Host-Equipment tab to identify the equipment attached to that host. Next, select each control element of the equipment. Since the encoder is a host that monitors equipment, it is possible to identify the individual control elements specified when it produces events on the equipment. For example, the radio equipment may have a control element of Low Battery. When the battery voltage dips below normal, the system generates an event. When IRISnGEN receives the event, it identifies it as coming from the Low Battery element on the radio.

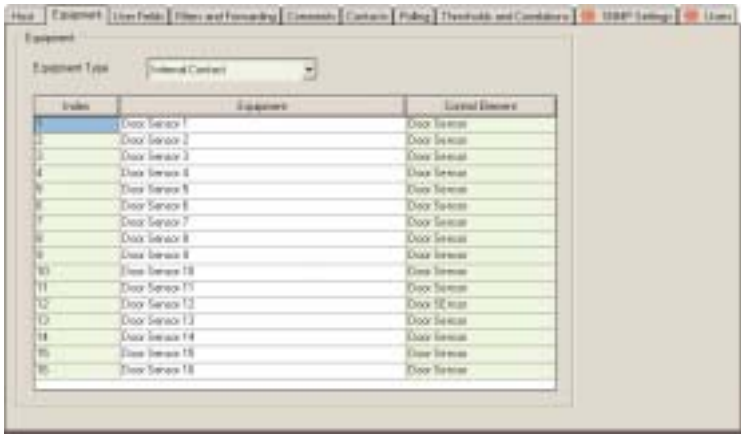
The Host-Equipment tab can also be used for a decoder host to similarly link between equipment and control elements. A decoder does not monitor the status of equipment, but sends requests to the equipment through relay actions. For example, selecting radio equipment that has two separate control elements (antenna and channel-select) lets you control those items with an action request.

When the equipment attaches directly to the SEBea/NET-PATH and not to a host device, it is still possible to monitor the equipment and send control commands. However, in these cases you must define the equipment in IRISnGEN as both a host device and as the attached equipment. Use the Host tab to define your equipment as a host, and then use the Host-Equipment tab to define your equipment.



To create an equipment record

1 Click the **Equipment** tab.



2 Select the type of equipment to be attached to the host from the **Equipment Type** list. The equipment type defines what operations are possible for each piece of equipment connected to the host. For more information about equipment types, see ’Equipment Types’, page 5-54.



Note *The Index column contains the number of equipment entries defined in Max Number Equipment field on the Host Type tab (see ’Host Types’, page 5-65). The system uses this index to link an alarm to a specific piece of equipment. You cannot edit this column.*

3 Click a row under the Equipment column; then, select a piece of equipment from the list. Repeat this step as needed.



Note *If you have not yet defined your equipment, do so now. You must define your equipment before you can save your equipment action record. For more information about defining equipment, see ’Equipment’, page 5-47.*

4 Click a row under the Control Element column; then, select a control element from the list. Repeat this step as needed. The list only displays control elements configured for the equipment selected in the Equipment column.

5 Click the ***Save*** button on the toolbar.

Removing Equipment from the Data Table

When an equipment or control element is removed from the Host-Equipment data table (and it will not be reassigned to another host), make sure to physically disconnect the device, as well. If not, the device may continue to deliver events to IRISnGEN via the Multi Drop network. These delivered events will appear in the List Viewer, but will not show in the Equipment Viewer or the Map Viewer. IRISnGEN will not indicate that it received events from a device not listed in its database.

Periodically check the List Viewer to identify events that may not appear in the Equipment or Map Viewer. This is a good indication that an equipment or control element was removed from the data table, or that it was defined in the data table, but not referenced in the Remote Agent Manager's Devices & Hosts tab, see ’Devices & Hosts Tab’, page 2-32.



Polling Tab

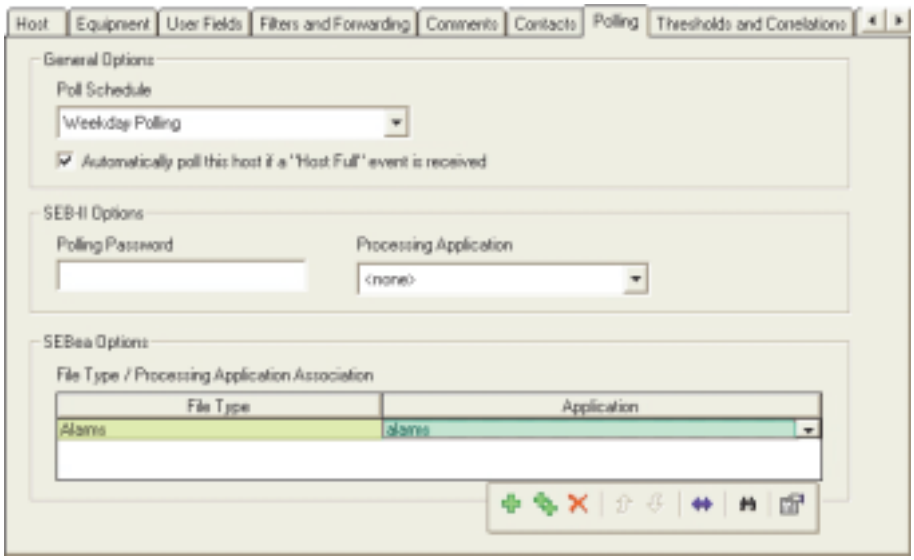
Polling parameters can be included when creating a host record. Polling parameters tell IRISnGEN how to retrieve stored data from a host. Use the Polling tab to define when to poll, how to format the data and what application is used to process the data.



Note *You must create your customer, site, host type, and message library records before creating host records. To simplify creating a new database, define your filter, escalation groups, and special procedures BEFORE you create your host records.*

To create a polling record

1 Click the **Polling** tab.



2 Select a schedule for polling the remote agent from the **Poll Schedule** list.

3 Select the **Poll Host if Full** checkbox to poll the host's data when the SEBea/NET-PATH remote agent is full. The poll is triggered by the XF event (SEBea/NET-PATH) or the fixed event FE12 (SEB II).

4 If your remote agent is an SEB II, type a password in the **Polling Password** field. Passwords are defined in the Remote Agent Manager's Security Library for SEBea/NET-PATH devices.

5 From the **Processing Application** list, select the processing application that tells IRISnGEN where to store the incoming data.

6 If your remote agent is an SEBea/NET-PATH, select a file type from the **File Type** list. The file type contains the data storage characteristics for the remote agent you wish to poll.

7 Select an application from the **Application** list. You can choose **alarms**, **SL1Traf**, or **TCMgr**.

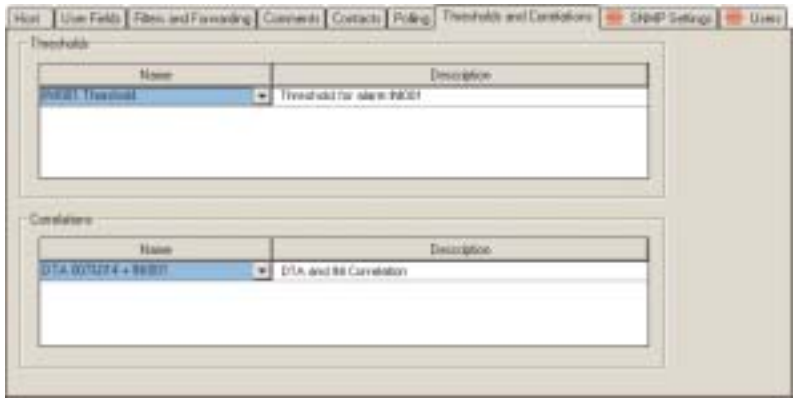
8 Save your record.

Thresholds and Correlations Tab

Use the Thresholds and Correlations tab to define the thresholds and correlations of alarms received from a single host. Threshold and correlation parameters can be included while handling event data. Threshold and correlation parameters filter unwanted event data when IRISnGEN receives it from the remote agent. Thresholds filter and remove data that exceed defined levels, such as counts levels and time constraints. Correlations monitor for the occurrence of multiple events within a defined time and combine related events.

To create a thresholds and correlations record

1 Click the **Thresholds and Correlations** tab.



2 Select the threshold parameters from the **Name** list under the Threshold section. The description is automatically filled.

3 Select the correlation parameters from the **Name** list under the Correlation section. The description is automatically filled.

4 Click the ***Save*** button on the toolbar.

To add a threshold

1 Click in the **Name** field.

2 Use the Insert Row button to insert a blank row in the Threshold data table, or press the button to add multiple thresholds.

3 Select a threshold from the list.

4 Repeat steps 2 and 3 to add additional thresholds.

IRISnGEN automatically fills the Description field with the description entered when the threshold was created. See ’Thresholds’, page 5-40.

To add a correlation

1 Click in the **Name** field.

2 Use the Insert Row button to insert a blank row in the Correlations data table, or press the button to add multiple correlations.

3 Select a correlation from the list.

4 Repeat steps 2 and 3 to add additional correlations.

IRISnGEN automatically fills the Description field with the description entered when the correlation was created. See ’Single Host Correlation’, page 5-3.

SNMP Settings Tab

If the host device is monitored via a network, the SNMP settings must be defined. SNMP defines a protocol for the managing TCP/IP based networks.

SNMP Version 1 (SNMPv1) is the first implementation of the SNMP protocol. However, this version lacks some security features, leaving it vulnerable to a variety of security threats. Because of this, many vendors do not implement all the functions that SNMPs offers and, therefore, limits SNMP to little more than a monitoring facility.

SNMP Version 3 (SNMPv3) offers strong authentication and data encryption for privacy. Because of its enhanced security, SNMPv3 is much more complex than SNMPv1. Privacy can only be used if Authentication is also used. Security choices include:

- No Authentication and No Privacy
- Authentication only
- Authentication and Privacy

Use the SNMP Settings tab to define the V1 and V3 settings.

To create and SNMP settings record

1 Click the **SNMP Settings** tab.



2 Type the number of the TCP/IP port used to receive SNMP traps from the host in the **Port** field. The default port is 161, however, this number can be modified.

3 Configure a security setting:

To configure V1 security settings

1 Select the **V1 Security Settings** checkbox. The default for this box is not selected. The Community Name field is activated.

2 Type a name in the **Community Name** field. A commonly used name is "public," although another name can be used.

To configure V2 security settings

1 Select the **V2 Security Settings** checkbox.

2 Type a name in the **Community Name** field. A commonly used name is "public," although another name can be used.

To configure V3 security settings

1. Select the **V3 Security Settings** checkbox. The default for this box is not selected. The fields below are activated.
2. Select the HMAC-MD5 or the HMAC-SHA protocol from the **Authentication** list.
3. Type a password in the **Authentication Password** field. Type something that is easy to remember. This password automatically converts to an authentication key.
4. Select an encryption protocol from the **Encryption** list. Select DES.
5. Type a password in the **Encryption Password** field. The system displays the hexadecimal characters of the encryption key for DES. This field cannot be edited.
6. Type a name to secure the setting in the **Security Name** field.
7. Type the ID of the SNMP engine in the **Security ID** field.
8. Type the context name for the V3 security setting in the **Context Name** field. This field is mostly used in the case of proxies and is usually empty in the case of normal agents.
9. Type the context ID in the **Context ID** field. It is usually the same as the Security ID.

Users Tab

Use this tab to define the users (Item) or user groups (Groups) that can access that host.

To create a user record

1. Click the **Users** tab.



2. Select a group to grant access rights to the current host from the **Group** list. For more information about groups, see ’User Groups’, page 6-118.
3. Select an individual user to grant access rights to the current host from the **Items** list. For more information about users, see ’Users’, page 6-116.
4. Click the ***Save*** button on the toolbar.



To add a group

1. Click inside the **Name** field under the Groups section.
2. Click to add a blank row , or click to add multiple groups.
3. Select a group from the list.
4. Repeat steps 2 and 3 to add additional groups.

To add a user

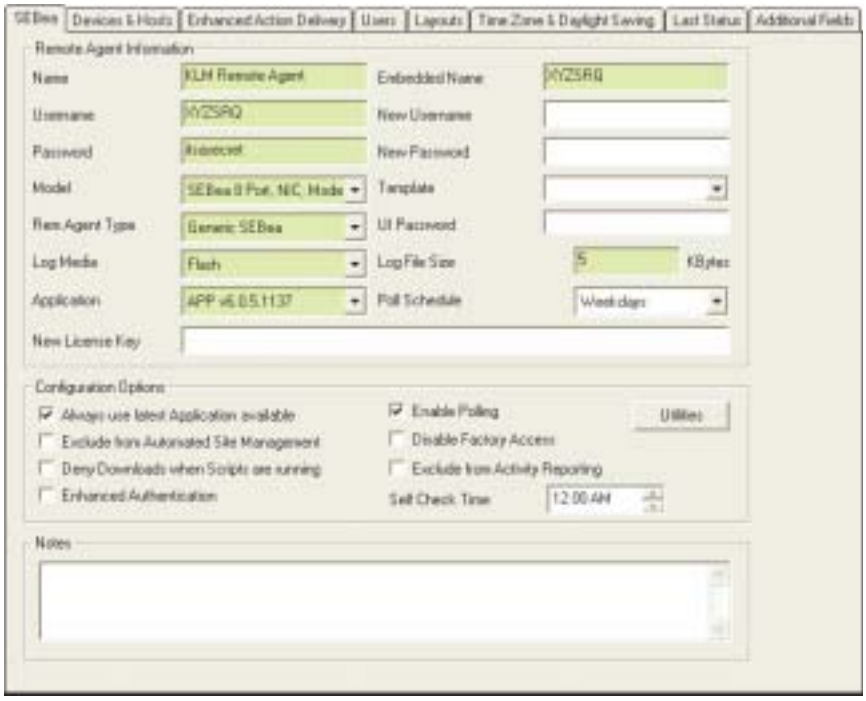
1. Click inside the **Name** field under the Items section.
2. Click to insert a blank row, or click to add multiple users.
3. Select a user from the list.
4. Repeat steps 2 and 3 to add additional users.

SEBea/ NET-PATH Remote Agent Tab

Use the Remote Agent (SEBea/NET-PATH) tab to configure and manage existing SEBea/NET-PATH remote agents.

To create the SEBea/NET-PATH remote agent record

1. Right-click the site name in the tree view and choose **Add SEBea/NET-PATH**.



2. Type the name that identifies the SEBea/NET-PATH remote agent in the **Name** field; then, type the name that uniquely identifies the embedded name of the SEBea/NET-PATH remote agent in the **Embedded Name** field. Both fields are required.



Warning *Be careful when using special characters 129 (0x81) though 143 (0x8F) and 152 (0x98) though 159 (0x9F). The characters are* **,ƒ„…†‡ˆ‰Š‹Œ_** *and* **˜™š›œ_Ÿ***. The characters appear correctly in record, but will appear as the* **|** *character in the IRISnGEN tree view.*

3 Type the master user's name and the remote agent password in the **Username** and **Password** fields respectively; then, select the SEBea/NET-PATH application version form the **Application** list. The password field can hold up to 20 characters.



Note *The New Password field is optional. It specifies a new password for the SEBea/NET-PATH remote agent. The new password becomes effective the next time a database is downloaded to the SEBea/NET-PATH remote agent. Creating a new password marks the database as "dirty," as applicable in the ASM functions (see 'Automated Site Management', page 4-9.*

4 Select an SEBea/NET-PATH model and template from the respective **Model** and **Template** lists. Selecting a model enables the system to fill in the Devices and Hosts tabs with generic named devices available for the remote agent. The models are pre-configured at the factory. Selecting a template populates the Device Library field in the Devices and Hosts tab.

Only templates using the same model as this remote agent are available in the list. Although assigning a template is not required, it shortens the manual data entry for each remote agent. It is not necessary to select a device library for each remote agent.

5 Select a remote agent type from the **Remote Agent Type** list; then, type a password to access the SEBea/NET-PATH User Interface panel in the **UI Password** field. This password provides access to the SEBea/NET-PATH remote agent's LCD display and menu selections.

6 Select a media type to store log files from the **Log Media** list; then, type the maximum log file size for each SEBea/NET-PATH remote agent in the **Log File Size** field. For the Log Media type, select RAM or Flash. RAM is temporary storage. Information is lost during power outages or system resets. Flash is a more permanent storage area and, under normal conditions, its content is not lost during power outages or system resets.

7 Type the SEBea/NET-PATH license key you received from Teltronics with your remote agent in the **New License Key** field. The license key controls the features available in your SEBea/NET-PATH. If you purchased additional features or upgraded your SEBea/NET-PATH, enter the new license key number in this field and download the database to the SEBea/NET-PATH to activate those features.



8 Select one, all, or none of the SEBea/NET-PATH configuration options:

Select	To
Always use latest application available	Download an updated version of the SEBea/NET-PATH application to the SEBea/NET-PATH remote agent.
Exclude form Automated Site Management	Exclude the SEBea/NET-PATH remote agent form ASM. The remote agent will not appear in the ASM batch or selector lists, even if it matches the filtering criteria.
Deny downloads when scripts are running	Refuse any type of download to the SEBea/NET-PATH while a Python script is running in the SEBea/NET-PATH. This field is for SEBea/NET-PATH remote agents only.
Enhanced Authentication	Enable the remote agent to use Enhanced Authentication. See “Enhanced Authentication” on page 3-10.
Enable Polling	Enable this remote agent for polling. If not selected here, the SEBea/NET-PATH remote agent can still be polled using the Manual Polling or Remote Agent Manager feature.
Disable Factory Access	Deny access to Teltronics technicians.
Exclude from Activity Reporting	Exclude the remote agent from the Sites Not Reporting report. Selecting this box also disables the color change function for the icon that represents this remote agent in the Equipment Explorer. For example, it prevents an icon from turning red when the site fails to respond.

9 Select the time the SEBea/NET-PATH will call IRISnGEN to report its self-check results from the **Self Check Time** list; then, select the schedule that tells IRISnGEN when to poll the remote agent attached to this host from the **Poll Schedule** list.





Note *Although the self-check time default is midnight, we recommend that you stagger the self-check times between the SEBea/NET-PATH remote agents to balance the reporting load in IRISnGEN. This is a required field.*

10 Click the ***Utilities*** button to use the SEBea/NET-PATH Database Utilities feature. After completing the other selections on the SEBea/NET-PATH Remote Agent tab, the SEBea/NET-PATH Database Utilities dialog screen enables you to verify that all devices and logical information the system needs is in the database. You can also view an XML formatted version of the database in NotePad.

11 Type any notes, comments, or hyperlinks in the **Notes** field.

12 Click the ***Save*** button on the toolbar.



SEBea/NET-PATH Database Utilities

After completing the SEBea/NET-PATH Remote Agent tab, click the Utilities button to create, view, or download the database. The system displays the Advanced Remote Agent Utilities dialog.



Make a selection:

Click	To
Create	Create the SEBea/NET-PATH database and verify that all devices and logical information the system needs is in the database.
View	View an XML formatted version of the database in Internet Explorer.
Download	Download to display the Download Utility dialog for Telnet. Use the Download Utility dialog to send a database, application, operating system, or loader to the SEBea/NET-PATH remote agent.
Close	Close the Advanced Remote Agent Utilities window.

Telnet Download Utility

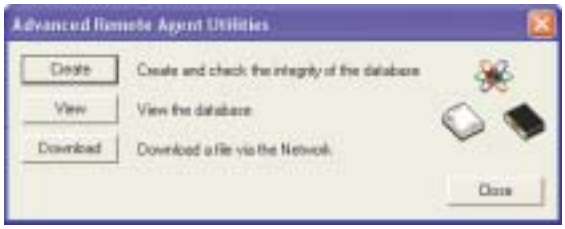
IRISnGEN's Telnet Download Utility can be used to transfer a database, application, operating system, or loader to a remote agent device (SEBea/NET-PATH or NET-PATH) if you are communicating with remote agent containing an application version 3.0 or later. You can also use this utility to establish a Telnet connection to the remote agent.



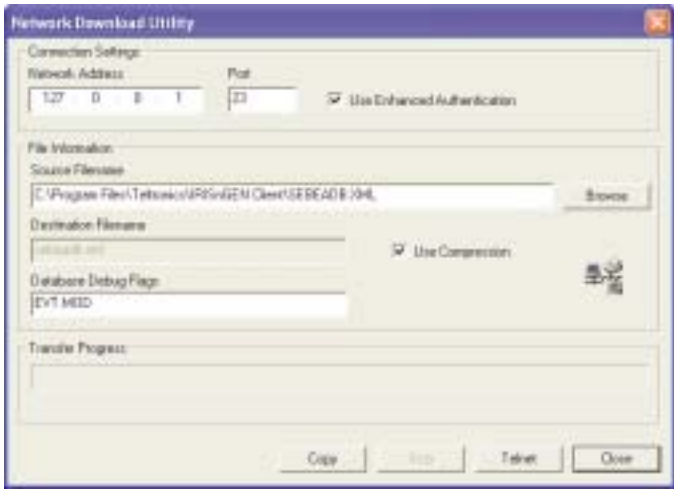
Warning *If you are running IRISnGEN Ver6.x, you should not download an application Ver 4.x to a remote agent currently loaded with a database. If you are running IRISnGEN Ver 6.x, you cannot download a Ver 5.x database to a remote agent loaded with a Ver 4.x application.*

To download a file using the Telnet Download Utility

1. Click the ***Utilities*** button on the Remote Agent tab to open the Advanced Remote Agent Utilities dialog.



2. Click ***Download*** to open the Download Utility window.



3. Type the IP address of the targeted remote agent in the **IP Address** field, if different from the default IP address. The default IP address is defined in the Networks section of the Devices & Host tab.
4. Type the Telnet port of the remote agent in the **Port** field. The default port is 23.
5. If you are using Enhanced Authentication with your remote agent, select the **Use Enhanced Authentication** checkbox.



Note *To successfully use Enhanced Authentication, you must also select the Enhanced Authentication checkbox on the Remote Agent tab (SEBea or NET-PATH).*



6 Type the path to the directory containing the database, application, operating system, or loader you wish to download to the remote agent in the **Source Filename** field. If necessary, click ... to browse to the directory.



Note *If you are downloading a database, the default path and filename is \Program Files\Teltronics\IRISnGEN Client\SEBEADB.XML. If you are downloading an application, operating system, or loader, the default path is \Irishome\Apps and the filename will contain the .IMG extension for an application or operating system, or BMG for a loader.*

The file type must match the actual files; otherwise, a mismatch could leave the remote agent in an inoperable state.

7 Verify the file in the **Destination File** field. Depending on the file you are downloading, IRISnGEN automatically displays its destination filename and extension. These include:

- Database: SEBEADB.XML
- Application:SEBEA.IMG
- Operating System:SEBEA.BAK
- Loader:SEBEA.BMG

8 Select the **Use Compression** checkbox to compress the database. This will speed the transfer of data. The remote agent will decompress the information as it receives it.

9 Type the debug commands that will select the debug information displayed in the remote agent debug output in the **Database Debug Flag** field.



Note *To enable debug output, be sure you name a serial port "Debug" in the Remote Agent Devices and Hosts tab.*

10 Make a selection:

Click	To
Copy	Transfer the database, application, operating system, or loader to a remote agent device.
Telnet	Communicate with the remote agent via Telnet. See page 2-30.

11 Check the progress of the download in the **Transfer Progress** area of the box.

Communicating with the remote agent via Telnet

Use the Telnet Utility to communicate directly with the SEBea/NET-PATH remote agent.

To establish a Telnet connection with the remote agent

1 Click ***Telnet*** on the Download Utility dialog, shown on page 2-28. The Telnet dialog window opens.



2 Type you user ID and password to log in; then, press ***Enter***.

3 Enter the commands when the system returns the SEBea/NET-PATH> prompt.

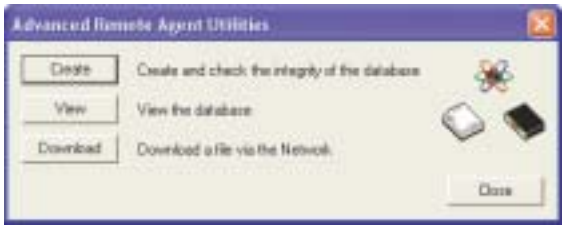
SNMP Download Utility

If the IRISnGEN system connects to an SNMP network, use the SNMP Download Utility to transfer a database, application, operating system, or loader to the SEBea/NET-PATH remote agent device.

To use this feature, the SEBea/NET-PATH must be running App version 3.0 or above. If the SEBea/NET-PATH has an earlier App version, contact Teltronics Customer Service for instructions to use an alternate SNMP download method, or download the SEBea/NET-PATH using the dialup method. You can also use this utility to establish a Telnet connection to the SEBea/NET-PATH.

To download a file using the SNMP Download Utility

1 Click ***Utilities*** on the SEBea/NET-PATH Remote Agent tab to open the SEBea/NET-PATH Database Utilities dialog box.



2 Press Ctrl+Download to open the Download Utility window.

3 Type the IP address of the targeted SEBea/NET-PATH remote agent in the **IP Address** field.

4 Type the size of the packet data to be sent across your SNMP network in the **Packet Size** field. The default is 1024. Generally, you will not need to change this number unless you are receiving errors on your modem and you need to send smaller packets.

5 Type the SNMP port of the SEBea/NET-PATH remote agent in the **Port** field. The default port is 162.

6 Type the path to the directory containing the database, application, operating system, or loader you wish to download to the SEBea/NET-PATH in the **Source File** field. If necessary, click ... to browse to the directory.



Note *If you are downloading a database, the default path and filename is \Program Files\Teltronics\IRISnGEN Client\SEBEADB.XML. If you are downloading an application, operating system, or loader, the default path is \Irishome\Apps and the filename will contain the .IMG extension for an application or operating system, or BMG for a loader.*

7 Verify the file in the **Destination File** field. Depending on the file you are downloading, IRISnGEN automatically displays its destination filename and extension. These include:

- Database: SEBEADB.XML
- Application: SEBEA.IMG
- Operating System: SEBEA.BAK
- Loader: SEBEA.BMG

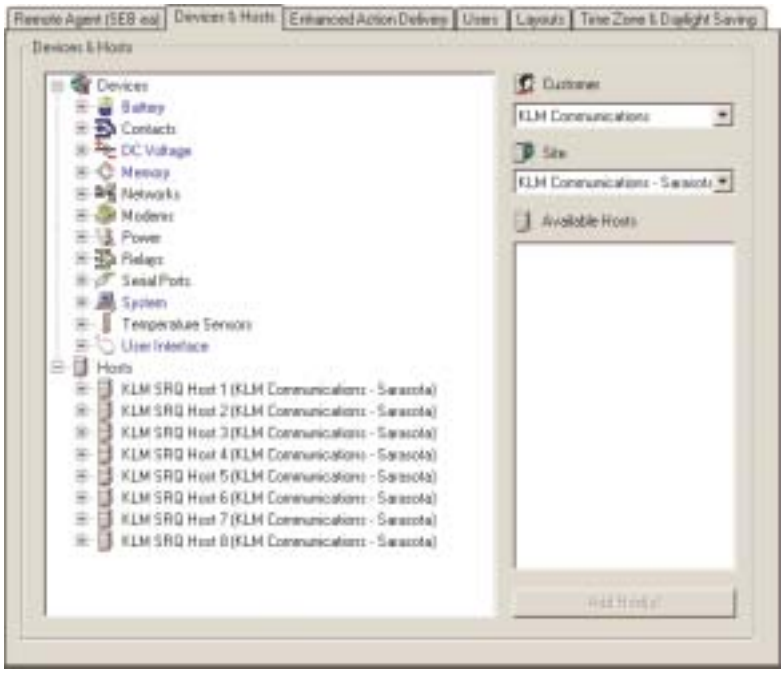
8 Type the debug commands that will select the debug information displayed in the SEBea/NET-PATH debug output in the **Database Debut Flag** field.

9 Click ***Copy***.

10 Check the progress of the download in the **Transfer Progress** area of the box.

Devices & Hosts Tab

Use the Devices & Hosts tab to create new device records and assign hosts. This tab includes two data table controls: devices and host. Use the bidirectional drag and drop function lets to assign any configured device to any host, or any host to any device.



The devices and hosts data table is helpful when configuring new devices. after a device is configured, it can be assigned to a host, or a host can be assigned to the device, making a logical link between the device (hardware) and the host information (logical/software definition).

Use the drag and drop feature when assigning the two fields. Select a host and drop it onto a device, the device name expands to present the assigned host. Expanding the device name, selecting the undesired host, and then pressing the ***Delete*** key to delete the host will break the assignment. The host remains and only the assignment is deleted.

To	Select
Use a specific customer option,	The option from the **Customer** list. The default is the current customer to which the remote agent is assigned.
Use a specific site option,	A site from the **Site** list. The default is the current site to which the remote agent is assigned.

The available hosts automatically display in the **Available Hosts** box depending on the Customer and Site options you choose.

To add hosts to a tree view, highlight the hosts you wish to add, and click ***Add Hosts***.

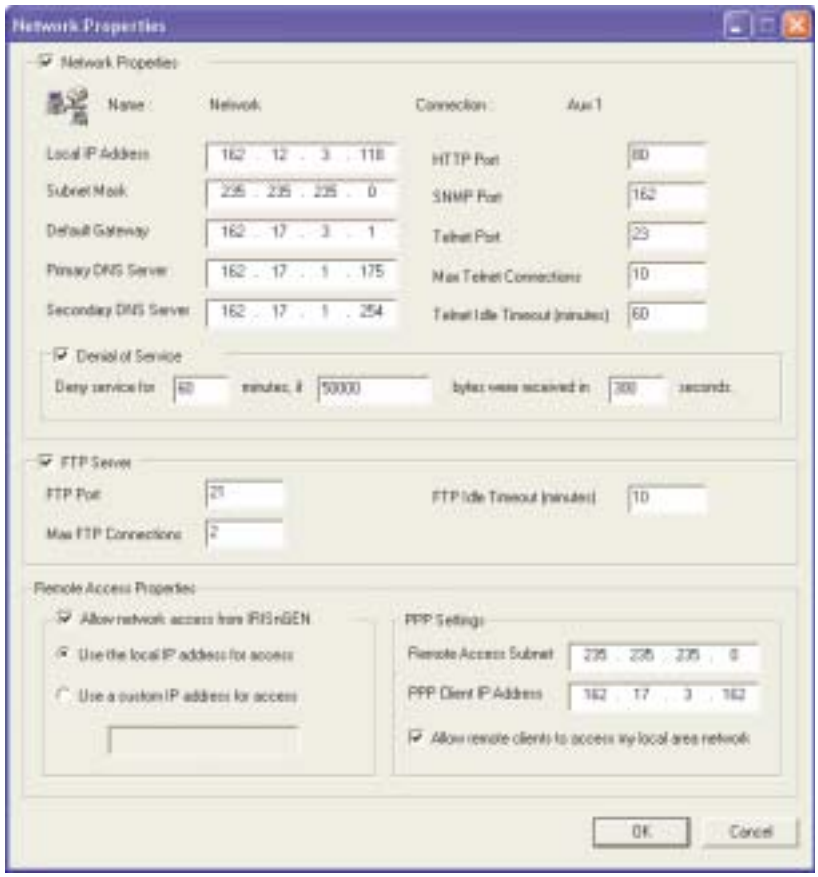


To add hosts from a different site

1. Select an option from the **Customer** list.
2. Select an option from the **Site** list. The host names are listed in the **Available Hosts** box.
3. Select the hosts to add to the Devices & Hosts tree view; then, click ***Add Hosts***. The selected hosts appear in the Devices & Hosts tree view.
4. Use drag and drop to drop the hosts from the Devices & Hosts tree view.

Editing the Network Properties dialog

Use the Network Properties dialog to configure the Network Interface (NIC) parameters IRISnGEN needs to establish a network connection with the remote agent.



To edit the Network Properties dialog

1. From the **Devices & Hosts** tab, click the **+** symbol to expand the Networks folder.
2. Right-click a network name; then, select **Properties** from the pop-up menu. Click the **Network Properties** checkbox to activate the fields and other boxes on this dialog.
3. Set the IP address properties in the next five fields.
   - Type the remote agent's IP address in the **Local IP Address** field. This is the number used when connecting to the remote agent via a network—for example, with Telnet.
   - Type the IP address for the subnet mask in the **Subnet Mask** field.
   - Type the gateway address for your network in the **Default Gateway** field. (optional)

- Type the IP address for your primary DNS sever in the **Primary DNS Server** field. (optional)
- If your network uses a second DNS server, enter its IP address in the **Secondary DNS Server** field. (optional)

4 Enter the port and connection settings in the next five fields. If you are using Telnet, be sure to include the maximum number of connections and a timeout value.



Warning *Do net set the HTTP, SNMP, or Telnet ports with the same value. The remote agent cannot run multiple services on the same port.*

5 Set Denial of Service in the next four fields.

- Select the **Denial of Service** checkbox to enable recognition of too many network packets sent within a defined period.
- Type the number of minutes to deny service in the **minutes** field.
- Type the number of bytes that must be received before denying service in the **bytes** field.
- Type the number of seconds in which the system must receive the bytes in the **seconds** field.



Note *Setting the Denial of Service parameters may affect your ability to transfer files using FTP. Be sure to specify an adequate number of bytes in the Bytes field to handle larger files transferred using FTP.*

6 Set the FTP Server attributes in the next three fields.

- Select the **FTP Server** checkbox to enable all other FTP server fields below.
- Type the port number used for FTP communications in the **FTP Port** field. The default is 21.
- Type the maximum number of simultaneous FTP connections allowed by the remote agent in the **Max FTP Connections** field. The range is 1 - 128. The default is 2.
- Type the number of minutes that an idle FTP connection will remain open in the **FTP Idle Timeout** field. The range is 0 - 60. The default is 10.

7 Set Remote Access Properties. This will allow you to access the remote agent from IRISnGEN.

- To allow IRISnGEN to connect with the remote agent, select the **Allow network access from IRISnGEN** checkbox. If you do not check this box, IRISnGEN cannot connect with the remote agent; however, other devices on the network still can.
- Click a radio button to select an IP address for access. If you click the **Use a custom IP address for access** button, be sure to enter the IP address in the next field.

8 Enter the PPP settings in the next three fields.

- Enter the subnet mask needed to establish access to the remote subnet in the **Remote Access Subnet** field. See “Establishing access to the remote subnet” on page 2-35.

- If you wish to connect with the remote agent using a PPP connection, type the IP address that you will assign to the remote agent.
- Click the **Allow remote clients to access my local area network** checkbox if you want remote clients to access your local network via a PPP connection.



9 If your are configuring a NET-PATH Plus remote agent, set the **Secure Router Properties**.

- Type the password for the root user in the **Root Password** field. The default password is "Default."



Note *The information in this field is for references purposes, only. Changing a password here does not change the root password in the Secure Router. To change the root password, you must use the Secure Router's web interface. If you change the root password, we recommend you update this field as well.*

- If you want your Secure Router to connect to the WAN, enter its public IP address in the **Public IP Address** field.
- If you want your Secure Router to connect to the LAN, enter its private IP address in the **Private IP Address** field.
- Enter the port number used by the Secure Router to connect to the WAN and/or LAN in the **HTTP Port for Web Management** field. The default is "8000."
- Click the **Use Public Interface for Web Management** checkbox to all the Secure Router public access to the web.
- Click the **Use Private Interface for Web Management** checkbox to allow the Secure Router private access to the web.



Note *If you created a new NET-PATH Plus remote agent record.*

10 Click ***OK*** when done.

Establishing access to the remote subnet

The remote subnet mask is not the subnet mask reported by Windows. The remote subnet mask acts as a firewall mask. The subnet mask in the Device Library is a routing mask that determines if the packet is sent directly to the destination (because it is in the same sub-net) or to the gateway. The remote subnet mask determines which packets pass and which packets are discarded. When establishing a PPP link, the remote agent has two interfaces, PPP and NIC. The subnet mask is used to determine which packets are forwarded between the two interfaces. The remote subnet mask is bit AND-ed with the source IP to give value1 and with destination IP to give value2. If value1 and value2 are equal, the packet passes.

The Remote Access Subnet setting defines which data is local and directly accessible by the remote user.

The following formula must be true for data to pass through the filter:

[IP assigned to PPP] & [Remote Access Subnet] = [Destination IP] & [IP Remote Access Subnet]

The following examples show how this would work given various situations:

Example 1

172.16.3.123 & 255.255.255.0 = 172.16.3.0 /* Data from IP's within 172.16.3.x pass the filter.

Example 2

172.16.3.22 & 255.255.0.0 = 172.16.0.0 /* Data from IP's within 172.16.x.x pass the filter.

Example 3

172.16.3.12 & 0.0.0.0 = 0.0.0.0 /* Data from all IP addresses pass the filter.

How does the AND operator work?

The AND or '&' operator is used to make a bit wise comparison of numbers. The number is first converted to binary, and a comparison is then done on the binary number. The last table below show's the binary value of the decimal numbers followed by an example of the bit wise operation, and the result.

The bit wise AND operator		
Bit 1	Bit 2	Resulting Bit
0	0	0
0	1	0
1	0	0
1	1	1

172.16.3.123	
Decimal Value	Binary Value
172	10101100
16	10
3	11
123	111011

255.255.255.0	
Decimal Value	Binary Value
255	11111111
255	11111111
255	11111111
0	0

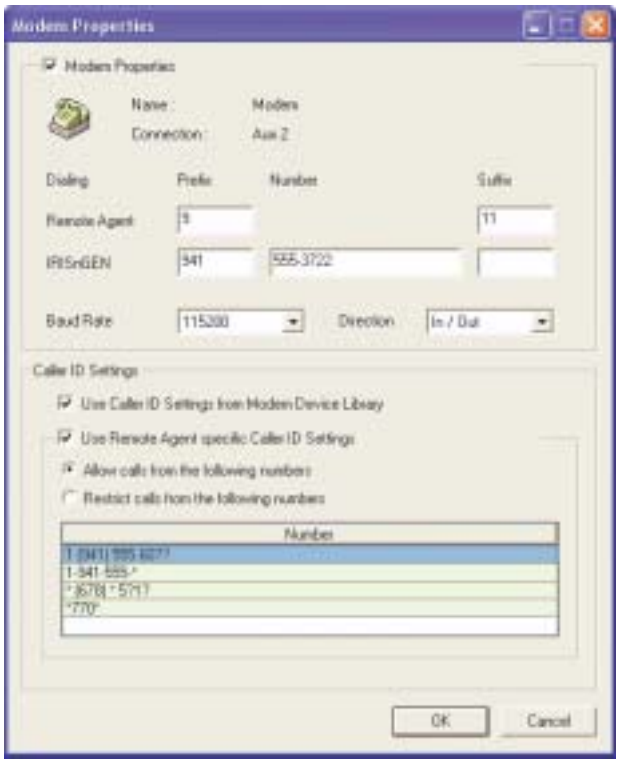
Example of AND operator in relation to the Remote Agent Subnet				
Destination IP Address	10101100	00000010	00000011	1111011
Remote Destination Subnet	11111111	11111111	11111111	0000000
Resulting Binary Value	10101100	00000010	00000011	111011
Resulting Decimal Value	172	16	3	0



Editing the Modem Properties dialog

Use the Modem Properties dialog to configure the modem parameters IRISnGEN needs to establish a network connection with the remote agent.

1. From the **Devices & Hosts** tab, click the **+** symbol to expand the **Modem** folder.
2. Right-click a Modem name; then, select **Properties** from the pop-up menu to open the Modem Properties dialog.



3. Click the **Modem Properties** checkbox to activate the fields and other boxes on this dialog.
4. Type the dialing prefix in the **SEBea Prefix** field and the suffix in the SEBea Suffix field. The prefix is the number required by some telephone switches (PBX) to access an outgoing line, for example, "9". The suffix is the number used as an access code, for example, to dial a foreign country.
5. Type the prefix, number, and suffix that IRISnGEN uses to dial into the remote agent in the **Prefix**, **Number**, and **Suffix** fields.
6. Select your modem's baud rate from the **Baud Rate** list.
7. Select the call direction (In, In/Out, or Out) from the **Direction** list. Calls can be inbound, outbound, or both.



Note *You must configure at least one inbound modem in the remote agent.*

8.
9. Click ***OK*** when done.

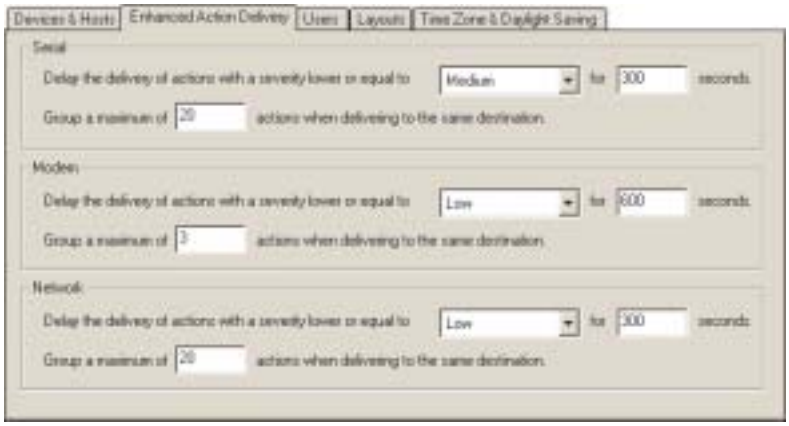
Enhanced Action Delivery Tab

The delivery of lower severity actions for each host can be delayed using the Enhanced Action Delivery function. Use this function to configure the way the SEBea/NET-PATH remote agent manages action delivery for each device type used for delivering actions:

- Serial port
- Modem
- Network

To create an enhanced action delivery record

1 Click the **Enhanced Action Delivery** tab.



2 Select a severity level from the **Delay the delivery of actions...** list; then, type the delay in seconds before proceeding with less important actions in the adjacent box. The system defaults to zero if a value is not entered.

The severity refers to the severity of the event that triggered the action. The action takes the severity from the event.



Note *If an action occurs with a severity greater than that specified, that action reports immediately. If you specify grouping (see Maximum Number of Actions below) and there are actions within the specified severity range waiting, those actions will be delivered at the same time (up to the maximum number specified).*

3 Type the number of actions that should be grouped together when more than one action specifies delivery to the same destination in the **Group a maximum of...** field. The system defaults to zero if a value is not entered.



Note *The maximum number of actions to process per delivery is extremely important. For example, in cases where the delivery destination is a fax machine, delivering multiple faxes could tie up the SEBea/NET-PATH modem and prevent the SEBea/NET-PATH from delivering other events.*

4 Click the ***Save*** button on the toolbar.



Example

Look at the previous figure. Assume a report action called IRISReport uses the first available modem to deliver events to IRISnGEN and has an assigned severity of Low. Six events occur that use the IRISReport action. Two events queue for Modem1 and four events queue for Modem2. Three minutes pass and an event occurs that uses a High severity action associated with Modem2. The High severity action begins immediately. IRISnGEN checks to see if there are other actions pending in the Modem2 queue that deliver to the same destination. If all four of the pending actions specify the same destination, then three of those are delivered in addition to the High severity action event (three is the maximum specified in the figure above). The remaining action is kept in queue until the next higher severity action or until the timeout expires.

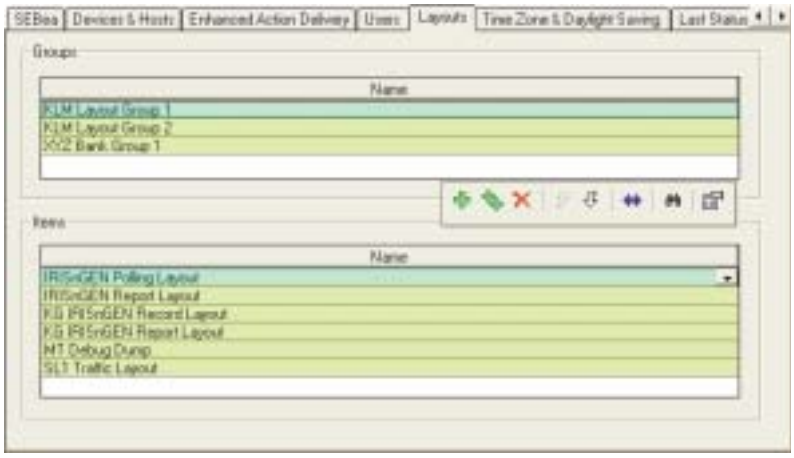
Meanwhile, the two low severity actions pending in the Modem1 queue are still awaiting delivery. The actions will proceed once the timeout period is reached for the oldest entry in the queue, or when a higher severity action uses Modem1 to deliver to the same destination. The queue will only be checked for new entries to combine before delivery. Once delivery starts, new entries will be grouped and stored for the next delivery time.

Layouts Tab

Use this tab to define the layouts (Items) or layout groups(Groups) that can access the host.

To create a layout record

1. Click the **Layouts** tab.



2. Select a group to grant access rights yo the current host from the **Group** list. For more information about groups, see 'User Groups', page 6-118.
3. Select an individual layout grant access rights to the current host from the **Items** list. For more information about users, see 'Layouts', page 6-93.
4. Click the ***Save*** button on the toolbar.

To add a layout group

1. Click inside the **Name** field under the Groups section.
2. Click to add a blank row , or click to add multiple groups.
3. Select a group from the list.
4. Repeat steps 2 and 3 to add additional groups.

To add a layout

1. Click inside the **Name** field under the Items section.
2. Click to insert a blank row, or click to add multiple users.
3. Select a user from the list.
4. Repeat steps 2 and 3 to add additional users.

Last Status Tab

Use the Last Status option to display the last status received from the remote agent. It contains hardware and boot information, as well as database and operating system information. The system updates the display each time you select the tab. The following figure shows a typical last status display.



SEB II Remote Agent Tab

Use the SEB II tab to configure and manage SEB II remote agents.

To add SEB II information

1 Right-click the site name in the tree view and select **Add SEB II**. The system opens the SEB II tab.



2 Type a unique name to identify the SEB II remote agent in the **Name** field. The IRISnGEN system references the SEB II device by this name. This is a required field.



Warning *Be careful when using special characters 129 (0x81) though 143 (0x8F) and 152 (0x98) though 159 (0x9F). The characters are* **ƒ„…†‡ˆ‰Š‹Œ_** *and* **˜™š›œ_Ÿ**. *The characters appear correctly in record, but will appear as the* **|** *character in the IRISnGEN tree view.*

3 Type the same name as in the previous field or a different name in the **Embedded Name** field. The embedded name is the name the SEB II remote agent uses to identify itself when sending alarms to the IRISnGEN system. Entering a different name adds another level of security to the system. Up to ten characters can be entered. This field is required.

4 Type the SEB II remote agent's password in the **Password** field. Up to twenty characters can be entered. This field is required.

5 If necessary, type the new password for the SEB II remote agent in the **New Password** field. The new password becomes effective the next time a database is downloaded to the SEB II remote agent. Changing this password marks the database as "dirty," as applicable in the ASM functions.

6 Select a model for the SEB II remote agent from the **SEB Model** list. The system populates the Devices & Hosts tabs with generic named devices available for this remote agent. The models are pre-configured at the factory. This field is required.

7 Select the SEB II ASP (Application Specific Program) version from the **Application (ASP)** list. ASP is the software that controls the available SEB II database options.

8 Type a self-check time for this remote agent to call the IRISnGEN system in the **Self Check Time** field. Stagger the self-check times for the remote agents so that the modems are not overloaded with calls. Enter time in 24-hour format.

9 Select available poll schedules from the **Poll Schedule** list if you want to periodically poll the entire contents of this remote agent.

To add Modem Information

1 Type the number or group of numbers required to dial an outside line in the **Phone Prefix** field, if the PBX requires you to dial a special prefix (such as the number 9) to access an outside line. A comma denotes a two-second pause.

2 Type the telephone number used to contact the remote agent in the **Phone Number** field.

3 Type any suffix dialed to reach the remote agent, such as an authorization code, in the **Phone Suffix** field. A comma denotes a two-second pause.

Suppose the remote agent is not connected to a dedicated phone line, but is assigned to an extension number, for example, extension 7408. You would need to dial the extension number after the main phone to reach the device. In that case, your phone suffix is 7408.

4 Select a baud rate from the **Modem Speed** list. This is the maximum baud rate at which the SEB II is expected to communicate. Baud rates range from 300 to 57600.



To add Configuration Flags and notes

1 Make a selection:

Select	When
High Speed/External Modem	The remote agent has a high speed (14.4KBPS) modem or a true external modem. ***Note*** *The 14.4 KBPS modem board does not physically reside on the SEB motherboard. It is external to its motherboard.*
Poll if Full	You want the system to automatically poll this device (must be an SEB) when a memory full message (FE12 memory alarm) is delivered to the IRISnGEN system. When SEB II devices are full, they overwrite older data. If you want to prevent data loss, always check this box and program the SEB II to deliver the FE12 event.
Daylight Savings	The remote agent resides in an area where Daylight Savings Time is observed.
Enable Polling	You want to enable scheduled polling of this remote agent. If you do not enable polling, the IRISnGEN system does not contact this device to extract information. Enable polling for any remote agent that you schedule for regular polling
Exclude from ASM Activity	You do not wish to include this remote agent in the automated site management process.
Exclude from Activity Reporting	You want to exclude this remote agent from the Sites Not Reporting report. Checking this box also disables the color change function for the icon that represents this remote agent in the Equipment Explorer. For example, it prevents an icon from turning red when the site fails to respond.

2 Click the ***Save*** button on the toolbar.

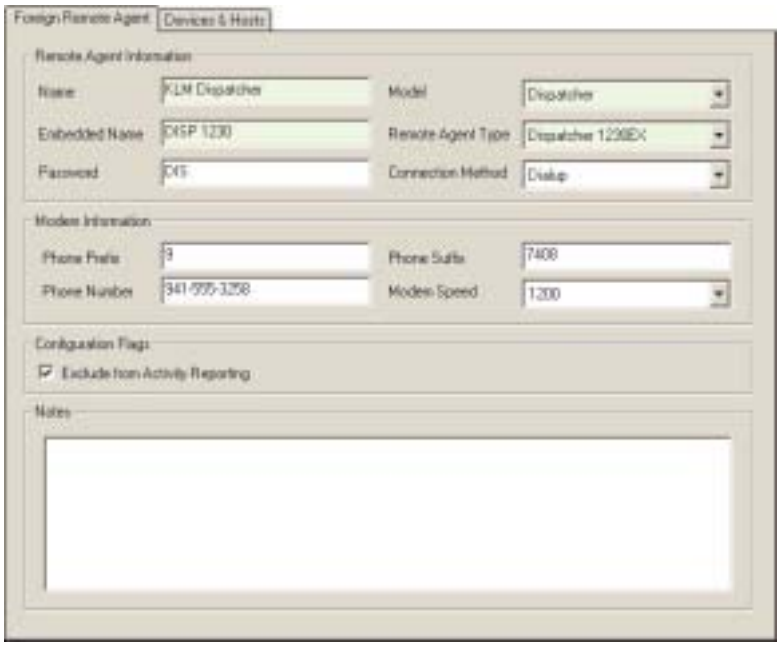


Foreign Remote Agent Tab

Use the Foreign Remote Agent tab to configure and manage foreign remote agents.

To add foreign remote agent information

1 Right-click the site name in the tree view and choose **Add Foreign Agent**. The Foreign Remote Agent tab opens.



2 Type a name to for the foreign remote agent in the **Name** field.



Warning *Be careful when using special characters 129 (0x81) though 143 (0x8F) and 152 (0x98) though 159 (0x9F). The characters are* **ƒ„…†‡ˆ‰Š‹Œ_** *and* **˜™š›œ_Ÿ***. The characters appear correctly in record, but will appear as the* **|** *character in the IRISnGEN tree view.*

3 Type a name that identifies the embedded name of the foreign remote agent in the **Embedded Name** field. The foreign device uses this name to identify itself when it sends alarms to the IRISnGEN system. Up to ten characters can be entered.

4 Type the foreign remote agent's password in the **Password** field.

5 Select a model for the foreign remote agent from the **Model** list.

6 Select a foreign agent type from the **Remote Agent Type** list.

7 Select one of the following from the **Connection Method** list:

- Dialup, a modem-to-modem connection
- Dialup Protocol, a modem connection using the SEB II protocol
- Network, a TCP IP connection
- Network Protocol, a network connection using the SEB II protocol
- Telnet, a standard Telnet connection protocol

The connection method identifies how the IRISnGEN system connects to the foreign remote agent.



To add Modem information, configuration flags, and notes

1. Type the number or group of numbers required to dial an outside line in the **Phone Prefix** field, if the PBX requires you to dial a special prefix (such as the number 9) to access an outside line. A comma denotes a two-second pause.
2. Type the telephone number used to contact the remote agent in the **Phone Number** field.
3. Type any suffix dialed to reach the remote agent, such as an authorization code, in the **Phone Suffix** field. A comma denotes a two-second pause.

   Suppose the remote agent is not connected to a dedicated phone line, but is assigned to an extension number, for example, extension 7408. You would need to dial the extension number after the main phone to reach the device. In that case, your phone suffix is 7408.
4. Select a baud rate from the **Modem Speed** list. This is the maximum baud rate at which the SEB II is expected to communicate. Baud rates range from 300 to 57600.
5. Select the **Exclude from Activity Reporting** checkbox to exclude this remote agent from the Sites Not Reporting report. Selecting this checkbox also disables the color change function for the icon that represents this remote agent in the Equipment Explorer. For example, it prevents an icon from turning red when the site fails to respond.
6. Type any description or comments, such as why and when you created the record, and its purpose in the **Notes** field. This is an optional field and allows a maximum of 256 characters.
7. Click the ***Save*** button on the toolbar.



Notes



3

IRIS Administration

Overview

The IRIS Administration folder contains several sub-folders, each containing a collection of component records that you can use to control your IRISnGEN system. These sub-folders include:

- **Alarm Colors** defines the foreground and background colors of alarm displayed in the Alarm Viewer.
- **Communications** defines the IRISnGEN modem parameters and operations.
- **Day/Night Forward Selectors** lists the forward selectors used to forward alarms during day and night modes.
- **Day/Night Mode** lists the schedules used to identify when to forward alarm in day and night modes.
- **Enhanced Authentication** provides two-factor authentication to strengthen IRISnGEN's security
- **Processing Applications** lists the programs running in the IRISnGEN system and determines the storage location (file, folder, or database) for incoming event data.
- **System Parameters** lists the component used to associate a set of characteristics with IRISnGEN.
- **User Defined Fields** adds unique fields to customer, site, and host records.
- **User Groups** lists group names with specific sets of permissions for accessing the IRISnGEN system functions.
- **Users** define users in your IRISnGEN system and their associated permissions.
- **Zip Codes** defines the zip codes used in your IRISnGEN system.

Alarm Colors

You can change the foreground and background colors for the alarms that appear in the Alarm Viewer. You cannot add or delete alarms or change alarm status or severity in this window, only change the display colors.

To edit alarm colors

1. Expand the **IRIS Administration** folder.
2. Expand the **Alarm Color** folder and select an alarm from the list. The system opens the Alarm Color tab for that alarm.
3. Select a background color from the **Background Color** list.
4. Select a foreground color from the **Foreground Color** list. Notice your choices display in the Sample field to the right.
5. Save your changes.

Communications

The Communications folder contains a collection of configuration parameter records for all the modems and communication operations in your IRISnGEN. The configuration parameters tell IRISnGEN how the modems are to operate when communicating with the remote agents.

The Communications folder contains four sub-folders. These sub-folders include:

- Communication Operations
- Modem Types
- Port Groups
- Ports

Select a sub-folder to display its configuration parameter records.

Communication Operations

You can define the types of operations that your modems perform. This lets you group and prioritize activities, making sure your most important functions complete before your less critical tasks.



Note *Your IRISnGEN software came with basic operations already defined in the database. Making changes to the software can cause adverse results. Please contact Teltronics before making any changes.*

To edit a communication operations record

1 Expand the **Communications Operations** folder and click an operation to select it—for example, click **Forward Alarm**. The system opens the Communication Operation tab.



2 Type the name of the record, as assigned by the factory, in the **Name** field.

3 Type the time (in minutes) that the system is to wait between repeated attempts to complete the call in the **Retry Interval** field.

4 Type the priority level (1- 255) for your record in the **Default Priority** field. IRISnGEN processes the operations with the highest priority number (1) first.

5 Type the number of retries (1 – 99) to complete the operation in the **Retry Count** field. You must leave the field blank for Listen group.

6 Type a description of the record in the **Notes** field. You can type up to 256 characters.



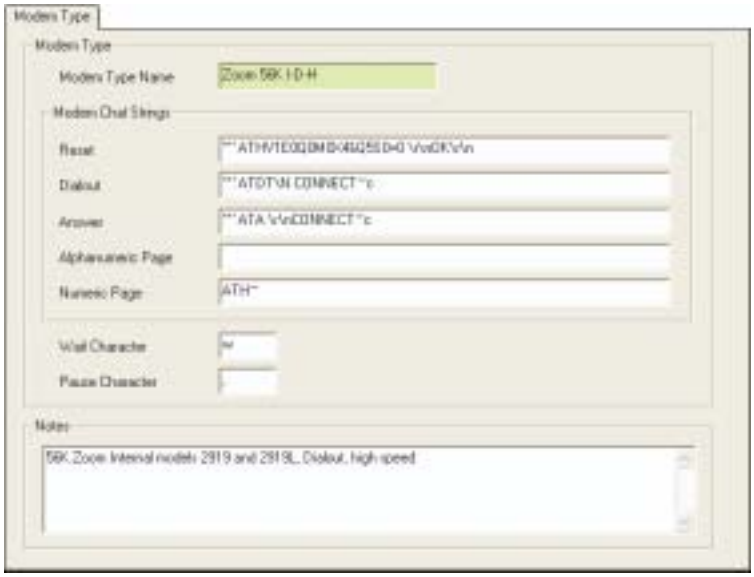
When IRISnGEN detects a busy signal during an outgoing call, it retries the call based on the retry parameters set in the Port Group record. When it reaches the retry limits set in Port Groups record, it waits the time specified in the Operations record Retry Delay field, then starts the Port Group retries again. IRISnGEN repeats this cycle until it completes the call or reaches the Retry Count limit in the Operations record. IRISnGEN creates an internal alarm for failed calls. The Port Group retry parameters apply to busy signals, only. All other communication problems use the retry interval and retry counts defined in the Operations record.

Modem Types

The IRISnGEN system lets you logically group modems based on the devices they communicate with and by the types of operations that you can perform while online. Modem groups support a variety of remote agents and modem combinations. You should create a modem type record for each kind of modem that you use to communicate, such as Zoom 56K.

To create a modem type record

1 Right-click the **Modem Type** folder and select **Add Modem Type**. The system opens the Modem Type tab.



2 Type the name of your modem in the **Modem Type Name** field.

3 Type the modem character strings in the next five fields. Include:

Field	What to enter
Reset	The command string used to reset the modem. Refer to your modem user manual for information about these commands.
Dialout	Type the following dial-out command string. “ “ ATDT\N CONNECT~c

Answer	Type the following answer command string. `"" ATA\r\n CONNECT~c` Determine whether to enter the answer string by the port where you assign the modem type. If it is a dial-out port, the answer string is never used.
Alphanumeric Page	Type the paging code. The paging code has its own initialization strings, depending on the type of modem it finds. However, if the paging modem needs a special string to initialize, you can use this field to set an override initialization string.
Numeric Page	Type the init string that is sent to the modem before dialing out to a numeric pager.

4 Type the character used in command strings to indicate that the modem should wait (usually for a response from the remote modem or for connection tone) in the **Wait Character** field. In Hayes-compatible modems, this character is **w**.

5 Type the character used in command strings in the **Pause Character** field to indicate that the modem should pause before continuing. For example, put a pause character after the dial-out access code to signal the system to wait for a dial tone before dialing the phone number. In Hayes-compatible modems, this character is a comma (,), a two second pause.

6 Type any description in the **Notes** field, such as record information. The maximum length is 256 characters.

Port Groups

Use the Port Groups option to logically group modems based on the devices they communicate with, and by the types of operations that you will perform while online. You can group them by assigning them to port groups defined as Dialout or Listen. This allows you to easily support a variety of remote agents and modem combinations.

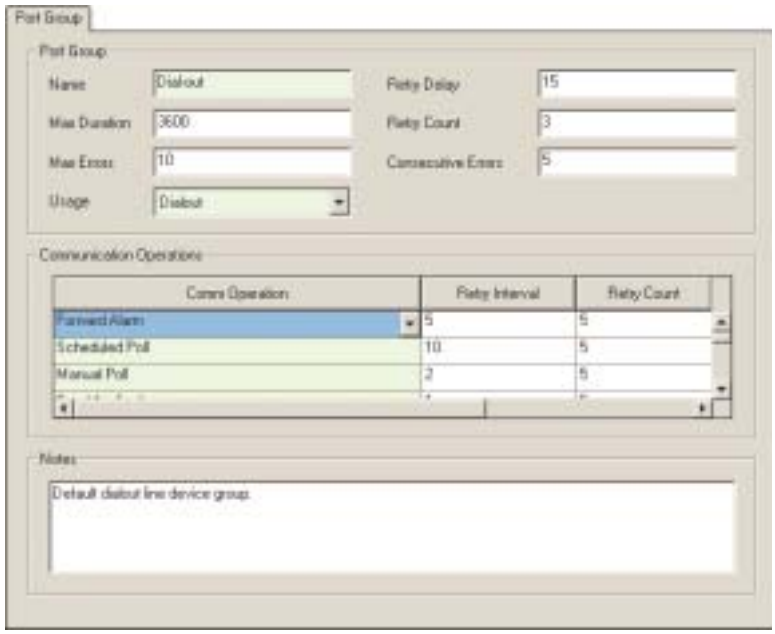


Note *Teltronics ships your database with two port groups already assigned: Dialout and Listen.*



To create a port group record

1 Right-click the **Port Groups** folder and choose **Add Port Group**. The system opens the Port Group tab.



2 Type the name for the port group you are defining in the **Name** field.

3 Type the time (in seconds) that the system waits between repeated attempts to complete the call in the **Retry Delay** field.

4 Type the maximum time (in seconds) that a call can be active in the **Max Duration** field.



Note *For the Dialout group, be sure to allow enough time for completion of an automatic poll. For the Listen group, allow sufficient time to receive multiple alarms or alarms with large attachments.*

5 Type the number of times you want the system to try to complete the call in the **Retry Count** field.

6 Type the maximum number of errors the system will allow before terminating the call in the **Max Errors** field. For example, assume you enter **10.** After the tenth error, the system ends the call. If you want the system to keep the connection open, regardless of errors, leave this field blank.

The Port Groups retry parameters apply to busy signals, only. All other communication problems use the retry interval and retry counts defined in the Operations record. When IRISnGEN detects a busy signal during an outgoing call, it retries the call based on the retry parameters set in the Port Groups. When it reaches the retry limits set in Port Groups record, it waits the time specified in the Operations record Retry Delay field, then starts the Port Group retries again. This cycle is one Operation record retry count. IRISnGEN repeats this cycle until it completes the call or reaches the Retry Count limits in the Operations record. IRISnGEN creates an internal alarm for failed calls.

7 Type the number of consecutive errors that the system tolerates before shutting down communication in the **Consecutive Errors** field. For example, assume you enter **10**, then after the tenth consecutive error, the system hangs up the call. If you want the system to keep the connection open, regardless of errors, leave this field blank

8 Select *Listen*, *Dialout*, or *Disabled* from the **Usage** list. This defines whether modems in this port group receive calls (listen), make calls (dial), or are not used by IRISnGEN (disabled).

9 Click inside the Communication Operations data table and Click the button to add a row; then select an operation from the Comm Operation list. Assign the Listen Comm Operation to port groups that will be used exclusively for listening.

10 Type any descriptions or comments in the **Notes** field. The maximum length is 256 characters.



Ports

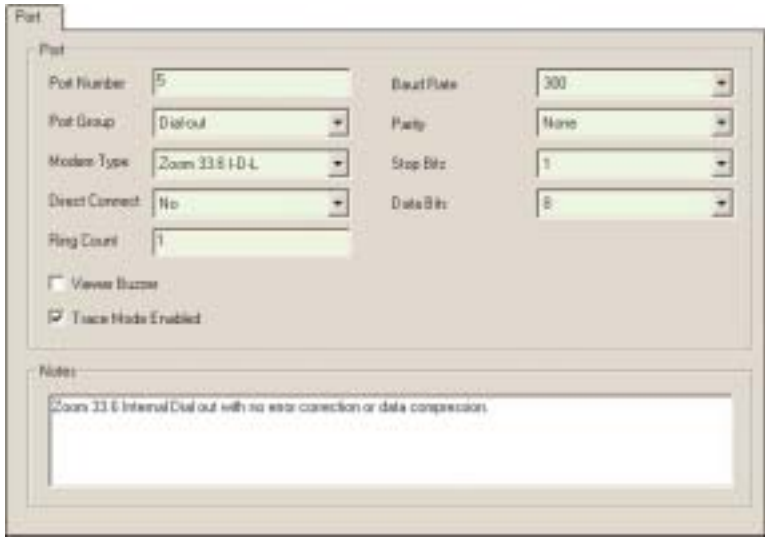
You can define the ports on your IRISnGEN server in your port records. Through these ports, you communicate with your remote hosts.



Note *You must define your port groups and modem types before creating a port record. See defining port groups and defining modem types.*

To create a port record

1 Right-click the **Ports** folder and choose **Add Port**. The system opens the Port tab.



2 Type the port number to define the serial port on your IRISnGEN server in the **Port Number** field. The port number must match the physical port to which this modem is attached. IRISnGEN is often configured with available ports beginning with Com 5. Check with Teltronics Customer Service to confirm your specific configuration.

3 Fill in the fields on the tab to define your port record. The following list describes the fields on the Port tab.

Field	Definition
Port Group	Select ports to organize into groups: Dialout, Listen, Disabled, Pagers Plus Listener Groups, or user-defined groups.
Modem Type	Select a modem type from the list. This modem type should have a corresponding initialization string for this physical modem. The Modem Type must match the modem physically attached to the port.
Direct Connect	Select **No**.
Baud Rate	Select the highest baud rate available for this modem. Baud rates range from 300 to 115200.
Parity	Select one of the five parity options. Most SEB remote agents operate with a parity of None. For other devices, check with your user's manual. Parity seldom ever needs to be changed from the default of None.
Stop Bits	Select 1 stop bit for SEB II and SEBea remote agents.
Data Bits	Select 7 or 8. Most SEBs operate with 8 data bits.



Note *Data bits are the number of bits in a byte that are used for communication. Often the eighth bit is used as a parity check, making that bit unavailable for communication. If you have selected a parity of None, then set your data bits for 8. If you have selected a parity of odd or even, then set your data bits for 7.*

4 Type the maximum number of times the line is permitted to ring before the modem answers in the **Ring Count** field. Usually, the port ring count is set to 1.

5 Select the **Viewer Buzzer** checkbox to enable the VBUZZER application. Viewer buzzer requires a physical connection to one of the communications ports and an external buzzer or light. The connected buzzer or light is triggered each time an alarm reaches the viewer.

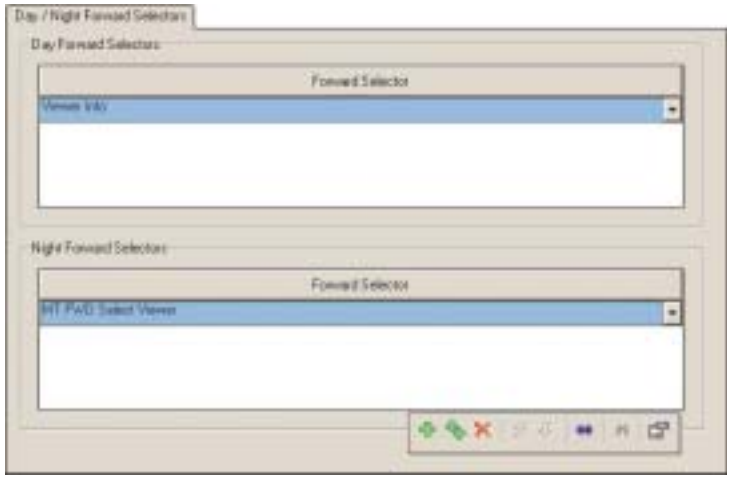
6 Select the **Trace Mode Enabled** checkbox to enable Trace mode. Trace mode is a very important troubleshooting tool for setting up new ports or finding data collection problems with existing ports. The trace file shows information on data going in both directions on the port. It also shows the status of leads, similar to a data analyzer. Click the **Trace Mode Enabled** checkbox to enable this feature. The system pre-allocates the drive space for the trace log according to LOG_SIZE parameter in System Parameters.

7 Type any description or comments in the **Notes** field. The maximum length is 256 characters.



Day/Night Forward Selectors

You can choose where you want your alarms and other event data to go during the day and night. Day/Night forward selectors are most often used to forward alarms to the Alarm Viewer during the day or to an on-call technician's pager after hours. Night service cut-over is automatic based on an assigned schedule.



- Assign forward selectors from the Forward Selectors list.
- An icon on the viewer list and geographical viewer indicates if the system is in normal or night service mode. It also appears in the Day/Night Mode window.
- As forward selectors are added and removed from this section, they are also added and removed from the active or queued forward selectors lists.

To create a forward selector record

1. Click inside the **Day Forward Selectors** data table.
2. Click the ✚ button to insert a new line into the table.
3. Select a forward selector from the list.
4. Repeat steps 2 and 3 to add more forward selectors.
5. Click inside the **Night Forward Selectors** data table.
6. Click the ✚ button to insert a new line into the table.
7. Select a forward selector from the list.
8. Repeat steps 6 and 7 to add more forward selectors.
9. Save your record.

You can define both daytime and nighttime forward selectors and assign several selectors to the day/night service. In other words, you can have many active forwarding scenarios based on normal and non-business hours.

This feature automatically starts when the schedule transitions to the next mode (from day to night or night to day). A simple way to activate new changes manually is to toggle from day to night, back to day, or night to day and back to night. The viewer displays a sun icon on the viewer during day mode and a moon icon during night mode.

Day/Night Mode

When you select this option, you will see either a sun or moon in the right-hand corner. It indicates the system is currently in day (sun) or night (moon) mode. The Alarm Viewer also displays these icons.

You can define both day and night forward selectors and assign several selectors to the day/night service. In other words, you can have many active forwarding scenarios based on normal business hours and after-business hours.

Day/Night Mode automatically starts when the schedule transitions to the next mode (from day to night, or night to day). A simple way to activate new changes is to toggle from day to night, then back to day (or, if night is the current mode, toggle from night to day and back to night).

To create a day/night mode record

1 Click the **Day/Night Mode** folder. The system opens the Day/Night Mode tab.



2 Select a day schedule from the **Day Forward Schedule** list.

Enhanced Authentication

Teltronics offers the optional Enhanced Authentication module to promote a greater level of security in IRISnGEN when accessing remote agent devices (SEBea and NET-PATH). The Enhanced Authentication module incorporates the Digipass Software from VASCO Data Security, Inc. and extends authentication beyond static IDs and passwords, and uniquely authenticates users before granting them network access over dial-up, ISDN, on-LAN, Internet, or intranet connections. The module uses a standards-based challenge/response technology to create a one-time password that is far more secure than static passwords.

The Enhanced Authentication module provides two-factor authentication to strengthen IRISnGEN's security by requiring a token issued by the security administrator and a PIN to enable the token. The token computes a one-time password when challenged by the remote agent device. Without the authorized user's unique token and PIN to activate the token, potential intruders cannot compute the one-time password. No damage can be done even if the password is captured. Once used, the password is never again valid.

The Enhanced Authentication module includes two token types: the software token, referred to as a system token; and a hand-held token, referred to as a security token. A system token eliminates the need for a user to carry a separate hand-held security token. The user's laptop computer or PC becomes a token when the Enhanced Authentication module is active. A system token is just as secure as and easier to use than a hand-held security token. The system token is transparent to the user and therefore not easily lost or stolen. A system token is ideal for users who employ a single device to log on to the network, whereas security tokens are best utilized by users who frequently log on from many different devices at many different remote locations and who frequently log on with a transparent connection.



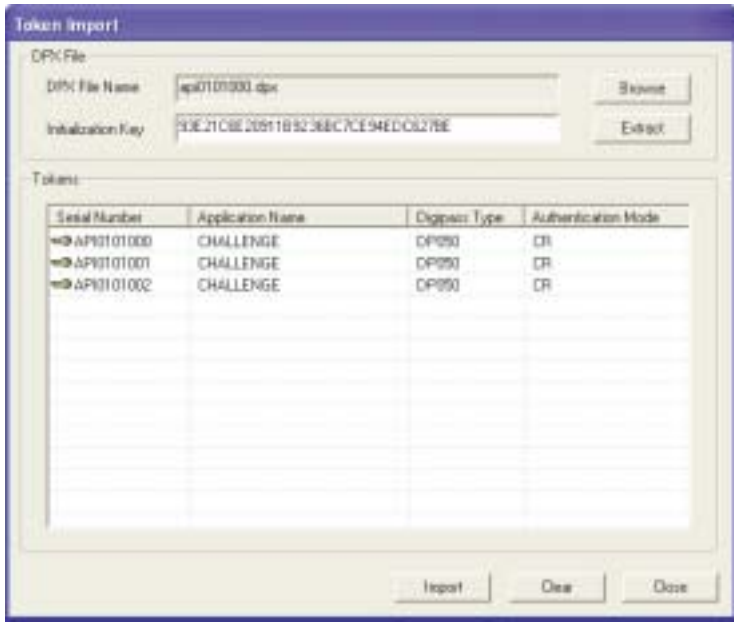
When enabled for remote agent devices, IRISnGEN uses a Challenge/Response method to control access to those devices. As the user logs into the system, the remote agent displays a challenge to which the user must respond. For system tokens, this procedure is completely automatic and unseen by the user. For security tokens, the user must enter the challenge into the security token device to receive a response code. The user then types the response code in at the system prompt to gain access to the remote agent device.

Importing System and Security Tokens

Before using Enhanced Authentication, you must first import the system and security tokens into IRISnGEN. You must import at least one system token before you can import a security token. The process involves extracting the necessary data from the .DPX file. Initially, you can place the .DPX file in any folder accessible by IRISnGEN. Then, during the import process, IRISnGEN copies the .DPX file to the IRISHOME/TOKENS directory. It is from this directory that IRISnGEN imports each token. Once the import process completes, it is a good idea to delete the .DPX file from the original folder, since leaving it could compromise security, if the original folder is easily accessible. Remember, you will have a copy of the .DPX file in the IRISHOME/TOKENS directory.

To import a system token

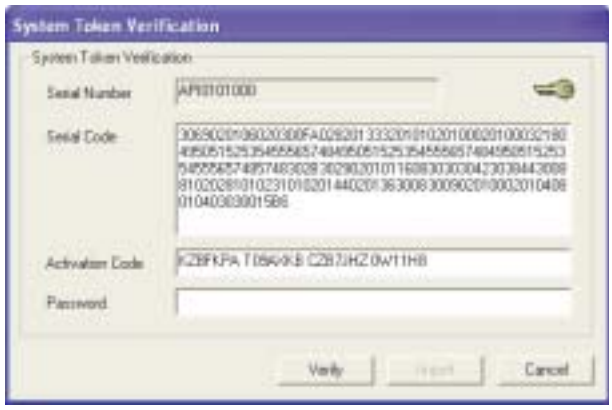
1. Copy the .DPX file to a folder accessible to IRISnGEN.
2. Right-click **System Token** folder (IRIS Admin > Enhanced Auth > IRISnGEN System Tokens) and select Import IRISnGEN System Tokens. The system opens the Import Token dialog for system tokens.



3. Click ***Browse*** and navigate to the location of the stored .DPX file.
4. Select the appropriate .DPX file. IRISnGEN does the following:
   - copies the file to the IRISHOME/TOKENS directory
   - places the file name in the .DPX File Name field
   - activates the Initialization Key field and Extract button
5. Type the initialization key supplied by Teltronics in the **Initialization Key** field and click ***Extract***. The system display token information in the Tokens data table.

6 Repeat steps 3 through 5 for each additional token. You can add up to five tokens to your list. Once you have added your tokens, you can begin to import them into your IRISnGEN system.

7 Click a icon in the Tokens data table to select it, and then click ***Import***. The system opens the System Token Verification dialog.



8 Type the input supplied by Teltronics in the **Serial Number**, **Activation Code**, and **Password** fields. You can find this input in the security file included in your Enhanced Authentication package.

9 Do one of the following:

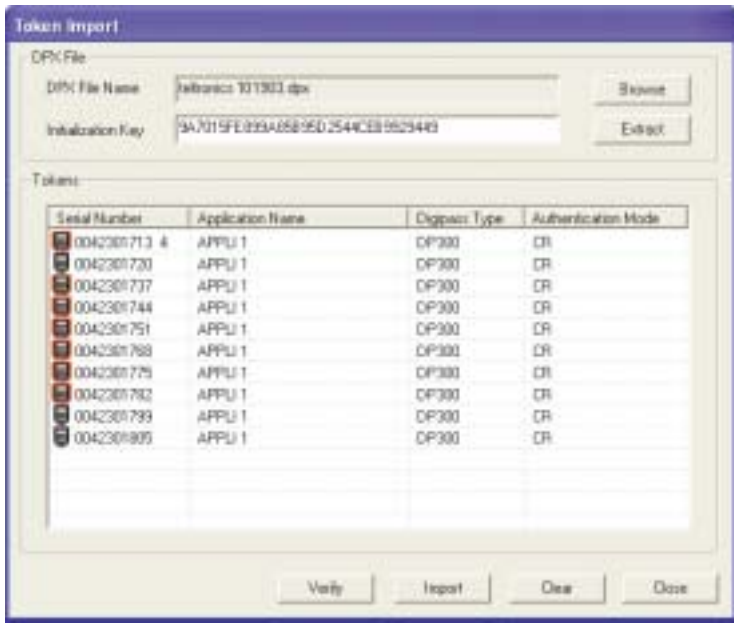
- Click ***Import*** to verify the token and begin the import process automatically.
- Click ***Verify*** to verify the token manually, without importing it.



Note *You must import at least one system token before you can import a security token.*

To import a security token

1 Right-click the **Security Token** folder (IRIS Administration > Enhanced Authorization > IRISnGEN System Tokens) and select Import IRISnGEN Security Tokens. The system opens the Import Token dialog for security tokens.



2 Click ***Browse*** and navigate to the location of the stored DPX file.

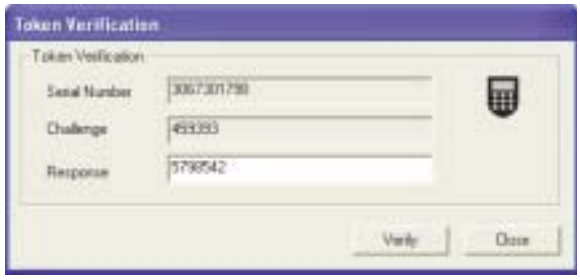
3 Select the appropriate DPX file. IRISnGEN does the following:

- copies the file to the IRISHOME/TOKENS directory
- places the file name in the DPX File Name field
- activates the Initialization Key field and Extract button

4 Type the initialization key supplied by Teltronics in the **Initialization Key** field and click ***Extract***. The system displays token information for all security tokens contained in the DPX file in the Tokens data table.

5 Select an icon(s) in the Tokens data table, and then do one of the following:

- Click ***Import*** to verify the token and begin the import process automatically
- Click ***Verify*** to verify the token manually, without importing it. The system opens the Token Verification dialog.



6 Type the challenge displayed in the **Challenge** field into your security token device, then enter the response from that challenge in the **Response** field.

Deleting System and Security Tokens

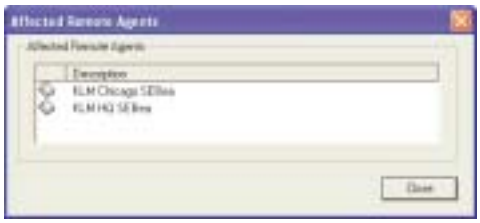
You can delete a system or security token from the IRISnGEN system. Once deleted, you can only restore the token by importing it again.

To delete a system token

1 Right-click a token icon from the tree view and select ***Delete***. The system opens the Delete dialog.



2 Click ***Show Agents*** to display a list of all remote agents referencing this token. This list is for informational purposes, only.

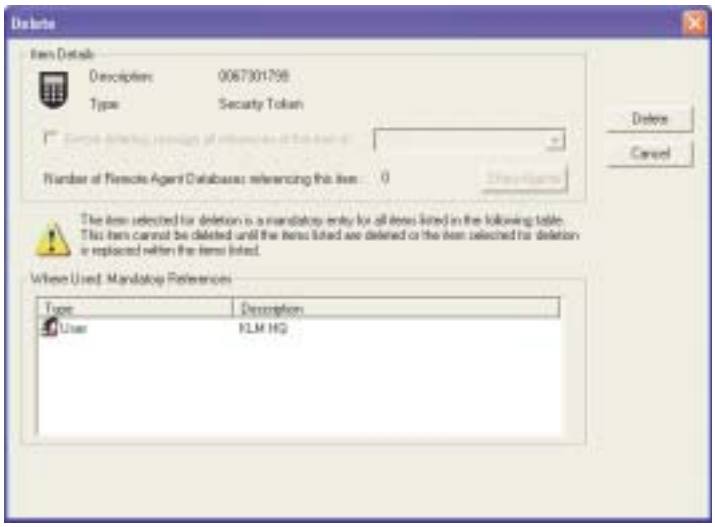


3 Click ***Close*** to close the Affected Remote Agents dialog.

4 Click ***Delete*** to remove the token from the system.

To delete a security token

1 Right-click a token icon from the tree view and select ***Delete***. You can only delete tokens that have been in the system for more than thirty days. The system opens the Delete dialog.



2 Note the users listed in the Where Used Mandatory Referenced data table. You must remove them prior to deleting the token.

3 Click ***Cancel*** to exit the Delete dialog.

4 Go to the Remote Agent Library's User folder (Remote Agent Libraries > Security Libraries > User) and select the user listed in the in the Delete dialog data table.

5 Select <none> from the **Security Token** list.

6 Repeat steps 4 and 5 for each user in the dialog table.

7 Exit the User tab by right-clicking the token icon in the Security Token list and selecting ***Delete***.

8 If there are no more users listed in the data table, click ***Delete***. IRISnGEN removes the token from the list.

Enabling Enhanced Authentication in the Remote Agent

To use Enhanced Authentication, you must be licensed for Enhanced Authentication in your IRISnGEN license.xml file and for each remote agent license key that you wish to enable.

To enable Enhanced Authentication in a remote agent device

1 Open the **Site** folder (Customer > Site) and select a remote agent device from the tree view. The system opens the Remote Agent tab.

2 Select the **Enhanced Authentication** checkbox in the Configuration Options.



3 Exit the tab.

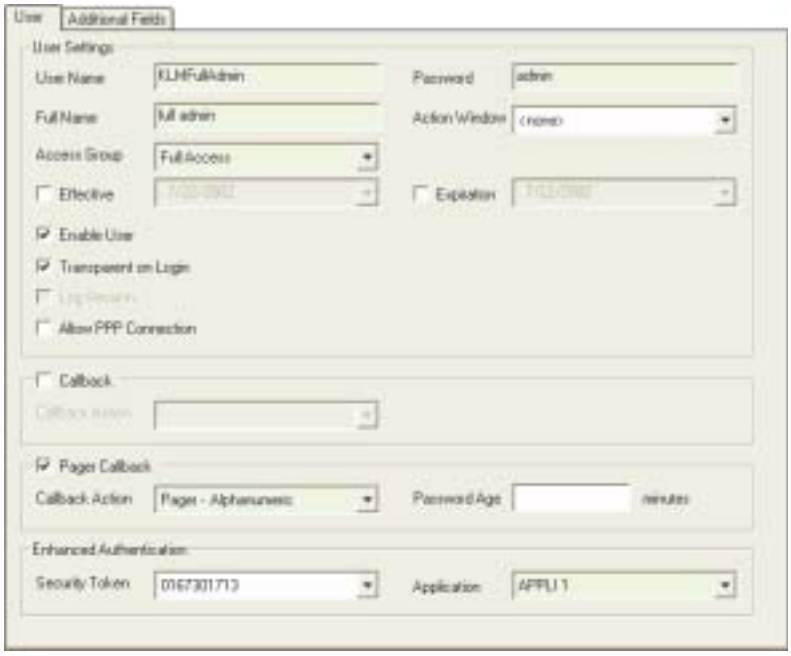
Assigning a Security Token to a Remote Agent User

Use the Enhanced Authentication fields in the Remote Agent Libraries' User tab to assign a security token to a user. This information is included in the Remote Agent database that will be downloaded to the remote agent as part of the normal download process. You can assign a single security token to multiple users.

A remote agent user can access remote agent devices using normal authentication (user name and password) or Enhanced Authentication (security tokens). The remote agent which the user is assigned determines which authentication method is used. If the Enhanced Authentication fields contain entries, then the user is authorized to use Enhanced Authentication. If the fields contain no entries, the user is authorized to access only remote agents that do not support Enhanced Authentication. Users with Enhanced Authentication privileges can still access remote agents not supporting Enhanced Authentication.

To assign a security token to a remote agent user

1 Select a user from Remote Agent Libraries' **User** folder (Remote Agent Libraries > Security Libraries > User). The system opens the User tab.



2 Select a security token from the **Security Token** list. The system automatically enters the application for that token in the **Application** field.

3 Exit the User folder.



Note *Enhanced Authentication overrides Pager Callback. Remote agent devices enabled with Enhanced Authentication will not call back a remote agent user. Only remote agent devices using normal authentication use Pager Callback.*

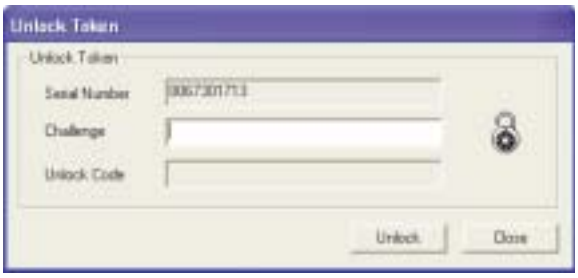


Unlocking a Security Token

A user has five tries to enter the correct PIN number into a security token. If, after the fifth try, the user still has not entered the correct PIN number, the security token locks and displays a challenge number in the Display field. Once locked, the token can only be unlocked by a system administrator using this challenge number.

To unlock a security token

1. Open the **Security Tokens** folder in the IRISnGEN menu view.
2. Right-click the icon with the serial number matching the locked token and select **Unlock Token**. The system opens the Unlock Token dialog.



3. Type the challenge number from the security token in the **Challenge** field. The challenge number displays automatically on the security token when it becomes locked.
4. Click ***Unlock***. IRISnGEN displays an unlock code in the Unlock Code field.
5. Using the security token's keypad, enter the unlock code into the token.
6. When prompted by the token, enter a new four-digit PIN number. The security token is now ready for use.



Note *Should the Unlock operation fail, the security token automatically inactivates for twenty-four hours at which time you can try again. Any attempts to unlock the token before the inactivation period is over will be unsuccessful.*

Remote Agent Access

When enabled, Enhanced Authentication uses the Challenge/Response method to access all the remote agent. The remote agent will reject any user not authorized for Enhanced Authentication (no token assigned to the user).

When a user enters his or her name at login, the remote agent generates a random challenge number, which displays for the user. The user must enter this challenge into his or her handheld security token to produce a response. The user then enters the response at the SEBea or NET-PATH prompt so the remote agent device can verify the response. If the response is correct, access is granted; otherwise, access is denied.



Note *If Enhanced Authentication is enabled, the Secure Login method (login –s) to the remote agent will be disabled.*

Remote Agent User Access

The remote agent user can gain access to the remote agent from IRISnGEN via Protocol. IRISnGEN automatically generates responses for the challenges produced by the remote agent. The remote agent user also is used for network downloads (Telnet) from IRISnGEN to the remote agent.

Non-Protocol Access

All non-protocol access to the remote agent uses the following access methods:

- Command line using Serial access
- Command line using Modem access
- Telnet using Modem PPP access
- Telnet using Network access

The Challenge Response access will work as follows:

```
SEBea> login
Username: Bob
Challenge: 4537423
Response: 2334711

SEBea>
```

The following matrix describes non-protocol login with no Enhanced Authentication.

Login Command	Description
login	Username prompt displays for the user. When the user enters the username, the Password prompt displays. The remote agent does not echo the password to the user. If the username and password are correct, the remote agent prompt displays for the user. login Username: Bob Password: SEBea>



The following matrix describes non-protocol login with Enhanced Authentication.

Login Command	Description
login	Username prompt displays for the user. When the user enters the username, the Password prompt displays. The remote agent does not echo the password to the user. If the username and password are correct, the remote agent prompt displays for the user. login Username: Bob Challenge: 1445874 Response: 0208926 SEBea>

The following matrix describes a non-protocol login in the DEFAULT state. When in the default state, the remote agent automatically turns off Enhanced Authentication.

Login Command	Description
login	The remote agent automatically logs in using the DEFAULT state username and password. Only limited commands are available. The Remote Agent prompt displays for the user. login SEBea>

Multiple Challenge Response

The remote agent device is equipped to generate multiple challenges when the security token is programmed for multiple challenges. The challenges display as a list of values separated by a comma. The user must enter the challenges into the token one by one. The token generates a single response once all the challenges are entered. The user then enters the single response generated by the token at the prompt to gain access to the remote agent.



The Multiple Challenge/Response is used only for non-protocol access using the security tokens. The Multiple Challenge/Response access works as follows:

```
SEBea>login
Username: BillyBob
Challenge: 453123,456123,786625
Response: 2347187

SEBea>
```

Protocol Access

Users can access SEBea remote agent devices in protocol using Remote Agent Manager. Users can also perform manual and scheduled polling with authentication.

Scheduler Access

The Scheduler Access works without using the Challenge/Response authentication method. User may need to use the Scheduler sometimes to log into the command line to execute a command line task. The Scheduler uses the main remote agent username and password to log into the command line.

Network Downloads

When Enhanced Authentication is enabled, IRISnGEN controls the Network Downloads (Telnet) using the Challenge/ Response method.

IRISnGEN uses the Remote Agent User profile to gain access to the remote agent. IRISnGEN automatically generates responses for the challenges produced by the remote agent.

PPP Connections Using Enhanced Authentication

The IRISnGEN system uses the Teltronics Extensible Authentication Protocol (Teltronics EAP) module to facilitate peer-to-peer protocol (PPP) logins for remote agent devices that are using Enhanced Authentication and are connected to a LAN. The Teltronics EAP and the PPP allows users to connect to a remote agent device via a modem. Once connected to the remote agent, the user can then access the other attached devices on the same LAN, provided the user has security rights to those devices. The remote agent automatically offers a challenge to which the user must respond in order to gain access to that remote agent and any attached devices on the same LAN.

Before attempting a PPP connection to a remote agent device using Enhanced Protocol, you must install the Teltronics EAP module on his or her PC. You can obtain a copy of the Teltronics EAP Installation Program from you system administrator. The installation program is an executable. Simply install it on your PC as you would any other executable program and follow the directions displayed in the Install Wizard. Once installed, you must then configure network connection parameters using the New Connection Wizard, which is launched from the Network Configurations folder.



To configure a network connection for EAP

1. From your Start menu, select **Control Panel > Network Connections**.
2. Under Network Tasks, select **Create a new connection**. Your system should display the New Connection Wizard dialog. If it does not, check with your system administrator to determine how to start the New Connection Wizard.
3. At the Welcome dialog, click ***Next***.
4. At the Network Connection Type dialog, choose Connect to the Internet; then, click ***Enter***.
5. At the Getting Ready dialog, choose **Set up my connection manually**; then, click ***Enter***.
6. At the Internet Connection dialog, choose **Connect using a dial-up modem,** and then click ***Enter***.
7. At the Connection Name dialog, type the name of your ISP (for example, EAP) in the **ISP Name** field, and then click ***Enter***.
8. At the Phone Number to Dial dialog, type telephone number of you remote agent's modem in the **Phone number** field, and then click ***Enter***.
9. At the Connection Availability dialog, choose **Anyone's use** if security is not an issue; otherwise, choose **My use only**, and then click ***Enter***.
10. At the Internet Account Information dialog, click ***Enter***. You do not need to enter anything is this dialog.
11. At the Completing the New Connection Wizard dialog, click ***Enter***. You are now ready to select the properties for your newly created connection.

To set the properties for the connection

1. From your Start menu, select **Control Panel**, then select **Network Connections**.
2. Right-click the dial-up icon for the connection you just created and select **Properties** from the list.
3. Click the General tab and type the telephone number of the remote agent's modem in the **Phone number** field.
4. Click the Security tab and choose **Advanced custom settings**.
5. On the Security tab, click ***Setting*** to display the Advanced Security Settings dialog.
6. Select **No encryption allowed** from the Data encryption list.
7. Choose Use Extensible Authentication Protocol and select Teltronics Extensible Authentication, and then click ***OK***.
8. Click the Networking tab and choose PPP:Windows 95/98/NT4/2000, Internet from the **Type of dial-up server** list.
9. Select the **Internet Protocol (TCP/IP)** checkbox, and then click ***Properties*** to display the Internet Protocol Properties dialog.
10. Choose **Use the following IP address** and type the address in the **IP** field. Check with your system administrator if you are not sure what IP address to use.
11. Click ***OK*** to save your properties. You are now ready to connect to the remote agent.
12. From the Network Connections window, right-click the dial-up icon for the connection you created and select **Connect** from the list. The system will establish your connection.



PPP connections to remote agents not using Enhanced Authentication

You can connect to a remote agent that does not use Enhanced Authentication using PPP. Unlike connection to remote agents using Enhanced Authentication, you do not need to install the Teltronics EAP module first. However, you must still create a network connection (found in the Network Configuration folder) and set its properties.

To configure a network connection for non-EAP

1. From your Start menu, select **Control Panel > Network Connections**.
2. Under Network Tasks, select **Create a new connection**. Your system should display the New Connection Wizard dialog. If it does not, check with your system administrator to determine how to start the New Connection Wizard.
3. At the Welcome dialog, click ***Next***.
4. At the Network Connection Type dialog, choose **Connect to the Internet**; then, click ***Enter***.
5. At the Getting Ready dialog, choose **Set up my connection manually,** and then click ***Enter***.
6. At the **Internet Connection** dialog, choose **Connect using a dial-up modem,** and then click ***Enter***.
7. At the Connection Name dialog, type the name of your ISP (for example, NON EAPea) in the **ISP Name** field, and then click ***Enter***.
8. At the Phone Number to Dial dialog, type telephone number of you remote agent's modem in the **Phone number** field, and then click ***Enter***.
9. At the Connection Availability dialog, choose **Anyone's use** if security is not an issue; otherwise, choose **My use only**, and then click ***Enter***.
10. At the Internet Account Information dialog, type the username (as defined in the Remote Agent Libraries' User folder) in the Username field, type the password (also defined in the Remote Agent Libraries's User folder) in the Password field, and type the password again in the Confirm Password field. Click ***Enter***.
11. At the Completing the New Connection Wizard dialog, click ***Enter***. You are now ready to select the properties for your newly created connection.

To set the properties for a non-EAP connection

1. From your Start menu, select **Control Panel**; then; select **Network Connections**.
2. Right-click the dial-up icon for the connection you just created and select Properties from the list.
3. Click the General tab and type the telephone number of the remote agent's modem in the **Phone number** field.
4. Click the Security tab and choose Typical security options, and choose **Allow unsecured password** from the list. Click ***OK***.
5. Click the Networking tab and choose PPP:Windows 95/98/NT4/2000, Internet from the **Type of dial-up server** list.
6. Select the **Internet Protocol (TCP/IP)** checkbox, and then click the ***Properties*** button to display the Internet Protocol Properties dialog.
7. Choose **Use the following IP address** and type the address in the **IP** field. Check with your system administrator if you are not sure what IP address to use.
8. Click ***OK*** to save your properties. You are now ready to connect to the remote agent.
9. From the **Network Connections** window, right-click the dial-up icon for the connection you created and select Connect from the list. The system will establish your connection.



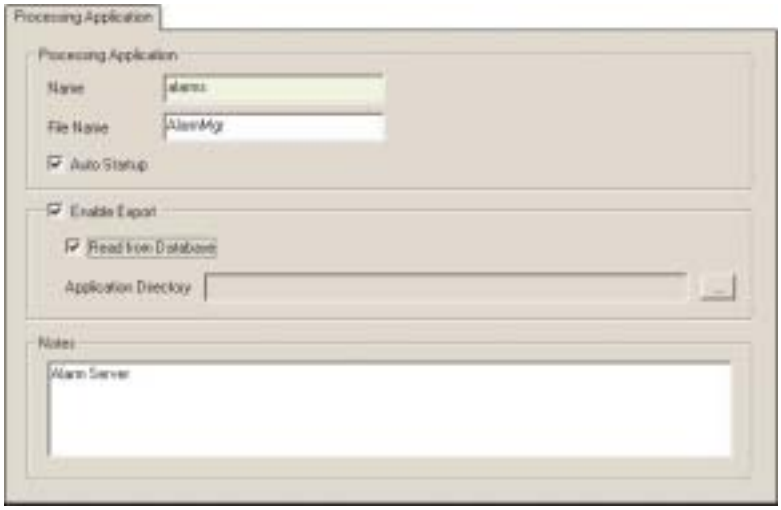
Processing Applications

Processing applications are programs running on the IRISnGEN server that tell IRISnGEN how to retrieve, store, or remove data. For example, the CommMgr and ViewerMgr applications handle data retrieval. AlarmsMgr and Traffic applications handle data storing and AgingMgr handles data removal. Teltronics includes several processing applications with your IRISnGEN system.

Use the Processing Applications tab to assign an alias name for the application—aliases appear in lists—and to determine the storage location (file, folder, or database) for incoming data.



Warning *Do not make changes to the Processing Applications windows unless directed to do so by a Teltronics Customer Service Engineer. Unauthorized changes could cause the system to fail.*



To create a processing application record

1. Choose **IRIS Administration > Processing Application**.
2. Type a name (alias) for this processing application in the **Name** field. This name will appear in several lists throughout the IRISnGEN system. This name is for your benefit, so enter something meaningful to you.
3. Type the file name of the processing application in the **Filename** field. For example, AlarmMgr is the file name of the Alarms Processing application supplied by Teltronics.
4. Select the **Auto Startup** checkbox if you want this application to start automatically when the IRISnGEN system loads.
5. Select the Enable Export box to enable the next two fields.
6. Select the **Read from Database** checkbox to enable the processing application to read data from the *raw_data* table in the IRISnGEN database.
7. Type the directory location in the **Application Directory** field for the file from which the processing application retrieves data, if different from the raw_data table file. Use the Browse button (...) to browse your directories for a file.
8. Type any description or comments about the application in the Notes field. You can type up to 256 characters.

System Parameters

You can change the system parameters for IRISnGEN by changing the values in the System Parameters windows.



Warning *Do not change these values without consulting your service representative. Your service representative can help you make certain that any changes will not negatively affect your system.*

To change a system parameter

1 Select **IRIS Administration > System Parameters**, and then click a parameter filename. The system opens the System Parameter tab.



2 Type the name of your system parameter in the **Parameter** field.



Warning *Do not enter a new name or change the existing name of any parameter without consulting your service representative first. Changes to any system parameter file could cause your IRISnGEN system to malfunction.*

3 Type a value to specify the limits of your parameter in the **Value** field. For example, entering a “1” value in the Internal_Alarms system parameter record instructs IRISnGEN to generate an alarm each time it receives an internal alarm condition.

To add a new system parameter

1 Right-click the **System Parameter** folder and choose **Add System Parameter** from the popup menu.

2 Edit the fields, as described above.

User Defined Fields

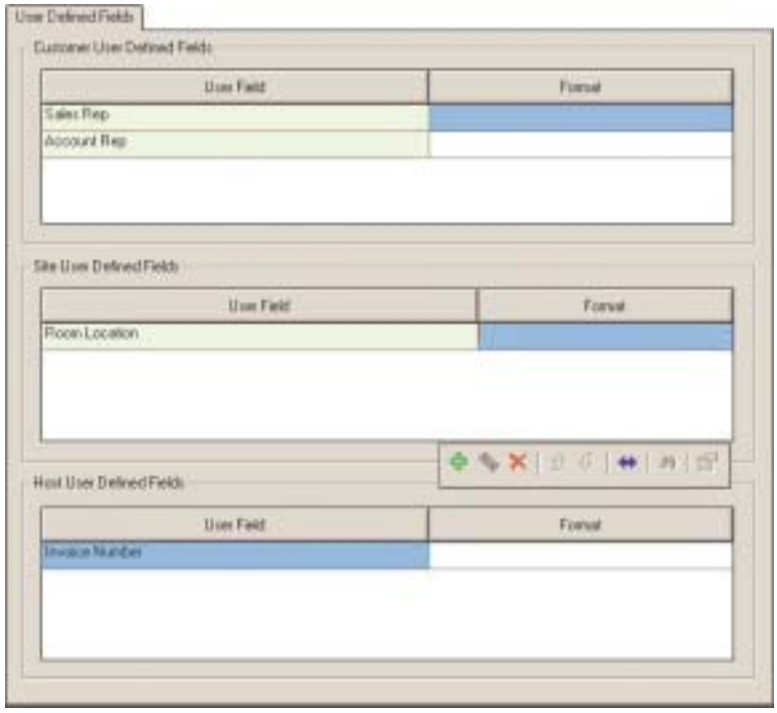
The IRISnGEN system lets you add an unlimited number of fields for use with customer, site, and host database records. Create fields to store any information you need to efficiently run your operation. Once created, user-defined fields display under User Fields tab for Customer, Site, and Host, records.

Some examples of why you might create a user-defined field:

- to store PBX passwords for host devices
- to store service contract information for that customer



The User Fields tab allows you to assign a value to the field for a selected record.



To define new fields for use with customer, site, or host records

1. From the Explorer window, choose the **IRIS Administration** folder, and then click the **User-Defined Fields** folder.
2. Select one of the three data tables on the **User Defined Fields** tab (Customer, Site, or Host).
3. Click the button to insert a table row.
4. In the **User Field** column, type a name for your field. The maximum length is 256 characters.
5. Enter the entry format in the **Format** column.

To change the name of an existing user-defined field for customer, site, or host records

1. Highlight the user field that you wish to change.
2. Type a new name for your field. The maximum length is 256 characters.

To enter or change a value for a user-defined field

1. At any customer, site, or host record, select the **User Fields** tab.
2. Type a value for the field names that display in the **Value** column.
3. You must enter data with the proper format; otherwise, an error will occur when you attempt to save the records.

Defining Values of User-Defined Fields

Choose the User Defined Fields tab on any customer, site, or host record to access the user-defined fields and change their contents.

To enter a value for a user-defined field

1. Highlight the field you want to edit.
2. In the **Value** column field, enter the information for this field.
3. When you are finished making your changes, click the Save toolbar button.

User Groups

You can logically group access permissions to various IRISnGEN functions for users based on the activities that they are allowed to perform. Start by creating a unique user group name with the access privileges desired, and then assign the user group to the user. With your user groups, you can easily support and control access for many users at one time.

To create a user group record

1. Right-click the **User Groups** folder and choose **Add User Group**. The system opens the User Group tab.



2. Type the name of the group—for example, Administrator, Viewer, or IRISnGEN Reporting—in the **User Group Name** field.
3. Select the Disabled box if you do not want this group to have user access privileges. Any user assigned to a disabled group will not be able to log on to the IRISnGEN system.
4. Type any descriptions or comments in the **Notes** field. The maximum length is 256 characters.
5. Use the Permissions table to define the access type that group members have to the listed objects. The Security Key column displays the objects for which this group has restricted access. The checkboxes in the Visible, Read, Update, Create, Delete, and Execute columns indicate the group's current access level. A check mark indicates the group has permission to perform that column's function; when the box is not checked, they cannot.

To add an object to the access list

1 Click the button to insert a new row in the data table, and then select a security key from the **Security Key** list.

Permission checkboxes appear in the other data table columns (Visible, Read, Update, Create and Execute).

2 To assign group permissions for these functions, check the box for the permissions you want to assign to this group.

Warning *You should not allow Non-Administrator groups to access to the User Group screen.*

To delete any one object from the access list

- Highlight the item you wish to delete and press the button. The system deletes this object from the appropriate access list for this user group only.

Warning *You must select (check) the Visible column checkbox to allow the group to view the object shown in the Security Key column. If you do not, the user will not see the object listed in the tree view.*

Users

You can assign users their passwords and their user group. This lets you control what access each user has to your IRISnGEN system.

Note *You must create your user group records before you can assign a user to a user group. (See Editing User Groups and About User Privileges.)*

To create a user record

1 Right-click the **User** folder and select **Add User** from the pop-up menu. The system opens the User tab.



2 Type the name of the individual user or his or her job title in the **User Name** field. Type any of the following characters in this field: **a-z**, **A-Z**, **0-9**, **_**, **@**, **#**, **$**, **%**, ^.

3 Select a user group from the **User Group** list.

4 Type the user's password in the **Password** field. Type any of the following characters in this field: **a-z**, **A-Z**, **0-9**, **_**, **@**, **#**, **$**, **%**, ^. The system replaces the characters with asterisks.

5 In the **Confirm Password** field, re-type the password exactly as you entered it in the Password field.

6 Select a hierarchy from the **Hierarchy** list. Selecting a hierarchy limits the user's Viewer display with only that hierarchy. When you select a hierarchy, you must also select a node in the next field. This affects selectivity in the following viewers:
- List Viewer
- History Viewer
- Map Viewer
- Equipment Explorer

7 Select a node from the **Node** list. Selecting a node limits the user's Viewer display with only that node. You must select a hierarchy from the Hierarchy list before you can select a node.



Warning *Do not set default selectivity parameters for users assigned to user group that has permission to change selectivity for example, user group "Administrator." On assign default selectivity parameters to users with do not have permission to change selectivity for example, user group "Restricted User."*

When you choose default selectivity parameters for users assigned to non-restrictive user groups, those users can change the Hierarchy and Node fields in the List Viewer's Viewer Selectivity dialog. However, IRISnGEN ignores these changes and only displays the hierarchy and node that was programmed in the Default Selectivity Parameter fields. Users with restricted permissions cannot change the fields in the Viewer Selectivity dialog. The appeared dimmed.

8 Type any descriptions or comments in the **Notes** field.

Zip Codes

Use the Zip Codes tab to add, edit, or delete zip codes in the Zip Code data table. Use the Selection Criteria options to find and display a zip code.

To search for a zip code:

1 Click ***Clear*** to clear the **Selection Criteria** fields.

2 Do one of the following or any combination of the three:
- Type the zip code in the **Zip Code** field.
- Type a city in the **City** field.
- Select a state from the **State** list.

3 Click ***Refresh*** to update the Zip Code data table.

To add a zip code:

1 Click **Clear** to clear the **Selection Criteria** fields and the Zip Code data table.

2 Type a new zip code in the **Zip Code** field of the data table.

3 Type a city, state, latitude, and longitude for that zip code in the corresponding fields of the data table.

4 Save your record.



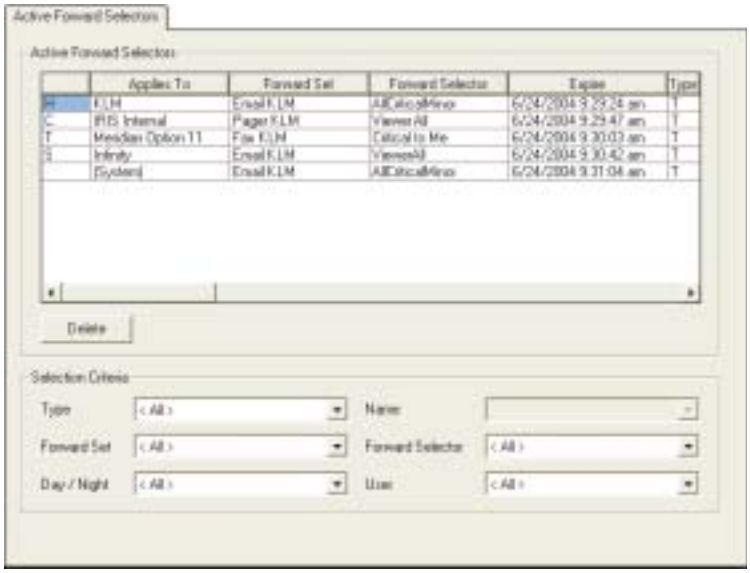
4

IRIS Tools

Active Forward Selectors

Use the Active Forward Selectors option to display all the forward selectors that are currently active in IRISnGEN. You can also use this option to insert a forward selector manually.

To view specific selectors, set your parameters in the Selection Criteria section at the bottom of the tab. IRISnGEN automatically displays those selectors meeting your criteria.



The following list describes the fields on the Active Forward Selectors tab:

Field	What it displays
Applies To	The name of the host, site, or customer predefined in the Host, Site, and Customer tabs.
Forward Set	The predefined forward set chosen for this host, site, or customer.
Forward Selector	The predefined forward selector chosen for this host, site, or customer.

Expire	The time the selector ends. IRISnGEN will automatically remove the selector from the display at the expired time.
Type	The scheduled timed filter for a host (H), site (S), or customer (C).
User	The user who inserted the forward selector that is currently active.

To use the selection criteria

- Click the down arrow beside each Selection Criteria list box and select an option to limit your display. The system refreshes the window and displays the new selections each time you choose another option from the list.

To delete a selector from the display

- Highlight a selector in the display table and click **Delete**.

Inserting Forward Selectors

Sometimes you may need to activate a forward selector for a limited time. For example, you may want to forward critical alarms for a particular host

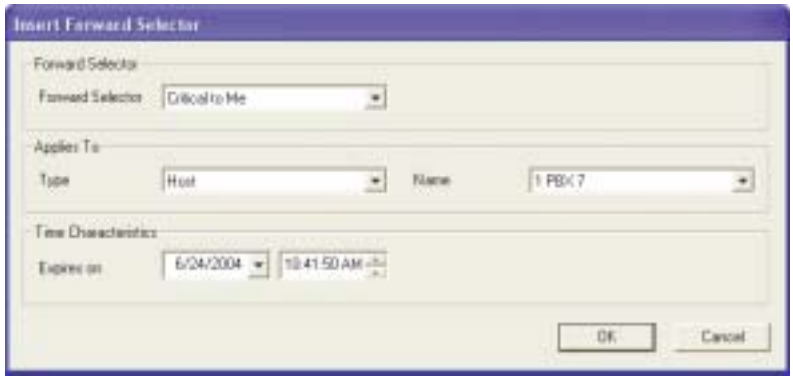
A forward selector becomes active as soon as you insert it. It overrides forward selectors assigned directly to the same customer, site, host, or host type record. Inserted forward selectors work in parallel with scheduled forward selectors (that is, they are both applied when selectivity matches).



Note *You must create your forward selector before you can insert it.*

To insert a forward selector

1 Right-click the **Active Forward Selector** icon and select **Insert Forward Selector** from the drop menu. The system displays the Insert Forward Selector dialog.



2 Choose a selector from the **Forward Selector** list of pre-defined forward selectors.

3 Select a type from the **Type** list to apply the selector to a host, site, customer, system selectors, or all.

4 Select a name from the **Name** list of available hosts, sites, or customers (depending on your Type selection). No selection is required if you chose system.

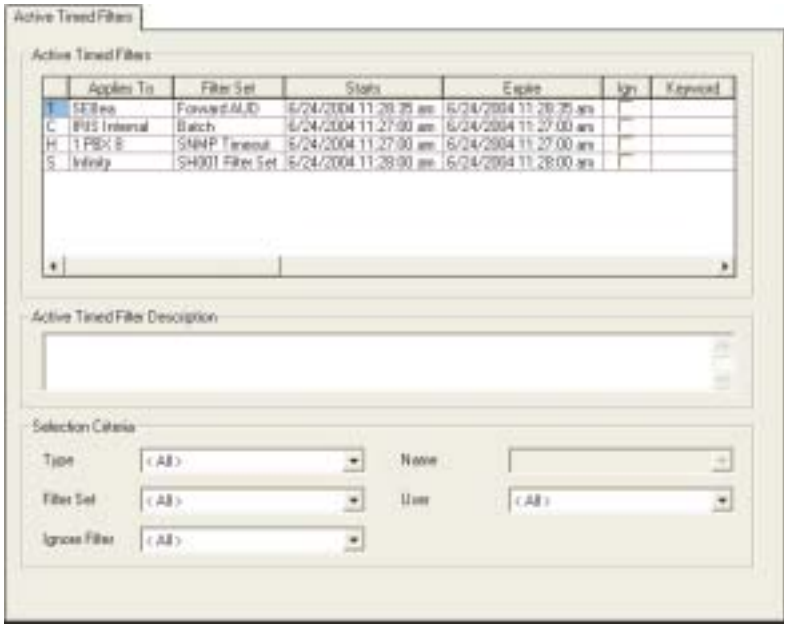
5 Enter the date and time that you wish this filter to expire in the **Expires On** fields. Times are in the format *yyyymmdd hhmmss*, where *yyyy* is the four-digit year, *mm* is the two-digit month, *dd* is the two-digit day, *hh* is the two-digit hour, *mm* is the two-digit minute, and *ss* is the seconds. Do not enter any slashes as separators between the fields; the IRISnGEN system does this for you. Enter any leading zeros in each field (for example: 04 for April).

6 When you finish creating your new filter, click ***OK***.

Active Timed Filters

Timed filters are filters that have an expiration date. They override standard filters and are in effect only for a limited time. For example, assume a PBX at a remote site has a malfunctioning card. It generates several hundred alarms per day, but this is not interfering with the performance of the PBX. A new card will be installed in next week. To prevent these alarms from appearing in the Viewer, a timed filter is set to ignore those alarms and the filter is to expire in one week.

Use the Active Timed Filters option to view all the active timed filters, or use the Selection Criteria fields to display only those selectors that meet your criteria. You can also use this option to insert timed filters manually.



The following list describes the fields on the Active Timed Filter tab:

Field	What it displays
Selection Criteria	Use the Selection Criteria parameters to limit your display by type, name, filter set, user, or ignore filter.
Type	Select a type from the drop-down list to limit your display to hosts, sites, or customers, or select ALL to display all types.
Name	Select a name from the drop-down list to limit your display. You must select a type before the list activates for this field. Only names matching the type you select appear in the list. If you chose all, no selection is necessary.
Filter Set	Select a filter set from the list to limit your display to a single set, or select ALL to display all filter sets.
Ignore Filter	Select from the list to set the Ignore filter. You have the following options: **All** – ignore all filters that match other selection criteria. **ignore only** – implements all Ignore actions from the Viewer **not–ignore only** – shows all non-ignored filters.
User	Select a name from the drop menu of users. The system finds only filters created by that user.

Inserting New Active Timed Filters

Insert a new active timed filter when you need you need it for a limited time.



Note *You must create your filter before defining your timed filters.*

To insert a new active timed filter

1 Highlight the **Active Timed Filter** icon on the tree.



2 Right-click and select **Insert Timed Filter** from the popup menu. The system displays the Insert Timed Filter dialog.



3 From the drop-down list, select a filter set, type, and name. You must select a value for each field.

4 Set the start and stop dates and times for this filter. The system displays the current date and time setting in this field. If you do not change the date and time, the filter will start immediately. Select a different date from the list.

5 Click the **Duration** radio button when you want to specify a finite duration; then, select an option from its accompanying list.

6 Click the **Infinity** button when you do not want the timed filter to end.

7 Type any additional information about this filter into the **Notes** field.

8 Select ***OK*** to save your filter; otherwise, select ***Cancel***.

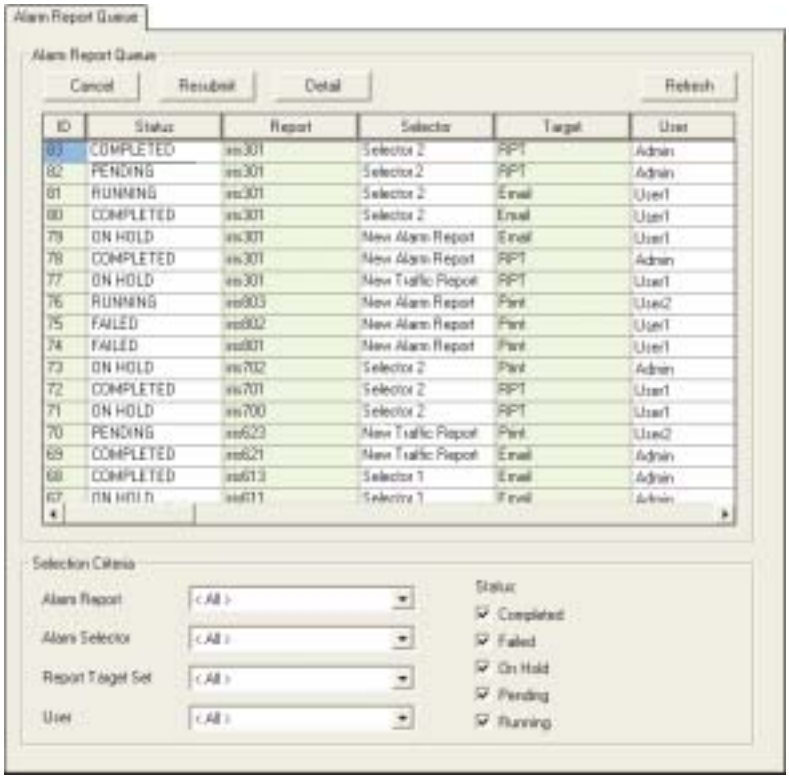
Alarm Report Queue

Use the Alarm Report Queue to display information about alarm reports that are currently running, queued to run, or have already completed. From this queue, you can also run reports manually, or rerun reports that failed to complete.

The entries in the Alarm Report Queue age according to the system parameters set by the system administrator. Each entry moves down the list depending on its priority and time in queue.

To view specific records in the Alarm Report Queue, set your parameters in the Selection Criteria section at the bottom of the window, and then click the Refresh button. IRISnGEN displays only those reports meeting your criteria.





The following describes the fields in the display window.

Field	What it displays
ID	The number IRISnGEN assigned to the entry in the Alarm Report Queue.
Status	The current report status: COMPLETED, FAILED, ON HOLD, PENDING, RUNNING.
Report	The name of the report in the queue.
Selector	The name of the report selector used to create this report.
Target	The destination of the report.
User	The person who initiated the report. The field will show AUTO if the report it ran automatically via scheduling.
Priority	The priority assigned to the report., from 1 to 255. Numbers with the highest priorities (1) process first.
Submitted	The time and date that the report entered the queue.
Run	The time and date that the report ran.

To display alarm reports using selection criteria

1 Choose a selection parameter from the list for each of the following fields:

For	Choose
Alarm Report	An alarm report pre-defined by Teltronics and shipped with your IRISnGEN software, or ALL for all alarm reports.
Alarm Selector	Report selectivity parameters, or select ALL for all alarm selectors.
Report Target Set	The destination of your report, or select ALL for all target sets.
User	The user's name, or select ALL to display traffic reports for all users.

2 Select a **Status** checkbox for each status you want to include: Completed, Failed, On Hold, Pending, Running.

3 Click ***Refresh*** to display those reports matching your parameters in the display window.

Choose an operation

- Make a selection on the Alarm Report Queue window:

Click	To
Cancel	Cancel any report with a status of PENDING or RUNNING.
Resubmit	Resubmit a FAILED or ON HOLD report for processing.
Detail	Display additional information about the highlighted report, including the Failure Code field. A failure code of 0 means that the report completed without failure.
Refresh	Refresh the Alarm Report Queue window.

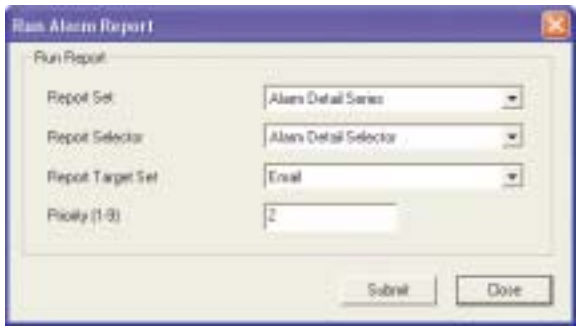


Generating Alarm Reports Manually

The Run Alarm Report option lets you run a report manually, as needed. IRISnGEN queues the report to run based on its priority. You can check the status of your report in the Alarm Report Queue.

To run a report manually

1 Right-click the **Alarm Report Queue** icon and select **Run Alarm Report**. IRISnGEN displays the Run Alarm Report dialog.



2 Select a report set from the **Report Set** list.

3 Select a report selector from the **Report Selector** list. A report selector contains report selectivity parameters.

4 Select a target set from the **Report Target Set** list. A target set identifies where IRISnGEN will deliver your report: to a printer, email, fax, or combination of these devices.

5 Type a priority for your report in the **Priority** field. Priorities can range from 1 to 9. IRISnGEN processes the reports with the highest priority (1) first.

6 Click ***Submit*** to submit your report to the Report Queue to generate immediately.

Automated Site Management

Using Automated Site Management (ASM), you can create selectors and batch files that update several remote agents at once. This speeds the update process and saves you time.

Use the Selector tab to choose the criteria the remote agents; then, use the Selector Results tab to see the results of your selection. You can also use this tab to create the batch update file. For example, suppose you want to update a database and then download it to one hundred remote agents belonging to a customer. You can call each remote agent and download the database, or you can use ASM to select those same remote agents, and then create a batch file that automatically downloads the database during off hours. This saves you valuable processing time and makes efficient use of your facilities.

Selector Tab

Selectors are database queries that identify those remote agents that meet specific criteria. Use the Selector tab to create and name your selector; then, choose from a list of pre-defined criteria to identify those remote agents that you want to update. For example, create a selector named KLM Selector; then, use the criteria fields to select all remote agents for customer KLM Corp. with databases updated but not yet downloaded. Click the Selector Results tab to display a list of those remote agents matching your criteria, that is, those whose databases changed, but still awaiting download.

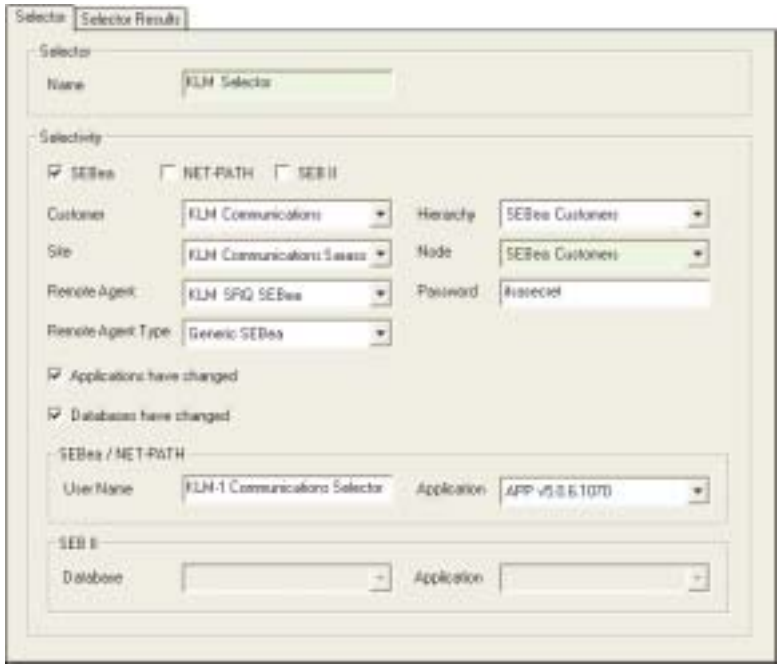
The results of a selector are dynamic and can change often. Once you download the databases, the remote agents no longer meet the selection criteria and will not appear in the next query. This can be a benefit when you want to update only those remote agents with databases that changed since the last download.

The following shows an example of the Selector tab. Notice the various criteria fields on the tab. Many of these fields include lists used to limit your selection. These fields are hierarchical. The information they display depends on the item you selected in the previous field. For example, the Remote Agent list only displays those remote agents defined for the site selected from the Site list, which only displays the sites for the customer you selected from the Customer list. Selecting <NONE> from any of the lists increases the number of remote agents listed in the Selector Results tab.



To create a selector record

1 Choose **IRIS Administration** > **Automated Site Management**. Right-click the **Automated Site Management** folder and select **Add Selector**. The system displays the Selector tab.



2 Type the name of your selector in the **Name** field. Be sure to choose a name that will easily identify the selector.

3 Select the **SEBea**, **NET-PATH**, and/or **SEB II** boxes to specify the type of remote agent you want to query.

4 Select the parameters for your query:

Field	Description
Customer	Select a customer from the **Customer** list. Only the remote agents that belong to this customer will appear in the Selector Results list.
Site	Select a site from the **Site** list. Only those sites defined for the customer selected in the previous field will appear in the list. If you selected **<none>** in the previous field, the system will display all sites in the list.
Remote Agent	Select an agent from the **Remote Agent** list. Only those agents defined for the customer and site selected in the previous fields will appear in the list. If you selected <none> in the previous fields, the system will display all remote agents in the list.

Remote Agent Type	Select a type from the **Remote Agent Type** list. If you selected <none> in the previous field, the system will display all types in the list.
Hierarchy	Select a hierarchy from the **Hierarchy** list.
Node	Select a node from the **Node** list. Only the nodes available for the hierarchy selected in the previous field will appear in the list. You must select a node if you selected a hierarchy in the previous field.
Password	Type the password to search in the **Password** field. The system will display all remote agents using that password, regardless of case. For example, if two remote agents use "telt" and "TELT" (respectively), both will display.

5 Select the **Applications have changed** checkbox to find remote agents in which an application has changed, but has not yet been sent to the remote agent. The selectivity you choose (SEBea, NET-PATH, or SEB II) determines the search criteria the system uses.

6 Select the **Database has changed** checkbox to find remote agents in which a database has changed, but has not been sent to the remote agent. The selectivity you choose (SEBea, NET-PATH, SEB II, or all) determines the search criteria the system uses.

7 Do one of the following:

- If you clicked the SEBea or NET-PATH checkbox above, you can type a name in the **User Name** field and select an application from the list.
- If you clicked the SEB II checkbox above, you can select a database from the **Database** list, the select an application from the list.

After you define and save your selector, you can run it immediately, or schedule it to run later.



To run the selector

1 From the tree view, right-click a selector; then, select **Execute** from the popup menu. The



system opens the Selector/Batch Execute dialog.

2 Select the **Execute Type**, **Execute Date/Time**, and **Priority** desired; then, press ***OK***.



Note *If your current selectivity is not saved, the Save window appears before letting you proceed. Save your selectivity and the Run Selector window appears.*

To delete a selector

1 Right-click the selector name and choose **Delete** from the pop-up menu.

2 At the system prompt, choose **Delete**.

To duplicate a selector

1 Right-click the selector name and choose **Duplicate** from the pop-up menu.

2 Type the new name of the copied selector and save it.

Selector Results Tab

Once you create and define a selector, you can use the Selector Results table to display a list of remote agents that match your criteria. You can also use this tab to convert a selector to a batch file.

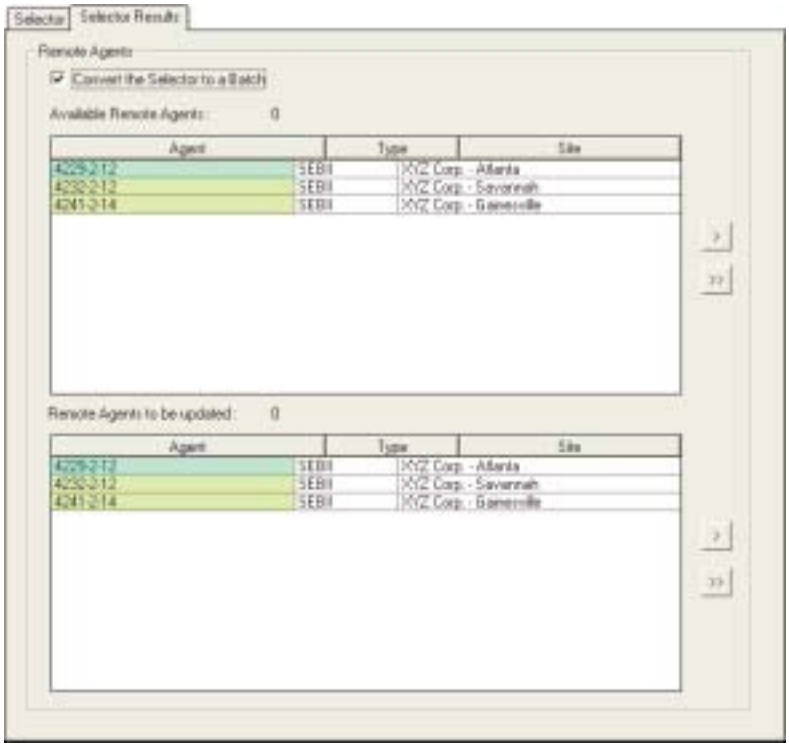
Batch files work differently than selector files. While selectors are dynamic and the results vary every time you execute them, batch files are static and the results do not change. Convert your selectors to batch files and execute them when performing scheduled updates. For example, as a matter of security you may want to download a new password to each remote agent device that belongs to a particular customer. You can create one selector that identifies those devices, and then convert it to a batch file. You can then execute this same batch file each month to download a new password to the same remote agent devices.



Note *A batch and a selector can have the same name. Selectors appear with the*  *icon. Batches appear with the*  *icon.*

The following shows an example of the Selector Results tab.





To view the selector results

1. Select the **Convert the Selector to a Batch** checkbox to convert your selections to a batch file for updating remote agents.
2. When you select this option, the icon changes in the tree view. You cannot revert to a selector after converting to a batch. You must create a new selector.
3. The Available Remote Agents data table displays a list of the remote agents that match your selection criteria. It shows the agent name, type, and the site. Select a button:

Click	To
>	Move selected hosts from the **Available Remote Agents** field to the **Remote Agents to be updated** field.
>>	Move the entire list from the **Available Remote Agents** field to the **Remote Agents to be updated** field.

4 The **Remote Agents to be Updated** data table shows all remote agents selected for updating, based on your selection criteria. You can add new agents to this table by changing the selectivity criteria in the Selector tab and then moving the results from the **Available Remote Agents** data table (above) to this data table.

Click	To
>	Remove selected hosts from the **Remote Agents to be updated** field.
>>	Remove the entire list from the **Remote Agents to be updated** field.

To change the remote agent password

1 Create a selector and save it.

2 Click the **Selector Results** tab. IRISnGEN populates both the Available Remote Agents and the Agents to be Updated data tables.

3 Use the single right arrows to move agents in or out of the **Remote Agents to be Updated** pane, or use the double right arrow to move all of them.

4 Select **Convert the Selector to a Batch** checkbox.

5 Right-click the batch in the tree and select **Change Password.** The system opens the Selector/Batch – Change Password dialog.



6 Type the new password in the **New Password** field. This will change the password for all selected remote agents in the IRISnGEN database.

7 Select the **Execute Selector/Batch** checkbox if you want to run the batch name; then, click ***OK***. Executing the Batch Selector modifies and downloads the database containing the new password for all the remote agents listed in the Agents to be Updated data table.

To run the batch

1 Right-click the batch name and select **Execute** from the menu.



2 In the pop-up window, choose the **Execute Type**, **Date/Time**, and **Priority** desired and press ***OK***.

3 The system handles numbers the highest priorities first. If you do not enter a number in this field, the system inserts a priority of “10” for you. If you did not previously save your selectivity, the system will prompt you to do so. Once saved, the system displays the Run Selector dialog.

To delete a batch

1 Right-click the batch name and select **Delete** from the pop-up menu. The system prompts you to verify your choice.

2 Select **Delete**.

To duplicate a batch

1 Right-click the batch name, and then choose Duplicate from the pop-up menu.

2 The system creates a copy and highlights the **Name** field.

3 Type the new name of the copied batch; then, save it.

You can now change the selection criteria and view the results. Be sure to save those changes, too.

Bad Data

Bad data is any alarm that the IRISnGEN system cannot process properly. The result is an error. IRISnGEN stores an alarm’s bad data in the Bad Alarm file.

Some common reasons for bad data include:

- no processing application was assigned to the host (NO APPLICATION)
- couldn't match on a keyword (NO ENTRY)
- no host assigned (HOST UNKNOWN)
- couldn't write to alarms file (INSERT ALARM) —This happens when the system is running a diagnostic that locks the alarm table.

Viewing Bad Data

Use the Bad Data option to view the alarms that IRISnGEN could not process. You can select and view bad data by the remote agent’s embedded name, application, host, event, and/or time. This is an excellent tool for trouble-shooting system problems. Once you correct a problem, you can resubmit the alarm for processing.





The following describes the buttons, message fields, and section criteria fields on the Bad Data tab.

Button	What it does
Delete	Deletes the highlighted alarm.
Resubmit	Resubmits the highlighted alarm for reprocessing. If you corrected the error that caused this alarm to be stored as bad data, the alarm should now be processed normally.
Resubmit All	Resubmits all bad data for reprocessing. If you corrected the error that caused these alarms to be stored as bad data, they should now process normally.
Detail	Displays details about the selected alarm.
Refresh	Refreshes the Bad Data window.

Field	Description
Records	Enter the number of records to be displayed when the Refresh button is pressed. The default is 500 records.
ID	The alarm number as assigned by the IRISnGEN system.
Host	The host that originated the alarm data.
Embedded Name	This is the name that uniquely identifies the SEBea remote agent. Embedded names are defined in the SEBea Remote Agent record.
Port	The port number on the remote agent that sent the alarm data.
Poll	0 = polled 1 = unsolicited alarm 2 = event generated by correlation 3 = internal event 4 = events generated by threshold
Time	Time that the IRISnGEN system received the alarm data.
Application	The IRISnGEN application that generated the error event that caused the alarm to be placed in the bad data file.
Event	The IRISnGEN system message describing the cause of the alarm
Data	Alarm data sent by the remote agent.
Host Address	IP network address of the host as defined in the Host record.

Selection Criteria

1. Select an embedded name from the **Embedded Name** list or select ALL to see bad data for all embedded names.
2. Select an application from the **Application** list or select ALL to see bad data for all applications.
3. Enter the start time for your query in the **Min Time** field. The format is *yyyy/mm/dd hh:mm:ss*.
4. Select a host from the **Host** list or select ALL to see bad data for all hosts.
5. Select an event from the **Event** list or select ALL to see bad data for all events.
6. Enter the end time for your query in the Max time field. The format is *yyyy/mm/dd hh:mm:ss*.



To view bad data

1. Create a query to selectively search for bad data. Leave query fields blank to see all bad data.
2. Click ***Refresh*** when you have set your query parameters to your satisfaction. The IRISnGEN system displays the bad data that meets your search criteria.
3. For further information about any alarm, highlight the alarm and press the **Detail** command button.

To delete bad data

1. Highlight the alarm you want to delete from bad data.
2. Click ***Delete***.
3. Click ***Close*** to exit.



Note *If you do not delete bad data, IRISnGEN will do so automatically according to the IRISnGEN system parameter, AGE_BAD_DATA.*

Resubmit Bad Data for Processing

Use this option to resubmit alarms for reprocessing. Some system or database problems may cause IRISnGEN to mark alarms as bad data. Correct the problem and resubmit alarms for processing.

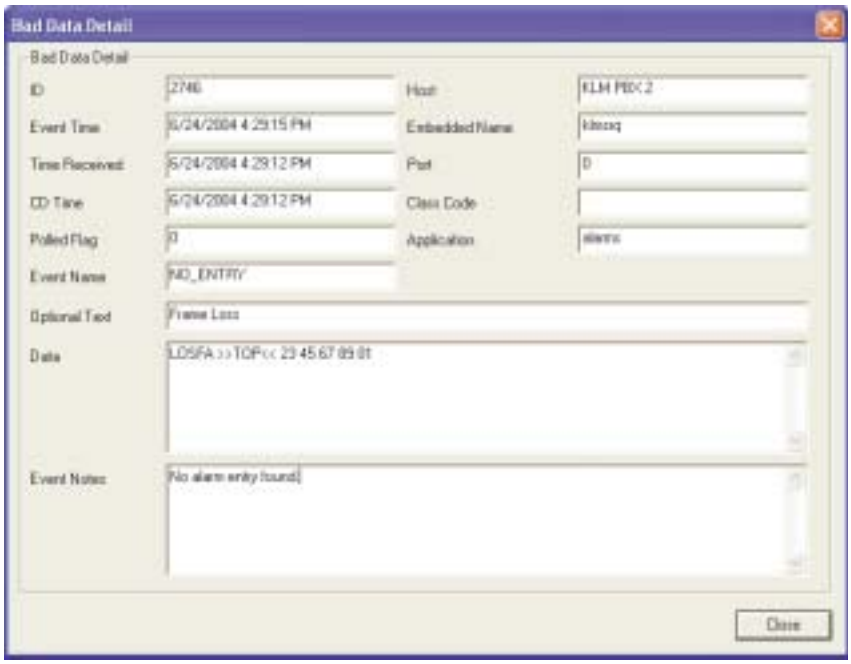
To resubmit bad data

1. Create a query to selectively search for the data you want to resubmit. Leave query fields blank to see all bad data.
2. Select Find when you have set your query parameters to your satisfaction.
   IRISnGEN displays the bad data that meets your search criteria.
   - TO RESUBMIT ONE ALARM: highlight the alarm you want to resubmit for processing and click ***Resubmit***.
   - TO RESUBMIT ALL ALARMS: click ***Resubmit All*** to resubmit all the displayed alarm for reprocessing.
3. Click ***Close*** to exit.



Bad Data Detail

Use this screen to view details about each bad data record. All the data fields on this window are informational. You cannot edit these fields.



The following describes the fields on the Bad Data Detail window.

Field	What it means
ID	The number of the alarm, as assigned by the IRISnGEN system.
Host	The host that originated the alarm data.
Event Time	Time that the system inserted this alarm into the bad data file.
Embedded Name	The name of the remote agent used to identify itself when sending alarms to the IRISnGEN system.
Time Received	Time that the IRISnGEN system received the alarm data.
Port	The port on the remote agent device from where the data was sent.
CD Time	Time that the remote agent received the alarm data.
Class Code	Class code from the remote agent.

Polled Flag	0 = polled 1 = unsolicited alarm 2 = correlation-generated event 3 = internal event 4 = threshold-generated event
Application	The IRISnGEN application that generated the error event that caused the alarm to be placed in the bad data file.
Event Name	The event type that caused the alarm to be inserted in the bad data file.
Optional Text	Additional data provided in the alarm.
Data	Alarm data sent by the remote agent.
Event Notes	Description of the event type that caused the alarm to be inserted in the bad data file.

To exit

Do one of the following:

- Click ***OK***.
- Click  in the upper right-hand corner of the window.

Bad Data Events List

This is a list of bad data event names, which application generated the event, and a description of each event. These events cause incoming alarms to be diverted to the bad data file.

Event	Application	Description
BAD_COLLECT_TIME	Comm	Could not determine collect time
BAD_0TEXT	Comm	Unable to parse optional alarm text
BAD_PORT	Comm	Unable to determine remote agent port
BAD_SYNCH_CODE	Comm	Unable to parse SYNCH_CODE from remote agent alarm
BAD_TEXT	Comm	Unable to parse alarm text
RA_UNKNOWN	Comm	Remote Agent not in database
CORR_ERR	Alarms	Error during correlation
ENTRY_ERR	Alarms	Error reading alarm entry information
ESCAL_ERR	Alarms	Error during escalation procedure
FILTER_ERR	Alarms	Error while performing filter

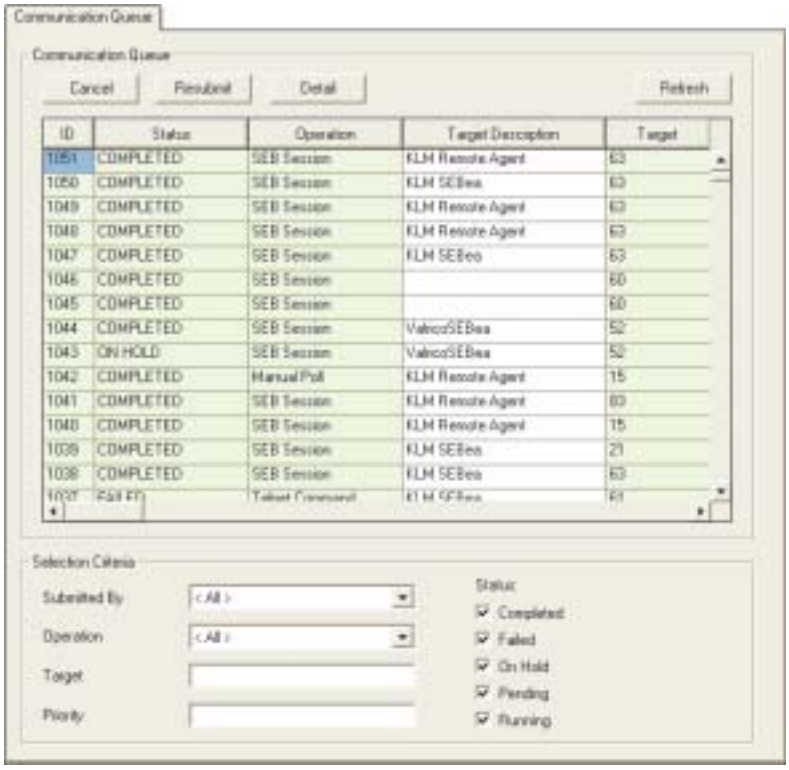
FRWD_FILE	Alarms	Unable to open forwarding file
HOST_ERR	Alarms	Error reading host information
HOST_UNKNOWN	Comm	Host not in database
IDENTITY	Alarms	Error reading alarms identity record
INS_AL_TXT	Alarms	Error inserting alarm text record
INS_ALARM	Alarms	Error inserting alarms record
NO_ENTRY	Alarms	No alarm entry found
PARSE_ERROR	Comm	General error parsing the alarm data
RAW_DATA	Comm	Unable to insert data in raw data table, check host processing ID(s)
THRESH_ERR	Alarms	Error while applying threshold
UNKNOWN_EVENT	Alarms	Failure while looking up event information
VIEWER	Alarms	Error inserting alarm record in viewer file



Communication Queue

In IRISnGEN, use the Communication Queue option to check the status of any communication operation that is queued for execution. To view specific records in the queue, set your parameters in the Selection Criteria section at the bottom of the tab; then, press Refresh. IRISnGEN displays only those requests meeting your criteria.

The entries in the queue age according to the system parameters set by the system administrator.



The following describes the fields in the display window.

Field	What it means
ID	The number IRISnGEN assigned to the entry in the Communication Queue.
Status	The current request status; COMPLETED, FAILED, ON HOLD, PENDING, RUNNING.
Operation	The type of operation requested. Operations are defined on the Communication Operation tab.
Target Description	The name of the destination system--for example, the remote agent name.
Target	The SQL ID number of the target system.

Arguments	Varying data appears in this field depending on the operation that you selected from the Operation list. *Forward Alarm*: the forward destination appears in this field. *Manual or Scheduled poll*: a blank indicates a complete SEB poll; -SP indicates selective polling. *Page operation*: the ID of the alarm (that caused the page displays) sent to the pager.
User	The user who submitted the operation for processing.
Priority	The priority number assigned to the operation. Priorities range from 1 to 255. If IRISnGEN has more operations pending than it can handle, it services the operations with the highest priority (1) first.
Time	The time the request entered in the queue.
Attempt	The number of times that the system attempted to complete this operation.



To display requests using selection criteria

1 Enter a selection parameter for each of the following fields:

For	Do the following
Submitted By	Select a user from the list, or select ALL to list operations from all users.
Operation	Select an operation from the list, or select ALL to view all operations. (Operations are defined in the Operations records.)
Target	Type a device target number for a queue operation, or leave this field blank to view operations for all targets.
Priority	Type the priority number of the operations you wish to view. Leave this field blank to view operations for all priorities.

2 Click a **Status** checkbox for each status you want to include: Completed, Failed, On Hold, Pending, Running.

3 Click ***Refresh*** to display those requests matching your parameters in the display window.

Choose a Communication Queue operation

- Make a selection on the Communication Queue tab.

Click	To
Delete	Delete the highlighted operation.
Resubmit	Resubmit the highlighted operation for reprocessing.
Detail	Display the Communication Queue Detail dialog.
Refresh	Refresh the Communication Queue.

Communication Queue Detail

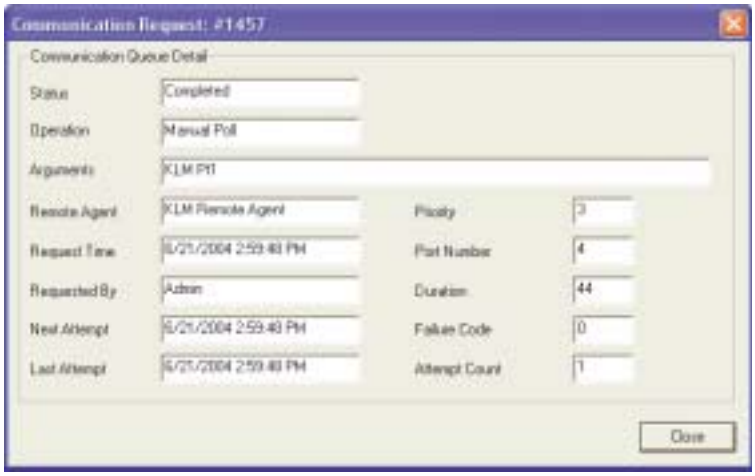
In IRISnGEN, you can view the status and detail information for any communication request that is (or was) queued for execution.

To view details

1 Highlight a listing in the **Communication Request Queue** dialog box.



2 Select **Detail**. The system displays the Detail window. You cannot change any of the fields in this window. This is strictly for display so that you can check the status of your operations.



The following list describes the fields you can see in the dialog box:

Field	What it displays
Status	The five states the request is in: COMPLETED, FAILED, ON HOLD, PENDING, RUNNING
Operation	The type of operation requested. These are defined in Communication Operations.
Arguments	Different data appears in this field, depending on the operation that you selected from the Operation drop-down menu. *Forward Alarm:* the forward destination appears in this field. *Manual or Scheduled poll*: a blank indicates a complete SEB poll, -SP indicates a single-port poll. *Page operation*: the ID of the alarm that caused the page is displayed.
Remote Agent	The remote agent that will receive the operation request.
Requested Time	The time that the request was placed in the queue.
Requested By	The name of the person who requested this operation. If this was an automated operation, this field is blank.
Next Attempt	The time the system will next attempt to complete the operation.
Last Attempt	The time of the last attempt to complete the operation.



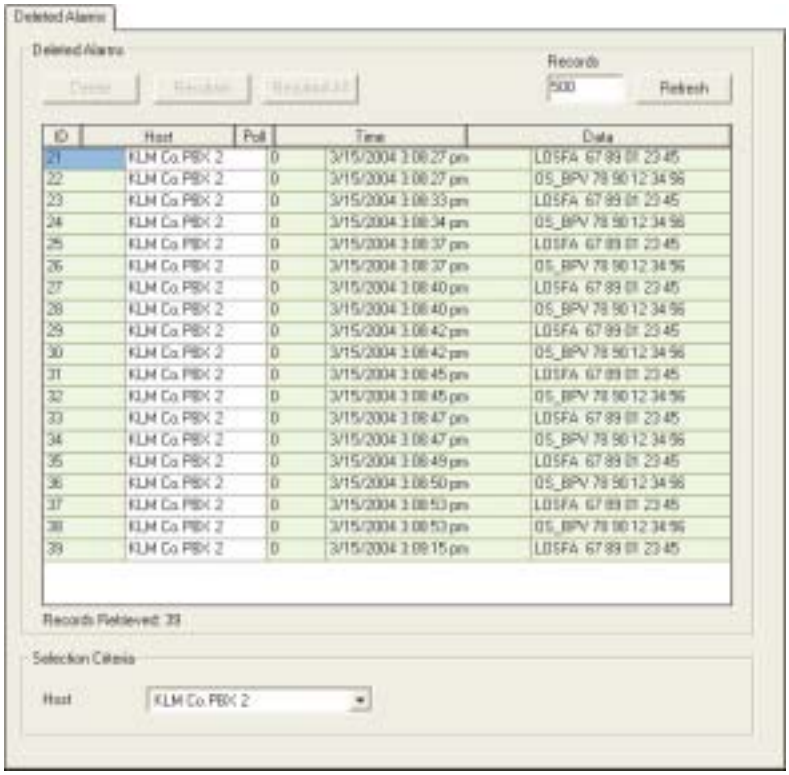
Priority	The priority number assigned to the operation. Priorities can be from 1 to 255. If more operations are being attempted than can be handled, the operations with the lowest priority number are implemented first.
Port Number	The IRISnGEN serial port where the operation was executed.
Duration	Length of time (in seconds) that the operation took to complete.
Failure Code	A code returned by the device to explain why the operation failed. If the code is 0, the operation was successful.
Attempt Count	The number of times that the system attempted to complete this operation.

3 Click ***OK*** to return to the Communication Request Queue window.



Deleted Alarms

In IRISnGEN, you can view deleted alarms. The deleted alarms appearing in the window are unsolicited alarms (alarms sent to IRISnGEN, but not polled) that were deleted by filters, thresholds, or correlations. You can view selected alarms by their host, if you choose.



To view deleted alarms

1. To view deleted alarms from only one host, select the host from the **Host** list. Leave this field blank to view deleted alarms from all hosts.
2. Select ***Refresh***. The following describes the buttons, message fields, and section criteria fields on the Deleted Alarms tab.

Field	What it displays
ID	The alarm number as assigned by the IRISnGEN system.
Host	The host that originated the alarm data.
Poll	0 = polled 1 = unsolicited alarm 2 = correlation-generated event 3 = internal event 4 = threshold-generated event
Time	Time that the IRISnGEN system received the alarm data.
Data	Alarm data sent by the remote agent.

Choose an operation

Make a selection on the Alarm Report Queue window:

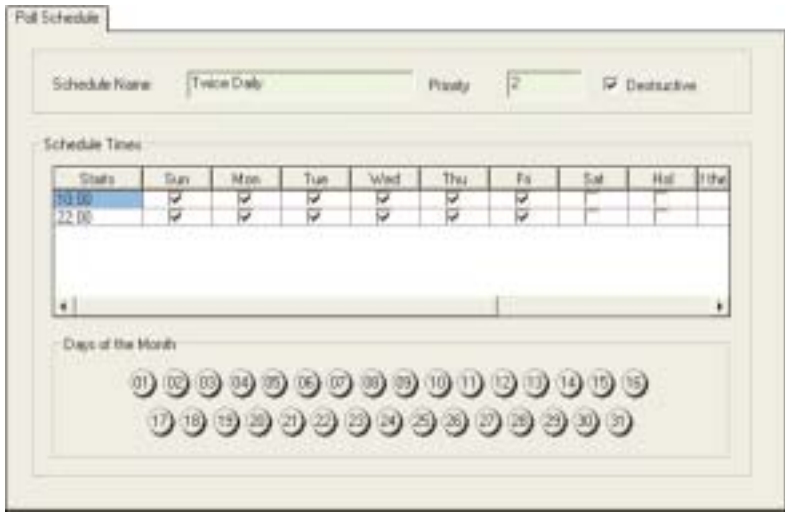
Choose	To
Delete	Delete the highlighted alarm permanently
Resubmit	Resubmit the highlighted alarm for reprocessing.
Resubmit All	Resubmit all the deleted alarms that you have displayed for reprocessing.
Refresh	Refresh the Deleted Alarms window.

Poll Schedule

You can schedule polling to occur daily, weekly, or by day of the month. IRISnGEN selects modems according to settings in the Port Groups screen.

To create a poll schedule

1 Right-click **Poll Schedule** in the tree and select **Add Poll Schedule**. The system opens the Poll Schedule tab.



2 Type the name of the schedule in the **Schedule Name** field.

3 Type a priority for the schedule in the **Priority** field.

4 If it is a destructive poll, click the **Destructive** checkbox. A destructive poll deletes the event data stored in the remote agent during the polling process. You cannot recover deleted data after a poll.

5 Click in the Schedule Times data table to activate the data table toolbar.

6 Click the button to add a row to the poll schedule table.

7 Double-click in the **Starts** column and enter the time when the system should begin polling.

8 Select the days of the week when the system will poll by clicking the checkboxes in the appropriate columns.

9 Select the specific days to generate a poll by clicking the appropriate **Days of the Month** buttons.

10 Save your poll schedule.

11 You can now assign the schedule to the remote agents by selecting this poll schedule from the list in the **Poll Schedule** field on a Remote Agent tab.

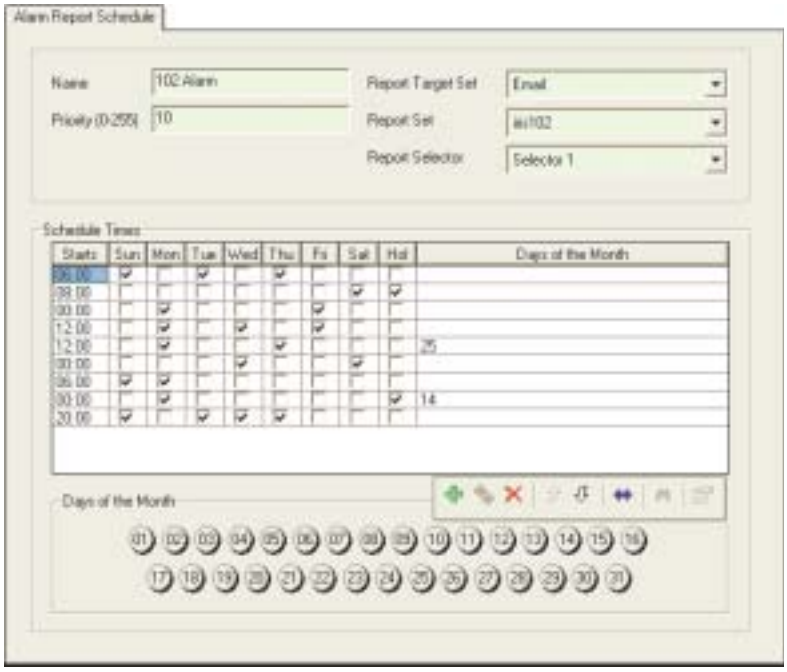
Reports

Alarm Report Schedules

Use the Alarm Report Schedule option to schedule reports that run on selected days of the week, a particular day of the month, or a specific holiday, each with its own start time. You can schedule periodic reports on critical customer accounts for your personal attention, or send them directly to your customers via fax or email on a periodic, recurring basis.

To create an alarm report schedule record

1 Right-click the **Alarm Report Schedule** folder and choose **Add Alarm Report Schedule** from the list. The system opens the Alarm Report Schedule tab.



2 Type a name for the schedule in the **Name** field.

3 Type the priority level for this action in the **Priority** field. You can enter a number from 1 to 255. If more reports queue than the system has resources, the reports with the highest priority start first. We recommend that you set a priority of 2 or lower for reports, since critical operations use priority 1 and you do not want to interfere with those functions.

4 Select a target set from the **Report Target Set** list. Target sets identify the delivery destination for reports generated by the IRISnGEN server: printer, email, fax, or combination of these devices.

5 Select a report set from the **Report Set** list. Report Sets are user-defined records containing groups of individual reports (as defined by Teltronics) that run as a batch.

6 Select a report selector from the **Report Selector** list. A selector contains the selectivity parameters used to determine which records to include in the report.

7 Enter the report's start time in the **Start Time** field. Format is hh:mm (hours:minutes). You must enter all four digits, for example enter 04:00 to start at 4:00 AM. Enter 18:00 to start at 6:00 PM.

8 Select a **Day** checkbox for each day of the week you want your report to generate. For example, to generate every business day, check Monday, Tuesday, Wednesday, Thursday, and Friday.



Note *If the boxes do not appear automatically, click a Day heading--for example, Sun-- and then click the + button.*

9 Choose the **Days of Month** button(s) that corresponds to the day(s) you want your report to generate. Reports will generate on the same date each month. For example, choose "15" to generate your report on the 15th of each month. You can select any number of days.

Alarm Report Selectors

Use the Report Selectors to define the criteria for your report. The more criteria you select, the more detailed the report. Use this information to run reports automatically or manually.

To create an alarm report selector record

1 Right-click the **Alarm Report Selector** folder and select **Add Alarm Report Selector**. The system opens the Alarm Report Selector tab.



2 Type the name of the selector record in the **Name** field.

3 Select the most appropriate criteria from the list for each of the following fields:

- Host
- Site
- Customer
- Host Type
- Hierarchy

- Node
- User

4 Select which alarms to view from the **Include** list. The list includes:
- **All Alarms** – all alarms received by IRISnGEN.
- **All Filtered Alarms** – all alarms not sent to the Alarms Viewer.
- **All Viewer Alarms** – all alarms sent to the Alarms Viewer.
- **None** – ignore this field.

5 Select a status for the current state of an alarm from the **Status** list.

6 Select the severity of the alarms you wish to report from the **Severity** list.

7 Select an alarm type from the **Alarm Type** list.

8 Type a class code, as defined in the SEB II, in the **Class Code** field, or leave the field blank to report all class codes. Use this field only when reporting alarms from SEB II remote agent devices.

9 Type a keyword found in specific alarms in the **Keyword** field, or leave the field blank to report all keywords.

10 Type the name of the remote agent you want to report in the **CD** field, or leave the field blank to report alarms from all remote agents.

11 Type the address of the network device in the **Host Address** field. The address identifies alarms sent to IRISnGEN via a remote agent or a hard contact with attached hosts identified as HC1 though HC8.

12 In the next four fields, type two entries to establish a range parameter. Include:
- **At Least** – the lowest alarm ID, escalation number, day of week, or time of day range.
- **Not More Than** – the highest alarm ID, escalation number, day of week, or time of day range.

Field	Definition
Alarm ID	IRISnGEN assigns IDs to alarms as it processes them for display in the Viewer or the Alarm History file. Enter the same ID number in both fields to report only one alarm.
Escalation	IRISnGEN assigns each new alarm an escalation of “0”. Alarms are escalated automatically when defined in an Escalation Group record or manually by escalating them in the Alarms Viewer.
Day of Week	Enter day numerically. For Sunday, enter 1; for Monday, 2; Tuesday, 3…Saturday, 7.
Time of Day	Times are in the format *hhmm*, where *hh* is the two-digit hour, and *mm* is the two-digit minute. You do not need to enter any colons as separators between the hours and minutes.



13 Select one Absolute or Relative button and type a range parameter for your selection.

Field	Definition
Absolute Time	Under the At Least heading, enter the start time; under the Not More Than heading, enter the end time. Times are in the format *yyyymmdd*, where *yyyy* is the four-digit year, *mm* is the two-digit month, *dd* is the two-digit day.
Relative Months Ago	Under the At Least heading, enter the start number; under the Not More Than heading, enter the end number.
Relative Days Ago	Enter the relative number of days ago. For example, 1 and 2 indicate alarms received between one to two days ago.
Relative Time (Minutes Ago)	Enter how long ago you want to show alarms. For example, 1 and 20 indicate alarms from at least one minute ago, but not more than twenty minutes ago
None	Choose this button to ignore Absolute and Relative parameters fields.

14 Do one of the following:

- Click **Time Received** to select the time that the IRISnGEN system received the alarm data.
- Click **Time Occurred** to select the time the alarm occurred.

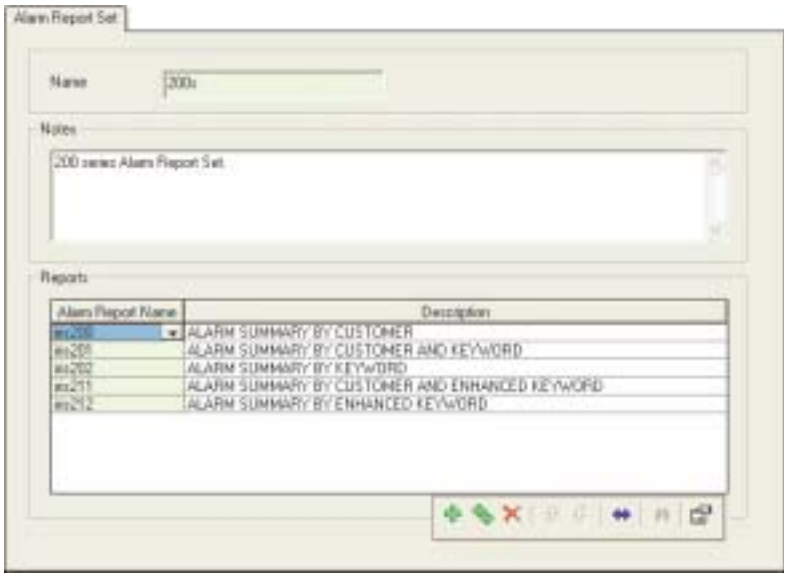


Alarm Report Sets

Use the Alarm Report Sets option to group several alarm reports into a single set to run as a batch. You can also create a set with only one report.

To create a report set

1 Right-click the **Alarm Report Sets** folder in the tree view, and select **Add Alarm Report Set**. The system opens the Alarm Report Set tab.



2 Enter the name of your report set in the **Name** field.

3 Enter a description or comments about the report set in the **Notes** field. The maximum length is 256 characters

4 Click the button to insert a blank row in the **Reports** data table, or click the button to add multiple rows.

5 Select a report name from the list.

6 Repeat steps 4 and 5 to add additional report names.

7 IRISnGEN automatically enters the description for each report contained in the report set.

To delete a report from the set

- Highlight an alarm report name and click the button.

Alarm Reports

IRISnGEN comes with a variety of pre-defined alarm reports. Use the Alarm Reports option to access information about these reports, or if you have the optional IRISnGEN Ad Hoc Report module, create your own custom reports and add them to your report list.

To display an alarm report

1 Expand the **Alarm Report** folder.

2 Click on a report from the list to display the Alarm Report tab.



The following list describes the fields in this window. Do not edit these fields.

Field	What it means
Name	The name of the report
File Name	The name of the report file as defined by Teltronics. Do not change this name.
Notes	Information explaining the content of the report type.

Report Target Set

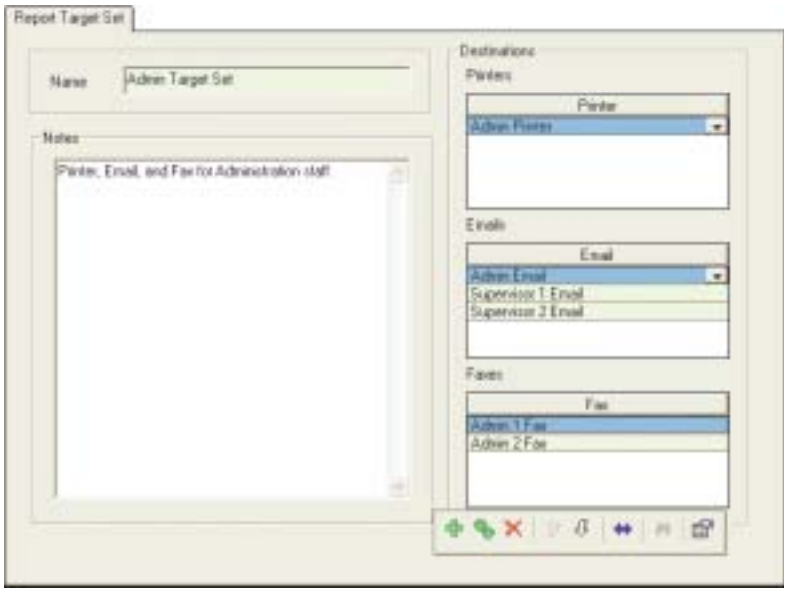
Use the Report Target Set option to create sets that identify where you want to deliver your reports: printer, email, fax, or a combination of these devices. Later, you will assign these sets in the Report Queue and in the Run Report dialogs.



Note *You must pre-define your printer, email, and fax records in IRISnGEN's Forwarding windows before you can use them in your target set.*

To add a target set

1 Highlight the **Report Target Sets** folder and select **Add Report Target Set**. The system opens the Report Target Set tab.



2 Type the name of your target set in the **Name** field.

3 Type a description or comments about the report set, in the **Notes** field. The maximum length is 256 characters.

4 Click inside a **Destination** field (Printer, Email, or Fax) to activate the mini toolbar.

5 Click the ✚ button to add a blank row to a **Destination** data table, or click the ✚ button to add multiple rows.

6 Select a destination from the list.

7 Repeat steps 3 through 5 to add additional destinations to each field.

To delete a destination from the set

- Highlight a destination name and press the ✕ button.

Traffic Report

The IRISnGEN Traffic System is a complete software package that streamlines the analysis of traffic data from your *Meridian 1*™ PBX. IRISnGEN Traffic not only gives you more control over your traffic data, it unleashes your computer so it can operate at full power, unhampered by previous restrictions. This means you can analyze, study and report traffic data in almost limitless ways.

IRISnGEN Traffic lets you collect, store, retrieve, and report traffic data from your *Meridian 1*. Built on a Windows NT platform as a member of the IRISnGEN family of products, IRISnGEN Traffic combines its highly successful data collection and storage subsystem with its superior reporting system.

IRISnGEN Traffic collects data specific to each *Meridian 1*, then automatically builds customer, route, loop and attendant files. The IRISnGEN Traffic design lets you enter meaningful names for each switch resource. IRISnGEN Traffic provides selective reporting capabilities, such as reporting by company, route set, and user-defined dates and events. It also provides for the creation of traffic studies and reports using a selection of alternative Grade of Service formulae on a per-study or per-route set basis.

An important IRISnGEN Traffic feature is its production of detailed management reports. Using the Reports option, you can include specific traffic data in your reports. You can choose several criteria, including:

- specific reports
- date and time ranges
- collection devices
- ports
- customers
- sets of trunks
- attendants
- loops

IRISnGEN Traffic lets you schedule reports to generate automatically. Throughout the day, IRISnGEN Traffic automatically submits reports once or many times, as you choose. For example, you may wish to create a report every hour, every day. Simply create one report using the previous hour's data. This flexibility lets you create continuous reports with a single line entry. Using the Run Reports and Run Scheduler, you can create countless varieties of reports.

Standard Reports

The IRISnGEN Traffic System includes over thirty standard reports that provide both traffic summary and detail information. You can execute the reports on the server and send them to any printer accessible by the server.

You have many selectivity parameters that you can set to help you manage your reports. You can save the parameters you have entered, giving the report selector any name you choose. Then, later, you can run any report using your previously defined report selector.

Traffic reports are easy to schedule. Just choose a report and a report selector, define a scheduled time, and pick your report target. The rest is automatic. You can schedule reports to execute on selected days of the week or a certain day of the month or you can run a report on demand. A report queue display shows the status of scheduled reports.

With the optional Forwarding feature package, you can concurrently send reports to network printers, email them to multiple individuals, and fax them to multiple locations. You activate this feature using the report target sets. Each morning you can have an email in your inbox that summarizes the previous night’s activity. You can schedule periodic reports on critical



customer accounts for your personal attention, or send them directly to your customers via fax or email.

Traffic Studies

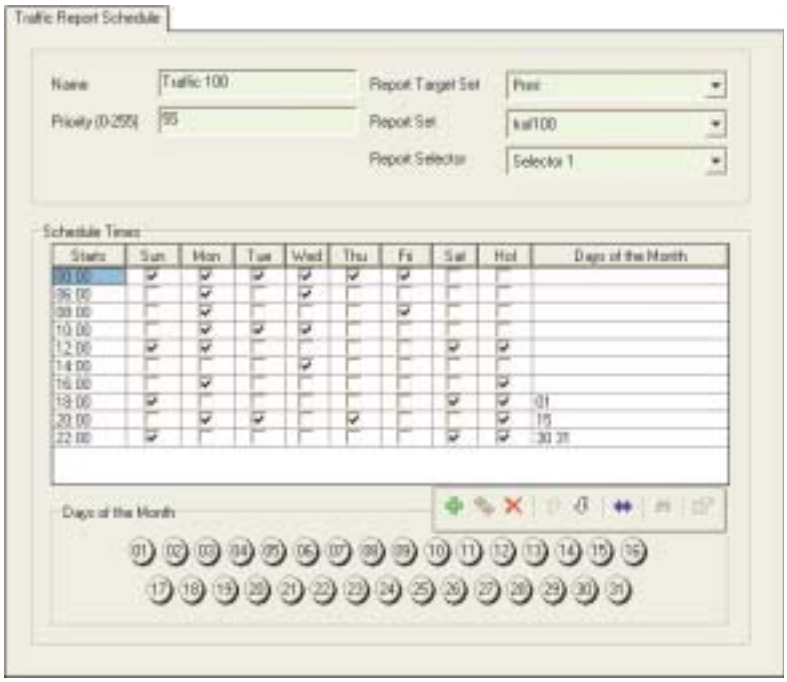
Traffic studies are essential for monitoring the performance of a *Meridian 1* because they help you identify potential network congestion problems and plan for future growth. The capabilities of IRISnGEN Traffic management allow you to execute detailed traffic studies for trunk, attendant, loop, and CPU service utilization. With these studies, you can determine your switch's needs and initiate corrective measures to maximize performance and improve cost-effectiveness.

Traffic Report Schedule

Use the Traffic Report Schedule option to schedule reports that run on selected days of the week, a particular day of the month, or a specific holiday, each with its own start time. You can schedule periodic reports on critical customer accounts, for your personal attention, or send them directly to your customers via fax or email on a periodic, recurring basis.

To create a traffic report schedule record

1 Right-click the **Traffic Report Schedule** folder and select **Add Traffic Report Schedule** from the list. The system opens the Traffic Report Schedule tab.



2 Type a name for the schedule in the **Name** field.

3 Type the priority level for this action in the **Priority** field. You can enter a number from 1 to 255. If more reports start than the system has resources, the reports with the highest priority start first. We recommend that you set a priority of 2 or lower for reports, since critical operations use priority 1 and you do not want to interfere with those functions.

4 Select a target set from the **Report Target Set** list. Sets identify the delivery destination for reports generated by the IRISnGEN server: to a printer, email, fax, or combination of these devices.

5 Select a set from the **Report Set** list. Report Sets are records containing groups of individual reports (as defined by Teltronics) to run as a batch.

6 Select a selector from the **Report Selector** list. A selector contains the selectivity parameters used to determine which records to include in the report.

7 Type the report's start time in the **Start Time** field. Format is *hh:mm* (hours:minutes). You must enter all four digits. For example, enter 04:00 to start at 4:00 AM. Enter 18:00 to start at 6:00 PM.

8 Select a **Day** checkbox for each day of the week you want your report to generate. For example, to generate every business day, select Monday, Tuesday, Wednesday, Thursday, and Friday.

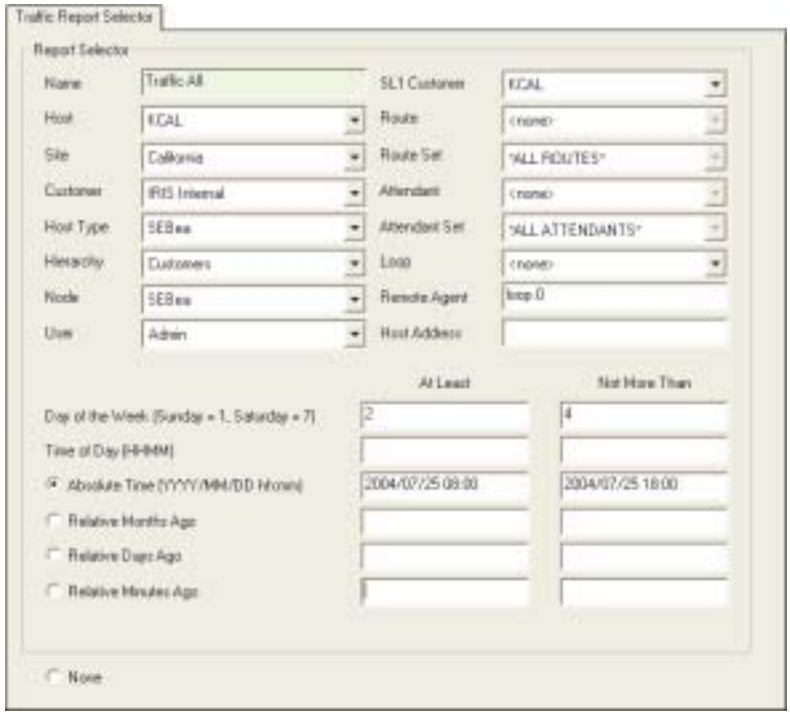
9 Select the **Days of Month** button that corresponds to the day(s) you want your report to generate. Reports will generate on the same date each month. For example, select **15** to generate your report on the 15th of each month. You can select any number of days.

Traffic Report Selectors

Use the Report Selectors option to define the criteria for your report. The more criteria you select, the more detailed the report. Use this information to run reports automatically or manually.

To create a traffic report selector record

1 Right-click the **Traffic Report Selector** folder and select **Add Traffic Report Selector**. The system opens the Traffic Report Selector tab.



2 Enter the name of the selector record in the **Name** field.



3 Select the most appropriate selection criteria for the selector record from the list for each of the next seven fields:
   - Host
   - Site
   - Customer
   - Host Type
   - Hierarchy
   - Node
   - User

4 Select an SL1 customer to limit your report to a single customer from the **SLI Customer** field. You must choose a host name before choosing an SL1 customer.

5 Select a route number in the **Route** list. IRISnGEN automatically collects and stores route information when it receives traffic data from the SL1. You must choose an SL1 customer before entering a route.

6 Select a route set from the **Route Set** list. Route sets are defined in the Route Sets Window, see page. You must choose an SL1 customer before entering a route set.

7 Select an attendant from the **Attendant** list. IRISnGEN automatically collects and stores attendant information when it receives traffic data from the SL1. You must choose an SL1 customer before entering an attendant.

8 Select an attendant set from the **Attendant Set** list. Attendant sets are defined in the Attendant Sets Window, see page. You must choose an SL1 customer before entering an attendant set.

9 Select a loop number from the **Loop** list. IRISnGEN automatically collects and stores loop information when it receives traffic data from the SL1. You must select a host before selecting a loop.

10 Type the name of the remote agent you want to report in the **CD** field, or leave the field blank to report traffic from all remote agents.

11 Type the address of the network device in the **Host Address** field. The address identifies host reporting to remote agents via hard contacts identified as HC1 though HC8, or network connections.

12 In the next two fields, type two entries to establish a range parameter. Include:

Field	What to enter
Day of the Week	Type the day numerically. For Sunday, enter 1; for Monday, 2; Tuesday, 3…Saturday, 7.
Time of Day	Enter the format *hhmm*, where *hh* is the two-digit hour, and *mm* is the two-digit minute. You do not need to enter any colons as separators between the hours and minutes.



13 Select one Absolute or Relative button and type a range parameter for your selection.

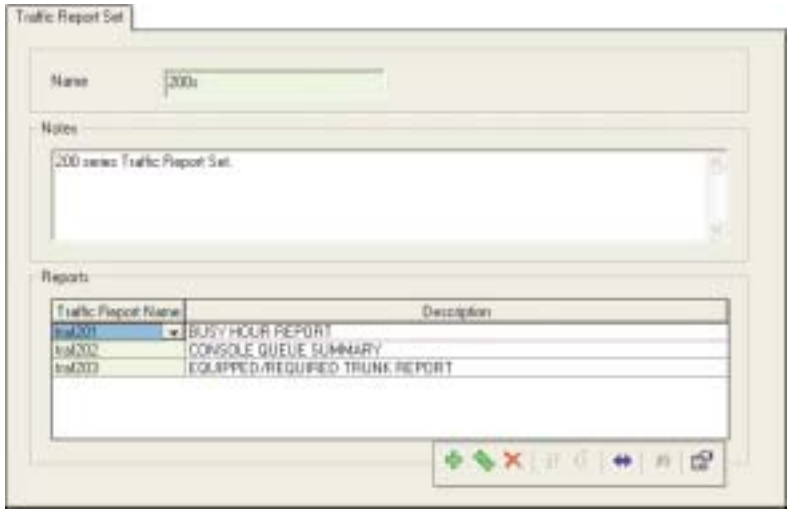
Field	What to enter
Absolute Time	Under the At Least heading, type the start time; under the Not More Than heading, enter the end time. Times are in the format *yyyymmdd*, where *yyyy* is the four-digit year, *mm* is the two-digit month, and *dd* is the two-digit day.
Relative Months Ago	Under the At Least heading, type the start number; under the Not More Than heading, enter the end number.
Relative Days Ago	Type the relative number of days ago. For example, 1 and 2 indicate traffic received between one and two days ago.
Relative Time (Minutes Ago)	Type how long ago you want to show traffic. For example, 1 and 20 indicate traffic from at least one minute ago, but not more than twenty minutes ago.
None	Select this button to ignore Absolute and Relative parameters.

Traffic Report Sets

You can group several traffic reports to run as a batch by use of Traffic Report Sets, or you can create a set with only one report, designated by a name of your choice.

To create a report set

1 Right-click the **Traffic Report Sets** folder and select **Add Traffic Report Set**. The system opens the Traffic Report Set tab.



2 Type the name of your report set in the **Name** field.

3 Type a description or comments about the report set in the **Notes** field. The maximum length is 256 characters.

4 Click the button to insert a blank row in the **Reports** data table, or press the button to add multiple rows.

5 Select a report name from the list.

6 Repeat steps 4 and 5 to add additional report names.

IRISnGEN automatically enters the description for each report contained in the report set.

To delete a report from the set

- Highlight a traffic report name and press the button.

Traffic Reports

Your IRISnGEN system comes with a variety of pre-defined traffic reports. Use the Traffic Reports option to access information about these reports, or if you have the optional IRISnGEN Ad Hoc Report module, create your own custom reports and add them to your report list. Use these reports when defining a report schedule or when you run reports manually.

To display a traffic report

1 Expand the **Traffic Report** folder.

2 Click a report from the list to display the Traffic Report tab for that report.



3 The following list describes the fields in this window:

Field	What it means
Name	The name of the report.
File Name	The name of the report file as defined by Teltronics. Do not change this information.
Notes	Information entered to explain the content of this report type.

Custom Reports

If you purchased the IRISnGEN Ad Hoc Reporter module, or the Crystal Reports Pro module, you can create your own custom traffic report. Once created, you must save the report with the .rpt extension and store the report in a location that IRISnGEN can access.

To create a custom traffic report record

1. Create and save your report using the IRISnGEN Ad Hoc Reporter or Crystal Reports Pro module.
2. Right-click the **Traffic Reports** folder and select **Add Traffic Report**.
3. Type the name of your report in the **Name** field.
4. In the **File Name** field, click the ... button and navigate to the location where you stored your custom report.
5. Select the report you want to include and click ***Open***.
6. Type any additional information about this report in the **Notes** field.

Traffic Report Formats

The IRISnGEN Traffic System management reports condense traffic data into a printed form that you can use to isolate, diagnose, and report problems occurring in *Meridian 1* PBXs. Use the Reports window to define the parameters for each report. Then use the Report Number Selection field to select a variety of predefined report formats.

Report formats offered by the IRISnGEN Traffic System:

100 TRUNK USAGE HOURLY DETAIL BY ROUTE
101 TRUNK USAGE DAILY DETAIL BY ROUTE
102 TRUNK USAGE SUMMARY BY ROUTE
103 TRUNK USAGE SUMMARY - PART1
104 TRUNK USAGE SUMMARY - PART2
110 TRAFFIC HOURLY DETAIL
111 TRAFFIC DAILY DETAIL
112 TRAFFIC SUMMARY
120 ATTENDANT QUEUE HOURLY DETAIL
121 ATTENDANT QUEUE DAILY DETAIL
122 ATTENDANT QUEUE SUMMARY
130 ATTENDANT HOURLY DETAIL
131 ATTENDANT DAILY DETAIL
132 ATTENDANT SUMMARY
140 SYSTEM LOOP HOURLY DETAIL
142 SYSTEM LOOP SUMMARY
143 TRAFFIC LOOP BRIEF SUMMARY
150 DIAL TONE DELAY AND CPU LOAD HOURLY DETAIL
151 DIAL TONE DELAY AND CPU LOAD DAILY DETAIL
152 DIAL TONE DELAY AND CPU LOAD SUMMARY
153 CPU LOAD HOURLY DETAIL
154 CPU LOAD DAILY DETAIL



155 CPU LOAD SUMMARY
160 SERVICES UTILIZATION HOURLY DETAIL
162 SERVICES UTILIZATION SUMMARY
163 SERVICES UTILIZATION BRIEF
179 PARSED DATA DAILY DETAIL
180 JUNCTOR TRAFFIC REPORT SUMMARY

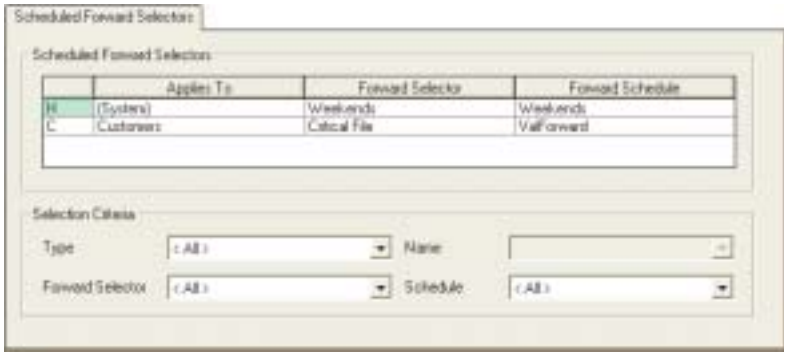
Most IRISnGEN Traffic System reports use the same output formats. In many cases, these reports share common headers. These headers help identify the reports and include the location name, selector name, report number, and time and date the report prints. The headers also include constraint information, as well as columns displaying a breakdown of data.

Scheduled Forward Selectors

You can create forward selectors that become active on a schedule. Scheduled forward selectors override forward selectors assigned directly to the same customer, site, host, or host type record. Should you modify a forward selector while that schedule is active, IRISnGEN will not implement the modification until the next scheduled start time. To stop forwarding before a schedule expires, use the Delete option on the Active Forward Selectors tab. You must create your forward selectors and forward schedules before assigning them in this screen.

To add a scheduled forward selector record

1 Click the **Scheduled Forward Selectors** folder. The system opens the Scheduled Forward Selectors tab.

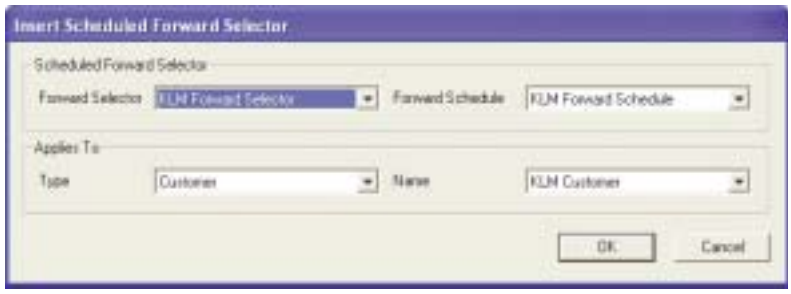


2 Select a type to assign this selector to a host, site, customer, system, or host type from the **Type** list.
3 Select a host, site, or customer (depending on your Type selection) from the **Name** list. No selection is necessary if you select “System.”
4 Select a pre-defined forward selector from the **Forward Selector** list.
5 Select a pre-defined forward schedule from the **Schedule** list.

When you finish your selection criteria the results appear in the Scheduled Forward Selectors data table (grid) portion of the screen.

To insert a new scheduled forward selector

1 Click the **Scheduled Forward Selector** folder; then, select **Insert Scheduled Forward Selector**. The system opens the Insert Forward Selector dialog box.



2 From the lists on the dialog, select a forward selector, forward schedule, type, and name. You must select a value for each field.

3 Click ***OK***.

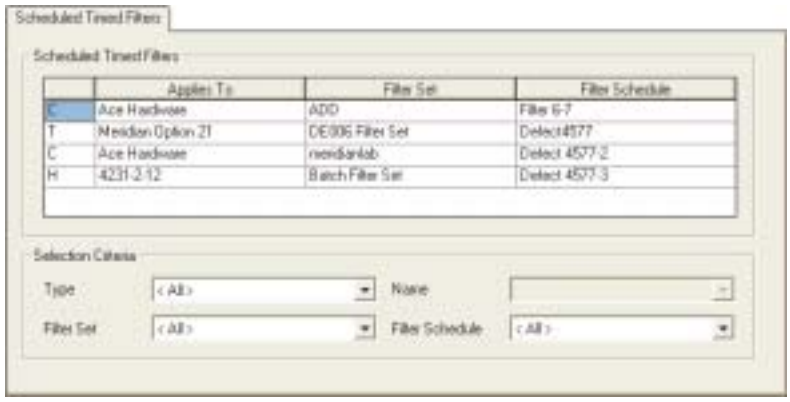
The system inserts a new line into the Scheduled Forward Selector screen with the information you choose.

Scheduled Timed Filters

Timed filters function like standard filters, but are valid for a limited time, only. For example, you may have alarms that you want to ignore for one hour while performing system maintenance; then, return to normal processing when that time expires. Use the Scheduled Timed Filters tab to schedule filters for host, sites, and customers. You must have already created your Filter Sets and Filter Schedules before assigning them in this screen.

To view a scheduled timed filter

1 Click the **Scheduled Timed Filters** folder. The system opens the Scheduled Timed Filters tab.



2 Select a type to assign this selector to a host, site, customer, system, or host type from the **Type** list.

3 Select a host, site, or customer (depending on your Type selection) from the **Name** list. No selection is necessary if you select “System.”

4 Select a pre-defined filter set from the **Filter Set** list.

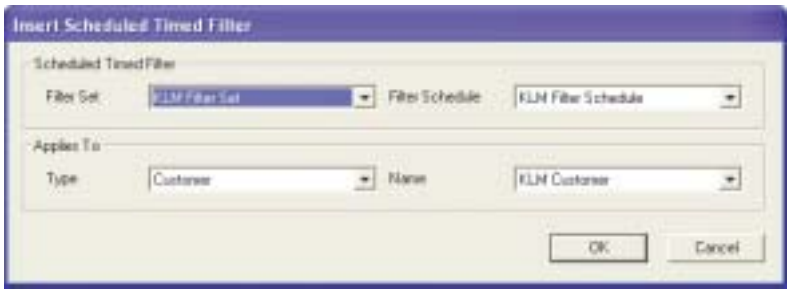
5 Select a pre-defined filter schedule from the **Filter Schedule** list.

6 When you finish your selection criteria the results appear in the Scheduled Timed Filters data table (grid) portion of the screen.



To insert a new scheduled timed filter

1 Right-click the **Scheduled Timed Filter** folder and select **Insert Scheduled Timed Filter**. The system opens the Insert Scheduled Timed Filter dialog.



2 From the lists, select a filter set, filter schedule, type, and name. You must select a value for each field.

3 Click ***OK***.

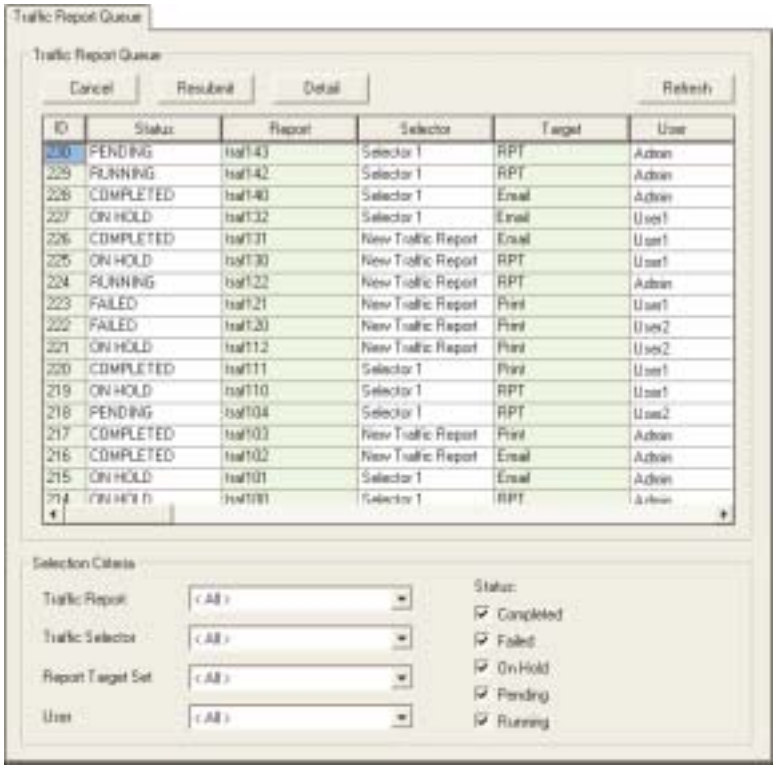
The system inserts a new line into the Scheduled Timed Filter screen with the information you chose.

Traffic Report Queue

Use the Traffic Report Queue to view information about traffic reports that ran recently, or that are queued to run at a later time. The entries in the Report Queue age according to the system parameters set by the system administrator. An entry moves down the list depending on its priority and time in queue.

To view records in the Traffic Report Queue

1 Click the **Traffic Report Queue** folder. The system opens the Traffic Report Queue tab.



2 Select a report type from the **Traffic Report** list. These reports are pre-defined by Teltronics.

3 Select a report selector from the **Traffic Selector** list. This selector contains report selectivity parameters.

4 Select a target set from the **Report Target Set** list. These sets determine your report destination: printer, e-mail, fax, pager, or combination of these devices.

5 Select a user from the **User** list, or select Auto to view all.

6 Select a **Status** checkbox for each status type you want to include. You can select up to five checkboxes.

The following describes the Traffic Report Queue grid fields.

Field	What it displays
ID	The number assigned to each entry in the Traffic Report Queue.
Status	The current status: completed, failed, on hold, pending, running.
Report	The name of the report in the queue.
Report Selector	The name of the report selector used to create this report.
Target	The destination of the report assigned in the Report Target Set Screen.
User	The name of the person who initiated this report. The field will say AUTO if the report was automatically generated.
Pri (Priority)	The priority assigned to the report. This is a number from 1 to 255. Numbers with the highest priorities are handled first.
Submitted	The time and date that the report was submitted to the queue.
Run	The time and date that the report ran.
Cancel Request	Cancel any report with a status of PENDING or RUNNING. The status changes to HOLD and remains visible on the screen. The system purges it when it reaches the age-date threshold.
Resubmit	Submit a FAILED or ON HOLD report for processing.
Detail	Display additional information about the highlighted report, including the Failure Code field. A failure code of **0** means that the report completed without failure. See “Failure Codes” in the online help for a complete list of failure codes.



Selectivity	Open the Report Selectivity parameters screen. This shows you the parameters assigned to the report currently in the queue. This is for display purposes only — you cannot change this information here.
Close	Exit the tab.



Note



5

IRISnGEN Libraries

Using IRISnGEN Libraries, you can configure actions and attributes for customers, sites, hosts, and remote agents in the IRISnGEN system. The IRIS Libraries folder contains several sub-folders containing the records that control your IRISnGEN system. These sub-folders include:

- **Alarms** define when and how to process alarms generated by the host.
- **Contact** lists the addresses, telephone numbers, and other information necessary to reach key personnel when reporting alarms to IRISNGEN.
- **Hierarchies** list logical groupings of customers, sites, or host types in the IRISNGEN system.
- **Holidays** lists the holidays or non-business days when the IRISnGEN system handles alarms different from normal business days.
- **Host Types** defines logical characteristics of the hosts.
- **Remote Agent Types** defines and classifies the remote agents (SEBea, SEB II, Dispatcher) that your IRISnGEN system monitors.

This chapter explains how to use IRISnGEN to create the IRISnGEN libraries and library records and how to define the parameters for each record. Once you create a library record, you can assign it to customers, site, or hosts, as needed.

Alarms

With the IRISnGEN system's Alarm feature, you can identify and select the alarms and other events generated by your host and remote agents. You can then combine alarms and group them according to their level of importance, filter unwanted data, add plain-English text messages, apply action thresholds and scripts that automatically respond to the alarm.

The Alarms folder includes several sub-folders that help you define the alarms in your IRISnGEN system. These folders include:

- **Correlations** combine multiple events into a single alarm.
- **Escalation Groups** increase an alarm's level of importance and the actions the IRISnGEN system should take when the level increases.
- **Filters** allow you to skim through the alarm data and to report only the information that interests you.
- **Forwarding** defines when and how to send alarms to selected destinations, such as email addressed or printers.
- **Messages** define alarm keywords, text messages, and special procedures used to handle the alarms.
- **Superscripts** automate actions in response to alarms.
- **Thresholds** define the minimum and maximum alarm levels the IRISnGEN system uses to act on an alarm.



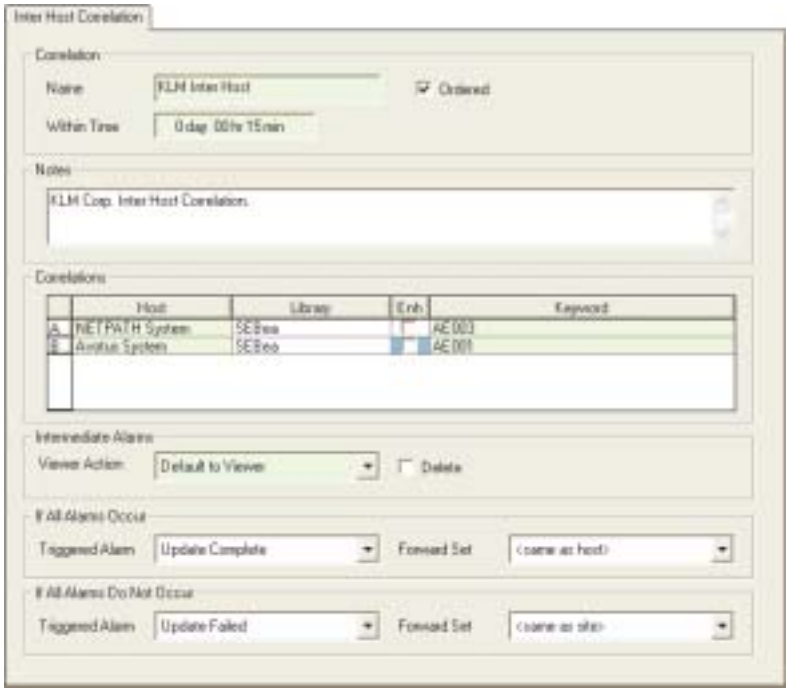
Correlations

Alarm correlation monitors the occurrences of multiple events within a defined time. This reduces your alarm count by associating and combining related events. Use the Inter Host Correlation tab to correlate alarms occurring within multiple hosts. Use the Single Host Correlation tab to correlate alarms within a single host. You can include an unlimited number of alarm keywords as part of a correlation set on either tab.

Inter Host Correlations

To create an inter-host correlation

1 Right-click the **Inter Host Correlations** folder; then, select **Add Correlation** from the pop-up menu. the system opens the Inter Host Correlation tab.



2 Type a name for the correlation set in the **Name** field. Enter something meaningful to remind you of the record's purpose.

3 Select the **Ordered** checkbox to evaluate the correlation keywords by order of entry. In the example above, the system must find the keyword AE003 before finding AE001 for the correlation to be valid.

4 Type the time that the system must find all keywords for the correlation to take affect in the **Within Time** field. Type all numbers in a two-digit format (*DDHHMM*). Do not type colons between fields. You must enter a minimum of 01 minutes. In the example above, the system must find the second keyword within fifteen minutes from finding the first keyword for the correlation to be valid.

5 Type any description or comments in the **Notes** field. You can enter up to 256 characters.

6 Use the **Correlations** data table to display detail information for each keyword and library in the correlation. The first column specifies the order of occurrence for each keyword with an alpha character.

7 Select a predefined host from the **Host** list. Inter Host Correlation requires at least two different hosts.

8 Select a library from the **Library** list.



9 The **Enh** checkbox is information-only. A checkmark in the checkbox indicates the keyword is an enhanced keyword. An enhanced keyword has variables assigned to it in a keyword template. See ”Keyword Templates’, page 5-34.

10 Select a keyword from the **Keyword** list.

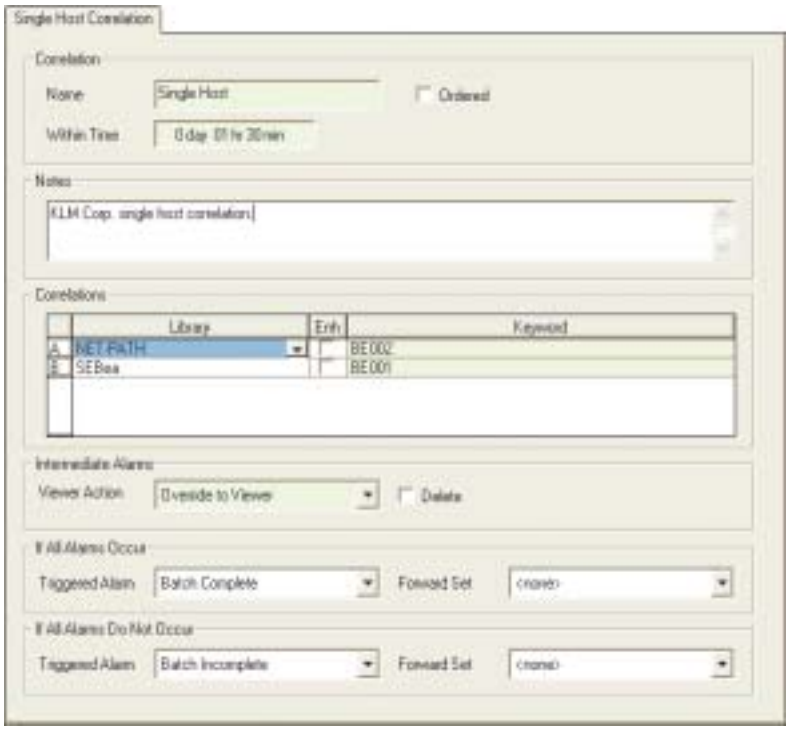
11 Use the **Viewer Action**, **Triggered Alarm**, and **Forward Set** lists to select the parameters that define how IRISnGEN should process the alarms and whether to trigger alarms.

Single Host Correlation

Single host correlations associate and combine keywords for a single host. You can assign single host correlations to a host using the host’s Threshold and Correlations tab. See ”Thresholds and Correlations Tab’, page 2-20.

To create a single host correlation

1 Right-click the **Single Host Correlations** folder; then, select **Add Correlation** from the pop-up menu. the system opens the Single Host Correlation tab.



2 Type a name for the correlation set in the **Name** field. Enter something meaningful to remind you of the record’s purpose.

3 Select the **Ordered** checkbox to evaluate the correlation keywords by order of entry.

4 Type the time that the system must find all keywords for the correlation to take affect in the **Within Time** field. Type all numbers in a two-digit format (*DDHHMM).* Do not type colons between fields. You must enter a minimum of 01 minutes. In the example above, the system must find the second keyword within one hour and thirty minutes from finding the first keyword for the correlation to be valid.

5 Type any description or comments in the **Notes** field. You can enter up to 256 characters.

6 Use the **Correlations** data table to display detail information for each keyword and library in the correlation. The first column specifies the order of occurrence for each keyword with an alpha character.

7 Select a library from the **Library** list.

8 The **Enh** checkbox is information-only. A checkmark in the checkbox indicates the keyword is an enhanced keyword. An enhanced keyword has variable assigned to it in the keyword template. See ”Keyword Templates’, page 5-34.

9 Select a keyword from the **Keyword** list.

10 Use the **Viewer Action**, **Triggered Alarm**, and **Forward Set** lists to select the parameters that define how IRISnGEN should process the alarms and whether to trigger alarms.



Note *You must assign your correlation to a host before will become effective.*

Passing event variables to triggered events

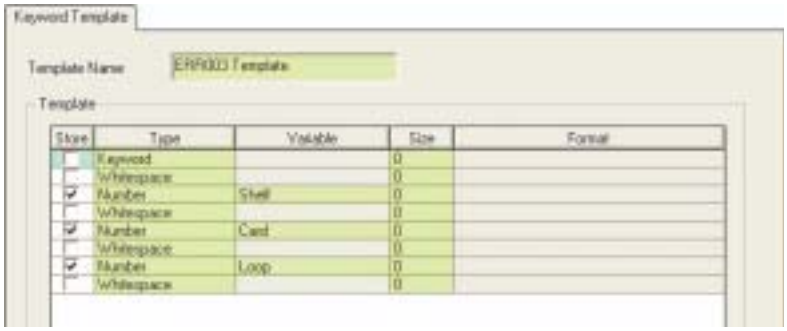
IRISnGEN can pass variables and data from one event to a second event triggered by a threshold or a correlation. The variables and data of the first event become the variable values of the triggered event.

For IRISnGEN to pass the variables and data, it must apply a keyword template to both events. The data passes to the triggered event in the order it was received and defined in the keyword template. The variables from the first event take the form variable_name:variable_data in the triggered event. Therefore, it is important that the keyword template you apply to both events accurately match the structure of the event and have meaningful variable names.

Example 1 – Simple Threshold Event

You receive frequent alarms from faulty equipment. It is not a problem until it occurs three times within ten minutes. You have decided to use a threshold to determine the frequency of the alarm and to stop any additional reporting of the same alarm.You then want to look for the events that are triggered when the threshold is reached and, if the threshold is exceeded, what equipment caused the fault, so that a repair can be initiated. In this example, assume we receive the event ERR003 with the variable data 001, 002, 003. It appears as: *ERR003 001 002 003*, which identify the shelf, card, and loop.

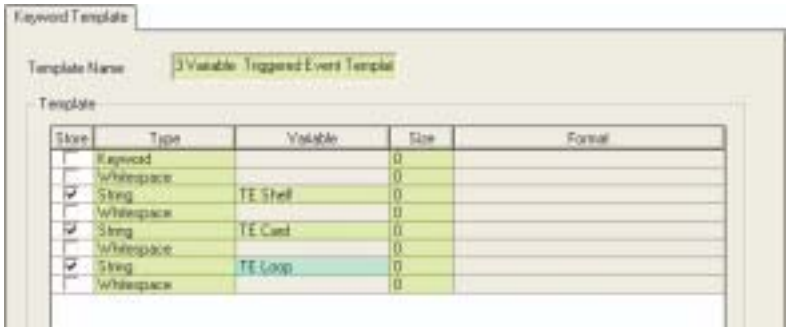
1 Create a keyword template and apply it to the first event so that you can capture the variable data. Here we define variables, **Shelf**, **Card**, and **Loop**.





Warning *Be sure to selectthe* ***Store*** *checkbox for each variable. Do not select the checkbox for Keyword. Selecting the Keyword checkbox prevents the variables frompassing to the triggered event.*

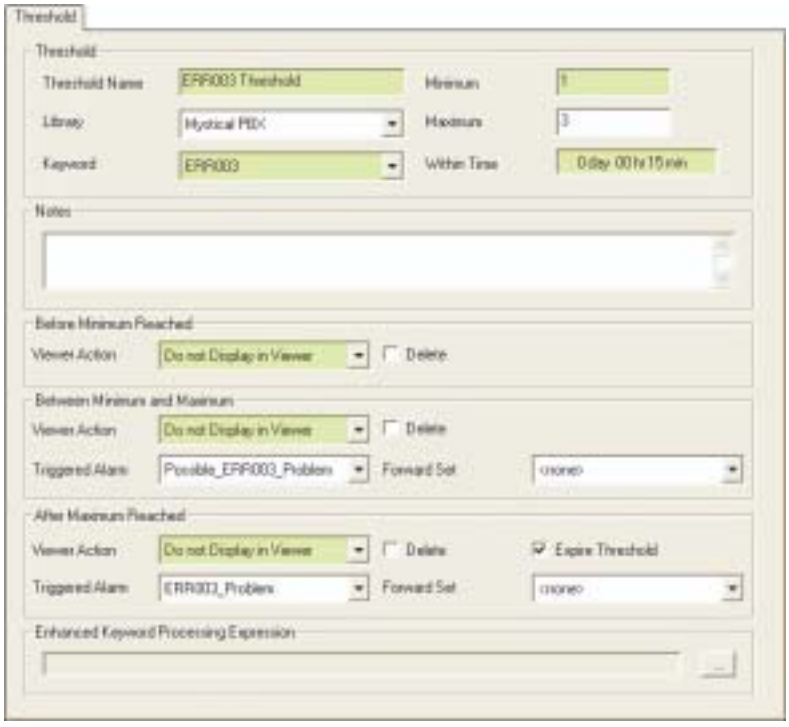
2 Create a second keyword template and apply it to the triggered event.



Notice that the variable types differ between the two templates. This is because the first event variable data is numeric in type. When the data passes to the triggered event, it is pre-pended with a variable name. Therefore the keyword template for the triggered event must have a type defined as a string.

You could simplify this process by assigning the String variable type to the first template; then, apply the template to both events. However, if a processing expression is involved (e.g. LOOP > 100), you cannot use a String variable type since it is inconsistent with a mathematical expression.

3 Create a threshold that lists the event, prevents intermediate events from displaying on the List Viewer, and triggers new events that will then be displayed in their place.

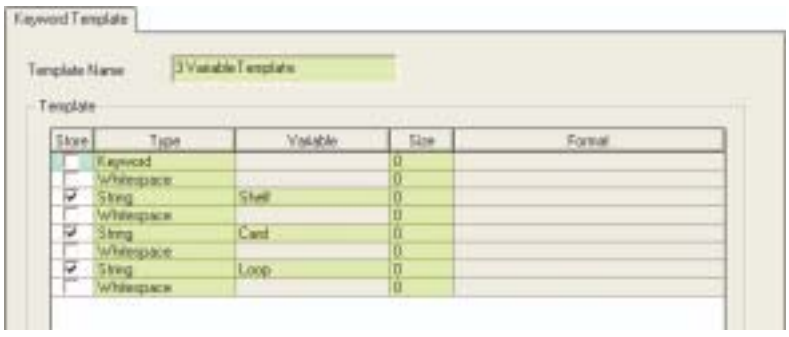


If you are unsure of how to construct the triggered event's template, you can generate one and look at the alarm text. Notice that alarm text will generally expand as variable data is passed along from stage to stage.

Example 2 – Simple Ordered Correlation

You want to monitor for two events from the same piece of equipment. If either event occurs, it is not a problem. However, if both occur within ten minutes of one another, a problem has occurred and you need to take action. Use a simple ordered correlation to monitor for this situation, telling it to trigger events based on the correlation being satisfied, or not satisfied. If the correlation is satisfied, it is to inform you which piece of equipment caused the fault so that it can be repaired. In this example, assume we are looking for the events DTA005 and DTA007.

1 Create a keyword template (as you did in Example 1); then apply it to both events (DTA005 and DTA007). To simplify matters, we assigned a String value type to the variables.





Note *The system passes the variable data from the first event received to the correlation's triggered events.*

2 Create a correlation. Be sure to define the triggered events to apply if all alarms occur, or if no alarms occur.

Example 3 – Variables Before the Keyword

You need to track an event using a threshold, but the incoming event has pertinent variable data that appears before the keyword.

When all or part of the variable data occurs before the keyword of the first event, it passes to the triggered event and is placed after the keyword. In this case, you must apply different keyword templates to the first and triggered events.

1 Create a keyword template and apply it to the first event so that you can capture the variable data.

2 Create a second keyword template and apply it to the triggered event.

passed to the triggered event.

Escalation Groups

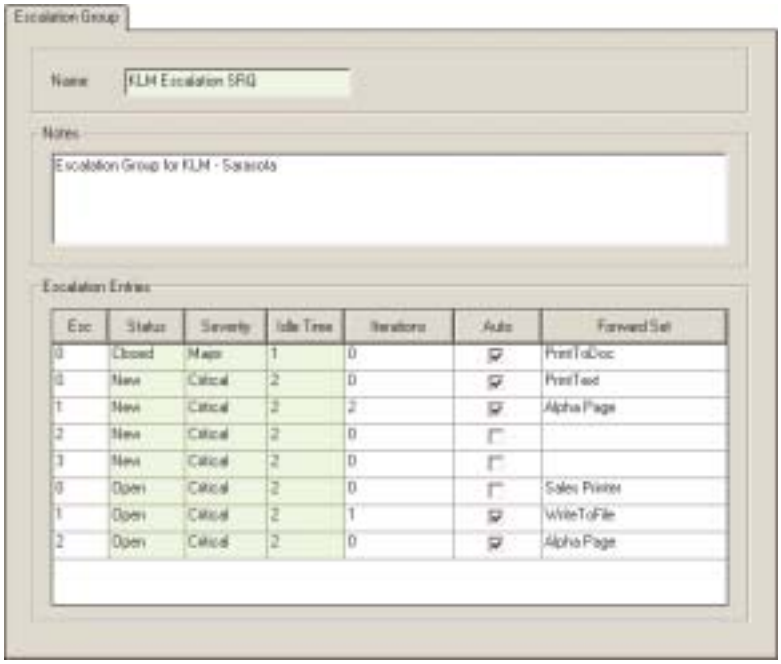
You can define when alarms (in a particular state) increase to the next level of importance and what actions the IRISnGEN system should take when the escalation occurs.

The system uses escalation groups to look for alarms using four parameters: current escalation level (0-99), alarm status (new, open, closed), severity (critical, major, minor, informational, undefined), and the amount of time the alarm is in that state. When an alarm matches the escalation criteria, the system increments the level of that alarm, thus making it more noticeable to the user. The system can also forward the alarm. The severity of an alarm is unchanged by the correlation group. A minor alarm remains a minor alarm even though it may reach escalation level 99. Be sure to define your forward sets in your database BEFORE you create your escalation groups.



To add an escalation group record:

1 Right-click the **Escalation Groups** folder and choose **Add Escalation Group**. The system opens the Escalation Group tab.



2 Type the name of the escalation group in the **Name** field.

3 Type any description or comments, such as why you created the record, in the **Notes** field.

4 The Escalation Entries display shows you all the line entries defined in this escalation group. The fields for the Escalation Entries data table follow.

5 Type the escalation level for this entry in the **Esc** field. All new alarms enter the system with an escalation number of 0. The maximum level is 99. The higher the number, the higher the escalation.

6 Select a status code from the **Status** list; then, select a severity code from the **Severity** list.

7 Type the idle time in seconds in the **Idle Time** field.

8 Type the number of iterations allowed in the **Iterations** field. Iterations define how many times the idle timer can expire before moving to the next escalation level. Enter values between 0 and 99.

9 Select the **Auto** checkbox to set the escalation level to automatically increment when the idle time expires. If set to 0, the alarm can only be escalated manually from the Viewer window.

10 Select a pre-defined forward set from the **Forward Set** list.

11 Save your record.



Filters

A filter examines each event coming into IRISnGEN for qualifying criteria; then, processes and forwards it accordingly. A filter analyzes input data, determines an action, then passes it on for continued processing.

Using the IRISnGEN system's Filter feature, you can selectively sort alarms and other events passing through a desired range of alarms while suppressing the others. The Filter folder contains files and sub-folders you can use to define the filters in your IRISnGEN system. It includes:

- **Filter Actions** defines how an alarm is processed.
- **Filter Schedules** defines when to filter alarms.
- **Filter Sets** group filter definitions into sets for processing.

Filter Actions

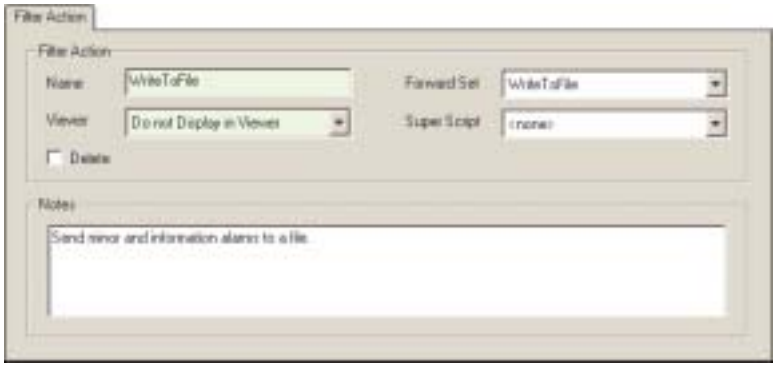
Filter actions control how IRISnGEN processes each alarm. IRISnGEN starts a filter action when it matches a keyword in a filter set with data from the alarm text.



Note *If you wish to use forward sets in your filter action, you must define these before creating the filter action record.*

To add a filter action record

1. Right-click the Filter Actions folder; then select Add Filter Action. The system opens the Filter Action tab.



2. Type the filter action name in the **Name** field.
3. Select a forward set from the Forward Set list to forward the alarm to a pre-defined set of destinations.
4. Select an option from the **Viewer** list.
   - **Override to Viewer** displays selected alarm in the Viewer. This option overrides all other filter viewer selections, except Delete.
   - **Do Not Display in Viewer** prevents the selected alarm from displaying in the Viewer, but still stores the event in the database.
   - **Default to Viewer** sends alarms to the Viewer if not other process prevents it.
5. Select a script from the **Superscript** list to start when IRISnGEN matches a keyword.
6. Select the **Delete** checkbox to delete any events that match the filter. Deleted events will not appear in the List Viewer or in the History file, nor will any forward set or Superscript execute.



Warning *Selecting the Delete checkbox overrides all other selections! The alarm will not be stored anywhere in the system.*

7 Type any description or comments about the filter action in the **Notes** field. The maximum length is 256 characters.

8 Save your Filter Action record.

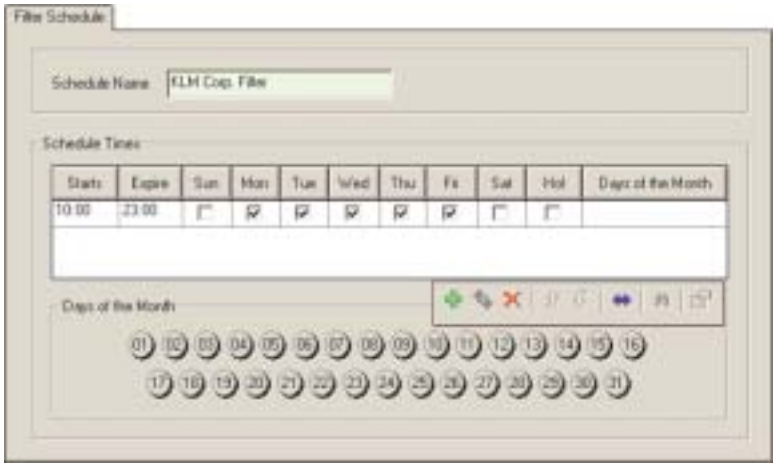
Filter Schedules

You can define filter schedules for nights, weekends, holidays or any time when your alarms processing is handled differently than normal.

Note *You must create your filter sets before defining your timed filters.*

To add a filter schedule record

1 Right-click the Filter Schedule folder; then, select Add Filter Schedule from the pop-up menu. The system opens the Filter Schedule tab.



2 Type the name of the schedule in the **Schedule Name** field.

3 Type the time that the schedule should start in the **Starts** field. The field format is *hh:mm* (hours:minutes). You must enter all four digits. For example, type 16:00 to start at four o'clock in the afternoon.

Note *Use the right and left arrow keys to move between the time digits or to move between columns. Use the up and down arrow keys to move between rows. Press the space bar to add or remove the checkmark in a checkbox field.*

4 Type the time the filter should stop in the **Expire** field.

Note *This field appears on the Filter Schedule or the Forward Schedule windows. It does not appear on the Poll Schedule window.*

5 Select a **Day** checkbox for each day you want this schedule to be active. Select the **Holiday** checkbox if you want it active on holidays.

6 Using the thirty-one **Days of the Month** buttons, select the day(s) that you want your filter schedule to run. Be sure you do not have any Days selected. Days of the Month override days of the week selections.

7 Save your Filter Schedule record.

Filter Sets

You can use the IRISnGEN system's Filter Sets feature to separate groups of alarms for special processing. You can assign filter sets to customer, site, host, or host type records.

The Filter Sets folder contains three sub-folders you can use to define filter sets. It includes:

- **Keyword Filter Sets -** filter alarms by keywords.
- **Severity Filter Sets -** filter alarms by severity.
- **String Filter Sets** - filter alarms by character strings.



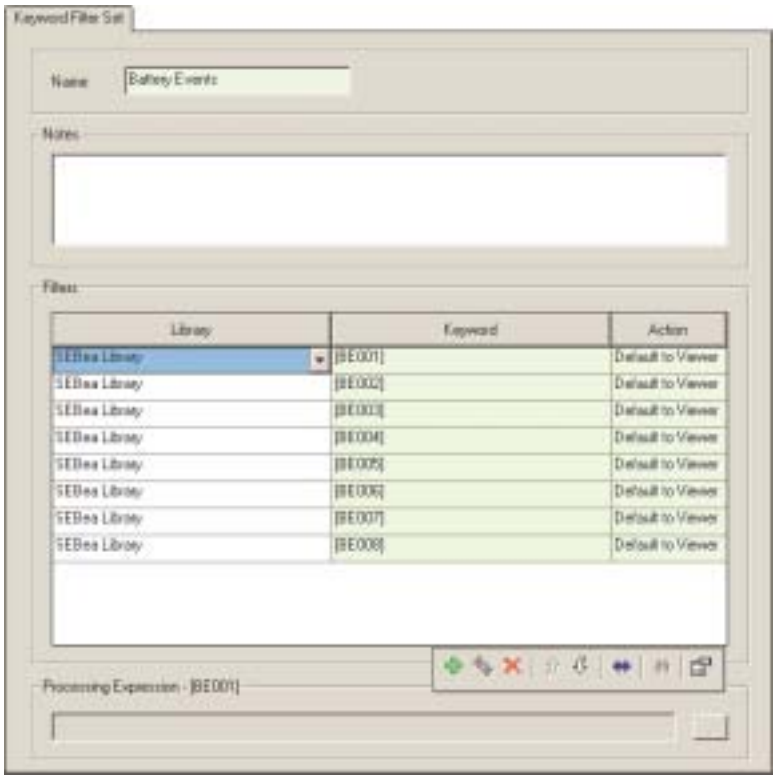
Note *You must define your filter actions in your database before you create your filter sets.*

Keyword Filter Sets

Use keyword filter sets to filter alarms using keywords or enhanced keywords.

To add a keyword filter set record

1 Right-click the Keywords Filter Sets folder; then, select Add Filter Set. The system opens the Keyword Filter Set tab.



2 Type the filter set name in the **Name** field.

3 Type any description or comments about the keyword filter set in the **Notes** field. The maximum length is 256 characters.

4 Select a keyword library from the **Library** list.

5 Select the keyword you want to trigger the filter from the **Keyword** list.

6 Select the action IRISnGEN should take if the keyword is found from the **Action** list.

7 Click the ... button to open the Expression Builder; then, create an expression to evaluate the variable. The expression appears in the **Processing Expression** field. The Processing Expression field is only available when you select a keyword that has a template assigned.

8 Save your Keywords Filter Set record.



Regular Expression Filter Sets

Regular expressions specify the rules for the set of possible strings that you want to match; this set might contain English sentences, or e-mail addresses, or TeX commands, or anything you like. You can then ask questions such as ``Does this string match the pattern?", or ``Is there a match for the pattern anywhere in this string?". You can also use REs to modify a string or to split it apart in various ways.

Regular expressions can be concatenated to form new regular expressions; if A and B are both regular expressions, then AB is also a regular expression. In general, if a string p matches A and another string q matches B, the string pq will match AB. This holds unless A or B contain low precedence operations; boundary conditions between A and B; or have numbered group references. Thus, complex expressions can easily be constructed from simpler primitive expressions.

The regular expression language is relatively small and restricted, so not all possible string processing tasks can be done using regular expressions. There are also tasks that can be done with regular expressions, but the expressions turn out to be very complicated. In these cases, you may be better off writing Python code to do the processing; while Python code will be slower than an elaborate regular expression, it will also probably be more understandable.

To create a regular expression filter set record

1. Right-click the **Regular Expression** folder; then, select **Add Filter Set**. The system opens the Regular Expression Filter Set tab.
2. Type a descriptive name in the **Name** field.
3. Type any description or comments about the string filter set in the **Notes** field.
4. Use the data table toolbar to add rows to the **Filters** data table.
5. Click inside the **String** field; then, enter the string you want to filter.

   Regular expressions can contain both special and ordinary characters. Most ordinary characters, like "A", "a", or "0", are the simplest regular expressions; they simply match themselves. You can concatenate ordinary characters, so last matches the string 'last'. Some characters, like "|" or "(", are special. Special characters either stand for classes of ordinary characters, or affect how the regular expressions around them are interpreted. For a list of valid regular expression characters, see ”Regular Expression Characters’, page 5-14.
6. Select a filter action from the **Action** list.
7. Type the position (0-32767) where the text string you are filtering for will appear in the **Position** field.
8. Select a type from the **Type** list that determines if the filter string will be in the Alarm text, or in the Optional text of the alarm.
9. Save your record.



Regular Expression Characters

Character	Description
"." (Dot.)	In the default mode, this matches any character except a newline. If the DOTALL flag has been specified, this matches any character including a newline.
"^" (Caret.)	Matches the start of the string, and in MULTILINE mode also matches immediately after each newline.
"$"	Matches the end of the string or just before the newline at the end of the string, and in MULTILINE mode also matches before a newline. foo matches both 'foo' and 'foobar', while the regular expression foo$ matches only 'foo'. More interestingly, searching for foo.$ in 'foo1\nfoo2\n' matches 'foo2' normally, but 'foo1' in MULTILINE mode.
"*"	Causes the resulting RE to match 0 or more repetitions of the preceding RE, as many repetitions as are possible. ab* will match 'a', 'ab', or 'a' followed by any number of 'b's.
"+"	Causes the resulting RE to match 1 or more repetitions of the preceding RE. ab+ will match 'a' followed by any non-zero number of 'b's; it will not match just 'a'.
"?"	Causes the resulting RE to match 0 or 1 repetitions of the preceding RE. ab? will match either 'a' or 'ab'.
*?, +?, ??	The "*", "+", and "?" qualifiers are all greedy; they match as much text as possible. Sometimes this behavior isn't desired; if the RE <.*> is matched against '<H1>title</H1>', it will match the entire string, and not just '<H1>'. Adding "?" after the qualifier makes it perform the match in non-greedy or minimal fashion; as few characters as possible will be matched. Using .*? in the previous expression will match only '<H1>'.
{m}	Specifies that exactly m copies of the previous RE should be matched; fewer matches cause the entire RE not to match. For example, a{6} will match exactly six "a" characters, but not five.
{m,n}	Causes the resulting RE to match from m to n repetitions of the preceding RE, attempting to match as many repetitions as possible. For example, a{3,5} will match from 3 to 5 "a" characters. Omitting m specifies a lower bound of zero, and omitting n specifies an infinite upper bound. As an example, a{4,}b will match aaaab or a thousand "a" characters followed by a b, but not aaab. The comma may not be omitted or the modifier would be confused with the previously described form.
{m,n}?	Causes the resulting RE to match from m to n repetitions of the preceding RE, attempting to match as few repetitions as possible. This is the non-greedy version of the previous qualifier. For example, on the 6-character string 'aaaaaa', a{3,5} will match 5 "a" characters, while a{3,5}? will only match 3 characters.



"\"	Either escapes special characters (permitting you to match characters like "*", "?", and so forth), or signals a special sequence; special sequences are discussed below. If you're not using a raw string to express the pattern, remember that Python also uses the backslash as an escape sequence in string literals; if the escape sequence isn't recognized by Python's parser, the backslash and subsequent character are included in the resulting string. However, if Python would recognize the resulting sequence, the backslash should be repeated twice. This is complicated and hard to understand, so it's highly recommended that you use raw strings for all but the simplest expressions.
[]	Used to indicate a set of characters. Characters can be listed individually, or a range of characters can be indicated by giving two characters and separating them by a "-". Special characters are not active inside sets. For example, [akm$] will match any of the characters "a", "k", "m", or "$"; [a-z] will match any lowercase letter, and [a-zA-Z0-9] matches any letter or digit. Character classes such as \w or \S (defined below) are also acceptable inside a range. If you want to include a "]" or a "-" inside a set, precede it with a backslash, or place it as the first character. The pattern []] will match ']', for example. You can match the characters not within a range by complementing the set. This is indicated by including a "^" as the first character of the set; "^" elsewhere will simply match the "^" character. For example, [^5] will match any character except "5", and [^^] will match any character except "^".
"|"	A|B, where A and B can be arbitrary REs, creates a regular expression that will match either A or B. An arbitrary number of REs can be separated by the "|" in this way. This can be used inside groups (see below) as well. As the target string is scanned, REs separated by "|" are tried from left to right. When one pattern completely matches, that branch is accepted. This means that once A matches, B will not be tested further, even if it would produce a longer overall match. In other words, the "|" operator is never greedy. To match a literal "|", use \\|, or enclose it inside a character class, as in [|].
(...)	Matches whatever regular expression is inside the parentheses, and indicates the start and end of a group; the contents of a group can be retrieved after a match has been performed, and can be matched later in the string with the \number special sequence, described below. To match the literals "(" or ")", use \(or \), or enclose them inside a character class: [(] [)].
(?...)	This is an extension notation (a "?" following a "(" is not meaningful otherwise). The first character after the "?" determines what the meaning and further syntax of the construct is. Extensions usually do not create a new group; (?P<name>...) is the only exception to this rule. Following are the currently supported extensions.



(?iLmsux)	(One or more letters from the set "i", "L", "m", "s", "u", "x".) The group matches the empty string; the letters set the corresponding flags (re.I, re.L, re.M, re.S, re.U, re.X) for the entire regular expression. This is useful if you wish to include the flags as part of the regular expression, instead of passing a flag argument to the compile() function. Note that the (?x) flag changes how the expression is parsed. It should be used first in the expression string, or after one or more whitespace characters. If there are non-whitespace characters before the flag, the results are undefined.
(?=...)	Matches if ... matches next, but doesn't consume any of the string. This is called a lookahead assertion. For example, Isaac (?=Asimov) will match 'Isaac ' only if it's followed by 'Asimov'.
(?!...)	Matches if ... doesn't match next. This is a negative lookahead assertion. For example, Isaac (?!Asimov) will match 'Isaac ' only if it's not followed by 'Asimov'.

(?<=...)	Matches if the current position in the string is preceded by a match for ... that ends at the current position. This is called a positive lookbehind assertion. (?<=abc)def will find a match in "abcdef", since the lookbehind will back up 3 characters and check if the contained pattern matches. The contained pattern must only match strings of some fixed length, meaning that abc or a|b are allowed, but a* and a{3,4} are not. Note that patterns which start with positive lookbehind assertions will never match at the beginning of the string being searched; you will most likely want to use the search() function rather than the match() function:
	>>> import re
	>>> m = re.search('(?<=abc)def', 'abcdef')
	>>> m.group(0)
	'def'
	This example looks for a word following a hyphen:
	>>> m = re.search('(?<=-)\w+', 'spam-egg')
	>>> m.group(0)
	'egg'

(?<!...)	Matches if the current position in the string is not preceded by a match for .... This is called a negative lookbehind assertion. Similar to positive lookbehind assertions, the contained pattern must only match strings of some fixed length. Patterns which start with negative lookbehind assertions may match at the beginning of the string being searched. The special sequences consist of "\" and a character from the list below. If the ordinary character is not on the list, then the resulting RE will match the second character. For example, \$ matches the character "$".
\number	Matches the contents of the group of the same number. Groups are numbered starting from 1. For example, (.+) \1 matches 'the the' or '55 55', but not 'the end' (note the space after the group). This special sequence can only be used to match one of the first 99 groups. If the first digit of number is 0, or number is 3 octal digits long, it will not be interpreted as a group match, but as the character with octal value number. Inside the "[" and "]" of a character class, all numeric escapes are treated as characters.
\A	Matches only at the start of the string.



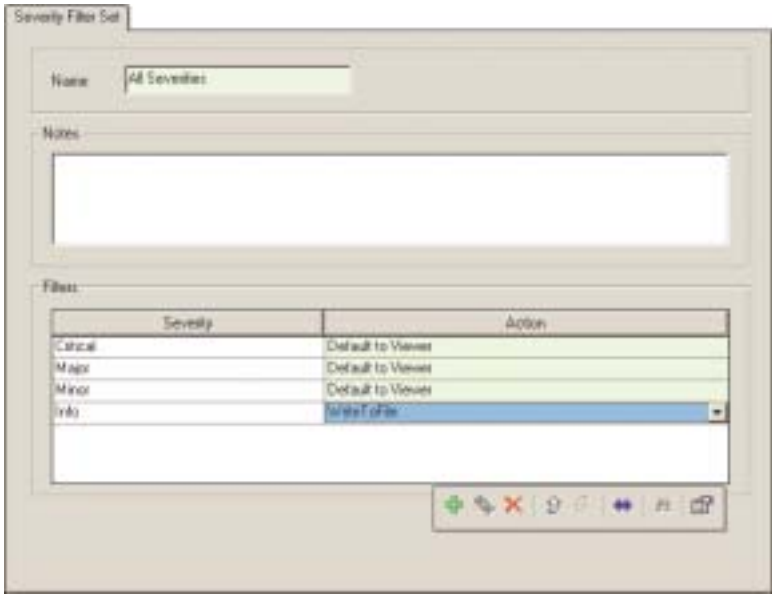
\d	Matches any decimal digit; this is equivalent to the set [0-9].
\D	Matches any non-digit character; this is equivalent to the set [^0-9].
\s	Matches any whitespace character; this is equivalent to the set [\t\n\r\f\v].
\S	Matches any non-whitespace character; this is equivalent to the class [^ \t\n\r\f\v].
\w	Matches any alphanumeric character; this is equivalent to the class [a-zA-Z0-9_].
\W	Matches any non-alphanumeric character; this is equivalent to the class [^a-zA-Z0-9_].

Severity Filter Sets

Use severity filter sets to filter alarms and to apply user-defined actions to the alarms based on severity.

To add a severity filter set record

1 Right-click the Severity Filter Sets folder; then, select Add Filter Set. The system opens the Severity Filter Set tab.



2 Type the name of the severity filter set in the **Name** field.

3 Type any description or comments about the severity filter set in the **Notes** field.

4 Select the severity you want to apply to your filter from the **Severity** list. Select: Critical, Major, Minor, Info or Undefined.

5 Select the action IRISnGEN should take from the **Action** list.

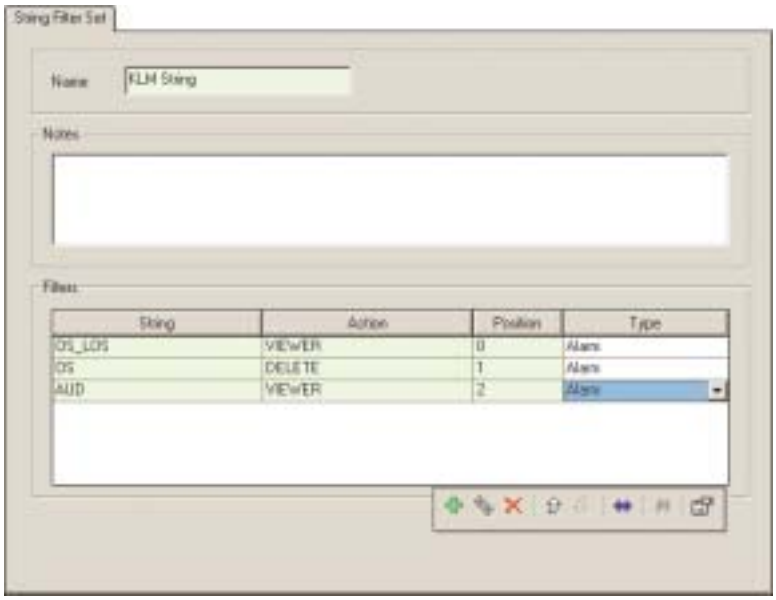
6 Save your Severity Filter Set record.

String Filter Sets

Use string filter sets to filter alarms and to apply user-defined actions to the alarms based on character strings.

To create a string filter set record

1 Right-click the **String Filter Sets** folder; then, select **Add Filter Set**. The system opens the String Filter Set tab.



2 Type a descriptive name in the **Name** field.
3 Type any description or comments about the string filter set in the **Notes** field.
4 Use the data table toolbar to add rows to the Filters data table.
5 Click inside the **String** field; then, enter the text string you want to filter.
6 Select a filter action from the **Action** list.
7 Type the position (0-32767) where the text string you are filtering for will appear.
8 Select a type from the **Type** list that determines if the filter string will be in the Alarm text, or in the Optional text of the alarm.



Note *When filtering for multiple strings, the order in which you list them in the filter set is important. The system begins at the top of the list and works down until it finds a match, and then it stops searching. For proper detection, you must list sub-strings first. List last any strings that contain wild card characters.*



Forwarding

You can forward alarms and other events to various destinations—such as, email addresses, fax machines, printers, and pagers—based on forward selectors and schedules. Use the IRISnGEN system's Forward feature to create the forwarding records used to handle alarms.

The forwarding folder contains files and sub-folders you can use to define the records that contain the forwarding parameters. It includes:

- **Active Forward Selectors** display active timed or scheduled selectors for customers, sites, and hosts, host types, or system.
- **Emails** lists the email addresses of users that can receive alarm information.
- **Faxes lists** the telephone number for faxes that can receive alarm information.
- **Forward Schedules** define when a forward selector is active, such as nights, weekends, and holidays.
- **Forward Selectors** identify which alarms to forward automatically.
- **Forward Sets** define one or more destinations for forwarding alarms or data.
- **Pagers/Pager Services** lists the pager types and access numbers used to receive forwarded alarm information.
- **Print** lists the printers used to receive alarm information.
- **Scheduled Forward Selectors** defines which selectors and schedules to activate.



Email

You can create records that identify the email address that received the event message.



Note *To forward alarms and reports via email, the IRISnGEN system must have access to an email server and have an active account on that server.*

To add an email record

1 Right-click the Email folder; then, select Add Email from the pop-up menu. The system opens the Email tab.



2 Type the name of the e-mail record in the **Name** field.

3 Type the e-mail address for each user you want to receive the event notice in the **To** field. Separate each e-mail address with a semi-colon.

4 Type the e-mail address for each user you want to receive a courtesy copy (CC) of the e-mail.

5 Select the **Disabled** checkbox to disable forwarding to e-mail addresses within this record. IRISnGEN tracks all disabled e-mail records by entering them in the *disable_alarm_forwarding* table.

6 Type any description or comments about the e-mail group in the **Notes** field.

7 Save your Email record.

Faxes

You can create records that identify the telephone number for the fax machines that receive event messages.

To fax events and reports, do the following:

- Ensure your IRISnGEN system has access to a Microsoft Exchange server and the Exchanger server be configured with GFI Fax and Microsoft Word.
- Install Gold-Fax for NT on the IRISnGEN Server, or other server. To use GoldFax NT, set the following IRISnGEN system parameters:

Parameter name	Value
FAX_DESTINATION	GOLD_hp
FAX_TRANSPORT	GOLD_FAX_PRINTER

To add a fax record

1 Right-click the Fax folder; then, select Add Fax from the pop-up menu. The system opens the Fax tab.



2 Type the name of the fax report in the **Name** field—for example, *John Smith's fax* or *Service Department fax*.

3 Type the phone number for the fax machine in the **Fax Number** field. Be sure to include any access code needed to access an outside line. Do not enter dashes, parentheses, or other non-numeric characters.

4 Select the **Disabled** checkbox to disable forwarding to this fax. IRISnGEN generates a log record for all disabled fax records.

5 Type any description or comments about the fax record in the **Notes** field.

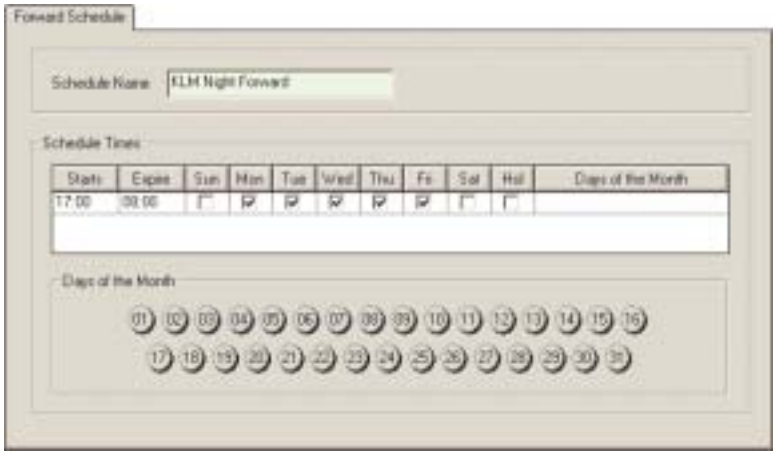
6 Save your fax record.

Forward Schedules

Create forward schedules that define when a forward selector is active, such as nights, weekends, and holidays or any time you want to change the time when IRISnGEN handles alarm processing. If you modify a forward selector while that schedule is active, IRISnGEN will not implement the modification until the next scheduled start time. Use the Delete option on the Active Forward Selectors tab to stop forwarding before the scheduled end time.

To add a forward schedule record

1. Right-click the Forward Schedule folder; then, select Add Forward Schedule from the pop-up menu. The system opens the Forward Schedule tab.



2. Type the name of your forward schedule in the **Schedule Name** field.
3. Type the time that the schedule should start in the **Starts** field. The field format is *hh:mm* (hours:minutes). You must enter all four digits. For example, type 16:00 to start at four o'clock in the afternoon.



Note *Use the right and left arrow keys to move between the time digits or to move between columns. Use the up and down arrow keys to move between rows. Press the space bar to add or remove the checkmark in a checkbox.*

4. Type the time the schedule should stop in the **Expire** field.
5. Select a **Day** checkbox for each day you want this schedule to be active. Select the **Holiday** checkbox if you want it active on holidays.
6. Using the thirty-one **Days of the Month** buttons, select the day(s) that you want your schedule to run.
7. Save your forward schedule record.

Forward Selectors

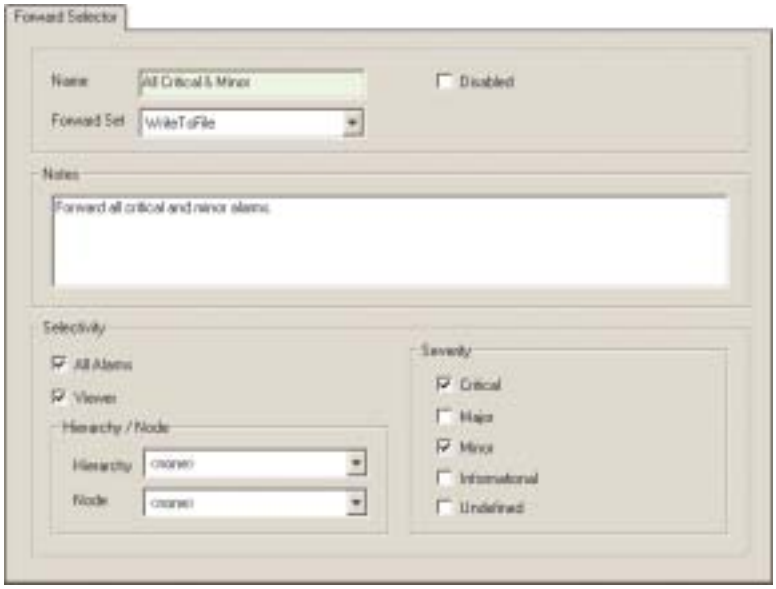
Use forward selectors to define which alarms you want automatically forwarded. Forward selectors can be used stand-alone or with a schedule. You can assign forward selectors to a customer, site, host, host type, or globally. Forward selectors assigned directly to a customer, site, host, or host type are ignored when a scheduled or timed forward selector is assigned at that same level.



Note *You must pre-define your forward sets BEFORE you create the forward selector. You cannot define them in the Forward Selectors dialog box.*

To add a forward selector record

1. Right-click the Forward Selectors folder; then, select Add Forward Selector from the pop-up menu. The system opens the Forward Selector tab.



2. Type the name of the forward selector in the **Name** field.
3. Select the **Disabled** checkbox to disable the selector. IRISnGEN generates SQL entries for all disabled forward selectors.
4. Select a pre-defined forward sets from the **Forward Set** list, or select **<none>**. When you select <none>, IRISnGEN uses the forward set defined for customer, host, host type, or site.
5. Type any description or comments about the forward selector in the **Notes** field.
6. Choose the selectivity parameters for the events you want to forward.

For	Do the following
All Alarms	Select the checkbox to forward all events.
Viewer	Select the checkbox to forward only Viewer events.
Hierarchy	Select a hierarchy name from the list.
Hierarchy node	Select the extended hierarchy node from the list.

7. Select the **Severity** checkbox for each severity you want to forward.
8. Save your forward selector record.

Forward Sets

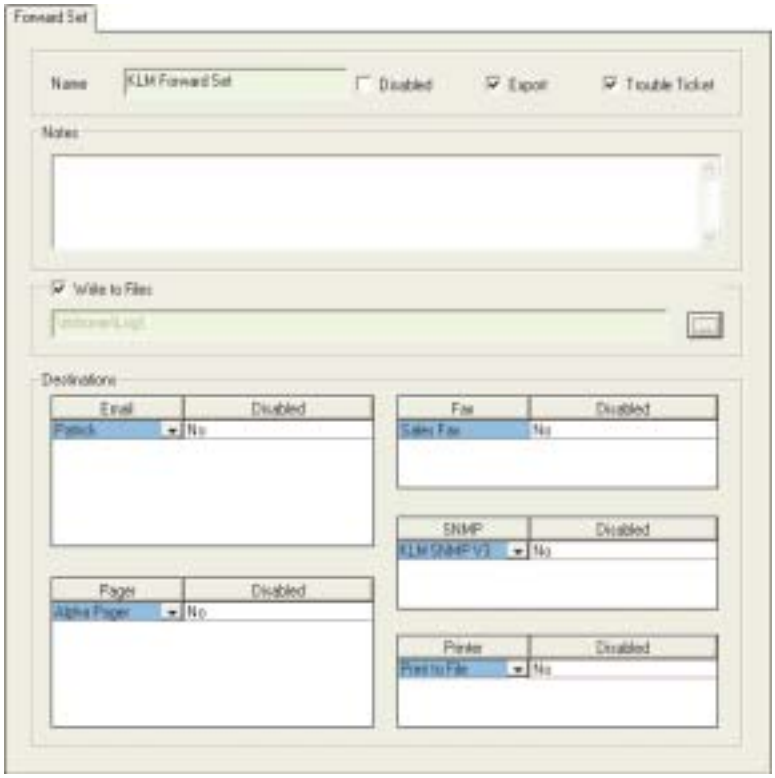
You can define how you wish an alarm forwarded—that is, if you want copies of the alarm sent to certain people, tables, or devices. You can forward alarms to one or more printers, email addresses, fax machines, and/or pagers.



Note *You must pre-define in your database the email addresses, fax machines, printers, and pagers that you wish to name in your forward sets BEFORE you create the forward set. You cannot define them in the Forward Sets dialog box.*

To add a forward sets record

1 Right-click the Forward Sets folder; then, select Add Forward Set from the pop-up menu. The system opens the Forward Set tab.



2 Type the name of the forward set record in the **Name** field.

3 Select the checkboxes you want to handle forwarding.

Select	To
Disabled	Disable forwarding to all destinations. IRISnGEN generates SQL entries for all disabled forward sets.
Export	Send events to the Export table (ALARM_EXPORT-QUEUE). **Caution:** Records in the export table are not aged out; they remain in the table until an application specifically removes them.
Trouble Ticket	Send events to the Trouble Ticket table (ALARM_TROUBLE_TICKET_QUEUE). ***Caution:*** *Records in the trouble ticket table are not aged out; they remain in the table until an application specifically removes them.*

4 Enter any description or comments about the forward set in the **Notes** field.

5 Select the **Write to Files** checkbox to enable writing alarms to the appropriate text file(s). When selected, IRISnGEN creates a file in the defined file path (directory). Use the … button to browse for the file. The destination directory must reside on the IRISnGEN server.

6 Use the Destinations data tables to display where e-mail, printer, fax, or pager data is forwarded.

7 Save your forward set record.

To add to or edit destinations for email, pager, fax, SNMP, or pager

1 Use the toolbar Insert Row button ( ) to insert a row in a selected destinations table.

2 Select a predefined object name from the list in Email, Printer, Fax, SNMP, or Pager column.

3 Repeat steps 1 and 2 as necessary to continue selecting destinations for this forward set.

To delete a forwarding destination

1 Highlight the item(s) you wish to delete.

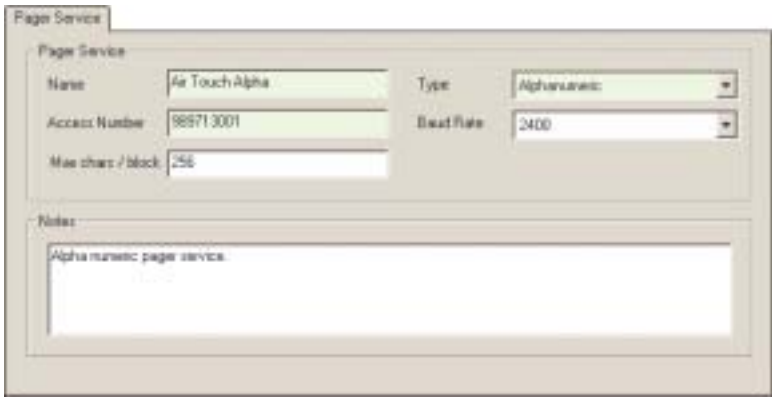
2 Click the ***Delete*** button ( ) on the mini toolbar.

Pagers/Pager Services

You can define the pager service used by a paging group. Pager records reference this information.

To add a pager service record

1 Right-click the Pagers/Pager Services folder; then, select Add Pager Service from the pop-up menu. The system opens the Pager Service tab.



2 Type the name of your pager service record in the **Name** field.

3 Select a pager service type from the **Type** list. Select: numeric, alphanumeric or email.

4 Type the access number for your pager in the **Access Number** field.

For alphanumeric pagers, enter the number used to access the pager service. Modern modems can handle dashes or parentheses, but some older modems might not handle these, so to be safe, do not use these characters. And be sure to select Alphanumeric from the Type list.

For paging services via email, type the domain name of the pager company preceded by the @ symbol, Example: @airtouchpaging.com. You must set up a pager to receive messages via e-mail.

For numeric pagers, enter digits of your choice to designate a priority or other code meaningful to your operation. These digits appear at the beginning of the numeric message sent to the pager, followed by the alarm ID. To place a dash between the access number and the alarm ID, enter an asterisk after the access number. For example, if the access number is 411* and the alarm ID forwarded is 1000, the numeric pager will show 411-1000. Be sure to select Numeric Pagers from the list. (You enter the phone number to reach the pager in the Pagers screen.)

5 Select a baud rate from the **Baud Rate** list. Available baud rates range from 300 to 115200.

6 Type the maximum number of characters that the paging company allows per block in the **Max Characters per Block** field. Check with the company or your pager reference documents to determine this value. 256 characters is normal.

7 To customize the message sent to pagers, enter any text and/or tags in the Custom Output field for the customized message. The system will replace the tags with its value, as defined throughout the IRISnGEN database.

Example

Port: %HOST_PORT, Alarm: %ALARM_ID, Occurred: %TIME_OCCURRED, Received: %TIME_RECEIVED

8 Type any description or comments in the **Notes** field.

9 Save your pager record.

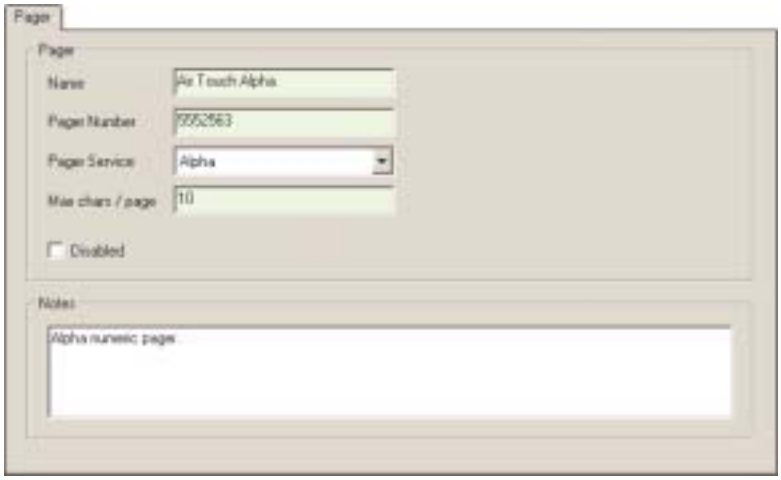


Creating and Editing Pager Records

Use the Pager tab to define the pagers that receive alarms. You must create your Pager Service records before creating your Pager records..

To add a pager record

1 Right-click the Pager folder; then, select Add Pager. The system opens the Pager tab.



2 Type the name of your pager in the **Name** field. You can use a descriptive name to identify the device, person or the position that uses this pager, such as *Air Touch Alpha*, *John Smith* or *Customer Service Night Shift*.

3 Type the number to dial to contact the pager in the **Pager Number** field. Enter only digits (no dashes or parentheses). Modern modems can handle dashes or parentheses, but some older modems might not, so do not use these characters. If you must dial an access code for an outside line, type that number as well. For example: 99417535000. You can use a "**w**" (wait character) to instruct the modem to wait for dial tone or a "**,**" (comma), which tells the modem to pause for a pre-set time.

4 Select a pager service from the **Pager Service** list. You must have already defined the services used. See "Pagers/Pager Services', page 5-26.

5 Type the maximum number of characters that the pager will allow in the **Max chars/page** field. Check with the paging company or your pager reference documents to determine this value.

6 Select the **Disabled** checkbox to disable forwarding to this pager. IRISnGEN generates SQL entries for all disabled pager records.

7 To customize the message sent to pagers, enter any text and/or tags in the **Custom Output** field for the customized message. The system will replace the tags with its value, as defined throughout the IRISnGEN database.

Example

Port: %HOST_PORT, Alarm: %ALARM_ID, Occurred: %TIME_OCCURRED, Received: %TIME_RECEIVED

will appear on the pager as:

Port: 1, Alarm: 3775, Occurred: 13:23:02, Received: 13:25:14

8 Type any description or comments about the pager in the **Notes** field.

9 Save your pager record.

Print

Printer records are part of the IRISnGEN system database. IRISnGEN uses them in forward sets when determining which printers should receive alarm messages. You can define one printer per record. If you have connected and installed printers on your Windows NT, or Windows 2000 server, you may use them in your printer records.

To add a print record

1 Right-click the **Print** folder; then, select **Add Printer** from the pop-up menu. The system opens the Print tab.



2 Type a name to identify the printer in the **Name** field. For example, *Printer in Jane's Office* or *HP Color LaserJet*.

3 Select a print format from the **Print Destination** list. Select one of the following:

- ASCII (.txt)
- Crystal Report (.rpt)
- Printer
- Rich Text Format (rtf)
- Word Document (.doc)

4 Type the name and file path for the printer in the **Print Path** field, or click ... and browse to the file. You must enter the printer name exactly as it appears in your server's printer list. When you select one of the Print to File options, this field must contain the path name of the directory where the system prints the file. If you specify a file name in the print path, that file name is used. If you do not, IRISnGEN uses the default naming convention for Print to File names, which is the name of the report followed by a unique identifier— for example: traf402-12356789.rtf. If a file name already exists in a directory, the system overwrites the previous file.



Note *The path name must end in a backslash for the system to interpret it as a directory name instead of a file name.*

5 Select the **Disabled** checkbox to disable forwarding to this printer. IRISnGEN generates SQL entries for all disabled printer records.

6 Type any description or comments about the printer record in the **Notes** field.

7 Save your printer record.



To create a printer

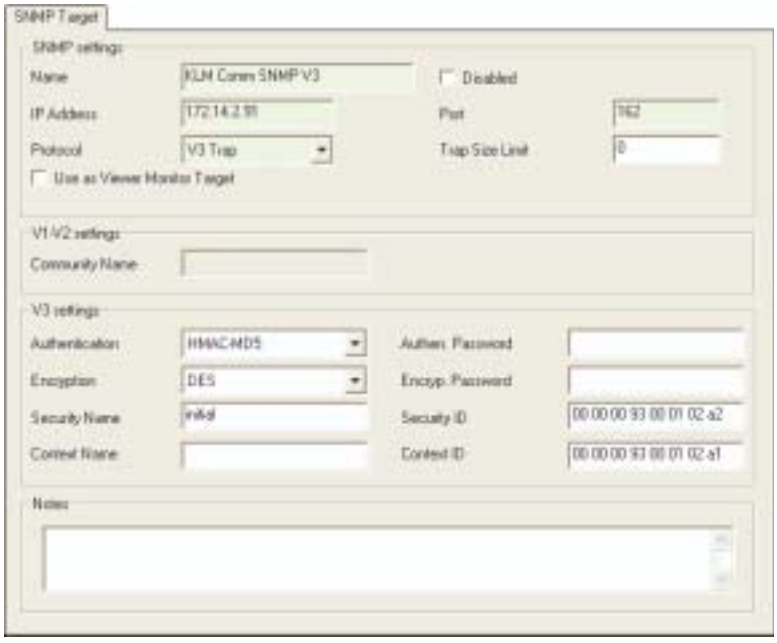
1. Log into the server as the account that starts the IRISnGEN System service.
2. Install the desired printer in the server's operating system.
3. Log into the IRISnGEN interface as a user who has permissions to create printers.
4. Right-click the **Printers** folder; then, select **Add Printer** from the pop-up menu.
5. Select the desired output format from the **Print Destination** list.
6. Type the name of the printer exactly as it appears in the operating system of the server.
7. Save the printer record.

SNMP Targets

SNMP Managers are remote systems that can receive SNMP traps from IRISnGEN. You must define an SNMP Manager for each traget destination and trap type. Include the IP address, protocol, and nay necessary security information for sending a trap to a particular destination. Use the SNMP Targets folder to define the SNMP Managers you will use.

To add an SNMP target record

1. Right-click the **SNMP Target** folder; then select **Add SNMP Target** from the pop-up menu. The system opens the SNMP Target tab.



2. Type a name to identify the SNMP target in the **Name** field.
3. Type the IP address of the target in the **IP Address** field.
4. Select a trap protocol from the **Protocol** drop-down menu. Select on of the following:
   - V1 Trap
   - V2 Trap
   - V3 Trap

   Selecting a trap from the drop-down menu enables the corresponding fields for that trap, described below.

5 Select the **Use as Viewer Monitor Target** checkbox to identify which SNMP objects you wish to associate with IRISnGEN's Viewer function. It instructs the Viewer Manager to use this SNMP definition when sending traps. A warning message appears informing you of the possible consequences of your actions.

See "SNMP Viewer Monitoring', page 5-31 for more information about the SNMP Viewer Monitor.

6 Select the **Disabled** checkbox to disable the generation of all SNMP traps to this target. Clear the checkbox to allow trap generation.

7 Type the number of the TCP/IP port used to receive SNMP traps from the host in the **Port** field. The range is 1 - 65535. The default port is 162.

8 Enter the maximum amount of packet data to include in the trap in the **Trap Size Limit** field. This allows you to adjust the tap for network conditions that may set a size limitation on the transmission reliability of packets. The range is 0 and 200 - 65535. Enter **0** to indicate no limit to the packet size.

9 Configure a trap setting:

To configure a V1 or V2 trap

1 Select **V1 Trap** or **V2 Trap** from the **Protocol** drop-down menu, described above.

2 Type a name in the **Community Name** field. A commonly used name is "public," although another name can be used.

To configure a V3 trap

1 Select **V3 Trap** from the **Protocol** drop-down menu, described above.

2 Select a protocol from the Authentication drop-down menu. Choose one of the following:
- HMAC-MD5
- HMAC-SHA
- none

3 Type a password in the **Authentication Password** field. Type something that is easy to remember. This password automatically converts to an authentication key.

4 Select an encryption protocol from the **Encryption** drop-down menu. Choose one of the following:
- AES-128
- AES-192
- AES-256
- DES
- Triple-DES
- none

5 Type a password in the **Encryption Password** field.

6 Type a name to secure the setting in the **Security Name** field.

7 Type the ID of the SNMP engine in the **Security ID** field.

8 Type the context name for the V3 security setting in the **Context Name** field. This field is most often used with proxies and is usually blank when using normal agents.

9 Type the context ID in the **Context ID** field. It is usually the same as the Security ID.

10 Save your record.



SNMP Viewer Monitoring

Using the SNMP Viewer Monitoring module, you can monitor your IRISnGEN system without the Alarm Viewer. The module uses SNMP traps to send the information to any number of remote systems. The module can send V1, V2, and V3 traps. You must use your own remote viewer software to view the data in the trap.

The module duplicates the information displayed in the Alarm Viewer, then breaks the display into two components, the initial alarm and alarm updates. The initial alarm trap contains all the textual information necessary to display the event in the viewer. Alarm updates trap contains only the alarm identifier, the field that changed, and its new value. This reduces additional bandwidth by eliminating redundant information.

To forward the traps to a remote system, be sure to select the **Use as Viewer Monitor Target** check box on the SNMP Target tab. It instructs the server to use that SNMP manager as a destination for SNMP Viewer Monitor traps. When you select this checkbox, the system will notify you that the target may receive large volumes of SNMP traps from IRISnGEN.

Alarm Trap

IRISnGEN sends this trap when a new event enters the viewer. The following shows the Alarm Trap definition.

Object ID	Name	Type
1.3.6.1.4.1.3600.2.2.2.1	SystemName	String
1.3.6.1.4.1.3600.2.2.2.3	Customer	String
1.3.6.1.4.1.3600.2.2.2.5	Site	String
1.3.6.1.4.1.3600.2.2.2.14	Host	String
1.3.6.1.4.1.3600.2.2.2.16	HostType	String
1.3.6.1.4.1.3600.2.2.2.23	AlarmID	Integer
1.3.6.1.4.1.3600.2.2.2.24	Status	Integer
1.3.6.1.4.1.3600.2.2.2.25	Severity	Integer
1.3.6.1.4.1.3600.2.2.2.26	AlarmType	Integer
1.3.6.1.4.1.3600.2.2.2.27	Keyword	String
1.3.6.1.4.1.3600.2.2.2.28	Description	String
1.3.6.1.4.1.3600.2.2.2.33	TimeOccurred	String
1.3.6.1.4.1.3600.2.2.2.34	TimeReceived	String
1.3.6.1.4.1.3600.2.2.2.29	ClassCode	String
1.3.6.1.4.1.3600.2.2.2.30	AlarmText	String
1.3.6.1.4.1.3600.2.2.2.32	OptionalText	String
1.3.6.1.4.1.3600.2.2.2.35	EquipmentIndex	Integer
1.3.6.1.4.1.3600.2.2.2.36	EquipmentName	String
1.3.6.1.4.1.3600.2.2.2.37	ControlElement	String
1.3.6.1.4.1.3600.2.2.2.38	EscalationLevel	Integer

You can find more information about the alarm trap and its contents in the Teltronics MIB.

Alarm Update Trap

IRISnGEN sends the alarm update trap in response to a change in an event located in the Viewer. The change can be one of the following:

- status
- escalation
- removal from the Viewer

The folowing show the Alarm Update Trap definition.

Object ID	Name	Type
1.3.6.1.4.1.3600.2.2.2.1	SystemName	String
1.3.6.1.4.1.3600.2.2.2.23	AlarmID	Integer
1.3.6.1.4.1.3600.2.2.2.39	UpdateType	Integer
1.3.6.1.4.1.3600.2.2.2.40	UpdateValue	String

You can find more information about the alarm update trap and its contents in the Teltronics MIB.

Sending a test trap

To help you troubleshoot your network, IRISnGEN includes the **Send Test Trap** feature that tests the SNMP communication from IRISnGEN. Use this feature to send a trap based on the definition of the selected target. IRISnGEN then places an entry in the communications queue. You can view the queue to check the status of the test.

To send a test trap

1. Right-click the SNMP Target file that you wish to test and select **Send Test Trap** from the pop-up menu. IRISnGEN displays the SNMP Test Trap dialog.



2. Type the number of tries in the **Count** field. The default is “1”.
3. Enter the trap packet size in the **Data Size** field. The default is “500”.
4. Use the Communications Queue to check the status of your test and to determine if IRISnGEN sent the trap. (See “Communication Queue” on page 22.)
5. Use a network protocol analyzer, such as Ethereal (included on your Installation CD) to determine if the trap reached the target device.



Messages

You can detect and isolate specific alarms for processing by identifying specific keywords in the incoming alarm message string. Once detected, you can assign plain-English text messages that explain the alarm, and then classify it by its severity. You can also define any special procedures necessary to handle the alarm. Use the Messages folder to create the record used to handle alarm messaging.

The Messages folder contains three sub-folders:

- **Keyword Templates** define the expected format for keywords and variables within an alarm string.
- **Message Libraries** translate machine text into plain-English text and classifies alarm severity.
- **Special Procedures** provides plain text (or hypertext messages) that explain what actions a technician should take when an alarm is received, or any other special operation you wish to define.

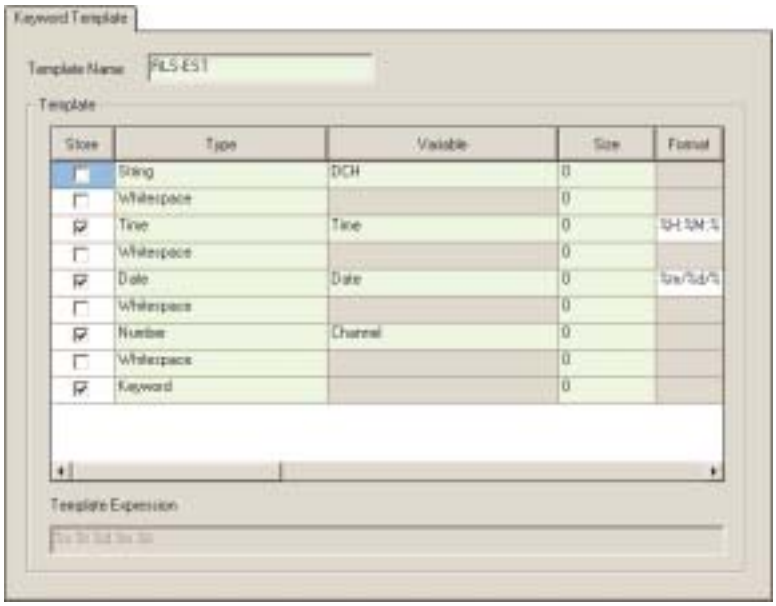


Keyword Templates

From the Keyword Template tab, you can create and edit templates for keyword variables. Each template has distinct units called tokens and each token has properties (Name, Type, Length, Format).

To add a keyword template

1 Right-click the Keyword Template folder; then, select Add Keyword Template from the pop-up menu. The system opens the Keyword Template tab.



2 Type the name of the template in the **Template Name** field.

3 Select the **Store** checkbox to store the template data associated with an alarm. The data associated with the variables are stored in a database table associated with the alarm.

4 Select a token type from the **Type** list.

Type	Description
Date	A string variable representing a date.
Keyword	The position of the keyword variable within the template. Use only one keyword per template.
Number	A numeric variable that contains any whole number up to nine digits.
Static Text	A string variable containing any alphanumeric sequence of characters expected in the alarm text.
String	A string variable containing any type of data.
Time	A string variable with text representing a time.
White Space	A portion of the alarm text that does not contain any characters (spaces between words or variables.

5 Type the token format for the Date, Time, and Static Text data types in the **Format** field. For date and time data types, this field contains tokens to describe the format of the field. Token format strings are as follows:

Type	Description
%a	Abbreviated weekday name
%b	Abbreviated month name
%d	Day of month as decimal number (01 – 31)
%H	Hour in 24-hour format (00 – 23)
%m	Month as decimal number (01 – 12)
%M	Minute as decimal number (00 – 59)
%S	Second as decimal number (00 – 59)
%y	Year without century, as decimal number (00 – 99)
%Y	Year with century, as decimal number
%%	Percent sign

For example, to represent *04/28/2000 07:28*, the token format string is *%m/%d/%Y%/H%M*. The format field for a static text string contains the text expected in the alarm, associated with a specific keyword in a specific position.

6 Use the **Template Expression** field displays a representation of your choices in the Template data table.



Message Libraries

Message libraries translate machine text to plain-English, identify alarms received from a host, and classify alarm severity. The message library contains a list of keywords or remote agent class codes that may appear in alarm text. You can create different message libraries for each host type.

Using the message library, you can find all keywords in an alarm. The IRISnGEN system generates a new alarm for each new keyword it finds. This lets you support hosts that send multiple alarms embedded within a single record, each with a different severity.

Once the system finds a keyword or class code in the text, the system can:

- Attach a description field for the keyword to the alarm. Use this to translate alarm text into plain English messages.
- Assign a severity code.
- Attach a procedure note. This note can provide instructions about fixing the problem or more details about the host.

You can set the message library to auto-learn new messages. To auto-learn, the system automatically adds to a message library any alarms that do not match existing keywords or class codes. The system captures the keyword starting at the default column position. The system then marks the alarm severity as undefined. The alarm description contains part of the alarm text.

The IRISnGEN system has a special library named User. Here you can define alarm messages and translations that are not restricted to a specific host or host type system. You can use these library entries to generate your own internal alarms. For example, you can instruct the IRISnGEN system to intercept a power failure alarm and hold it for five minutes. If the system receives a power restoration message within five minutes, the IRISnGEN system creates a message that states a short power failure occurred.

You may want to combine several minor alarms to generate one new alarm message that has a higher severity. The User library controls this message and the severity of the generated alarm.

To add a message library

1 Right-click the Message Library folder; then, select **Add Message Library** from the pop-up menu. The system opens the Message Library tab.



2 Type the name for the message library in the **Library Name** field.

3 Select the **Class Code Library** checkbox to match an SEB class code rather than alarm text.

4 In the **Column Offset** field, type the column position at which the keyword appears, or type **0** (zero) to search the entire string for the keyword. You can enter an offset position from 0 to 999.



Note *The column designator applies to the entire library. You can set keyword-specific column identifiers in the Message Library Alarm records.*

5 Select the **Auto-learn** checkbox to add undefined alarms to the database during alarms processing. For undefined alarms, the first twenty characters of the alarm become a new keyword.

6 Type any description or comments in the **Notes** field.

7 Save your Message Library record.

Creating and Editing Message Library Alarm Entries

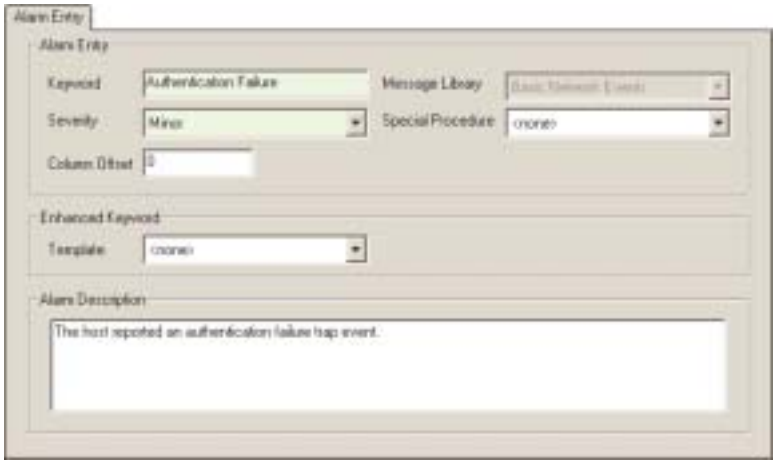
Library Alarm Entries define keywords to be matched in incoming alarm text. The library name is matched from the Host Information screen. Using this tab, you create, edit, and view message library alarm entries.



Note *Create your message libraries and procedures before defining your message library alarms.*

To add an alarm entry record

1 Right-click a message library record; then, select Add Alarm Entry from the pop-up menu. The system opens the Alarm Entry tab.



2 Type the keyword in the **Keyword** field. When entering a keyword, use a string of characters that are contained within the alarm text. Keywords can be single words, groups of words, or any combination of alpha and numeric characters. When the system finds a keyword match, other processes take place depending on filter, escalation, and threshold actions. Never use a wild card as part of a programmed keyword.



Note *Incoming data processed by the Alarm Manager is case-sensitive. Be sure you enter your keyword exactly as it is defined in the host device; otherwise, it will not match.*

3 Use the **Message Library** field to display the library name containing the keywords that you are editing. You cannot modify this field.

4 Select the keyword severity from the Severity list. When assigning a severity to a keyword, you must know what the keyword means within the context of an alarm. IRISnGEN uses the assigned severity to color-code the alarms.

5 Select a predefined, special procedure from the **Special Procedure** list.
6 Type the column position at which the keyword appears in the **Column Offset** field. This entry overrides the column number in the Message Library screen. The value is applicable to the current keyword only.
7 Select a predefined keyword from the **Enhanced Keyword Template** list.
8 Type a description about an alarm containing the programmed keyword in the **Alarm Description** field. The text you enter will be included with the alarm. This extra information can be very helpful to those personnel monitoring alarms. The description you enter here will appear in the Notes field on the Alarm Detail screen.
9 Save your Alarm Entry record.

Special

Special Procedure records define the text that is attached to certain alarms. You can use this text to explain what action a technician should take when this alarm is received and any other special protocols that you wish to define.

To define a special procedures record

1 Right-click the Special Procedures folder; then, select Add Special Procedure from the pop-up menu. The system opens the Special Procedure tab.



2 Type the name of the procedure in the **Procedure Name** field.
3 Type any description or comments in the **Notes** field.
4 Type the text of the special procedure exactly as you wish it to be viewed by technicians or other personnel who receive the alarm in the **Text** field.
5 Once you create a special procedure, you can assign it to an alarm keyword, customer, site, or host. The text should tell how and why you assigned the special procedure.
6 Save your special procedure record.

Superscripts

A Superscript is a program written in a script language, such as C++, and executed within your IRISnGEN system. Use Superscripts to automate daily tasks, perform predefined functions and communicate with remote agents and hosts.

A Superscript can be triggered:

- by an alarm sent by the remote agent
- by a scheduled event
- manually



To add a superscript

1. Right-click the Superscripts folder; then, select Add Superscript from the pop-up menu. The system opens the Superscript tab.



2. Type the name to identify this superscript in the **Name** field. This is not the name of the superscript file, but merely a label to help you remember its purpose.
3. Type the file name and path of the script in the **File Name** field, or click ... and navigate to the superscript file.
4. Type any additional information that will help you identify the name and purpose of the superscript in the **Notes** field.
5. Save your superscript record.

Thresholds

A well-designed alarms management system should filter minor alarms so that support personnel only take action when the volume of alarms exceeds defined levels. A powerful option included in the basic package is the Alarm Thresholds. You can define thresholds by picking an alarm keyword from the message library, defining a minimum count, and defining a maximum count. You can also define a time within which the maximum number of alarms with the designated keywords that the system must receive to activate stages of the threshold.

An alarm threshold has three stages:

- **Stage 1** – A specific alarm has not exceeded a defined minimum count.
- **Stage 2** – A specific alarm count has exceeded the minimum count, but has not **exceeded the maximum count.**
- **Stage 3** – A specific alarm count has exceeded the maximum count.

As an alarm condition progresses through these three stages, each stage may require unique handling.

Stage 1 (Before Minimum Reached)

In Stage 1, the alarm has not reached the minimum occurrence count. In this stage, the alarm is likely minor in nature. If the goal is to reduce minor alarm traffic in the Alarm Viewer, then stage one alarms can be stored directly to history or deleted.

The options available in stage one include:

- Send the alarm to the viewer.
- Send the alarm to history.
- Delete the alarm until the threshold minimum has been satisfied.

Stage 2 (Between Minimum and Maximum)

In Stage 2, the alarm has exceeded the minimum count, but has not exceeded the maximum count. Once the alarm exceeds a defined threshold, the alarm is most likely severe. The display options for this stage let IRISnGEN generate a new triggered alarm message that is sent to the Alarm Viewer in place of the original alarm if the Delete or Do not display in Viewer options were chosen; otherwise, both the original and triggered alarms go to the viewer. IRISnGEN can also execute a forward set, which notifies additional people of the alarm threshold activity.

- The options available in Stage 2 include:
- Send the original alarm to the viewer.
- Send the original alarm to history.
- Delete the alarm.

If the Stage 2 is generating a triggered alarm, the user may not want to keep the original alarm. Do the following:

- Generate a user-defined alarm message with a defined severity for each original alarm that occurs within the minimum and maximum values.
- Execute a forward set for each alarm that occurs within the minimum and maximum values.



Stage 3 (After Maximum Reached)

In Stage 3, the alarm has exceeded the maximum count. This stage could be used to filter excessive alarms for a given period, such as a runaway error condition.

The options available in Stage 3 include:

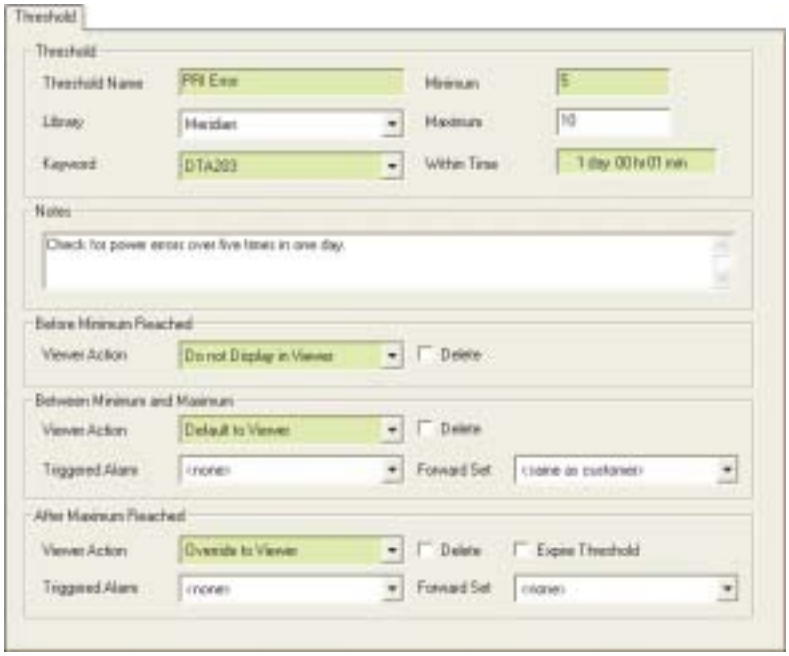
- Send the original alarm to the viewer.
- Send original alarm to history.
- Delete original alarms that exceed the maximum until the time period expires.
- Expire (reset) the threshold counters and timers with the first alarm that exceeds the maximum count.
- Generate a user-defined alarm message with a defined severity for each original alarm occurrence over the maximum value until the threshold expires.
- Execute a forward set for each alarm that exceeds the maximum values until the threshold expires.

Example

If the system activates hard contact #1 on the remote agent more than twenty-five times in two hours, you have a serious problem. Several hundred alarms will generate until you correct the problem. To suppress these alarms, automatically send them to history during stage one (minimum of twenty-five alarms), display two alarms during stage two (maximum of twenty-seven alarms), and delete all alarms during stage three (overall time of two hours).

To create a threshold record

1 Right-click the Threshold folder; then, select Add Threshold from the pop-up menu. The system opens the Threshold tab.



2 Type the name of the threshold in the **Threshold Name** field.

3 Select a message library from the **Library** list.

4 Select a keyword from the **Keyword** list.

5 Type the minimum number of alarms that must occur for this threshold to become active in the **Minimum** field. The minimum and maximum entries work in conjunction with the three different actions on the bottom of the tab.

6 Type the maximum number of alarms that must occur before this threshold reaches stage three in the **Maximum** field. The minimum and maximum entries work in conjunction with the three different actions on the bottom of the tab.

7 Type the time that these events must occur within for the threshold to take affect in the **Within Time** field. Format is *DDHHMM* (for days, hours, minutes). Colons are displayed on screen, but you do not need to enter the colons. All numbers should be entered in a two-digit format, for example, enter 05, not 5, for five days. You must enter a value of at least one minute.

8 Type any description or comments in the **Notes** field.

9 Select one of the following actions from the **Viewer Action** list:

- **Override to Viewer** displays selected alarm in the Viewer. This option overrides all other filters' viewer selections, except Delete.
- **Do Not Display in Viewer** prevents the selected alarm from displaying in the Viewer, but still stores the event in the database.
- **Default to Viewer** sends the selected alarm to the Viewer. You can override this option by deleting it or by selecting Do Not display in the Viewer window.

10 Select the **Delete** checkbox to delete alarms in the threshold stage. Once deleted, the alarms will not appear in the List Viewer or in the History file. Neither forward sets nor Superscripts will execute.

11 Select that alarm that occurs when the threshold is met from the **Triggered Alarm** list. The selection on the list are from the USER message library.

12 Save your Threshold record.

Contact

You can create records that identify the people you need to contact when an alarms occur; then, assign the records to customers, sites, and hosts. You can also group your contacts by their function within your organization, so that you can better manage your facilities. The IRISnGEN system includes a Contact function for defining the contact types and contacts. The Contacts folder includes two sub-folders:

- **Contact Types** grouping contacts by function
- **Contacts** list the personnel (and their contact information) who can assist in the response to events at the customer, site, or host location.

Contact Types

You can group contacts by contact type. This helps you organize your contacts by their function. For example, you can group all your technicians trained to service Vision PBXs under one group than those qualified to service Meridian PBXs under another group. Contact Type records are referenced by Contact records.



To create a contact types record

1 Right-click the **Contact Type** folder; then, select **Add Contact Type**. The system opens the Contact Type tab.



2 Type a name to describe the type of contact in the **Contact Type Name** field. For example, use a descriptive name, such as Vision service technicians or Product Managers. The maximum length is 40 characters.

3 Enter any description or comments in the **Contact Type Notes** field.

4 Save your contact type record.

Contacts

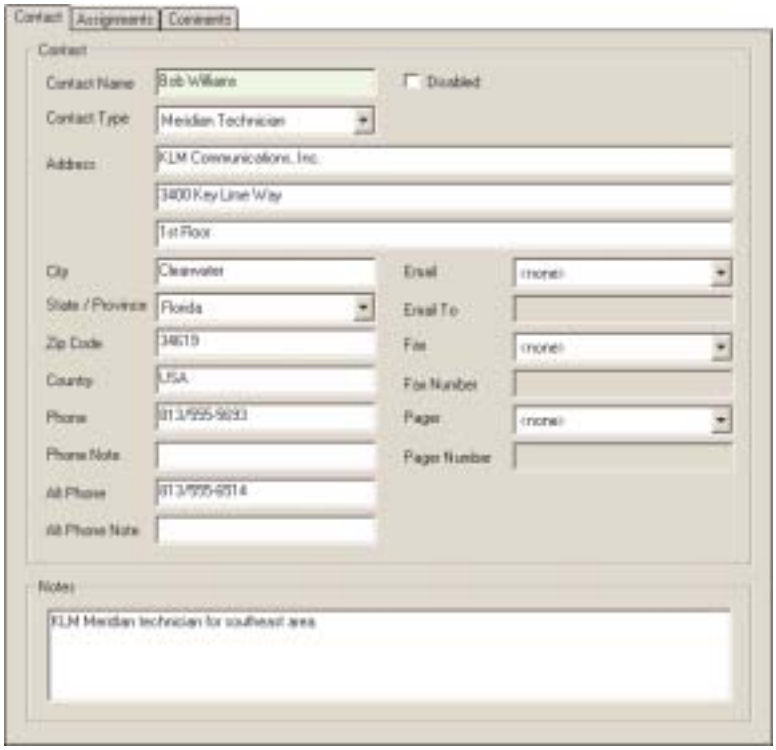
You can create contact records that identify the people who should be contacted when alarms occur. This can include technicians who can correct the alarms or on-site personnel who need to be kept informed about critical alarms. Contacts can be assigned to customer, site, and host records.



Note *Create your contact type, email group records, fax, and pager records in your database BEFORE you create your Contact records.*

To add a contact record

1 Right-click the **Contact** folder; then, select **Add Contac**t from the pop-up menu. The system opens the Contact tab.



2 Type the name of the contact in the **Contact Name** field.

3 Select the **Disabled** checkbox to disable all forwarding to the contact via email, fax, or pager. A disabled contact name does not appear in the Contact Name list in Customer, Site, or Host windows. The email, fax, and pager records are marked as enabled/disabled. The default of new entries is enabled.



Warning *When you disable a contact name, any fax in the record is also disabled. If this fax is shared by many people, you may need to create individual fax records for each person.*

4 Select a contact type from the **Contact Type** list. You can only select from pre-defined types. (See Creating Contact Types records)

5 Enter the contact's address and phone information in the next nine field. The IRISnGEN system allows up to 40 characters per address field.



Note *If you are entering a Canadian Postal Code, be sure to enter it in the following format: XXX XXX, where X represents any number or letter in the postal code. Be sure to include a space between the third and fourth characters.*

6 Select the contact's e-mail ID from the **Email** list. When you select an e-mail ID, IRISnGEN automatically fills in the **Email To** field.

7 Select the contact's fax ID from the **Fax** list. When you select a fax from the list, IRISnGEN automatically fills in the **Fax Number** field.



8 Select the contact's pager number from the **Pager** list. When you select pager from the list, IRISnGEN automatically fills in the **Pager Number** field.

9 Type any description or comments in the **Notes** field.

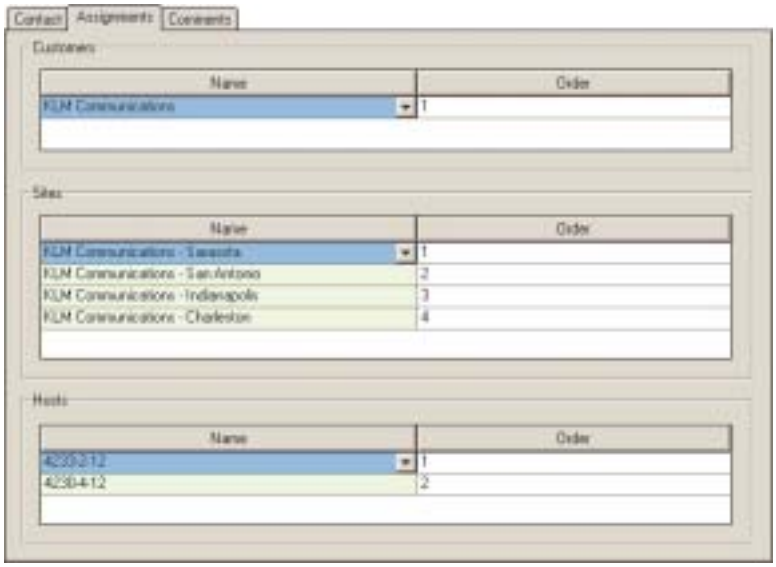
10 Save your Contact record.

Assigning Contacts

From the Assignments tab, you can assign a contact name to customers, sites, and hosts.

To assign a contact

1 Click the Assignments tab.



2 Use the data table toolbar button ( ) button to insert a blank row any of the three data tables.

3 Select a contact name from the **Name** list.



Note *A disabled contact name does not appear in the contact name list in customer, site, or host windows.*

4 Continue making selections as needed, repeating steps 2 and 3 for customers, sites, and hosts.

5 As you add each name, the number in the **Order** column defaults to 1. You can place the names in order of importance, by highlighting that row and typing another number, or by using the spin control to select a number.

To remove a contact assignment

1. In the Contacts area data table highlight the contact that you wish to delete.
2. Click on the mini toolbar. The Current area of the window updates.
3. Continue making selections as needed, repeating steps 1 and 2.
4. Before you select another object in the tree, save your changes to this table by pressing the Save button.

Adding Comments

You can add comments for each customer, site, or host. Select the Comments tab to enter any additional information.

Equipment Libraries

IRISnGEN defines equipment as devices attached to the SEBea remote agent. You can monitor each piece of equipment for events and take action when you receive an alarm.

The Equipment libraries are a collection of records that define the various equipment that you monitor and control. Use the Equipment Libraries to define each piece of equipment used in your IRISnGEN system.

The Equipment Libraries folder contains four sub-folders, each containing its own set of specialized library records. These sub-folders include:

- **Equipment** defines a device attached to the SEBea remote agent or to a host.
- **Equipment Actions** defines what action IRISnGEN can perform on each piece of equipment.
- **Equipment Icons** are the graphical representation of equipment that appears in the Map Viewer and Equipment Explorer.
- **Equipment Types** defines the operations assigned to Equipment Actions and the parameter strings for each operation.



Equipment

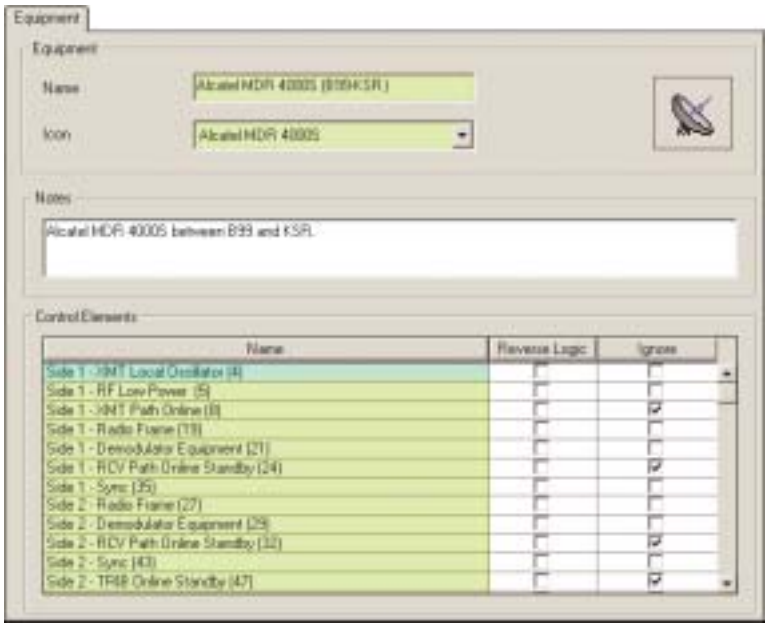
IRISnGEN defines equipment as devices attached to the SEBea remote agent. You can monitor each piece of equipment for alarms and take action when you receive an alarm.

You can create the Equipment library records that define each piece of equipment in your IRISnGEN system. Each library record contains the name of the equipment, an icon representation that will appear on the Map Viewer and throughout your IRISnGEN system, control elements on which you can take action, and any additional notes you wish to make about the equipment.

When defining your Equipment records, pay particular attention to the control elements you define for your equipment. A control element is the smallest, separate component of a piece of equipment that you can handle. For example, you may choose to define a radio device. That radio has two control elements: antenna and channel selector. You must enter the control elements in the equipment record. Later, using the Equipment Action tab, you will define the actions to take for each control element, such as lowering the antenna or changing channels.

To create an equipment record

1 Right-click the Equipment folder; then, select Add Equipment from the pop-up menu. The system opens the Equipment tab.



2 Type a name for your equipment in the **Name** field.

3 Select an icon from the **Icon** list. IRISnGEN uses this icon as a visual representation on the Map Viewer and in the Explorer for this equipment.



Note *If you have not yet defined your icons, do so now. You must define your icons before you can save your equipment record. For more information about defining icons, see* *"Equipment Icons', page 5-52.*

4 Type any description or comments in the **Notes** field.

5 Type the control element name for this piece of equipment in Control Element table's **Name** field. Control elements are the components on which you can take action.

6 Select the **Reverse Logic** checkbox to convert the active event or status received from this control element to an inactive event or status. Inactive events or status will convert to an active event or status. The IRISnGEN server reverses the logic when it receives the event or status from the remote agent. Reversing the logic is transparent to the user.



Note *The state of the equipment will not show in reverse logic until one of the following occurs:*

- *IRISnGEN processes a new event due to a change in the equipment state.*
- *A user performed a manual request from the Detail View window.*

7 Select the **Ignore** checkbox to indicate that events or status from this control element will not be ignored when the system status is determined. This is the case when the control element is a status or a control (output). If you check this box, the control element will NOT display in the System Status view of the Equipment Explorer. If you do not select this checkbox, the control element will display in the System Status view of the Equipment Explorer, provided its status is active.

8 Save your equipment record.

To add a control element

1 Click inside the Control Element field.

2 Use the Insert Row button ( ) to insert a blank row in the Items data table.

3 Enter a control element name—for example, Antenna.

4 Repeat steps 2 and 3 to add additional control elements for this equipment.

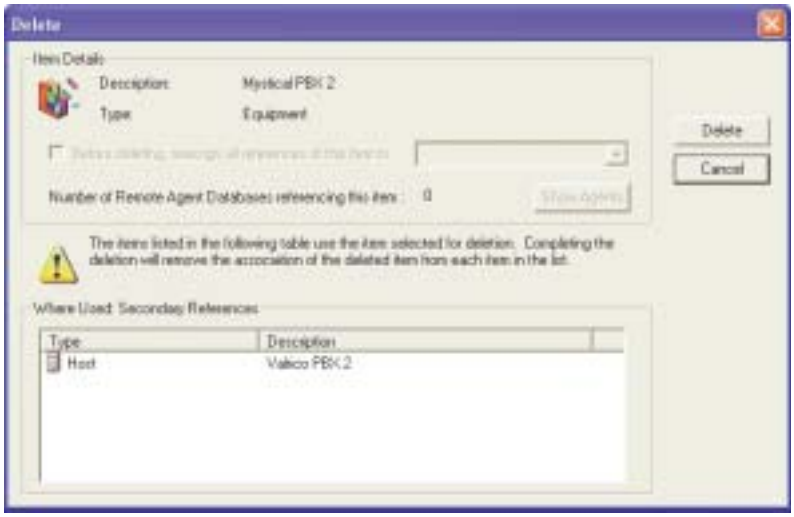
Deleting an Equipment Record

You can delete equipment records from your IRISnGEN system.

To delete an equipment record

1 Right-click the Equipment folder in the tree view, and then choose Delete. The system opens the Delete dialog box.





2 Click **Delete**.

Note *You cannot reassign references to the Equipment record before deleting that record. If the Mandatory References table appears on the dialog showing action references, you must first manually delete each action record BEFORE you can delete the Equipment record (see ”Equipment Actions’, page 5-50. Once you have removed all actions, the Mandatory References table disappears and you can then delete the record. You do not need to delete any secondary references before deleting the Equipment record.*

Duplicating an Equipment Record

You can duplicate an equipment record and modify it to create a new equipment record. When you do this, the entire contents of the old equipment record is copied into the new record.

To duplicate an equipment record

1 Right-click the Equipment folder in the tree view, and then choose Duplicate. IRISnGEN displays the duplicate record and shows “Copy of” in the Name field.

2 Change the name of the record and modify any fields you wish, such as adding or deleting control elements.

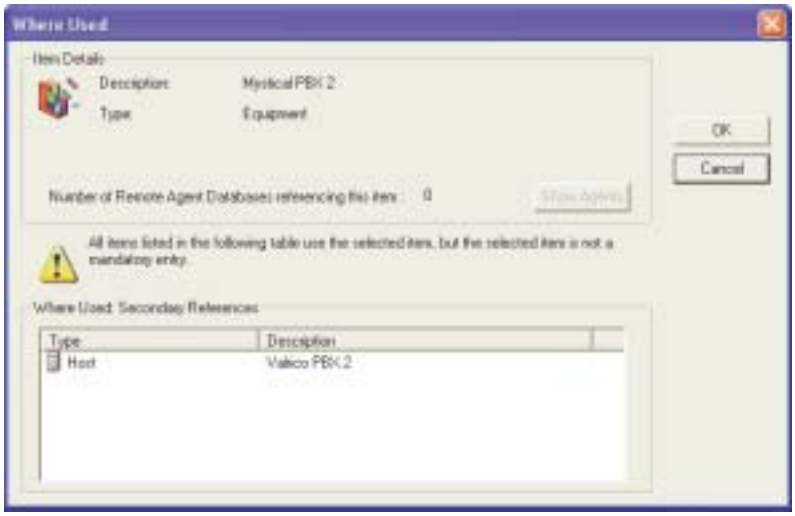
3 Save your changes.

Where Used

You can quickly identify all hosts or actions referencing your equipment record using the Where Used feature.

To display Where Used

1 Right-click an equipment name in the tree view and choose Where Used. The system opens the Where Used dialog box.



2 Double-click a host to display that host's record.

3 Edit the record as necessary.

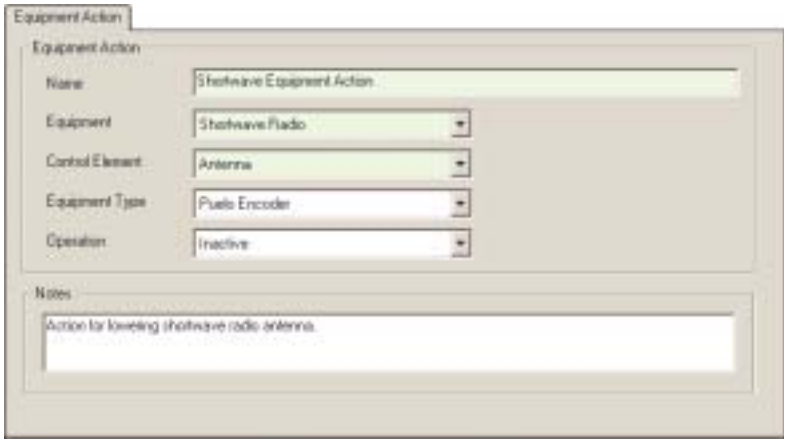
4 Save your changes.

Equipment Actions

You can define the actions the system will perform on each control element. Use the Equipment Action tab to create a library records that define your equipment actions.

To create an equipment action record

1 Right-click the Equipment Action folder; then, select Add Equipment Action from the pop-up menu. The system opens the Equipment Action tab.



2 Type a name for the equipment action in the **Name** field.

3 Select an equipment from the **Equipment** list.



Note *You must define your equipment before you can save your equipment action record.*

4 Select a control element from the **Control Element** list—for example, Antenna. You will take action on this control element. The list only displays those control elements configured for the equipment you chose in the previous field.

5 Select an equipment type from the **Equipment Type** list. Only those equipment types that are assigned to hosts and which the selected equipment/control element combinations are assigned will appear in the list. See ”Host-Equipment Tab’, page 2-17.

6 Select an operation from the **Operation** list. The operation is a parameter string that passes to a script running on the remote agent when you request to perform an action. The list only contains those operations defined for the equipment type you selected in the previous field. See ”Equipment Types’, page 5-54.

7 Type any description or comments in the **Notes** field.

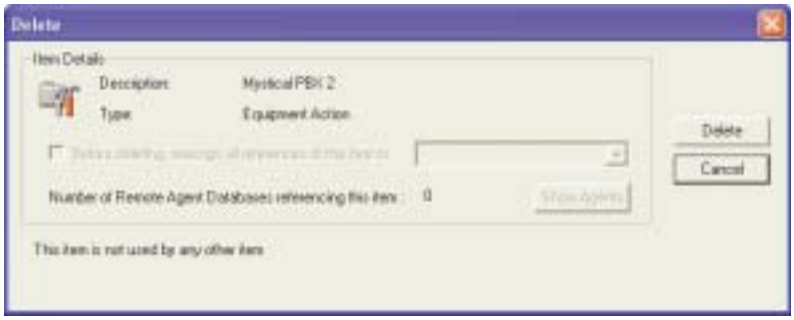
8 Save your equipment action record.

Deleting an Equipment Action Record

You can delete an equipment action from your IRISnGEN system.

To delete an equipment action

1 Right-click the Equipment Action folder in the tree view; then, select Delete. The system opens the Delete dialog box.



2 Click ***Delete***.

Duplicating an Equipment Action Record.

You can duplicate an equipment action record and modify it to create an equipment action record. When you do this, the system duplicates the entire contents of the record.

To duplicate an equipment action record

1. Right-click the Equipment Action folder in the tree view; then, select Duplicate. IRISnGEN displays the new equipment record and displays “Copy of” in the Name field.
2. Change the name of the record and modify any fields you wish, such as selecting new equipment.
3. Save your changes.

Equipment Icons

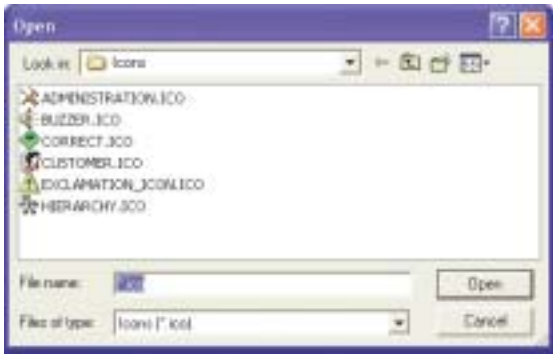
The Equipment Icons library contains a list of all icons used in the multi-drop system. Each icon represents a piece of equipment defined in IRISnGEN and appears throughout the system, such as in the Map Viewer and Explorer. Use the Equipment Icon tab to define the icons in your IRISnGEN system.

To create an equipment icon record

1. Right-click the Equipment Icons folder and choose Add Equipment Icon. The system opens the Equipment Icon tab.



2. Type the name for your icon in the **Name** field.
3. Do one of the following:
   - Type the file name and path of the icon file (.ico) in the **File Name** field
   - Click the Browse button (...) to open a standard Open dialog.



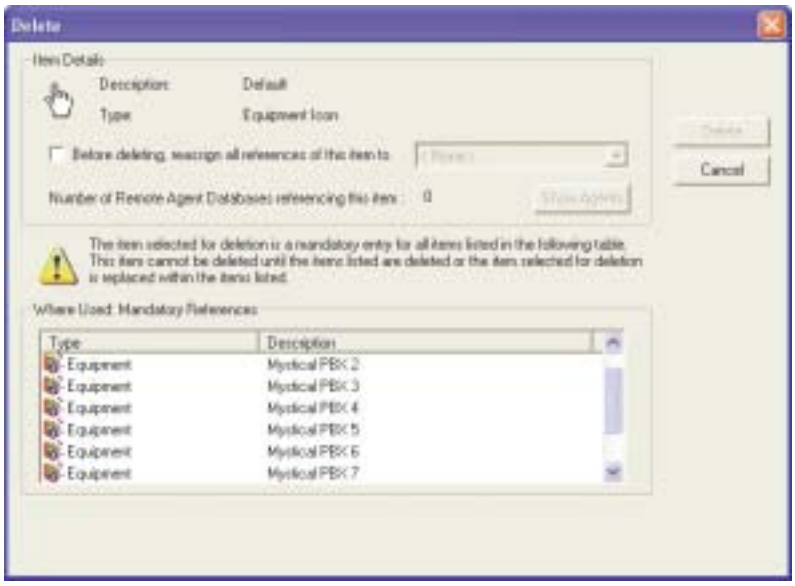
4. Navigate to the folder containing the icons and select the icon file.
5. You can only select icon file types with an .ico extension.
6. Click ***Open***. IRISnGEN copies the icon file to the \\IRISHOME\ICONS directory.
7. Save your equipment icon record.

Deleting an Icon Record

You can delete an icon record from your IRISnGEN system. When you delete an icon record, the system verifies no equipment is using this icon (see ”Equipment’, page 5-47. If you have equipment records that references this icon record, you must assign them a different icon before deleting this record.

To delete an icon record

1. Right-click the Icon folder in the tree view, and then choose Delete. The system opens the Delete dialog box identifying the icon and asks you to reassign any equipment using that icon with another icon.



2. Select the **Before deleting** checkbox; then, select a new icon from the list.
3. Click ***Delete***.
   IRISnGEN reassigns all the referenced equipment with the new icon you chose and deletes the old icon from your IRISnGEN database.



Note *If you do not wish to reassign all the equipment listed to the same icon, you must go to each Equipment record and choose a new icon.*

Duplicating an Icon Record

You can duplicate an icon record and modify it to quickly create a new icon record. When you do this, the entire contents of the icon record is duplicated.

To duplicate an icon record

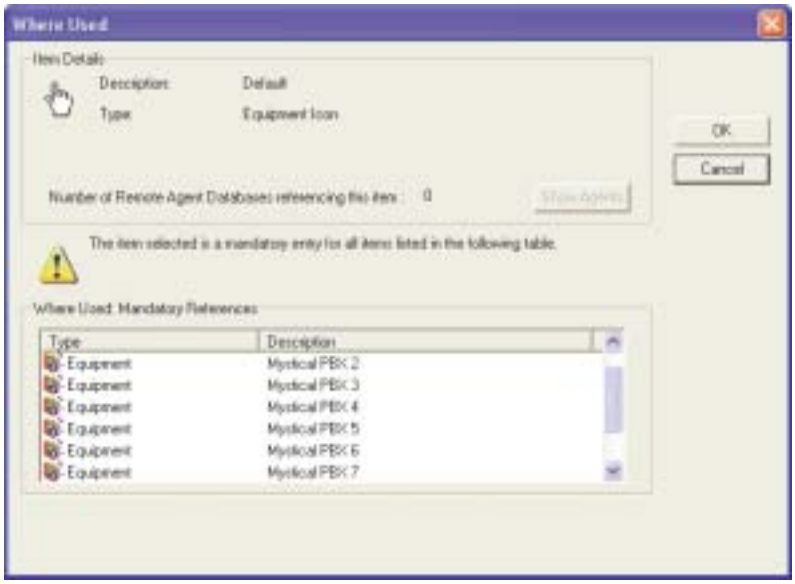
1. Right-click the Equipment Icon folder in the tree view, and then choose Duplicate. IRISnGEN displays the duplicate record and displays “Copy of” in the Name field.
2. Change the name of the icon record.
3. Save your changes.

Where Used

You can quickly identify which equipment references an icon using the Where Used feature. This can speed your operation, especially when you need to reassign equipment with a new icon.

To display Where Used

1 Right-click an icon name in the tree view and choose Where Used. The system opens the Where Used dialog box.



2 Double-click a site to display the icon record, if necessary.

3 Edit the record as necessary.

4 Save your changes.

Equipment Types

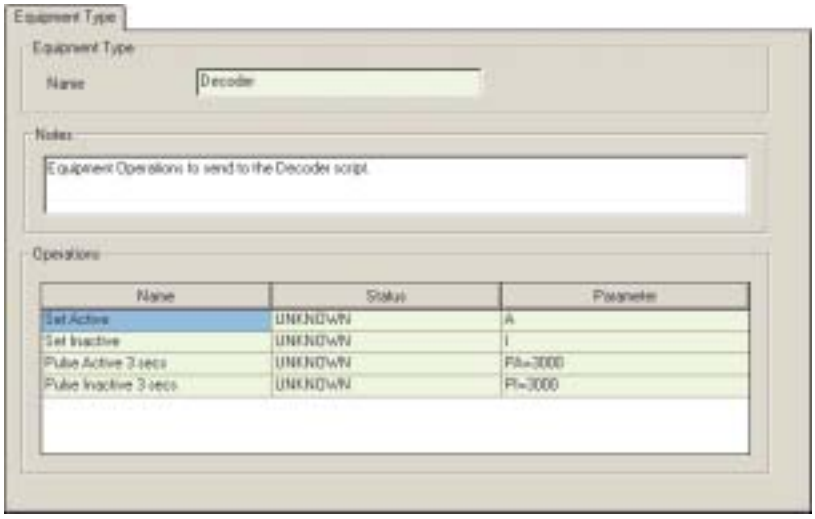
An equipment type record contains the operation parameters (commands) used to execute actions on a piece of equipment. For example, a record could contain the parameters required to send active, inactive, or pulse commands to various equipment, which could turn them on, off, or reset them.

Use the Equipment Types tab to create equipment type records that list the operations and parameters for executing actions. Later, you will assign your equipment type record to a host device (see, ”Host-Equipment Tab’, page 2-17) where you will also list all the different equipment that uses these operation parameters.



To create an equipment type record

1 Right-click the Equipment Types folder; then, select Add Equipment Type from the pop-up menu. The system opens the Equipment Type tab.



2 Type the name of your equipment type in the **Name** field.

3 Type any description or comments in the **Notes** field.

4 Type the name of your operation in the **Operations Name** field. The name should reflect the operation's purpose.

5 Type the parameter string for each operation in the **Parameter** field. The parameter string tells the control element to execute an action. For example, IRISnGEN will pass this string to a script program running on the SEBea remote agent. The script interprets the string and executes the operation.



Note *Check your equipment manufacturer's documentation if you are unsure of your equipment's operation parameters.*

6 Save your equipment type record.

To add an operation

1 Click inside the data table.

2 Use the Insert Row button ( ) to insert a blank row in the data table.

3 Enter an operation name—for example, Active.

4 Enter the parameter that will pass to a script running on the remote agent.

5 Repeat steps 2 and 3 to add additional operation names.

Deleting an Equipment Type Record

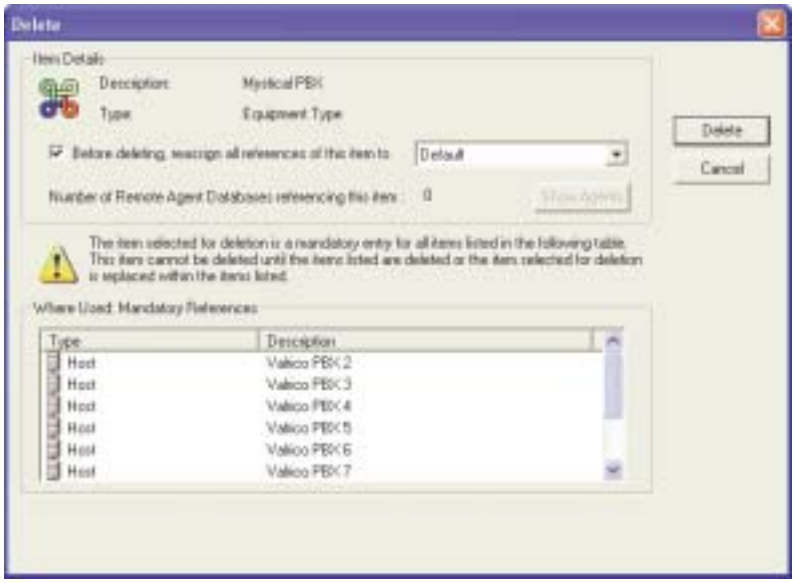
You can delete an equipment type record from your IRISnGEN system. When you delete a record, the system verifies no hosts or equipment actions reference this equipment type record. If you have hosts that reference this record, you can assign them a different equipment type before deleting this record. However, if you have actions that reference this equipment type record, you must delete those actions before you can delete the equipment type record.

To delete an equipment type record

1 Right-click the Equipment Type folder in the tree view; then, select Delete from the pop-up menu. The system displays the Delete dialog box and prompts you to reassign any hosts referencing this equipment type.



Note *If any equipment actions reference this icon, you must delete those actions before you can delete the equipment type record. You cannot reassign actions.*



2 Select the **Before deleting** checkbox and select another equipment type from the list.

3 Click ***Delete***.

IRISnGEN reassigns all the referenced hosts with the new equipment type you chose and deletes the old equipment type record from your IRISnGEN database.



Note *If you do not wish to reassign all the hosts to the same equipment type, then you must manually choose a different equipment type for each host.*

Duplicating an Equipment Type Record

You can duplicate an equipment type record and modify it to create a new record. When you do this, the entire contents of the equipment type record is duplicated.

To duplicate an equipment type record

1 Right-click the Equipment Type folder in the tree view; then, select Duplicate from the pop-up menu. IRISnGEN displays the duplicate record and displays “Copy of” in the Name field.

2 Change the name of the equipment type and the data table entries, if necessary.

3 Save your changes.

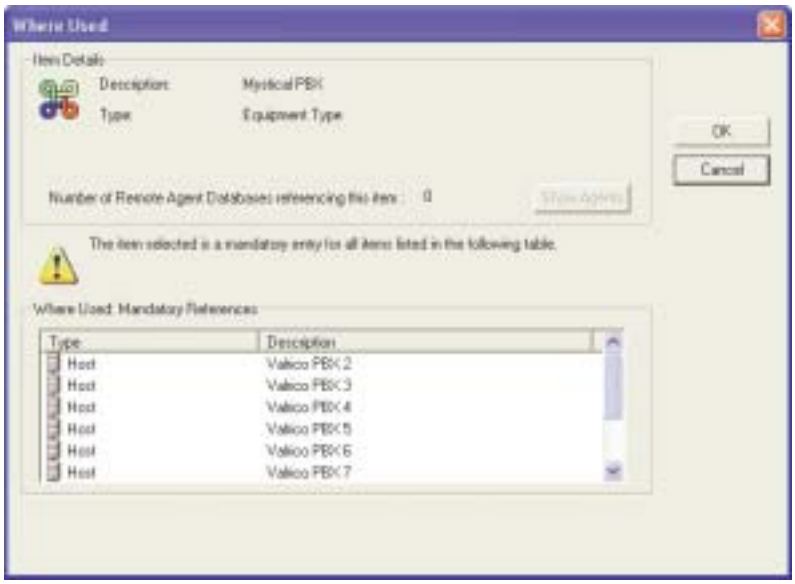


Where Used

You can quickly identify all the hosts referencing an equipment type using the Where Used feature. This can speed your operation, especially when you need to modify a particular host record.

To display Where Used

1 Right-click an equipment type name in the tree view; then, select Where Used. The system opens the Where Used dialog box for that equipment type.



2 Double-click a type (Host in the example above) to display its record.

3 Edit the equipment type for the host.

4 Save your changes.

Multi Media

You can assign any type of file to a piece of equipment. The files are stored on the IRISnGEN Server computer. Examples of files that you can assign include:

- Images (Photos / Diagrams / Drawings)
- Video clips
- Sound files
- Documentation (Word, Excel, etc)
- Maps / Directions
- Web Links

In order to properly view the Multi Media files, you must also install the appropriate program application – for example, Windows Media Player, Word, Paint Shop Pro, etc.– associated with each file type (extension) on the computer that is running the Equipment Explorer application.

To create a multi-media record

1 Right-click the **Multi Media** folder; then, select **Add Multi Media** from the pop-up menu.

2 Type a name for your multi-media object in the **Name** field.

3 Select an icon from the **Icon** list. IRISnGEN uses this icon as a visual representation on the Map Viewer and in the Equipment Explorer for this object.

4 Do one of the following:
   - Type the file name and path of the multi-media object in the **File Name** field.
   - Click the Browse button ( ) to open a standard Open dialog; then, select your multi-media object. The system automatically inserts the size (in bytes) of the object in the File Size field.

5 Type any description or comments in the **Notes** field.

6 Save your multi-media record.



Extended Hierarchy

If your business requires a more complex database structure than the standard database for an IRISnGEN system, you can define your own hierarchy with the Extended Hierarchy function. This lets you create unlimited logical groupings of customers, sites, or host types that conform to your organizational structure and how you run your business.

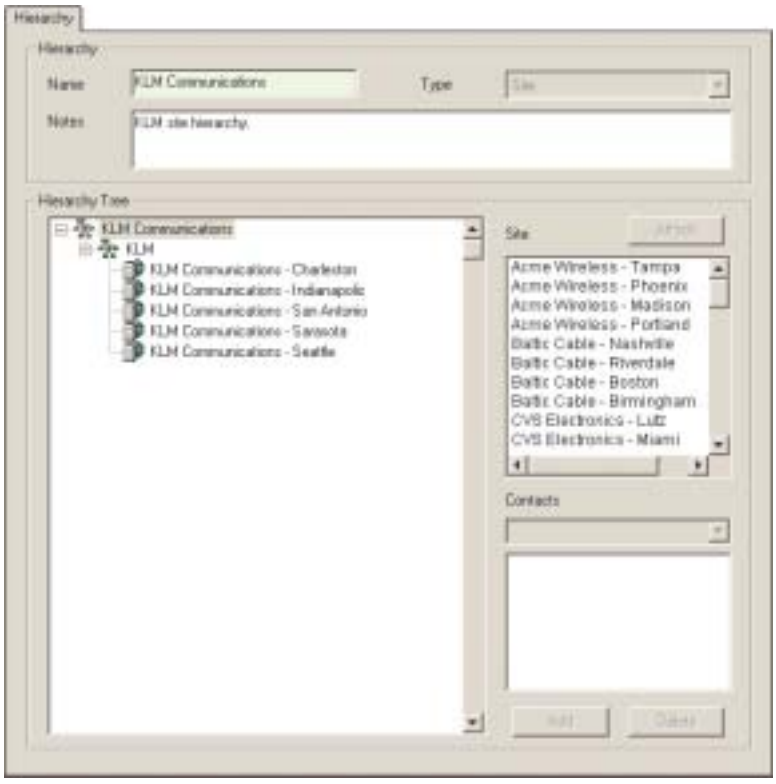
For example:

- You can group all of your sites by region and by state within the region. If you want to view or report on only the southeastern region, simply select the appropriate hierarchy node.
- You can group all hosts by categories. You can have a top level called PBXs, with second-level nodes for each PBX manufacturer, and third-level nodes for each model. With the click of a button, you can get a quick view of how a particular PBX type is performing, right down to the model.
- You may want to create a hierarchy for new customers. This lets you specially monitor these sites during their startup phase. Once the customer is operating properly for several weeks, you can remove them from the new customer hierarchy.

A customer, site or host type can belong to several hierarchy schemes.

To create a hierarchy record

1 Right-click the Hierarchy folder; then, select Add Hierarchy from the pop-up menu. The system opens the Hierarch tab.



2 Type a name for this hierarchy in the **Name** field.



Note *The hierarchy name also becomes the top-level node name displayed in the tree when you save the hierarchy.*

3 Select a type from the **Type** list to group objects logically. You can choose from Customer, Site, or Host Type.

4 You cannot change a type once you select it. When you select a type, the Type combo box dims.

5 Type any description or comments in the **Comments** field.

6 Insert a node into the hierarchy tree, or under an existing node, right-click the hierarchy or note and select Insert from the pop-up menu.

7 Once you have inserted a node, the system enters the Edit mode so you can edit the node name. You must enter a name for each node in the hierarchy. Clicking outside the edit box ends node name editing.



Note *You cannot edit the top-level node name in the tree view, but it will change to the Hierarchy name when you save the record.*

8 Attach items to hierarchies by clicking Attach and selecting the names from the list box. As you attach items, the system removes the names from the list of available names. You can attach an item to a hierarchy once.

9 Click ***Attach*** to display a list of objects in the Customer, Site, or Host Type fields.

10 Select a contact from the **Contacts** list. You can add multiple contacts to each node.

11 Click ***Add*** to assign the contact to that node.

To remove a contact from a node

- Highlight the contact or contacts that you wish to remove; then, click ***Delete***.

Inserting and Renaming Nodes

To insert a node

1 Under an existing node, right-click the hierarchy or node; then, select Insert from the pop-up menu.



Once you insert a new node, the system enters edit mode allowing you to edit the node name.

2 Enter a name, then click outside the name field to end edit mode.



To rename a node

1 Right-click the hierarchy (or node); then, select Rename from the pop-up menu.

2 Select the node by clicking on its name. The system enters edit mode and the node name highlights.



3 Enter the new name; then, click outside the field to exit edit mode. You cannot rename the hierarchy or objects in the hierarchy tree.

Deleting Nodes and Objects

To delete node and objects

1 Right-click the name of the node or object; then, select Delete from the pop-up menu, or select the node.

2 Press the Delete key on your keyword. If the node contains other nodes or objects, the system will prompt you for confirmation before deleting the node.



3 Click ***Yes*** to continue deleting the node; otherwise, select ***No***.

As you delete objects from the nodes in the hierarchy, the system adds them back to the list of available objects displayed in the Object list box.

Attaching Objects

To attach an object to a node

1 Select the node, and then select an object or objects in the Objects list box.

2 Click ***Attach***.

3 Select the node, and then double-click the object in the Object list box.



Adding and Deleting Contacts for Hierarchies

You can add multiple contacts to each node in the hierarchy. The contact name displays in the Contact list box. When you select something other than a node type, IRISnGEN disables the Add and Delete functions.



To add contacts to nodes

1. Select a node; then, select a contact from the Contact choice list.
2. Click ***Add***.

   As you add contacts to nodes in the hierarchy, the system removes them from the list of available contacts displayed in the Contact combo box.

To delete contacts from nodes

1. Select a node; then, select a contact from the Contact choice list.
2. Click ***Delete***.

   As you delete contacts from nodes in the hierarchy, the system adds them to the list of available contacts displayed in the Contact combo box.

Dragging and Dropping Nodes and Objects

You can drag and drop nodes and objects from one position to another in the hierarchy.

To drag and drop nodes and objects

1. Click on a node or an object to highlight it.
2. While holding down the left mouse button, drag it over a hierarchy or another node and release the mouse button.

If you drag a node that has other nodes or objects under it, they will move as well.

- You cannot drag nodes onto objects, only hierarchies.
- You cannot drag objects onto hierarchies.
- You cannot drag a hierarchy.
- You cannot drag a node onto its child node, nor to its parent node.

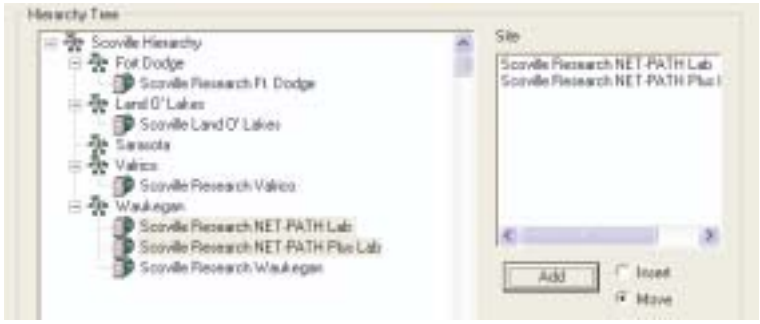


Moving several items within a hierarchy

You can move several items within the hierarchy tree at one time without having to drag and drop each item..

To move several items within a hierarchy

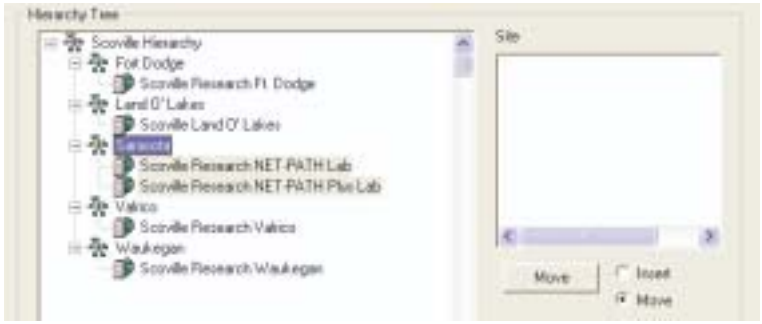
1 Click on an item to highlight it, as shown below.



2 Click the **Move** radio button to clear the list on the right; then, click the **Add** button. IRISnGEN copies the item to the list.

3 Repeat steps 1 and 2 for each item you wish to move. You can double-click any item in the list to remove it.

4 Click the node that is to receive the items, as shown below. Notice the **Add** button is replaced with the **Move** button.



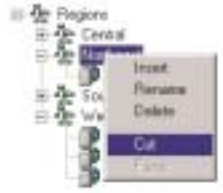
5 Click the **Move** button to move the items to the destination node.

6 Click the **Save** button to save your changes.

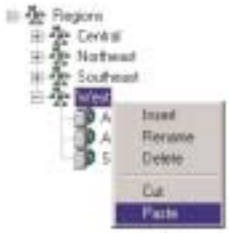
Cutting and Pasting Nodes and Objects

To cut and paste nodes and objects

1 Right-click on a node or object and select Cut from the pop-up menu.



2 Move your mouse pointer to the new location; then, right-click the mouse and select **Paste** from the pop-up menu.



Duplicating Hierarchies

You can duplicate an entire hierarchy.

To duplicate a hierarchy

1 Choose a hierarchy; then, right-click the mouse and select Duplicate from the pop-up menu.



2 Rename the duplicated hierarchy with a unique name that easily identifies its use.

Holidays

The IRISnGEN system lets you filter alarms selectively based on whether or not they occur on a holiday. You can define what days are holidays for your system.

To create a holiday record

1. Right-click the Holidays folder; then, select Add Holiday from the pop-up menu. The system opens the Holiday tab.



2. Type the name of the holiday in the **Name** field—for example, Flag Day, Good Friday, Yom Kippur, or Martin Luther King Day.
3. Select the day and month from the **Date** lists.
4. Save your Holiday record.

Host Types

The Host Type record defines all of the host device types that the IRISnGEN system monitors. You can take advantage of this database feature by creating host type definitions for each model of product you monitor. You can assign alarm filters, alarm thresholds, and alarm correlation to each host type using this tab. This greatly reduces database maintenance when working with several hundred hosts of the same type. You can also use the host type as selection criteria for viewing and reporting alarm data.

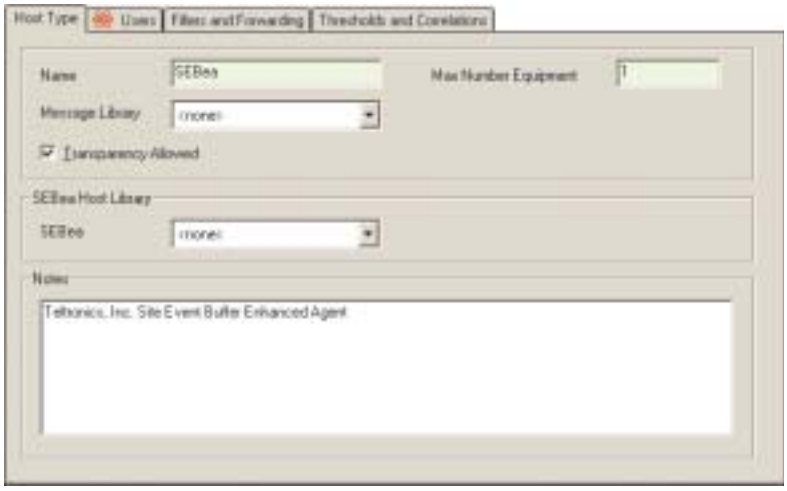
Use the host type during modem communications. For each modem group, define a list of host devices that are compatible with the modems assigned to a group. The modem initialization strings are customized to support communications with the associated host types. This ensures more consistent and reliable modem communications when performing remote diagnostics and fault correction.



Note *You must create your filter sets before defining your host types.*

To create a host type record

1 Right-click the Host Types folder; then, select Add Host Type from the pop-up menu. The system opens the Host Type tab.



2 Type the name of your host type in the **Name** field.

3 Select a predefined message library from the **Message Library** list.

4 If the host type is a device that connects to other devices and supports transparent communication through that connection, select the **Transparency Allowed** checkbox.

5 Enter the maximum number of equipment that can be connected to this host in the **Max Number Equipment** field. The number you enter will determine the number of Index fields on the Host Equipment tab. See ”Host-Equipment Tab’, page 2-17. This field is only valid if you are licensed for Teltronics’ Multi-Drop Alarm Delivery and Control System software.

6 Enter any applicable notes about the host type in the **Notes** field.

7 Save the host type record.

To add thresholds and correlations

1 Select the host type from the tree; then, click the Thresholds and Correlations tab.

2 Click on the toolbar to add rows to the Thresholds and Correlations data tables.

3 Select a name(s) from the Select Items dialog box.

4 Save your changes.

To add users to a host type

1 Select the host type from the tree; then, click the Users tab.

2 Click on the toolbar to add rows to the Groups and Items data tables.

3 Select a group(s) from the Select Items dialog box.

4 Adding a group adds all members of that group as users of the host type.

5 Save your changes.



To add filters and forwarding to a host type

1. Select the host type from the tree; then, click the Filters and Forwarding tab.
2. Click on the toolbar to add rows to the Groups and Items data tables.to add rows to the Filter Set and Forward Selector data tables.
3. Use the Name list to select predefined Filter Sets and Forward Selectors.
4. Save your changes.

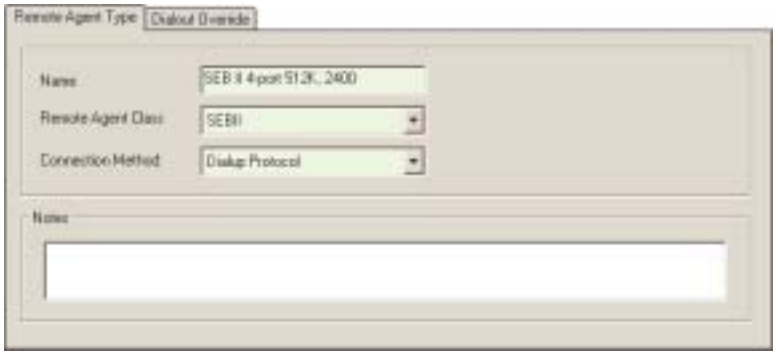
Remote Agent Type

You may have several types of remote agent operating in different environments with different connects and modem speeds. The IRISnGEN system lets you define your remote agents and classify them by their functions. For example, you can define a remote agent to use a dial-up connection, or perhaps use a direct network connection. Once you define a remote agent type, you can apply it to many remote agents in your pool of devices.

Many users refer to remote agents as collection devices. In the IRISnGEN system, remote agents are SEB II, SEBea, and foreign agents. While SEB II and SEBea agent types refer to all varieties of SEB devices, foreign agents refer to all non-SEB type devices, including Dispatchers, Visionaries, and Positrons.

To create a remote agent type

1. Right-click the Remote Agent Type folder; then, select Add Remote Agent Type from the pop-up menu.

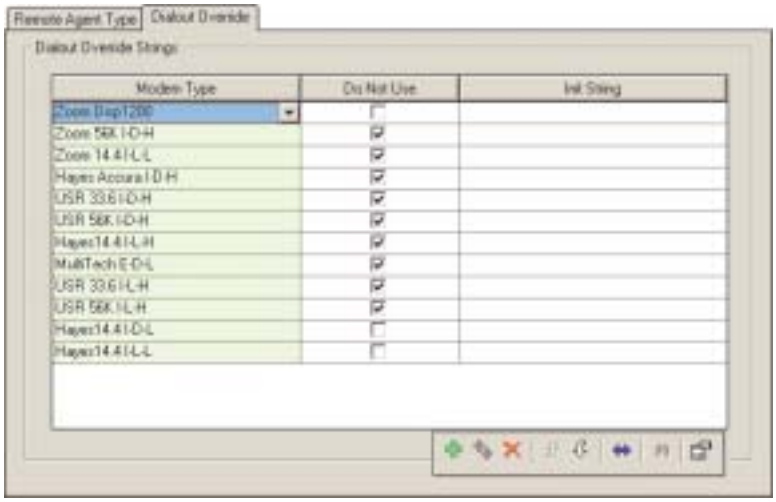


2. Type a name for the remote agent type in the **Name** field.
3. Select a class (FOREIGN, SEBEA, or SEB II) from the **Remote Agent Class** list.
4. Select a connection method (Dialup, Dialup Protocol, Network, Network Protocol, or Telnet) from the **Connection** list.
5. Save your record.

Dialout Override

To add dialout override strings

1. Select a remote agent type from the tree view.
2. Click the Dialout Override tab.



3. Click on the toolbar to add rows to the data table.
4. Select a predefined modem type from the **Modem Type** list.
5. If you do not want to use a selected modem type to connect to the remote agent type you are editing, select the **Do Not Use** checkbox.
6. Type the modem initialization string in the **Init String** field. IRISnGEN uses this string to override the default string when calling the remote agent type, which you are now editing.
7. Save your record.



Warning *Even one wrong character in the modem initialization string can cause the modem to malfunction. Consult the modem manufacturer's user guide before entering a modem initialization string.*

6

Remote Agent Libraries

Overview

Your SEBea and NET-PATH remote agents are event-processing devices that detect event data and take action based on a predefined set of parameters. The Remote Agent Libraries are a collection of those parameters defined and saved in library records. The library records detail the physical characteristics of each remote agent and the actions each remote agent should take when an event occurs.

The Remote Agent Libraries folder contains six sub-folders, each containing its own collection of specialized library records.

- **Device Libraries** define the remote agent hardware parameters.
- **Event Libraries** define which events require action and what those actions should be, including events generated by the remote agent.
- **Host Libraries** define all the parameters for remote agents and the hosts they monitor.
- **Model Libraries** define the various remote agent models and which hardware devices to enable.
- **Security Libraries** define all the users, user groups, and their access permissions for the remote agent and the host(s) it monitors.
- **Template Libraries** combine the Device Libraries and Model Libraries into one record that you can assign to the remote agent.

This chapter explains how to use your IRISnGEN system to create the various remote agent libraries and library records and how to define the parameters in each record. Once you create a library record, you can download it to one or many remote agents, as needed.



Device Libraries

Device Libraries contain a collection of the configuration parameter records for the various hardware devices—modems, batteries, contacts, etc.—built into your remote agents. Each device has its own set of configurable parameters and event definitions. The parameters tell the remote agent how the device should operate. The fixed event definitions tell the remote agent how to notify you when an event occurs. How you configure these parameters and definitions will depend on what you want that device to do. For example, you may want to configure your remote agent's modem device to transmit at 9600 baud, its DC voltage device to use an external sensor, and its temperature sensor device to take a reading every ten seconds. The choice is yours.

Create records and configure the parameters and event definitions for each hardware device in the remote agent. Save your library record; then, assign it to the devices in the Template Library or the hardware device fields in the Devices and Hosts tab for the remote agents.

The Device Libraries folder contains twelve sub-folders.

- **Battery** defines the events associated with your remote agent's UPS battery.
- **Contact** defines the contact sensor states and fixed event definitions.
- **DC Voltage** defines the logical parameters for the DC voltage sensor.
- **Memory** configures the sample frequency and RAM disk size and fixed events definitions.
- **Modem** configures the remote agent modem settings.
- **Network** defines the NIC settings, denial of service, and fixed event definitions.
- **Power** defines the fixed event and logging settings for commercial power.
- **Relay** defines the default relay state for the remote agent's RJ45 relay jack.
- **Serial Port** defines port characteristics—baud rate, parity, transmit buffer size, etc.—and the fixed events definitions.
- **System** defines the system fixed event definitions.
- **Temperature** configures the parameters for the remote agent's temperature sensors.
- **User Interface** defines which events display on the remote agent's front panel.

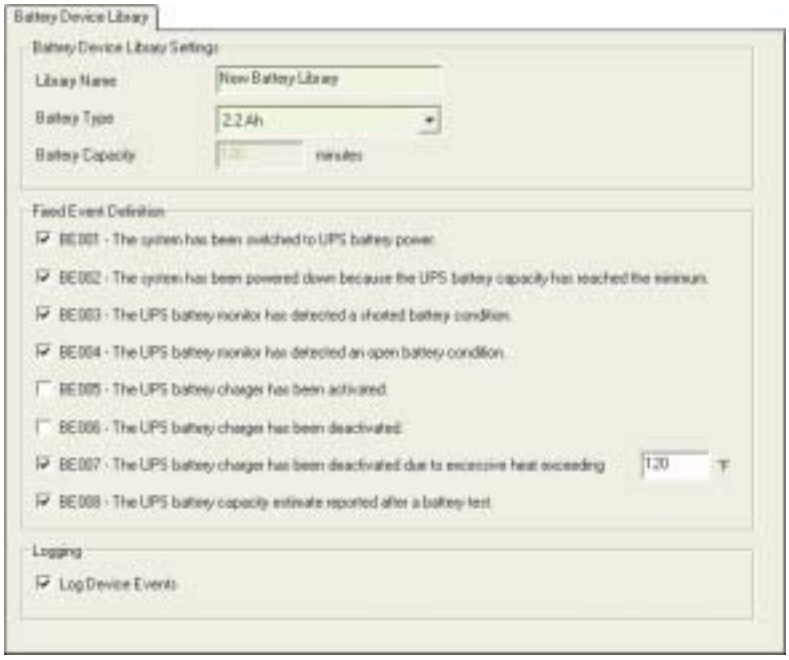


Battery Device Library

Use the Battery Library to configure the events for your remote agent's UPS battery. For example, you can configure your remote agent to report a low voltage in its battery.

To create a battery device record

1 Right-click the **Battery** folder and select **Add Battery Library**. The system opens the Battery Device Library tab.



2 Enter a name in the **Library** field that will identify this battery library in IRISnGEN.

3 Select a battery type from the Battery Type list.
- Acid
- NiCad

Check with your administrator if you are unsure of our remote agent's battery type.

4 Select the **Fixed Event Definition** checkbox for each battery fixed event you want to include in this library. The remote agent devices using this library will report only those fixed events that you selected.

5 Select the **Log Device Events** checkbox to keep a log of the battery's fixed events. All logs are circular, that is they always retain the newest events. You can retrieve these logs though polling, see "Polling', page 7-35.



Note *Use the SEBea or NET-PATH Remote Agent tabs to specify the size of the log file and where to store it (RAM or Flash).*

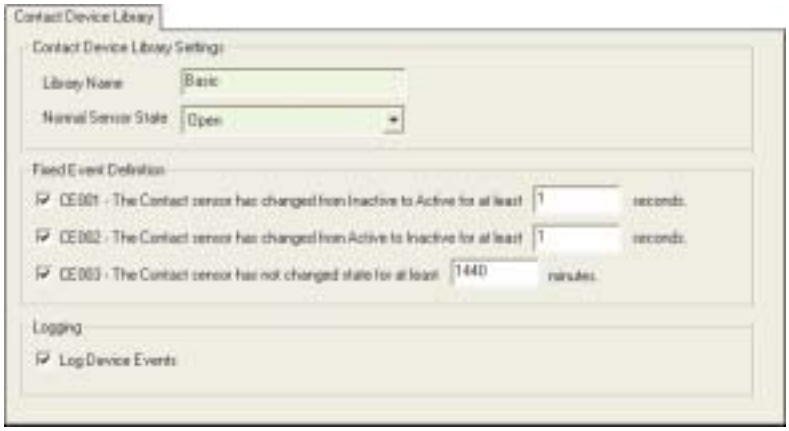
6 Save your record.

Contact Device Library

Your remote agent comes with up to sixteen pairs of contact sensor inputs. You can program the remote agent to generate an event when any of the inputs change electrical state. The contacts are set as “normally open” or “normally closed.” When the contacts are set normally open, the active state is a short across the physical sensor inputs. When the contacts are normally closed, the active state is no short across the physical sensor inputs.

To create a contact device record

1. Right-click the **Contact** folder and select **Add Contact Library**. The system opens the Contact Device Library tab.



2. Type a name **Library Name** field to help you identify it when you assign the record to the template libraries.
3. Select a sensor state (Open or Closed) from the **Normal Sensor State** list.
4. Select the **Contact Sensor Events** checkbox for each fixed event you want to include in this library. You can choose any of three fixed events.
5. For each checkbox you select, enter the duration (seconds or minutes) that the contact sensor must remain in a given state after the remote agent detects a change of state.
6. Select the **Log Device Events** checkbox if you want to keep a log file of fixed events for the contact device. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling see ”Polling’, page 7-35.*

7. Save your record.

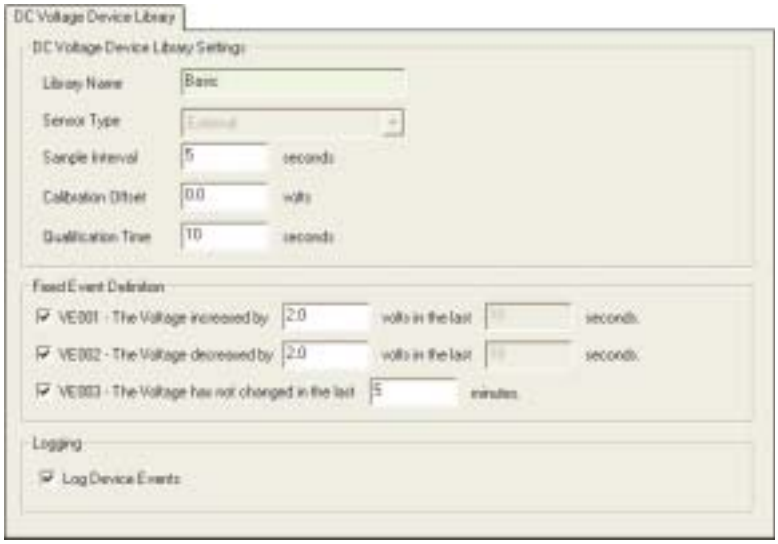
DC Voltage Device Library

The remote agent accommodates one external DC voltage sensor that monitors changes in voltage. When the remote agent detects a voltage change, it can report the change as an event.

Use the DC Voltage Device Library to create library records and define the logical parameters for DC voltage sensor. You can define the sample frequency, voltage increase and decrease thresholds (delta), and event duration. Later, you will assign these records to the Template Libraries or directly to hardware device fields in the Devices and Hosts tab for the remote agent.

To create a DC voltage device record

1 Right-click the **DC Voltage** folder and select **Add DC Voltage Library**. The system opens the DC Voltage Device Library tab.



2 Select the DC voltage settings in the first five fields.

Field	What to enter
Library Name	Enter a name to identify the library when assigning it to the template library.
Sensor Type	This combo box displays “External” for the current DC voltage sensor type. You cannot edit this field at this time.
Sample Interval	Enter the frequency (in seconds) for the voltage sampled. This field requires a numeric entry ranging from 1 to 3600. The default entry is 5 seconds.

Calibration Offset	Enter a decimal value for the DC voltage sensor calibration offset in volts. Use this offset when there is a known calibration problem with the voltage sensor. The device adjusts the voltage reading taken at the sample time by the number of volts specified in this field. The valid range of entries is –10.900 to 10.900. If you enter additional decimal places, the system truncates them to three decimal places without rounding the number. The default entry is 0.0.
Qualification Time	Enter an integer (in seconds) for the qualification time. Use qualification time in conjunction with voltage increases or decreases defined with the corresponding VE001 and VE002 fixed events. Refer to the example at the end of this section for a more complete description of the Qualification Time. The valid entries for this field are numbers from 1 to 3600 (0 or blank is not allowed). The default is 10 seconds.

3 Select the **Fixed Event Definition** checkbox for each fixed event you want to include in this library. You can select from three fixed events.

Field	What to enter
VE001 Fixed Event	Enter a decimal value to define the minimum positive voltage change (in volts, resolution to .001) allowed before generating an event. The change must last for, at least, the period entered in the Qualification Time field before the system generates the event. The system accepts a decimal value from .1 to 59.9. Zero (0) and blanks are not allowed.
VE002 Fixed Event	Enter a decimal value to define the minimum negative voltage change (in volts, resolution to .001) allowed before generating an event. The change must last for, at least, the period entered in the Qualification Time field before the system generates the event. The system accepts decimal values from .1 to 59.9. Zero (0) and blank entries are not allowed.
VE003 Fixed Event	Enter an integer to define the inactivity period, in minutes. The system generates an event when the sensor is inactive for a period longer than time specified here. The system accepts integers from 1 to 1440 in whole numbers. Zero (0) and blank entries are not allowed. The default entry is 5 minutes.



4 Select the **Log Device Events** checkbox if you want to keep a log file of fixed events for the voltage sensor device. The file is circular and always keeps the newest events.

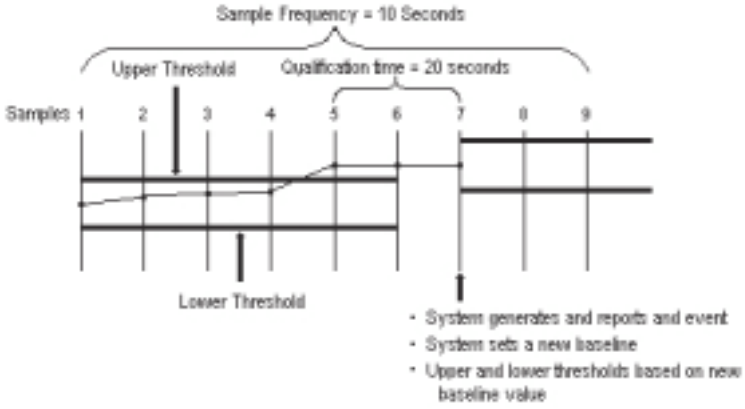


Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling see "Polling', page 7-35.*

5 Save your record.

Example

Look again at the figure on page 6-5 and note the settings. Assume we want to monitor the DC voltage for a UPS battery attached to a PBX and report any changes of +/-5 volts that last more than 20 seconds. Setting a qualification time of 20 seconds prevents the remote agent from sending a flood of event messages, should the remote agent experience random power spikes. We did not set a calibration offset and we did enable logging. Next, look at the sampling chart below.



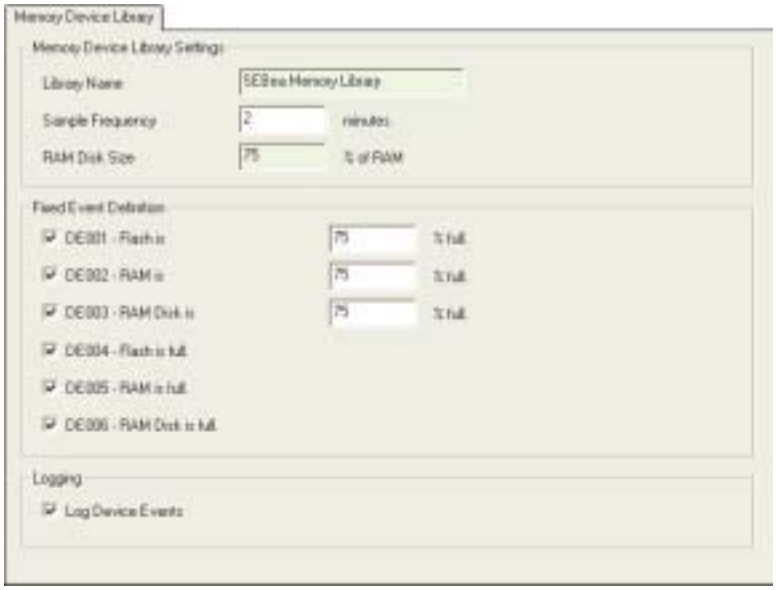
In the sampling chart above, the remote agent records the voltage at Sample 1 that becomes the baseline reading. Upper and lower thresholds are set at 5 volts above and below this baseline reading. Every ten seconds the remote agent takes another sample (Samples 2, 3, 4, and so on) and checks for and increase or decrease in voltage of more than 5 volts. Between Samples 4 and 5, the voltage exceeds the upper threshold, so the remote agent begins tracking the qualification time at Sample 5. Samples taken at 6 and 7 show the voltage remained above the upper threshold for more than twenty seconds, so the qualification time is met. At Sample 7, the remote agent generates an event to report the voltage increase. The event includes the old voltage reading, the new voltage reading, and the time from the baseline through the qualification time. At Sample 7, the remote agent also records the new voltage as the new baseline and continues using same upper and lower thresholds of 5 volts.

Memory Device Library

The remote agent comes with RAM memory. Use the Memory Device Library tab to configure the sample frequency and RAM disk size as a percentage of memory, and to select fixed events you want the system to report. Later, you will assign these records to the Template Libraries or directly to hardware device fields in the Devices and Hosts tab for the remote agent.

To create a memory device record

1 Right-click the **Memory** folder and select **Add Memory Library**. The system opens the Memory Device Library tab.



2 Type a name in the **Library Name** field to help you identify it when you assign the library to the memory templates.

3 In the **Sample Frequency** field, type the frequency (in minutes) the system should poll the remote agent's memory.

4 In the **RAM Disk Size** field, type the percent of SDRAM that you want allocated to RAM disk. Allocation occurs after you load the application and database, so the actual percentage allocated is based on unused memory, not total memory.



Note *RAM disk space is volatile and any data stored is lost during a power failure or system reset. We recommend that you use RAM disk space to store data that is not critical, such as information-only events.*

5 Select the **Fixed Event Definition** checkbox for each memory event you want to include in this library.

6 If you selected any of the first three checkboxes, enter the percentage that memory must use before the system reports the event.

7 Select the **Log Device Events** checkbox if you want to keep a log file of fixed events for the contact device. The file is circular and always keeps the newest events.



Note *Use the Remote Agent tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling, see 7-10.*



Modem Device Library

Each remote agent comes equipped with an internal modem it uses to deliver event records to IRISnGEN system, or other devices—for example, printers, pagers, and faxes. Each remote agent also supports external modems connected to its serial ports. Technicians can also use the internal (or external) modem to gain transparent access to the remote agent and the host device it monitors.

Use the Modem Device Library to create records that define the modem settings—for example, connection speed, command strings, and response strings—and to select the fixed events you want reported.



Note *The Modem Device Library records are assigned only to SEBea and NET-PATH modems. Do not confuse these records with the Modem Type records found under IRIS Administration. Modem Type records are sued with those modems directly connected to the IRISnGEN server.*

To create a modem device record

1 Right-click the **Modem** folder and select **Add Modem Library**. The system opens the Modem Device Library tab.



2 Enter the library settings in the **Modem Device Library Settings** fields.

Field	What to enter
Library Name	Enter a name to identify the library when assigning it to the modem device in the template library.

Modem Type	Select the remote agent modem type from the list. Choose: • North American 56K (Conexant) • International 56K (Multitech) • Australian/New Zealand 56K
Serial Device Library	Select a serial device library from the list. The Serial Device library links serial port parameters with the modem device. The parameters apply for an internal modem on AUX 2 and an external modem on one of the primary serial ports. When selecting a serial device library, you must choose a library with flow control set to Hardware. If you do not set flow control to Hardware, the remote agent may fail to respond. See ”Serial Port Device Library’, page 6-19 for more information about serial devices.
Maximum Connect Speed	Select a connection speed from the list to specify the maximum DTE connection speed supported by the modem.
Maximum Time to Connect	Enter the maximum time (in seconds) that the remote agent should allow the modem to establish a connection. If the remote agent fails to establish a connection within this time, dialing aborts. The default is 180 seconds.
Idle Line Input Timeout	Enter the time (in seconds) that the line can remain idle while receiving input before it times out and the remote agent disconnects. The DTE input to the remote agent from the external modem is monitored in conjunction with this setting. The default is 360 seconds.
Idle Line Output Timeout	Enter the time (in seconds) that the line can remain idle when sending output before it times out and the remote agent disconnects. The DTE output from the remote agent to the external modem is monitored in conjunction with this setting. The default is 360 seconds.
Delay After Connect	Enter the time (in seconds) to wait after establishing a connection and before attempting to communicate with the remote modem. This delay screens any line noise incurred when the connection is first established and allows clean communication between the remote agent and the modem. The default is 5 seconds.



3 Enter the modem command settings in the **Modem Command Strings** fields.

Field	What to enter
Modem Initialization String	Enter the initialization string to be sent to the modem prior to dialing. This field supports any command character accepted by the modem. You can enter up to 256 characters in this field. ***Note*** *We recommend that you do not change the default settings. Check with Teltronics Customer Service for valid modem command characters.*
Dial Command	Enter the command sequence used to dial a telephone number. This field will support any valid command character accepted by the modem. You can enter up to 256 characters in this field. The default is ATDT (tone dialing).
Answer Command	Enter the command sequenced that the remote agent device issues to the modem to answer when a ring-in occurs. ***Warning*** *Do not modify this string without first contacting Teltronics Customer Support. Entering an incorrect answer command string may result in an inability to access the remote agent from a remote location.*
Hang-up Command	Enter the command sequence that the remote agent device must issue to the modem to terminate (hang-up) an active connection. You can enter up to 256 characters in this field.

4 Enter the modem response settings in the **Modem Response Strings** fields.

Field	What to enter
Connect String	Enter the connection string containing the expected modem response when the remote agent modem connects to another modem. You can enter up to 256 characters in this field.
OK Response String	Enter the string that the modem returns when a successful command occurs.
Ring Response String	Enter the string that the modem returns when a ring is detected from the remote modem.
Busy Response String	Enter the string that the modem returns when a busy response is detected from the called number.



No Carrier Response String	Enter the string that the modem returns when a “No Carrier” response occurs. A No Carrier occurs when the other modem answers, yet the two modems cannot establish a connection.
Dial Tone Response String	Enter the string that is returned by the modem when it receives a “Dial Tone” response.
No Answer String	Enter the string that is returned by the modem whit it receives a “No Answer” response. For example, No Answers may occur due to a bad phone line, and unplugged phone line, or a wrong phone number.
No Dial Tone Response String	Enter the string that the modem returns when a “No Dial Tone” response occurs. Dial tone may fail to occur due to a bad telephone line, bad telephone cable or missing telephone cable.

5 Select the **Fixed Event Definition** checkbox for each modem event you want to include in this library.

6 Select the **Log Device Events** checkbox if you want to keep a log file of events for the modem. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling, see ”Polling’, page 7-10.*

7 Save your record.

The Caller ID tab

You can configure caller ID identification for the remote agent using either or both of two methods:

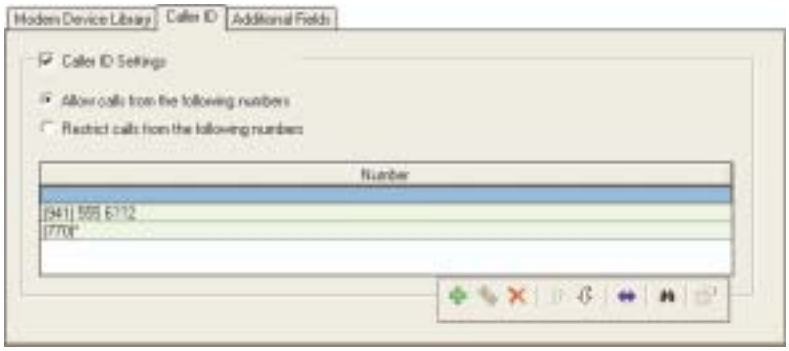
- Caller ID setting from the shard Modem Device Library
- Remote agent specific caller ID settings in the Modem Properties dialog

Use the Modem Device Library's Caller ID tab to configure the caller ID settings that are shared across multiple remote agents. All remote agents using this library automatically use these settings, unless you disallow them in the remote agent's Modem Properties dialog.



To edit the Caller ID tab

1 Click the Caller ID tab.



2 Select the **User Caller ID Settings** checkbox to enable the caller ID features.

3 Select one of the following:

- Choose the **Allow calls from the following numbers** radio button to only allow calls from the numbers listed in the Numbers table. All other numbers will be restricted.
- Choose the **Restrict calls from the following numbers** radio button to restrict all numbers in the Numbers table.

4 Enter the telephone numbers used in the **Numbers** table. If you enable the Caller ID fields, you must enter at least one number in this table. Failure to do so may cause a modem lockout to occur. Choose from the following:

- **numerals** (0-9)
- space
- **(** left bracket
- **)** right bracket
- **-** dash
- ***** asterisk
- **?** question mark

Spaces, dashes, and brackets are nut used during the processing of numbers, but are simply used for presentation and ease of reading.

The * (asterisk) wildcard represents any collection or combination of numbers. The * can be used anywhere in the numbers. Multiple asterisks can be used in the definition of the same number.

The ? (question mark) represents any single number. The ? can be used anywhere in the number. Multiple question marks can be used in the definition of the same number.

5 Save your record.

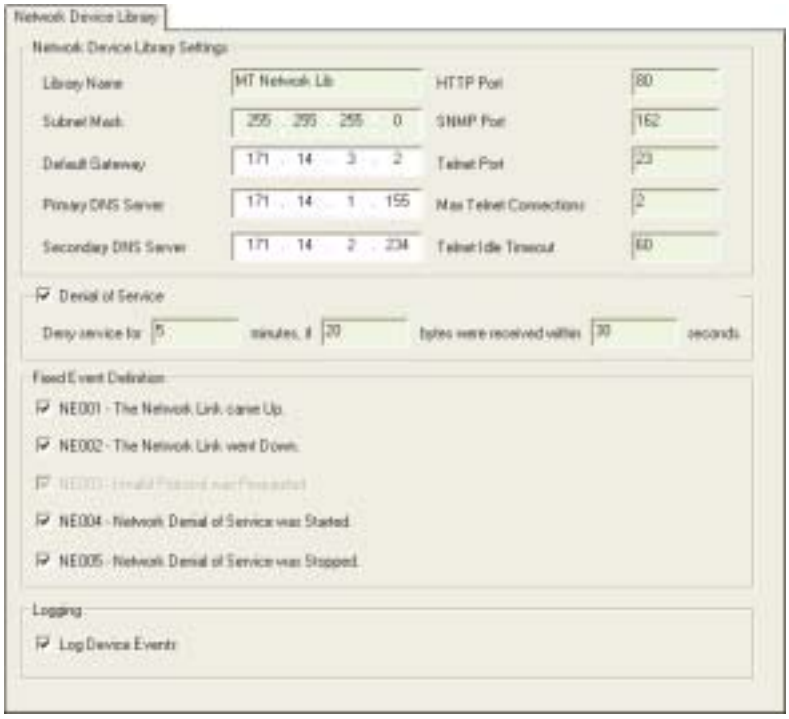
Network Device Library

Some remote agents come equipped with a network interface card (NIC) that can provide a dedicated, full-time connection to a local area network (LAN).

Use the Network Device Library to create the library records and define the NIC settings—such as the subnet mask, gateways, DNS servers, HTTP, SNMP, and Telnet ports—to define Denial of Service, to select the fixed event definitions, and enable logging. Later, you will assign these records to the Template Libraries or directly to hardware device fields in the Devices and Hosts tab for the remote agent.

To create a network device record

1 Right-click the **Network** folder and select **Add Network Library**. The system opens the Network Device Library tab.



2 Enter the library settings in the **Network Device Library Settings** fields.

Field	What to enter
Library Name	Enter a unique name to identify it in the Remote Agent window.
Subnet Mask	Enter the subnet mask on the network that attaches to the remote agent's NIC.
Default Gateway	Enter the IP address for the default gateway on the network that attaches to the remote agent's NIC. ***Note*** *This is a required field when you are using a network element that is on a different subnet than the one used by the remote agent—for example, a router, PBX, etc.*



Primary DNS Server	Enter the numbers and periods that represent the IP address of the first DNS server on the network to which the remote agent NIC is attached. Do not use computer names instead of IP addresses.
Secondary DNS Server	Enter the numbers and periods that represent the IP address of a secondary DNS server on the network to which the remote agent NIC is attached. Do not use computer names instead of IP addresses.
HTTP Port	Enter the port number to be used for HTTP communications. You can enter up to 256 characters in this field. The default is 80.
SNMP Port	Enter the port number to be used for SNMP communications. The default is 162.
Telnet Port	Enter the port number to be used for telnet communications. The default is 23.
Max Telnet Connections	Enter the number of client connections allowed simultaneously to the telnet server. The default is 1.
Telnet Idle Timeout	Enter the number of seconds after which the Telnet session ends if some event has not occurred. For example, failing to issue or respond to a command within the timeout period causes IRISnGEN to end the session.

3 Select the **Denial of Service** checkbox and enter the denial conditions in the next three fields. A Denial of Service condition disconnects a remote agent communication with the network when the remote agent receives too many network packets within a given period.

4 Select the **Fixed Event Definition** checkbox for each network event you want to include in this library.

5 Select the **Log Device Events** checkbox if you want to keep a log file of events for the network. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling, see "Polling', page 7-10.*

6 Save your record.



Power Device Library

Commercial power refers to the external power source of the remote agent. Use the Power Device Library tab to set the parameters that tells the remote agent how to respond when it loses or regains commercial power.

To create a power device record

1 Right-click the **Power** folder and select **Add Power Library**. The system opens the Power Device Library tab.



2 Type a name in the **Library Name** field to help you identify it when you assign the library to the power templates.

3 Select the **Fixed Event Definition** checkbox for each power event you want to include in this library (EE001 and EE002).

4 Select the **Log Device Events** checkbox if you want to keep a log file of events for power. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling see "Polling', page 7-10.*

5 Save your record.

Under normal conditions commercial power is present and the UPS battery has ample capacity, so the remote agent remains operational when commercial power is removed. The remote agent will generate the EE001 event while it is running on UPS battery power. The remote agent does not have enough time to record this event if it does not have UPS power.

Commercial Power Lost - Controlled Shut Down

A controlled shutdown occurs when commercial power is removed and then the UPS battery is removed. You can perform a manual controlled shut down, or the remote agent can perform an automatic controlled shutdown. The remote agent records both instances and will use this information the next time the remote agent boots.

When the remote agent loses commercial power and detects that the UPS battery is depleted (either by time or capacity) during normal operation, the remote agent turns off itself. You can also turn off the remote agent through a command sequence on the user interface, or through one of the communications devices, when the remote agent loses commercial power during normal operation. In either of these cases, the remote agent logs that it lost commercial power and how long it operated on UPS battery power before turning off. During the power up sequence, the remote agent reports that commercial power was restored and how long it was without power. It also reports the battery's current capacity estimate.

The UPS battery needs time to recharge. While charging, the remote agent monitors and records its estimated battery capacity. The system uses this information in the event that the remote agent loses commercial power before the UPS battery is completely recharged. This ensures that the remote agent has adequate time to perform an orderly shutdown.

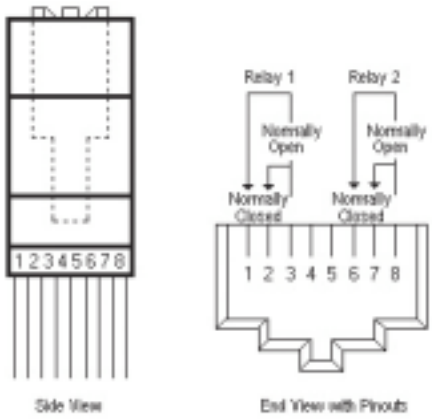
Commercial Power Lost - Abnormal Power Down

An abnormal shut down occurs when the remote agent loses commercial power and the UPS battery is unavailable. The remote agent performs an abnormal shutdown, but does not record it. Often, the remote agent will detect the UPS battery is not functioning and will attempt to close its database files. However, it is possible that the remote agent will not detect a malfunctioning battery and will not be able to close its files before shutting down.

When the remote agent has commercial power restored, it notes an abnormal power outage and reports the event. The remote agent has date and time information written to a non-volatile memory location (once per minute) and uses this information to estimate how long it was without commercial power.

Relay Device Library

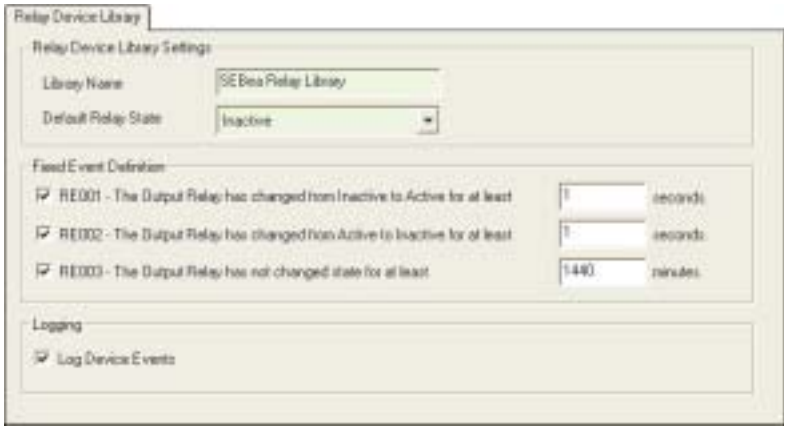
Your remote agent comes equipped with one RJ45 output relay jack, located on the back of the device. This jack supports an RJ45 cable with pinouts for two relays showing “normally open,” or “normally closed” relay states, as seen in the diagram below. A normal relay state (either open or closed) is un-energized, or inactive. Once power is applied, the relay is no longer in a normal state, but is now energized, or active. You or your technician must pinout the cables to meet your device requirements (normally open, or normally closed) before plugging the cable into the jack.



Once you set the cable pinouts, you can use the Relay Device Library tab to assign a default relay state in the remote agent database. You can choose Inactive or Active. Assigning Inactive tells the remote agent to put the relay in an un-energized (normal) state. Assigning Active tells the remote agent to put the relay in an energized state. You can also use this tab to name the relay library, define the fixed event definitions, and set logging. The following shows a sample Relay Device Library tab.

To create a relay device record

1 Right-click the **Relay** folder and select **Add Relay Library**. The system opens the Relay Device Library tab.



2 Type a name in the **Library Name** field to help you identify it when you assign the library to the relay templates.

3 Select a relay state from the **Default Relay State** list to define how to initialize the output relay jack during a power-up sequence. Once powered up, an application or script controls the relay. For example, suppose you configured your RJ45 cable relay as normally open. Setting the default state inactive tells the remote agent to reset the relay to an un-energized state. Setting the default state as active tells the remote agent to reset the relay to an energized state.

4 Select the **Fixed Event Definition** checkbox for each relay event you want to include in this library (RE001, RE002, and RE003).

5 Select the **Log Device Events** checkbox if you want to keep a log file of events for relays. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling ,see ”Polling’, page 7-10.*

6 Save your record.



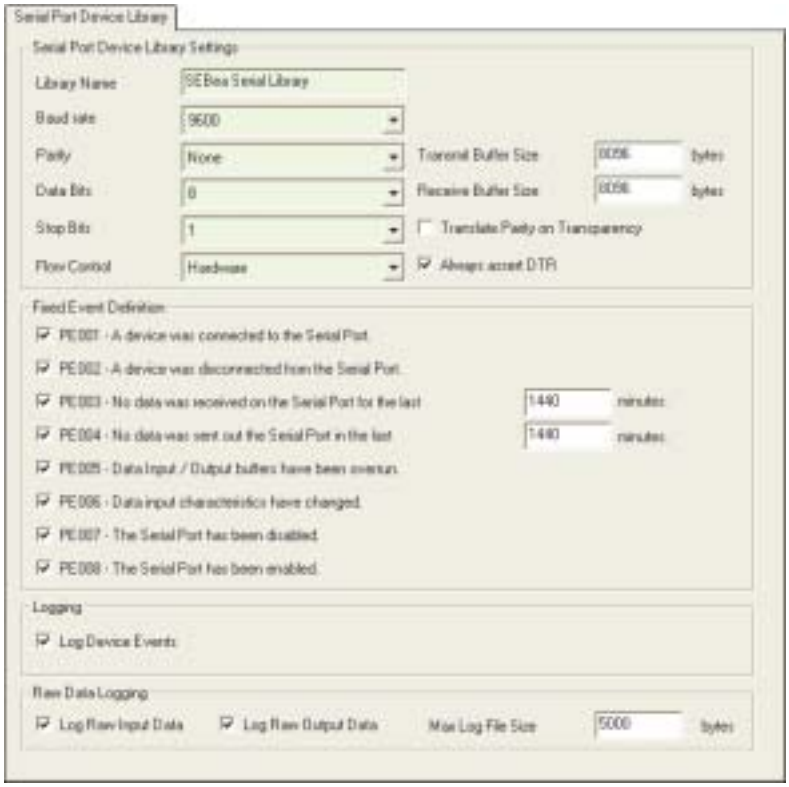
Serial Port Device Library

Remote agent models are available with up to nine serial ports. These ports provide a standard connector and protocol so that you can attach devices that you want to monitor, such as the host devices.

Use the Serial Port Library to create the library records that define port characteristics—baud rate, parity, transmit buffer size, etc.—and to select the fixed events and set logging.

To create a serial port device record

1 Right-click the **Serial Port** folder and select **Add Serial Library**. The system opens the Serial Port Device Library tab.



2 Enter the serial port settings in the **Serial Port Device Library Settings** fields.

Field	What to enter
Library Name	Enter a name that you can easily identify when you assign this library to the Serial template.
Baud Rate	Select a baud rate from the list. The baud rate must match the baud rate setting for the attached host. Mismatched baud rates may result in flawed data or no data being stored or evaluated by the remote agent device.

Parity	Select a parity from the list. The parity entry must match the parity setting on the attached host. Mismatched parities may result in flawed data, or no data being stored or evaluated by the remote agent. Options include: • **None** shows that no parity bit is to be sent, regardless of the number of bits received or sent. • **Even** sends the specified parity bit when the total number of bits received or sent is an even number. • **Odd** sends the specified parity bit when the total number of bits received or sent is an odd number. • **Mark** shows the parity bit is always 1. • **Space** shows the parity bit is always 0.
Data Bits	Select the number of data bits from the list. The Data Bits entry must match the data bits setting on the attached host. Mismatched data bits may result in flawed data, or no data being stored or evaluated by the remote agent. Options include: • **7** seven bits in the packet • **8** eight bits in the packet
Stop Bits	Select the number of stop bits from the list. The setting must match the stop bits setting on the attached host. Mismatched stop bits may result in flawed data, or no data being stored or evaluated by the remote agent. Options include: • **1** one parity bit • **2** two parity bits
Flow Control	Select the flow control setting from the list. Flow control specifies how one device tells another device to stop sending data to prevent loss of bytes. The RS232 serial leads DTR, RTS, DSR, and CTS enable flow control. Options include: • **None** no flow control for data exchange. • **Hardware** serial device hardware manages data flow. • **Software** serial device software manages data flow.
Transmit Buffer Size	Enter the maximum size of the transmitting buffer (in bytes). The system reserves this buffer space during initialization. The default size is 8096 bytes. You can increase or decrease this amount based on your installation's needs.



Receive Buffer Size	Enter the maximum size of the receiving buffer (in bytes). The system reserves this buffer space during initialization. The default size is 8096 bytes. You can increase or decrease this amount based on your installation's needs.
Translate Parity on Transparency	Select this checkbox to automatically translate parity during a transparent session. You must configure the remote agent serial host port with the same data structure and baud rate of the host device to which it connects. The remote agent supports features for the data structure that is passed through a transparent connection during a transparency session with the modem or a local serial port. When you select the Translate Parity on Transparency option, the data presented to the user is 8 bit, 1 stop bit, and no parity. If you do not select the Translate Parity on Transparency option, the data presented to the user is the same as the associated host serial port. For most applications, you should select the Translate Parity on Transparency option because it normalizes the data so that the user does not need to know the host serial port configuration to communicate with it.



Always assert DTR	Check this box if you want to assert DTR during port initialization; otherwise, leave it unchecked. When attaching a host to the serial port you will most likely want to leave this box in the checked state. By doing so, you can ensure that DTR is asserted, thus giving the host device a chance to respond with DTR and providing the Device Present condition to the remote agent. You can assert DTR from within the remote agent using a Python script. If you expect the serial port to recognize a device connected only when a script is running, you can uncheck this box and assert DTR as part of the script. You may also use scripting to wink DTR if the host requires it. When attaching a modem to a serial port, you may want to uncheck this box. Assigning a Modem Device library to the port automatically asserts DTR to facilitate communication with the modem. Entering transparency will automatically assert DTR. If the DTR checkbox is unchecked, DTR is lowered when you exit transparency, returning it to the state it was in before transparency began. In most cases you can leave this option selected without any ill effects.

3 Select the **Fixed Event Definition** checkbox for each serial port event you want to include in this library.

4 Select the **Log Device Events** checkbox if you want to keep a log file of events for serial ports. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling ,see "Polling', page 7-10.*

5 Select the **Log Raw Input Data** checkbox to enable logging of I/O data coming into the serial ports. Lead status changes are not logged, only serial data are logged. Other port logging is available at the host type and system level.

6 Select the **Log Raw Output Data** checkbox to enable logging of I/O data going out the serial ports. The system generates the file name. Lead status changes are not logged, only serial data are logged.

7 Enter the maximum size of the log file (in bytes) in the **Max Log File Size** field. Use this field for serial data I/O logging, not fixed event logging. It works with both input and output raw data passing through the serial ports. The default is 5000 bytes.

8 Save your record.

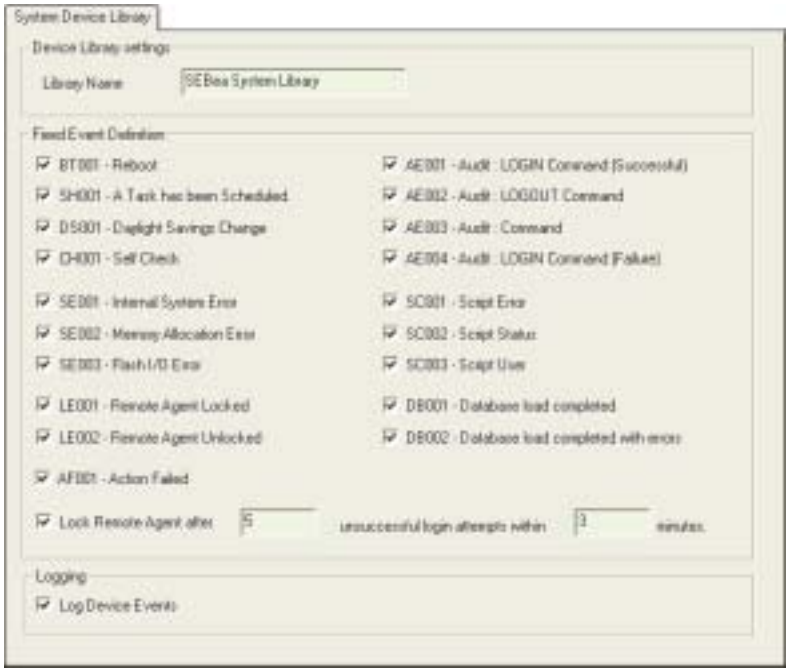


System Device Library

In addition to selecting the fixed event definitions that report remote agent device errors, you can also select fixed events that report system errors, including a self-check, internal system, reboot, etc. Use the System Library to create the records that contain the system fixed event definitions.

To create a system device record

1. Right-click the **System** folder and select **Add System Library**. The system opens the System Device Library tab.



2. Type a name **Library Name** field to help you identify it when you assign the library to the system device templates.
3. Select the **Fixed Event Definition** checkbox for each system event you want to include in this library.
4. Enter the number of unsuccessful login attempts and the number of minutes in which the attempts can occur in the **Lock Remote Agent** fields. When the unsuccessful login attempts exceed these values, the system locks and prevents users from gaining access to the system.

   All non-protocol logins to the remote agent are blocked. To unlock the remote agent, you must log into a protocol session using Remote Agent Manager, and then enter the system password. Next, you must select the Unlock option from the Action menu, or choose the Unlock icon.
5. Select the **Log Device Events** checkbox if you want to keep a log file of events for system devices. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling, see "Polling', page 7-10.*

6. Save your record.

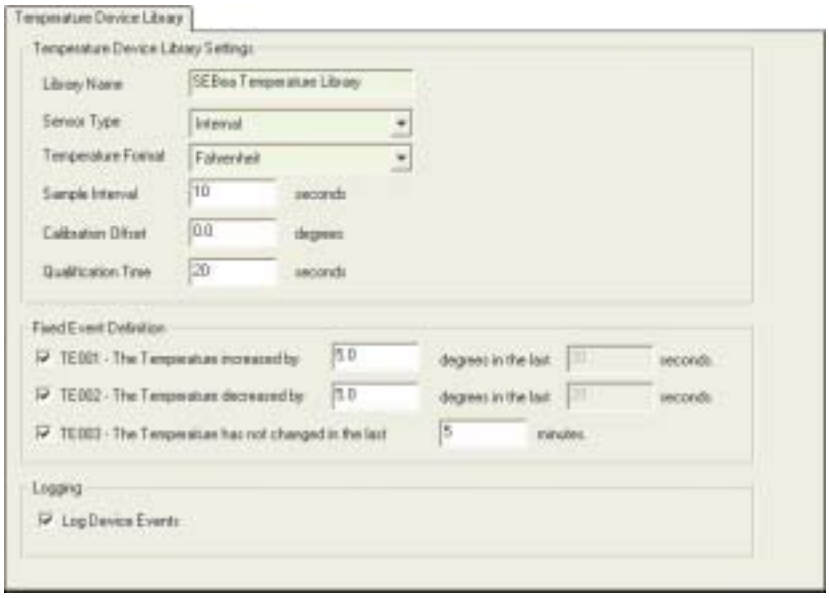
Temperature Device Library

Your remote agent comes equipped with an internal and an external temperature sensor. The internal sensor monitors the internal temperature of the remote agent device. The external sensor attaches to an RJ45 connection on the remote agent and can be placed near the remote agent to monitor such things as the ambient room temperature, or placed next to a battery charger to monitor for overheating. When the remote agent detects a temperature change, either internal or external, it reports the change as an event.

Use the Temperature Device Library to create library records and to configure logical parameters for both types of temperature sensors. This includes defining sample frequencies, temperature increase and decrease thresholds (delta), and durations used to qualify how long the temperature must exceed the threshold before the remote agent generates an event.

To create a temperature device record

1 Right-click the **Temperature** folder and select **Add Temperature Library**. The system opens the Temperature Device Library tab.



2 Type a name in the **Library Name** field to help you identify it when you assign the library to the temperature device templates.

3 Select a sensor type from the **Sensor Type** list. Select Internal or External.

4 Select a temperature format from the **Temperature Format** list. Once you select a format, all fields requiring a degree specification will refer to degrees in that format. Select Celsius, Fahrenheit, or Kelvin.

5 Type the frequency—1 to 3600 seconds—in the **Sample Interval** field to sample the temperature. The default entry is 5 seconds.

6 Type the temperature sensor calibration offset— –10.900 to 10.900 degrees— In the **Calibration Offset** field. Use the offset when there is a known calibration problem with the temperature sensor. The offset adjusts the temperature reading taken at the sample time by the number of degrees specified in this field. The application truncates entries that exceed three decimal places. The default entry is 0.0.

7 Enter the qualification time—1 to 3600 seconds—in the **Qualification Time** field. Qualification time is the parameter used when measuring the temperature increase or decrease. The system reports it with the TE001 and TE002 fixed events. Refer to the example at the end of this section for a complete description of qualification time. The default is 10 seconds.



8 Select the **Fixed Event Definition** checkbox for each temperature event you want to include in this library.

9 Select the **Log Device Events** checkbox if you want to keep a log file of events for temperature devices. The file is circular and always keeps the newest events.

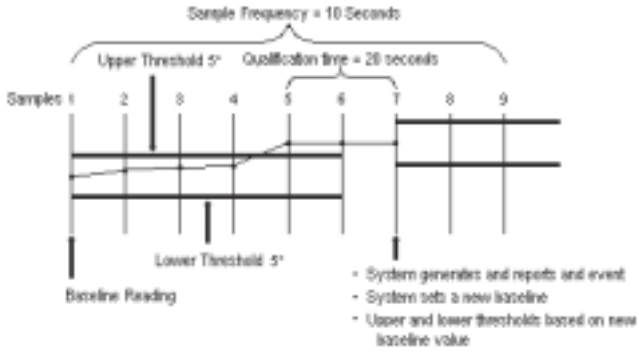


Note *Use the Remote Agent tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling, see "Polling', page 7-10.*

10 Save your record.

Example

Look again at the previous figure and note the parameter settings. Assume we want to monitor the internal temperature of the remote agent and report any temperature changes of +/-5° that last more than 20 seconds. Setting a qualification time of 20 seconds prevents the remote agent from sending a flood of event messages, should the remote agent experience random temperature spikes. This also allows us to see any gradual, but acceptable, increases in the internal temperature, which may occur during the power up sequence. We did not set a calibration offset, but we did enable logging. Look at the sampling chart below.



In this chart, the remote records a temperature at Sample 1, which becomes the baseline reading. Upper and lower thresholds are set at 5° above and below this baseline temperature. Every ten seconds the remote agent takes another sample (Samples 2, 3, 4, and so on) and checks for and increase or decrease in temperature of more than 5°. Between Samples 4 and 5, the temperature exceeds the upper threshold, so the remote agent begins tracking the qualification time at Sample 5. Samples taken at 6 and 7 show the temperature remained above the upper threshold for more than twenty seconds, so the qualification time is met. At Sample 7, the remote agent generates an event to report the temperature increase. The report includes the old temperature reading, the new temperature reading, and the time from the baseline through the qualification time. At Sample 7, the remote agent also records the new temperature as the new baseline and continues using same upper and lower thresholds of 5°.

User Interface Device Library

When setting your remote agent parameters, you can select device event definitions that report the changes to the remote agent's front panel display, or report when a button is pushed. For example, you may select an event definition to report that the alarm LED illuminates or you may select the event definition that reports when a user pushes a navigation button.

To create a user interface device record

1 Right-click the **User Interface** folder and select **Add User Interface Library**. The system opens the User Interface Device Library tab.



2 Type a name **Library Name** field to help you identify it when you assign the library to the user interface device templates.

3 Select the **Fixed Event Definition** checkbox for each user interface event you want to include in this library.

4 Select the **Log Device Events** checkbox if you want to keep a log file of events for user interface devices. The file is circular and always keeps the newest events.



Note *Use the SEBea and NET-PATH tabs to define the location and size of the log file (Flash or RAM). You can retrieve log files though polling, see "Polling', page 7-10.*

5 Save your record.



Event Libraries Menu

Event Libraries are collections of configuration parameter records that define the four stages of event processing—event detection, event matching, event processing, and event actions. Using event libraries, you can define how a remote agent finds an event in a raw data stream, how it parses the event to determine its importance, how it analyzes the event to determine needed action, and how it takes that action—for example, storing and reporting the event, activating an alarm buzzer, or executing a script.

The Event Libraries folder contains fifteen sub-folders, each containing its own collection of specialized library records. These sub-folders include:

- **Action** defines the operations that execute after the remote agent processes an event.
- **Action Windows** defines the times when the remote agent will take action in response to an event occurrence.
- **Correlation** defines the actions when the remote agent receives a specific sequence of events that relate to each other.
- **Event Detection** defines the parameters for grouping incoming data into logical event records.
- **Event Match** defines the matching parameters the remote agent uses to determine individual alarm conditions.
- **Expect** identifies the anticipated events and the actions to handle them.
- **File Types** defines the file handling parameters.
- **Filter** identifies an event by its predefined definition; then, links it with an action (fixed events or event matches).
- **Fixed Event** selects the fixed events upon which the remote agent takes action.
- **Holiday Libraries** defines the holidays.
- **Layout** formats event text for reporting purposes.
- **Script** identifies which scripts (written in Python) to include in the database download.
- **SNMP Layouts** formats SNMP traps for reporting purposes.
- **Task** schedules actions or commands to execute at specific times or at intervals.
- **Threshold** triggers an action when the system detects a specified number of events.

This chapter explains how to create the various event library records and how to define the parameters in each record. Once you create a library record, you can assign it to one or more remote agents, as needed.



Action Libraries

The Event Libraries control each stage of event processing—detection, matching, processing, and action. It is during the action stage that the remote agent determines what action it should carry out and how to carry out that action. For example, after your remote agent processes an event, you may choose to sound a buzzer to alert you of a problem, or you may choose to send a fax report, execute a script, or store the information for later review. You can choose one or more of each type.

Action libraries define the configuration parameters for each action. Once created, you can assemble the actions into action groups so you can perform several actions at once. Later, you can assign these actions or action groups to the correlation, expect, filter, and threshold libraries.

The Action Libraries folder contains twelve sub-folders that contain all the action definitions. These sub-folders include:

- Buzzer
- Fax
- LCD
- LED
- Pager
- Relay
- Report
- Script
- SNMP
- Store
- Terminal
- Trigger Event

The following sections cover each action in the Actions folder.



Buzzer Action Tab

When taking an action in response to an event, you may choose to sound the buzzer located inside the remote agent to alert you of an event. Using the Buzzer Action tab to create a library record and to set the buzzer parameters.

To create a buzzer action record

1 Right-click the **Buzzer** folder and select **Add Buzzer Library**. The system opens the Buzzer Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want to start the action.

5 Select a sound type from the **Sound Type** list. Select:

- Count - the buzzer executes an on-off sequence for a specific number of counts
- Duration - the buzzer sounds (executes an on-off sequence) for a specific duration of time.

6 Enter the number of times or seconds the buzzer should sound in the **Sound Buzzer** field. If you selected Count in the previous field, the buzzer will sound for the number counts entered in this field—for example, the buzzer will sound for three times (counts). If you selected Duration in the previous field, the buzzer will sound for the number of seconds entered in this field—for example, the buzzer will sound for three seconds.

7 Enter the duration (1-10 seconds) of the buzzer's on/off sequence in the **Active** and **Inactive** fields.

8 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

9 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a buzzer action fails.

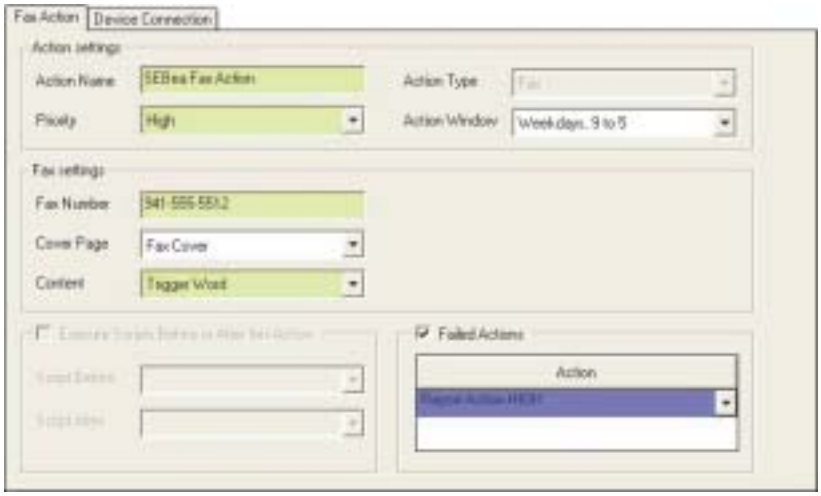
10 Save your record.

Fax Action

You can report an event to a fax machine. Use the Fax Action tab to create a Fax Library record and to define the fax setting, such as telephone number, cover page, and content. When complete, click the Device Connection tab and define the fax device setting, such as the device type and name, general connection settings, and modem settings.

To create a fax action record

1 Right-click the **Fax** folder and select **Add Fax Action**. The system opens the Fax Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want to start the action.

5 Type your fax number in the **Fax Number** field. Be sure to include any special dialing codes, spaces, or dashes.

6 Select a layout from the **Cover Page** list. The layout will serve as a cover page for your fax. If you leave this field blank, no cover page will be added to your fax (see ”Layouts’, page 6-93).

7 Select a layout from the **Content** drop that defines the content of the report.

8 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

9 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a fax action fails. You cannot select the same action twice.

10 Save your record.

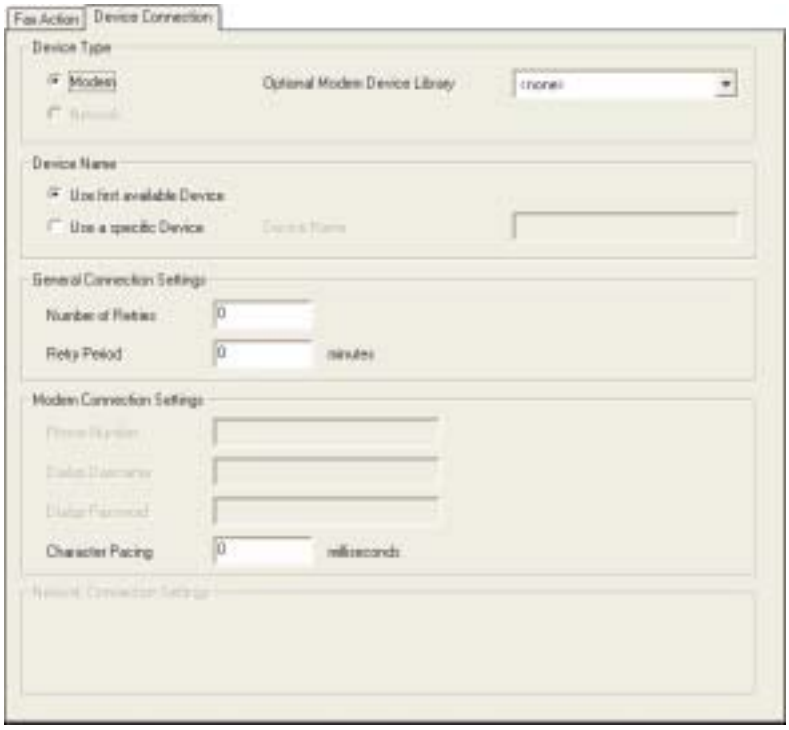


Fax Device Connection Tab

Use the Device Connection tab to define the fax device settings, such as the device type, device name, general connecting settings, and modem connection settings, for your fax device.

To add fax connection settings

1 Click the **Device Connection** tab.



2 Select the **Modem** radio button to send reports to a fax machine via a modem. This is the only option available with this release.

3 Select a library from the **Optional Modem Device Library** list to override the modem's current library settings. For example, you need to slow the modem's speed when faxing to slower equipment. Select a new library with slower speed settings that the modem will use when faxing. All other times the modem will use its original settings, see "Modem Device Library', page 6-9.

4 Select a device name radio button for the modem you want to use.

Click	To
Use first available Device	Use the first available outgoing modem in your remote agent.
Use a specific Device	Use a specific modem in your remote agent. If you choose this button, you must also enter the modem name in the Device Name field to the right. The name you enter must already be defined in the Devices and Host tab of your remote agent record.

5 Enter the number of delivery attempts the remote agent should make before telling the modem to hang up in the **Number of Retries** field. Once it reaches the number of retries, the remote agent abandons any further attempts to deliver the event information.

6 Enter the number of minutes the remote agent should wait between retries in the **Retry Period** field. The remote agent will not deliver the event information once it has exceeded the number of minutes defined in this field.

7 Enter the time (in milliseconds) that the modem should pause between characters when sending them to the fax machine in the **Character Pacing** field.

8 Save your record.



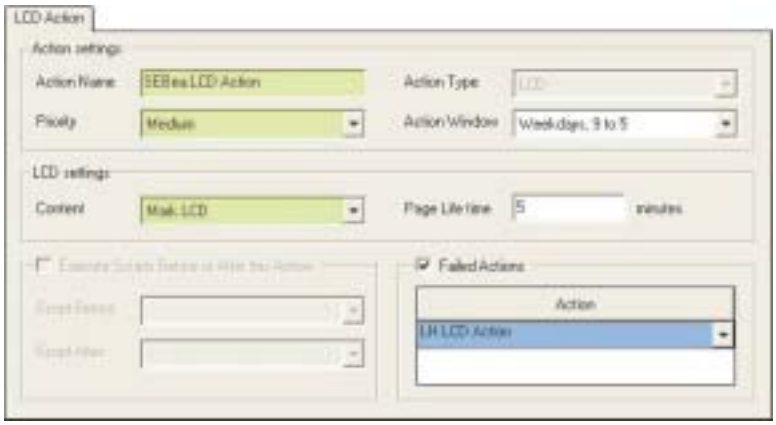
LCD Action

You may want to display some event information, such as remote agent internal alarms, on the remote agent LCD screen. The LCD screen can display up to four lines of text at a time. Each line of text can contain up to twenty characters. The text displayed on each line is configured in a Layout library record. If you have not created a layout for this action, do so now, then return to this section. For more information, see ”Layouts’, page 6-93.

Use the LCD Action tab to create the LCD library records and to define the LCD settings.

To create an LCD action record

1. Right-click the **LCD** folder and select **Add LCD** Action. The system opens the LCD Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

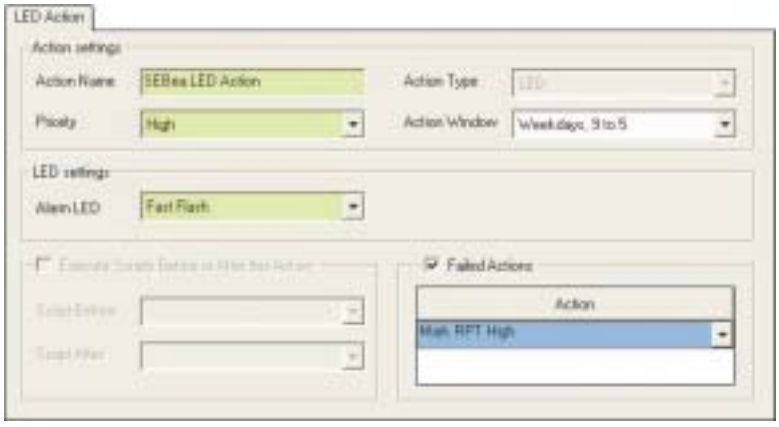
2. Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.
3. Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.
4. Select an action window from the **Action Window** list to set the time you want the action to start.
5. Select a layout from the **Content** list to display event information on the LCD screen. The layout defines the format for the text display. We recommend that you select a layout that adjusts the message content to fit the remote agent display (4 lines, 20 characters per line). For more information, see ”Layouts’, page 6-93.
6. Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.
7. Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a LCD action fails. You cannot select the same action twice.
8. Save your record.

LED Action Tab

When taking action in response to an event, you may choose to illuminate the Alarm LED on the remote agent's front panel. Use the LED Action tab to create LED library records and to define the LED settings, such as priority, flash speed, and failed actions.

To create an LED action record

1 Right-click the **LED** folder and select **Add LED Action**. The system opens the LED Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Select an illumination state for your LED display from the **Alarm LED** list. Select On, Off, Normal Flash, Slow Flash, or Fast Flash.

6 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

7 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a LED action fails. You cannot select the same action twice.

8 Save your record.

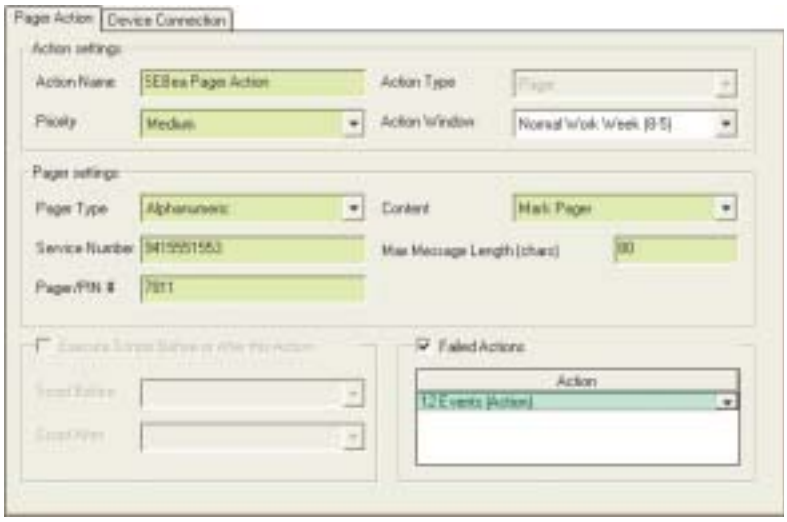


Pager Action

You can report an event via a pager device. Use the Pager Action tab to create a Pager Library record and to define the pager settings, such as telephone number, PIN number, and content. When complete, click the Device Connection tab and define the pager device setting, such as the device type, device name, general connection settings, and modem connection settings.

To create an pager action record

1 Right-click the **Pager** folder and select **Add Pager Action**. The system opens the Pager Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Select a pager type from the **Pager Type** list. Select Numeric or Alphanumeric.

6 Enter your pager number in the **Service Number** field. Be sure to include any special dialing codes, spaces, or dashes.

7 If your pager requires a PIN number, enter it in the **Pager/PIN#** field. This field is not used for numeric pagers.

8 Select a layout from the **Content** list to adjust the content of the event so it more readable on the pager display. For more information, see ”Layouts’, page 6-93.

9 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

10 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a pager action fails. You cannot select the same action twice.

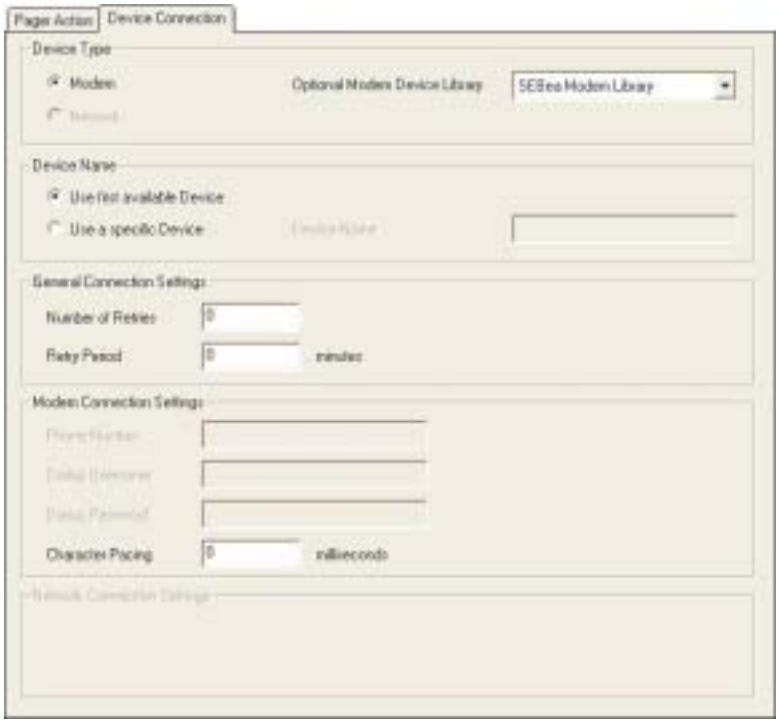
11 Save your record.

Pager Device Connection Tab

Use the Device Connection tab to define the paging modem device settings, such as the device type, device name, general connection settings, and modem connection settings, for your paging device.

To add pager connection settings

1 Click the **Device Connection** tab.



2 Select the **Modem** radio button to send reports to a pager via a modem. This is the only option available with this release.

3 Select a library from the **Optional Modem Device Librar**y list to override the modem's current library settings. For example, you may need to slow the modem's speed or change the initialization string when paging. All other times the modem will use its original settings.

4 Select a device name radio button for the modem you want to use.

Click	To
Use first available Device	Use the first available outgoing modem in your remote agent.
Use a specific Device	Use a specific modem device in your remote agent. If you choose this button, you must also enter the modem name in the Device Name field to the right. The name you enter must already be defined in the Devices and Host tab of your remote agent record.



5 Enter the number of delivery attempts the remote agent should make before telling the modem to hang up in the **Number of Retries** field. Once it reaches the number of retries, the remote agent abandons any further attempts to deliver the event information.

6 Enter the number of minutes the remote agent wait before delivering the event information in the **Retry Period** field.



Note *The Phone Number, Dialup Username, Dialup Password, and Network Connection Settings fields are not implemented in this release.*

7 Enter the time (in milliseconds) that the modem should pause between characters when sending them to the pager in the **Character Pacing** field.

8 Save your record.



Relay Action

In response to an event, you may choose to activate an external device, such as bell or flashing light. To do this, you must signal the remote agent's RJ45 jack to change its relay state (energized or un-energized). It is this change in state that tells the external device that an event has occurred. Use the Relay Action tab to create the library records that define the action and relay settings.

To create a relay action record

1 Right-click the **Relay** folder and select **Add Relay Action**. The system opens the Relay Action.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Type the device name for this relay in the **Relay Name** field as defined in the remote agent's Devices and Hosts tab. See "Devices & Hosts Tab" on page 2-32.

6 Select the Default Power-up Relay State checkbox to use the default power-up state of the output relay, as defined in the Relay Device library, see "Relay Device Library', page 6-17.

7 Enter the lapse time (in seconds) that is required before the relay begins a new activity state in the **Delay** field. The system measures time lapses from the moment the relay begins its default power-up state.

8 Select an activity state from the **Activity State** list. Select: Active, activate the relay; Inactive, deactivate the relay; or Toggle; change Active to Inactive, or Inactive to Active.

9 Enter the duration time (in seconds) that is required before the relay resumes an activity state in the **Duration** field.



10 Select the **This Action overrides** checkbox to override all other relay actions and to execute before all other relay actions waiting execution.

11 Select the **No other Relay Action can override** checkbox when you do not want any other relay actions to override this relay action, even if the other action's priority is higher.

12 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

13 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a relay action fails. You cannot select the same action twice.

14 Save your record.

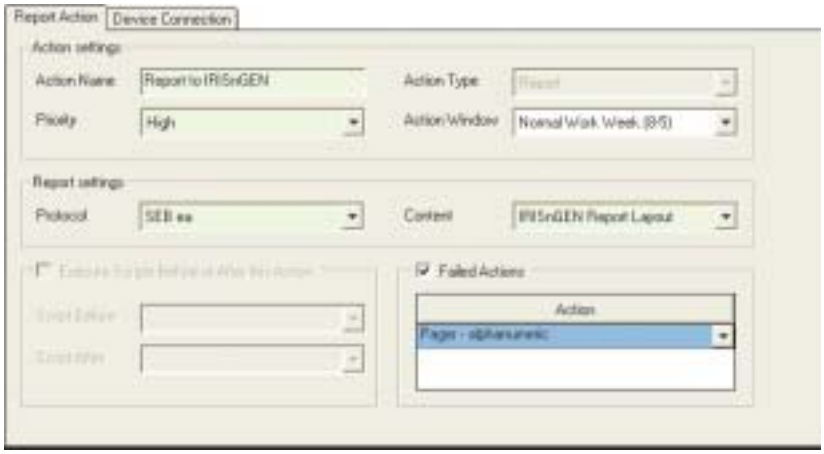


Report Action

When responding to an event, you may want to report your event to a specific device or in a format that is different from that originally received from the host system. Use the Report Action tab, shown below, to create a Report Action library record that defines how you want to report your event. When complete, click the Device Connection tab and define the modem or network settings used to report the event.

To create a report action record

1 Right-click the **Report** folder and select **Add Report Action**. The system opens the Report Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Select a protocol setting from the **Protocol** field list. Select SEBea, SEBII, or None.

6 Select a layout from the **Content** field list to adjust the content of the event to make it more readable when reported. For more information, see ”Layouts’, page 6-93.

7 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

8 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a report action fails. You cannot select the same action twice.

9 Save your record.

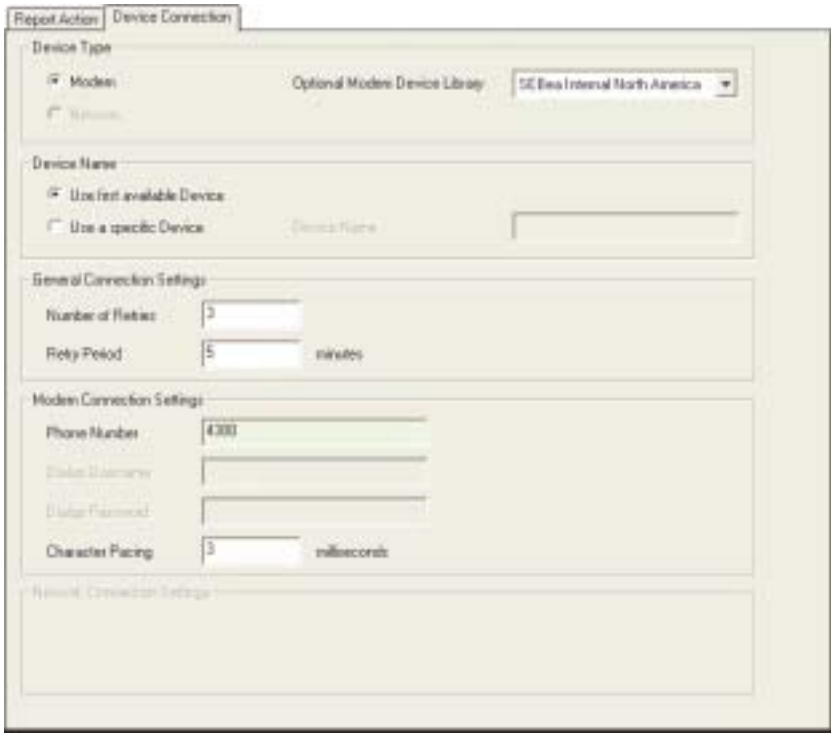


Report Action Device Connection Tab

Use the Device Connection tab to define the reporting modem device settings, such as the device type, device name, general connection settings, and modem connection settings, for your reporting device.

To set device connection properties

1 Click the **Device Connection** tab.



2 Select the **Modem** radio button to report events via a modem. This is the only option available with this release.

3 Select a library from the **Optional Modem Device Library** list to override the modem's current library settings. For example, you may need to slow the modem's speed or change the initialization string when reporting. All other times the modem will use its original settings.

4 Select a device name radio button for the modem you want to use.

Click	To
Use first available Device	Use the first available outgoing modem in your remote agent.
Use a specific Device	Use a specific modem device in your remote agent. If you choose this button, you must also enter the modem name in the Device Name field to the right. The name you enter must already be defined in the Devices and Host tab of your remote agent record.

5 Type the number of retries the remote agent should make when delivering the event before telling the modem to hang up in the **Number of Retries** field. Once the remote agent reaches the number of retries, it stops any further attempts to deliver the event.

6 Type the number of minutes the remote agent should wait to deliver the event information in the **Retry Period** field. The remote agent will not deliver the event information once it has exceeded the number of minutes defined in this field.

7 Type the remote agent's phone number in the **Phone Number** field.



Note *The Dialup Username, Dialup Password, and Network Connection Settings fields are not implemented in this release.*

8 Type number of milliseconds to pause between numbers when dialing in the **Character Pacing** field, if needed.

9 Save your record.

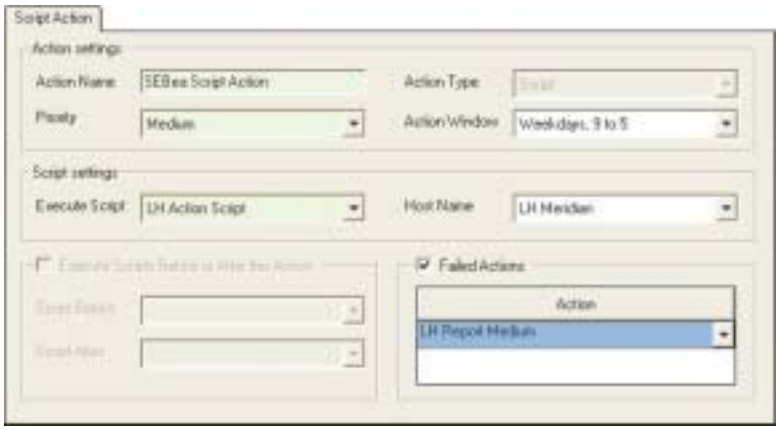


Script Action

When taking action in response to an event, you may choose to execute a Python script. For example, your PBX host device reports a T1 line error so you execute a script that attempts to re-initialize the line. Using Script Action Libraries, you can create script library records that define the actions settings and identify the script you want to execute.

To create a script action record

1 Right-click the **Script** folder and select **Add Script Action**. The system opens the Script Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Select a script from the **Execute Script** field list to execute when an event occurs. The list contains the action scripts configured for your system. For more information about creating and maintaining scripts, see ”Script’, page 6-98.

6 Select a host from the **Host Name** field list to limit your script action to a specific host.

7 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

8 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a script action fails. You cannot select the same action twice.

9 Save your record.

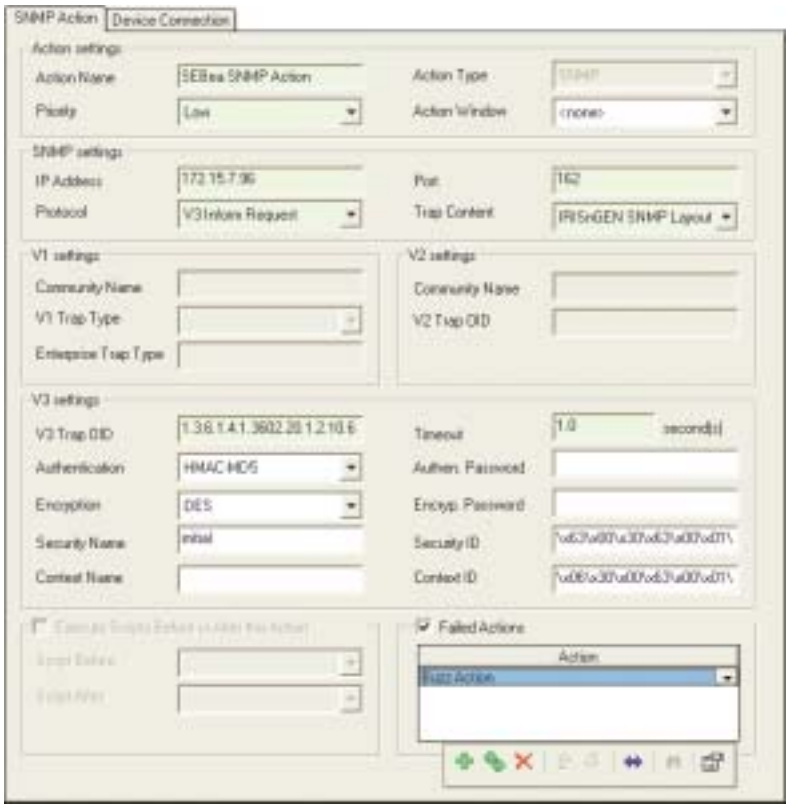
SNMP Action

Your remote agent can act as an SNMP agent sending and receiving event information from SNMP-based Network Management Systems (NMS). Using the a combination of SNMP Action libraries and SNMP Layout libraries, you can respond to events by configuring the V1 and V2 traps, and the V3, and V3 Inform Requests accepted by most SNMP-based NMS systems. You can also configure for enterprise-specific devices.

Use the SNMP Action tab to create SNMP library records that define the action, SNMP, V1, and V3 settings used to respond to an event. When you have finished with these settings, click the Device Connection tab and set the device and general connection settings used to connect to your SNMP network.

To create a SNMP action record

1 Right-click the **SNMP** folder and select **Add SNMP Action**. The system opens the SNMP Action tab.



2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Type the IP address of the TCP/IP port used to receive SNMP traps from the remote agent in the **IP Address** field.

6 Type the number of the TCP/IP port used to receive SNMP traps from the remote agent in the **Port** field. The default port is 162.



7 Select the SNMP protocol from the Protocol field list to match your network's SNMP protocol. Select V1 Trap, V2 Trap, V3 Trap, or V3 Inform Request.



Note *The protocol you select will activate the corresponding fields below.*

8 Select a layout from the **Trap Content** list. The layout defines the objects that are sent as part of the trap. This field is only used with V3 Trap or V3 Inform Request protocol.

V1 Settings

1 Select a V1 trap type from the **V1 Trap Type** list—for example, Warm Start. Each V1 trap type contains a list of pre-programmed objects that are sent to the device monitoring the SNMP traps.

2 Type the name of the V1 community in the **Community** field. The community is a security tool that identifies who can access the SNMP system. The most common community is "public."

3 If you chose *Enterprise Specific* in the V1 Trap Type field, type the trap ID for the device you are monitoring in the **Enterprise Trap Type** field. Check with your network administrator or the enterprise equipment manufacturer if you are unsure of the enterprise trap type ID.

V2 Settings

1 Type the name of the V2 community in the **Community** field. The community is a security tool that identifies who can access the SNMP system. The most common community is "public."

2 Enter the object identifier for the V2 trap in the **V2 Trap OID** field. Each manufacturer has an assigned OID. Check with the manufacturer when using.

V3 Settings

1 Enter the object identifier for the V3 trap in the **V3 Trap OID** field. V3 Inform Requests use OID 1.3.3.1.4.1.3600.2.1.1.1 when delivering events to IRISnGEN.

2 Select a protocol from the **Authentication** list to match the one used by the SNMP device receiving the trap. Select HMAC-MD5, HMAC-SHA, or None. Check with your NMS system administrator to determine which protocol the receiving device uses.

3 Type the authentication password in the **Authentication Password** field to match the password required by SNMP device receiving the trap. Check with your NMS system administrator to determine the password used, if any.

4 Select the encryption protocol from **Encryption** list to match the one used by the SNMP device receiving the trap, if any. Select DES or None.

5 Type the encryption password in the **Encryption Password** field to match the password used by the SNMP device receiving the trap. Check with your NMS administrator to determine the password used, if any.

6 Type the security name in the **Security Name** field to match the one used by the SNMP device receiving the trap. Check with your NMS system administrator to determine the name used, if any.



7 Type the security ID in the **Security ID** field if the SNMP device receiving the trap requires an ID. The security ID is a hexi-decimal representation containing the port number and IP address of the target system. Check with your NMS system administrator to determine the ID used, if any. This must match the value in the Security field when delivering events to IRISnGEN.



Note *The following shows the Security and Context IDs needed for an SEBea / NETPATH SNMP Action. The first eight octets are static information. You must include this information as it appears here. Enter the hexadecimal representation of the IP address for the trap's destination in the last four octets.*

Security ID:
\x00\x00\x00\x63\x00\x01\x00\xa2\x__\x__\x__\x__

Context ID:
\x00\x00\x00\x63\x00\x01\x00\xa1\x__\x__\x__\x__

8 Type the context name in the **Context Name** field to match the one used by the SNMP device receiving the trap. Check with your NMS system administrator to determine the name used, if any.

9 Type the context ID in the **Context ID** field if the SNMP device receiving the trap requires an ID. Check with your NMS system administrator to determine the ID used, if any. This must match the value in the Security field when delivering events to IRISnGEN.

10 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

11 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a SNMP action fails. You cannot select the same action twice.

12 Save your record.

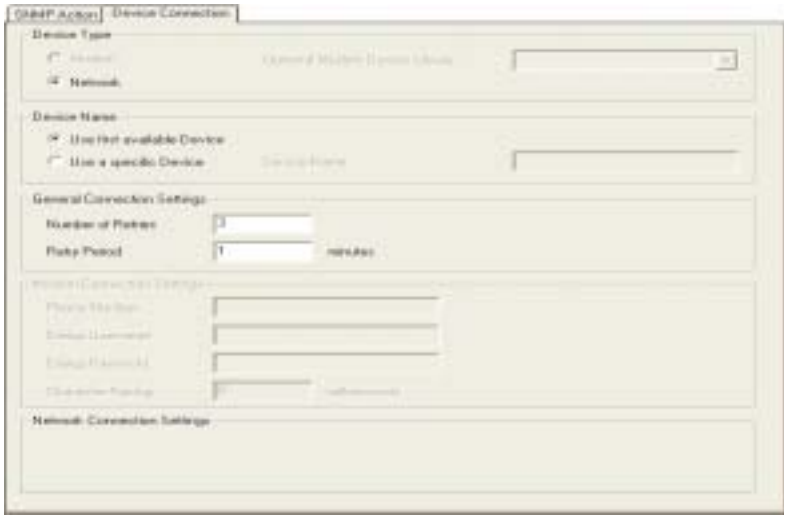


SNMP Device Connection

Use the Device Connection tab to define the SNMP settings, such as the device type, device name, and general connecting settings for your network.

To set device connection properties

1 Click the **Device Connection** tab.



2 Select the **Network** radio button to send reports via the network. This is the only option available with this release.

3 Select the Use First available Device radio button. This is the only option available with this release.

4 In the **Number of Retries** field, type the number of delivery attempts the remote agent should make before abandoning the operation and marking it “failed.”

5 Type the number of minutes the remote agent should wait between retries in the **Retry Period** field. The remote agent will wait to connect for the time specified in this field..

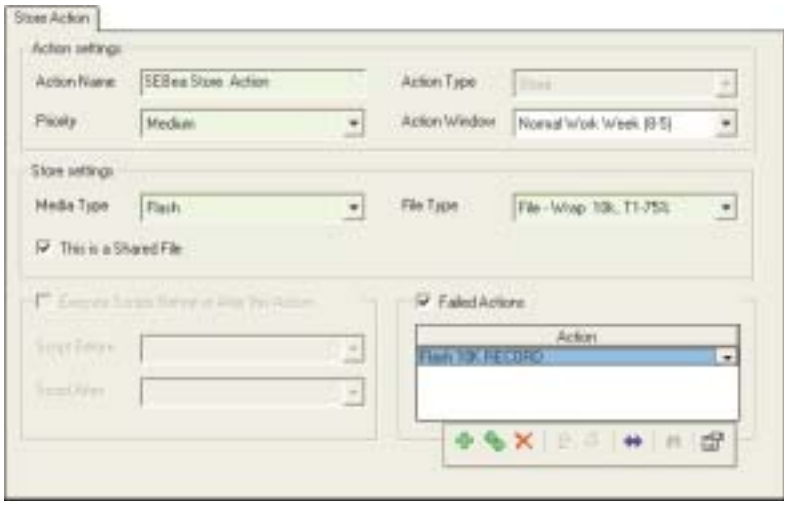
6 Save your record.

Store Action

Some events, such as minor events, may not need an immediate response, but may need to be reviewed at a later time. For these events, you can create a Store Action. Event information is stored in the remote agent database and later retrieved through polling. Use the Store Action tab to create records that defines how you want to store event data.

To create a store action record

1 Right-click the **Store** folder and select **Add Store Action**. The system opens the Store Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Select the destination to store a file from the **Media Type** list. Select:
- **Flash** – non-volatile memory, stored data is retained when you reboot the remote agent.
- **RAM** – volatile memory, stored data is deleted when you reboot the remote agent.

6 Select the type of file you want to save from the **File Type** list. A three-letter extension denotes each file type.

7 Select the **Shared File** checkbox to share the current file with two or more hosts that write to the same file. Do not check this box if you do not want to share the file.

8 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

9 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a store action fails. You cannot select the same action twice.

10 Save your record.

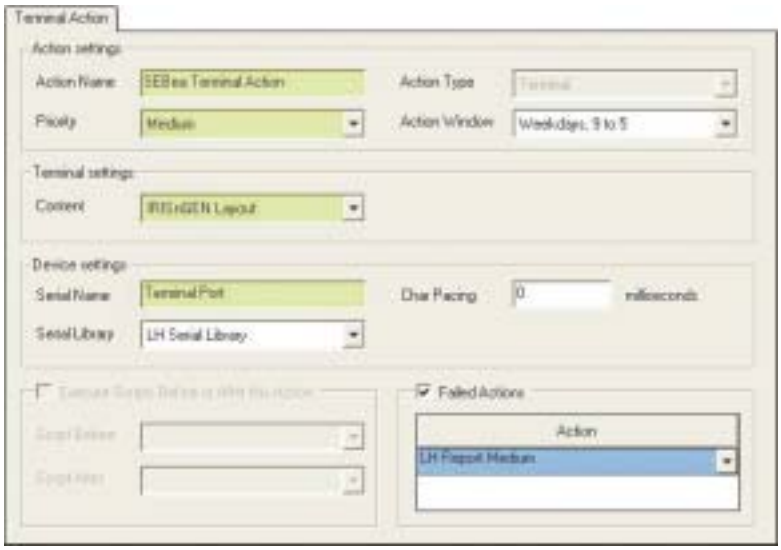


Terminal Action

When responding to an event, you may want to send some of the event data to a display terminal (via a serial port) or to a device using a terminal emulation package, such as Procomm. Use the Terminal Action tab to create library records that defines how you want to send event data to terminals.

To create a terminal action record

1 Right-click the **Terminal** folder and select **Add Terminal Action**. The system opens the Terminal Action tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Select a layout from the **Content** list to define which event information you want sent to the terminal. For more information, see ”Layouts’, page 6-93.

6 Enter the device name for the serial port you are using in the **Serial Name** field. This is the same name defined in the remote agent’s Devices & Hosts tab (see ”Devices & Hosts Tab’, page 2-32.) and in the Device Name field of the Template Library (see ”Template Libraries’, page 6-120).

7 Enter the number of seconds that the modem should pause between characters when sending data in the **Char Pacing** field.

8 Select a library from the Serial Library field list to the serial port settings. Serial libraries are defined in the Device Libraries, see ”Serial Port Device Library’, page 6-19.

9 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table.

10 Click the ✚ button to insert rows in the Actions data table; then, select an action from the list to execute when the a terminal action fails. You cannot select the same action twice.

11 Save your record.

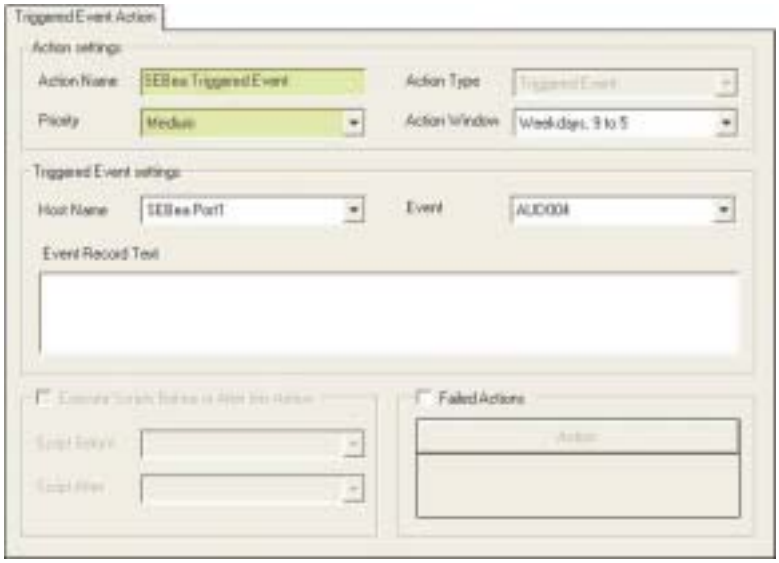
Triggered Event Action

As a response to an event or events, you may want to trigger another event. For example, if your system issues both a power-down event and a power-up event within an acceptable period, you may want to create a third event to notify you that both events occurred and that no action is needed.

Use the Triggered Event Action tab to create the Triggered Event Action library that defines the new event. The new triggered event you define will be sent through the processing engine and handled like any other event.

To create a triggered event action record

1 Right-click the **Triggered Event** folder and select **Add Triggered Event Action**. The system opens the Triggered Event tab.





Note *The Execute Scripts, Script Before, and Script After fields are not implemented in this release.*

2 Enter a unique library name for this action in the **Action Name** field. The name you enter in this field will appear in the Action fields and tabs for Correlation, Expect, Filter, and Threshold libraries.

3 Select a priority from the **Priority** list to rank the order of system actions. Select Low, Medium, High, or Top.

4 Select an action window from the **Action Window** list to set the time you want the action to start.

5 Select a host from the **Host Name** list containing a list of all the hosts defined in your system. The remote agent assigns the triggered event to this host device before processing the event.

6 Select an event from the **Event** list to use as the current triggered event. The list contains all the matched events (defined in the Event Match library).

7 Type the text that you want to send in the **Event Record Text** field. If you chose an event in the Event field, this field is unavailable.



8 Select the **Failed Actions** checkbox to specify which actions to execute should this action fail. Selecting this checkbox enables the Actions data table below.

9 Click the button to insert rows in the Actions data table; then, select an action from the list to execute when the a triggered event action fails. You cannot select the same action twice.

10 Save your record.

Action Group

Action Groups are a collection of actions that execute. You can assemble several actions into one action group, which you can assign to filters (RA Libraries/Event Libraries/Filters). Use the Action Group tab to create and maintain action groups.

To create an action group record

1 Right-click the **Action Group** folder and select **Add Action Group**. The system opens the Action Group tab.



2 Enter a group name in the **Group Name** field. The name represents the action group in the IRISnGEN system.

3 Use the **Grouped Items** data table to help you define action groups. This data table displays all the actions currently configured in the system. Each action can appear in one or more groups at the same time. The following describes the Grouped Items data table fields.

For	Do the following
Group	Select the checkbox to include this item in the action group.
Name	This read-only field displays all the configured actions in the system, by name. This field can assist you when selecting items for grouping.

4 Save your record.

Action Window Libraries

Use Action windows to program the times when the remote agent should respond to events. For example, program the window to report PBX line errors that occur during business hours, such as 9:00 A.M. to 5:00 P.M. The remote agent acts upon those events that occur between these hours and ignores those that occur at any other time.

When programming Action windows, you can include time zone and daylight saving parameters. In most cases you will want to program the time parameters for the zone in which you installed the remote agent. This allows you to share a single action library with several remote agents throughout your installed base, regardless of the time zones they are in. However, you may want to program your action window based on the IRISnGEN server's time zone. Do this when you want to base your response on event that occur during the specified action window, according to the time zone in the server location. For example, you may want to have separate actions that apply to daytime working hours versus nights and weekends.

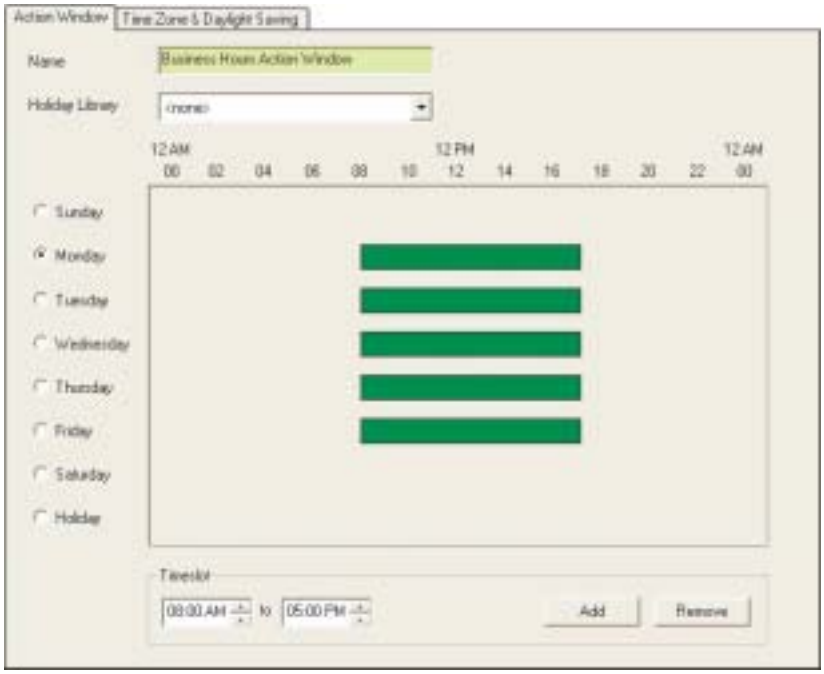
The remote agent libraries that use action windows include: Filters, Expect, Threshold, Correlation, Event Match, Scheduled Tasks, Users, and All Actions. The Action window contains two tabs, the Action Window tab and the Time Zone and Daylight Saving tab.

Action Window

Use the Action Window tab to create action windows; then set the time slot parameters for the days you want to take action.

To create and action window record

1 Right-click the **Action Window** folder and select **Add Action Window** from the drop menu. The system opens the Action Window tab.



2 This name in the **Name** field to identify its use—for example, Business Hours Action Window.

3 Select a holiday from the **Holiday Library** list to apply holiday setting to the window. Holiday records are configured in the Holiday Library, see "Holiday Libraries', page 6-92.

4 Use the **Timeslot** fields to program the start and stop times of the action window. Seconds are always applied as 00.

To add a timeslot

1. Select a weekday or holiday radio button.
2. Enter the start and stop times in the **Timeslot** fields; then, click ***Add*** to add them to the window. The valid range for hour input is 0 – 12 (or 00 – 23 in 24-hour format). The valid input range for minutes is 0 – 59.
3. Repeat steps 1 and 2 for each weekday you want to include.
4. Save your record.

Once you complete these steps, the system adds a graphical representation of the time to the Timeslot table.

When programming a time slot that spans two days, you must configure each day's segment separately. Should you happen to enter a start time that is later than the end time, IRISnGEN assumes the times are incorrect and reverses the order in the Timeslot fields when you select the Add button.

You can configure multiple time slots for a day or a holiday, but once a timeslot has an end time that is later than another timeslot's start time, the two slots merge into one timeslot. IRISnGEN then displays the merged start and end times.

To remove a timeslot

1. Select a weekday or holiday radio button.
2. Click ***Remove***.
3. Repeat steps 1 and 2 for each weekday you want to remove.

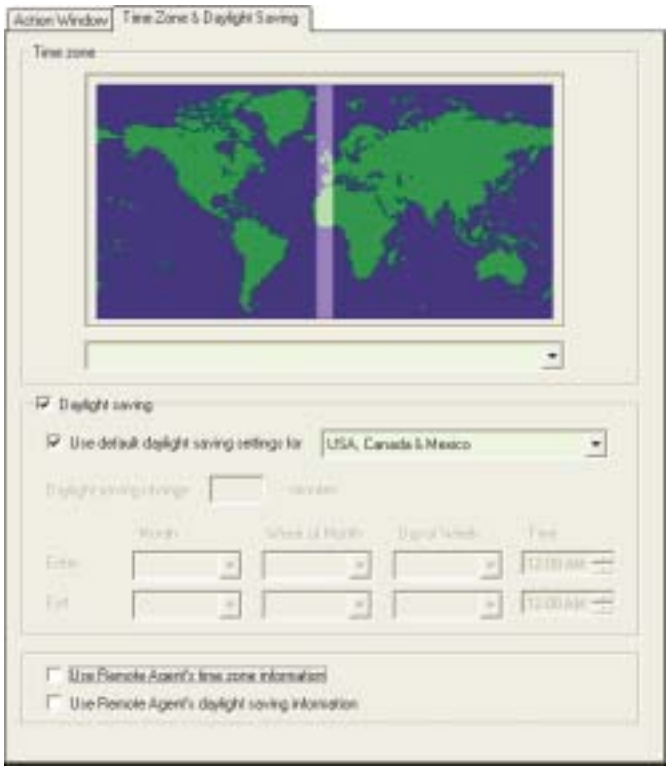


Time Zone and Daylight Saving

Use the Time Zone and Daylight Saving tab to select the appropriate time zone and daylight saving setting.

To create a time zone and daylight saving record for an action window

1 Click the **Time Zone & Daylight Saving** tab.



2 Select a time zone for the action window from the **Time Zone** list.

3 Select the **Daylight saving** checkbox to activate the day and time parameter fields. Use these fields to set the daylight saving parameters for countries that do not appear in the Time Zone list, or for countries with daylight saving times that vary from year to year.



Note *Some countries—such as South Africa—vary their daylight saving times each year. This includes the dates daylight saving begins and ends and the number of minutes to adjust. Be certain you know the country's schedule before setting daylight saving parameters.*

4 Select the **Use Default daylight saving setting for** checkbox; then, select a country from the list to add the default settings to your action window. Selecting this checkbox dims the date and time parameter fields.

5 Type the number of minutes to adjust for daylight saving (spring and fall) in the **Daylight saving change** field. The default is 60 minutes.

6 Select a month, week of month, day of week, and time from the **Enter** lists to program when daylight saving begins.

7 Select a month, week of month, day of week, and time from the **Exit** lists to program when daylight savings should end.



8 Select the **Use Remote Agent's time zone information** checkbox to use the remote agent's local time zone. If you do not select this checkbox, the system applies the time zone for the IRISnGEN server. Selecting this checkbox overrides the Time Zone field.

9 Select the **Use Remote Agent's daylight saving information** checkbox to use the daylight saving parameters configured in the site's Time Zone and Daylight Saving tab, see "Time Zone & Daylight Saving Tab', page 2-14. Selecting this checkbox overrides the daylight saving fields.

10 Save your record.

Correlation Libraries

During standard event processing, the remote agent searches for trigger words in incoming event data strings. When it finds a trigger word, it then takes action based on the parameters set in its event libraries. Correlations expand the event processing operation by searching incoming event data for sequences or patterns of multiple events.

A correlation relates two or more events or alarms. The IRISnGEN system uses correlations to take action when it receives a specific sequence of events or alarms over a defined period. For example, your remote agent detects an event but waits ten minutes to receive an event clear message. It is correlating two events; event detection and event clear, to avoid reporting an error that corrected itself. If the event clear message fails to arrive the remote agent reports the event. Other examples of correlations include event sequences that indicate a specific failure type, or event sequences that indicate the power-up process started. In either of these last two scenarios, the system takes action during the correlation process when it receives some or all of the specific events.

You can create correlation definitions based on an event expression and how the system evaluates that expression when the event occurs. One of two things can happen; the system takes one action when all events occur, or it takes a different action when all events do not occur.

A correlation activates when the system evaluates the first event and finds it meets the correlation criteria. It expires when the entire event expression is satisfied, or when the duration exceeds its allotted time before the correlation expression is satisfied. When a correlation activates, the system classifies all events that occur before and including the events that complete a correlation as intermediate events. You can process all intermediate events by assigning actions to the Intermediate Correlations Actions table.

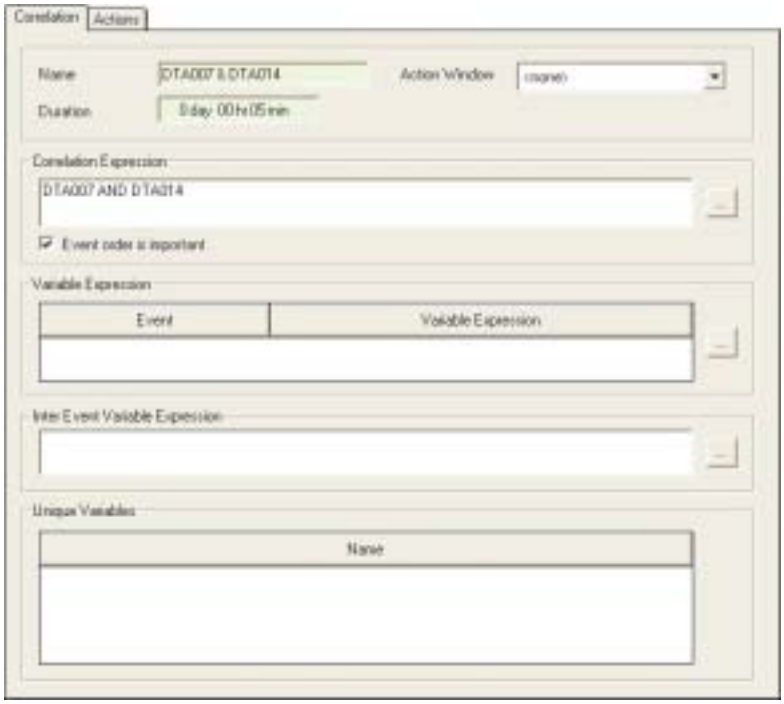


Correlation Tab

Use the Correlation tab to create event correlations. Use the tab to define the correlation expression, to qualify each event, to compare events, and/or define unique variables shared between events.

To create a correlation

1 Right-click the **Correlation** folder and select **Add Correlation**. The system opens the Correlation tab.



2 Type the name of the correlation in the **Name** field to uniquely identifies it in the system.

3 Select an action from the **Action Window** list to define the time you want the correlation to start.

4 Type the number of minutes in the **Duration** field that the correlation should remain active. The correlation begins when the system receives the first event in its correlation expression.

5 In the **Correlation Expression** field, do one of the following:

- Enter event matches and operators to create a correlation expression—for example, *(AE001 AND AE002) OR AE003*.
- Click the ... button to launch the Expression Builder dialog. Use this dialog to create your correlation expression.

You can only use the "( )", "AND", and "OR" operators in your correlation expressions.

6 Select the **Event order is important** checkbox when events must occur in the order specified in the previous field—for example, event AE001 must occur before AE002.



7 Use the **Variable Expression** table to qualify each event in the correlation expression—for example, events AE001 and AE002 must each meet certain criteria before the system will take action.

Field	Description
Event	Identify the event you want to qualify. Click anywhere inside the table **1** Click the ✚ button to insert a row into the table. **2** Click the down arrow and choose an event from the list. Notice that your only choices are those events you chose in the Correlation Expression field. **3** Continue clicking the ✚ button to insert additional rows for each event you want to qualify.
Variable Expression	Build your qualifying expression. Enter the expression into the field, or click the ... button to activate the Expression Builder dialog. For example, for event AE001, enter _DEVICE_INSTANCE = 4 and for event AE002, enter _DEVICE_INSTANCE = 15. This tells the system that each time it detects event AE001, the event must have a device instance equal to “4” and event AE002 must have a device instance equal to “15” before the system will take action, such as reporting the event.

8 Enter an expression that combines the effects of two or more events in the **Inter Event Variable Expression** field. For example,

AE001: _DEVICE_INSTANCE > = AE002: DEVICE_INSTANCE.

In the example above, the system verifies that the device instance for event AE001 is greater or equal to the device instance for AE002. If it is, then the system will take action. If not, the system will not take action.

9 Enter variables that apply to all events specified in the correlation expression in the **Unique Variable** field. For example,

_DEVICE_NAME.

Each variable you choose must appear in all the events listed in the Correlation Expression field; otherwise, the expression is invalid and the system will not take action. For example, if we choose the unique variable _DEVICE_NAME, then it must be defined for event AE001, AE002, and AE003, which were listed in the Correlation Expression field.

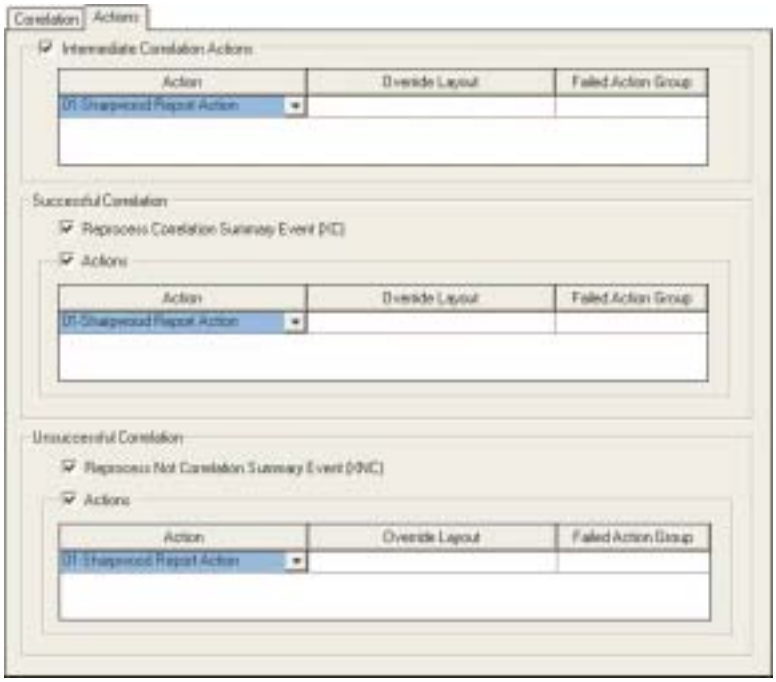


Correlation Actions

The Actions tab lets you define what actions the system should take during each stage of the correlation. The tab includes three tables, Intermediate Correlation Actions, Successful Correlation, and Unsuccessful Correlation. Use the Intermediate Correlation Actions table to define the actions needed to process information as event sequences unfold. Use the Successful Correlation table to define what to do when the correlation is successful. Finally, use the Unsuccessful Correlation table to define what actions the system should take when a correlation fails.

To add a correlation action

1 Click the **Actions** tab, shown below.



2 Select the **Intermediate Correlation Actions** checkbox to activate the Intermediate Correlation data table.

3 Select an action from the **Action** list. You cannot select the same action twice.

4 Select a layout for the action selected in the previous field from the **Override Layout** list. If the action you selected in the previous field already has its own layout, this layout will override it. If you do not select a layout in this field, the system will use the layout already defined for the action, if any.

When you select an action that does not require a layout—for example, a Relay Action—the system ignores this entry. You can select and associate any layout with actions any number of times.

5 Select an action from the **Failed Action Group** list. You cannot select the same action twice. When the action you selected in the Action field already has a failed action defined for it, the system overrides it with the failed action you choose in this field. If you do not select a failed action, the system uses the failed action previously defined for the action.

6 Select the **Reprocess Correlation Summary (XC)** checkbox to perform additional event matching on the XC event.

7 Select the **Actions** checkbox to activate the Successful Correlation data table.

8 Repeat steps 3 through 5 for the Successful Correlation.

9 Select the **Reprocess Not Correlation Summary (XNC)** checkbox to perform additional event matching on the XNC event.



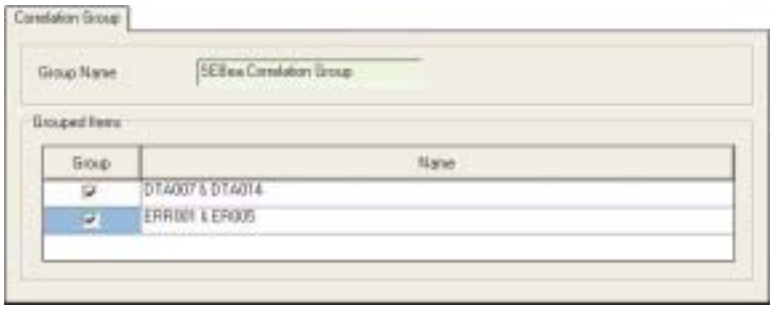
10 Select the **Actions** checkbox to activate the Successful Correlation data table.
11 Repeat steps 3 through 5 for the Unsuccessful Correlation.
12 Save your Actions record.

Correlation Groups

When assigning correlations to remote agents, you can speed the process by creating correlation groups. Correlation groups are a collection of correlation records.

To add a correlation group

1 Right-click the **Correlation Group** folder and select **Add Correlation Group** from the drop menu. The system opens the Correlation Group tab.



2 Type the name of the correlation group in the **Group Name** field.
3 Use the Grouped Items data table to define your correlation groups. The data table displays all the correlations currently configured in the system. You can compose a correlation group by selecting one or more available correlations. Each correlation can appear in one or more groups at the same time. The following describes the Group Items data table fields.

For	Do the following
Group	Select the checkbox to include this item in the correlation group.
Name	This read-only field displays all the configured correlations in the system, by name. This field can assist you when selecting items for grouping.

4 Save your record.

Event Detection Libraries

Event detection is the process used to group serial data into logical records. As the remote agent receives streams of unprocessed serial data from the host device, it groups the data into logical records from which it can later extract event information. Event detection processed data in three steps:

- Pre-Processing
- Record Detection
- Post-Processing

During the Pre-Processing step, the remote agent receives serial data from the host device. The data can arrive as unsolicited input, or the remote agent can retrieve it using a port control script. The script communicates directly with the host and fully controls the data received through the remote agent's port. The data is then conditioned using either the Find and Replace or the Execute Script function. Find and Replace removes or changes various data characters. For example, the data may has embedded NULL characters that are removed using Find and Replace to speed processing. In cases in which the data requires manipulation beyond the capabilities of Find and Replace, you can add a special pre-process script using the Execute Script function.

Within the Record Detection step, the remote agent groups the data into logical records. The remote agent applies one of three user-defined methods to group the data: markers, length, or timeout. Markers group data by distinguishable beginning and/or ending character sequences, such as CR/LF (carriage return/line feed). Length groups data by a minimum and maximum number of characters. Data lengths not meeting this minimum and maximum are discarded, if specified. Timeout groups records based on the amount of idle time between characters received. For example, the host device sends a stream of serial data, pauses for three seconds, then send another stream of data. The remote agent looks for this pause; then, groups the data between pauses into a logical record.

With the data grouped into logical records, it then passes through the Post-Processing step. Post-Processing is occurs when selected characters used in the record definition must be altered in the logical record (remove or replace characters) before the logical record moves to the event matching stage. For example, assume the serial data received from the host is line-oriented text terminating with a single line feed and you defined the Record Detector step to use the line feed as the EOL character. With the data now logically grouped, you determine that the line termination be a carriage return followed by a line feed. Use the Post-Processing step to enable scripts that alter the data, or to reformat it before sending for event matching.

Use the Event Detection Library to create the event detection records that group the incoming bytes of data into logical records. Once created, you can assign the library records to the Host libraries (Remote Agent Libraries > Host Libraries).

The Event Detection Library contains three tabs, Record Definition, Pre-Processing, and Post-Processing. Notice that the Record Definition tab appears first, since it is the one used most often with event detection. However, you do not need to define the parameters on this tab first. You can define the parameters on the Pre-Processing or Post-Processing tab first, if you choose.



Record Definition

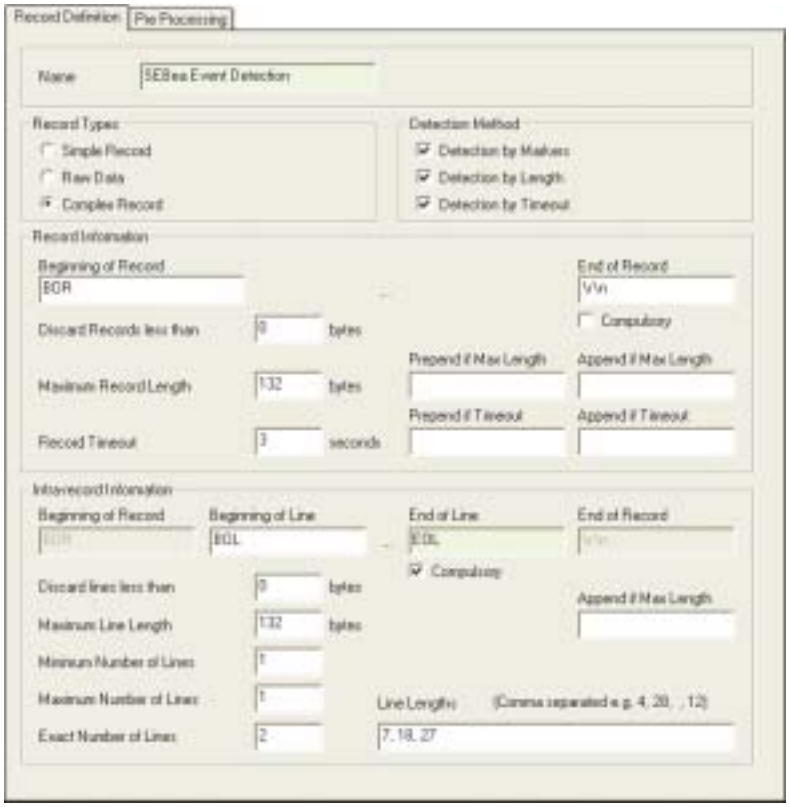
Use the Record Definition tab to create and maintain the record definition for an event detection library. You can create an event detection library or you can edit an existing event detection library by selecting the desired event detection library from the Event Detections folder. This invokes the Record Definition tab and populates it with the selected library's details. Once displayed, you can edit the fields. A sample of the Record Definition tab appears below. Access to this tab and the fields contained within, will be controlled through the IRIS security system.

Each event detection definition requires a unique name, which you can define on the Record Definition tab. You can manage the Record Definition page by selecting one of three record definition types: Simple Record, Raw Data, and Complex Record. Each of these record definition types handles selected elements on the Record Definition tab. The default record definition type is Simple Record, the most common record type.

Each of the record definition types offers three processing features that manage the event detection process. These processing features are known as detection methods and include markers, length, and timeout. The system activates certain fields, depending on the record type and detection method you choose. For example, choosing Simple Record type and Detection by Markers method activates only the Beginning of Record and End of Record fields in the Record Information area. Choosing Complex Record type and all three detection methods activates all the fields on the tab.

To create a record definition record

1 Right-click the **Event Detections** folder, and then select the **Add Event Detection** from the drop menu. The system opens the Event Detections tab.



2 Type a name to identify the record definition in **Name** field.

3 Select the radio button for your record type.

Button	What it does
Simple Record	A simple record contains event record markers and event data. The event markers are unique character sequences that identify where a record starts or ends. Selecting the Simple Record definition type enables the field options contained in the Record Information section. The Record Information input fields enabled are also base on the detection method. A simple record definition can have four possible record formats. Example 1 does not have BOR or EOR markers. You can detect this event data using record length and/or record timeout. This is the same as the Raw Data record definition.  Example 1 Example 2 represents the most common simple record format. A single record data ends with the EOR character sequence (typically carriage return and line feed characters 0X0D and 0X0A). Length and timeout definitions further qualifies this type.  Example 2 Example 3 is similar to the second record; however, the distinguishing marker is at the beginning of the record. Length and timeout definitions can further qualify this type of data.  Example 3 Example 4 shows a block of data that has unique markers (BOR and EOR) at both ends. Length and timeout definitions can further qualify this type of data.  Example 4

Raw Data	Raw data records support event processing for data input that does not have markers to identify the logical beginning and/or end of a record. This differs from the simple record type because the marker detection method is not available for raw data records. However, all remaining processing options are the same as those used for a simple record. Setup recommendations include defining a maximum record length of at least 132 characters and a record timeout of three seconds. This allows you to group input characters before sending them to the next stage. By doing so, you will improve processing efficiency.
Complex Record	Complex record definitions support the processing of records that have multiple lines within an event record. To be a complex record, data must have unique BOR and/or EOR markers and unique beginning-of-line (BOL) and/or end-of-line (EOL) markers. The Markers detection method is permanently selected when you choose the complex record type. All of the input fields are available when you select a complex record type. The record information section manages all record boundaries, the same as it does for the other two record types. The intra-record information section manages the intra-record lines. A complex record definition does not support line timeout parameters. When an input data timeout occurs, the record timeout processing applies, as programmed.

4 Select the checkbox for your detection method.



Note *You must choose a definition method option for the record type selected in the previous field. If you do not choose a Detection Method option, the remote agent cannot detect events during normal event processing. However, you do not need to choose a detection method if you are using an event detection to initiate a port control script.*



Button	What it does
Detection by Markers	Select Markers when the incoming data is well defined and has distinguishable beginning and/or ending character sequences. Selecting Markers activates the fields used to define and manage markers. Selecting this option in conjunction with a complex record type also activates the Inter-Record Information fields that you can use to specify line boundaries within a record. This option is not available when you select the Raw Data record type. ***Warning*** *Be careful when only choosing this option. If you only choose this option and no other, the system only looks for markers and does not look for record information and/or intra-record information, even if you checked the Compulsory box for each. If the system does not detect a marker, the data does not become a record and the remote agent takes no action. This may cause the remote agent's memory to fill and the device to reboot.*
Detection by Length	Use this option with the **Discard records less than field** to define a minimum record length. If a record is less than the one specified. The overall event record length includes all markers, including markers that were prepended or appended. The system tests for minimum length before sending the record for event matching. The system uses the maximum record length to define a maximum limit for an event record length. It then checks it as the event detector gathers characters for a completed event record. When this value is reached, the Event Detector collects all the data (to this point) to be a valid event record and passes the event to the next stage. You can prepend BOR and/or append EOR characters to this event when the maximum length is reached. Exceeding the maximum length is an abnormal circumstance. By adding BOR and EOR characters, the remote agent normalizes this record for further processing. The maximum length is also a safeguard that prevents data from building in the Event Detector stage when the system does not receive defined markers as expected. We recommend that you always define a maximum length, even for records without markers.



Detection by Timeout	Select this checkbox when the idle time (in seconds) occurs between input characters. When the time expires, all data collected to that point is a record. You have the option to prepend BOR characters and/or append EOR characters tot he collected data. Usually, a host will transmit entire event records to the remote agent. The record timeout prevents the system from holding data too long after host input stops and the data collected up to that point has not satisfied the record definition. Although this field is not mandatory, we strongly recommend that you use it.

5 Enter the character parameters for the record in the **Record Information** fields.

Field	What to enter
Beginning of Record (BOR)	Type a character or character sequence to identify the beginning of a record (BOR). The BOR must be unique from the content of the event and any other markers. This field becomes available when you select the markers detection method. The maximum length is 256 characters. This field will accept any of the following as input: • Any single ASCII character • Any multi-length text string • Special characters appear as follows. Special Character — Character Description \a — Bell \b — Backspace \f — Form Feed \n — New Line \r — Carriage Return \t — Horizontal Tab \v — Vertical Tab \? — Literal Quotation Mark \" — Double Quotation Mark \\ — Backslash \0 — Null \x — Hexadecimal value

End of Record (EOR)	Type a character or specific character sequence to define the end of a record (EOR). The maximum number of characters is 256. The EOR must be unique from the content of the event and any other markers. You can enter any of the inputs described for the beginning of record. The default for simple and complex record types is **\r\n**, which represents the carriage return and line feed characters. This field activates when you select the Detection by Markers checkbox. It is a required field when you select the Compulsory checkbox.
Compulsory Flag (EOR)	Select this checkbox to indicate the EOR character(s) must have a valid detection. Be careful when using this option. The system does not have an upper limit defined for the size of an event record. If you checked a compulsory option, the system considers the detection valid only if it also detects the specified EOR. As a result, event data collected to this point could use all available system memory. Use the Maximum Record Length and Timeout features to prevent an overrun condition. This field activates when you select the Detection by Marker checkbox.
Discard Records Less Than	Type the minimum length required for a record to be valid. If a record does not meet the specified length, the system discards it. The overall event record length includes all markers, including markers prepended or appended in the Event Detector stage. The system tests for minimum length prior to sending a detected event to the next stage. Valid lengths range from 1 – 9,999. You may not enter a value in this field that is greater than the value defined for the maximum record length. The default minimum is “0,” which disables this feature. A blank character also disables this feature. This field activates when you select the Detection by Length checkbox.



Maximum Record Length	Type the maximum number of characters expected for any event record. When the number of characters collected reaches this value, the event detector considers the data collected up to that point to be a valid event record; then, passes the event to the next stage. You have the option to prepend and/or append characters to this event when it reaches the maximum length. The recommended value for this field should always be greater than the largest event record that you expect to process. For example, a host produces event records that will reach a maximum of 132 characters (including markers). The maximum record length value should be set at 133 or higher. Valid lengths range from 1 – 9,999. The default is 132. The “0” character or a blank character disables this feature. This field activates when you select the Detection by Length checkbox.
Prepend If Maximum Length	Type the characters that prepend to a record when the system reaches the maximum record length (if specified) for the current record. This normalizes data when line length errors occur. Use any of the inputs described for BOR. This field activates when you select the Detection by Length checkbox.
Append If Maximum Length	Type the characters that append to a record when the system reaches the maximum record length (if specified) of the current record. This normalizes data when line length errors occur. Use any of the inputs described for BOR. This field activates when you select the Detection by Length checkbox.
Record Timeout	Type the idle time (in seconds) that can occur between input characters. When the idle time expires, the system marks any data collected up to that point as a record. This prevents the system from holding data too long in the event detection stage. You can prepend characters and/or append characters to the data collected. You can enter integer values from 1-3600. The “0” character disables this feature. The default is 3 seconds. This field activates when you select the Detection by Timeout checkbox.



Prepend If Timeout	Type the characters that the system prepends to a record when a record timeout (if specified) occurs. This normalizes data when a timeout error occurs. Enter any of the inputs described for BOR. This field activates when you select the Detection by Length checkbox.
Append If Timeout	Type the characters that the system appends to a record when a record timeout (if specified) occurs. This normalizes data when a timeout error occurs. Enter any of the inputs described for BOR. This field activates when you select the Detection by Length checkbox.

6 Enter the line parameters for the record in the **Intra-Record Information** fields.

Field	What to enter
Beginning of Line	Type a character or a character sequence to define the beginning of a line (BOL). The BOL must be unique from the content of the event and any other markers. Use any input as described for the BOR. The maximum number of characters for this is 256. This field activates when you select the Detection by Markers checkbox.
End of Line	Type a character or character sequence that defines the end of a line (EOL). The maximum number of characters is 256. This field activates when you select the Detection by Marker checkbox.
Compulsory Flag (End of Line)	Select this checkbox when the EOL character(s) requires valid detection. Be careful when using this option since the system does not have an upper limit defined for the size of an event record. The system marks the detection valid only if it also detects the specified EOL. This could result in the event data consuming all available system memory. To prevent this overrun, set the Maximum Record Length and Timeout features. This checkbox activates when you select the Complex Record radio button. ***Note*** *There is no separate timeout for the line gathering process, so the record timeout applies to this process. When a timeout occurs, the system regards it as a record timeout.*



Discard Lines Less Than	Type the minimum length required for a line to be valid. If a record does not meet the specified length, the system discards it. The overall event line length includes all markers, including the marker appended in the Event Detector stage. The system tests for minimum length before adding the line to an event record that is building in the event detector. Valid lengths range from 1 to 9,999. The default minimum is “0,” which disables this feature. This field activates when you select the Complex Record radio button.
Maximum Line Length	Type the maximum number of characters expected for any complex record line. When the number of characters collected reaches this value, the event detector marks the line data collected up to this point as a valid line and adds it to the event record. You can append characters to this line when the system reaches the maximum line length. The recommended value for this field should always be greater than the longest line size that you expect to process. For example, a host produces event records with lines that have a maximum of 132 characters (including markers). Here you would set the maximum record length value to 133, or higher. Valid length ranges are from 1 to 9,999. A “0” disables this field. The default is 132. This field activates when you select the Complex Record radio button.
Minimum Number of Lines	Type the minimum number of lines the system should receive to be a valid record. When the a record that does not contain the specified number of lines, the system discards it.
Maximum Number of Lines	Type the maximum number of lines the system should receive to be a valid record. When the record contains more than the specified number of lines, then the system discards it.
Exact Number of Lines	Type the specific record formats containing an exact number of lines. When the number of lines is not known, this field is left in its default state (empty). Use only integer values when specifying the actual number of lines the record should contain.



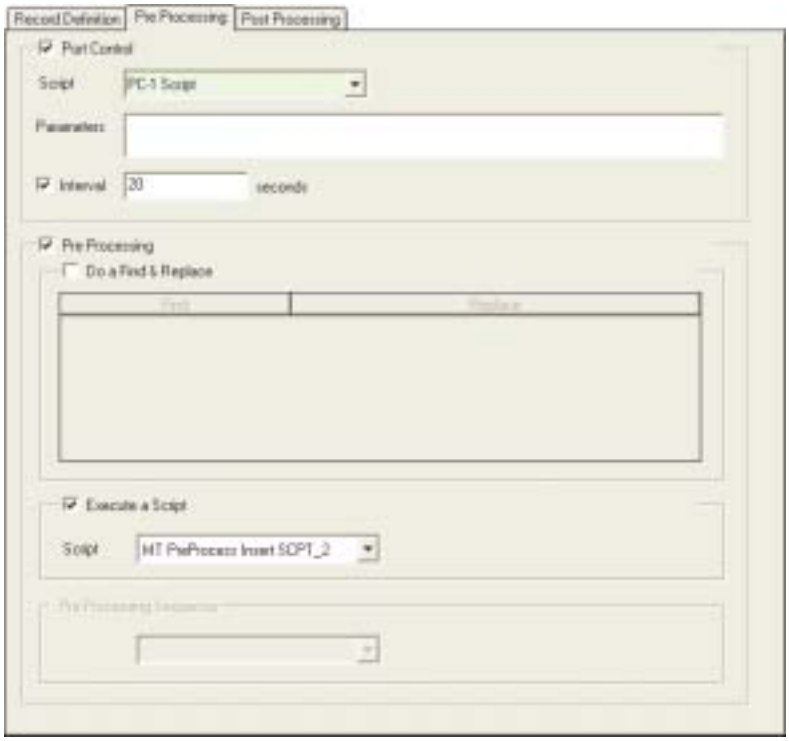
Append If Max Length	Type the characters that append to a line when the system reaches the maximum line length (if specified) for the current line. This normalizes data when line length errors occur. Use any of the inputs as described for BOR. This field activates when you select the Complex Record radio button.
Line Lengths	Type the lengths of all the lines previously specified and detected in the record. The entries (line lengths) are integers separated by commas—for example, 24,32,4,54,32 represents five lines with varying line lengths. Use this option with the Exact Number of Lines option to further define an exact record format.

Pre-Processing

Pre-Processing provided several options for manipulating incoming data before it is analyzed and grouped into logical records. The Pre-Processing tab is available for all event detection records. Use this tab to configure all pre-processing options.

To set the pre-processing parameters

1 Click the **Pre-Processing** tab.



2 Select the **Port Control** checkbox to enable script control; then, select a script from the Script list.

3 Select the **Pre-Processing** checkbox to manipulate incoming data before the system analyzes and groups it into event records.

4 Select the **Do a Find & Replace** checkbox to activate the data table. Once active, type the characters you wish to find and replace in the table fields. You can enter any of the following:

- Any single ASCII character
- Any multi-length text string up to 256 characters
- Certain special characters, preceded with a "\", as follows:

Special Character	Character Description
\a	Bell
\b	Backspace
\f	Form Feed
\n	New Line
\r	Carriage Return
\t	Horizontal Tab
\v	Vertical Tab
\?	Literal Quotation Mark
\"	Double Quotation Mark
\\	Backslash
\0	Null
\x	Hexadecimal value

You can also use this field to find any item you wish to delete. Type a value in the **Find** field; then, leave the **Replace** field empty. The system will find the desired item and delete it.

5 Select the **Execute a Script** checkbox to enable scripts; then, select a script from the **Scripts** list.

6 Select the pre-processing sequence to define the order that the Find & Replace and Scripts execute from the **Pre-Processing Sequence** list. Select one of the following:

- Find & Replace, Script
- Script, Find & Replace



Post-Processing

The Post-Processing tab is available for all event detection records. Use tab to configure all post-processing requirements. By default, all post-processing options are disabled for new event detections records.

To set the post-processing parameter

1 Click the **Post-Processing** tab.



2 Select the **Post-Processing** checkbox to handle event record data after the system detects it and before it is sent to the next state in the event processor.

3 Select the **Do a Find & Replace** checkbox to activate the data table. Once active, type the characters you wish to find and replace in the table fields. You can enter any of the following:

- Any single ASCII character
- Any multi-length text string up to 256 characters
- Certain special characters, preceded with a "\", as follows:

Special Character	Character Description
\a	Bell
\b	Backspace
\f	Form Feed
\n	New Line
\r	Carriage Return
\t	Horizontal Tab
\v	Vertical Tab
\?	Literal Quotation Mark
\"	Double Quotation Mark
\\	Backslash
\0	Null
\x	Hexadecimal value

You can also use this field to find any item you wish to delete. Type a value in the Find field; then, leave the Replace field empty. The system will find the desired item and delete it.

4 Select the **Execute a Script** checkbox to enable scripts; then, select a script from the Scripts list.

5 Select the post-processing sequence to define the order that the Find & Replace and scripts execute from the **Post-Processing Sequence** list. Select one of the following:

- Find & Replace, Script
- Script, Find & Replace

Event Detection Groups

It is possible to configure and assign more than one event detection definition to specific remote agent devices. This allows the remote agent to process many different data patterns from the same physical device. Use the Event Detection Groups option to create and maintain groups of event detection records.

To create an event detection group record

1 Right-click the **Event Detection Groups** folder and select **Add Event Detection Group**. the system opens the Event Detection Group tab containing all the event detection libraries defined for the system.



2 Type the name of the event detection group in the **Group Name** field.

3 Use the **Grouped Items** data table to assist to create an event detection group. The data table displays all the event detection libraries currently configured in the system. Create an event detection group by selecting one or more of the available event detection libraries. Once grouped and saved, the selected items appear in the list in alphabetical order. Any event detection library can be a member of one or more groups. The data table includes the following fields:

Field	What to enter
Group	Select the checkbox for each library you want to include in the group.
Name	This read-only field lists all the configured event detection libraries in the system. It does not require any input and is only there to assist you in the selection process.

Event Matches

Event Match is the second stage of the Event Manager. Detected events pass to the Event Match stage from the Event Detector stage. Event matching is required for unknown events—for example, serial data events—when the contents must be analyzed before the system can make any event processing decisions.

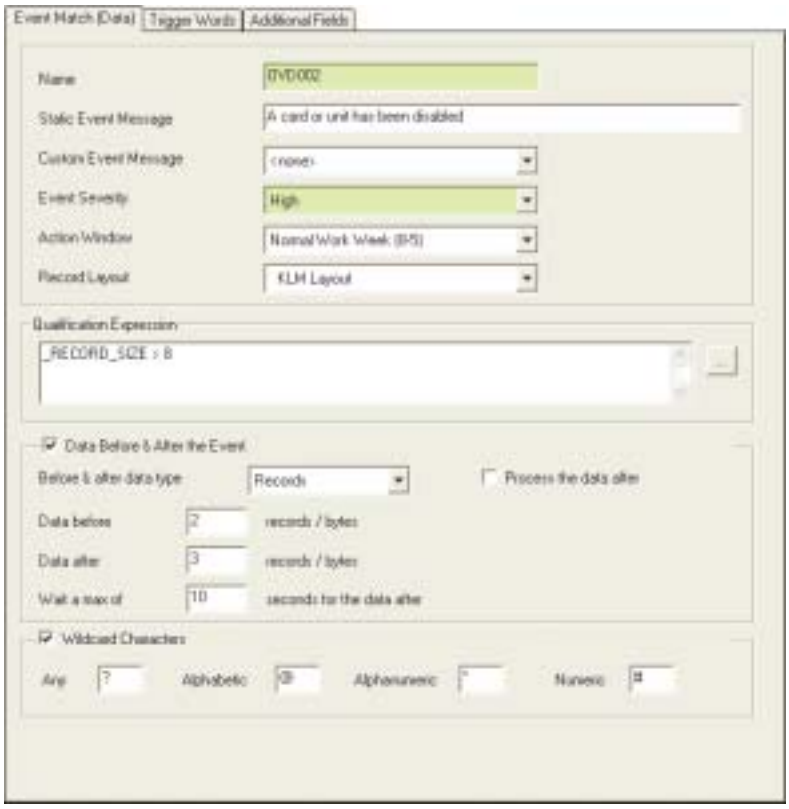
When working with event match records, note that the order of event delivery is not the same as the input order, but rather the order of output. When there are multiple alarms in a record, IRISnGEN searches the record for event matches in the order the event matches are listed in the database.

Event Match (Data) Tab

Use the Event Match (Data) tab to create and maintain each event match definition. You can create event match records for data, SNMP, and fixed events.

To create an event match (data) record

1 Right-click the **Event Matches** folder and select **Add Event Match (Data)** from the drop menu. The system opens the Event Match (Data) tab.



2 Type the name of the data event match record in the **Name** field.

3 Type a description of the event in the **Static Event Message** field. Each event match supports one static message entry. The system stores this information as a system variable with the event and is available when defining event-processing layouts.

4 From the **Custom Event Message** list, select a layout that contains the components needed to configure a custom event message that includes event variable data. When the remote agent finds a match, it formats the event based on the layout. The message is added as a system variable.

5 Select a severity for each event match from the **Event Severity** list. Select Low, Medium, or High.



The system adds the severity information to the event as a system variable. Later, you can use this information as part of an expression when determining what actions to take. For example, you can later define a filter to deliver all events with a high severity to the IRISnGEN system.

6 Select an action window to define the time you want to use the associated event match from the **Action Window** list. Leave this field blank if you do not wish to specify a time.

7 Select a layout from the **Record Layout** list. The layout determines the format of the event record.

8 Type an expression to eliminate unwanted events before parsing, or to refine further an event match definition, in the **Qualification Expression** field, or click the ... button to display the Expression Builder dialog box.

9 Select the **Data Before and After the Event** checkbox to attach secondary information to a specific event. Secondary information can help you when diagnosing a problem. It provides bytes or records before and after the specified event. You can also use this field to append additional data to an event that belongs to the matched event.

10 Select the type of data you want to append to the event from the **Before and After Data Type** list. Select Bytes or Records.

11 Type an integer value that represent the exact number of bytes or records that you want to add before the current event record in the **Data Before** field. The system includes any data available up to the number entered in this field.

12 Type an integer values that represent the exact number of bytes or records that you want to add after the current event record in the **Data After** field. The system includes any data available up to the number defined in this field.

13 Select the **Process the data after** checkbox to add data and processed as an independent event. When using a Data After definition, bytes or records collected may or may not be independent events that warrant additional processing.

14 Type the number of seconds that the remote agent should wait for data associated with the Data After option in the **Wait seconds for data after** field. If time expires before the system can collect the number of records or bytes specified; then, the data collected up to that point appends to the event record.

15 Select the Wildcard Characters checkbox to enable wildcards; then, type a wildcard set for each event match.

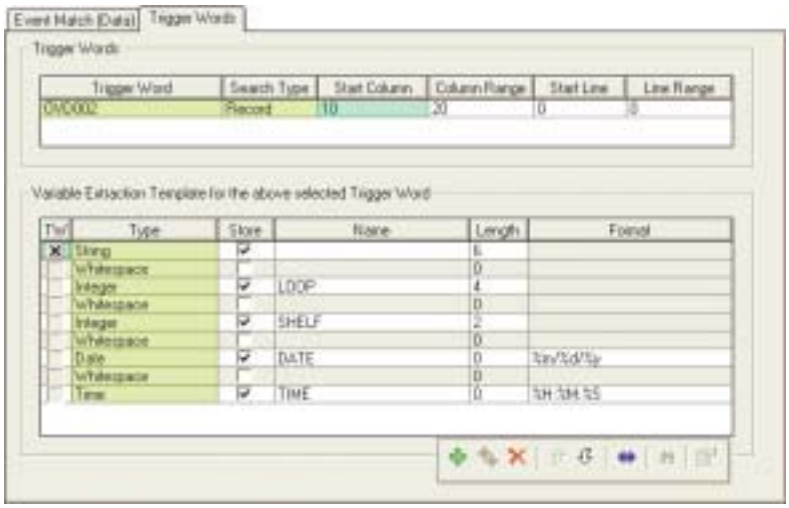
Wildcard Type	Description	Default Character
Any	This input specifies any printable character, or any hex notation 0X00 – 0XFF	?
Alphabetic	This input specifies the alphabetic wildcard character, **A** to **Z** and **a** to **z**.	@
Alphanumeric	This input specifies any alphabetic and numeric character **A** to **Z, a** to **z**., **0** to **9**, or any hex notation **20** – **7F**	*
Numeric	This input specifies any number (**0** to **9**)	#

Trigger Words Tab

The Trigger Word tab contains Trigger Words and Variable Extraction data tables. The Trigger Words data table displays at the top of the tab. The Variable Extraction data table displays in the lower portion of the tab and is associated with the trigger word highlighted in the Trigger Word data table. You can edit both data tables using the same editing convention found in the other IRISnGEN tables. Use the mini toolbar to add new entries. To display the mini toolbar, left-click the mouse button while its pointer is inside the table. You can select existing entries by clicking the mouse button.

To create a trigger word record

1 Click the **Trigger Word** tab.



2 Click inside the **Trigger Word** table; then, click the button to a insert row.

3 Type the trigger word text string in the **Trigger Word** field. The trigger word can contain the NULL character. It can also contain any of the wildcards defined on the Event Match tab.

4 Select a search type for the event data from the **Search Type** list. Select one of the following:

- **Line** to search complex records, as defined in the Event Detection tab.
- **Record** to search all other types of records.

5 Type the exact column position where a trigger word search starts in the Column Position field. Enter **1** to begin searching from the first character in the record/line. Enter **0** to search the entire record.

6 Type the number of columns to search in the **Column Range** field. The system begins searching at the column specified in the Column Position field. Enter **1** to search only the column specified in the Column Position field. Enter **0** to search all columns after the one specified in the Column Position field.

7 Type the line position where a trigger word search starts in the Line Position field. Enter **1** to begin searching in the first line of the record. Enter **0** to search all lines.

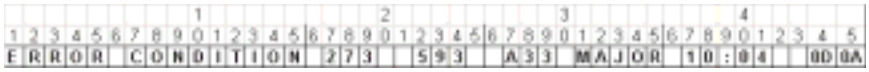
8 Type the number of lines to search in the Line Range field. The system begins searching with the line specified in the Line Position field. Enter **1** to search only the line specified in the Line Position field. Enter **0** to search all lines in the record.



Sample Trigger Words

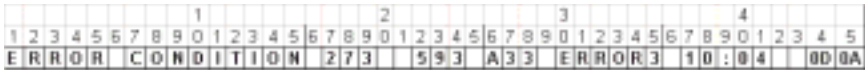
Example 1

This example shows a simple event record containing an EOR marker. The two rows above the event text show character positions. Assume you are using a Record search type.



Suppose the trigger word text is “MAJOR,” the column position is “0,” and the column range is blank. The search finds the phrase “MAJOR” at character position “31.” If you know that all trigger words begin at position “31,” it is more efficient to define a start column of “31.”

Example 2



Here, we modified the event text to show how it is more efficient to use column searches based on the data content. The figure shows two occurrences of the word “ERROR.” If the second occurrence is the one we are looking for, it is better to define an exact column position, or a general region where we expect to find the text. We can specify a region by leaving the Column Position value at “0” (search the entire record) and specify a value in the Column Range field. In this example, something like 29 to 40 will work.

Example 3

The most complicated scenario is a multi-line record (a complex record definition). The main reason for offering column range searching is based on the overall size of a record. It is more efficient to search in specific column ranges for a record that containing 10,000 bytes rather than to search from the first character to the last character in the record.

Variable Extraction Table

The Variable Extraction table is located at the bottom of the Trigger Word tab. Use this table to find data within an event record and to add this data to an event as a user variable.The table provides navigation information used to select data contained in the event record. The navigation information is based on the relative position of the defined trigger word, so this table requires that you create a trigger word before defining a table. The system only uses this table when the associated trigger word is found in the event. The success of a defined event match does not depend on the success of finding available data.

To add a variable extraction

1. Select the trigger word from the Trigger Word table; then, click inside the Variable Extraction table. The mini toolbar appears to help you with your tasks.
2. Select the **TW** checkbox for the table entry you wish to assign to the trigger word above. The entry is the trigger word. Each Variable Extraction template must have a trigger word. The trigger word can be anywhere in the list depending on the data you are trying to extract occurs before or after the trigger word. You can check only one trigger word in the Variable Extraction template.

3 Select a type from the **Type** list to define an event variable in the event record, which you will search for. For example, select String if the system will be searching for a string of characters, or select Integer if the system will be searching for a series of numbers.

4 Select the **Store** checkbox to store the entry as an event record variable. The system adds both the variable name and the value it represents to the event record. You can later use the variable name in expressions and layouts.

5 Type a name for the variables in the **Name** field. The system stores this name as a user name variable, along with the variable values it represents, when you select the Store checkbox. The name can be used in later event processing. For example, suppose you want the system to search for a string of variables that represent loop data in your PBX. Name the variables "Loop." The system adds this name to the event record, which can be used in future event processing, or when using the Expression Builder with correlations, expects, filters, and thresholds.

6 Type the length of the variable in the **Length** field. if known. If you do not know the exact length, enter **0**, the default value. If you use the default value, you can still use other options to assist with matching and/or the extraction of the variables, such as configuring static text or floating text that occurs before or after the variable.

7 Enter the format of the date and time in the **Format** field. For example, you should format the date *14 October 2000* as *%d %B %Y* (note the spaces). Specify the date *14/10/00* as *%d/%m/%y* (note the slash characters "/"). Use the following formats.

Format	What it means
%a	Abbreviated weekday name (Mon for Monday)
%A	Full weekday name (Monday)
%b	Abbreviated month name (Feb for February)
%B	Full month name (February)
%d	Day of month as decimal number (01 – 31)
%H	Hour in 24-hour format (00 – 23)
%I	Hour in 12-hour format (01 – 12)
%j	Day of year as decimal number (001 – 366)
%m	Month as decimal number (01 – 12)
%M	Minute as decimal number (00 – 59)
%p	Current locale's AM/PM indicator for 12-hour clock
%S	Second as decimal number (00 – 59)
%U	Week of year as decimal number (00 – 53). Sunday is the first day of the week.
%w	Weekday as decimal number (0 – 6; Sunday is 0)
%W	Week of year as decimal number (00 – 53). Monday is the first day of the week.
%x	Date representation for current locale
%X	Time representation for current locale



%y	Year without century, as decimal number (00 – 99)
%Y	Year with century, as decimal number
%z, %Z	Time-zone name or abbreviation; no characters if time zone is unknown
If you do not specify a format, the system uses the default remote agent Date and Time formats, show below.	
Default remote agent Date Format: mm/dd/yyyy	
Default remote agent Time Format: hh:mm:ss	



Note *The default data formats may later be replaced by the Current Locale Date and Time formats: %x and %X.*

About All User Variables

Use the _ALL_USER_VARIABLES to format all user variables as follows:

Name1 : Value1<CR><LF>

Name2 : Value2<CR><LF>

Name3 : Value3<CR><LF>

…

*Name**n** : Value**n***

User variables are defined as:

- Non System Variables. All system variables start with ' - '.
- Non OID Variables. All OID variable names start with ' 1 '.

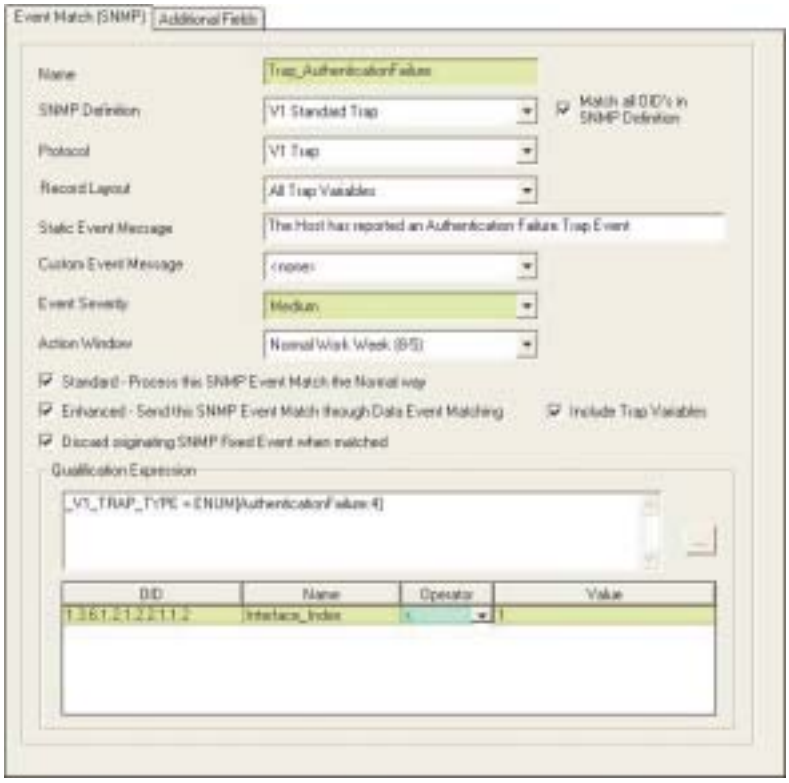
Event Match (SNMP) Tab

If your network supports SNMP, you can use your remote agent to receive and filter trap data for specific alarms and events. Use IRISnGEN's Event Match (SNMP) tab to define event-matching records. Each record identifies an SNMP definition (layout) that contains a list of all Operator Identifiers (OIDs) found in the trap and the qualifying parameters that match the alarms or events. If you choose, you can also include qualifying expressions that enable the system to match sequential or non-sequential values that may be contained within a specific OID. When complete, you save your record and then assign it to a Filter record that you will later download to the remote agent, see "Filters', page 5-9.

SNMP event matching requires SNMP definitions, which are contained in SNMP layouts. Define your SNMP layout definition before creating your SNMP event match record. See "SNMP Layouts', page 6-99, for more information about SNMP definitions.

To create an event match (SNMP) record

1. Right-click the **Event Matches** folder and select **Add Event Match (SNMP)** from the drop menu. The system opens the Event Match (SNMP) tab.



2. Type a name to identify your SNMP event match record in the **Name** field. The name you enter in this field will appear in the Event field list of the Filter record, see "Filters', page 5-9.
3. Select an SNMP layout from the **SNMP Definition** list. The list includes all the SNMP layouts currently in the system. Each layout contains a list of all OIDs, their names, and their types found in the trap.
4. Select the **Match all OIDs in SNMP Definition** checkbox if you want the remote agent to match all OIDS in the trap before filtering the data. This is useful when you need to distinguish between similar traps.
5. Select a protocol from the **Protocol** list to specify the kind of SNMP trap the remote agent should receive.
6. Select a layout from the **Record Layout** list. The layout determines the format of the event record.



7 Type any additional message text that you would like to include with this alarm or event in the **Static Event Message** field. The static event message will appear in the Alarm Viewer window.

8 Select a custom event message from the **Custom Event Message** list. A custom event message is a layout defined in the Layouts Library (see ”Layouts’, page 6-93) that defines how to deliver events in a format that is different from that originally sent from the host system. The event data is formatted according to the layout you select from the list. The custom event message data displays in the Alarm Viewer window.

9 Select a severity level for each event match from the **Event Severity** list. The system adds the severity information to a matched event as a system variable.

10 Select an action window from the **Action Window** list that defines the time event matching should occur. Leave the field blank if you want the system to always perform event matching.

11 Select the **Standard - Process this SNMP Event Match in the Normal Way** checkbox to send the fixed event match to the processing stage.

12 Select the **Enhanced - Send this SNMP Event match through Data Event Matching** checkbox to send the fixed event match to the data event matching stage.

13 Select the **Discard originating SNMP Event when matched** checkbox to delete the original fixed event when matching occurs.

14 Type a qualifying expression in the **Qualification Expression** field to eliminate unwanted events before performing a parsing operation, or to refine further an event match definition, or click the button to open the Expression Builder dialog that enables you to build an expression.

15 Use the Qualification Expression data table to further simplify the expression. Click the button to insert a blank row in the data table; then, select an OID from the list. You can use the same OID more than once in the data table.

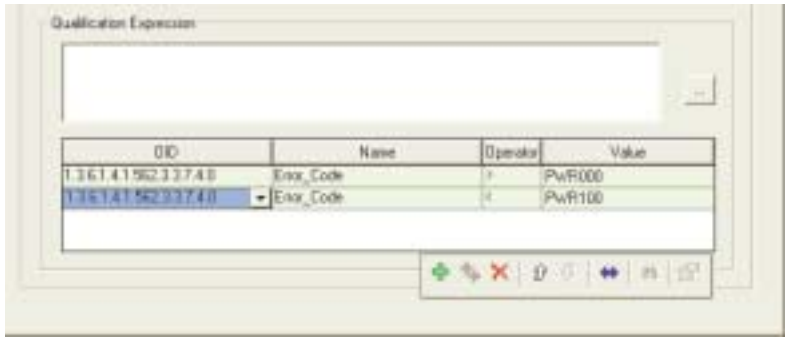
16 Click in the **Name** field to automatically insert the name defined in the SNMP definition layout for the OID. If the name is not known for the OID, then the system omits it from this field.

17 Select an operator from the **Operator** list. An operator is a mathematical expression that use can use to qualify a match.

18 Type a value to qualify this expression in the **Value** field. For example, entered “>” in the Operator field and “1” in this field to build an expression that searches for all values greater than 1.

Example 1- Range Matching

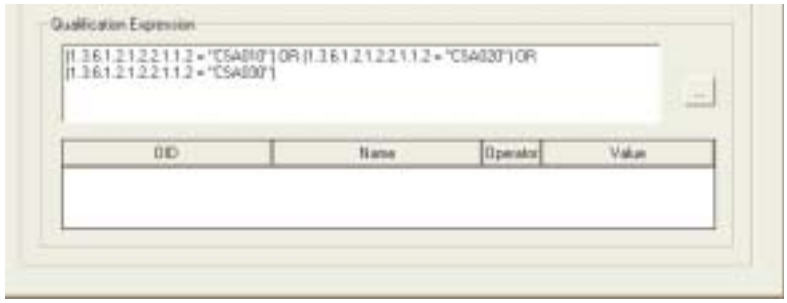
Look at the following figure. Assume you want to match an error code OID containing a specific sequential range of values between PWR001 and PWR099.



The event match will occur for any PWR error code between PWR001 and PWR099. PWR000 or PWR100-999 will not be included in the match. Note that this is an AND condition, which requires two parameters to function. If you entered only one parameter—for example, >PWR000—any alphabetic value greater than PWR000 will match. This means that any PWR value up to PWR999 will match, plus any alphabetic value For example, “QWR100” will also match, because it is greater than PWR. The value LWR100 will not match, because its alphabetic numbering is less than PRW.

Example 2 - Non-Sequential Matching

You can use a qualification expression to match non-sequential values that may be contained in a specific OID. Look at the following figure.



The expression shown in this figure contains the following string:

(1.3.6.1.2.1.2.2.1.1.2 = “CSA010”) OR (1.3.6.1.2.1.2.2.1.1.2 = “CSA020”) OR (1.3.6.1.2.1.2.2.1.1.2 = “CSA030”)

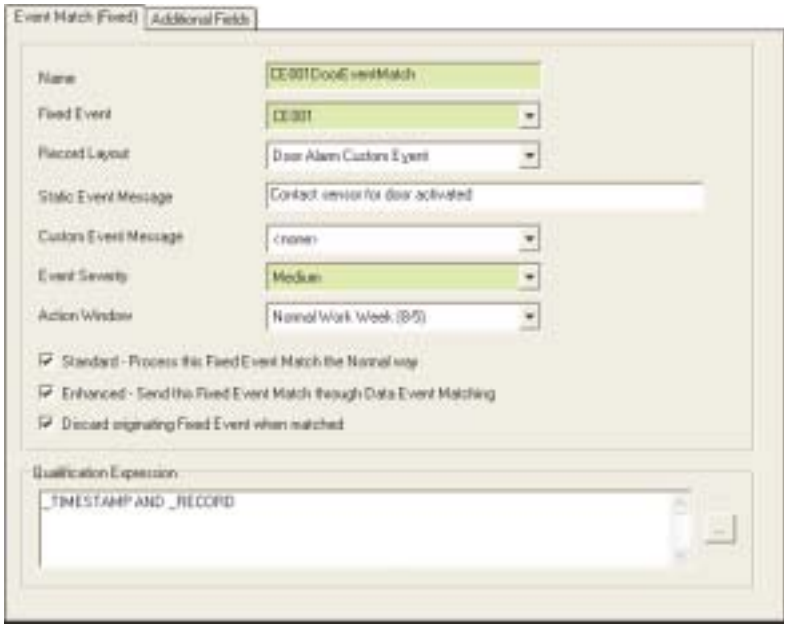
It produces an event match for CSA010, CSA020, and CSA030. It will not match any other CSA values.

Event Match (Fixed) Tab

You can use your remote agent to receive and filter fixed events. For example, you may want to report only the CE001 fixed events (contact sensor activated) when a door opens. Use the Event Match (Fixed) tab to create you event match record. Include the fixed event type and any additional text that identifies the event (Static Event Message). You can also specify a custom event message (layout), severity, action window, and a qualifying expression to eliminate unwanted messages.

To create an event match (fixed) record

1. Right-click the **Event Match** folder; then, select the **Add Event Match (Fixed)** from the menu. The system opens the Event Match (Fixed) tab.



2. Type the name of your event match in the **Name** field.
3. Select a layout from the **Record Layout** list. The layout determines the format of the event record.
4. Select a fixed event from the **Fixed Event** list.
5. Type any additional message text that you would like to include with this event in the **Static Event Message** field. The system stores this information as a system variable within the event data and is available when defining event-processing layouts.
6. Select a layout to configure a custom event message that includes event variable data from the Custom Event Message list. When an event matches, the system formats the data based on the layout selected in this field. The resulting message is added as a system variable.
7. Select a severity for each event match from the **Event Severity** list. The system adds the severity information to a matched event as a system variable. Later, you can use this as part of an expression when determining what actions to take. For example, you could define a filter to deliver all events with a High severity to the IRISnGEN system.
8. Select an action window from the **Action Window** list that defines the times to use the event match. Leave the field blank if you want the system to always use the event match.
9. Select the **Standard - Process this Fixed Event Match in the Normal Way** checkbox to send the fixed event match to the processing stage.
10. Select the **Enhanced - Send this Fixed Event match through Data Event Matching** checkbox to send the fixed event match to the data event matching stage.
11. Select the **Discard originating Fixed Event when matched** checkbox to delete the original fixed event when matching occurs.

12 Type a qualifying expression in the **Qualification Expression** field to eliminate unwanted events before performing a parsing operation, or to refine further an event match definition, or click the ... button to open the Expression Builder dialog that enables you to build an expression.

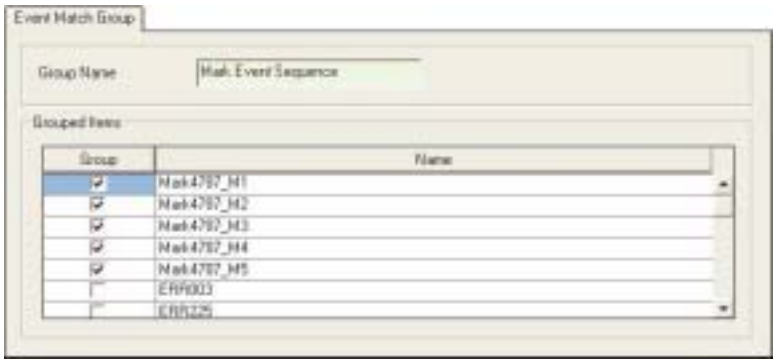
13 Save your record.

Event Match Group

Each event match entry is unique and is used to search for specific information received from a host device. You can assemble groups of event match entries into libraries, typically to support specific hosts. Next, assign each event match to several event match groups to create custom event match libraries without duplicating the event match details. You can assign event match groups to a host library. Any changes to an event match group will affect all of the remote agents using that event match group.

To create an event match group

1 Right-click the **Event Match Groups** folder; then, select **Add Event Match Group** from the menu. The system opens the Event Match Group tab.



2 Type the name of the group in the **Group Name** field.

3 Select the **Group** checkbox for each event match you want to include in the group.

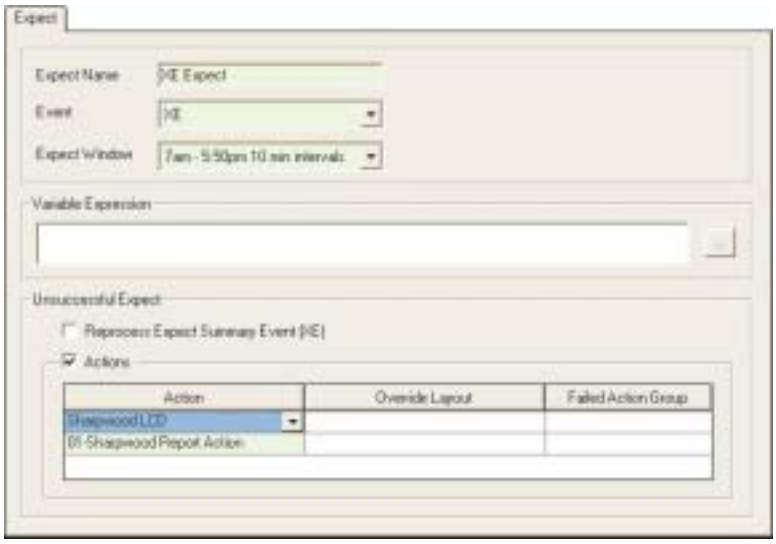
4 The **Name** field displays the name of the configured event matches in the system, by name. This field can assist you when selecting items for grouping.

Expect

The Expect Library is a collection of event matches and fixed events used to search for the absence of events during a specific time window. If the system does not receive the expected event, it can take action, such a reporting it to the system operator. For example, assume that you expect a remote agent to run a self-diagnostic routine each day and send you the results. If the expected event occurs within the time window, no action is required. However, if the expected event do not occur within the window, you can instruct the system to take appropriate action.

To create an expect record

1 Right-click the **Expect** folder; then, select **Add Expect** from the menu. The system open the Expect tab.



2 Type a name for the expected event in the **Expect Name** field.

3 Select an event from the **Event** list. If you select None, you can still use a variable expression.

4 Use the Expect Window field to define when the expected event should occur. Select an action window from the list.

5 Type a variable expression in the **Variable Expression** field that determines when an event is valid, or click the ... button to open the Expression Builder dialog box.

6 Use the Unsuccessful Expect fields to defines what action the system should take when the Expect operation fails, that is, what to do when the event you expect does not occur.

7 Select the **Reprocess Expect Summary Event (XE)** checkbox when you want the system to process the XE summary event. The system generates the XE fixed event when the expected event (defined in the Event field) fails to occur. The system will not process the XE event until you select this box. Since the XE event is a fixed event, you must also define a filter to handle it. For more information about defining filters, see ”Filter’, page 6-88.

8 Select the **Actions** checkbox to activate the Action table. Use the table to define which actions the system should take when it detects the expected event.

9 Click inside the **Action** field; then, select an action from the list. You cannot select the same action twice.

10 Click inside the **Layout** field; then, select a layout for the action from the list. This layout overrides any layout already assigned to the action. If you do not select a layout, the system will use the layout already defined for the action. If you select an action that does not require a layout—for example, a Relay Action—the system ignores this entry.

11 Click inside the **Failed Action Group** field; then select an action from the list. You cannot select the same action twice. When the action already has a failed action defined for it, the system overrides it with the failed action you select in this field. If you do not select a failed action, the system uses the failed action previously defined.

Expect Groups

Use the Expect Group tab to create and maintain groups of expected events.

To create a expect group record

1 Right-click the **Expect Group** folder; then, select **Add Expect Group** from the menu. The system opens the Expect Group tab.



2 Type a name for the group in the **Group Name** field.

3 Select the **Group** checkbox for each expected events you want to include in the group.

4 The **Name** field is read-only field and displays the expected events in the system, by name.

File Types

A file type record contains the data storage characteristics for the remote agent's Store file containing the poll data. This includes the file handling properties, storage size, and File Full fixed event information.

To configure a file type record

1 Right-click the **File Types** folder; then, select **Add File Type** from the menu. IRISnGEN opens the File Type tab.



2 Enter the name of the file type in the **File Type Name** field. If the data will be polled via IRISnGEN, either manually or scheduled, you must use the file name IRISnGEN.

3 Select the store action that the remote agent should take when the compartment fills from the **File Handling** list. Select one of the following:

- **Delete** - Delete the entire contents of the compartment when filled. Writing to the file begins again.
- **Stop** - Stop writing to the compartment when filled. No other action is taken.
- **Wrap Around** Write over the oldest data with the newest data when the compartment fills.

In all cases, the file handling options are only effective within the compartment using a particular file type. They do not affect the rest of the store file.

4 Type a maximum size (in kilobytes) for a compartment in the **Max File Size** field. This setting is only affects the compartment. It does not determine the size of the entire store file. When configuring Max File Size settings, allow for needed extra space, which is approximately 400 bytes per record stored.

5 Select the File Full Events checkbox to generate fixed events based on the amount of data stored in each compartment; then enter the percentage full amounts. The system will generate fixed events when the stored data reaches the percent full at each level.

Fixed events provide information that can help you make decisions when managing your stored data. If you are storing large quantities of data, we recommend that you enable these events so that you can better monitor the status of your data storage.



Note *The first XF event reported to IRISnGEN will trigger a destructive poll, if you checked the Poll Host If Full box in the Host's Polling tab, see "Polling', page 7-10.*

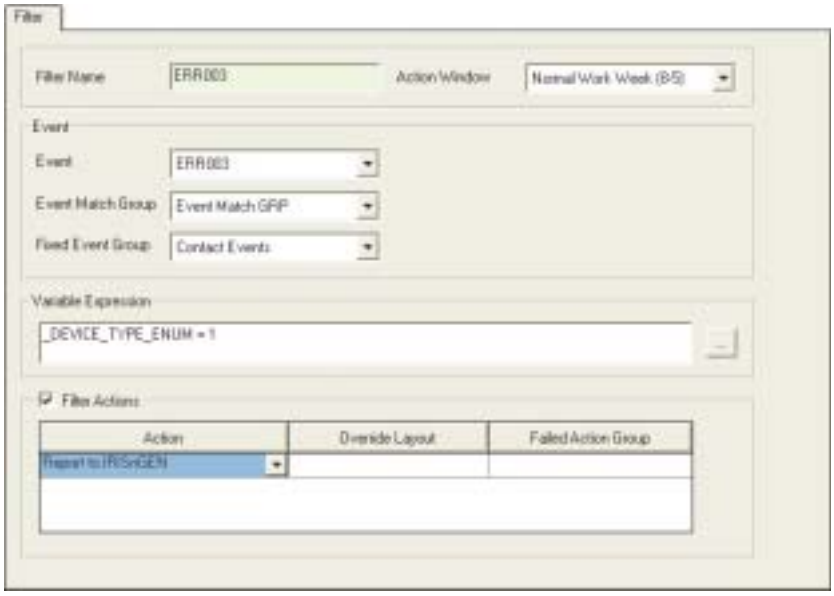
Filter

You can find filter libraries in a container folder (Filter) that expands into two collection folders, Filter and Filters Groups. Define filters for events that require an immediate action. A filter checks for a particular event match or fixed event within an event record and initiates a defined set of actions. Filter definitions can also use logical expressions to qualify further a filter definition match. Each event record may include a number of variables and values that the system added to the event as it passed through earlier stages. You can define a logical expression to reference the variables and the variable data, further narrowing the definition of which events require action. You can base the filter definition solely on the event code, on the event code and a qualifying logical expression, or only on a qualifying expression.

You can assign each event filter definition to any number of libraries, which you can then assign to host libraries. In this scenario, modifying a single event filter record tells the IRISnGEN system that every remote agent is using this particular event filter, regardless of the filter library to which it is assigned. You can associate an action window with each filter definition. It determines when the associated filter definition is valid.

To create an event filter record

1 Right-click the **Filters** folder; then, select **Add Filter** from the menu. The system opens the Filter tab.



2 Type a unique name to identify each filter entry in the **Filter Name** field.

3 Select an action window from the **Action Window** list to specify when to use the filter.

4 Select an event (event matches and fixed events) from the **Event** list. When you select an event, the associated filter only applies to that event.

5 Select a match group to limit your filter to a single event match from the **Event Match Group** list, see ”Event Match Group’, page 6-84.

6 Select a event group to limit your filter to a single fixed event group from the **Fixed Event Group** list, see ”Fixed Event Groups’, page 6-91.

7 Use this field to describe the variable expression and to qualify an event. The variable expression can only refer to the variables of the event.

8 Select the **Filter Actions** checkbox to activate the Filter Actions table listing a group of one or more actions, which will execute when it associated filter evaluates as true.

9 Click inside the **Action** field; then, select an action from the list. You cannot select the same action twice.



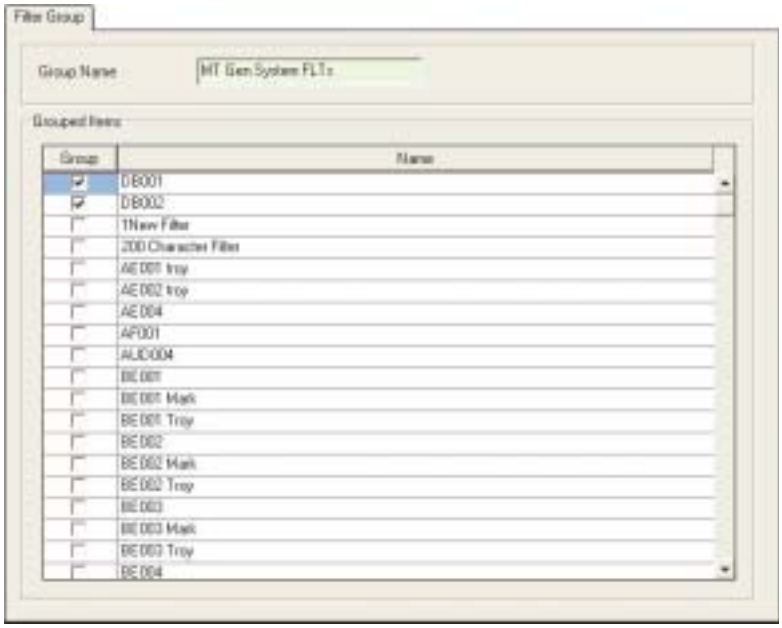
10 Click inside the **Layout** field; then select a layout from the list for the action selected in the previous field. If the action you selected already has ia layout, this layout will override it. If you do not select a layout in this field, the system will use the layout already defined for the action.

Filter Groups

Use the Filter Group tab to create and maintain groups of filter records.

To create a filter group record

1 Right-click the **Filter Group** folder; then, select **Add Filter Group** from the menu. The system opens the Filter Group tab.



2 Type the name of the group in the Group Name field.

3 Select the Group checkbox for each filter you want to include in the group.

4 The Name field is read-only and displays all the configured filters in the system, by name.

Fixed Event

Use the Fixed Event tab to maintain the fixed event filters.

To select a fixed event record

1. Right-click the **Fixed Event** folder; then, double-click a fixed event record. The system opens the Fixed Event tab and displays the details for that record.



2. The **Name** field identifies each fixed event. These names are pre-defined in your IRISnGEN system. You cannot edit this field.
3. Type a description of the fixed event in the **Static Event Message** field. Each event match supports one static message entry. The system stores this information as a system variable with the event and is available when defining event-processing layouts.
4. Select a layout from **Custom Event Message** list to configure a custom event message that includes event variable data. A custom event message is similar to the static event message; however, it has more flexibility through the use of a layout. When an fixed event occurs, the system formats the data from the event based on the layout selected in this field. The resulting message is added as a system variable.
5. Select a severity for each event match from the **Event Severity** list. Select Low, Medium, or High.

   The system adds the severity information to the event as a system variable. Later, you can use this information as part of an expression when determining what actions to take. For example, you can later define a filter to deliver all events with a high severity to the IRISnGEN system.



Fixed Event Groups

Each fixed event entry is unique and is used to search for specific information received from the host device. Fixed Event Groups allow you to assemble groups of fixed event entries into libraries, typically to support specific hosts. You can assign each fixed event to any number of fixed event groups to create custom, fixed event libraries without duplicating the fixed event details. You can assign fixed event groups to a host library. Any changes to an fixed event group will affect all of the remote agents using that fixed event group.

To create a fixed event group record

1 Right-click the **Fixed Event Groups** folder; then, select **Add Fixed Event Group** from the menu. The system displays the Fixed Event Group tab.



2 Type a name for the group in the **Group Name** field.

3 Select the **Group** checkbox for each expected events you want to include in the group.

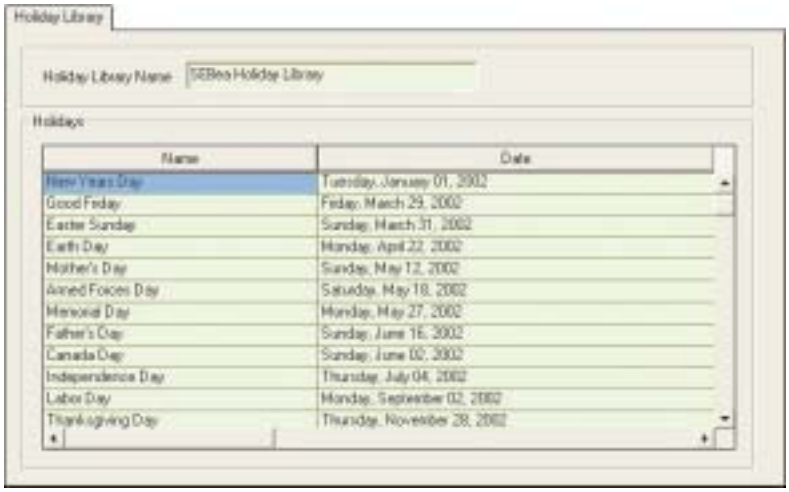
4 The **Name** field is read-only field and displays the fixed events in the system, by name.

Holiday Libraries

Create a holiday library listing all the dates for your recognized holidays. You can then assign your holiday library to an Action window. The Action Window processing will be based on the entries in the holiday row of the action window as the days defined in the holiday table occur.

To create holiday record

1 Right-click a **Holiday** folder, then select **Add Holiday Library** from the menu. The stem opens the Holiday tab.



2 Enter a name for your holiday library in the **Holiday Library Name** field. For example, you may choose to name the holiday library by country, or region.

3 Click inside the Holidays data table; then, click the button to a insert row.

4 Type the holiday name in the **Name** field.

5 Type the date of the holiday in the **Date** field. You can use the Date selection tool when configuring the date. The date displays in the long-date format, based on how you configured the client computer's regional settings.

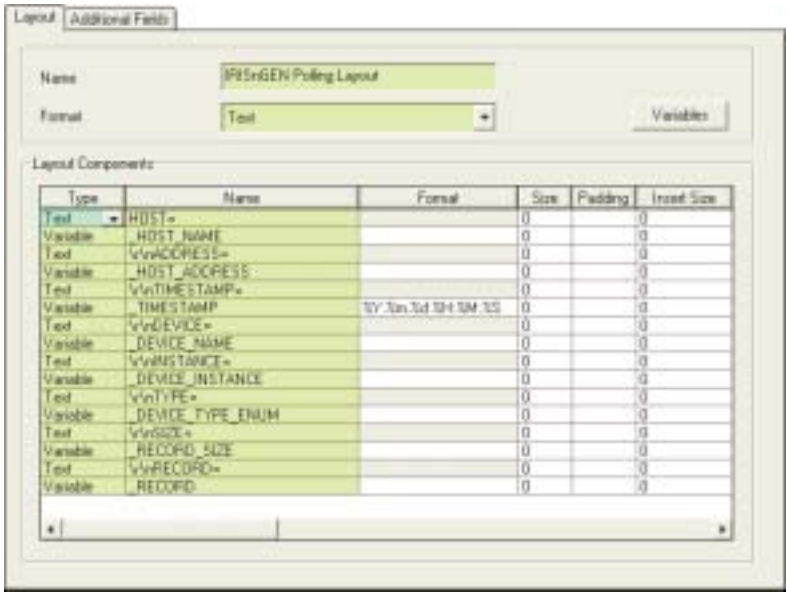
6 Select the **Annual** checkbox if the holiday falls on the same date each year. If the holiday falls on a different date each year, make separate entries for each date. Be sure to leave the Annual box unchecked for holidays that do not fall on the same date each year.

Layouts

The remote device supports configured event formats called layouts. During event processing, any new information gathered during the processing stages append to the event record. Occasionally, an event action may occur that needs a different record format. Use the Layouts library to create custom layouts for events processed by the remote agent. All the data collected during event processing is available when defining a custom layout.

To create a layout record

1. Right-click the **Layout** folder; then, select **Add Layout** from the menu. The system opens the Layout tab.



2. Type a name for your layout in the **Name** field. For example, if you use a layout to handle polling, you could name it "IRISnGEN Polling Layout."
3. Select the layout format from the **Format** list. Select Text or Binary.
4. Click the **Variables** button to display the User Variables dialog that lets you select the source for your variables.
   - Select an event match from the **Event Match** list. The system displays all the data, SNMP, and fixed event matched configured in the system. Once selected, the variables defined in the event match will be available for selection in the Name field in the Layout Components data table. For data event matches, the extracted variable defined in the Variable Extraction templates for the trigger words will be available for selection. For SNMP event matches, the names and OIDs defined in the SNMP definition will be available for selection. For fixed event matches, the specific variables for the fixed event will be available for selection.
   - Select an SNMP layout from the **SNMP Definition** list. The system displays all the SNMP layouts configured in the system. Once selected, the trap variables used in the SNMP definition are available for selection in the Name field of the Layout Components data table. The selection of an SNMP layout is not compulsory.
5. Use the Layout Components table to define the event message format. Each layout component represents a segment of the complete message format. The remote device processes each segment and appends the resulting data into a single event message.

<table>
<tr><th>Field</th><th>What to enter</th></tr>
<tr><td>Type</td><td>Select the type of data for the segment from the Type list. Select Text if the data for the associated segment is static user-defined text. Select Variable if the data for the associated segment is to be based on a system or user-defined variable. All event variables defined in the system are available when creating a layout.</td></tr>
<tr><td>Name</td><td>The content of the Data column depends on the entry defined in the Type column. When the Type column entry is Text, then you will use the Data column to enter static text. When the Type column entry is Variable, you will enter the name of a system or user-defined variable name. If you did not create a user-defined variable name before you began defining the current layout, you can manually enter the name. However, the layout will not function as programmed until you create a user variable of the same name and you associate the layout with an event that has that variable. This field is mandatory.</td></tr>
<tr><td>Format</td><td>Type the date and/or time format in the Format field. For example, the format for 18 October 2000 is “%d %B %Y”. This field is only available when you selected Variable in the Type field. Use the following formatting styles:

Format — Description
%a — Abbreviated weekday name (Mon for Monday)
%A — Full weekday name (Monday)
%b — Abbreviated month name (Feb for February)
%B — Full month name (February)
%d — Day of month as decimal number (01 – 31)
%H — Hour in 24-hour format (00 – 23)
%I — Hour in 12-hour format (01 – 12)
%j — Day of year as decimal number (001 – 366)
%m — Month as decimal number (01 – 12)
%M — Minute as decimal number (00 – 59)
%p — Current locale’s A.M./P.M. indicator for 12-hour clock
%S — Second as decimal number (00 – 59)
%U — Week of year as decimal number. Sunday is the first day of the week (00 – 53)
%w — Weekday as decimal number (0 – 6; Sunday is 0)</td></tr>
</table>



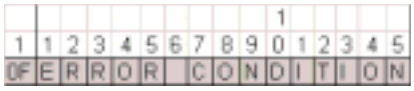
	%W Week of year as decimal number. Monday is first day of week (00 – 53) %x Date representation for current locale %X Time representation for current locale %y Year without century, as decimal number (00 – 99) %Y Year with century, as decimal number
	%z, %Z Time-zone name or abbreviation; no characters if time zone is unknown Although this is not a required field, if you do not specify a format, the remote agent device uses the default date and time format. Default remote agent date format mm/dd/yyyy Default remote agent time format hh:mm:ss ***Note*** *The default formats may later be replaced by the current locale date and time formats, "%x" and "%X."*
Size	Type the exact number of bytes used for the associated data element. Size applies to both text and variable components. When the Size value is zero (0), the length of the data item determines how many characters the system appends to the event message. When the value entered in the Size column is less than the number of bytes in the data, and then the system truncates the data to the specified size. The system truncates the characters at the right, which means the least significant digits of the integer data are truncated. When the value entered in the Size column is greater than the length of the data, and then the system pads the data to the right. The Pad column lets you define specific pad characters.
Padding Character	Type the padding characters in this field. The system only applies padding characters when the Size column has a value larger than the size of the data. Type components pad to the right of the data. Components of the Type variable pad characters to the left of the data. You can define a single padding character for each component; however, the padding column supports up to four characters. You can also enter special characters when specifying non-printable characters as padding character, or enter the hex value when the table does not support a character. The following table shows these characters. This column is optional and the default padding character is the space character (20 hex).



	Character	Name
	\a	Bell
	\b	Backspace
	\f	Form Feed
	\n	New Line
	\r	Carriage Return
	\t	Horizontal Tab
	\v	Vertical Tab
	\?	Literal Quotation Mark
	\"	Double Quotation Mark
	\\	Backslash
	\0	Null
	\x00	Hexadecimal value (for example "\x0A")
Insert Size	Use this field to enter a special format that is only available for the Binary layout. This option also requires that you select a Variable component type. This feature allows you to generate event messages that are formatted as Length/Data pairs. This assumes that the application that is receiving the event message expects a defined number of bytes that represent the length of the data element followed by the data. The number entered in this column defines the number of bytes that will be used to store the length information. The length information will always be inserted before the associated data. If this number is zero (0) or blank, the length information will not be inserted. The insert size value must be set large enough to handle the maximum number of bytes that you expect a particular data element to be.	

Example 1

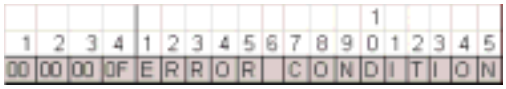
If Insert Size is "1" and the data element text was "ERROR CONDITION," the following data (shown in gray) would result from that layout definition:



0F is the hex representation of 15, the size of the Value. 0F is only 1 byte.

Example 2

If Insert Size is 4 for the example above, then 0000000F is the hex representation of 15, the size of the Value. 0000000F is 4 bytes long.

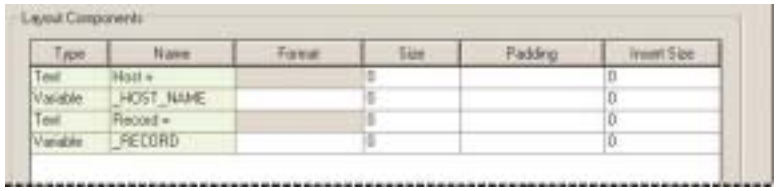




More About Layouts

Polling Layouts

When creating a layout to be used when polling an remote agent via Remote Agent Manager (see ”Layouts’, page 6-93.), you must include the Type and Name layout components (minimum) in the order shown. Failure to include these layout components will result in incorrect or missing poll data.



Report Layouts

When creating a report layout, you must include the variable type _RECORD. If you plan to make changes to the default IRISnGEN Report Layout record, we recommend that you first make a copy of the record before editing it. It will ensure you have complete record available the next time you want to create another report layout record.

SEBII Protocol Layouts

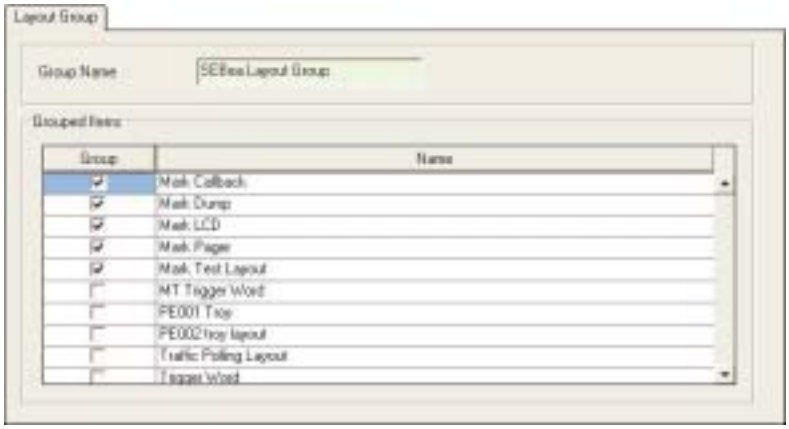
When creating an SEBII protocol layout, be sure the port number specified in the layout record (the port number entry follows the text entry \x20\x20Port\x20) matches the physical host port used on the rear of the SEBII remote agent.

Layout Groups

Use Layout Groups to assemble several layout entries into libraries, typically to support a specific host(s). You can assign each layout to any number of layout groups to create custom, layout libraries without duplicating the layout details. Assign layout groups to a host library. Any changes to a layout group will affect all the remote agents using that layout group. The same result occurs when you make changes to individual layouts.

To create a layout group

1. Right-click the **Layout Groups** folder; then, select **Add Layout Group** from the menu. The system opens the Layout Group tab.



2. Type a name for the group in the **Group Name** field.
3. Select the **Group** checkbox for each layout you want to include in the group.
4. The **Name** field is read-only field and displays the layouts in the system, by name.

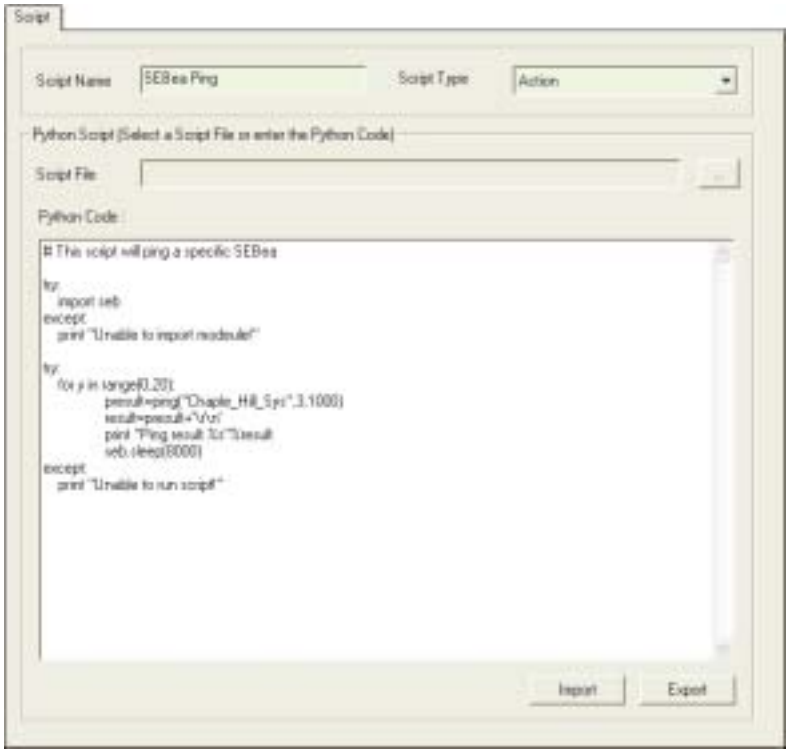
Script

Your IRISnGEN system includes a scripting option that you can use to create and save Python scripts. Use these scripts to automate daily tasks, perform predefined functions, and communicate with your host device. You can also import existing Python scripts and export those you create.

Use the Script tab to create and maintain Python scripts. Once you have created your script, you need only to save it before you send it to the remote agent for execution. You do not need to compile the script first.

To create a script record

1 Right-click the **Script** folder; then, select **Add Script** from the menu. The system opens the Script tab.



2 Type the name of the script in the **Script Name** field. Script names are case-sensitive.

3 Select a script type from the **Script Type** list.

4 Type your script code in the **Python Script Code** field. You must enter the code using the same rules you would use when writing a Python script with any other scripting tool. Once complete, click the **Save** icon to save your work. You do not need to compile the script before sending it the remote agent for execution.

5 Click the ***Import*** button if you want to import a Python script for execution in your IRISnGEN system. The system prompts you for the path name to that script file. Select the script you want; then, click ***OK***.

6 Click the ***Export*** button if you want to export your Python script for use with other devices. Select a directory to save your script as prompted. Click ***OK*** on the Export pop-up dialog.

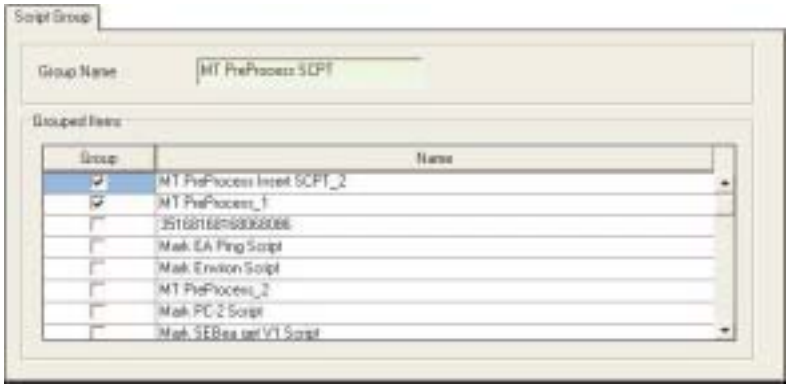


Script Groups

Use Script Groups to assemble groups of script entries into libraries, typically to support specific hosts. You can assign each script to any number of layout groups to create custom, script libraries without duplicating the script details. You can assign script groups to a host library. Any changes to a script group will affect all of the remote agents using that script group.

To create a script group record

1 Right-click the **Script Groups** folder; then, select **Add Script Group** from the menu. The system opens the Script Group tab.



2 Type a name for the group in the **Group Name** field.

3 Select the **Group** checkbox for each script you want to include in the group.

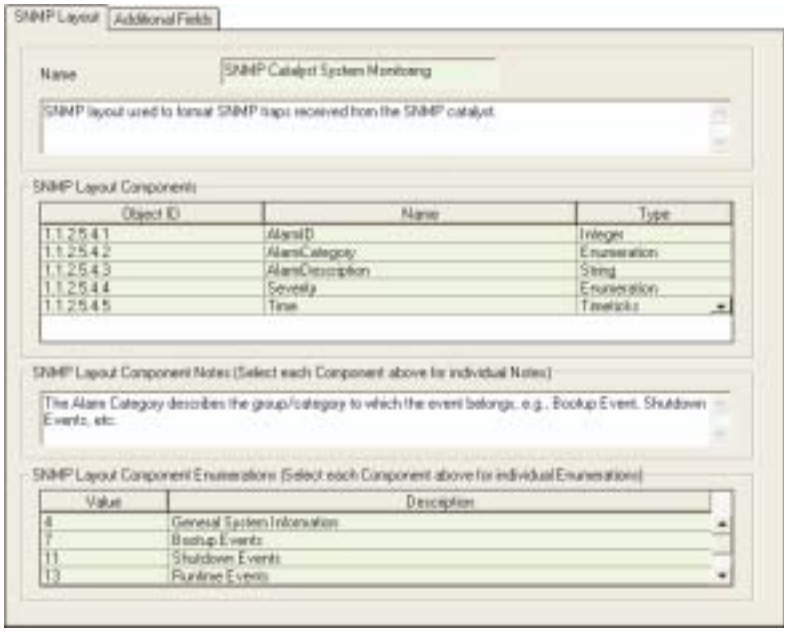
4 The **Name** field is read-only field and displays the scripts in the system, by name.

SNMP Layouts

SNMP layouts tell the system how to act as an SNMP agent when sending event information to SNMP-based Network Management System (NMS). Use this tab to add object IDs with an Enumeration Type.

To create an SNMP layout

1 Right-click the **SNMP Layout** folder; then, select **Add SNMP Layout** from the menu. The system displays the SNMP Layout tab.



2 Type the name of the SNMP layout in the **Name** field. For example, use a layout to define a pager format that supports a limited number of characters and name it “My Pager Service – 80 Char.”

3 Type a description for the overall SNNP layout in the **Name** description field. This is an optional field that also supports hyperlinks.

4 In the **SNMP Layout Components** section, do the following:

- Type the MIB object ID, found in the host device where the data value is stored, in the **Object ID** field.
- Select a predefined object name from the **Name** list. The name describes the data contained in the Object ID.
- Select an SNMP type from the **Type** list.

5 In the **SNMP Layout Component Notes** field, type a description for any selected SNMP Layout Component object, listed in the table above. You an include hyperlinks, if you choose.

6 In the **SNMP Layout Components Enumerations** field, type a value and description to furthed define the enumeration listed in the field above. This field activates automatically when you select an enumeration in the Object ID field above. Note that the values in the **Value** field do not have to be consecutive.

Tasks

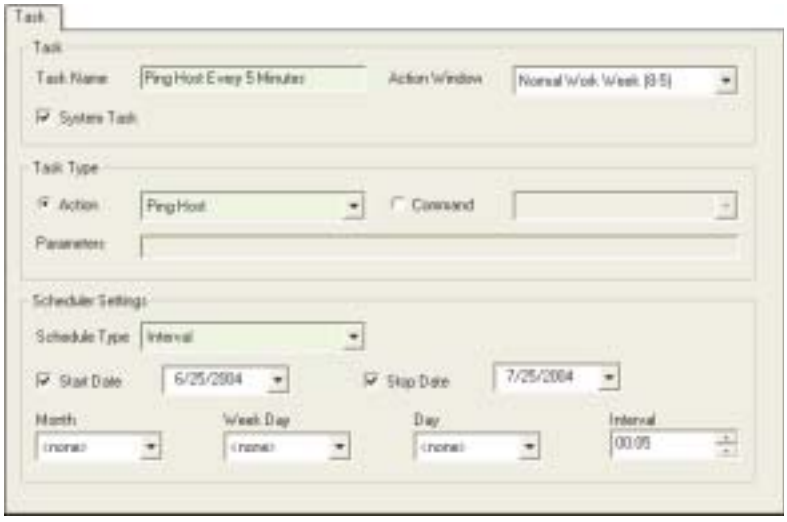
If you are using a remote agent with your IRISnGEN system, you can create task records that execute actions or commands from a schedule. The actions you select are those defined in your Action libraries—for example, an action that pings the host device—and available in a list on the tab. The commands are the pre-defined Command Line commands that you normally issue from the Command Line Interface—for example, issuing the SCRIPT command—and are also available in a list.

You can schedule your action or command to execute at intervals or at specific times. You can schedule actions or commands to execute at monthly, weekly (or day), and timed interval, or you can schedule them to execute at specific times (month, day of week, day, and time of day).

Once you create and save your task record, you can then assign it to a task group (see ”Task Groups’, page 6-102), which you will then assign to a Host Library record (see ”Host Libraries’, page 6-108).

To create a task record

1 Right-click the **Task** folder; then, select **Add Task** from the menu. The system opens the Task tab.



2. Type the name of the task in the **Task Name** field.
3. Select an action window to define the time you want the task to start from the **Action** list.
4. Select the **System Task** checkbox if you want this task to be a system task. Designating a task as a system task will prevent it from being canceled while executing. Those tasks not marked as a system task can be canceled anytime.
5. Do one of the following:
   - Click the **Action** radio button; then, select an action from the list.
   - Click the **Command** radio button; then, select a command from the list.
6. Type the parameters for the command you selected in the previous field in the **Parameters** field. For example, if you selected the SCRIPTS command, enter any specific parameters used to run that script.
7. Select a time or interval schedule from the **Schedule Type** list. Selecting the Specific Time option activates the time control fields below and lets you specify the week, weekday, day, and/or time to execute the task—for example, June 5 at 02:30 AM or every Thursday in September at 13:42 PM. Selecting the Interval option also activate the time control fields and lets you specify an interval cycle—for example, every Monday in August at three hour intervals.
8. Select the **Start Date** checkbox; then, type the date the task should start.
9. Select the **Stop Date** checkbox; then, type the date the task should stop.
10. Select the month you want the task to execute from the **Month** list. When you also select a day in conjunction with the month, IRISnGEN schedules the task for that particular day of the month. When you do not select a month, IRISnGEN schedules the task for every month of that year.
11. Select the day of the week (all weekdays or weekend) you want the task to execute from the **Week Day** list. When you select a weekday, IRISnGEN schedules that task for that day of the week—for example, Tuesday. Select Weekday to schedule the task to run every weekday (Monday – Friday). Select Weekend to run the schedule on Saturday and Sunday. When you select the Week Day option, the Day field becomes unavailable.
12. Select the day of the month to execute the task from the **Day** list. This field works in conjunction with the Month field. When you select the Day option, the Week Day field becomes unavailable.
13. Type a time or time interval (depending on the option you selected in the Schedule Type field) to execute the task in the **Interval** field. If you selected the Specific Time option, enter a time based on your system's time format (24-hour or 12-hour format). If you selected the Interval option, enter number of hours/minutes between intervals.

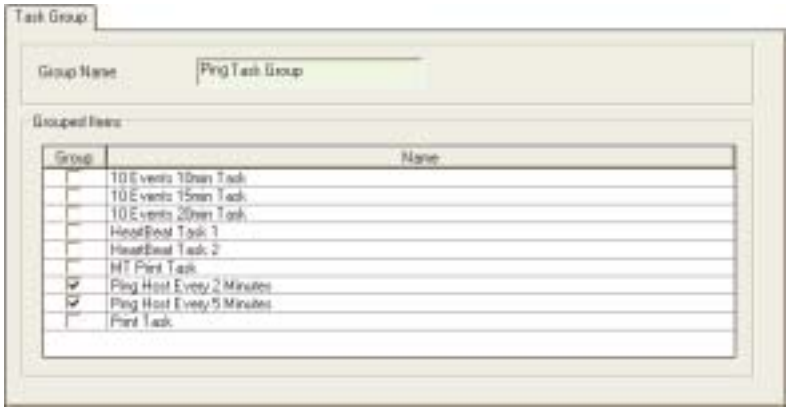
    You can highlight the time and enter a new time/interval, or use the Up and Down arrows to adjust the time/interval.

Task Groups

You can group system tasks into Task Group libraries that support specific remote agents and their attached hosts. Assign the same tasks to any number of task groups to create custom, task libraries without duplicating the task details. Once you create a task group, you can assign it to a host library, see ”Host Libraries’, page 6-108.

To create a task group record

1 Right-click the **Task Group** folder; then, select **Add Task Group** from the menu. The system opens the Task Group tab.



2 Type a name for the group in the **Group Name** field.

3 Select the **Group** checkbox for each task you want to include in the group.

4 The **Name** field is read-only field and displays the tasks in the system, by name.



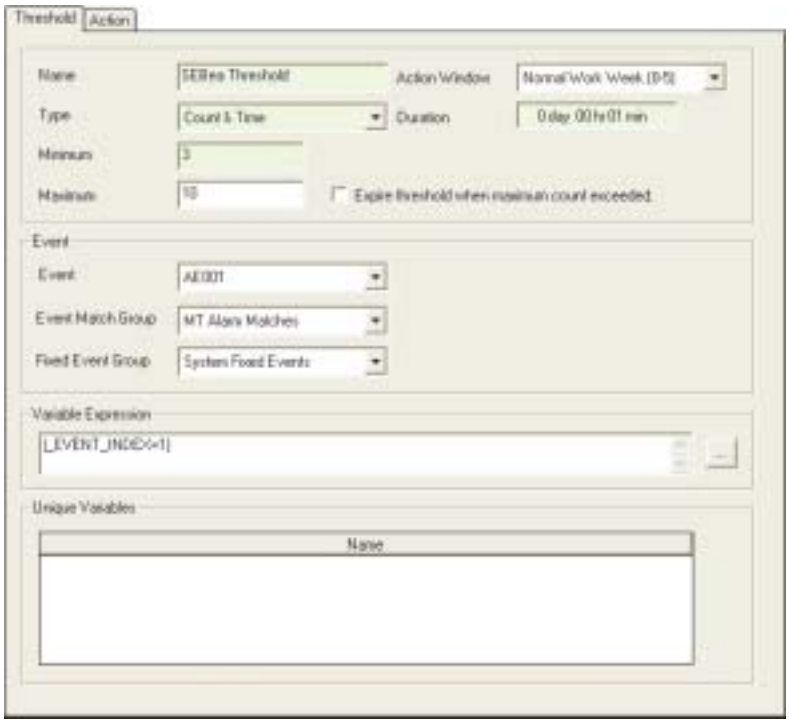
Threshold

Use thresholds to delay any action the system takes until a specific number of events occur. For example, you may define a threshold that instructs the system to wait until it receives three critical events before it takes action. You can define any number of thresholds for each event. The same event may have several, different thresholds for reporting, for storing, and for script execution. You can find the threshold libraries two folders, Threshold and Threshold Groups, both described below.

When defining thresholds, you can include features, such as time, minimum count, maximum count, action window, summary events, and actions based on minimum and maximum counts. You can further define each threshold by type, which identifies how the system will manage the threshold.

To create a threshold record

1 Right-click the **Thresholds** folder; then, select **Add Threshold** from the menu. The system opens the Threshold tab.



2 Type the name of the threshold in the **Name** field.

3 Select an action window from the **Action Window** list to specify when to use the threshold.

4 Select a threshold type from the **Type** list. Select one of the following:

- Fixed Count
- Fixed Time
- Count and Time
- Rolling Window.

See *Threshold Types*, covered earlier in this chapter, for a complete description of these thresholds.

5 Type the number of days, hours, and minutes that the threshold remains active in the **Duration** field. This field works with Fixed Time, Count and Time, and Rolling Window threshold types. It does not work with Fixed Count thresholds, since fixed count thresholds do not expire.

6 Type the minimum number of events that must occur before the system takes action in the **Minimum** field. The system will not take action until the threshold count is one more than the minimum value. You can enter a value from 1 to 100,000 in this field.



Note *If you entered an Event Match Group, or a Fixed Event Group, in the fields below, the minimum threshold will be for all events the system received for that group, not the minimum for each event. For example, assume the Fix Event Group contains the events: AE004, BE001, and BE002. If your minimum threshold is set to "3" and your system receives two AE004 and one BE002 events, then the minimum threshold was reached.*

7 Type the maximum number of events that must occur before the system stops taking action in the **Maximum** field. The system stops taking action when the threshold count is one more than the maximum value. You can enter a value from 1 to 100,000 in this field.



Note *If you entered an Event Match Group, or a Fixed Event Group, in the fields below, the maximum threshold will be for all events the system received for that group, not the maximum for each event. For example, assume the Fix Event Group contains the events: AE004, BE001, and BE002. If your maximum threshold is set to "10" and your system receives four AE004, five BE001, and one BE002 events, then the maximum threshold was reached.*

8 Select the **Expire threshold when maximum count exceeded** checkbox when either the Fixed Count or Count and Time thresholds exceed the maximum number of event occurrences. When you leave this box uncheck, the threshold expires when the system reaches the maximum time.

9 Select the event match or fixed event that you want to use in your threshold from the **Event** list. If you select None, you can still control the threshold by using a variable expression.

10 Select an event match from the **Event Match Group** list.



Note *Each occurrence of a event in an event group increments the threshold count. For example, assume the event group MT Alarm Matches contains the three events: M1_IO001, M1_IO002, and M1_IO003. The minimum threshold is **3** and the maximum is **10**. If the system detects two occurrences of event M1_IO002 and one occurrence of M1_IO003, then the system increments the threshold counter three times and meets the minimum threshold count.*

Adding the unique variable EVENT_NAME (in the Unique Variables field, below) changes the way the system increments the threshold count. In this case, each event must meet the threshold limit. Look again at the previous example. The system must detect three occurrences of M1_IO001, M1_IO002, or M1_IO003 to meet the minimum threshold, or ten of each to meet the maximum count. If the system detects two occurrences of event M1_IO002 and one occurrence of M1_IO003; then, it will wait until it detects one more occurrence of M1_IO002 (for a total of three), or two more occurrences of M1_IO003 to meet the minimum threshold.



11 Select an event group from the **Fixed Event Group** list.

12 Use this multi-line **Variable Expression** field to define a variable expression that determines if the event is valid. The variable expression can only refer to the event variables. If you do not select an event; then, the variables common to all events are available in the Expression Builder. Click the  button to access the Expression Builder dialog. You can find a complete description of the Expression Builder option later in this guide.

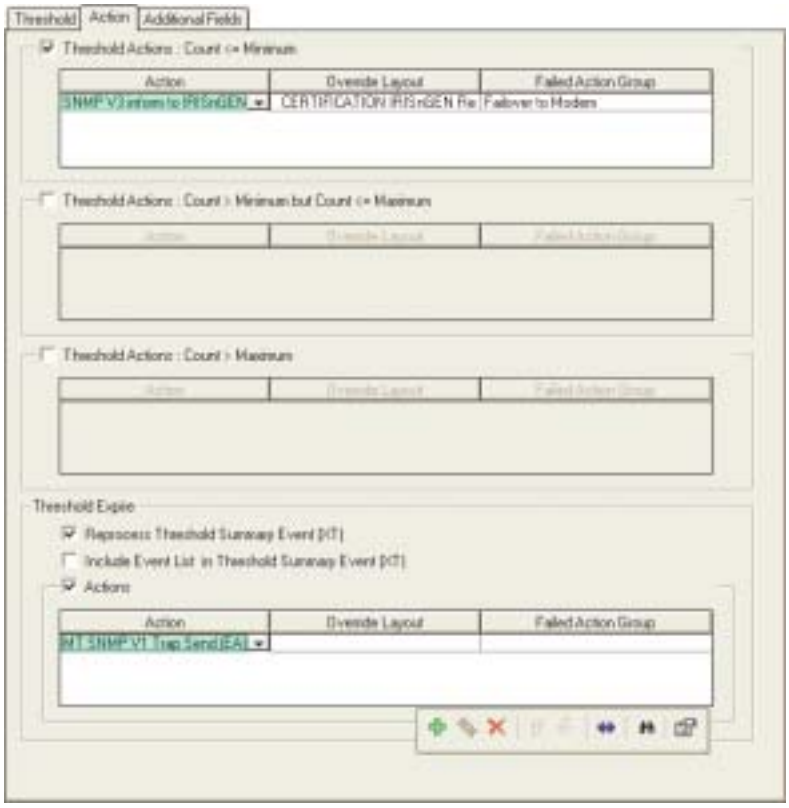
13 Use the Unique Variables data table to define the variables whose values must be unique for all events in the threshold. You must first select an event variable from the Event list. For example, assume you selected CE001 (a contact fixed event) from the Event list. Since all fixed events share numerous variables, including the _DEVICE_INSTANCE variable that specifies which contact produced the event. Selecting the _DEVICE_INSTANCE variable as a unique variable instructs the threshold to evaluate CE001 events separately for each contact pair. The unique variable ensures that the system groups only events with the same value.

Threshold Action

The Action tab contains three tables used to configure action assignments. The system executes the actions while a threshold is active (counting events). The system counts and evaluates each new event; then, takes action based on the count before minimum, between minimum and maximum, and above maximum. Use the following tables to specify each action.

To create a threshold action

1 Click the **Action** tab.



2 Select one of the following Threshold Actions checkboxes to activate the corresponding Action table:

- Count <= Minimum
- Count <= Maximum
- Count > Minimum
- Count > Maximum

3 Select an action from the **Action** list. You cannot select the same action twice.

4 Select a layout for the action selected in the previous field from the **Layout** list. If the action you selected in the previous field already has a layout assigned, this layout will override it. If you do not select a layout in this field, the system will use the layout already defined for the action, if any. If you select an action that does not require a layout, for example, a Relay Action, the system ignores this entry.

5 Select a group to be used if an action fails from the **Failed Action Group** list. You cannot select the same action twice. If the action you selected in the Action field already has a failed action defined for it, the system overrides it with the failed action you choose in this field. If you do not select a failed action, the system uses the failed action previously defined for the action.



6 Select the **Reprocess Threshold Summary Event (XT)** checkbox to reprocess the threshold event —for example, to perform a task or correlation.

7 Select the **Include Event List in Threshold Summary Event (XT)** checkbox to receive a list of threshold events, along with summary events.

8 Select the **Action** checkbox to perform an action for a summary event. Selecting this checkbox activates the Action table.

9 Select the Action, Override Layout, and Failed Action Group parameters from the lists.

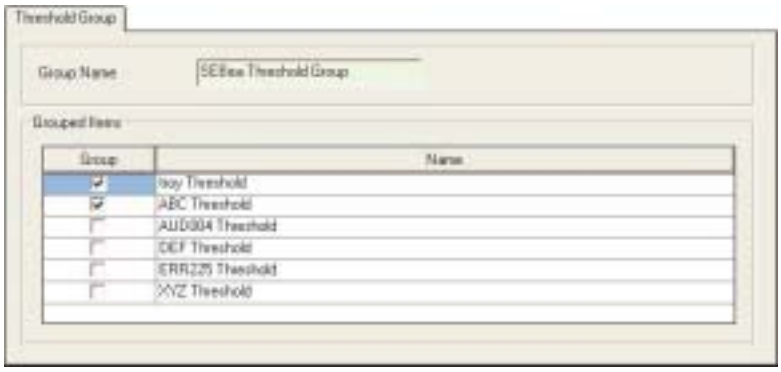
10 Save your record.

Threshold Group

You can group system thresholds into Threshold Group libraries that support specific remote agents and their attached hosts. Assign the same thresholds to any number of threshold groups to create custom, threshold libraries without duplicating the threshold details.

To create a threshold group record

1 Right-click the **Threshold Group** folder; then, select **Add Threshold Group** from the menu. The system opens the Threshold Group tab.



2 Type a name for the group in the **Group Name** field.

3 Select the **Group** checkbox for each threshold you want to include in the group.

4 The **Name** field is read-only field and displays the threshold in the system, by name.

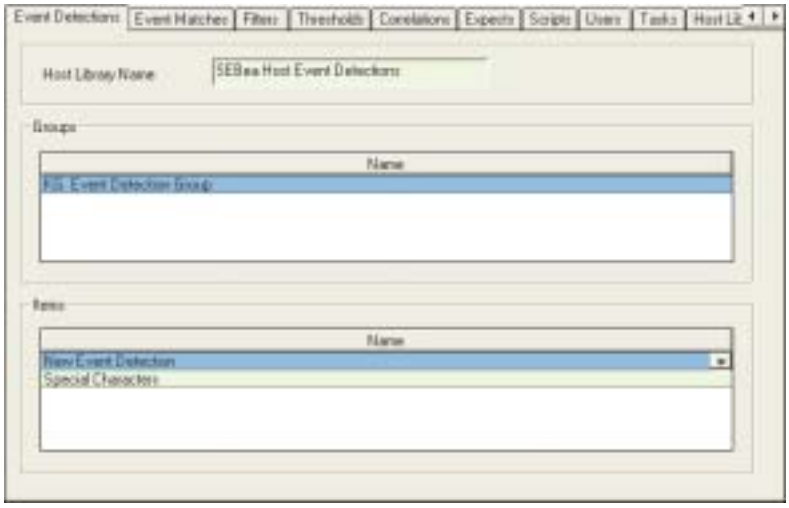
Host Libraries

The Host Library contains ten tabs that you can use to associate and assign individual items or elements to a host library.

- Event Detections
- Thresholds
- Expects
- Users
- Host Libraries
- Event Matches
- Filters
- Correlations
- Scripts
- Tasks

To create a host library

1 Right-click the **Host Library** folder; then, select **Add Host Library** from the menu. The system opens the Event Detections tab.



2 Type a name for the host library in the **Host Library Name** field. When you create a new host library, you must enter the library name on the Event Detections tab. The system then saves this name and automatically displays it on each of the other tabs. Likewise, any changes you make to the name will also appear on the other tabs. Be sure to create a name that easily identifies the library's use.

3 Use the **Groups** data table to assign the desired groups (Event Match Groups, Filter Groups, Threshold Groups, Correlation Groups, etc.) to the current host library. Click inside of the data table and press the button; then, select the group that you want to assign to the host library from the list. Click the button to add several groups to the host library at the same time.

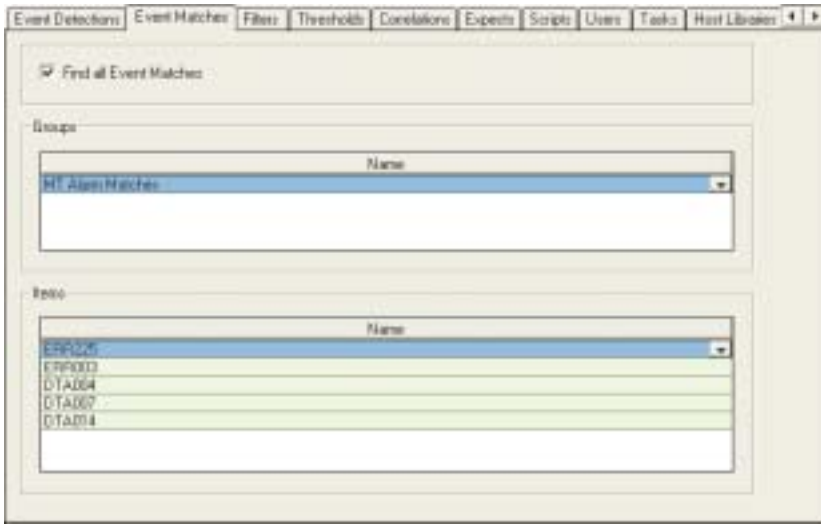
4 Use the **Items** data table to assign the desired items (Event Matches, Filters, Thresholds, and Correlations etc.) to the current host library. Click inside of the data table and press the button; then, select the item that you want to assign to the host library. Click the button and add several items to the host library at the same time.

Event Matches Tab

Each tab, like the one shown in the figure below, identifies a host library selection from which you can assign any number of items (event detections, event matches, thresholds, correlations, filters, etc.) to the current host library. You can also group these items and assign them to the host library. Each tab uses the same format and displays the same data fields.

To create an event library record

1 Click the **Event Matches** tab.



2 Select the **Find all Event Matches** checkbox to perform the matching process for each event assigned to the current host library, either individually or as a group. Leave the box unchecked to stop the matching process when it find the first match.

This option is only available on the Event Matches tab and applies to both the Event Match Group and Items data tables.

3 Use the **Groups** data table to assign the desired groups (Event Match Groups, Filter Groups, Threshold Groups, Correlation Groups, etc.) to the current host library. Click inside of the data table and press the + button; then, select the group that you want to assign to the host library from the list. Click the button to add several groups to the host library at the same time.

4 Use the **Items** data table to assign the desired items (Event Matches, Filters, Thresholds, and Correlations etc.) to the current host library. Click inside of the data table and press the + button; then, select the item that you want to assign to the host library. Click the button and add several items to the host library at the same time.

5 Repeat steps 1 - 4 for each remaining tab.

Host Library Group

You can group system host libraries into Host Library Group libraries that support specific remote agents and their attached hosts. Assign the same host library to any number of host library groups to create custom, host library group libraries without duplicating the host library details.

To create a host library group record

1 Right-click the **Host Library Group** folder; then, select **Add Host Library Group** from the menu. The system opens the Host Library Group tab.



2 Type a name for the group in the **Group Name** field.

3 Select the **Group** checkbox for each host library you want to include in the group.

4 The **Name** field is read-only field and displays the host library in the system, by name.

Model Libraries

The Model Libraries are a collection of remote agents available within your IRISnGEN system. Teltronics manufactures four models:

- 4 Port, 8 Contact
- 5 Port, 8 Contact
- 8 Port, 16 Contact
- 9 Port, 16 Contact

The Models tab displays hardware and data devices configured for each model, for example, the host serial data devices, the contact sensor devices, DC voltage, battery, etc. A check mark by the device indicates that device is configured and available for use in your remote agent. You can select the remote agent model in the Remote Agent tab, see ”SEBea/ NET-PATH Remote Agent Tab’, page 2-23.



Note *Use this tab for display purposes only. We strongly recommend that you do not change the setting for any of the models listed.*

The following figure shows the model tab for the remote agent devices configured with nine serial ports, a modem, and sixteen contact sensors.



Security Libraries

The remote agent contains security access controls for access to connected devices, data collected from connected devices, and remote agent management functions. You can assign each user a profile to control his or her level of access. You can then assign the user to an access group that defines which of the remote agent commands is available to the user and you can assign users to user groups.

You can grant access rights to hosts globally or to individual hosts. Grant global access rights to a user or user group when you assign that user or group directly to a remote agent node. Although the user can access all hosts, that user is still restricted by the access rights defined in the access group to which he or she is assigned. The system will check the user or user group assignments for the remote agent before checking the user or user group assignments for individual hosts.

When you need to restrict access to selected hosts that connect to the remote agent, you must assign the users and user groups to the matching host nodes. As mentioned before, you can do this by assigning users and user groups to host type definitions, or you can assign them directly to a host library or host definition in the remote agent database.

Your IRISnGEN system generates the password files, which provides a quick lookup capability when used the remote agent. The system encrypts the user password information in the file and in any protocol transactions that require a user name and password.

Define a profile for each user that contains specific parameters, and then assign the user to a user group. The functions that a user can perform are a combination of the profile, the access rights defined in the access group, and where you assign the user in the remote agent database (host, host type, or the remote agent).

Remote Agent Passwords

You can grant access to remote agent functions using a combination of user names and passwords. The remote agent supports the following types of passwords.

The system password permits full access to all functions listed in the Access Group Command list. Assign this password via the Remote Agent record, along with a corresponding user name.

The system password will not support automatic callback. You can define automatic callback in the User security window. However, the remote agent protocol does allow you to initiate a manual callback to a non-IRISnGEN caller, such as Procomm, if desired.



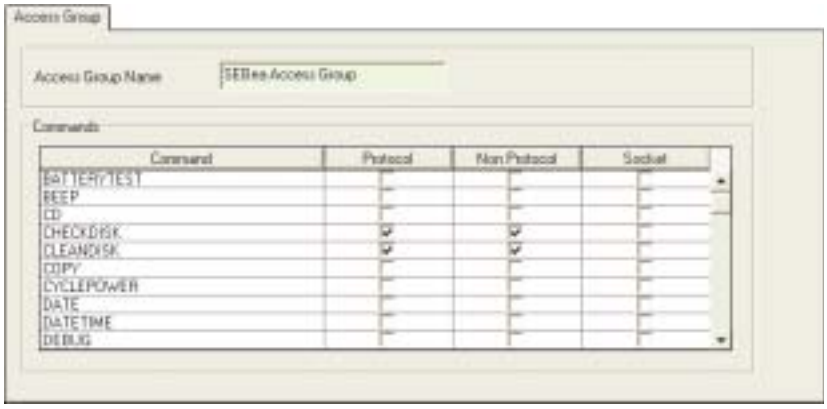
Access Groups

An access group defines the access rights for a selected collection of remote agent commands. Remote agent commands may be available through proprietary protocol, non-protocol mode, or socket connections. You can find the Access Groups folder under the Security Libraries folder.

Assign each access group to one or more users. By doing this, each user inherits the access rights defined in the access group.

To create an access group record

1 Right-click the **Access Group** folder; then, select **Add Access Group** from the menu. The system opens the Access Group tab.



2 Type the name of the access group in the **Access Group Name** field.

3 Use the Commands data table to configure each command access. Select the checkbox for each command that you want users to access. Remember this is a group of access rights that you will assign to many users, so be sure to create generic access groups, such as Administrator Access, Technician Access, or Master Access. Note that only users given system access can change these settings.

Command	Description
ALARM	Deliver / Receive alarms
BEEP	Sound the buzzer
CALL BACK	Request the slave system call the master system
CANCEL	Cancel the last command sent to the remote agent
COMMANDLINE	All users to discontinue use of protocol and enter command line dialogue
CONFIG	Set the current application and/or database
CYCLEPOWER	Cycle power on a hardware device
DATE	Set / Get current date
FORMAT	Format a drive
GETPM	Get the Personality Module
LANGUAGE	Select the language

LOADER	Replace the current loader with a new one. Does not re-boot
LOGIN	Begin a new protocol session or re-activates a disconnected session.
LOGOUT	Terminate a session,
PAGEMODE	Set / Show lines to display in pagination mode while interactive
REBOOT	Force the SEB to reboot
RELAY	Control an output relay
SETPM	Set the Personality Module.
SETSEBNUM	Set the serial number in both the RTC and in the PM.
TERMINATE	Close all Sessions and / or Disconnects the port connection.
TEXT	Write text to the LCD display
TIME	Set / Get the current time
TRANSPARENT	Initiate a transparent connection
USER	Replace the current user with a different user.
ATTRIB	Change the attributes of a file(s)
CD	Change the current directory
CHKDSK	Check a drive for errors
COPY	Copies a file(s)
DEL	Delete a file(s)
DIR	Get the current directory structure
DPOLL	Destructive Poll
GETFILE	Request a file from the SEB
GREP	Searches for a string in a file(s)
MD	Make a new directory
MEDIA	Change the current media or list all the available media.
MOVE	Moves a file(s)
NDPOLL	Non-destructive poll
PWD	Get the current working directory.
RD	Remove an existing directory



RENAME	Rename a file(s)
SENDFILE	Notifies the SEB that a file will be sent
TREE	Get the tree structure for a drive
TYPE	Type the File
BATTERY	Get the Battery Status
CONTACT	Get the Contact Sensor Status
HELP	Display help for all the commands or for a specific command.
MEMORY	Get the Memory Status
POWER	Get the Commercial Power Status
STATUS	Request the SEB return information about the current status of the SEB
SYSTEM	Give operating system level status

4 Select the **Protocol** checkbox to include the command from the access group for protocol communication. Protocol communication is made with IRISnGEN Remote Agent Manager.

5 Select the **Non Protocol** checkbox to include the access group for non-protocol communication. Non-protocol communication is made through the command line interface interaction with the remote agent.

6 Select the **Socket** checkbox to include the command from the access group for socket communication. Socket communication is made through a network connection and is a non-protocol connection.

Adding Commands to the Data Table

Occasionally, Teltronics, Inc. makes new commands available through system upgrades. New commands appear at the bottom of the data table and are unchecked. You must select (check) each command you want before IRISnGEN will allow its use. Once you select your new commands, press F5 to refresh your data table. IRISnGEN then displays those commands in alphabetical order in the data table with the other selected commands.

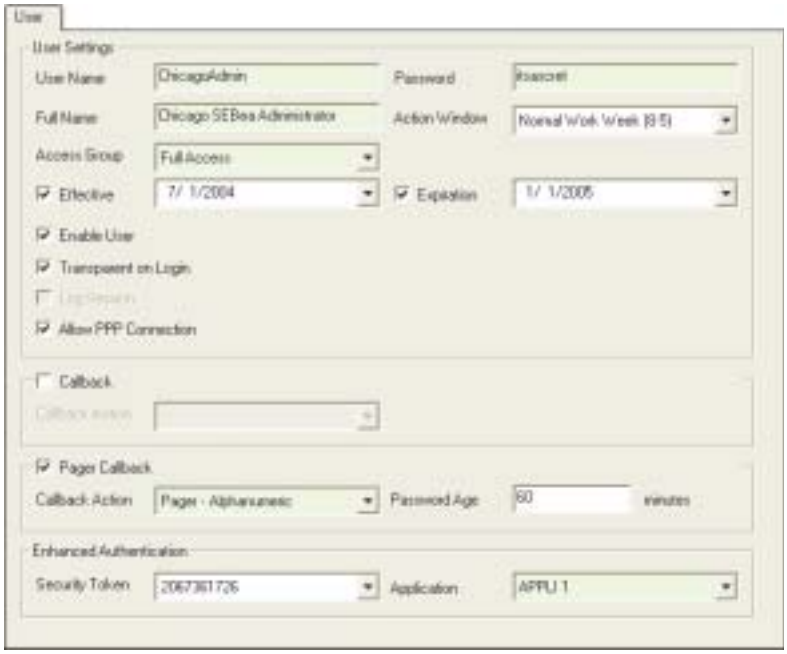


Users

The User folder contains a list of user profiles, each with a set of access rights. You cannot grant a user multiple sets of access rights.

To create a new user profile

1 Right-click the **User** folder; then, select **Add User** from the menu. The system opens the User tab.



2 Type a unique name that will help you quickly identify the user in the system in the **User Name** field. You can enter up to twenty characters. Use any of the following characters in this field: a-z, A-Z, 0-9, _, @, #, $, %, ^.

3 Enter a password for the user in the **Password** field. The system has two levels of passwords, system, and user. The system password grants full access rights to the user. User passwords offer limited access rights to functions or devices. We recommend you assign system passwords in the Remote Agent window and assign user passwords in this field.

You can create user passwords up to twenty characters. For security, the password you create is transmitted to the remote agent in an encrypted format. Also, the login sequences made in the interactive mode do not echo the password. The password information is not logged as part of the audit trail feature, which further adds to security. Use any of the following characters in this field: a-z, A-Z, 0-9, _, @, #, $, %, ^.

4 Enter the full name of the user who will use this login in the **Full Name** field.

5 Select and action to limit a user's access to specific times of the day or days of the week, including holidays from the **Action Window** list.

6 Select an access group for the user from the **Access Group** list.

7 Select the **Effective** checkbox; then, click the list arrow and select the date that the user's access rights become active from the calendar. Use the directional arrows to move through the months. When you reach the desired month, click the date you want. The system enters that date in the field. You must select an effective date.



8. Select the **Expiration** checkbox,; then, click the list arrow and select the date that the user's access rights expire from the calendar. The user cannot access the system after this date. Use the directional arrows to move through the months. When you reach the desired month, click the date you want. The system enters that date in the field. If you do not want the user's rights to expire, do not check the box.
9. Select the **Enable User** checkbox to enable the user's password and grant the rights assigned in the access group. If you do not select this checkbox, the remote agent will deny access to this user. We suggest you uncheck this box when you want to temporarily suspend a user's access rights.
10. Select the **Transparent on Login** checkbox to allow the user to connect directly to a host port when the password is verified. Assign a user or user group to the host to which this user should have immediate access upon login. If you assign a user to multiple hosts or to the remote agent, then the system will display a choice list of available hosts. Use this feature in conjunction with the callback and pager callback features. After the system verifies the password, it connects the user directly to the assigned host. For additional details on callback, see the Callback section below.
11. Select the **Log Session** checkbox to enable logging for the user. A session log records all of the commands that the user attempts. However, as a security measure, a log session never records passwords. Logs are stored in the remote agent on the media specified in the Remote Agent record (Flash or RAM).
12. Select the **Callback** checkbox to enable this feature. When selected, the system validates the user's login to the remote agent and waits for the remote agent to acknowledge the login. Once it receives acknowledgement from the remote agent, it terminates the session and waits for the remote agent to return the call using a pre-programmed telephone number (see Callback Action). Upon answer, the system validates a caller's identity.
13. Select a callback action from the **Callback** list. The list contains all the actions you created using the Report Action tab, found under the Remote Agent Libraries folder. Note that the number of retries and the retry period do not apply to callbacks.
14. Selecting an action gives the callback process access to an appropriate modem and telephone number. For example, a report action developed to call back John Barley is named Callback John Barley. Alternately, you can name the report action according to the telephone number it calls, for example, 941-555-5000.
15. Select the **Pager Callback** checkbox to enable IRISnGEN to validate the user's login to the remote agent and wait for the remote agent to acknowledge the login. Once it receives acknowledgement from the remote agent, IRISnGEN terminates the session and waits for the remote agent to return the call using a pre-programmed pager number or service. Upon answer, IRISnGEN issues a temporary password. Once the user terminates the session, the IRISnGEN invalidates the temporary password. IRISnGEN then resets the password to that defined in the User record. Should a callback disconnect abnormally, IRISnGEN will not invalidate the temporary password. Instead, it remains valid until the call terminates normally, or until it reaches the expiration date.
16. Select an pager action to give the callback process access to modem and pager information such as telephone number and PIN from the **Pager Callback Action** list.
17. Type the age (in minutes) for the pager callback password in the **Password Age** field. When the time expires, the user can no longer sign into the remote agent using the temporary password. The password reverts to the password defined in the User record.
18. Used as a security feature, representing a user's encrypted smart card information. The Token Data field is not available in this version of the IRISnGEN system.

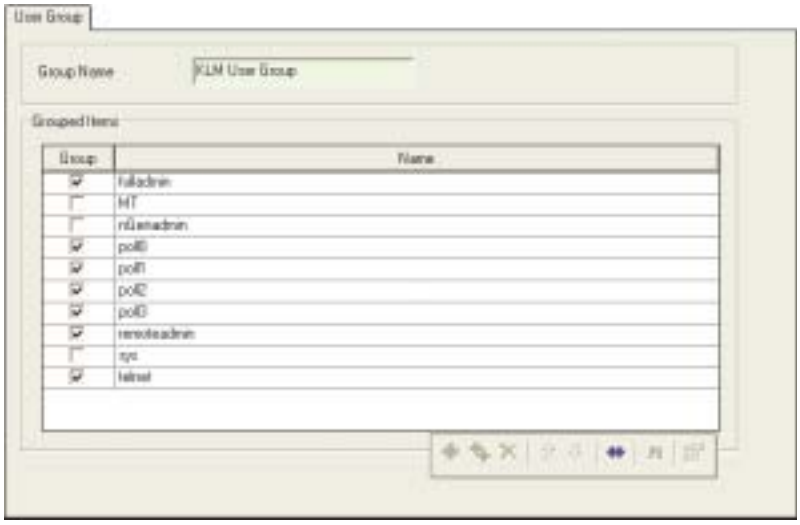


User Groups

You can group users into User Group libraries that support specific remote agents and their attached hosts. You can assign the same user to any number of user groups to create custom, user group libraries without duplicating the user details.

To create a user group record

1 Right-click the **User Group** folder; then, select **Add User Group** from the menu. The system opens the User Group tab.



2 Type the name of the user group in the **Group Name** field.

3 Select the **Group** checkbox for each user you want to include in the group.

4 This read-only field displays all the configured users in the system, by name.

Security Assignments

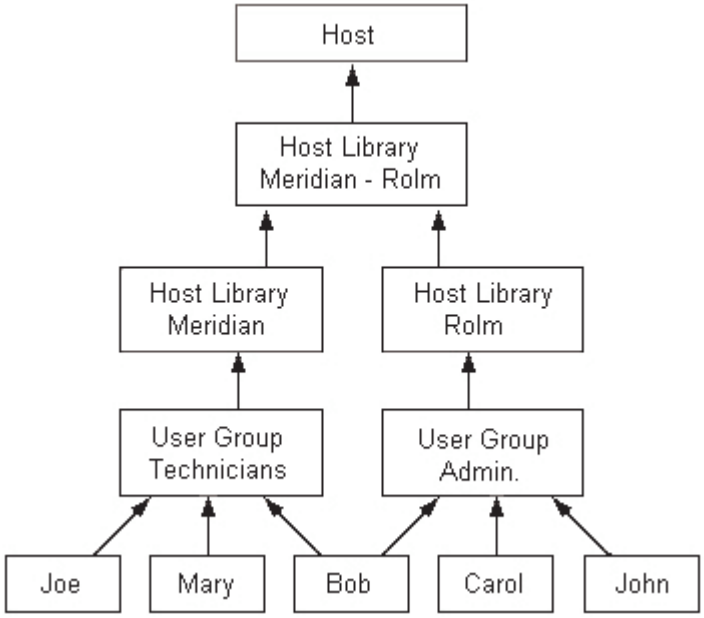
Your remote agent devices, hosts, and host types share security definitions and each may have multiple users and user groups assigned to it. When assigning users at the remote agent level, note that each user has access rights to all the hosts attached to that remote agent device. When assigning users at the host type level, the user only has access rights to hosts with the same host type. Assigning users or user groups at the host level overrides users and user groups at the host type level, applying the access rights just to that host.

For example, suppose you have five field technicians that routinely service Meridian Option 81 hosts. You assign those five users to a user group, and then assign that user group to the host type for Meridian Option 81. However, for security, you only want your two best technicians to have access to the Option 81. Create a user group containing your two top technicians and then assign that user group to the specific Option 81 host at that location. Since the host security assignments override the host type assignments, only those two technicians will have access rights to this specific host.

User assignments are cumulative when embedded in host libraries and assigned to hosts. For example, users Joe, Bob, and Cindy are assigned to user group Technicians. Users John, Lillie, and Bob are assigned to user group Admin. The two User Groups are then assigned to host libraries Meridian and Rolm, respectively. Both of these host libraries are assigned to host library Meridian-Rolm, and the Meridian-Rolm library is assigned to a host. All of the users assigned (Joe, Bob, Cindy, John and Lillie) have security rights to the host. This scenario is illustrated below.



.


Host
Host Library
Meridian - Rolm
Host Library
Meridian
Host Library
Rolm
User Group
Technicians
User Group
Admin.
Joe
Mary
Bob
Carol
John

Template Libraries

To speed the configuration of remote agents, your IRISnGEN system includes the Template Libraries. Create a template that includes the remote agent model and device libraries, and then assign that template library to the remote agent. The system automatically fills in the remote agent's model and device library fields with those from the template. This can save you a great deal of time by allowing you configure the template once and apply it to many remote agents.

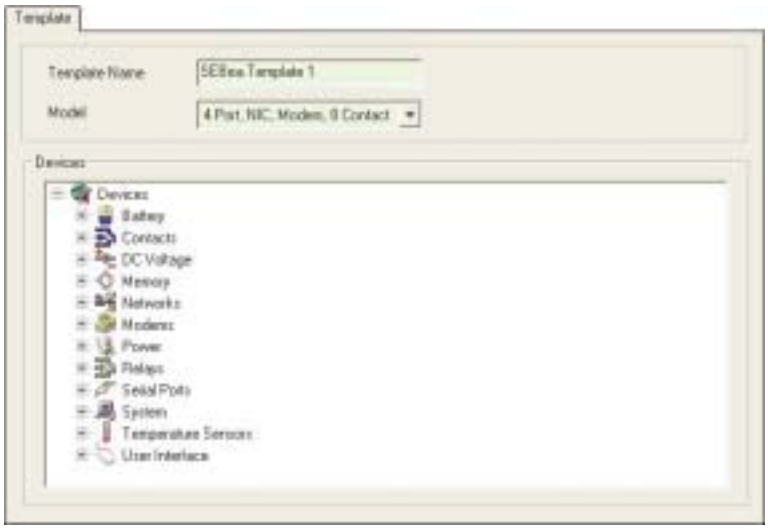


Note *NET-PATH Plus templates are included in all new installations of IRISnGEN; however, they are not included in IRISnGEN upgrades for v7 and higher.*

The model configurations are set at the factory. You cannot adjust these settings.

To create a template record

1 Right-click the **Template** folder; then, select **Add Template** from the menu. The system opens the Template tab.



2 Type the template name in the **Template Name** field. For example, name a template "Standard Alarms" to indicate that its assignment to remote agents that monitor your standard set of alarms.

3 Select a model for this template from the **Model** list of remote agent hardware models. Each model is preset at the factory with the physical devices available for use. When you select a model from the list, the system automatically fills in the Name, Type and Connection fields in the Devices section and places a check in the box next to each device name.

4 Select the **Devices** checkboxes in the left column of the Devices section to enable the device for this template. When selected, the device is logically enabled and is available to be programmed for event monitoring or other usage. When not selected, the device is effectively logically disabled and not available for programming in the database.

5 Type the name of the device in the **Device Name** field, or use the default names. The default names are provided by the IRISnGEN application. You can revise the names to correspond to standard hosts you plan to connect to each device. This name is extremely important. The name created here determined how this device is identified in the database, regardless of the physical instance to which the name is assigned. Assign names that are intuitive when creating the templates (e.g., Meridian Alarms, Meridian CDR, Door Sensor.) If you have designed Host Libraries to use specific device names (for example, in Action libraries) and used templates to configure those device names, changing a device name in a template will break the reference in



the Host Library. You will need to create new Action Libraries that reference the new device name, assign those to a new Host Library, and then use that Host Library for new Remote Agents. Failing to create a new reference in the Action Libraries will result in failed actions in the remote agent.

6 Select a device type from the **Device Type** list, or use the default type. IRISnGEN provides default device types for each model device you selected. Most entries have only one possible type to select. The serial ports have two types: Serial and Serial/Modem. Select Serial when this port is used only for a serial connection—for example, serial data input or a terminal action.) Select Serial / Modem when an external modem will be attached to the serial port.

7 The **Connection** name is assigned by IRISnGEN and cannot be changed. It references the physical connection of the device on the remote agent. The Connection name closely corresponds to the physical labeling of the hardware on the remote agent so that it is easily identified by field personnel. The logical name of the device (Device Name as discussed above) can be moved to any appropriate connection to maintain integrity in the database, since the remote agent will always take action based on the device name rather than the connection location. The physical attachment of the host must correspond to the Connection assignment of the device Name.

8 Select the device library that defines the physical and logical attributes, as well as selected Fixed Events for a device type, from the **Device Library** list. For example, the device library for a serial port contains information for baud rate, parity, data bits, stop bits, flow control, DTR control, buffer size, log files and fixed events. Other device libraries contain similar attributes as applicable to the type of device. Create or select device libraries carefully for your templates. Template libraries should reflect your most widely used remote agent configurations.



Note



7

Remote Agent Manager

The Remote Agent Manager application works with many types of remote agents, including the SEBea, SEBII, NET-PATH, Intelliman, and Dispatcher. Using Remote Agent Manager, you can easily tailor each remote agent to meet your data collection and reporting requirements. Remote Agent Manager provides the operation and maintenance tools required to maintain each remote agent device. The Remote Agent Manager lets you configure, upload, download, poll, and check the status of your remote agents.

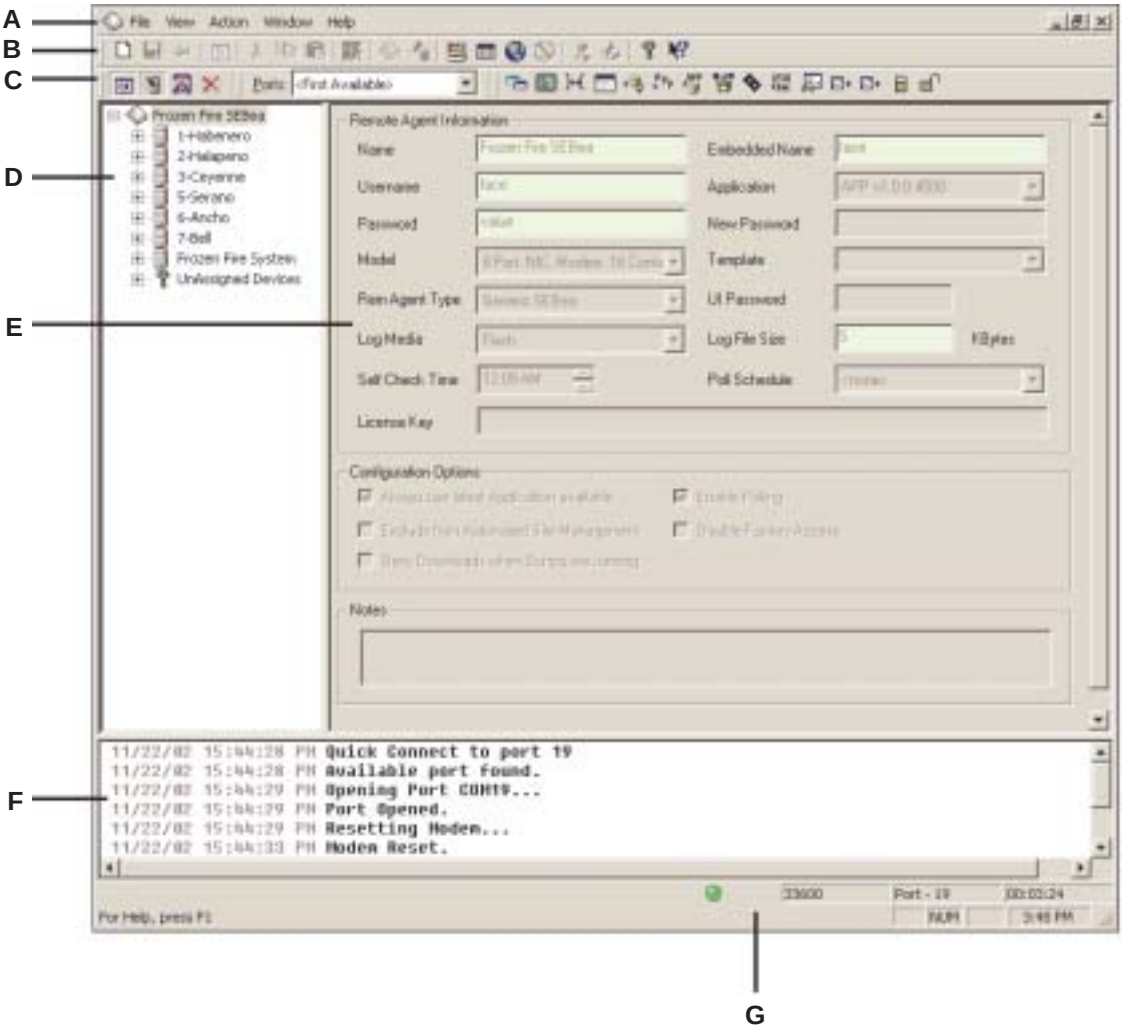
Accessing Remote Agent Manager

You can access Remote Agent Manager several ways:

- In the tree view pane, right-click a remote agent or host device, and then select Remote Agent Manager from the menu.
- Click the Remote Agent Manager icon ().
- Highlight the remote agent; then, select IRIS > Remote Agent Manager (or press F7 on your keyboard).

Your IRISnGEN system displays the Remote Agent Manager window, shown on the next page. Depending on the remote agent type you choose, your window may vary slightly.

Remote Agent Manager Window



A *Drop-down menus* display a list of options you can select from within Remote Agent Manager.
B Use the *Action toolbar* to perform additional functions in Remote Agent Manager.
C The *Remote Agent toolbar* gives quick access to Remote Agent Manager features.
D The *Tree View* pane shows the hierarchy between the remote agent and its hosts.
E The *Task Detail* pane lets you configure and manage your remote agent.
F The *History* pane displays the information logged when Remote Agent Manager is connected to the device.
G The *status bar* shows modem connection information. A green bubble shows that Remote Agent Manager is connected to the device. It shows a red bubble when it is disconnected.

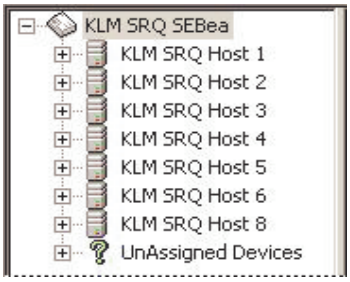


Tree View

The tree view pane, at the far left of the screen, shows the hierarchical relationship between a remote agent and its hosts.



Note *When you select a remote agent or host device from the tree view pane, the Task Detail pane and the toolbars change to display information for that remote agent or host.*



Displaying and Hiding the Tree View Pane

You can customize your Remote Agent Manager window by choosing to display or hide the tree view pane.

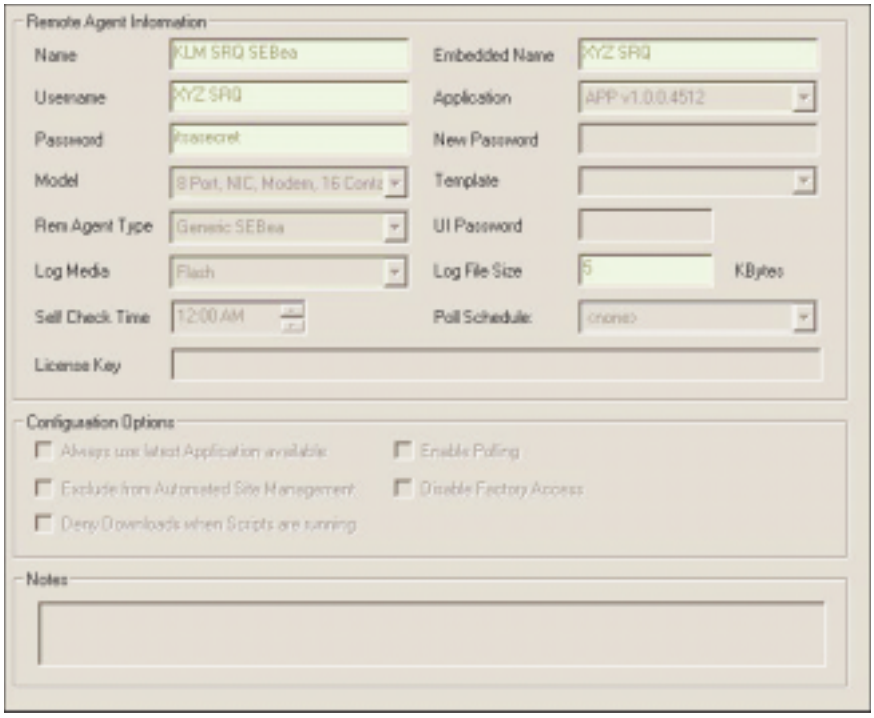
To display or hide the tree view pane

Do one of the following:

- Click the icon .
- Choose View > Show/Hide SEB/Host Views.

Task Detail Pane

The Task Detail pane lets you view your remote agent's configuration parameters. These are the parameters defined in the IRISnGEN libraries and previously downloaded to the remote agent. The following example shows the SEBea Task Detail pane. If you select the SEB II or foreign remote agent, your Task Detail pane will have fewer fields.



History Detail Pane

The Remote Agent Manager History pane displays the information logged when the IRISnGEN modem is connecting and connected to the remote agent modem. The log includes information, warning, and error messages. Each output line includes a timestamp identifying when the system logged the message. You can scroll the view, or resize it.



To display or hide the History Detail pane

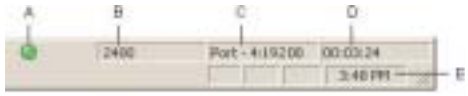
- Click the icon.

To clear the contents of the History Detail pane

- Click the icon.

Status Bar

The status bar at the bottom of the window displays modem connection information.



A. *Connection bubble* ***B.*** *Baud rate* ***C.*** *Dial-out port number and DTE rate*
D. *Time connected* ***E.*** *Local time*

A red bubble indicates that the Remote Agent Manager is not connected to the remote agent.

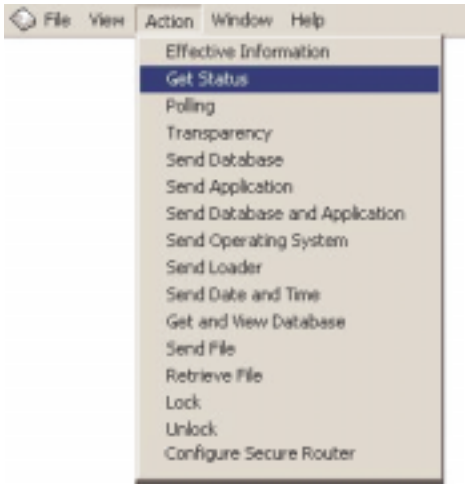
A green bubble indicates the Remote Agent Manager is connected to the remote agent. The numerical description indicates modem speed.

The status bar also displays the baud rate of the connection, the port number of the IRISnGEN modem dialing the remote agent, the length of time connected, and the client server local time.

Note the baud rate (DCE speed) shown on the status bar is the actual rate the modem returns as its baud when it connects. This may not be the same baud rate as defined in IRISnGEN for this modem. The DTE rate, shown with the dial-out port number, is the rate between the IRISnGEN server and its dial-out modem.

Remote Agent Manager lists

You can select command options from the lists listed at the top of the window.



To select a command

- Click a menu on the menu bar; then, click the command.



Note *The options available on each menu may differ depending on the type of remote agent you are using.*

Remote Agent Manager Active Toolbar

While working in Remote Agent Manager, you can also execute a limited number of options from the Active toolbar: List Viewer, History Viewer, Geographical Viewer, About, and Help. All other options are grayed and are unavailable. See Chapter 3 for more information about these options.



A. *List Viewer* ***B.*** *History Viewer* ***C.*** *Map Viewer*
D. *Equipment Viewer* ***E.*** *Help* ***F.*** *About*

To execute an option from the Active toolbar

- Click the icon for the option you want.

Remote Agent Manager Toolbar

Use the toolbar icons to quickly access commands specific to Remote Agent Manager.

To execute an option from the toolbar

- Click the icon for the option you want.

The following shows the Remote Agent Manager icons common to all remote agent devices.



A. *Show/Hide SEB/Hosts View* ***B.*** *Show/Hide History View* ***C.*** *Connect/Disconnect*
D. *Clear History Detail*



Note *Choosing the Toolbar option from the View list toggles the Remote Agent Manager toolbar on an off.*

The following shows toolbars and the icons available for each type of remote agent.

SEBea/NET-PATH Toolbar



A. *Effective information* ***B.*** *Get Status* ***C.*** *Polling* ***D.*** *Transparency* ***E.*** *Send Database*
F. *Send Application* ***G.*** *Send Database and Application* ***H.*** *Send Operating System*
J. *Send Loader* ***K.*** *Send Date and Time* ***L.*** *Get and View Database* ***M.*** *Send File*
N. *Retrieve File* ***O.*** *Lock* ***P.*** *Unlock* ***Q***. *Configure Secure Router*

SEB II Toolbar



A. *Edit Remote Agent Database* ***B.*** *Effective Information* ***C.*** *Get Status*
D. *Polling* ***E.*** *Transparency* ***F.*** *Get Database* ***G.*** *Send Database* ***H.*** *Send ASP*
J. *Send ASP and Database* ***K.*** *Send Date and Time* ***L.*** *Display Failure Codes*

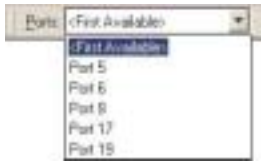
Foreign Agent Toolbar



A. *Effective Information* ***B.*** *Transparency*

Port Select

Also appearing on the Remote Agent Manager toolbar is the Port selection box. Click the down arrow and select from the list of available ports on the IRISnGEN system, or leave the default, *<First Available>*.





Note *The ports that appear in this list are those defined in the Ports library (IRIS Administration > Communication > Ports) and assigned a dial-out port group.*

Connecting/ Disconnecting from the Remote Agent

Before you can begin using the Remote Agent Manager functions, you must first establish a connection with your SEB remote agent device.

To connect to the remote agent

- Click the Connect icon ( ).

To disconnect from the remote agent

- Click the Disconnect icon ( ).



Warning *If you end Remote Agent Manager abnormally using Task Manager's End Task, or if you rebooted your client machine, any connection with the remote agent device can take up to six minutes to disconnect.*

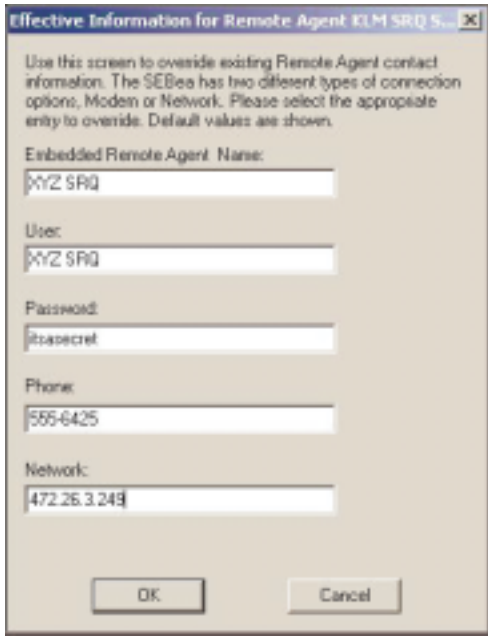
SEBea/NET-PATH Remote Agent Manager Functions

The following discusses the Remote Agent Manager functions used with SEBea/NET-PATH remote agents. See ”SEB II Remote Agent Manager Functions’, page 7-28 for a discussion of SEB II remote agent functions. See ”Foreign Agent Remote Agent Manager Functions’, page 7-44 for foreign agent functions.

Effective Information

The Effective Information function lets you quickly access SEBea/NET-PATH remote agents without reading each SEBea/NET-PATH’s database into memory. However, the entries you make in the Effective Information screen must match the entries programmed into the SEBea/NET-PATH remote agents. Only when they match will communication with the SEBea/NET-PATH remote agent be possible.

If you have not yet downloaded a database to the SEBea/NET-PATH remote agent, you can still communicate with it using the Effective Information functions. Simply enter the SEBea/NET-PATH remote agent name, password, and telephone number in the appropriate fields. If you are communicating via a network, enter its user name and network ID.



To display the Effective Information pop-up

Do one of the following:

- Choose Action > Effective Information.
- Right-click a remote agent and select Effective Information from the pop-up menu.
- Click the Effective Information icon ( ).

To override a SEBea/NET-PATH’s effective information

1. Type a new name to override the embedded remote agent ID in the **Embedded Remote Agent Name** field.
2. Type a new master user name to override the current master user in the **User** field.
3. Type a new password to override the remote agent’s current password in the **Password** field.
4. Type a new telephone number to override the remote agent’s current phone number in the **Phone** field.

5 Type a new IP address to override the remote agent's current IP address in the **Network** field.
6 When you are satisfied with your selections, click ***OK***.

Get Status

With the Get Status function, you can check the settings for each SEBea/NET-PATH remote agent.

To view SEBea/NET-PATH status

Do one of the following:

- Choose Action > Get Status.
- Right-click a remote agent; then, select Get Status from the pop-up menu.
- Click the Get Status icon ( ).

The Remote Agent Status dialog box appears.





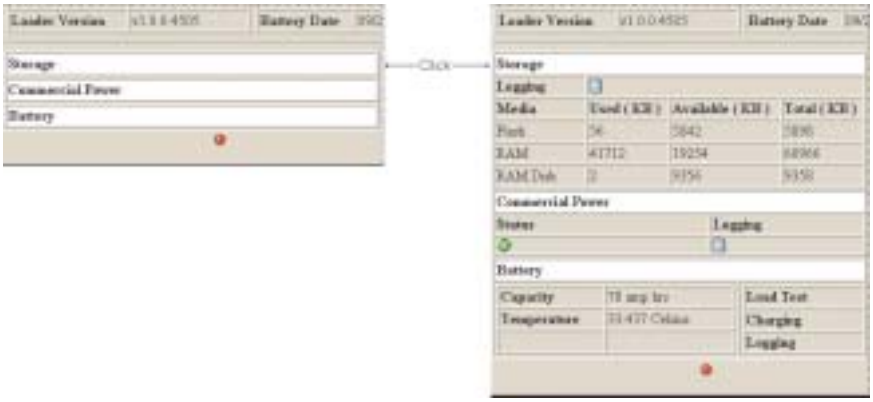
Note *Choosing Get Status defaults to a modem dial out, unless you already established a network connection using the Connect icon* ( ).

Expanding and Collapsing the Status Fields

You can expand and collapse the status fields on the SEBea/NET-PATH's Get Status screen to customize your view.

To expand and contract fields

1 Click the header bar to expand the field.



2 Click the header a second time to collapse the field.

Polling

You can retrieve data stored from the SEBea/NET-PATH remote agent using the Remote Agent Manager's Polling function. This function includes a wizard that steps you through the polling process. At each step, enter the parameters that meet your polling requirements.

To poll the SEBea/NET-PATH remote agent - Step 1

1 Do one of the following:

- Choose Action > Polling.
- Right-click a remote agent (or a host) and choose Polling from the pop-up menu.
- Highlight the remote agent (or host) and click the Polling icon ( ).

The system opens the Polling Options–Step 1 dialog box.



2 Select a **Type of Poll** radio button for your poll.

Field	Description
Destructive Poll	As the Remote Agent Manager receives and acknowledges each block of data, the SEBea/ NET-PATH clears the data from its memory.
Non-Destructive Poll	As the Remote Agent Manager receives and acknowledges each block of data, the SEBea/ NET-PATH does not clear the data from its memory.

3 Select a **Polling Data Storage Options** radio button for your poll.

Field	Description
Save polled data to file only	Store the polled data in the location specified in File Options (File Name textbox).
Save polled data to IRISnGEN's Database	Store data in the IRISnGEN database. IRISnGEN stores the data in the location specified by the polling application, see"Polling Tab', page 2-19. If the polling application is Alarms, the data is stored in the SQL database. If the polling application is a custom application, such as CDR, the data is stored in the location specified by that application.
Save polled data to file and IRISnGEN's Database	Store data in both the file and the database. IRISnGEN stores the data in the location specified by the polling application, see "Polling Tab', page 2-19. If the polling application is Alarms, the data is stored in the SQL database. If the polling application is a custom application, such as CDR, the data is stored in the location specified by that application.

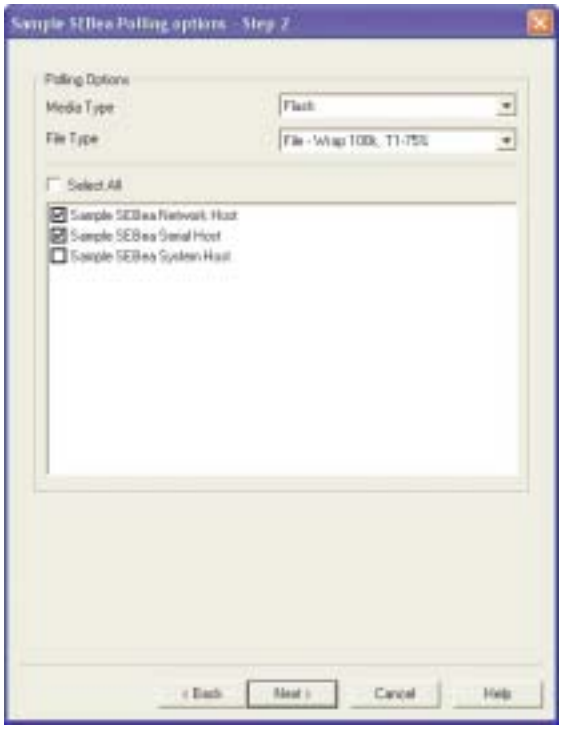
4 Type the poll file name and extension in the File Name field; then, select a File Option radio button.

Field	Description
Append	Keep the existing data in a file and save polled data to the end of the file.
Replace	Clear the file before saving the polled data.



To poll the SEBea/NET-PATH remote agent - Step 2

1 Click ***Next*** to display the Step 2 dialog box and continue entering parameters.



2 Select the medium of your stored data (Flash or RAM) from the **Media Type** list.

3 Select a file type for the SEBea/NET-PATH from the **File Type** list. File types are defined in the File Type library, see ”File Types’, page 6-87.

4 Select the **All Poll** checkbox if you want to poll all hosts.



Note *Only hosts matching the criteria selected in the Polling Options section above will poll successfully.*

5 Select the **Host** checkbox for each host you wish to poll.

To poll the SEBea/NET-PATH remote agent - Final Step

1 Click ***Next*** to display the Final Step dialog box and to review your polling parameter selection.



2 Click ***Finish*** to begin the polling process, or click ***Cancel*** to exit without polling.

Transparency

You can communicate directly with your SEBea/NET-PATH remote agent or with the attached host device by establishing a transparent connection through the SEBea/NET-PATH's internal modem, its serial port(s), or via Telnet. The SEBea/NET-PATH offer three transparency modes: Normal, Passive, and Active Bridge. Normal and Active Bridge offer transparent access to a command line interface. Use this interface to examine the status and control the various SEBea/NET-PATH functions, or to issue commands directly to the host.

Use Normal mode to interact fully with the SEBea/NET-PATH or its attached host device though Ttwin's emulation window. Use Passive mode to view data sent and received from the host device, only. Passive mode is a read-only transparency. You cannot issue any commands to the host device. Use the Active Bridge mode to send and receive data from the attached host. You can issue commands to the host device and SEBea/NET-PATH while in Active Bridge.

Your ability to access the SEBea/NET-PATH or host devices will depend on your security authorization level (user name and password). Check with your system administrator to determine your level of authority.

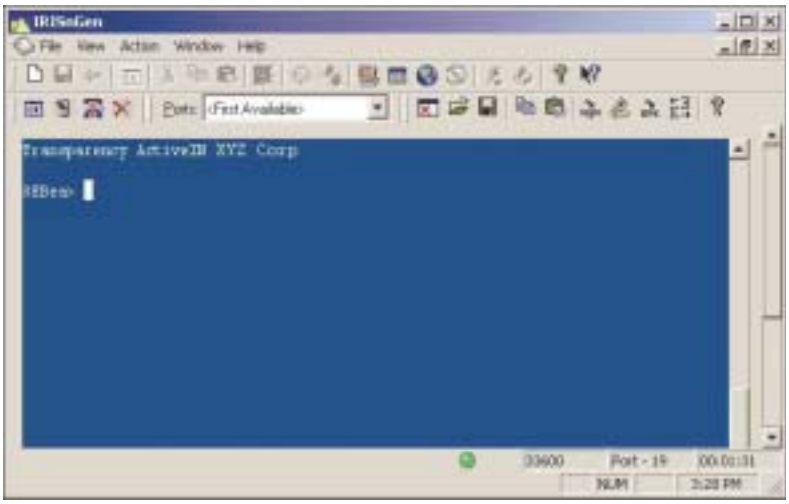
SEBea/NET-PATHSEBea/NET-PATH Normal Transparency

To establish Normal transparency with the SEBea/NET-PATHSEBea/NET-PATH remote agent while in Remote Agent Manager

Do one of the following:

- Choose Action > Transparency.
- Right-click a remote agent and select Transparency from the pop-up menu.
- Click the Transparency icon ( ).

Remote Agent Manager establishes a connection and displays a transparency window in Normal mode.



The Transparency window appears automatically when IRISnGEN establishes the communication link with the SEBea/NET-PATH or the attached host device. A green bubble on the status bar indicates you connected with the SEBea/NET-PATH device.

Host Normal Transparency

To establish Normal transparency with a host device attached to the SEBea/NET-PATH

- Highlight the Host icon ( ) in the tree view pane for the host device you wish to connect, and then click the Transparency icon ( ).

Remote Agent Manager establishes a connection; then, opens a transparency window in normal mode, as shown in the previous figure.

Passive Transparency

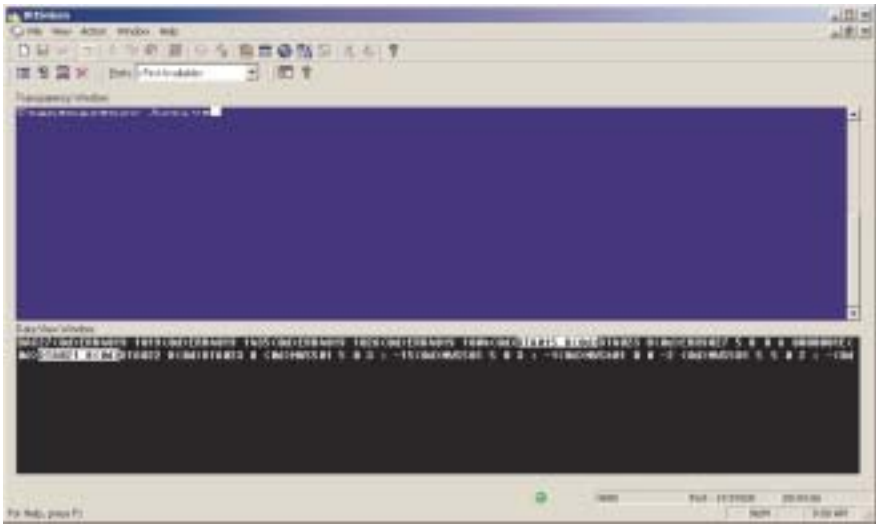
To establish Passive transparency with the host device

Do one of the following:

- Choose Action > Transparency – Passive.
- Right-click a remote agent; then, select Passive Transparency from the menu.

The Transparency window appears in Passive mode.





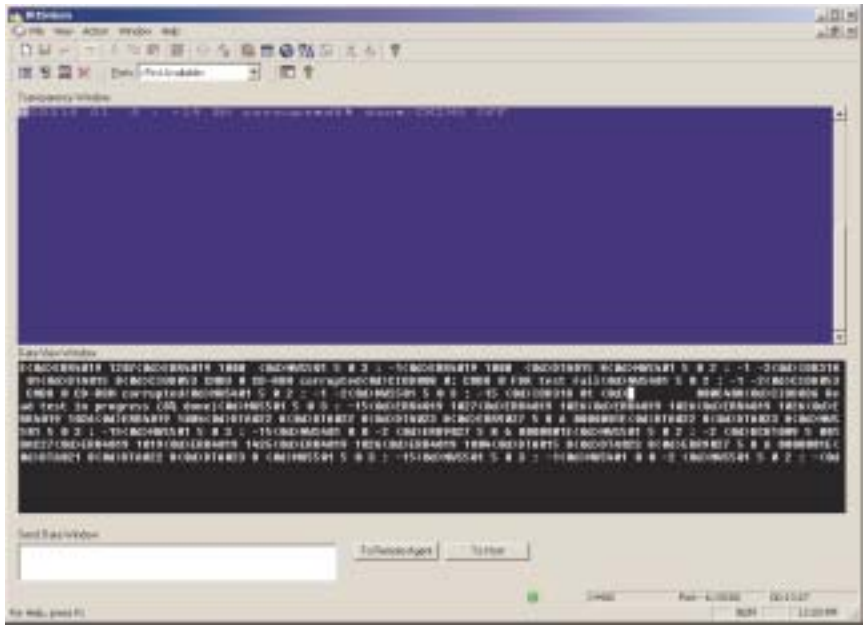
The Passive mode transparency window contains two areas: Transparency Window and Data View Window. The Transparency Window appears at the top of the screen. It displays data sent from the host device to the SEBea/NET-PATH. The Data View Window appears at the bottom of the screen. It displays data transmitted to and from the host device and the SEBea/NET-PATH. Data originating at the host device appears in reverse video mode. Data originating from the SEBea/NET-PATH appears in normal mode. You cannot enter commands while in Passive mode.

Active Bridge Transparency

To establish Active Bridge transparency with the host device

Do one of the following:

- Choose Action > Transparency – Active Bridge.
- Right-click a remote agent; then, select Active Transparency from the menu.



The Active Bridge window contains three areas: Transparency Window, Data View Window, and Send Data Window. The Transparency Window displays the data transmitted from the host device or SEBea/NET-PATH to the user. The Data View Window displays data transmitted to and from the host device and SEBea/NET-PATH. You can send data to the host device or SEBea/NET-PATH by entering commands in the Send Data Window, and then clicking the To Host button (to send commands to the host device), or the To Remote Agent (to send commands to the SEBea/NET-PATH).

Override Terminal Type

While transparent with a host device, you may wish to use a different emulation program than the one used to connect with the host. Use IRISnGEN's Override Terminal Type feature to select a new emulation program, use the default program, and/or save the new program as the default.

To use the Override Terminal Type feature

1 Do one of the following:
- Choose Action > Override Terminal Type.
- Right-click the Transparency window; then select Override Terminal Type.

IRISnGEN displays the Select Emulation dialog.



2 Do one of the following:
- Click the **Use default emulation** radio button to use the emulation selected for the host device.
- Click the **Override/change emulation** radio button; then select a new emulation from the list.

3 Select the **Make this the default emulation for the host** checkbox if you want IRISnGEN to replace the existing emulation selection in the Host record with the new one.

Using Command Line Interface Commands

Once you establish a transparent connection, you can enter commands that instruct the SEBea/NET-PATH remote agent or the host to perform an action.

To obtain a list of allowable commands for use with the SEBea/NET-PATH

- Type **help** at the command line, as shown below.

```
SEBea> help
```

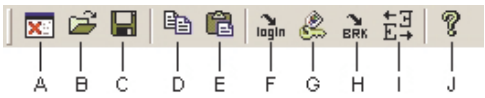


Caution *Some commands can have harmful effects. Do not execute a command unless you are fully aware of its impact.*



Transparency Window Toolbar

Notice that the icons on the toolbar change when you open a transparency window. Use these icons to perform a variety of functions while in transparent mode.



A. *End Transparency* ***B.*** *Open File* ***C.*** *Capture to log* ***D.*** *Copy text*
E. *Paste text* ***F.*** *Send Host Login* ***G.*** *Send Host Password* ***H.*** *Send Break*
I. *Local Echo* ***J.*** *Transparency Status*

Ending transparency

To end transparency

- Click the icon.

Opening a file

While in transparent mode, you can open a file on your PC and copy and paste the information into your transparent window using standard windows copy and paste commands. This is very helpful when you must enter a complicated command or a long path name.

To open a file

1 Click to display the Open dialog.



2 Navigate to the directory containing the file you wish to open.



Note *The default file type is .log. If you wish to open other file types—for example, a .txt file—select that file type from the Files of type list.*

3 Highlight the file name and click ***Open***.

Capturing to a Log File

You can save all the information appearing in the transparency window by capturing it to a log file. This can be very helpful when you are monitoring a port and need to save information about the attached host for later review.

To capture to a log

1 Click to display the Save As dialog.



2 Navigate to the directory you wish to store the log.



Note *The default file type is .log. If you wish to open other file types—for example, a .txt file—select that file type from the Files of type list.*

3 Enter the file name of the log.

4 Click ***Save***.

Copying and Pasting Text

You can copy and paste text to and from the Clipboard. When you use Copy, the copied text remains on the Clipboard until you choose Copy again.

To copy text

1 Highlight the text you wish to copy.

2 Do one of the following:

- Choose Action > Copy Text.
- Click the icon.

To paste text

1 Move the cursor to the point where you want to insert the text.

2 Do one of the following:

- Choose Action > Paste Text.
- Click the icon.



Sending Host Login Information

Some host devices require special login information—for example, a particular character sequence—before you can communicate with them. If you entered transparent mode and need to send your host device login information, you can send that information using the Host Login function.

To send host login information

Do one of the following:

- Choose Action > Send Host Login.
- Click the icon.



Note *For the Host Login function to work correctly, you must enter the information in the Host Information fields on the Host tab first, see "Host', page 2-15.*

Sending Host Password

Some host devices require a password before you can communicate with them. If you entered transparent mode and need to send your host device a password, you can do so using the Host Password function.

To send a host password

Do one of the following:

- Choose Action > Send Host Password.
- Click the icon.



Note *For the Host Password function to work correctly, you must enter it in the Host Information fields on the Host tab first, see "Host', page 2-15.*

Sending Break

Some host devices require that you send them a break command before you can communicate with them—for example, the host requires a break before displaying a prompt. Use the Send Break function to send a break.

To send a break command

Do one of the following:

- Choose Action > Send Break.
- Click the icon.

Turning on Local Echo

You can use Local Echo to repeat the text typed in back to the screen and or use it to echo to a peripheral on the IRISnGEN system, such as a COM port.

To turn on/off local echo

Do one of the following:

- Choose Action > Local Echo.
- Click the icon.

Viewing Transparency Status

While in transparency mode, you can check the status of your session.

To view your transparency status

- Click the icon to display the Transparency Status window, shown below.



Send Database

The SEBea/NET-PATH remote agent receives its unique identification and operating parameters, including the Site ID, password, trigger words, action tables, and telephone numbers through downloading. You can program these parameters in IRISnGEN and then download them to the SEBea/NET-PATH using Remote Agent Manager.



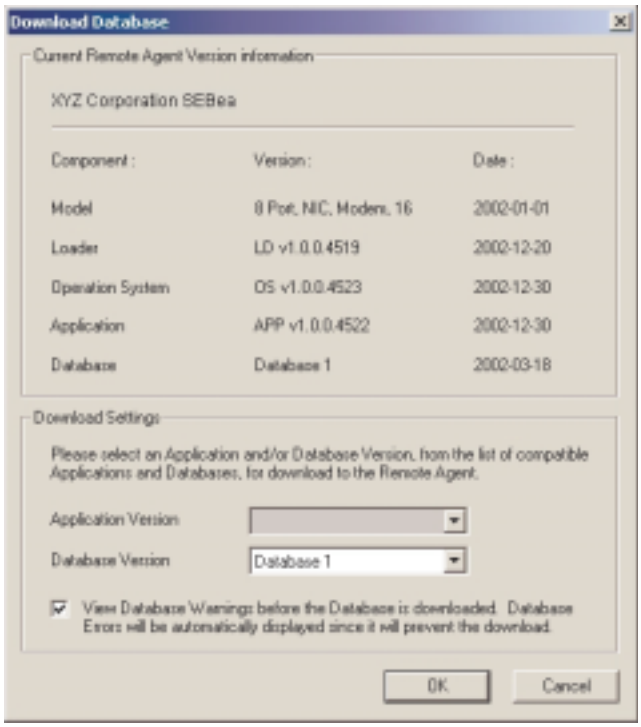
Warning *Sending a database to the SEBea/NET-PATH erases the stored data in the SEBea/NET-PATH. If you want to retain stored data, you must poll the SEBea/NET-PATH before sending the new database.*

To send a database to the SEBea/NET-PATH

1 Do one of the following:
- Choose Action > Send Database.
- Right-click a remote agent and choose Send Database from the pop-up menu.
- Click the Send Database icon ( ).



The Download Database dialog appears.



2 Select a database version from the **Database Version** list.

3 Click ***OK***.



Note *The Application Version field appears grayed. You cannot select an application version when you choose the Send Database function.*



Note *All Enumeration changes are incorporated into the Remote Agent XML database automatically. However, compatibility issues may arise when downloading a database to a remote agent. Databases created with newer IRISnGEN system cannot be loaded in other remote agents. Databases created with other IRISnGEN systems can be loaded into newer remote agents. Enumeration features are automatically incorporated in remote agent versions SEBea 7.1.2, NET-PATH 3.1.2, and later versions.*

Send Application

The system application controls most of the SEBea/NET-PATH's features and functions—for example, booting the SEBea/NET-PATH, validating system licenses, downloading databases, initializing serial ports, and processing and delivering event information, to name a few. Use the Send Application function to download a system application program to the SEBea/NET-PATH remote agent.

To send an application to the SEBea/NET-PATH

1 Do one of the following:

- Choose Action > Send Application.
- Right-click a remote agent; then, select Send Application from the pop-up menu.
- Click the Send Application icon ( ).

The Download Application dialog appears..



2 Click the down arrow and choose the application version you want to download.



Note *Sending the application to the SEBea/NET-PATH removes the database. The "New Available" indicator lets you know a newer version of the application is available for your system.*

3 Click ***OK***.



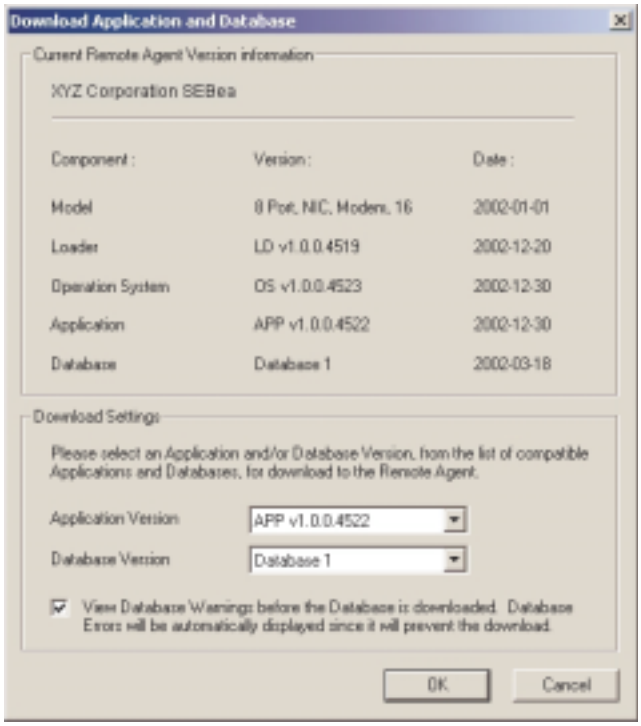
Note *The Database Version field appears grayed. You cannot select a database version when you choose the Send Application function.*

Send Database and Application

You can send both a database and an application to the SEBea/NET-PATH, if you choose.

To send a database and application to the SEBea/NET-PATH

1 Click the icon. The Download Application dialog appears.



2 Select an application from the **Application Version** list.
3 Select a database from the **Database Version** list.
4 Click ***OK***.

Send Operating System

The SEBea/NET-PATH's operating system is a modified version of the system application. It initializes the SEBea/NET-PATH in the event the system application is missing or is corrupt. The operating system can boot the SEBea/NET-PATH, initialize the modems, the serial ports, and the user interface (the LCD on the front panel). Use the Send Operating System function to download new versions of the operating system to the SEBea/NET-PATH remote agent.

To send an operating system to the SEBea/NET-PATH

1 Do one of the following:
- Choose Action > Send Operating System.
- Right-click a remote agent; then, select Operating System from the pop-up menu.
- Click the Operating System icon ( ).



You can check the results in the History pane.

Send Loader

The Loader module manages the tasks that boot the SEBea/NET-PATH, load and execute existing application programs. The Loader is written into flash memory at the factory, but you can replace it later, if you choose. Use the Send Loader function to replace a loader module in your SEBea/NET-PATH remote agent.



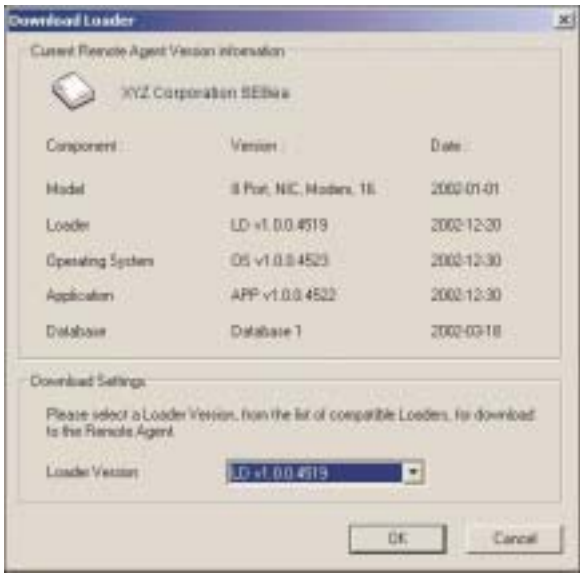
Note *For the SEBea/NET-PATH to work properly, you must download a Loader module compatible with the application and operating system downloaded to your SEBea/NET-PATH. If you are unsure, check with your system administrator before using the Send Loader function.*

To send a loader to the SEBea/NET-PATH

Do one of the following:

- Choose Action > Send Loader.
- Right-click a remote agent; then, select Loader from the pop-up menu.
- Click the Loader icon ( ).





You can check the results in the History pane.



Note *For the loader to download successfully, the SEBea/NET-PATH remote agent device must already have a database loaded and its battery must be charged (50% or higher).*

Send Date and Time

Occasionally, you may need to change the date and time programmed in your SEBea/NET-PATH remote agent device. Use the Send Date and Time function to send your IRISnGEN server's date and time to the SEBea/NET-PATH remote agent device.

To send the date and time to the SEBea/NET-PATH

Do one of the following:

- Choose Action > Send Date and Time.
- Right-click a remote agent; then, select Send Date and Time from the pop-up menu.
- Click the Send Date and Time icon ( ).

Remote Agent Manager sends the date and time to the SEBea/NET-PATH remote agent, based on the time zone information for that remote agent. You can check the results in the History pane.

Get and View Database

Use the Remote Agent Manager's Get and View Database function lets you retrieve the database stored in your SEBea/NET-PATH and display it as an XML file in Internet Explorer. Use this function to quickly review the contents of your entire database.



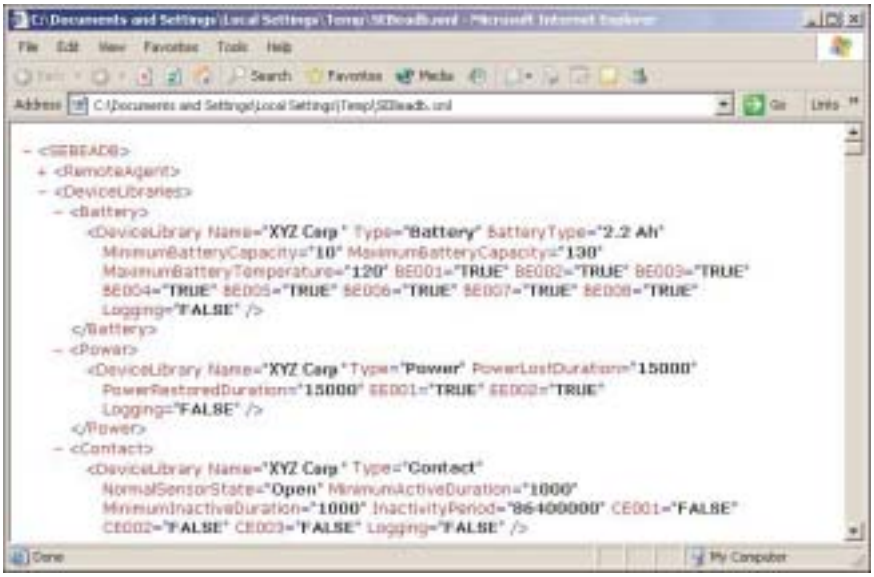
Note *You cannot edit or download the XML file to the SEBea/NET-PATH remote agent. You must make and download all changes to the SEBea/NET-PATH database using IRISnGEN.*

To get and view the SEBea/NET-PATH database

Do one of the following:

- Choose Action > Get and View Database.
- Right-click a remote agent; then, select Get and View Database from the pop-up menu.
- Click the Get and View Database icon ( ).

The Internet Explorer window appears displaying the contents of your database.



Send and Retrieve Files

You can send user files to or retrieve them from the SEBea/NET-PATH remote agent. The SEBea/NET-PATH stores your files in its root directory in either flash or RAM memory. For example, you may want to send a file containing information that a script file uses when performing a task. Later you can retrieve the contents of another file that contains the results of the executed script.

To send a file to the SEBea/NET-PATH

1 Do one of the following:

- Choose Action > Send File.
- Right-click a remote agent; then, select Send File from the pop-up menu.
- Click the Send File icon ( ).





2 Select the file you want to send.

3 Select either Flash or RAM from the **Media Type** list.

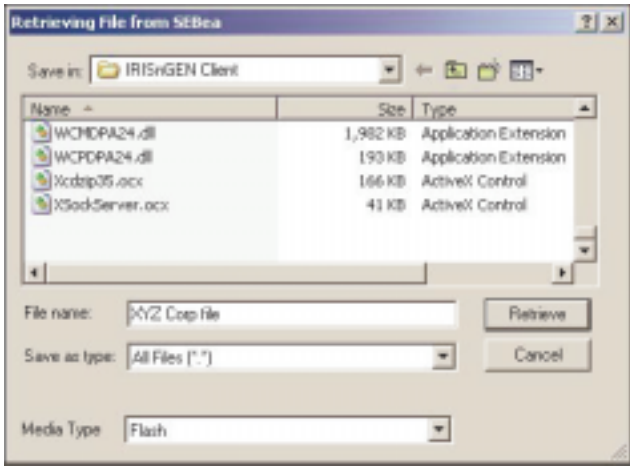
4 Click ***Send***.

Remote Agent Manager sends the file to the SEBea/NET-PATH remote agent. You can check the results in the History pane.

To retrieve a file from the SEBea/NET-PATH

1 Do one of the following:

- Choose Action > Retrieve File.
- Right-click a remote agent; then, select Retrieve File from the pop-up menu.
- Click the Retrieve File icon ( ).



2 Select the folder where you want to store the retrieved file.

3 Type the name of the file you want to retrieve.

4 Select either Flash or RAM from the **Media Type** list. Click ***Retrieve***.

Remote Agent Manager retrieves the file from the SEBea/NET-PATH remote agent. You can check the results in the History pane.

Lock and Unlock the Remote Agent

You can lock your SEBea/NET-PATH or NET-PATH remote agent to prevent unauthorized access. When locked, only authorized users can gain access to the remote agent using Remote Agent Manager. They cannot use other protocol programs—for example, Procomm and Telnet—to access the remote agent until you unlock it.

To lock the SEBea/NET-PATH

Do one of the following:

- Choose Action > Lock.
- Right-click a remote agent; then, select Lock from the pop-up menu.
- Click the Lock icon ( ).

The remote agent remains locked until you issue the Unlock command.

To unlock the SEBea/NET-PATH

Do one of the following:

- Choose Action > Unlock.
- Right-click a remote agent; then, select Unlock from the pop-up menu.
- Click the Unlock icon ( ).

When unlocked, users can also access the remote agent using a protocol program, such as Procomm.



Note *Your remote agent will automatically lock when the number of unsuccessful login attempts exceeds the retry limit. Your system administrator or authorized user must use Remote Agent Manager to unlock the remote agent. For more information about locking the remote agent, see "System Device Library', page 6-23.*

SEB II Remote Agent Manager Functions

The following discusses the Remote Agent Manager functions used with SEB II remote agents. See page 7-8 for a discussion of SEBea/NET-PATH remote agent functions and page 7-44 for foreign agent functions.

Edit Remote Agent Database

You can use the Edit Remote Agent Database function to make changes to your SEB II database. Choosing this function invokes the SEB II Database Manager program from which you can access the database fields.

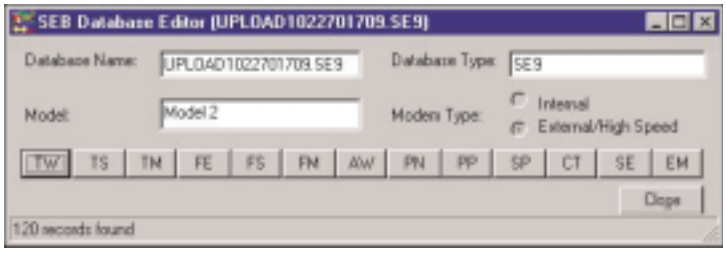
To edit the SEB II database

1 Do one of the following:

- Choose Action > Edit Remote Agent Databases.
- Right-click a remote agent; then, select Edit Remote Agent Databases from the pop-up menu.
- Click the Edit Remote Agent Databases icon ( ).

Remote Agent Manager displays the SEB Database Editor dialog box.





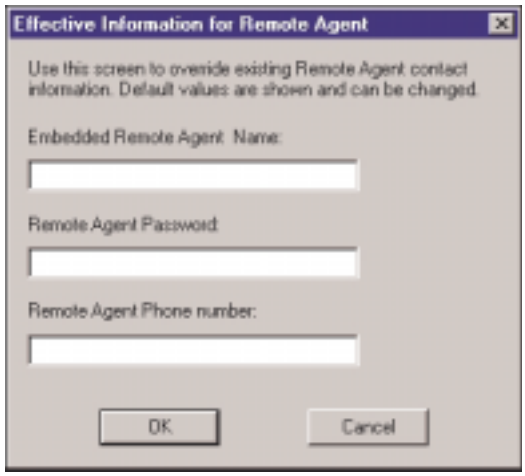
2 Click a button to open a database table—for example, click TW to open the Trigger Word table and end the appropriate fields.

See Chapter 8 for more information about SEB II databases.

Effective Information

You can use the Effective Information function to quickly access SEB II remote agents without reading each SEB II's database into memory.

If you have not yet downloaded a database to the SEB-II remote agent, you can still communicate with it using the Effective Information functions. Enter the SEB II remote agent name, password, and telephone number in the appropriate fields.



To display the Effective Information dialog

Do one of the following:

- Choose Action > Effective Information.
- Right-click a remote agent; then, select Effective Information from the pop-up menu.
- Click the Effective Information icon ( ).

To override the SEB II's effective information

1 Enter the information you wish to use to override (replace) in the fields displayed in the Effective Information dialog screen, shown below.

2 Type a new name to override the embedded remote agent ID in the **Embedded Remote Agent Name** field.

3 Type a new password to override the current remote agent password in the **Remote Agent Password** field.

4 Enter a new telephone number to override the current remote agent phone number in the **Remote Agent Phone Number** field.

5 Click ***OK***.

Get Status

You can use the Get Status function to check the settings for each remote agent. The number of fields may vary slightly depending on your remote agent model. The Remote Agent Status window contains three tabs (General, Ports, Miscellaneous) that display information for the remote agent you select from the Remote Agent Manager's tree view.

To get the SEB II status

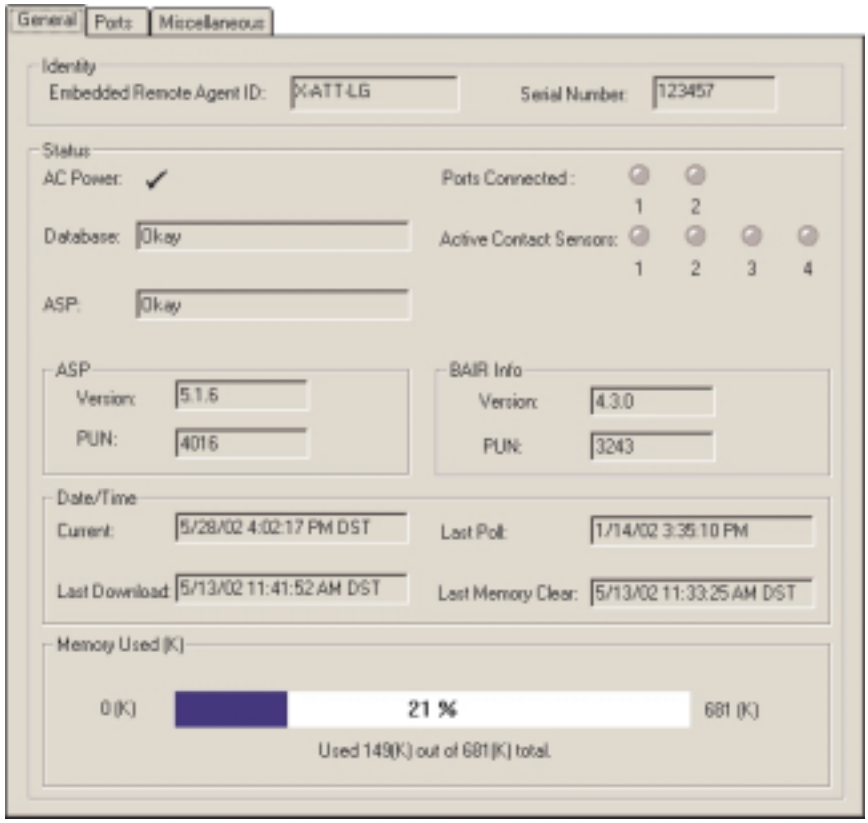
1 Do one of the following:

- Choose Action > Get Status.
- Right-click a remote agent; then select Get Status from the pop-up menu.
- Click the Get Status icon ( ).

2 Click a tab to view the status information for that category. You cannot alter any field on the Status information tabs.

Remote Agent Status: General Tab

The General Tab displays identity, date and time stamps for remote agent functions, hardware and software component status, and on-board memory status.



The following describes the read-only fields that display on the General tab.

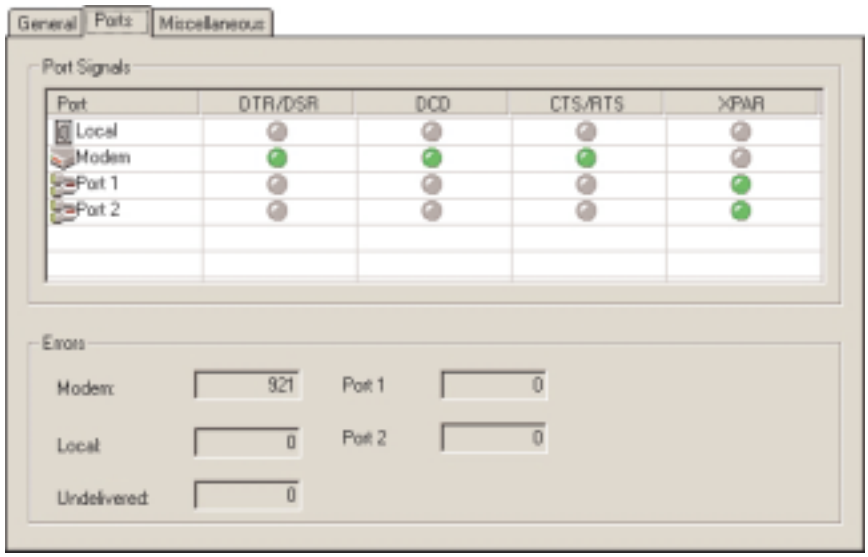
Field	Description
Identity	
Embedded Remote Agent ID	This is the remote agent device identification. This is a name stored in the memory of the remote agent. Every remote agent has a special identity.
Serial Number	This field displays the manufacturer's serial number of the remote agent.
Status	
AC Power	A check indicates power is on, an X indicates power is off.
Ports Connected	A green bubble indicates the port is connected. Red indicates the port is not connected.
Database	This field displays information about the remote agent’s database status.
Active Contact Sensors	A green bubble indicates the contact sensor is active. Red indicates the port sensor is not active.
ASP	This field displays information about the remote agent’s ASP status.
ASP and BAIR Info	These two fields display release information about the operating and application software in the remote agent. The BAIR (Basic Application Interface Routine) controls the detection and operation of the remote agent hardware. Its instructions are stored on the EEPROM. The ASP (Application Specific Program) controls the database functions available to the user. The ASP is the interface between the database and the BAIR. The ASP resides in RAM. Users can download newer versions as they become available.
Date/Time	
Current	The remote agent reports these values according to its internal clock. The remote agent reports the date in the mmddyy format, followed by the time in the hh:mm format. You can set the date and time using the Download option.
Last poll	This field shows the last date and time the remote agent was polled for stored data.



Last download	This field shows the date and time that Remote Agent Manager last downloaded a database to the remote agent.
Last memory clear	This field shows the date and time that all stored data were last erased from the remote agent's memory.
Memory Used (K)	This field indicates the amount of the remote agent's available memory that is used. If the memory threshold is reached, a message displays in red along with a description.

Remote Agent Status: Port Tab

The Ports Tab displays the status of the ports located on the remote agent and the status of hard alarms.



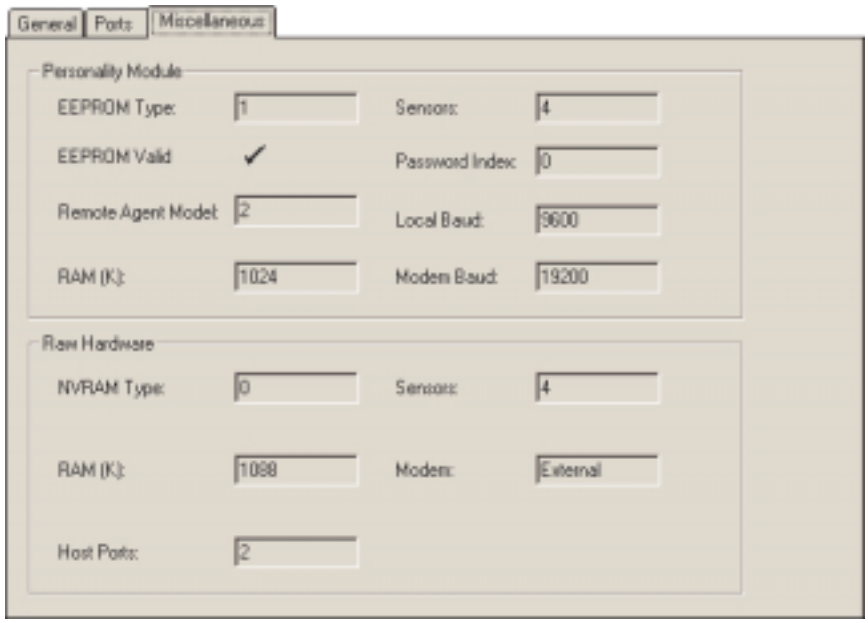
The following describes the read-only fields that display on the Ports tab.

Field	Description
Port Signals	The port signals data table shows each port on the remote agent along with its status.
Ports	Shows the port name/or number.
Port Connectivity	Indicates when a host is attached to the remote agent. This field does not apply to the local and modem ports. The port connection status maps directly to fixed events FE15 through FE18 and FE30 through FE33. An image indicates connection to the port as follows: = host connected = no host connected

Port Activity	This column indicates port activity. The ✓image indicates that there is port activity. The image indicates that there is no port activity. The port activity status maps directly to fixed events FE19, FE20, FE34, and FE35.
DTR/DSR, DCD, CTS/RTS, and TRANSPARENCY	These columns show the status of the RS232 control leads. A green bubble indicates the signal is on. A gray bubble indicates the signal is off.
Errors	The status fields in this area display the number of errors that occurred on the ports during attempts to deliver alarms.
Contact Sensors	This area displays any hard contacts located on the remote agent. A red bubble indicates the contact is on. A gray bubble indicates the contact is off. These status indicators map to fixed events FE1 through FE8 and FE22 through FE29.

Remote Agent Status: Miscellaneous Tab

The Miscellaneous tab displays Personality module and raw hardware status information about the remote agent. This is an information-only page. You cannot alter any field on this page.



The following describes the fields on the Miscellaneous tab.

.

Field	Description
Personality Module	
EEPROM Type	This field displays the current EEPROM type. A “0” indicates a 32 byte PROM. A “1” indicates a 128 byte PROM.
EEPROM Valid	If the EEPROM is valid for your system, a check mark appears in this field.
Remote Agent Model	This field displays the model of the remote agent device.
RAM (K)	This field shows the amount of memory allocated for use in the remote agent. SEB remote agents come equipped with 128Kb, 256Kb, 512KB, 1Mb, or 2Mb of memory.
Sensors	Shows how many of the sensors are made available though the firmware. This number is usually the same as the number of physical inputs.
Password Index	This field displays the index number of an optional customer, emergency password. You can use any number, except “0,” to indicate the customer is using this option.
Local Baud	This field shows the default baud rate of the local port on the remote agent device.
Modem Baud	This field shows the default baud rate of the internal or external modem.
Raw Hardware	
NVRAM Type	This field shows the type of non-volatile RAM in the remote agent device.
RAM (K)	This is the amount of physical RAM included in your remote agent device.
Host Ports	This field shows the number of physical ports available on your remote agent device.
Sensors	Shows the number of sensors on the remote agent devices.
Modem	This is the type of modem your remote agent device uses.



Polling

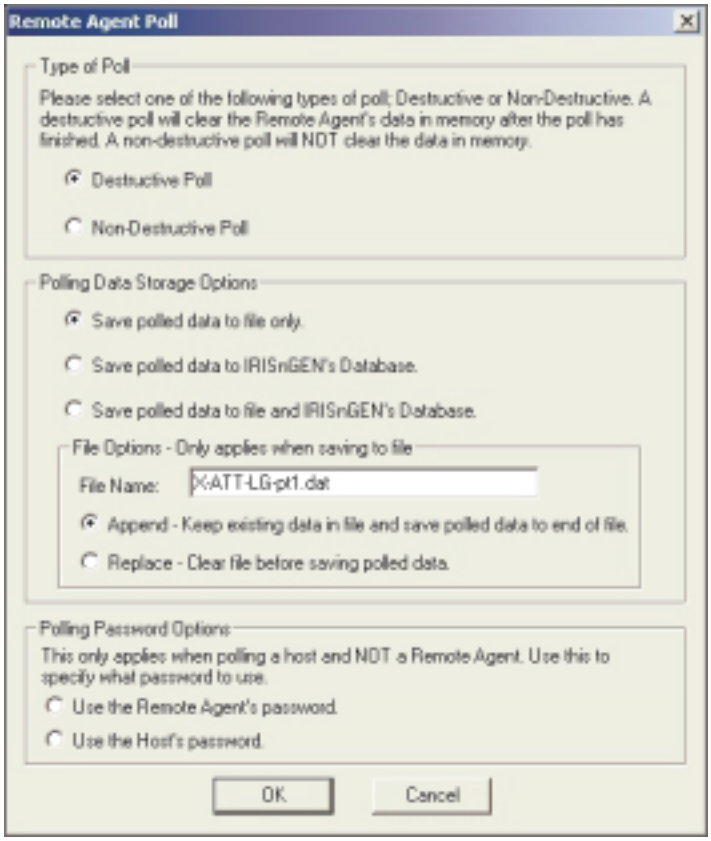
Remote Agent Manager retrieves data stored in the remote agent using the Poll option. Two types of polling are available: destructive and non-destructive. A destructive poll gathers all data a block at a time, and then clears each block of data from the remote agent's memory when Remote Agent Manager acknowledges that it received the block. A non-destructive poll copies the data, but leaves the remote agent memory intact.

You can also poll all the data or selective data in the SEB II. Selective polling requires that the SEB II is programmed with a regular application program of 4.5.X or above or an SCL application of 5.2.X or above.

To poll an SEB II

1 Do one of the following:

- Choose Action > Polling.
- Right-click a remote agent; then, select Polling from the pop-up menu.
- Click the Polling icon ( ]↔[ ).



2 Click a **Type of Poll** radio button to select a poll type.

Button	Description
Destructive Poll	As each block of data is received and acknowledged by the Remote Agent Manager, it is cleared from the SEB II's memory.
Non-Destructive Poll	A non-destructive poll copies the data, but leaves the remote agent memory intact.

3 Click a **Polling Data Storage Options** radio button define where you want the polled data stored.

Button	Description
Save polled data to file only	Store the polled data in the location specified in File Options (File Name textbox).
Save polled data to IRISnGEN's Database	Store data in the IRISnGEN database. To use this option, the alarms polling application must be assigned in the Host record.
Save polled data to file and IRISnGEN Database	Store data in both the file and the database. The Alarms polling application must be assigned in the Host record.

4 Type the name of the file used to store polled data in the **File Name** field. Be sure to add the .dat extension.

5 Click a **File Options** radio button to define how the system is to maintain the file.

Button	Description
Append	Keep the existing data in a file and save polled data to the end of the file.
Replace	Clear the file before saving the polled data.

Polling Password Options

The Password Options only apply when polling a Host. Select a radio button to poll using a password. Your options are:

- Use the remote agent's password
- Use the host's password

The polling process is completely automatic. When you click the OK button, Remote Agent Manager contacts the remote agent or host you selected. You can follow the progress of the poll in the History pane.

To selectively poll

1 Select a host from the IRISnGEN tree view.

2 Click the]↔[icon.

3 Select the appropriate Polling Password Options for your operation from the choices at the bottom of the Remote Agent Poll window.

To cancel polling

- Click ***Cancel***.



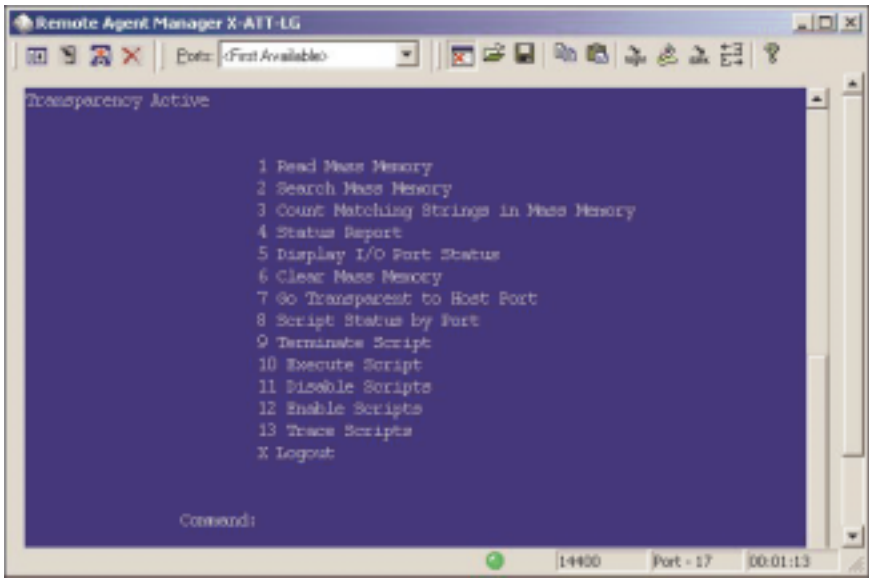
Transparency

Remote Agent Manager includes a transparency function so that you can communicate directly with both a remote agent and host device. Use this function when debugging or troubleshooting problems. Review stored data, check the status of your SEB II, or establish interactive communications with the host device.

To go transparent to the SEB II

Do one of the following.

- Choose Action > Transparency.
- Right-click a remote agent; then, select Transparency from the pop-up menu.
- Click the Transparency icon ( ).



The following describes the interactive menu items:

Item	Description
1 Read Mass Memory	Reads the contents of the remote agent memory (collected data only) one line at a time. The format is similar to the manual poll file.
2 Search Mass Memory	Scans the remote agent memory for a specific data string. You may perform a search on the data, not on the header information.
3 Count Matching Strings in Mass Memory	Counts the number of occurrences of a string in remote agent memory. You must specify a port number. You can use wildcards (as defined in the SP table).
4 Status Report	Lists information similar to the Status requested from the Online menu.

5 Display I/O Port Status	Lists information about each port on the remote agent. If there are any errors on the port, this option will show what type of error occurred last.
6 Clear Mass Memory	Removes all stored data from the remote agent's memory. The ASP and database remain intact.
7 Go Transparent to Host Port	Select a host port to connect to the host on that port. The status bar reflects Remote Agent Port 0 and the terminal emulation for the remote agent rather than the host port when you select this option.
8 Script Status by Port	Shows when scripts are executing or when they are queued to execute. Scripts execute serially on each port, but may execute simultaneously on separate ports. The script status also shows if the trace feature is enabled.
9 Terminate Script	Stops a script that is executing. The port number on which the script is running must be supplied. Select immediate or Graceful termination. Graceful termination is effective only if the proper commands are embedded in the scripts.
10 Execute Script	Allows you to execute manually a script stored in the remote agent. You are required to choose the number of the script to execute.
11 Disable Scripts	Stops execution of all scripts on the port you select.
12 Enable Scripts	Allows scripts to execute on the port you select. This option is not retroactive. Only scripts started after selecting this option will run.
13 Trace Scripts	Trace Scripts is a troubleshooting tool. When trace is enabled, each step the script performs is written to the remote agent's mass memory as a port 6 entry. The script writer can then find causes of problems in the script and correct them. Do not leave Trace Scripts enabled after troubleshooting completes. It significantly hampers the performance of the scripts.
X Logout	Enter X to logout of the remote agent interactive menu, and then click the Disconnect button at the Remote Agent Manager window to end your communication session.



Going Transparent with a Host Device

With the Transparent option, you can use your remote agent as a modem to set up a transparent communication link with the host device. In Transparent mode, the remote agent automatically matches the baud rate and communication options between the host port and modem port link.

The Transparency window appears automatically when IRISnGEN establishes the communication link. The title bar displays the active remote agent identification. The status bar displays the host name, host type, connected port, communication speed, port settings, and active emulation type. A green bubble on the status bar indicates you are connected and a red bubble indicates you are not.

You can use the Transparency toolbar icons to choose your options.

The Transparency toolbar icons work similar to those used by the SEBea/NET-PATH. See ”Transparency’, page 7-37 for a complete description of each icon function.

Get Database

Use the Remote Agent Manager’s Get Database option to upload (transmit) a remote agent’s database. Once uploaded to change the Remote Agent Manager, you can change the characteristics of a remote agent then download the database to that remote agent.

To get a remote agent database

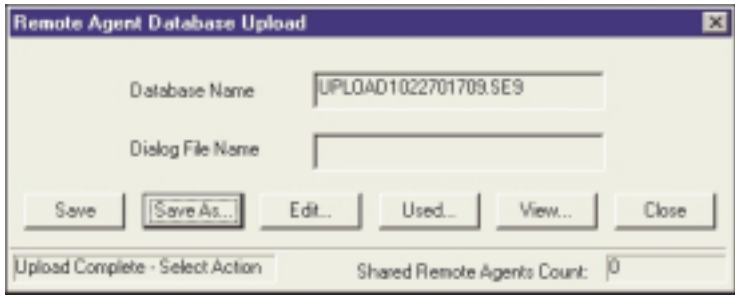
Do one of the following:

- Choose Action > Get Database.
- Right-click a remote agent; then, select Get Database from the pop-up menu.
- Click the Get Database icon ( ).

The upload procedure only takes a few minutes to complete. Should the upload fail, correct the problem, then re-select Get Database to restart the process. Once the system successfully uploads the database, it displays the Database Upload dialog.

If the remote agent has a database, that database name appears in the Database Name field. If it does not have a name, the database name “UPLOAD” appears.

When the Database Upload dialog box appears, choose an action by clicking its button.



The following describes the fields and buttons on the dialog.

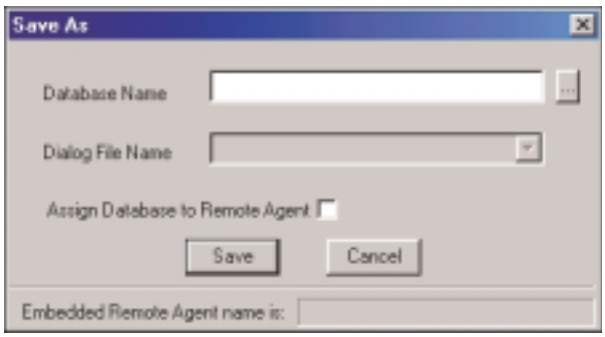
Button	Description
Save	Overwrite the previous data contained in the named database. This button activates when a remote agent has a database.
Save As	Save the uploaded database to a name other than the one in the Database Name field. This will prevent you from overwriting an existing database.
Edit	Load the Database Editor program. The Database Editor program lets you change the uploaded data before saving it, or downloading it to the remote agent.
Used	Display a list of other remote agents that share this database. This will only apply when the database exists within the IRISnGEN system.
View	Display the embedded remote agent name, password, and self-check time.
Close	Exit this dialog.

Save As Dialog

Use the Save As dialog to save the database with a specific name.

To use the Save As dialog

1 Click the ***Save As*** button on the Remote Agent Database Upload dialog. The system opens the Save Ad dialog.



2 Type a database name in the **Database Name** field.

3 Select a dialog name from the **Dialog File Name** list.

4 Select the **Assign Database to Remote Agent** checkbox to link this database with the remote agent.

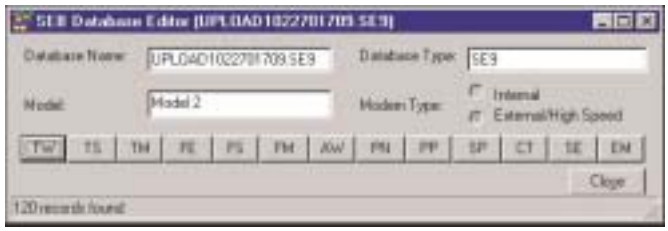
5 Do one of the following:

- Click ***Save*** to save the database information.
- Click ***Cancel*** to exit the Save As operation.



Edit Dialog

Selecting the Edit button from the Upload dialog displays the SEB Database Editor dialog (shown below). Use this dialog to edit the SEB's database. See Chapter 8 for a complete description of this option.



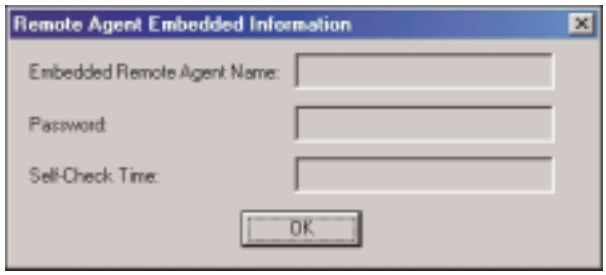
Used Dialog

When you choose the Used button from the Upload dialog, the IRISnGEN system displays the Used dialog. Use this dialog to display a list of remote agents that share the same database.



View Dialog

Selecting the View button from the Remote Agent Database Upload dialog displays the Remote Agent Embedded Information dialog. Use this dialog to display the embedded remote agent name, password, and self-check time.



Click ***OK*** to exit this dialog.

Send Database and ASP

A remote agent receives its features and functions through downloading. You can program these functions using Remote Agent Manager, and then download them to the remote agent.

For a remote agent to function properly, you must download two software components: the Application Specific Program (ASP) and the database. The ASP gives the remote agent most if its functions and features. The database gives the remote agent its unique identification and operating parameters, including the Site ID, password, trigger word an action tables, and telephone numbers.



Note *If the remote agent already has a database, upload that database before making any changes. However, if the remote agent does not have a database, choose one in the Dynamic window.*

To download (send) to a remote agent

1. Select the remote agent you wish to download to from the Remote Agent Manager's tree view.
2. Select one of the following:

   Send Database to Remote Agent - Select this option to download only database information. If you use this option when downloading an SE9 database, the system will erase any data stored in mass memory. Remote Agent Manager will prompt you before proceeding.

   Send Application - Select this option when upgrading the ASP program in the remote agent. Selecting this option causes the system to erase the database and any data stored in mass memory. The system will not prompt you before proceeding.

   Send Both Database and ASP - Select this option to define the characteristics of a remote agent that does not have an ASP or a database. Selecting this option will cause the system to erase the database and any data stored in mass memory.

   - To down load an ASP, choose an ASP from the list.
   - To download a Database, choose a database from the list.



Note *The Dialog File Name field displays the dialog file name associated with the database name you chose above. You cannot change this field.*

3. Click ***OK*** to begin, or ***Cancel*** to end the procedure.

Once started, downloading is automatic. If the remote agent is not already online, Remote Agent Manager dials the remote agent, enters the password and Site ID information, and then establishes a communication link. As the remote agent acknowledges that it successfully received the first block of data, its writes over the old database. If a download fails before it completes, the remote agent will not have a database. You must restart the download procedure.

Remote Agent Manager informs you of its progress in the History window.

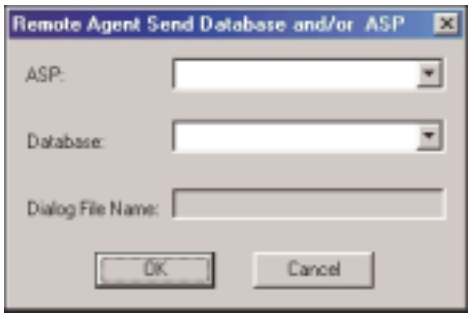


Remote Agent Send Database and ASP Dialog

The Remote Agent Send Database and ASP dialog appears when you download a database and an ASP to the remote agent.

To send a database and ASP

1 Click the icon.



2 Select an ASP for download to the remote agent from the **ASP** list.

3 Select a database for download to the remote agent from the **Database** list.

4 The **Dialog File Name** field is read-only and lists the dialog file name associated with the database named above.

5 Click ***OK*** to send this ASP and database to the remote agent.

Send Date and Time

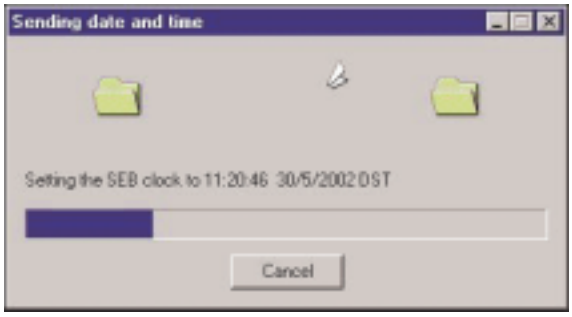
Occasionally, you may need to change the date and time programmed in your SEB II remote agent device. Use the Send Date and Time function to send your client server's date and time to the SEB II remote agent device.

To send the date and time to the SEB II

Do one of the following:

- Choose **Action > Send Date and Time**.
- Right-click a remote agent; then, select **Send Date and Time** from the pop-up menu.
- Click the Send Date and Time icon ( ).

Remote Agent Manager displays a dialog showing you its progress. You can check the results of the send in the History pane.



Foreign Agent Remote Agent Manager Functions

You can perform a limited number of Remote Agent Manager functions when managing a foreign remote agent. The following discusses the Remote Agent Manager functions used with foreign remote agents. See ”SEBea/NET-PATH Remote Agent Manager Functions’, page 7-8 for a discussion of SEBea remote agent functions and ”SEB II Remote Agent Manager Functions’, page 7-28 for SEB II functions.

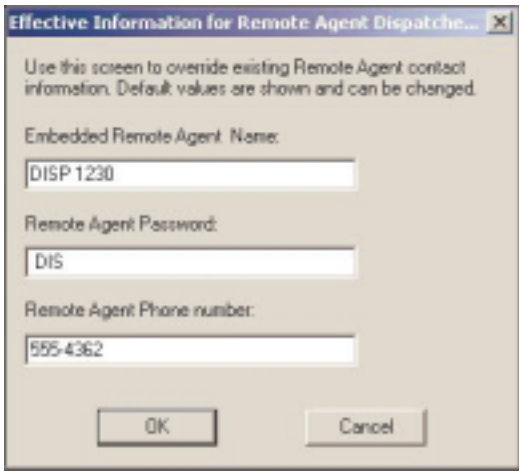
Effective Information

You can use the Effective Information function to quickly access foreign remote agents without reading each foreign agent’s database into memory.

To display the Effective Information screen

Do one of the following:

- Choose Action > Effective Information.
- Right-click a remote agent; then, select Effective Information from the pop-up menu.
- Click the Effective Information icon ( ).



To override a foreign agent’s effective information

1. Type a new name to override the embedded remote agent ID in the **Embedded Remote Agent Name** field.
2. Type a new password to override the current remote agent password in the **Remote Agent Password** field.
3. Type a new telephone number to override the current remote agent phone number in the **Remote Agent Phone Number** field.
4. Click ***OK***.

Transparency

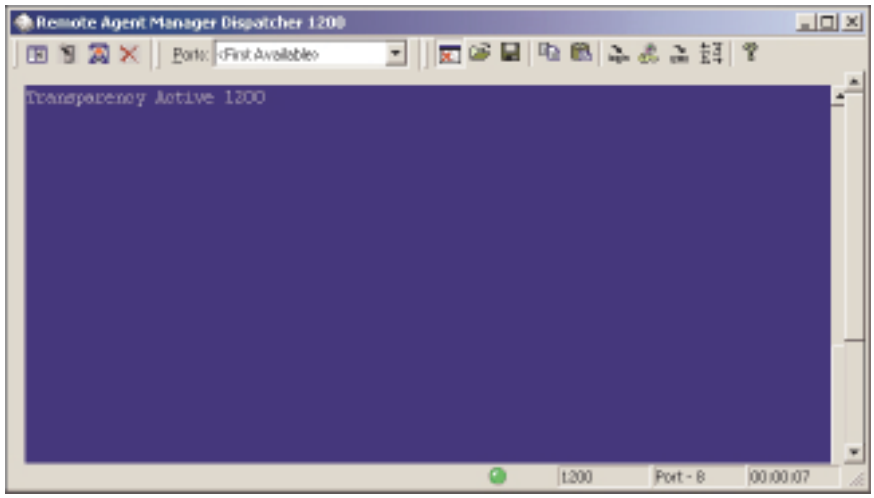
You can use Remote Agent Manager to communicate directly with both a foreign remote agent and its host device. Use this function to debug or troubleshoot problems, to review stored data, check the status of your foreign remote agent, or to establish interactive communications with the host device.

To go transparent to the foreign remote agent

1 Do one of the following:

- Choose Action > Transparency.
- Right-click a remote agent; then, select Transparency from the pop-up menu.
- Click the Transparency icon ( ).

The Transparency dialog box appears.



2 Type your interactive commands.

Going Transparent with a Host Device

You can use your foreign remote agent as a modem to establish a transparent communication link with the host device. In Transparent mode, the foreign remote agent automatically matches the baud rate and communication options between the host port and modem port link.

The Transparency window appears automatically when IRISnGEN establishes the communication link. A green bubble on the status bar indicates you are connected. A red bubble indicates you are not.

You can use the Transparency toolbar icons to choose your options. The Transparency toolbar icons work like those used by the SEBea. See ”Transparency’, page 7-13 for a complete description of each icon function.

Note



8

SEB II Database Manager

Use the SEB Database Manager feature to create and manage your SEB II databases. Once saved, you can download your databases to the SEB II devices using the Remote Agent Manager utility, see Chapter 7.

To display the SEB II Database Manager dialog

1 Choose IRIS menu > SEB II Database Manager. The system opens the SEB Database Manager window.



2 Select the database name from the **Database Name** list.



Note *IRISnGEN does not require the extension of a database name relate to the type of database (for example, SE8 or SE9). However, if you are accustomed to this naming convention, you may find it easier to continue using it for the sake of clarity.*

3 Type any description or comments about this database in the **Database Description** field.

4 Select a database type that corresponds with the ASP loaded into the SEB II from the **Database Type** list. Reference the following table:

ASP	Database Type
SEB II 3.1.X	SE3
NEAX 2.0.X	SE5
SEB II 4.0.X	SE5
MITL 1.0.X	SE6
NEAX 2.1.X	SE6
SEB II 4.1.X	SE6
MITL 1.1.X	SE7
NEAX 2.2.X	SE7
SEB II 4.2.X	SE7
MITL/XMITL 4.4.X	SE8
NEAX/XNEAX 4.4.X	SE8
SEB II/XSEB II/JSEB II 4.4.X	SE8
SCL/XSCL/JSCL 5.1.X	SE9
SEB II/XSEB II/JSEB II 4.5.X	S10
SEB II/XSEB II/JSEB II 5.2.X	S11

5 Select a model (Model 1, Model 2, Model 4, or Model SP) from the **Model** list. This is the number of ports—for example, Model 2 is an SEB II with two ports.

6 Type the dialog name in the **Dialog Filename** field if the SEB II database is type SE9 or SE11. This is the SCL script. Click ***Browse*** to select the dialog. You will find the dialog in the *IRISHOME\Dlgs* directory. If you have not created a dialog to work with this database, select the default dialog *default.dlg*.

7 Click the radio button that defines the type of modem:

- **Internal** Click this button if the device has an internal modem that has a baud rate of less than 14.4 KBPS. (An internal modem is housed within the remote agent, as opposed to a stand-alone external modem.) If this device has a 14.4 KBPS baud rate, regardless or whether it is located inside or outside the SEB II housing, you do NOT designate it an internal modem.
- **External/ High Speed** Select this button if the device has an external modem or has a high-speed 14.4 KBPS modem, regardless of whether that high-speed modem is located inside or outside the SEB II housing.



Note *The reason for this designation is that the 14.4 KBPS modem board does not physically reside on the SEB II motherboard. It is external to its motherboard.*

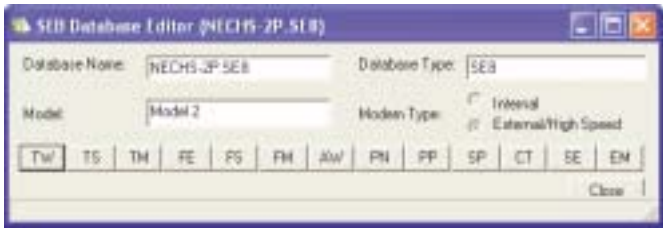
8 Do one of the following:

- Click ***Usage*** to view a list of all SEB IIs using this database. Click ***OK*** or ***Cancel*** when you are done viewing the list.
- Click ***Edit*** to edit the SEB II database currently selected.



To select a database for editing

1. Click ***Retrieve***. The system displays the first database record, which includes a description of the database, its type, model, and dialog filename.
2. Select the database you want from the **Database Name** list.
3. Click ***Edit***. The system opens the SEB II Database Editor dialog.



4. Click a button to open database table—for example, click **TW** to open the Trigger Word table.

The following sections describe each SEB II database table.

Trigger Words Table (TW)

Use the Trigger Words table to define your trigger words, where to look for them in the data stream, and what actions the SEB II should take when it finds a trigger word. You can enter up to 240 trigger words (depending on your ASP version) in this table.



Note *The order of the trigger words is very important. Trigger word matching begins with the first line and continues one line at a time, until the SEB II remote agent matches a trigger word. If you do not have the correct order, you might miss critical trigger words.*

To create a trigger word entry

1 Click the **TW** button to display the Trigger Words table.



2 Click the first TW Index number in the table to highlight it.

3 Select the number of the SEB II port attached to the host device from the **Port** list. The SEB II only searches for the trigger words defined for this port. Valid entries are 1, 2, 3, or 4.

4 In the **Starting Column** field, type the column position in the data stream where you want the SEB II device to start its search for the trigger word. Valid entries are 0 to 132. A 0 (zero) entry instructs the SEB II to search all columns. We recommend you enter a start column number greater than zero. Starting your search at a specific column greatly speeds the search process.

5 Type the trigger word that you want the SEB II to search for in the **Match String** field. In additional to literals, trigger words can include wildcards and relational operators.

You can also define relational expressions as trigger words. Relational operators are: <, =, >, and any combination of these (<=, > =, <>). You can also include characters in the trigger word that do not appear on your keyboard. Hold down the Alt key and type the decimal value of the ASCII character. You can use any ASCII character except for 0, 8, 9, 13, 27, 234–238, and 255, since these characters represent commands (for example, ASCII character 8 is the backspace command).



6 Select an end flag from the **End Flag** list to tell the SEB II how many trigger words to look for in the data stream.
- **0** - look only for the trigger word in this line.
- **1** - look for the trigger words listed in this line and the next line. It must find both to consider this a match.
- **2** - tells the device that this is the last entry in this table. The SEB II unit ignores any trigger words listed after the end flag.

7 Select a trigger sequence number (1 - 40) from the **TS Index** list. The TS number corresponds to the line in the TS table that indicates the action you want taken when this trigger word is found. You can reference the same TS number several times.

8 Repeat steps 2 though 7 for each trigger word you want to enter.

9 Click a command button to complete your record. The following lists the command buttons available.

Button	What it does
Move	Change the record's position in the list. A dialog prompts you to enter a value of from 1 to 240, depending on the database type. Whatever value you enter, becomes the record's new index number and is inserted in its numeric order.
Next	Highlight the next entry in the list. The values for the entry display in the Edit fields.
Previous	Highlight the previous entry in the list. The values for the entry display in the Edit fields.
Import	Import a trigger word table from another database.
Delete	Delete the entry. All following entries move up in the list.
Clear	Clear the on-screen edit fields and fill any unedited fields with default values. This does not affect any of the records in the database. Click this button to start a new entry.
Change	Update the window to reflect your changes.
Accept	Accept all the changes made to the Trigger Word table. ***Caution:*** *This process is irreversible.*
Undo	Undo all changes that you have made to the Trigger Word table.
Close	Close the SEB II database and exit the window. ***Caution:*** *If you have neglected to save your changes (by clicking the Accept button) the system prompts you before closing. Click Yes to save your changes, or No to exit without saving.*

Trigger Sequences (TS)

Use the Trigger Sequences table to define the action the SEB II should take when it finds a trigger word in the data stream. You may choose to store the information in mass memory, report it in an alarm message, or ignore it.

To create a trigger sequence

1 Click the **TS** button to display the Trigger Sequences table.



2 Click the first TS Index number in the table to highlight it.

3 Select an action window number (1 – 64, depending on the database type) from the **AW Index** list. The AW number references an entry in the AW (Action Window) table. Select **0** when you do not want to reference the AW table. The SEB II will process the trigger word continuously.

4 Select a trigger message number (1 – 32) from the **TM Index** list. The TM number references an entry in the TM (Trigger Messages) table. You can reference the same TM index number for several TS entries. Select **0** if you do not want to reference this table.

5 Select a script dialog number from the **Dialog #** list to execute when the action window opens. Only available with ASP 5.1 and later.

6 Click a **Store** radio button.

- **Yes** - store the alarm in the SEB II's mass memory. You can poll the stored data later.
- **No** - Do not store the alarm.

7 Select a **Report** checkbox.

- **Standard** - Deliver alarm text, only. You must select this option when using database type S9 or an earlier version.
- **Enhanced** - Deliver alarm text and threshold count information. Use with database types S10 and S11.

8 Select a phone number index (1 - 40) for each of the four entries from the **Phone Numbers** list. The phone number references an entry in the PN table that tells the SEB II which telephone numbers to call when reporting an alarm message. Enter **0** if you do not want to reference this table.



Note *When the SEB II cannot reach any of the three phone numbers, it calls the backup number. Should the backup fail, the SEB II flags the message as "undeliverable" and stores it in memory along with an indicator (a colon) identifying which phone number had the problem. One colon indicates that the first telephone number failed; two colons indicate the second telephone number failed; three colons indicate the third number failed.*

9 Set the threshold period in minutes (0 to 65,000) using the **Threshold Period** fields. A threshold period is the length of time the SEB II checks for trigger words. The threshold period begins when the device detects a trigger word. It counts the occurrences of that trigger word until the timer ends. At the end of the period, the SEB II resets the counter to 0. The threshold period starts again with the next occurrence of the trigger word.

10 Type the minimum number of events that must occur during the threshold period before the SEB II takes action in the **Min** field. For example, a 6 tells the device to ignore the first six occurrences of the event. A 0 (zero) instructs the SEB II to act on every event it receives.

11 Type the maximum threshold for acting on an alarm during the threshold period in the **Max** field. For example, a 5 tells the SEB II device to act on the first five events that occur after the minimum number of threshold events. The device ignores all occurrences over the maximum number until the next threshold period. A 0 (zero) tells the device to take action on every event (no maximum).

12 Type a two-character code to set the classification for soft events in the **Class** field. You can then use this code to sort alarm messages during reporting. The SEB II reports this classification with each alarm message it delivers.

13 Type the number of text lines preceding the trigger word that the SEB II device should report and/or store with the trigger word. in the **Catch Lines Before** field. You can capture up to nine lines, but the total size of the alarm cannot exceed the Max Alarm Size setting in the SP table.

14 Type the number of text lines following the trigger word that the SEB II device should report and/or store with the trigger word in the **Catch Lines After** field. You can capture up to nine lines. The maximum number of characters you can capture varies depending on the size of the line containing the trigger word, the size of the lines captured after the trigger word line, and the maximum size and maximum alarm size entries in the Parameters table. The SEB II alarm queue can hold 1,543 characters per host port message.

15 Repeat steps 2 though 14 for each trigger sequence you want to enter.



16 Click a command button to complete your record. The following lists the command buttons available.

Button	What it does
Next	Highlight the next entry in the list. The values for the entry display in the Edit fields.
Previous	Highlight the previous entry in the list. The values for the entry display in the Edit fields.
Clear	Clear the on-screen edit fields and fill any unedited fields with default values. This does not affect any of the records in the database. Click this button to start a new entry.
Change	Update the window to reflect your changes.
Close	Exit the table.

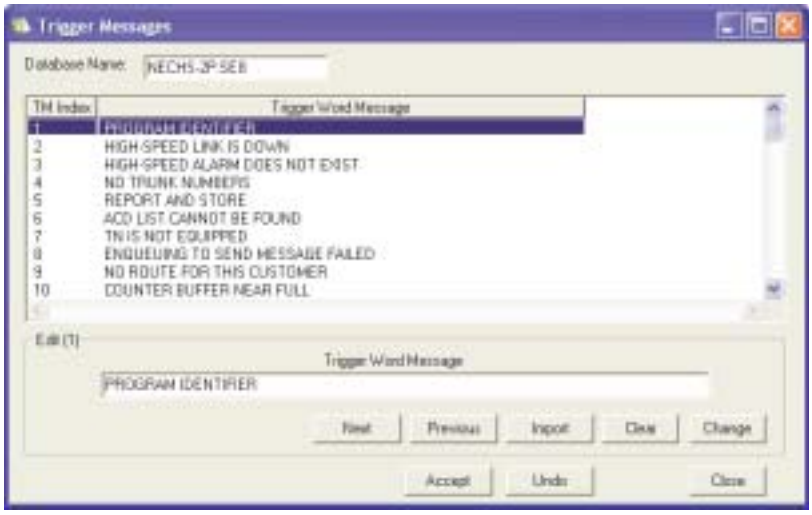


Trigger Messages Table (TM)

Use the Trigger Messages table to define optional text messages that the SEB II delivers with the event message when it matches a trigger word.

To create a trigger message

1 Click the **TM** button to display the Trigger Messages table.



2 Click the first TM Index number in the table to highlight it.

3 Type a trigger message (up to 50 characters) in the **Trigger Word Message** field.

4 Repeat steps 2 and 3 for each message.

5 Click a command button to complete your record. The following lists the command buttons available.

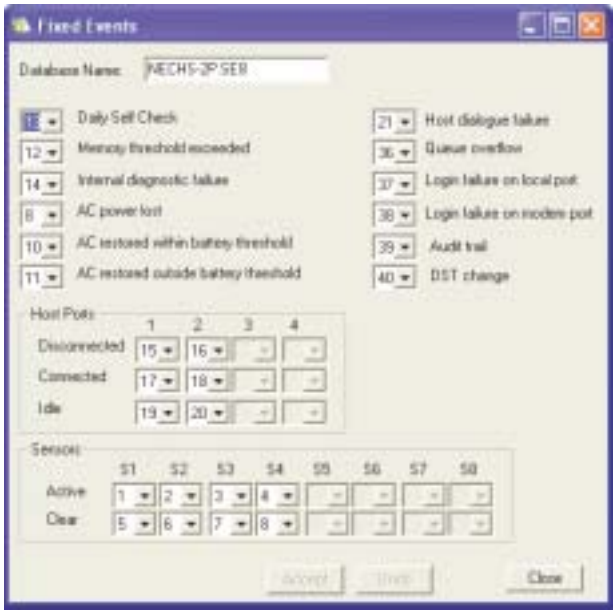
Button	What it does
Next	Highlight the next entry in the list. The values for the entry display in the Edit fields.
Previous	Highlight the previous entry in the list. The values for the entry display in the Edit fields.
Import	Import a trigger word table from another database.
Clear	Delete the entry.
Change	Save your edits. IRISnGEN updates the on-screen grid to reflect your changes.
Accept	Accept all the changes you have made to the table. This is an irreversible process.
Undo	Undo all changes that you have made to the table.

Fixed Event Table (FE)

Use the Fixed Event table to define fixed events. Fixed events identify a change of state in an external sensor, an alarm condition within the SEB II, or a change of condition in the host device. The number of possible fixed events will vary depending on your SEB II model. The number entry for each fixed event is the reference number of an entry in the FS table. The SEB II performs the action defined in the FS table when it detects a fixed event. For example, the Daily Self Check fixed event, shown in the figure below, references the entry on line 13 of the FS table.

To define a fixed event

1 Click the **FE** button to display the Fixed Events table.



2 Select a number from the lists from each event. The following table describes each event.

Fixed Event	What it means
Daily self check, FE13	This "call home" feature tells external monitoring software that SEB II is working properly. This feature works with the AW table; messages can be delivered daily or weekly.
Memory threshold exceeded, FE12	The SEB II Manager processes this action immediately. No daily or hourly periods apply to this threshold. The SEB II Manager automatically resets this threshold after a destructive poll or when users clear memory.

Internal diagnostic failure, FE14	The SEB II contains several diagnostic routines that continually monitor its operation. When it detects a malfunction, the SEB II performs the sequence referenced in this field. The messages transmitted and/or recorded for this type of event include a numeric value followed by a brief description of the failure: 1 SEB II database is corrupt or the BAIR detected a bad checksum in the ASP 2 Battery failure 3 Corrupt alarm message queue 4 Corrupt mass memory pointer 5 An exception trap was executed 6 Corrupt ASP 7 Modem failed to initialize or could not hang up 8 Modem reset because of its inability to communicate with the ASP
AC power lost, FE09	The SEB II performs an event sequence, defined in the FS table, for each AC power loss. The SEB II can detect a minimum AC power loss of 200 milliseconds.
AC restored within/outside battery threshold, FE10/FE11	The first field signals that power was returned within the threshold time (approximately two hours) and that internal stand-by power is available. The second field signals that power was returned after the internal stand-by threshold. Since the SEB II probably exhausted all stand-by power, this event prompts you to verify the SEB II is working properly.
Host dialogue failure, FE21	The SEB II lost its link with the host device or the InterAct script failed. This event applies only to NEAX devices or SEB IIs running ASP 5.1 or 5.2.
Queue Overflow, FE 36	The SEB II was not able to deliver alarms before the number of alarms received exceeded the value specified in the "Alarm Delivery Queue: Max Queue Entries" field in the SP table. When the queue fills, the SEB II removes the two oldest messages from the queue, flags them as queue overflowed messages, and stores them in memory. The SEB II then generates an FE36 message and adds it to the delivery queue.
Login failure on local/ modem port, FE37/FE38	The SEB II detected an incorrect password entered on the local port (FE37) or the modem port (FE38).
Audit trail, FE39	The SEB II generated an audit trail entry.



DST Change, FE40	The SEB II changed from Daylight Saving Time to Standard Time or from Standard Time to Daylight Savings time.
Host ports 1-4 connected, FE17/FE18/ FE32/FE33	These entries show that a device is connected to a port on the SEB II. The SEB II monitors DSR on pin six of the RS-232C connector. The SEB II is connected when a signal activates this pin.
Host ports 1-4 disconnected, FE15/FE16/ FE30/FE31	These entries show that a device was physically disconnected from the associated SEB II. The SEB II monitors DSR (Data Set Ready) on pin six of the RS-232C connector. When the signal on this pin is removed, the SEB II interprets a "disconnect".
Host port 1-4 idle, FE19, / FE20, FE34/ FE35	Each of these four fields show there is no activity on a port. If the SEB II does not receive data within the time specified in the Minimum Duration field of the FS table, the SEB II generates a fixed event. This feature is not available on SEB II-I Version 1.0.0 devices.
Physical sensors 1-8 active, FE1-4/ FE22-25	These fields correspond to pairs of screw terminals on the back of the SEB II. They are labeled HA1 through HA8. The FS index for each pair points to the series of instructions when the SEB II detects physical sensor activity. A physical sensor may be active in either the open or closed position, as defined in the PP table.
Physical sensors 1-8 clear, FE5-8/ FE26-29	These eight fields also correspond to the same pairs of screw terminals on the SEB II. The FS index points to a series of instructions when the physical sensor returns to its previous state.

3 Click ***Accept*** to save your changes or ***Undo*** to restore the original settings; then, click ***Close*** to exit the table.



Fixed Event Sequence Table (FS)

The SEB II uses the Fixed Event Sequence table parameters to determine what action it should take when it detects a fixed event. Each entry can control one or more fixed event conditions.

To define a fixed event

1 Click the **FS** button to display the Fixed Event Sequence table.



2 Click the first FS Index number in the table to highlight it.

3 Select an action window number (1 – 40) from the **AW Index** list. The AW number references an entry in the AW (Action Window) table. Select **0** when you do not want to reference the AW table. The SEB II will process the trigger word continuously.

4 Select a trigger message number (1 – 32) from the **FM Index** list. The FM number references an entry in the FM (Fixed Messages) table. You can reference the same FM index number for several FS entries. Select **0** if you do not want to reference this table.

5 Select a script dialog number from the **Dialog #** list to execute when the action window opens. Only available with ASP 5.1 and later.

6 Click a **Store** radio button.

- **Yes** - store the alarm in the SEB II's mass memory. You can poll the stored data later.
- **No** - Do not store the alarm.

7 Select a **Report** checkbox.

- **Standard** - Deliver alarm text, only. You must select this option when using database type S9 or an earlier version.
- **Enhanced** - Deliver alarm text and threshold count information. Use with database types S10 and S11.

8 Select a phone number index (1 - 40) for each of the four entries from the **Phone Numbers** list. The phone number references an entry in the PN table that tells the SEB II which telephone numbers to call when reporting an alarm message. Enter **0** if you do not want to reference this table.



Note *When the SEB II cannot reach any of the three phone numbers, it calls the backup number. Should the backup fail, the SEB II flags the message as "undeliverable" and stores it in memory along with an indicator (a colon) identifying which phone number had the problem. One colon indicates that the first telephone number failed; two colons indicate the second telephone number failed; three colons indicate the third number failed.*

9 Set the threshold period in minutes (0 to 65,000) using the **Threshold Period** fields. A threshold period is the length of time the SEB II checks for trigger words. The threshold period begins when the device detects a trigger word. It counts the occurrences of that trigger word until the timer ends. At the end of the period, the SEB II resets the counter to 0. The threshold period starts again with the next occurrence of the trigger word.

10 Type the minimum number of events that must occur during the threshold period before the SEB II takes action in the **Min** field. For example, a 6 tells the device to ignore the first six occurrences of the event. A 0 (zero) instructs the SEB II to act on every event it receives.

11 Type the maximum threshold for acting on an alarm during the threshold period in the **Max** field. For example, a 5 tells the SEB II device to act on the first five events that occur after the minimum number of threshold events. The device ignores all occurrences over the maximum number until the next threshold period. A 0 (zero) tells the device to take action on every event (no maximum).

12 Type a two-character code to set the classification for soft events in the **Class** field. You can then use this code to sort alarm messages during reporting. The SEB II reports this classification with each alarm message it delivers.

13 Type the number of text lines preceding the trigger word that the SEB II device should report and/or store with the trigger word. in the **Catch Lines Before** field. You can capture up to nine lines, but the total size of the alarm cannot exceed the Max Alarm Size setting in the SP table.

14 Type the number of text lines following the trigger word that the SEB II device should report and/or store with the trigger word in the **Catch Lines After** field. You can capture up to nine lines. The maximum number of characters you can capture varies depending on the size of the line containing the trigger word, the size of the lines captured after the trigger word line, and the maximum size and maximum alarm size entries in the Parameters table. The SEB II alarm queue can hold 1,543 characters per host port message.

15 Repeat steps 2 though 14 for each fixed event sequence you want to enter.



16 Click a command button to complete your record. The following lists the command buttons available.

Button	What it does
Next	Highlight the next entry in the list. The values for the entry display in the Edit fields.
Previous	Highlight the previous entry in the list. The values for the entry display in the Edit fields.
Clear	Clear the on-screen edit fields and fill any unedited fields with default values. This does not affect any of the records in the database. Click this button to start a new entry.
Change	Update the window to reflect your changes.
Close	Exit the table.

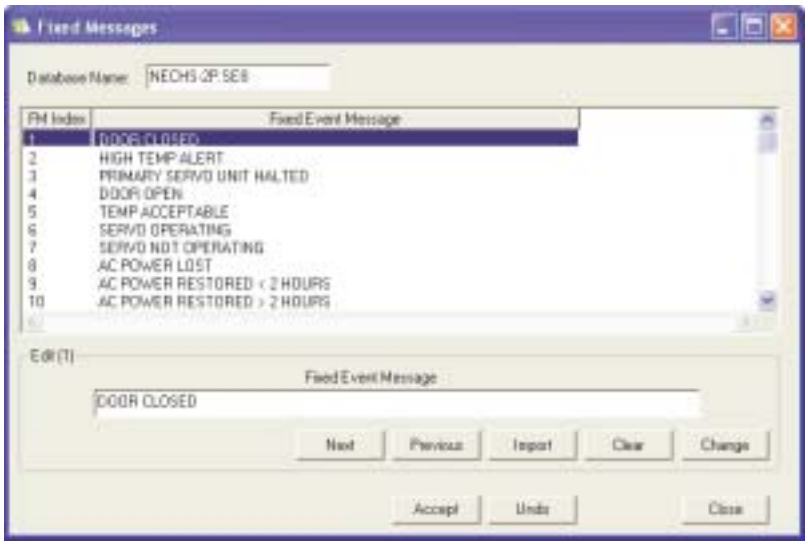


Fixed Message Table (FM)

Use the Fixed Messages table to include optional text with the reported event. The table holds forty message definitions, each with a maximum of fifty characters.

To create a fixed message

1 Click the **FM** button to display the Fixed Messages table.



2 Click the first FM Index number in the table to highlight it.

3 Type a fixed message (up to 50 characters) in the **Fixed Event Message** field.

4 Repeat steps 2 and 3 for each message.

5 Click a command button to complete your record. The following lists the command buttons available.

Button	What it does
Next	Highlight the next entry in the list. The values for the entry display in the Edit fields.
Previous	Highlight the previous entry in the list. The values for the entry display in the Edit fields.
Import	Import a trigger word table from another database.
Clear	Delete the entry.
Change	Save your edits. IRISnGEN updates the on-screen grid to reflect your changes.
Accept	Accept all the changes you have made to the table. This is an irreversible process.
Undo	Undo all changes that you have made to the table.

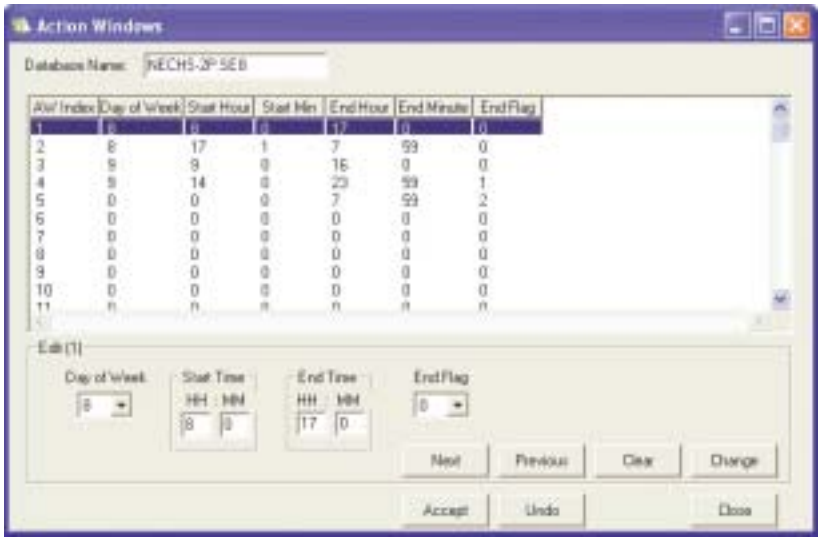
Action Window Table (AW)

The AW table contains entries that tell the SEB II when to execute an event sequence or trigger definition. Use the Action Window table to define the times when the SEB II should take action.

When the system receives an alarm, it checks the AW table and, if it meets the requirements, it processes the event. If not, no action is taken. You can assign action windows to the TS, FS, and PN tables. When you assign an action window to a TS or FS table, the system discards all events occurring outside the window. When you assign an action window to a PN table, the system reports the event to the phone number specified, but only within the defined AW period. In either case, the system can still store or report the event to a different phone number.

To create an action window

1 Click the **AW** button to display the Action Window table.



2 Click the first AW Index number in the table to highlight it.

3 Select a day(s) when the SEB II should process an event from the **Day of Week** list.
- **0** - The event is valid any day. Select one of the following:
- **1-7** - A day of the week, starting with Sunday.
- **8** - All weekdays.
- **9** - Weekends (Saturday and Sunday).

4 Type the time when the SEB II should begin processing events or verifying telephone numbers in the **Start Time** field.

5 Enter the time when the SEB II should stop processing events or verifying telephone numbers in the **End Time** field.

6 Select an end flag from the **End Flag** list to include multiple start and end times for processing events. Select one of the following:
- **0** - No more line entries are included in this action.
- **1** - The time and date listed in both this and the next line entry are part of the same table.
- **2** - Stop matching patterns. This prevents the SEB II from checking the rest of the table for entries.

7 Repeat steps 2 - 6 for each action window entry.

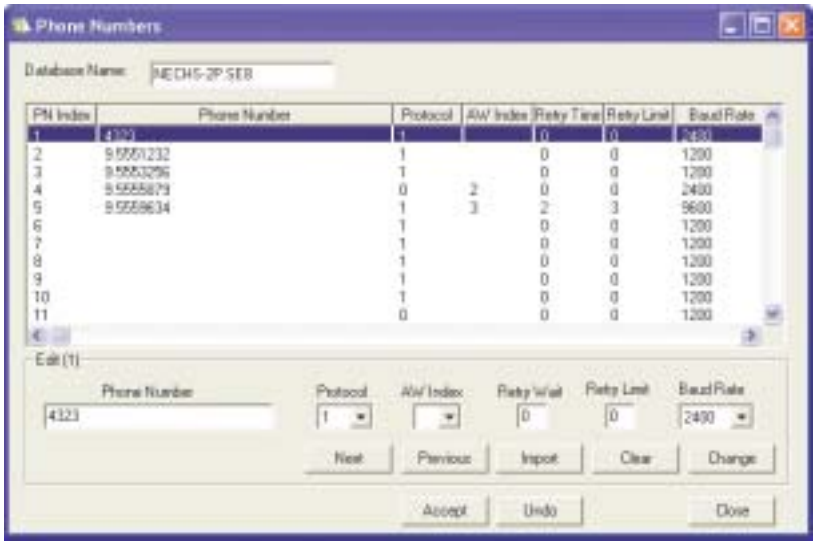
8 Click ***Accept*** to save your record; then, click ***Close*** to exit the table.

Phone Number Table (PN)

Use the Phone Numbers table to list the telephone numbers that the SEB II calls to report alarms, when to call, and how to call. If you configure the TS table and FS table, you must also configure the PN table if you want to deliver alarms. The PN table contains configuration parameters for forty telephone numbers.

To create a phone number record

1 Click the **PN** button to display the Phone Number table.



2 Click the first PN Index number in the table to highlight it.

3 Select a phone number index (1 - 40) from the **Phone Numbers** list. The phone number references an entry in the PN table that tells the SEB II which telephone numbers to call when reporting an alarm message. Enter **0** if you do not want to reference this table. The total number of characters in the Phone Number table cannot exceed 699.

4 Select a protocol number from the Protocol list to program the SEB II to deliver the alarm message to a communication device using a framing protocol or to a printer device that does not use framing. Select one of the following:

- **0** - Send only message characters, without framing (no protocol), and not to wait for a response.
- **1** - Send alarm data inside a data frame (protocol) and wait for a response frame acknowledgment.

The SEB II will deliver messages with the **D** indicator at the end of the message to indicate that it is delivering the message to the backup telephone number after failing to deliver it to the primary number. It delivers the message with the **L** when this is the last time the message will be reported today.

5 Select an action window number (1 – 40) from the **AW Index** list. The AW number references an entry in the AW (Action Window) table. Select **0** when you do not want to reference an action window

6 Select the number of minutes the SEB II should wait before attempting to deliver an event that it failed to deliver earlier from the **Retry Wait Minutes** list. The SEB II will not try to send the event if it has exceeded the Retry Limit.

7 Select the number of times the SEB II should dial a telephone number before abandoning that number and dialing the backup number from the **Retry Limit** list.



8 Select the baud speed of the SEB II modem dialing the telephone number from the **Baud Rate** list. SEB II devices equipped with high speed, internal modems (SEB II V.42bis and SEB II 14.4 V.42bis) can be set to 9600 or 19200.

9 Repeat steps 2 - 8 for each phone number entry.

10 Click a command button to complete your record. The following lists the command buttons available.

Button	What it does
Next	Highlight the next entry in the list. The values for the entry display in the Edit fields.
Previous	Highlight the previous entry in the list. The values for the entry display in the Edit fields.
Import	Import a trigger word table from another database.
Clear	Delete the entry.
Change	Save your edits. IRISnGEN updates the on-screen grid to reflect your changes.
Accept	Accept all the changes you have made to the table. This is an irreversible process.
Undo	Undo all changes that you have made to the table.

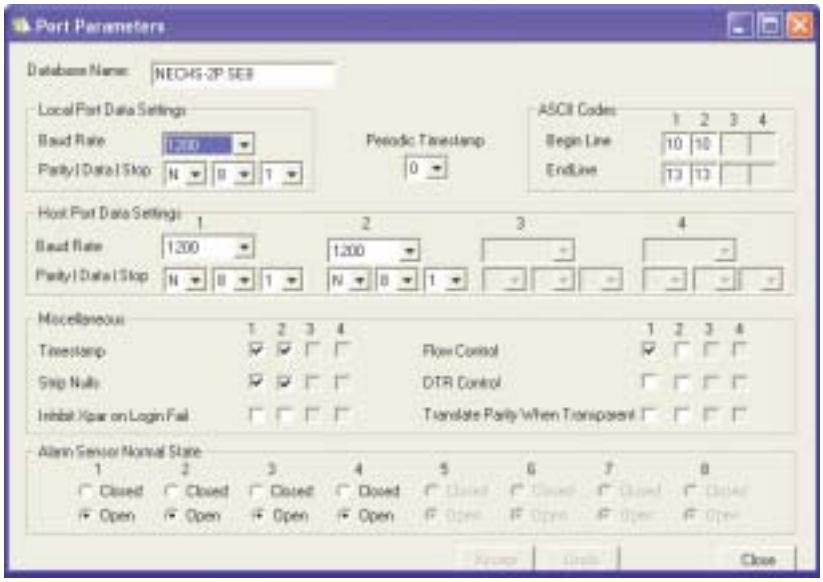


Port Parameters Table (PP)

The PP table lets you configure the parameters the SEB II uses to control four local and host port hardware interfaces. You can configure the flow control parameters for detecting and processing messages, and for controlling transparent connections. You can also configure the normal state for each of the SEB II's sensor terminals.

To create a port parameter

1 Click the **PP** button to display the Port Parameters table.



2 Select the baud that the SEB II sends or receives data through the local and host ports from the **Baud Rate** lists. The speed you define in this field must match the speed of the device connected to that port.



Note *The parity and baud rate must match the parity and baud rate settings of the host's data port connecting to the SEB II host port. If they do not match, the SEB II will not be able to receive data from the host, nor will you be able to communicate with your host through transparency.*

3 Select the port parity, data, and stop bits from the **Parity**, **Data**, and **Stop** lists for the local and host ports.

- Parity - **E**, **O**, **N**, **M**, and **S** to specify "even," "odd," "none," "mark," and "space"
- Data - **7** or **8**, for each character transmitted and received on the desired ports
- Stop - **1** or **2**, the number sent or received to mark the end of each character transmitted.

4 Select a value from the **Periodic Timestamp** list to define when the SEB II should place a timestamp in the mass memory. Select one of the following:

- 0 - No timestamp
- 1 - Timestamp every 15 minutes
- 2 - Timestamp every 30 minutes
- 3 - Timestamp every hour



5 Type the beginning line character code (ASCII) for host ports (1, 2, 3, and 4) in the **Begin Line** field. Enter an ASCII character code to match the first character in a line of text from a host port. The SEB II removes the character from the line before checking for a trigger word match. This character is neither stored in mass memory, nor delivered with an alarm message. Type **0** (null) to program the SEB II not to search for a beginning of line character.

6 Type the ending line character code in the **End Line** field. The SEB II neither stores the end-of-line character in mass memory, nor delivers it with an alarm message.

When the SEB II receives data without an end-of-line character, it checks the line size. If the number of characters exceeds the line size set in the SP table, the SEB II marks the characters as one line and stores or reports it. If the number of characters is less than the set line size, the SEB II waits three seconds, then times out and stores the characters as an entire line.

7 Select the **Timestamp** checkbox to assign a timestamp to every event triggered in the SEB II for the selected port. You should check it for alarm collection.

8 Select the **Strip Nulls** checkboxes to remove nulls from the data received through each port. Nulls embedded in the host data will affect the column position of trigger words. You must select these checkboxes to assure proper processing of polled data.

9 Select the **Inhibit Xpar on Login Fail** checkboxes to inhibit transparent mode on each port when the SEB II receives a login failure fixed event (FE37 and FE38). You can use the thresholds in the FS table to set the number of login failure the system will allow before blocking transparent access. Downloading an SEB II database will clear the blocked transparency.

10 Select the **Flow Control** checkboxes to enable flow control for each port. This feature lets the SEB II control the flow of data between the SEB II and the host device. The SEB II sends the host an ASCII XOFF character (Hex13 (Ctrl-S)) when the input buffer on the SEB II reaches "nearly full." When the input buffer is "nearly empty," the SEB II sends the host device an ASCII XON character (Hex11 (Ctrl-Q)) and restarts the host's output. The SEB II provides this protocol only for those devices supporting the XON-XOFF (in-bound) flow control protocol.

11 Select the **DTR Control** checkboxes to detect or ignore the DTR signal on each host port. Select the checkbox when the DTR signal is active only when the respective host port is in a transparent session with the modem or local port on the SEB II. Clear the box when the DTR signal is always asserted.

12 Select the **Translate Parity When Transparent** checkboxes to translate parity during transparency for each host. Clear the checkbox when you do not want to translate parity.

You must configure the SEB II serial host port with the same data structure and baud rate of the host device to which it connects. The SEB II supports features for the data structure that is passed through a transparent connection during a transparency session with the modem or a local serial port. When you select a Translate Parity on Transparency checkbox, the data presented to the connected user will be 8 bit, 1 stop bit, and no parity (the same as the serial port for the modem). If you do not select a checkbox, the data presented to the connected user will be the same as the associated host serial port. For most applications, you should select a checkbox because it normalizes the data so that the caller will not need to know how the host serial port is configured to communicate with it. You should not select a checkbox if you are using a communication tool that is hard coded to use a specified data structure that matches the associated host device.

13 Click the **Alarm Sensor Normal State** radio buttons to define the normal state of each physical sensor attached to the screw terminal pairs (HA1-HA8) on the back of the SEB II. Define sensors as "normally open" (O) or "normally closed" (C). The screw terminals are normally open when current cannot flow through them. The screw terminals are normally closed when current can flow through them.

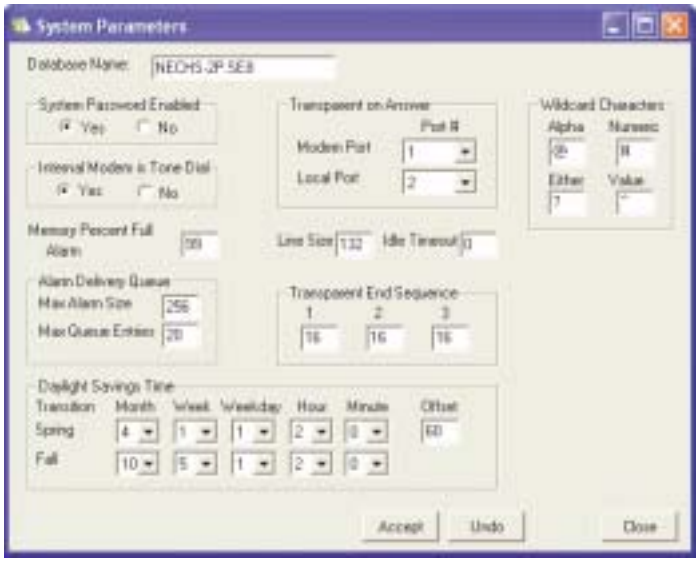


System Parameters Table (SP)

Use the System Parameters screen to define miscellaneous configuration parameters. The SEB II uses these parameters when detecting and processing messages, when enabling system passwords, and when automatically adjusting the SEB II's internal clock for Daylight Saving Time.

To create a system parameter

1 Click the **SP** button to display the System Parameters table.



2 Select a **System Password Enabled** radio button to enable (Yes) the system (master) password, as defined in the Remote Agent window, or disable (No) the system password. Selecting No programs the SEB II to accept only the passwords defined in the SE table, see ”Security Table (SE)’, page 8-26.



Note *If you disable the password, you must define a password in the SE table with all access rights. This will prevent you from accidentally blocking access to the SEB II. If you block access to your SEB II, you can clear the contents of the SEB II by pressing the reset button on the back of the SEB II twelve times. However, this process will erase all data in the SEB II.*

3 Select an **Internal Modem is Tone Dial** radio button to enable (Yes) your SEB II’s modem to use tone dialing, or disable (No) tone dialing. Selecting No programs the SEB II to use pulse dialing.



4 Select a port number from the **Transparent on Answer** list to enable transparent mode with the host device through the SEB II. While in transparent mode, you can then communicate directly with the host via a terminal or communications software.

Selecting **0** disables this feature and allows the caller communicate with the SEB II in Interactive mode or to access transparency using one of the passwords assigned in the SE table. We recommend disabling this feature to make use of the added security of the SE table.



Warning *Do not enable Transparent on Answer if you are using a high speed modem to communicate with the SEB II 2.4 V.22bis or SEB II External with a 2400 modem. Using this feature under these conditions may cause the SEB II device to function improperly.*

5 Type the ASCII wildcard characters that can appear in match strings (as defined in the TW table) in the four **Wildcard Characters** fields. The default wildcards are **@** (alpha), **#** (numeric),**?** (either), and ^ (value).

6 Type a value in the **Memory Alarm Percent Full** field to define the percent of mass memory the SEB II must fill before it generates a fixed event message. Type **0** if you do not want to generate a fixed event message.

7 Type the maximum number of characters the SEB II will allow before it processes the line of data in the **Line Size** field. The SEB II will process the line regardless of the SEB II receiving the end-of-line character. The SEB II processes excess characters as another line of data.

8 Type the number of minutes the SEB II device is to remain in an idle (inactive) state before hanging up in the **Idle Timeout** field. The SEB II terminates a the if it does not receive a request during the idle minutes. For example, setting this field to **5** programs the SEB II to hang up if does not receive a request within five minutes. The timeout is applicable under the following conditions:

- the SEB II calls a protocol device to deliver an event
- a user is transparent to a host device through the modem or local port
- a user is in the Interactive mode through the modem or local port

9 Type the maximum size of each alarm held in the delivery queue in the **Max Alarm Size** field. The delivery queue holds alarms until the SEB II can deliver them to the IRISnGEN system. Characters exceeding the maximum size are truncated.

10 Type the maximum number of alarms the system will hold in the delivery queue in the **Max Queue Entries** field. When the number of alarms exceeds the maximum size, the SEB II stores the oldest alarm in mass memory. You can use polling to retrieve alarms stored in mass memory, or you can leave them to be overwritten by newer alarms.

11 Type the code that programs the SEB II to terminate a transparent connection with the host in the **Transparent End Sequence** fields. The default is “16" (the delete character). When defining the end sequence codes, be sure to use characters that will not impede the operation of the host device. For example, do not use an end sequence character that the host device could interpret as a reload command.



12 Type the month, week, day, and time the SEB II should adjust for daylight saving time in the DTS Transition fields.

- Month (1-12) The default is 4.
- Week (1-5) A value of 5 always indicates the last week of the month. The default is 1.
- Day (1-7, Sunday = 1) The default is 1.
- Time (hh:mm) The default is 02:00.

13 Type the minutes (usually 60) the SEB II's clock adjusts for Daylight Saving Time in the **Offset** field. The SEB II automatically resets its clock the number of offset minutes at the days and times specified in the previous fields.

To disable the DST feature

1 Type **0** in the **Offset** field.

2 Include *set tz=0* in your AUTOEXEC.BAT file for the DOS version of SEB II Manager when disabling this feature. Otherwise, SEB II Manager will continue reporting DST time.



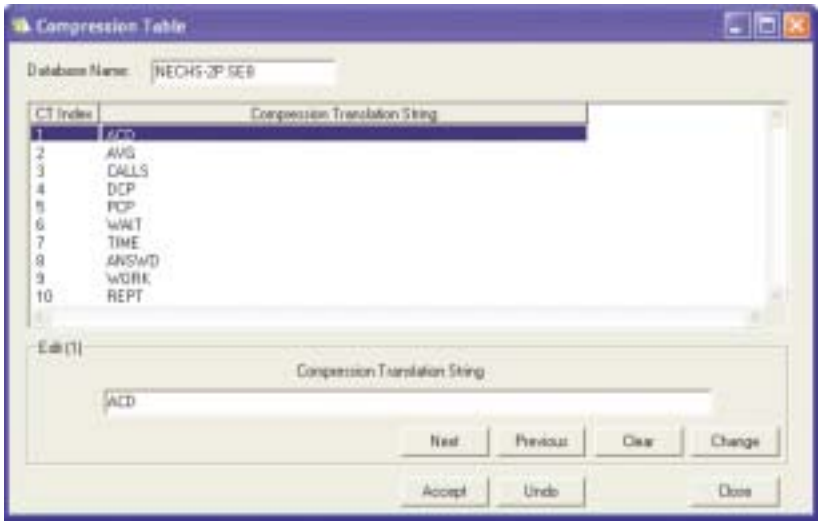
Compression Translation Table (CT)

The CT table speeds the process for storing and sending collected data. Its pattern matching facility lets you define up to ten patterns with ten characters each. Rather than storing the full character pattern, the SEB II substitutes a single byte value in memory. This value corresponds to the text indexed in this table.

The SEB II Manager receives a copy of this table from the SEB II during the polling process. For each pattern defined in the table, the SEB II sends a one byte index instead of the actual text. The SEB II Manager then reassembles the data into their original format and places the restored data in the output file. This technique saves data storage and speeds transmission. The key to maximum efficiency is to select character patterns that repeat frequently in the host's output data stream.

To create a compression translation record

1 Click the **ST** button to display the Compression Translation table.



2 Click the first CT Index number in the table to highlight it.

3 Type a compression string in the **Compression Translation String** field.

4 Repeat steps 2 and 3 for each string.

5 Click a command button to complete your record. The following lists the command buttons available.

Button	What it does
Next	Highlights the next entry in the list. The values for the entry display in the Edit fields.
Previous	Highlights the previous entry in the list. The values for the entry display in the Edit fields.
Clear	Deletes the entry.
Close	Exits the Compression Translation table.

Security Table (SE)

Use the Security table (SE) to set the controls that prevent unauthorized access to the SEB II device. You can define passwords that limit access to the SEB II, to the ports connecting to the host device, and to mass memory. You can also reference the AW table to determine when a caller can access an SEB II and to point to the PN table to identify a callback telephone number.

When accessing the SEB II, the caller can only access the functions defined for this password. You must enable the password and give full access to the ports and memory if the caller is to upload and download databases.

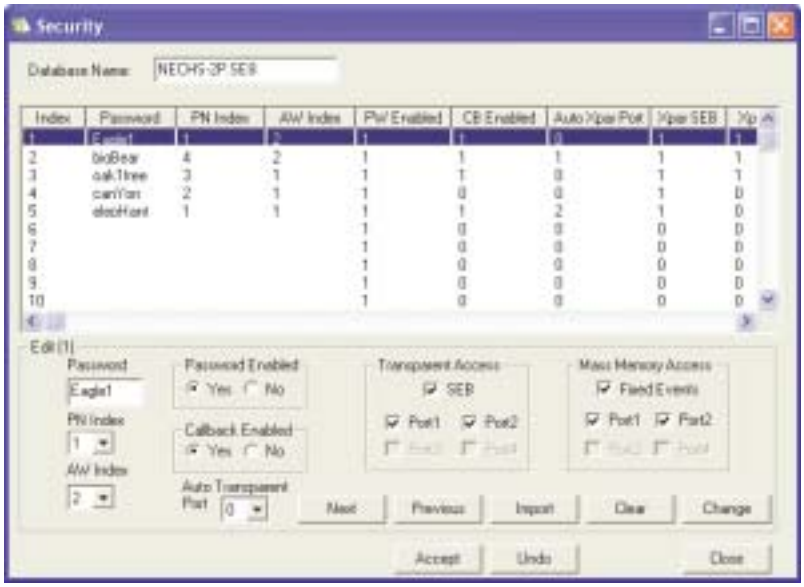
The callback feature protects the SEB II from unauthorized access. The SEB II denies access to those functions defined for the caller's password until the SEB II verifies the caller's telephone number. The SEB II automatically hangs up; then, calls the telephone number defined for that password. If the caller is dialing from the telephone number indexed in the PN table, the SEB II calls that number, prompts the caller for the password, then grants the caller access to those ports and sections of mass memory allowed for the password.



Warning *When adding the master password to the SE list, you may inadvertently lock yourself out of the SEB II features. We recommend that you do not include the master password in this list.*

To create a security record

1 Click the **SE** button to display the Security table.



2 Click the first Index number in the table to highlight it.

3 Type a password up to eight alpha-numeric characters in length in the **Password** field; then, click the **Password Enabled** radio button (Yes) to enable the password. When signing in to an SEB II, the caller must type the password exactly as defined here. For example, if the password contains all lower-case letters, the caller must enter the password with all lower-case letters or the SEB II will not accept it.



Warning *Do not define this password the same as the system password in the SP table. Doing so could block you from accessing the SEB II!*

4 Select a phone number entry from the **PN Index** list; then, click the **Callback Enabled** radio button (Yes) to enable callback. The PN number references an entry in the PN (Phone Number) table. You can reference the same PN index number for several SE entries. Select **0** if you do not want to reference this table.



Note *The callback process only uses the telephone number and baud rate defined in the PN table. All other entries are ignored.*

5 Select an action window number (1 – 40) from the **AW Index** list. The AW number references an entry in the AW (Action Window) table. Select **0** when you do not want to reference the AW table.

6 Select a host port number to gain transparent access to the host using a non-protocol communications program (such as PROCOMM) from the **Auto Transparent Port** list. When the SEB II receives this password, it immediately switches to transparent mode, unless you enabled the callback feature. The default for this field is "0." You may want to grant transparent access to the SEB II so the caller can display the port status in the event of communication problems with the host device.



Warning *Do not enable Transparent-on-Answer if you are using a high speed modem to communicate with and SEB II 2.4 V.22bis (or SEB II External with a 2400 modem). Using this feature under these conditions may cause the SEB II device to function improperly.*

7 Select the **Transparent Access** checkboxes to allow a transparent connection to the SEB II, or to the corresponding host ports, when the caller uses the associated password.



Note *You must check the SEB II field if you are going to allow access to mass memory for anyone using a non-protocol device.*

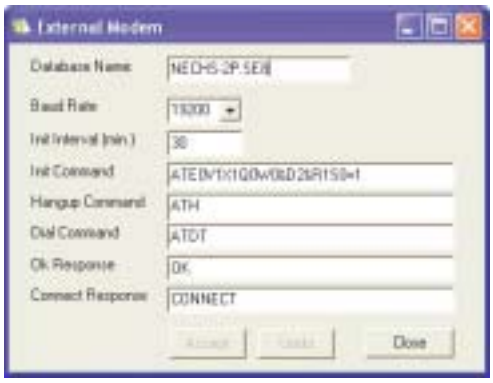
8 Select the **Mass Memory Access** checkbox for each port to let callers with this password view and poll mass memory.

External Modem (EM)

If you are using the SEB II 14.4 V42bis or SEB II EM (external modem) device, you can use the SEB II Manager's EM table to change the characteristics of the SEB II's modem.

To create a external modem record

1 Click the **EM** button to display the External Modem table.



2 Select the speed at which commands are sent the external modem from the **Baud Rate** list.

3 Type the interval (in minutes) that the system should send the SEB II's modem the initialization command in the absence of other activity in the **Init Interval** field. Sending this command ensures the external modem is reset to the required state in the event of a power loss.

4 Type the initialization command string in the **Init Command** field. The string was preset with a standard initialization command string. This string works with the SEB II 14.4 V42bis device and modems attached to the SEB II external modem model. In most cases you do not need to edit this string.



Warning *If you leave this field blank or enter an incompatible modem command, you may be denied access to the SEB II. You will only be able to regain access by pressing the SEB II's reset button twelve times.*

5 Type the command to disconnect the modem in the **Hangup Command** field. When you enter the "-" command, it is not sent to the modem. However, it does cause a one second delay. Use this command to switch Hayes compatible modems to the command state: -+++-.

6 Type the dialing prefix command (e.g., ATDT for tone dialing and ATDP for pulse dialing) in the **Dial Command** field. You can include line access number, if necessary.

7 Type the modem's response to indicate it accepted the command in the **OK Response** field. The default is "OK."

8 Type the response that the modem should make when connection is made in the **Connect Response** field. When the modem reports the connection speed (e.g., CONNECT 2400), the SEB II adjusts its data rate to match. The number reported must match the DTE speed, not the line speed.

9 Click ***Accept*** to save your entries; then, click ***Close*** to exit the table.



9

Monitoring Data

Your IRISnGEN system is available with the optional List Viewer and Map Viewer packages for monitoring and viewing alarm, event, and site data throughout your IRISnGEN network.

List Viewer

The List Viewer is a real-time display of incoming alarm information. The information in the IRISnGEN database presents the proper information to the right technician as it receives new alarms.

Alarm data from each host displays on a single line in a multi-column format. The IRISnGEN system color-codes each alarm to highlight its severity and status. You can determine a change in an alarm's severity and status just by observing a change in the color of the text. The alarm information includes its ID, escalation level, date and time received, date and time occurred, severity, status, host, alarm type, keyword, alarm text, alarm description, site, and customer. You can re-order the columns so that data important to you displays in the main window. You can even customize and save the settings in a user profile.

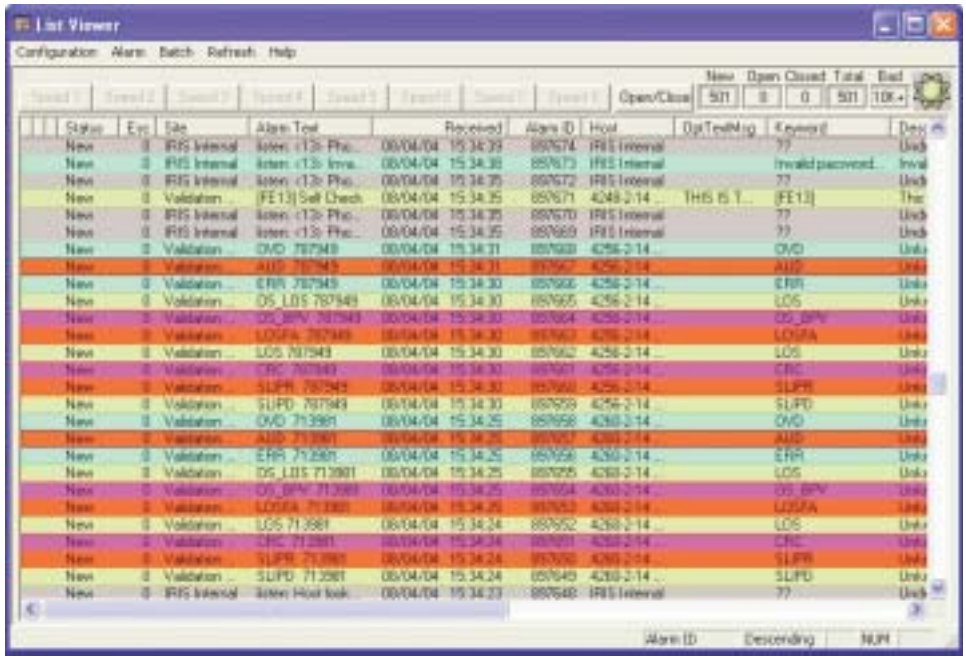
Map Viewer

Map Viewer is a geographical representation of your site locations. Map Viewer incorporates all the functions of Microsoft MapPoint and uses IRISnGEN's Equipment Explorer to display detailed information about a site. Each site appears as an icon on the Map Viewer map. You can click on a site to gain more information about that site, or to view alarms, events, and equipment information for that site. Each site icon displays varying colors to help you quickly determine the status of each site.

Map Viewer is available under license, only. If you purchased a Map Viewer license, the Map Viewer option becomes available on the IRISnGEN toolbar.

List Viewer

Use List View to display alarms in the List Viewer window. Alarms are color-coded to show severity and status. You monitor alarms so that you can take corrective actions.



For example, as the IRISnGEN system receives alarms, you can respond to them based on status, handling the most severe alarms first.

Not all this information appears in the window at once. Use the scroll bars at the side and bottom of the window to see more information.

Each alarm displays as a single line in a multi-column format. You can customize your display, rearranging the order of the information in the columns. Once you have the display as you like it, you can save it in your user profile.

To change the alarm data displayed in your viewer, define an alarm selectivity. You can save your selectivity choices and assign them to speed buttons. With the click of a speed button, you can view all critical alarms or view alarms from a unique host type or alarms from a selected customer. One feature of the speed button selectivity is the “same as current” option.

Note the three columns to the left of the Status column. Each column displays an icon that indicates the alarm has an attachment (denoted by a page icon), that a technician was dispatched (denoted by a car icon), and that this site has special procedures attached (denoted by an exclamation mark).

Configuration

Selectivity

Use the Viewer Selectivity feature to program eight speed buttons that quickly display the alarm data. You can program the speed button selectivity options, and then save them in a user profile. For example, you can program a speed button to show the last eight hours of host alarm information. Each time you click the speed button, the last eight hours of alarm activity displays. If you select a different alarm in the viewer and click the speed button, the last eight hours of activity for that host displays.



You can selectively view alarms in both the List and Geographic Viewers based on the following parameters. You can select as many or as few parameters as you want.

To set selectivity

1. From the List Viewer menu, choose **Configuration** > **Selectivity**.
2. Select the viewer parameters for your display from the **Host**, **Site**, **Customer**, **Host Type,** and **Host Address** lists.
3. Host addresses are specific devices on a network, or devices attached to hard alarm contacts on the remote agent units.
4. Type a hierarchy in the **Hierarchy** field, or click the ***Pick Node*** button and select a hierarchy from the list.
5. Type a note in the **Node** field, or click the ***Pick Node*** button and select a node from list.
6. Select a **Status** checkbox for each alarm state you want to view. Select New, Open, and/or Closed.
7. Select a **Severity** checkbox for each severity code you want to view. Select Critical, Major, Minor, Informational, or Undefined.
8. Select a user from the **User** list to display only those alarms that the user took action on.

9 Type the message text for the alarm you want displayed in the List Viewer in the **Alarm Text** field. The Viewer only displays alarms that have that text within the alarm message. Use the % symbol as a wildcard character, or enter the complete text.

10 Type a one- or two-character class code in the **Class Code** field. The viewer only displays alarms with that code.

11 Type the keyword text in the **Keyword** field. Use the % wildcard, or enter the complete text keyword.

12 Select an alarm type-for example, unsolicited-from the **Alarm Type** list.

13 Type a range of alarm IDs in the **Alarm ID** fields. You can use one or both fields to define your range.

14 Type a range of escalation numbers for alarms in the **Escalation Number** fields. You can use one or both fields to define your range. Escalation numbers can be from 0 to 99.

15 Type a time range for alarms in the **Absolute Time** fields. You can use one or both fields to define your range. Enter times using the format *yyyymmddhhmm*, where *yyyy* is the four-digit year, *mm* is the two-digit month, *dd* is the two-digit day, *hh* is the two-digit hour, and the last *mm* is the two-digit minute.

16 Type a relative time range in the **Relative Time** fields. You can use one or both fields to define your range. In the At Least field, enter how long ago you want to show alarms (as in, alarms from twenty minutes ago). In the Not More Than field, enter the most recent time you want to show alarms.

To use selectivity

1 While in the Viewer window, do one of the following:
- Press ***F2***.
- Choose Configuration > Selectivity.

2 While in the Selectivity window, do one of the following:
- Click the ***Load*** button for a set of selectivity parameters previously saved.
- Select the parameters you wish to view.

3 When you finish, click ***Save*** to save your choices.

4 Click ***OK***.

The system returns to the List Viewer and displays only those alarms matching your selectivity parameters.



Note *The Selectivity feature is the same for both List View and Geographic View.*

Refresh Time

You can control how often the List Viewer refreshes. Refresh time tells the IRISnGEN system how long to wait before updating the List Viewer with new alarm information. The default value is 60 seconds; the minimum value is 5.

To set the refresh time

1 Choose **Configuration > Refresh Time**. The system opens the Enter Refresh Time dialog.



2 Type a value (in seconds) for the refresh time.

3 Choose the ***OK*** button.

Speed Buttons

The IRISnGEN system lets you selectively display alarms, so you see only the alarms that interest you. This selectivity is the same for both List View and Geographic View. You can create up to eight speed button definitions to easily access your desired selectivity.

To create a speed button

1 From the List Viewer menu, choose **Configuration > Speed Buttons**; then, select a speed button (1 to 8). The system opens the Viewer Selectivity dialog.

2 Enter your selectivity selections; then, click ***OK***. The system opens the Enter Speed Button name dialog.



3 Type a name for speed button you chose in step 1. This name will appear on the button.

4 Click ***OK*** to save your work, or ***Cancel*** to return to the Viewer.

Grid Lines Horizontal/Vertical

You can add horizontal and vertical lines to your List Viewer screen to help visually separate the columns and rows of data.

To add grid lines

1 From the List Viewer menu, choose **Configuration > Grid Lines Horz** to insert horizontal lines.

2 Choose **Grid Lines Vert** to insert vertical lines.

Save Setting

Save the List Viewer and Geographic Viewer configuration settings for your user profile.

To save configuration settings

From the List Viewer or Geographic menu, choose **Configuration > Save Settings**.

Exit

Exit from the List Viewer or Geographic Viewer at any time. The IRISnGEN system continues running in the background.

To exit a viewer

From the List Viewer or Geographic Viewer menu, choose **Configuration > Exit**.



Note *You can exit from any window at any time by pressing the Exit button located in the upper right-hand corner of all windows.*

Alarm

Alarm Status Open/Closed

You can change any alarm that has a status of *new* or *closed* to *open.*

To open an alarm

1 Highlight the alarm you want to open.

2 Do one of the following:
- Right-click the mouse; then, select **Open** from the pop-up menu.
- Press ***F5*** to toggle the alarm status open or close.
- From the List Viewer menu, choose **Alarm > Open/Close**.

You can change any alarm that has a status of New or Open to Closed.

To close an alarm

In List Viewer, highlight the alarm you want to close and do one of the following:

- Right-click the mouse; then, select **Close** from the pop-up menu.
- Press ***F5*** to toggle the alarm status open and close.
- From the List Viewer menu, choose **Alarm > Open/Close**.

View Detail

When you double-click a highlighted alarm, IRISnGEN displays the alarm property folders containing all of the system data for a given alarm.



The property folders give the technician quick access to most information necessary to take corrective action. The alarm property folders include:

- **Detail** – all available detail for the selected alarm. This may include corrective action detail unique to the alarm keyword.
- **Host –** information from the associated host record
- **Site –** information from the associated site record
- **Customer –** information from the associated customer record
- **Comments** – free-form comments about the alarm, by user with timestamp
- **Disposition** – list of pending escalation and correlation events for the selected alarm
- **History** – a history of operations for each alarm, in chronological order by user
- **Linked Alarms** – alarm types correlation and threshold include a list of alarms that are linked to the displayed alarm
- **Attachment** – special attachment text sent to IRISnGEN from an SEB
- **Variables –** shows the keyword and its associated variable content for enhanced keywords

The host, site, and customer tabs also contain buttons that permit you to enter comments, display contact information, view special procedures, and view user-defined fields unique to each host, site, or customer record.

To access alarm details

1 Highlight an alarm and do one of the following:

- Double-click the highlighted alarm.
- Right-click the mouse; then, select **View Detail** from the pop-up menu.
- Press ***F4***.
- From the List Viewer menu, choose **Alarm > View Details**.

2 Browse the tabs for the information you want.



Note *Alarm Detail for a correlated or threshold alarm shows information about the alarm(s) that created the triggered alarm. The Alarm Text field shows the IDs of the alarms that make up the completed correlation or threshold. If in the threshold or correlation screen, the system deletes the intermediate alarms, then the alarm text field instead shows the alarm entry ID, that is, the system matched the ID of the keyword.*

View Attachment

You can view the special attachment text sent to the IRISnGEN system from the remote agent.

To view attachment

Highlight an alarm that has an attachment (indicated by a page icon in the attachment field) and do one of the following:

- Press ***F8***.
- From the List Viewer menu, choose **Alarm > View Attachment**.

Forward Alarms

You can manually forward a copy of any alarm to a predefined forward set or a printer. (In the optional Enhanced Alarm Forwarding package, you can also forward alarms to email, a pager, or a fax machine.)

To manually forward an alarm

1 Highlight an alarm and do one of the following:
- Right-click the mouse; then, select **Forward** from the pop-up menu.
- From the List Viewer menu, choose **Alarm > Forward**.

2 From the Option menu, choose one of the following:
- Forward Set
- Page (only Enhanced Alarm Forwarding package)
- Fax (only in Enhanced Alarm Forwarding package)
- Email (only in Enhanced Alarm Forwarding package)
- Print
- SNMP (only in Enhanced Alarm Forwarding package)

The Select pop-up window appears with a list of your forwarding choices (for example, a list of forward sets).



3 Make a selection from the list.

4 Click ***OK***.

Choosing a Format When Forwarding Alarms via E-mail

IRISnGEN offers two report formats for alarms forwarded via e-mail; Crystal Reports and HTML. Alarms forwarded in the Crystal Reports format arrive with a .RTF attachment. You must open the e-mail attachment to view the alarm report. Alarms forwarded in the HTML format display in the body of the e-mail and as a .HTM attachment. When choosing an alarm report format for forwarding via e-mail, you must first set the format value in the System Parameters.

To set the alarm format value

1. Expand the System Parameter folder (IRIS Administration > System Parameters).
2. Click the **FORWARD_FORMAT** file to display the System Parameter tab.



3. In the **Value** field, do one of the following:
   - Type **HTML** to set the alarm report in HTML format. (Default)
   - Type **CRYSTAL** to set the alarm report in the Crystal Reports format.
4. Save your record.

Changing the E-mail Subject Line Text for Forwarded Alarms

When forwarding alarms to an e-mail address, you may want to change the subject line text. Do this by setting its System Parameter value.

To change the e-mail subject line text

1. Expand the **System Parameter** folder (IRIS Administration > System Parameters).
2. Click the **ALARM_FWD_TITLE** file to display the System Parameter tab.



3. In the **Value** field, type the subject line text for your forwarded alarm.
4. Save your record.

Selecting a Style for HTML Alarm Reports

IRISnGEN comes with six HTML style templates for alarms forwarded via e-mail. Each template presents alarm data with varying information. Select the template that is right for you. The following table lists the style templates available.

File Name	Description
AlarmFwd.xsl	The file used by IRISnGEN to generate HTML
AlarmFwd_Default.xsl	Default report. Lists host and site contacts.
AlarmFwd_Host_Contacts.xsl	Lists primary host contacts, only.
AlarmFwd_Site_Contacts.xsl	Lists primary site contacts, only.
AlarmFwd_All_Host_Contacts.xsl	Lists all host contacts.
AlarmFwd_All_Site_Contacts.xsl	Lists all site contacts.
AlarmFwd_All_Contacts.xsl	Lists customer, site, and host contacts.

Selecting a style template involves renaming the template to the *AlarmFwd.xsl* filename. The IRISnGEN report engine uses the *AlarmFwd.xsl* file to generate the HTML report.



Caution *Before changing any .xsl filename, be sure to make a backup copy of that file first.*

To select a style template

1. Navigate to the *IRIS HOME\Reports* folder for your system server.
2. Highlight a style template file (for example, **AlarmFwd_Site_Contacts.xsl**).
3. Right-click the file and choose **Rename**. Rename the file **AlarmFwd.xsl**.

IRISnGEN will now forward alarm reports to e-mail addresses with this HTML format. You can alter the look of the style template using an HTML editor (not provided by Teltronics).

Escalate Alarms

If you personally cannot resolve an alarm, you can escalate it to the next level and alert personnel that are qualified to handle it. The following procedure increases the escalation one level.



Caution *Non-reversible procedure! Once you escalate the alarm, you cannot undo it.*

To escalate an alarm

From List Viewer, highlight the alarm; then, do one of the following:

- Right-click the mouse; then, select **Escalate** from the pop-up menu.
- From the List Viewer menu, choose **Alarm** > **Escalate**.
- Press **CTRL** + **E**.

The escalation level is immediately incriminated by one (for example, if the escalation level was 0, it is now 1). The maximum escalation value is 99. All new alarms have an escalation value of zero.



Dispatch Alarms

When you have dispatched a service technician to handle a call, you can mark the alarm to indicate this. The IRISnGEN system displays a car icon in the dispatch field. All alarms from the host at that site will also display the car icon. When the technician leaves the site, you can unmark the alarm. This disables the dispatch icon for future alarms.

To dispatch the alarm

1. Highlight the alarm.
2. Right-click the mouse; then, select **Dispatch > Start/End** from the pop-up menu.
   Select Start to mark the alarm with the dispatch icon, or select End to unmark the alarm.

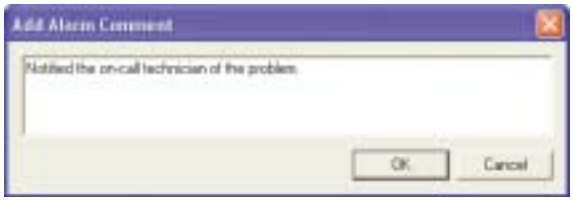
Adding Comments to Alarms

You can add your own free-form comments to any alarm.

To add comments

1. Highlight an alarm and do one of the following:
   - Right-click the mouse; then, select **Add Comments** from the pop-up menu.
   - Press **CTRL+U**.
   - From the List Viewer menu, choose **Alarm > Add Comments**.

   The system opens the Add Alarm Comments dialog.



2. Enter your comments.
3. Click ***OK***.

You cannot remove a comment from an alarm once you save it; however, the aging process will remove them from the system.

Ticket Alarms

While in the List Viewer, you can generate a trouble-ticket for any alarm. This means that the system copies the alarm to the Trouble Ticket table.



Caution *Non-reversible procedure! Once you have copied an alarm to the trouble ticket table, you cannot remove it from the table.*

To generate a trouble ticket for an alarm

1. Highlight an alarm.
2. Right-click the mouse; then, select **Trouble Ticket** from the pop-up menu.

Export Alarms

While in the List Viewer, you can export any alarm. This means that the system copies the alarm to the Export table.



Caution *Non-reversible procedure! Once you have copied an alarm to the export table, you cannot remove it from the table.*

To export an alarm manually

1. Highlight an alarm.
2. Right-click the mouse; then, select **Export** from the pop-up menu.



Note *You can also access and transfer Trouble Ticket table and Export table information to your legacy system. This requires software not included in your IRISnGEN package.*

Remove Alarms

You can remove an alarm from the List Viewer while leaving it in history.



Caution *Be very sure that you want to remove the alarm. When you select Remove, the system removes the alarm. You are not asked if you are sure you want to remove the alarm.*

To remove an alarm

1. Highlight an alarm.
2. Right-click the mouse; then, select **Remove** from the pop-up menu.

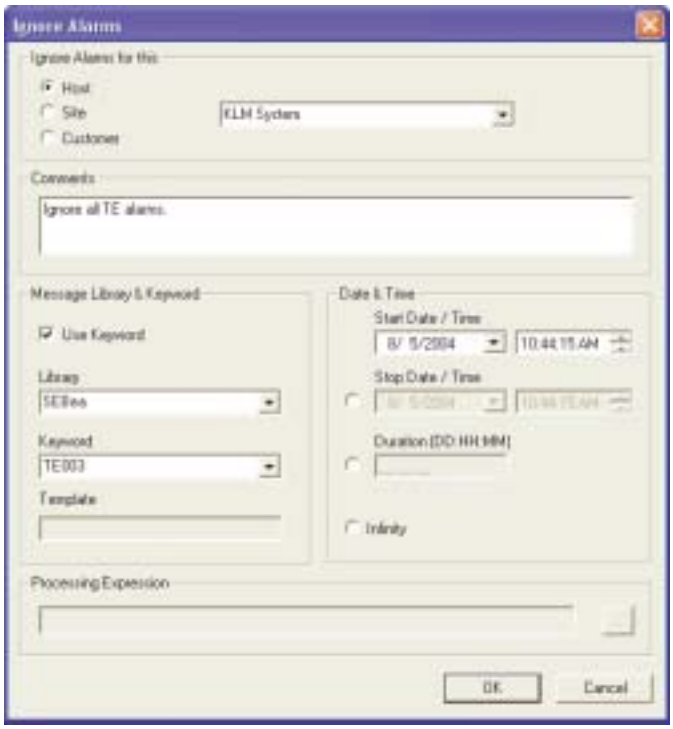
Ignore Alarms

You can define a time to ignore alarms from a particular host, site, or customer. The IRISnGEN system continues to store the alarms in history, but does not display them on the List Viewer.

To ignore alarms

1. Highlight an alarm.
2. Right-click the mouse; then select **Ignore** from the pop-up menu.

The system opens the Ignore Alarms dialog.



3 Click a radio button for the alarm category (Host, Site Customer) you want to ignore; then, select the matching criteria from the list.

4 Type any comments that may be helpful later in the **Comments** field.

5 Select the **User Keyword** checkbox; then, select a library or keyword from the Library or Keyword lists.

6 Type the date and time you want the system to start ignoring the alarms in the **Start Date/ Time** field. If you do not change the date and time, the starting time is immediate. Click the list button to display a calendar and select a different date. Use the arrows in the time field to change the time value.

7 Click a radio button to select an stop time.

Button	What to enter
Stop Date/Time	Type the number of days, hours, and minutes you want your filter active.
Duration (DD:HH:MM)	Type the date and time you want your filter to stop.
Infinity	Use the filter perpetually.

8 Click ***OK*** to save your parameters, or ***Cancel*** to exit without saving.

Access List Viewer History

From the List Viewer, you can launch the History Viewer with the selectivity set so that you can see the history of a particular alarm.

To access the History Viewer for a specific alarm

1. Highlight an alarm.
2. Right-click the mouse; then, select **History** from the pop-up menu.
3. From the submenu, choose one of the following selectivity options (or use the accelerator keys):
   - Customer (ALT+C)
   - Site (ALT+S)
   - Host (ALT+H)

IRISnGEN launches the History Viewer with a history of the alarm limited by the selectivity you chose.

Go Transparent

For troubleshooting and maintenance, you can launch Remote Agent Manager and connect to the host that originated the alarm, providing you secure access to the remote device. Access to a host or to the interactive menu of the remote agent is granted with the main remote agent password or with one of the password definitions available in the remote agent database.

To go transparent

Highlight an alarm and do one of the following:

- Press ***F7***.
- From the List Viewer menu, choose **Alarm > Remote Agent Manager**; then, click the ***Transparency*** button ( ).

See ”Transparency’, page 7-37 for a list of interactive commands.



Batch Status

Use Batch Status to update a range of alarm IDs. For example, you can change the status of all alarms IDs (numbered from 9510 to 9560) from open to closed.

> ***Caution*** *Restrict your updates to fewer than 500 alarms. Updating more than 500 alarms may cause the system to fail to update the screen.*

To update batch status

1. From the List Viewer menu, choose **Batch** > **Status Update**. The system opens the Batch Update dialog.



2. Select an **Update Alarm** option to determine which alarms are to be updated.
   - **Customer**
   - **Site** (default)
   - **Host**

   Based on the alarm you selected in step 1, IRISnGEN will update all alarms assigned to the same customer, site, or host—depending on which option you choose. For example, if the alarm you chose in step 1 is assigned to customer ABC and you choose the Customer option, all alarms assigned to customer ABC will be updated. If the alarm you chose is assigned to site XYZ and you choose the Site option, all alarms assigned to site XYZ will be updated.

3. Select a new alarm status from the **Update Status** list.
   - **No Change** - No change is made to the status of any alarm.
   - **Open** - The status for all alarms in the target set are changed to Open.
   - **Closed** - The status for all alarms in the target set are changed to Closed. All alarms that have a New status will change from New to Open to Closed to preserve the continuity of their status in the alarm history.
   - **New to Open** - The status for all new alarms in the target set are changed to Open.
   - **New to Closed** - The status for all new alarms in the target set are changed to Closed. All alarms that have a New status will change from New to Open to Closed to preserve the continuity of their status in the alarm history.
   - **Open to Closed** - The status for all open alarms in the target set are changed to Closed.
   - **Closed to Open** - The status for all closed alarms in the target set are changed to Open.
4. If you want to leave the status of the alarm you selected unchanged, select the **Update Alarm** check box.

5 Use the next two fields to add comments to all alarms in a target set. Choose which alarms are to get comments by selecting a type from the **Apply to** list.
- **None** - No comments are applied to any alarm.
- **All** - All alarms in the target set will get a comment.
- **New Only** - All alarms with a New status will get a comment.
- **Status Changed** - Only alarms in the target set that have their status changed will get a comment.

6 Type any comments in the **Alarm Comments** field. When updated, IRISnGEN will attach the comment to the tagged alarms. You can see the comment when you look at the Alarm Detail for a particular alarm.

7 Click ***OK*** to continue, or ***Cancel*** to exit without updating the dialog.

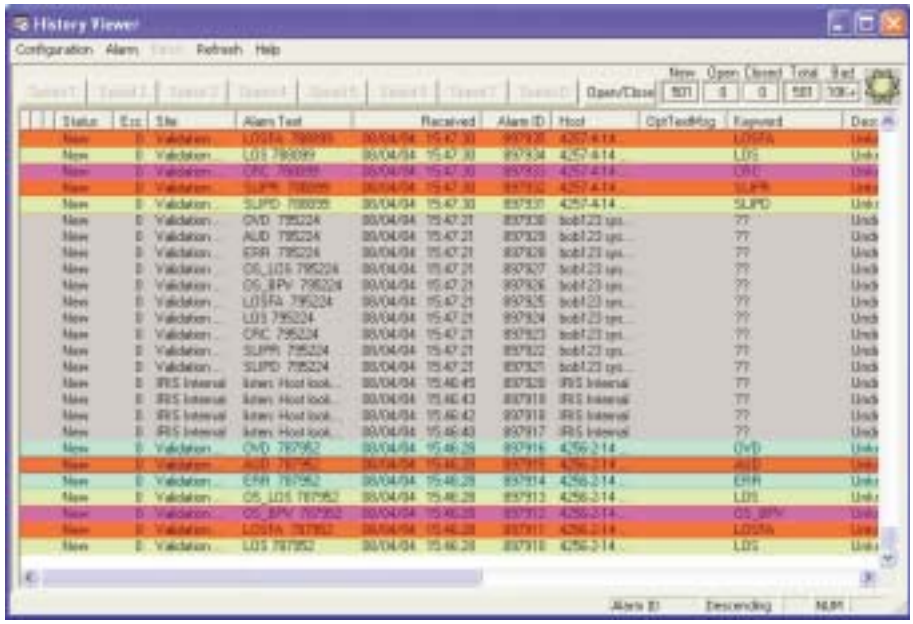


History Viewer

History Viewer gives you access to every alarm stored in the database (except bad alarms). It shows alarms that went to the List Viewer as well as those that did not.

You can selectively view alarms based on several criteria. You create a query to retrieve only the alarms that match your search parameters and to limit the number of alarms displayed. You can control the way alarms display by using selectivity parameters and by specifying limits.

When you choose Alarm History from the IRIS View list, an IRISnGEN Alarm History window, similar to the List Viewer. Note that unlike the List Viewer, the Day/Night indicator is not present and the Ignore Alarm and Remove Alarm options are no longer options. You can define speed buttons separately from the Viewer button option.



Field	Description
Attachment Status	IRISnGEN displays a page icon in the Attachment field of the viewer when the alarm has an attachment. Attachments are sent from the remote agent.
Dispatch Status	A dispatch icon displays in the Dispatch field of the viewer when a technician is dispatched to a site to handle an alarm.
Special Procedure	When a special procedure is attached to the alarm; then, an exclamation mark icon displays in the Special Procedure field of the viewer.
Status	This is an IRISnGEN code showing the current state of the alarm. The status codes are: closed, exported, forwarded, new, open, or ticketed.
Escalation	The alarm's escalation level (0 to 99.

Site	The physical location of the site as defined in the Site record.
Alarm Text	The alarm text as IRISnGEN received it.
Received	The time that the IRISnGEN system received the alarm from the remote agent.
Alarm ID	The number used to identify the alarm. IRISnGEN assigns ID numbers sequentially when it receives the alarm.
Host	The host device associated with the alarm.
OptTextMsg	The optional text message sent from the remote agent.
Keyword	The string of characters contained within the alarm text that matched the message library defined for the host. Keywords can be a single word or groups of words.
Description	The keyword description found in the Message Library.
Severity	A color-coded display identifying the severity of the alarm. Severity is used in the escalation process. Severity codes are: critical, major, minor, informational, or undefined.
Type	Alarm types include: Auto Entry, Batch event, Correlation, Interval, Polled, Polling Event, and Unsolicited.
Occurred	The time the alarm occurred and was recognized by the remote agent.
Customer	The customer associated with the alarm. The customer is at the top level of the IRISnGEN database hierarchy.



Customizing the History Viewer Display

Each alarm displays on a single line in a multi-column format. You can customize this display and rearrange the order of the information in the columns. Once you have the display exactly as you want it, you can save it in your user profile.

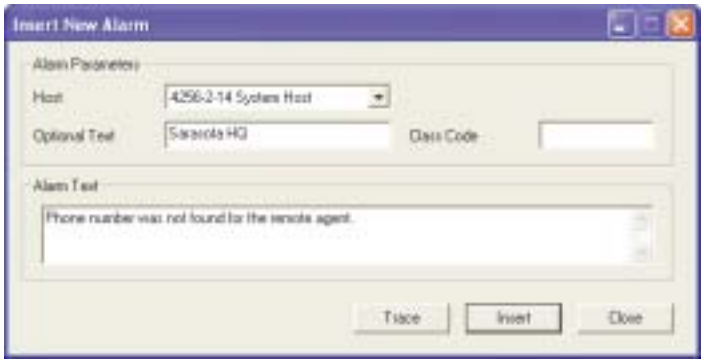
Change the data displayed in the History Viewer by changing the alarm selectivity just as you did in the List Viewer, see ”Selectivity’, page 9-3. You can also define speed buttons for your History viewer, see ”Speed Buttons’, page 9-5.

Add a New Alarm

Sometimes you need to manually enter an alarm into the IRISnGEN system. When you do this, the alarm that you define is inserted into the alarms sent to the List Viewer and assigned a number. It is then treated as any other alarm.

To add a new alarm

1 Choose **Iris > Add New Alarm**. The system opens the Insert New Alarm dialog.



2 Select a host device from the **Host** list. IRISnGEN will treat the alarm is if it came from the host device.

3 Type any addition message in the **Optional Text** field to appear with the alarm.

4 Type the class code for the remote agent in the **Class Code** field.

5 Type a message in the **Alarm Text** field to display in the text area of your alarm message.

6 Do one of the following:

- Click ***Insert*** to send your alarm into the normal alarm processing routines of the IRISnGEN system.
- Click ***Trace*** to trace the progress of the alarm through the Alarm Manager.
- Click ***Close*** to exit the dialog without saving.

View Menu

Server Time

Use this menu option to view the current time on the IRISnGEN server.

To view server time

- From the IRIS menu, choose **View > Server Time**. The Server time displays in the task tray of the Client interface with an “s” preceding it.



If you do not select Server time, the time of the Client machine displays in the same location, without the “s.”

When using the Server Time feature, you may notice a difference between the Client time and the Server time. This indicates your Client PC clock and your Server PC clock are not synchronized. This is usually not a problem unless you are performing tests—such as testing expiration times—in which case you may need to reset the time on either the Client or Server PC. If you choose to reset one of the PCs, be sure to toggle the Server Time off and on after you reset the PC. This will ensure the correct Server time displays in the task tray.

Toolbar, Status Bar, Shortcut Bar

Use the View options to display toolbars, status bars, and shortcut bars in your IRISnGEN windows

To display a toolbar, status bar, and shortcut bar

- From the View menu, select **Toolbars**, **Status Bar**, and/or **Shortcut Bar**.

The shortcut bar displays and contains shortcut buttons for the most common IRISnGEN functions.

Map Viewer

Map Viewer is a geographical representation of your site locations. It shows each site as an color-coded icon on a map. You can click each icon to display more information about a site, or to view alarms, alarm activity, and equipment at that site. The icon indicates which sites have alarms and the severity of those alarms. For example, the icon may appear red to indicate a critical alarm, or green to indicate a minor alarm. You must be a licensed user to use the Map Viewer function.

You can invoke the Map Viewer from IRISnGEN, or as a stand-alone application.



To start Map Viewer

1 Do one of the following:

- From the menu bar, choose **IRIS > View > Map Viewer**.
- From the IRISnGEN toolbar, click the Map Viewer icon ( ).

When you start Map Viewer from your desktop, IRISnGEN displays its login dialog box. Enter your user ID, password, and select a server from the list. The following figure shows a typical login dialog.



Note *You can start the Graphical Viewer from your desktop without running IRISnGEN Client; however, the IRISnGEN server must be running.*

.



2 Click ***Login*** to display the Map Viewer window.

Map Viewer Window

The Map Viewer is tightly integrated with the IRISnGEN Server. While IRISnGEN Server provides all the alarm processing functions, the Map Viewer allows you to pinpoint geographically all the various sites and displays them as color-coded icons on a background map. This geographical site information comes from the IRISnGEN database. All sites configured within IRISnGEN and having valid addresses (or geographic coordinates) display as icons on the vector-based map.

The Map Viewer uses Microsoft MapPoint 2002 as its graphical engine. All the capabilities possible in Microsoft MapPoint are available when you launch Microsoft MapPoint from the Map Viewer. See your MapPoint documentation for more information about MapPoint. The figure below shows a typical Map Viewer window.



Displaying Site Information on the Map Viewer

Your Map Viewer window incorporates all the functions of Microsoft MapPoint. Use MapPoint's Show Information and Show Name features to display site data in an information balloon. The Show Information balloon contains the name of the site, number of alarms, highest severity of alarms, and the number of new, open, and closed alarms. The Show name balloon only displays the name of the site. The following figure shows a typical Show Information balloon.



To display an information balloon

Do one of the following:

- Click a site icon ( ); then, choose **View > Show Information**.
- Click a site icon ( ); then, press ***F8***.
- Click a site icon ( ); then, right-click the mouse to display the pop-up menu and select **Show Information** or **Show Name** from the menu.

To close an information balloon

Do one of the following:

- Click the **Close** icon ( ) in the upper-right corner of the balloon.
- Choose **View > Show Information**.

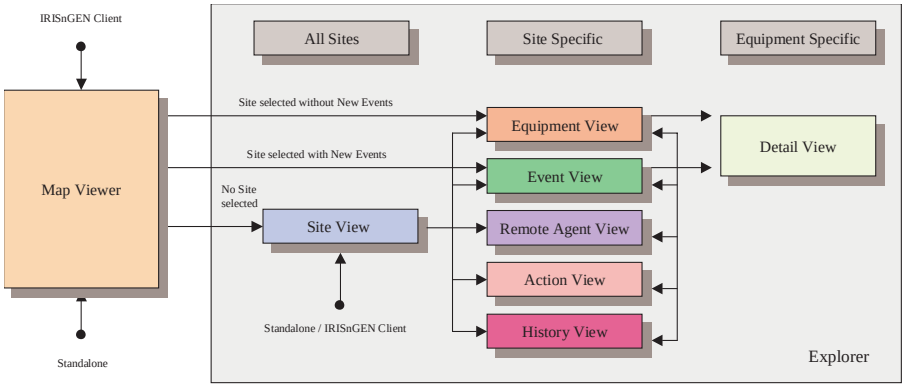
Using Equipment Explorer with Map Viewer

The Map Viewer uses the Equipment Explorer application to display detailed information about a site. From the Map Viewer window:

- Double-click any highlighted site icon showing event activity to launch the Equipment Explorer's Event List View window. This window displays a list of all the events for the selected site, see "Event List Viewer', page 9-47.
- Double-click a site that does not show any events to launch the Equipment Explorer's Equipment View window. It displays a list of all equipment for the selected site, see "Equipment View', page 9-39.
- Double-click the background map without selecting a site to launch the Equipment Explorer's Site View window displaying a list of all sites, see "Site View', page 9-37.

When the SEBea remote agent fails to respond to a PING request from the IRISnGEN Server, it generates a communication error event. IRISnGEN treats this event like any other event with the site containing this SEBea receiving the event. The site icon highlights to indicate event activity. You can double-click the icon to investigate the event. The Map Viewer launches the Equipment Explorer's Event View window displaying all the events for the selected site. You can then select the event that indicates an unresponsive SEBea, which will take you to the Remote Agent View that lists all the SEBea remote agents at that particular site.

The following figure shows the interaction between the Map Viewer and the Equipment Explorer application.



Map Viewer Pop-up Menu

From the Map Viewer pop-up menu, you can select items that control the Viewer settings that display on the Map Viewer window, choose speed buttons that quickly change the selectivity of the Map Viewer, or you can launch other Viewer windows.

To display the Map Viewer pop-up menu

1. Right-click the **Map Viewer** icon ( ) in the system tray to display the Map Viewer pop-up menu.
2. Choose an item from the menu list.
   The following figure shows the Map Viewer pop-up window.



- **About Map Viewer** – Displays the version number for the Map Viewer you are running
- **Help** – Displays context-sensitive help for the Map Viewer.
- **Speed Buttons** – Speed buttons let you quickly change the display on the Map Viewer window so that you can see specific site and event information. You can preprogram your speed buttons in the List Viewer and use them in the Map Viewer.
- **Map Settings** – Displays the Map Setting dialog. Use this dialog to set the displays on the Map Viewer map, for example, pushpin icons, event severity colors, and initial map displays, see ”Map Settings’, page 9-31.
- **Map Selectivity** – Displays the Map Selectivity dialog. Use this dialog to define site or event selectivity for the Map Viewer window. You can also make selections to save as a speed button, see ”Map Selectivity’, page 9-27.
- **Address Lookup –** Displays the Address Lookup dialog from which you can enter and store addresses and map coordinates for frequently used sites, see ”Address Lookup’, page 9-26.
- **Refresh** – Refreshes the Map Viewer window.
- **Equipment Explorer** – Opens the Equipment Explorer window in Site View mode. You can use the Equipment Explorer to manage the equipment configured for the sites, see ”Equipment Explorer’, page 9-32.
- **Event List Viewer –** Opens the List Viewer window displaying all Map Viewer alarms color-coded to show severity and status, see ”List Viewer’, page 9-2.
- **Event History Viewer –** Opens the Alarm History window that gives you access to all Map Viewer alarms stored in the database. It shows alarms that went to the Viewer as well as those that did not, see ”History Viewer’, page 9-17.
- **Exit –** Exit Map Viewer.

Address Lookup

Use the Address Lookup to pinpoint site location on the MapPoint map. The sites appear as icons on the map.

Each site defined in the IRISnGEN system appears in the Address Lookup list. Each Address Lookup record contains all the information defined in the site record. However, you can add addition address information to the record to help MapPoint pinpoint site location more accurately on the map.

Each time you add a new site, its corresponding Address Lookup record displays as an invalid coordinate site when you start Map Viewer. At that time, you can enter any additional information, if necessary, and press the Update button to update and add the Address Lookup record. The update will also produce a list of possible matches that display in the Possible field at the bottom of the window. Double-click one of those possible matches to use as your default. The address for that match choice is the location that appears on the MapPoint map.





Note *When you make any change or addition to an Address Lookup record, IRISnGEN automatically updated the corresponding Site record.*

To use Address Lookup

1. In the system tray, right-click the **Map Viewer** icon ( ); then, select **Address Lookup**.
2. Type the name of the Address Lookup record in the **Name** field; then, type any additional comments or hypertext in the **Notes** field.
3. Type the site address in the next seven fields.



4 Type the central phone number of the site (40 characters maximum) in the **Telephone** field. This field is for your own reference and is not used by the IRISnGEN system.

5 Type the latitude of the site in the **Latitude** field and the longitude in the **Longitude** field, or double-click a possible address match in the field below to automatically enter the latitude.

6 Click an entry in the **Possible address matches** field to populate the Match Type, Latitude and Longitude fields to the right of the Address List. Double-click an entry to replace the site's latitude and longitude in those fields above.

7 Select the **Automatic address lookup** checkbox to enable or disable the automatic lookup. When enabled, the system performs an automatic address lookup after you modify the site address. The lookup is done immediately for combo box changes and after two seconds for edit box changes. The delay for edit boxes prevents a lookup while you are busy typing an address. Pausing for two seconds will start the lookup.

8 The **Match Type** field displays the type of address match selected in the Address List.

9 Click and entry in the **Possible address matches** field to populate the Latitude and Longitude fields with the correct latitude and longitudes.

10 Click the **All Sites** radio button to view all sites defined by the Site Selectivity or click the **Invalid Coordinate Sites** radio button to view all sites with invalid latitude and longitude coordinates. The Address Lookup dialog will start with this option by default.

11 Select a button.

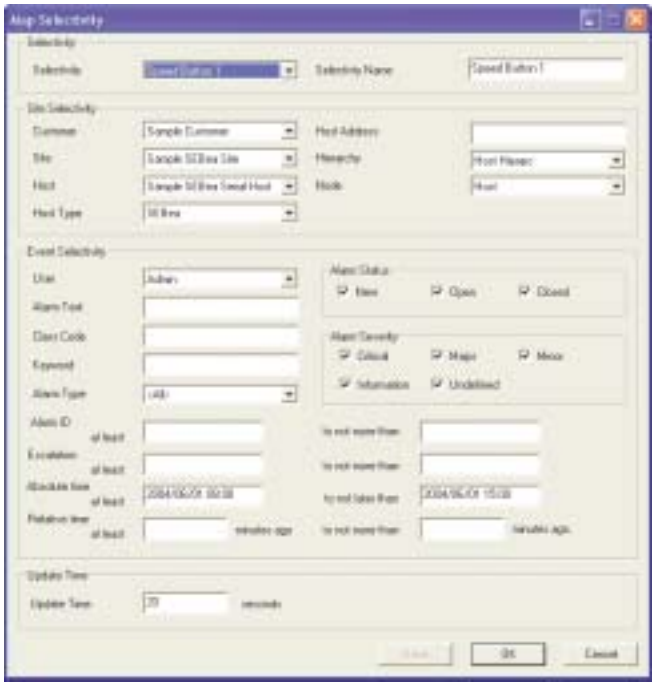
Button	Description
Previous	Move to the previous site record.
Next	Move to the next site record.
Find	Find and list possible address matches in the Address List. You must press this button, if you did not enable the Automatic Lookup feature.
Update	Update any changes made to the record. Clicking the Update button will also update the Site record, see"Site', page 2-12.
Exit	Close the dialog box.

Map Selectivity

Use Map Selectivity to determine which sites display in the Map Viewer window and which events display for each site. You can save your selectivity and assign them to speed buttons.

Speed buttons provide a convenient way to quickly change the selectivity of the Map Viewer to predefined settings. The speed buttons you define are only available for you and are saved in your user profile. The speed buttons are available each time you log into the IRISnGEN system. Other users can create their own speed button definitions. You can define up to eight Map Selectivity speed buttons.





To create a Map Selectivity record

1 Open the Address Lookup dialog and do one of the following:
- Choose **Tools > Map Selectivity**.
- Press **ALT + TS**; then choose **Map Selectivity**.
- In the system tray, right-click the icon; then, choose **Map Selectivity**.

2 Enter the selectivity for your record.

Field	Description
Selectivity	Select a speed button from the list.
Selectivity Name	Type a name for this speed button. The name you enter will appear in Map Viewer's pop-up menu.

3 Enter the site parameters from the **Site Selectivity** lists.

Field	Description
Customer	To limit your selectivity to a single customer, select that customer from the list, or select ALL customers.
Site	To limit your selectivity to a single site, select that site from the list, or select ALL sites.
Host	To limit your selectivity to a single host, select that host from the list, or select ALL hosts.

Host Type	To limit your selectivity to a single host type, select that host type from the list, or select ALL host types.
Host Address	Enter a host address that identifies a specific device on your network, or a device attached to a hard alarm contact on the remote agent.
Hierarchy	Select a hierarchy from the list.
Node	Select a node from the list.

4 Enter the event parameters in the **Event Selectivity** fields.

Field	Description
User	Select a user from the list. The Map Viewer will display only those alarms that the user took action on.
Alarm Text	Type the text in the field using the % symbol as a wildcard character. The Map Viewer only displays alarms that have that text within the alarm message. If you do not use a wildcard, you must enter the entire text.
Class Code	Type a one- or two-character class code in the text box. The Map Viewer displays only alarms with that code.
Keyword	Type the keyword text in the box. You can use the % wildcard character, or enter the entire keyword text.
Alarm Type	Select an alarm type from the list.
Alarm ID	Type a range of alarm IDs in the two fields, or just enter one parameter.
Escalation	Type a range of escalation numbers in the two fields, or just enter one parameter. Escalation numbers can be from 0 to 99.
Absolute time at least	Make two entries to establish an Absolute Time range or just enter one parameter. Times are in the format *yyyymmddhhmm*, where *yyyy* is the four-digit year, *mm* is the two-digit month, *dd* is the two-digit day, *hh* is the two-digit hour, and mm is the two-digit minute. Do not enter any slashes as separators between the fields. IRISnGEN does this for you.



Relative time at least	Make two entries to establish a Relative Time range or just enter one parameter. In the **at least** heading, enter how long ago you want to show alarms (as in, alarms from twenty minutes ago); in the **not more than** field, enter the most recent time you want to show alarms.
Alarm Status	Select the checkboxes for the alarm status you want to include.
Alarm Severity	Select the checkboxes for the severity codes you want to include.

5 Type the number of seconds that IRISnGEN should wait before refreshing Map Viewer in the **Update Time** field. You cannot enter a refresh time less than 5 seconds. The default is 20 seconds.

6 Click ***Save*** to save your selectivity record, or click ***Cancel*** to cancel without saving.

To use the Map Viewer speed buttons

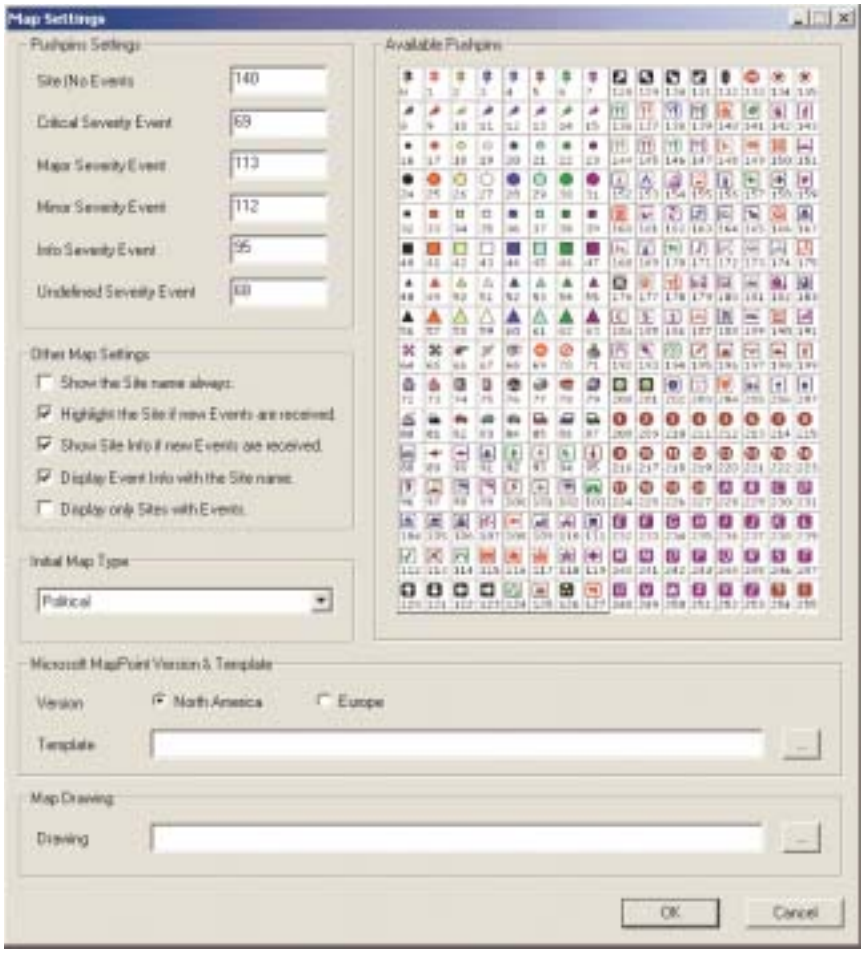
1 Right-click the **Map Viewer** icon in the system tray to display the Map Viewer pop-up menu.

2 Select a speed button from the menu list.



Map Settings

Use the Map Settings dialog to set the displays on the Map Viewer map. You can define settings for a site and site events. As the severity of an event changes, so will the pushpin displays on the Map Viewer.



To define the map settings

1. Open the Map Selectivity dialog and do one of the following:
   - Choose **Tools > Map Selectivity**.
   - Press **ALT + TS**; then choose **Map Selectivity**.
   - In the system tray, right-click the icon; then, choose **Map Selectivity**.
2. Enter the pushpin settings.
3. Type an icon index code for each pushpin setting for each site or event type In the **Pushpins Settings** fields. For example, enter 140 in the Site field to display the icon on the Map Viewer for sites with no active events.
4. Select the **Other Map Settings** checkboxes for each settings you wish to display in your Map Viewer window.
5. Select a map type from the **Initial Map Type** list. Each map can display in five different modes: Road Map, Road & Data Map, Data Map, Terrain Map, and Political Map.
6. Click a **MapPoint Version** radio button: North America or Europe.

7 Type the path and filename of the default map to open at startup in the **Template** field, or click the button to open the Open dialog and navigate to the map template directory. Choose map template from the directory.

8 Type the path and filename of the default map drawing to appear at startup in the **Drawing** field. The drawing file may be used to customize the map or click the button to open the Open dialog and navigate to the map drawing directory. Choose map drawing from the directory.

9 Click ***OK*** to save your settings record.

Equipment Explorer

If you are licensed to use Teltronics' Multi-Drop Alarm Delivery and Control System, you can use the Equipment Explorer application to monitor, manipulate, and control the equipment, and the events generated by that equipment, at the various sites. The Equipment Explorer shows detailed and status information about any selected site, event, or equipment located at a site. You can then issue actions in response to a particular event condition.

Launching Equipment Explorer

You can launch the Equipment Explorer from the IRISnGEN Client toolbar, main menu, Map Viewer, or as a standalone application to display a list of all available sites. You can also select a specific site or select any of the other available Views.

To start Equipment Explorer

Do one of the following:

- On the IRISnGEN toolbar, click the Equipment Explorer icon ( ).
- From the IRIS menu, choose **View > Equipment Explorer**.

When you launch the Equipment Explorer from the Map Viewer, the system presents the View based on the alarm activity. For example:

- Double-clicking an icon for a particular site that does not have any alarm activity, the Explorer displays an Equipment View window containing all the equipment configured for that site.
- Double-clicking an icon for a site that has an active alarm, the system displays an Event View window containing all the events for that site.
- Double-clicking the map background (not on a site), the system displays the Site View window.

Regardless of how you start the Equipment Explorer, you can select the various Views by clicking the navigation buttons available on each View.

Using Navigation Buttons

Navigation buttons appear on the right side of the window and display other View windows. Use these buttons to display more information about equipment, events, history, or remote agent information.

To use the navigation buttons

In the main area of the Equipment Explorer window, click on a icon to highlight it and choose one the following navigation buttons:

- **Sites –** Displays a list of all sites configured in IRISnGEN.
- **Equipment–** Displays a list of all equipment configured for a site.
- **Detail –** Displays a list of all the control elements for a piece of equipment.
- **Events –** Displays a list of all events for a site.



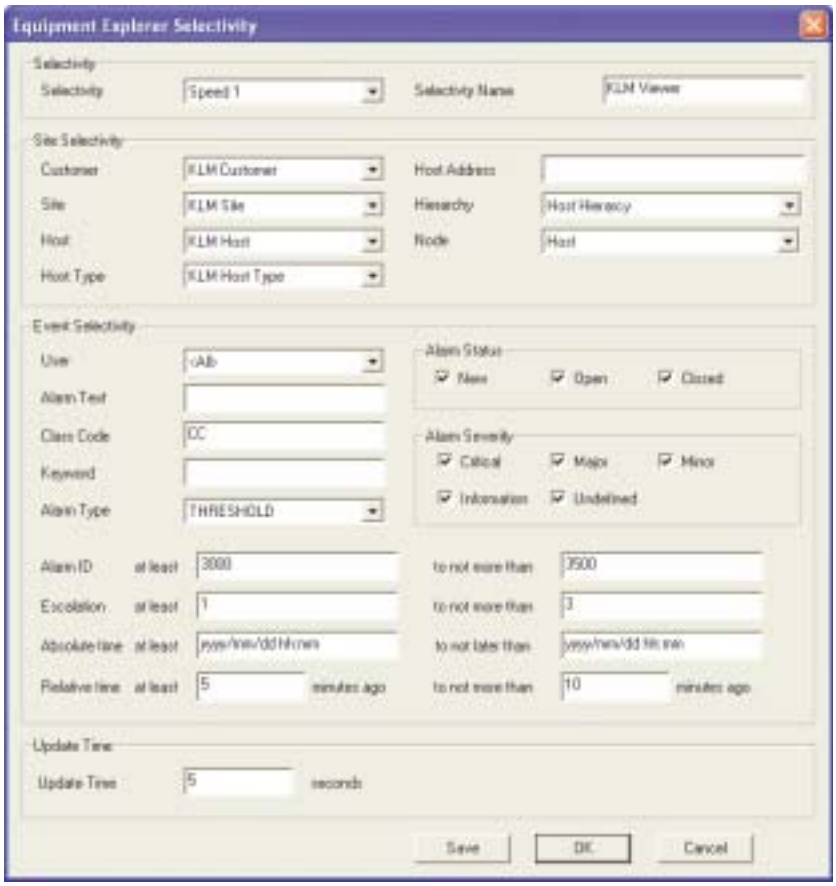
- **Action –** Displays a list of all the available actions for a site.
- **History –** Displays a list of all past requests executed for a particular site, including action, status, reset, and ping.
- **Remote Agents –** Displays a list of all SEBea remote agents at a site.
- **Back** – Return to the previous window.
- **Close** – Exit from the Equipment Explorer application.

Changing Equipment Explorer Selectivity

Use the Equipment Explorer Selectivity dialog to limit the information displayed on the Site View window.

To change the Equipment Explorer selectivity settings

1 Click the **Selectivity** button to open the Equipment Explorer Selectivity dialog.



2 Set the selectivity fields for the display. You may select as many or as few parameters as you wish.
   - Click the down arrow and choose a speed button from the **Selectivity** drop-down list. The button name will change when you enter a new name in the Selectivity Name field.
   - Type a name for this speed button in the **Selectivity Name** field. The name you enter will appear in the viewer's pop-up menu.

3 Fill in the Site Selectivity parameter fields to define you selectivity record.

- To limit your selectivity to a single customer, choose that customer from the **Customer** drop-down list, or choose **ALL** customers.
- To limit your selectivity to a single site, choose that site from the **Site** drop-down list, or choose **ALL** sites.
- To limit your selectivity to a single host, choose that host from the **Host** drop-down list, or choose ALL hosts.
- To limit your selectivity to a single host type, choose that host type from the **Host Type** drop-down list, or choose ALL host types.
- Enter a host address that identifies a specific device on your network, or a device attached to a hard alarm contact on the remote agent in the **Host Address** field.
- Choose a hierarchy from the **Hierarchy** drop-down list.
- Choose a node from the **Node** drop-down list.

4 Fill in the Event Selectivity parameter fields to define the events displayed.

- Choose a user from the **User** drop-down list. The viewer only displays those alarms that the user took action on.
- Enter the text in the box using the % symbol as a wildcard character in the **Alarm Text** field. The viewer only displays alarms that have that text within the alarm message. If you do not use a wildcard, you must enter the entire text.
- Enter a one- or two-character class code in the **Class Code** field. The viewer displays only alarms with that code.
- Enter the keyword text in the **Keyword** field. You can use the % wildcard character, or enter the entire keyword text.
- Choose an alarm type from the **Alarm Type** list.
- Set the alarm ID in the **Alarm ID** field.Under the **At Least heading**, type the smallest alarm ID you wish to see; under the **Not More Than** heading, type the largest alarm ID you wish to see. You can select a range of alarm IDs by making entries in both fields, or you can enter just one parameter.
- Set the escalation parameters in the **Escalation** field. **Under the At Least** heading, type the smallest escalation number you wish to see; under the **Not More Than** heading, type the largest escalation number you wish to see. You can select a range of escalation numbers by making entries in both fields, or you can enter just one parameter. Escalation numbers can be from 0 to 99.
- Set the absolute time parameters in the **Absolute time at least** field. Make two entries to establish an Absolute Time range or just enter one parameter. Under the **At Least** heading, enter the start time; under the **Not More Than** heading, enter the end time. Times are in the format *yyyymmddhhmm*, where *yyyy* is the four-digit year, *mm* is the two-digit month, *dd* is the two-digit day, *hh* is the two-digit hour, and *mm* is the two-digit minute. Do not enter any slashes as separators between the fields; the IRISnGEN system does this for you.
- Make two entries to establish a Relative Time range or just enter one parameter in the **Relative time at least** field. Under the **At Least** heading, enter how long ago you want to show alarms (as in, alarms from twenty minutes ago); under the **Not More Than** heading, enter the most recent time you want to show alarms.
- The IRISnGEN status code shows the current state of any alarm. Choose one or more **Alarm Status** checkboxes to select alarm status .
- Check the **Alarm Severity** checkbox for the severity code you want to view. You can select as many severity codes as you wish.

5 Type the number of seconds that IRISnGEN should wait before refreshing the viewer window in the **Update Time** field. You cannot choose a refresh time less than 5 seconds. The default is 20 seconds.



6 Click ***OK*** to save your selectivity record.

7 Click ***Cancel*** to cancel your selectivity record without saving.

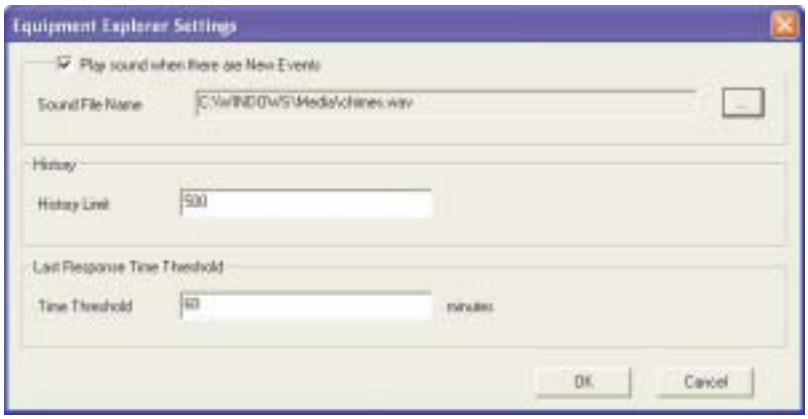
Programming Equipment Explorer Settings

Use the Equipment Explorer Settings dialog to choose an audio file that sounds when the Equipment Explorer receives an event. The dialog also lets you chose the number of events to display in the History View window.

Note *Only users with permission rights can access the Equipment Explorer Settings dialog. Check with your system administrator if you are unsure of your permission rights.*

To display the Equipment Explorer Settings dialog

- Click the **Settings** button. The system opens the Equipment Explorer Settings dialog.



To add sounds to an incoming event

1 Click the **Play sound when there are New Events** checkbox; then, press the **Browse** button (...) to display the Open dialog.

2 Navigate to the directory containing your .WAV file; then, click ***Open***.

Note *The system only accepts .WAV files (*.wav).*

3 In the **History Limit** field, enter the maximum number of events to display. The default is 500.

Note *This setting applies to all sites.*

4 Type a last time threshold value (in minutes) in the **Time Threshold** field. The system will redisplay the event when the threshold is reached.

Changing Modes

The Mode feature lets you display window information with a slightly different look. For example, you can display the view data as icons, or with detailed information. Experiment with the various modes to find the one that best suits your needs.

To change a View mode

Select a mode from the Mode list. Select one of the following:

- Icon
- List
- Details

Sample Mode Views



Figure 1 - View Window in Icon Mode



Figure 2 - View Window in List Mode

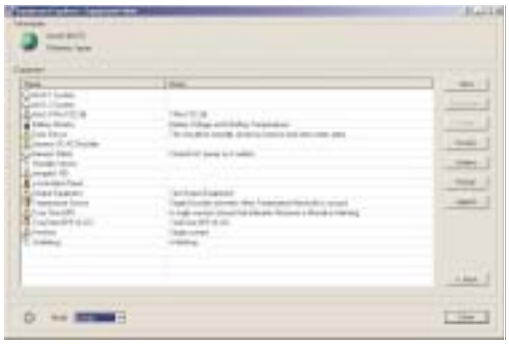


Figure 3 - View Window in Detail Mode

Displaying Several View Windows at Once

You can display several Explorer windows at the same time. For example, you may choose to display the Equipment View, Detail View, and Action View (or any combination of the View windows) to get a custom display.

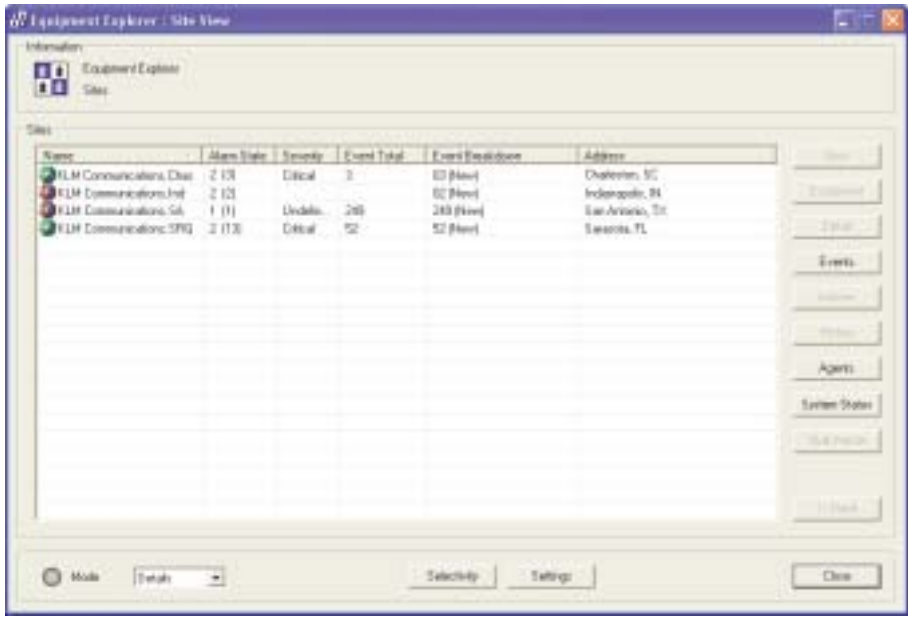
Site View

The Site View window displays the sites and their addresses configured in your IRISnGEN system along with the event information for each of those sites. The event information includes the total number of alarms for that site, a breakdown by event status (New, Open, Closed), and the highest alarm severity for all events at that site.

To display the Site View window

Do one of the following:

- On the IRISnGEN toolbar, click the **Equipment Explorer** icon ( ).
- From the Map Viewer pop-up menu, choose **Equipment Explorer**.
- Double-click the **Map Viewer** background.
- Click the **Site** button (if enabled) from any of the other View windows.



The following list describes the fields on the Site View window in Details mode.

Field	Description
Name	The name of the site, as defined in the IRISnGEN Customer window, see ”Customers’, page 2-1.
Alarm State	The number of equipment and control elements (in brackets) that are currently in an alarm state. ***Note*** *A site’s icon will only highlight if it has control elements in an alarm state. When an alarm clears, the icon returns to its default state.*
Severity	The highest severity for the alarms (events).
Total	The total number of alarms (New, Open, Closed) for that site.
Event Breakdown	The breakdown of alarms (New, Open, Closed) for that site. ***Note*** *If there are no alarm statuses for that site—for example, no Open alarms—then no alarms for that status will display in the window.*
Address	The customer’s address, as defined in the IRISnGEN Customer window, see ”Customers’, page 2-1.

Changing Selectivity

You can customize your Site View display by choosing the Selectivity button. The system displays the Map Selectivity dialog. Use this dialog to select which site to display and which combinations of site, alarm type, alarm severity, and/or alarm aging information you wish to include. You can choose a single site to display, or all sites. You can also configure the update interval in this dialog to set the refresh time for the Equipment Explorer. For more information about the Map Selectivity dialog, see ”Map Selectivity’, page 9-27.

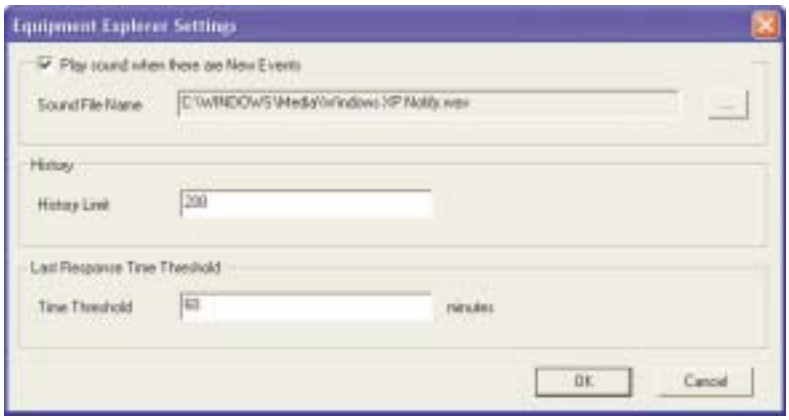
Changing Settings

You can set the display thresholds and add sound to your View displays by choosing the Settings button. Use the Sound File option to associate sound with an incoming event. The system displays the Equipment Explorer Settings dialog, shown below.

To display the Equipment Explorer Settings dialog

1 On the Site View window, click the **Settings** button.





2 Select the **Play sound when there are New Events** checkbox to enable the Sound File option. Use this option to associate a sound with an incoming event.

3 Click the ***Browse*** button (...) to browse to the directory containing your .WAV file. Select a .WAV file from the list. You can only use .WAV files with this option.

4 Type the maximum number of entries to display on the History View window in the **History** field. The default is 200.



Note *This is the maximum number of entries for all sites, not per site.*

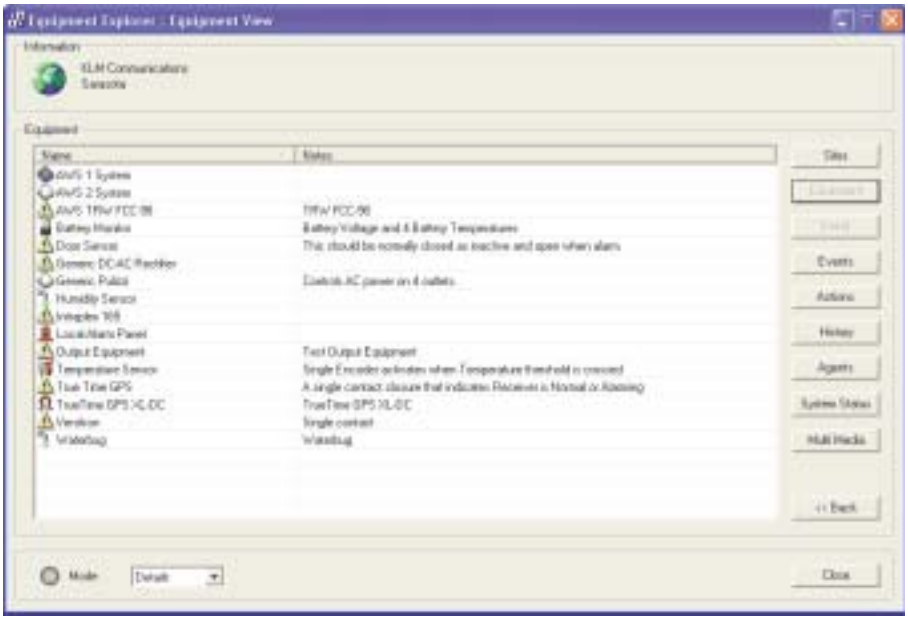
5 Type the number of minutes after which IRISnGEN considers the remote agent unresponsive and displays the remote agent icon as red in the **Last Response Time Threshold** field. The default is 60 minutes.

Equipment View

The Equipment View window displays all equipment configured and assigned in your IRISnGEN system for a specific site. Use this window to view all your site equipment and to select navigation buttons to display detailed information about each piece of equipment.

To display the Equipment View window

- From any View window, click ***Equipment***.
- From the Map Viewer window, double-click a site icon that shows no alarm activity.



The following list describes the fields on the Equipment View window in Details mode.

Field	Description
Name	The name of the equipment as defined in the Equipment Library, see ”Equipment’, page 5-47. This is a display-only field.
Note	Additional notes for the equipment, as defined in the Equipment Library, see ”Equipment’, page 5-47. This is a display-only field.

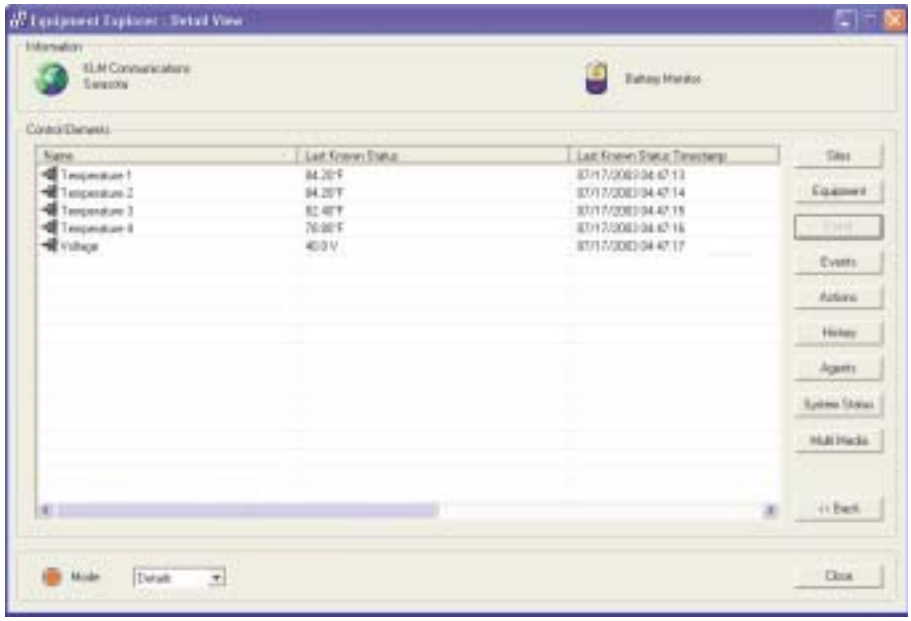
Detail View

The Detail View window displays all the control elements for a selected piece of equipment. Use this window to view all your control elements, get the status of a control element.

To display the Detail View window

Do one of the following:

- From the Equipment View window, double-click an equipment icon.
- Highlight an equipment icon; then, click ***Detail***.



The following list describes the fields on the Detail View window in Details mode.

Field	Description
Name	The name of the control element as defined in the Equipment Library, see ”Equipment’, page 5-47. This is a display-only field.
Last Known Status	The system displays the latest status for the selected control element. The status settings are predefined at the factory and are display-only in this field.
Last Known Status Timestamp	The date and time of the last status reading. This is a display-only field.

Get Status

You can retrieve the current status for any control element listed in the Detail View window. Click a control element icon to display the Get Status button at the bottom of the window. Choose the button or simply double-click the control element icon. The system then displays the status of the request: PENDING, RUNNING, ON HOLD, FAILED, or COMPLETED.

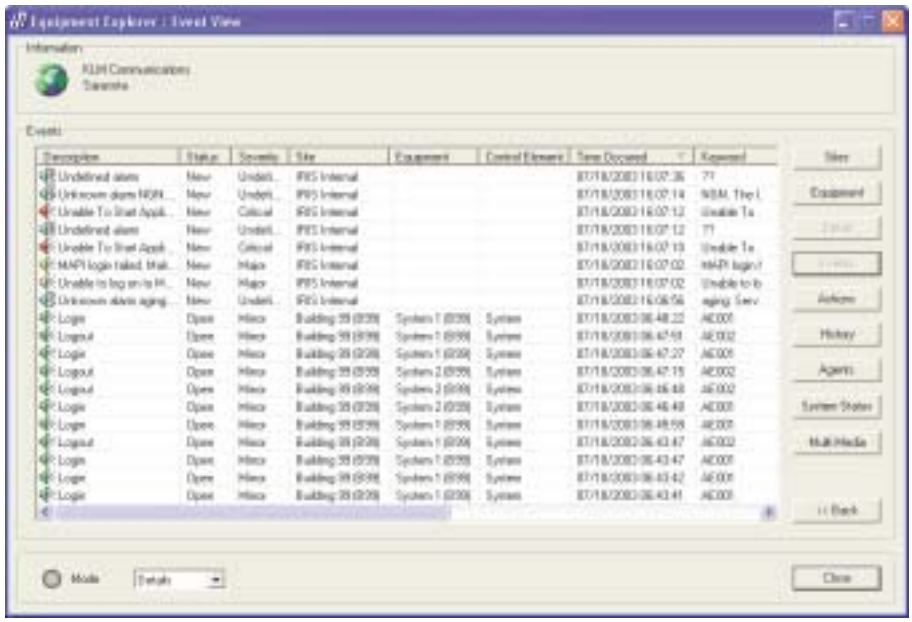
Event View

The Event View window displays all alarm activity for the selected site. Use this window to view detailed information about the event alarm.

To display the Event View window

Do one of the following:

- Highlight a site icon; then, click **Event**.
- From the Map Viewer, double-click a site icon.
- From the Site View window, double-click a site icon.



The following list describes the fields on the Event View window in Details mode.

Field	Description
Description	A short, customized description of the event as defined in the Message Library, see ”Creating and Editing Message Library Alarm Entries’, page 5-37.
Status	The latest alarm status for the selected event.
Severity	The severity code for the event as defined in the Message Library, see ”Creating and Editing Message Library Alarm Entries’, page 5-37.
Equipment	The equipment on which the event occurred.
Control Element	The equipment’s control element on which the event occurred.
Time Occurred	The time the event occurred.
Keyword	A character string defined in an IRISnGEN Message Library describing the event.
Event Text	A character string defined in an IRISnGEN Message Library describing the event.

Action View

The Action View displays all actions available for execution at the selected site or equipment. Use this window to issue actions—for example, turning on an outlet connector.

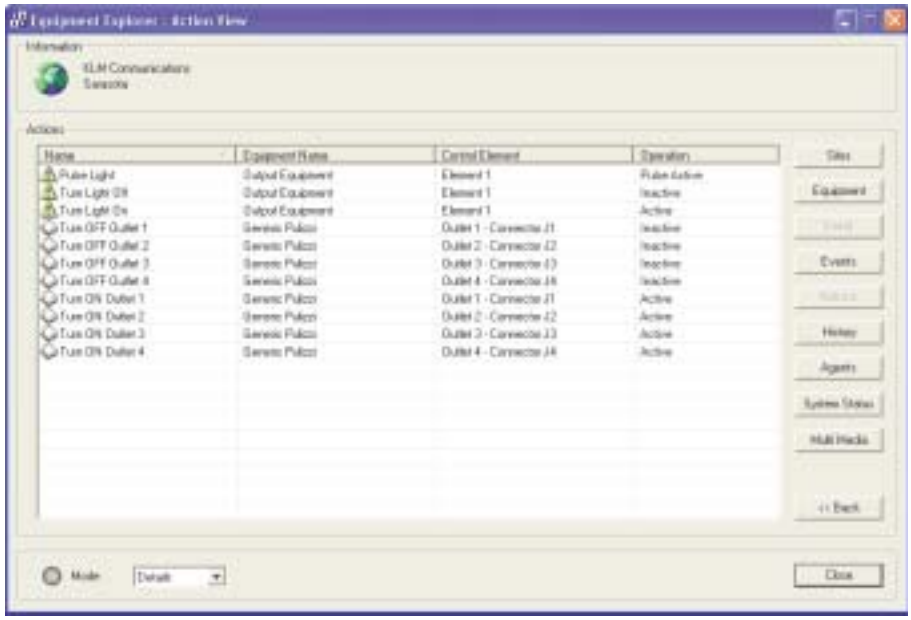
To display the Action View window

Do one of the following:

- Highlight a site icon; then, click ***Action***.
- Select the Action button from any View window, if available.

To display the Action View window for specific equipment

- Highlight and equipment icon in the Equipment View; then, click ***Action***.



If you first select an equipment icon from the Equipment View, and then the Action button, the Action View displays only those actions available for the equipment you selected. The icon for the selected equipment displays in the right column of the Action View window and indicates that the actions are only available for that equipment, not the entire site. In this case, you need only to double-click the icon to perform the action, or highlight an action icon and click the Execute button. The system then displays the status of the request: PENDING, RUNNING, ON HOLD, FAILED, or COMPLETED.

The following list describes the fields on the Action View window in Details mode.

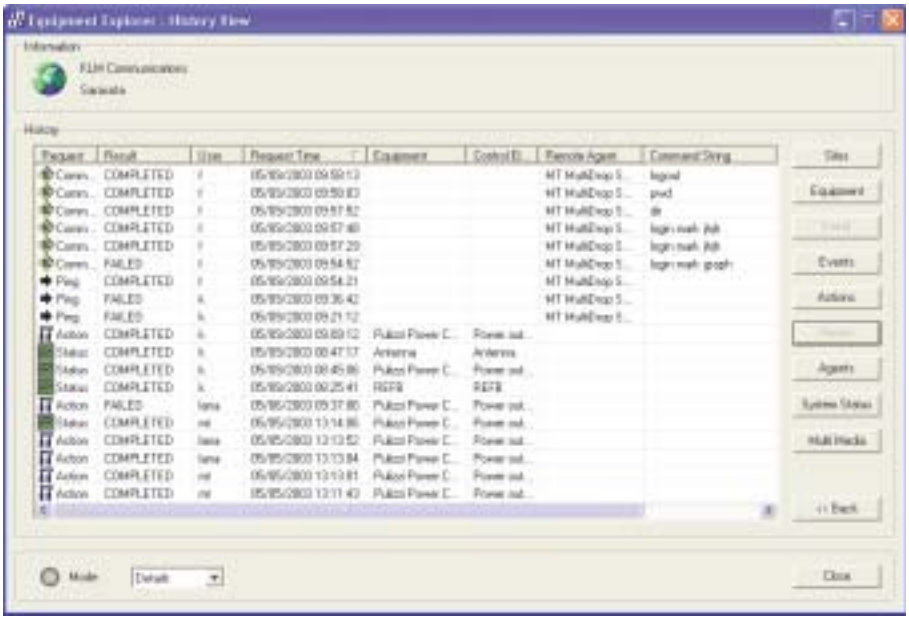
Field	Description
Name	The name of the action as defined in the Equipment Action library, see ”Equipment Actions’, page 5-50.
Equipment Name	The name of the equipment.
Control Element	The name of the control element on the equipment.
Operation	The action to perform as defined in the Equipment Action library, see ”Equipment Actions’, page 5-50.

History View

The History View displays a history of all requests issued by users for a specific site. Requests include:

- Action
- Status
- Reboot
- Date/Time
- Unknown
- PING
- Command

Although command, date/time, or unknown requests cannot be issued from the Equipment Explorer, they do appear in the History View window.



The following list describes the fields on the History View window in Details mode.

Field	Description
Request	The type of request issued.
Result	The status of the request: PENDING, RUNNING, ON HOLD, FAILED, or COMPLETED.
Requested Time	The time the request was issued.
Equipment	The equipment on which the request was made.
Control Element	The control element of the equipment on which the request was made.
Remote Agent	The remote agent that made the request (reboot or PING).
Command String	The command that was issued by the user. (Accessible to Teltronics personnel for troubleshooting purposes.)

Remote Agent View

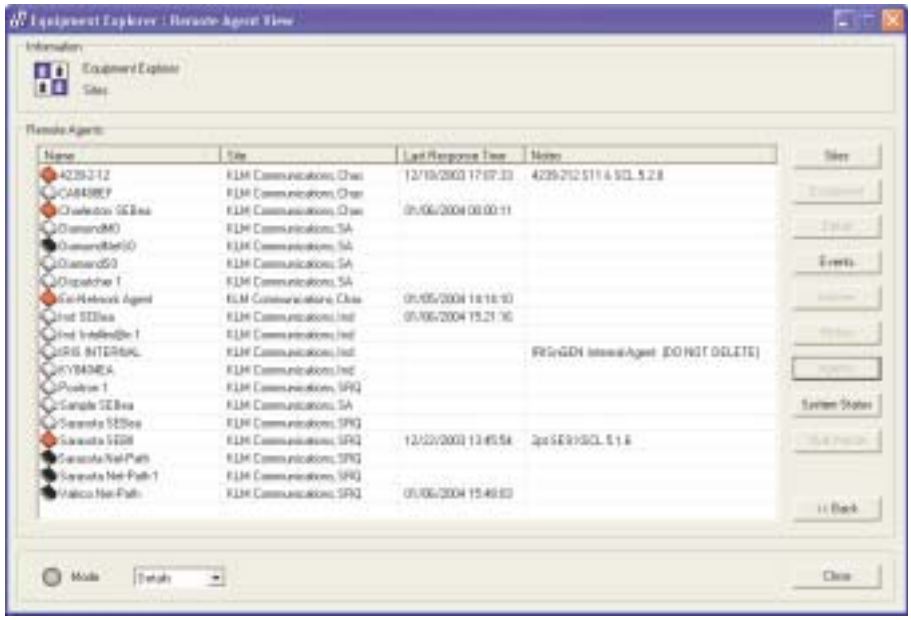
The Remote Agent View displays all SEBea remote agents configured for a selected site, or all sites. IRISnGEN generates events when an SEBea remote agent does not respond to a PING command issued during the polling cycle. When this happens, you can select that event in the Event View to invoke the Remote Agent View for the site that generated the event. You can PING any remote agent displayed in the Remote Agent View simply by double-clicking the SEBea remote agent icon, or by selecting the PING button. You can reboot (reset) the SEBea by selecting the Reboot button.

To display the Remote Agent View dialog

Do one of the following:

- Double-click an event icon (indicating an unresponsive remote agent) in the Event View window.
- Click the ***Remote Agent*** button from any other View window.
- From the Explorer application, hold down the ***Shift*** key and select the Agents navigational button.





The following list describes the fields on the Remote Agent View window in Details mode.

Field	Description
Name	The name of the SEBea as defined in the Remote Agent (SEBea) window, see”SEBea/ NET-PATH Remote Agent Tab’, page 2-23. This is a display-only field.
Site	The name of the site at which you installed the remote agent.
Last Response Time	The last date and time the remote agent responded.
Notes	Additional notes for the SEBea as defined in the Remote Agent (SEBea) window, see ”SEBea/ NET-PATH Remote Agent Tab’, page 2-23. This is a display-only field.
Reboot	When you highlight a remote agent, IRISnGEN adds the Reboot button to the display. Click the Reboot button to reload the remote agent device. ***Warning*** *Do not reboot the remote agent unless you are absolutely sure you want to do so. Rebooting a remote agent may cause it to lose data.*



Ping	When you highlight a remote agent, IRISnGEN adds the Ping button to the display. Click the Ping button to determine the availability of a remote agent. If the ping is successful, the remote agent icon that appears on the screen will be white. If the ping fails, the icon appears red. Corrective action should be taken to determine why the ping was unsuccessful.

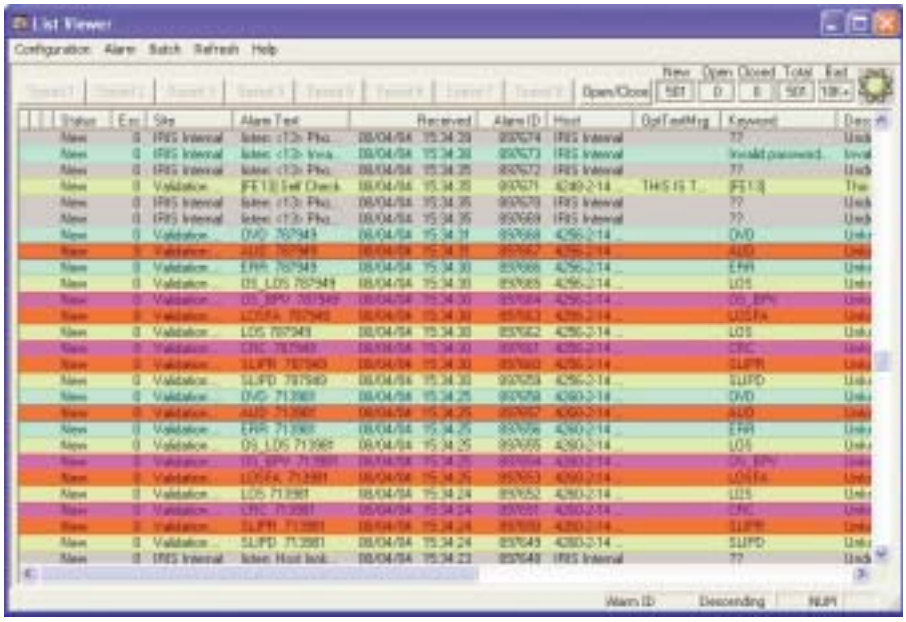
Icons and Colors

When displaying the Remote Agent View window, notice the remote agent icons that appear before each name. These icons can help you quickly identify the type of remote agent device and the device state.

Icon	Device	State
	SEBea	Responsive
	SEBea	Unresponsive
	NET-PATH	Responsive
	NET-PATH	Unresponsive

Event List Viewer

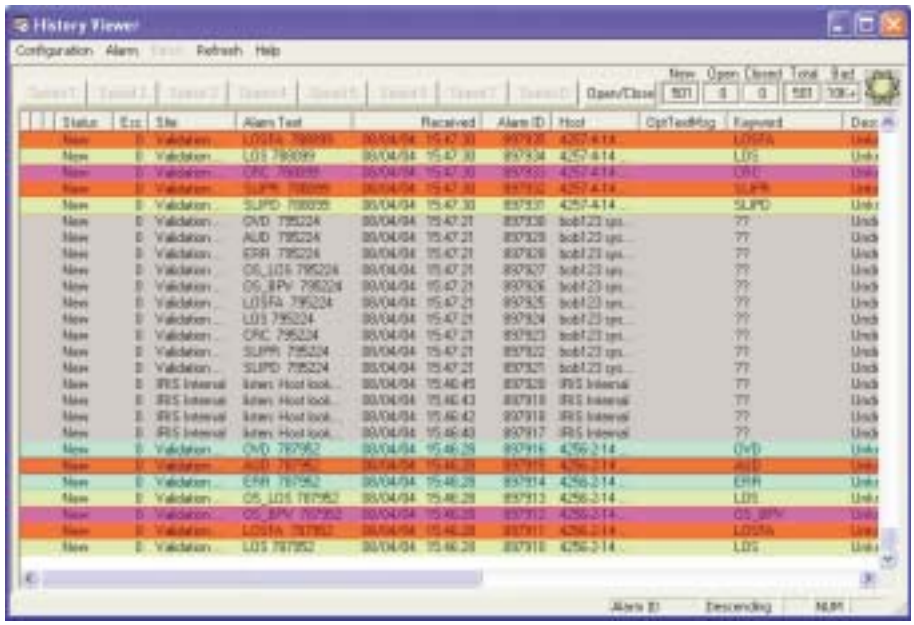
Choose the Event List Viewer option from the Tool menu, or right-click the Map icon in the system tray to display the List Viewer showing all alarms for the sites appearing on the Map Viewer. Alarms are color-coded to show severity and status. The following figure shows a typical List Viewer window.



For more information about the List Viewer, see ”List Viewer’, page 9-2.

Event History Viewer

Choose the Event History Viewer option from the Tools menu to display the Alarm History window showing all the alarms for sites appearing on the Map Viewer. The following figure shows a typical Alarms History option.



For more information about the Alarm History window, see ”History Viewer’, page 9-17.

10 Polling

The Polling process retrieves event data stored in SEBea, NET-PATH, and SEB II remote agents. This chapter covers what IRISnGEN and the remote agents require for polling to succeed. It also covers the steps necessary to poll SEBea, NETPATH, and SEB II remote agents.

We strongly recommend that you review all the sections in this chapter before polling your remote agent. It will help you prepare so that you can retrieve exactly the data you want. If you are polling an SEBea or NET-PATH remote agent and you are already familiar with IRISnGEN and its requirements for polling, you can go to the section “SEBea/NET-PATH Polling - Quick Setup” at the end of this chapter.

SEBea and NET-PATH

The SEBea and NET-PATH store data from host devices in a proprietary file: FLASH (non-volatile memory) or RAM (volatile memory). The file is divided into several compartments, each identified by the name of the host that is storing data in it and the file type that is used to store the data. Each compartment has its own data storage characteristics—the size of the compartment, the file handling procedure used (what to do when the compartment reaches its maximum size), and the File Full fixed events. Data from each host device is stored in a separate compartment. If you choose, you can program the SEBea or NET-PATH to store data in a shared file, that is, data from many hosts share the same file type and store in a single compartment.



Note *Polling shared data is not supported in IRISnGEN 5.0 and later releases.*

BeforeYou Begin Polling the SEBea or NET-PATH

Before you begin polling your SEBea or NET-PATH remote agent, it is a good idea to first verify all the IRISnGEN library records used during the polling process are properly defined and saved. The polling process requires the following library records:

- File Types
- Store Action
- Layouts
- Users
- Access Groups

The following sections discuss the library records and what IRISnGEN requires for polling.

File Types

Before you begin polling, be sure to create and download a file type record to the SEBea or NET-PATH remote agent. The file type record contains the data storage characteristics for the compartment containing the data you will be polling. This includes the file handling properties, storage size, and File Full fixed event information.

To configure a file type record

1. Choose Remote Agent Libraries > Event Libraries > File Types.
2. Right-click the File Types folder; then select Add File Type from the popup menu. The system opens the File Type tab.



3. Fill in each field on the tab to configure the data storage characteristics of the SEBea or NET-PATH's storage file. See "File Types', page 6-87 for a complete description of the File tab.
4. When done, save your file.

Store Actions

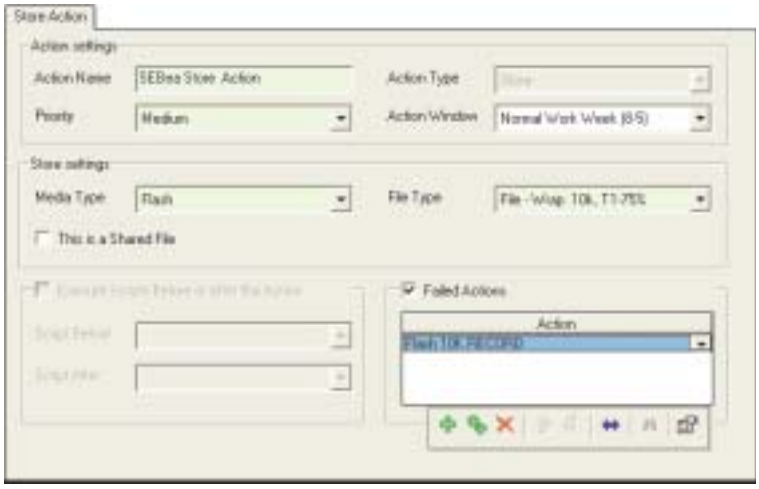
The store action record contains information about where and how to store the data you will later poll. This includes the priority and action properties, media type, file type, and failed actions.

To configure a store action record

1. Choose Remote Agent Libraries > Event Libraries > Action > Actions > Store.

Right-click the Actions folder; then, select Add Store Action from the popup menu. The system opens the Store Action tab.





2 Fill in each field on the tab to configure the action parameters of the SEBea or NET-PATH's store file. See "Store Action', page 6-48 for a complete description of the Store Action fields.

3 When done, save your file.

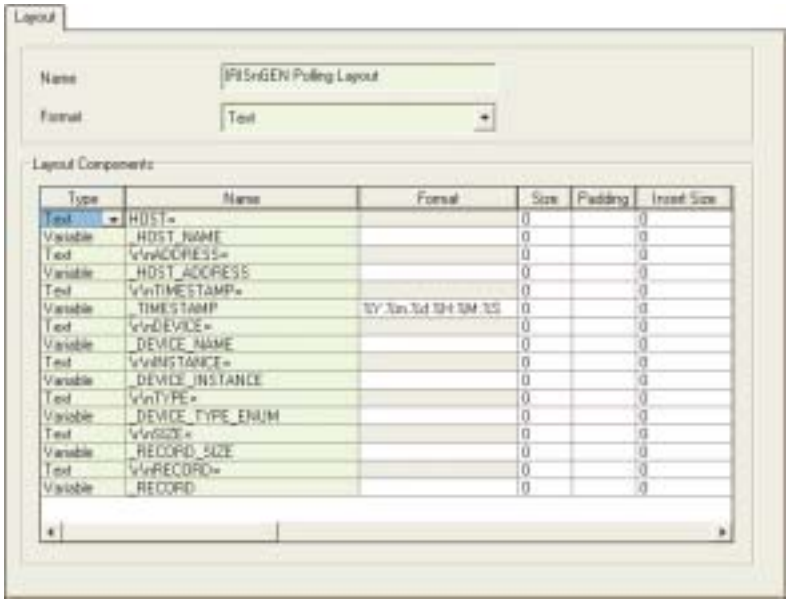
Layouts

When a Store Action executes, all the data for that event are stored in the store file. As you retrieve or view the event data by polling, the data displays in the format defined by a layout. The layout determines which variables are retrieved during polling, the variable order, and the format in which they are retrieved.

To configure a layout record

1 Choose Remote Agent Libraries > Event Libraries > Layout > Layouts.

2 Right-click the Layouts folder; then, select Add Layout from the popup menu. The system opens the Layout tab.



3 Fill in each field on the tab to configure the data storage characteristics of the layout. See ”Layouts’, page 6-93 for a complete description of the Layout tab.

4 When done, save your file.

Users

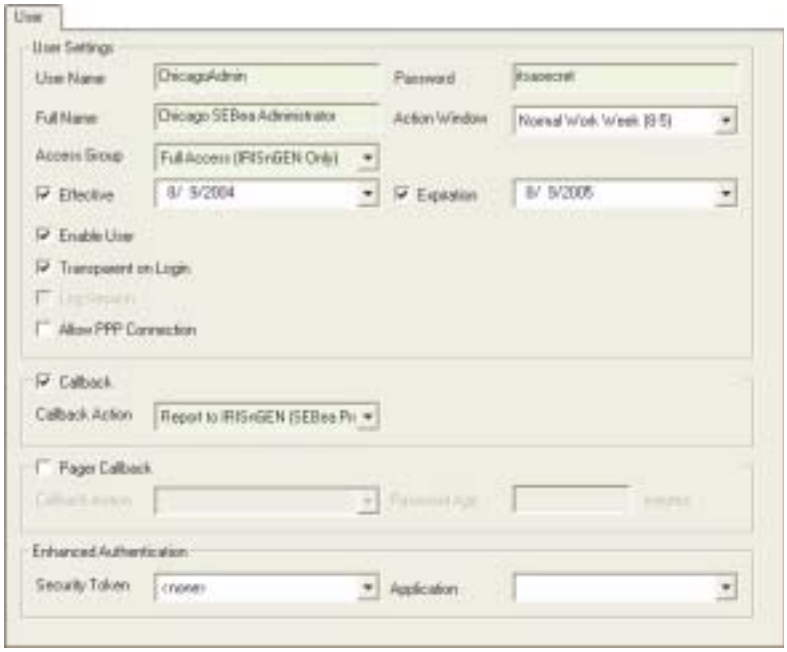
During the polling process, the remote agent determines who is requesting the data. The polling user can be either a person or an application process. The remote agent does not distinguish between the two and identifies both simply as a user.

A user is created in IRISnGEN and downloaded to the remote agent. When the SEBea or NET-PATH receives a request for polling, it verifies the calling user is the same user defined in its database. The SEBea and NET-PATH does this as a security precaution.

To configure a user record

1 Choose Remote Agent Libraries > Security Libraries > Users.

2 Right-click the Users folder; then, select Add User from the popup menu. The system opens the User tab.



3 Fill in each field on the tab to configure the user. See ”Users’, page 6-116 for a complete description of the Security Libraries’ User tab.

4 When done, save your file.

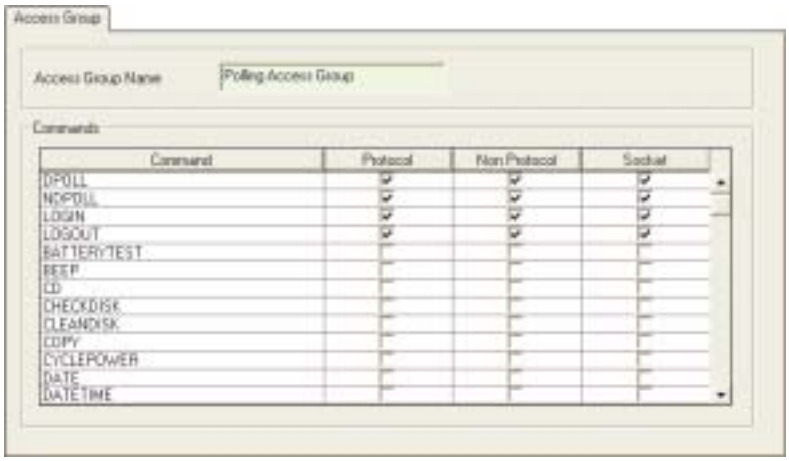
Access Groups

An access group defines the access rights for each remote agent user. Assign an access group to each user. By doing this, the user gains the access rights defined for that access group. This is a security precaution, as it lets you limit a user's access to various parts of the remote agent.

Before polling, check your user's access group to ensure that use has permission to poll the SEBea remote agent. The access group must have the following rights: DPOLL, NDPOLL, LOGIN, and LOGOUT. You can select these in the Protocol column for connections made via IRISnGEN. You can also select these rights for Non-Protocol and Socket communications as well.

To configure an access group record

1. Choose Remote Agent Libraries > Security Libraries > Access Groups.
2. Right-click the Access Groups folder; then, select Add Access Group from the popup menu. The system opens the Access Group tab.



3. Fill in each field on the tab to configure the data storage characteristics of the user's access group rights. See"Access Groups', page 6-113 for a complete description of the Access Group tab.
4. When done, save your file.

Polling Methods for SEBea and NET-PATH

You can use any of four methods to available to you to retrieve stored data from the SEBea remote agent:

- Manual
- Scheduled
- Command line
- Remote Agent Manager

Manual Polling SEBea and NET-PATH

Execute a manual poll from the IRISnGEN tree view for a highlighted remote agent or host. You cannot choose any configuration options when executing a manual poll. You must make all configurations prior to executing the poll. Data from a manual poll is saved to the location specified in the Polled Processing Application field on the host's Polling tab (see "Polling Tab', page 2-19).

When polling a single host manually, IRISnGEN only polls the data for that host. When polling a remote agent manually, IRISnGEN polls the data for all hosts assigned to that remote agent. In both instances, the way the data is polled and processed depends on the settings in the Polling tab for each host.

To perform a manual poll

1. Choose Customers folder > Customer > Site > SEBea (NET-PATH) Remote Agent.
2. Do one of the following:
   - Right-click a host; then, select Manual Poll from the popup menu.
   - Right-click the SEBea remote agent; then, select Manual Poll from the popup menu.



3. Type your polling options in the Manual Poll dialog; then, click ***OK***.

Scheduled Polling SEBea and NET-PATH

A scheduled poll works the same as a manual poll; however, it runs automatically.

To create a polling schedule

1. Choose Customer > Site > Host > Polling tab.
2. Enter the polling parameters for the polling schedule, see "Polling Tab', page 2-19.

Command Line Polling SEBea and NET-PATH

You can poll your SEBea or NET-PATH remote agent by entering commands on the command line. This involves logging into the command line of your SEBea or NET-PATH using a communications program, such as ProComm, or using Remote Agent Manager.

From the command line, you can poll data stored in either Flash or RAM and from shared or non-shared data files. Data polled using the command line displays on the screen.

You can view stored data by executing a command at the command line interface of the remote agent. There are two commands available for this purpose: NDPOLL and DPOLL.



To perform a command line poll

1 Log in with a user sign-on enabled for polling.

2 Type **DPOLL** or **NDPOLL**; then, click **Enter**.

Using the NDPOLL Command

The NDPOLL command performs a non-destructive poll of the specified storage area. The event data in the file compartment at the time it is polled remains and a copy of that data is retrieved.

The syntax for the NDPOLL command is:

NDPOLL FLASH | RAM TYPE: [*filetype*] [*hostname*] [*search expression*]



Note *Any parameter containing a space must be enclosed in quotes.*

When an event stores in the remote agent, all of its variables store as well. As you poll, you can determine which of those variables you want to display. When polling from the command line, you can use almost any layout.

Using the DPOLL Command

The DPOLL command performs a destructive poll of the storage area specified. All events that are in the storage area at the time it is polled are deleted at the completion of the poll. All other characteristics of DPOLL are the same as the NDPOLL command.

Remote Agent Manager Polling SEBea and NET-PATH

You can poll your SEBea or NET-PATH remote agent or host device using the IRISnGEN Remote Agent Manager polling application. You can choose the selectivity options and you can poll data stored in either Flash or RAM. Remote Agent Manager lets you save the access data stored in either flash or RAM. You can save data to a file or to the IRISnGEN database location specified by the processing application. You can poll one or more hosts.

Retrieve data stored from the remote agent using the Remote Agent Manager's Polling function. This function includes a wizard that steps you through the polling process. At each step, enter the parameters that meet your polling requirements.

To poll the SEBea and NET-PATH using the Polling function - Step 1

1 Do one of the following:

- Choose Action > Polling.
- Right-click a remote agent (or a host); then, select Polling from the pop-up menu.
- Highlight the remote agent (or host); then, click the Polling icon ( ]↔[ ).

The system opens the Polling Options–Step 1 dialog box.



2 Click a **Type of Poll** radio button to select the type of polling you want to perform.

Button	Description
Destructive Poll	As the Remote Agent Manager receives and acknowledges each block of data, the remote agent clears the data from its memory.
Non-Destructive Poll	As the Remote Agent Manager receives and acknowledges each block of data, the remote agent does not clear the data from its memory.

3 Click a **Polling Data Storage Options** radio button to select the polling storage options.

Button	Description
Save polled data to file only	Store the polled data in the field specified in File Options (File Name textbox).
Save polled data to IRISnGEN's Database	Store data in the IRISnGEN database. IRISnGEN stores the data in the location specified by the polling application, see "Polling Tab', page 2-19. If the polling application is Alarms, the data is stored in the SQL database. If the polling application is a custom application, such as CDR, the data is stored in the location specified by that application.



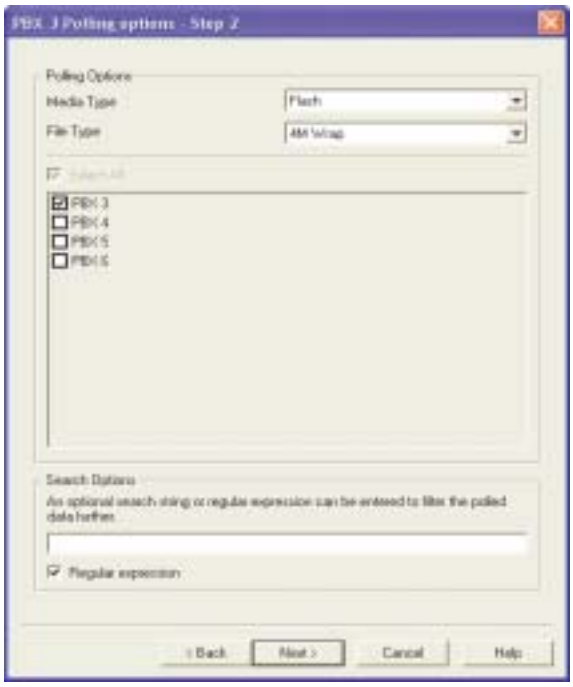
Save polled data to file and IRISnGEN's Database	Store data in both the file and the database. IRISnGEN stores the data in the location specified by the polling application, see "Polling Tab', page 2-19. If the polling application is Alarms, the data is stored in the SQL database. If the polling application is a custom application, such as CDR, the data is stored in the location specified by that application.

4 Type the name of your poll storage file in the **File Name** field; then select a save option radio button.

Button	Description
Append	Keep the existing data in a file and save polled data to the end of the file.
Replace	Clear the file before saving the polled data.

To poll the SEBea and NET-PATH using the Polling function - Step 2

1 From the Step 1 dialog, click ***Next*** to display the Step 2 dialog box and continue entering parameters.



2 Select the polling options from the three drops lists.

Button	Description
Media Type	From the list, choose the medium for which you have been storing your data: Flash or RAM.
File Type	From the list, choose a file type for the remote agent. File types are defined in the File Type library, see”File Types’, page 6-87.

3 Select the host checkboxes for the host devices you want to poll, or select the **Select All** checkbox or all hosts.

4 Type search string or regular expression in the **Search Options** field to filter the polled data. IRISnGEN will only retrieve the polled events containing the search string exactly as you entered it in this field.

5 Select the **Regular Expression** checkbox to treat the search string as a regular expression. Use Perl 5 Regular Expression syntax to qualify your expressions.

6 Do one of the following:

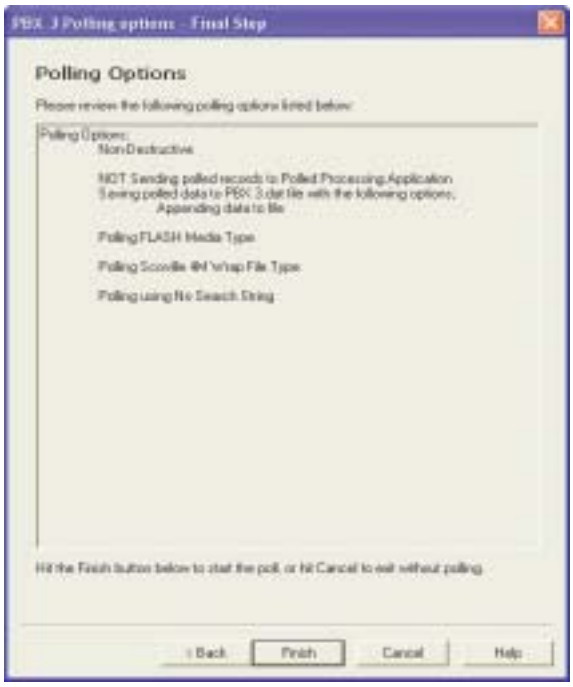
- Select the **All** checkbox if you want to poll all hosts.
- Select the checkboxes for the host you want to poll.



Note *Only hosts matching the criteria selected in the Polling Options section above will poll successfully.*

To poll the SEBea and NET-PATH using the Polling function - Final Step

1 From the Step 2 dialog, click ***Next*** to display the Final Step dialog box and review your polling parameter selections.



2 Click ***Finish*** to begin the polling process, or choose ***Cancel*** to exit without polling.

SEB II

Remote Agent Manager retrieves data stored in the remote agent using the Poll option. Two types of polling are available: destructive and non-destructive. A destructive poll gathers all data a block at a time, and then clears each block of data from the remote agent's memory when Remote Agent Manager acknowledges that it received the block. A non-destructive poll copies the data, but leaves the remote agent memory intact.

You can also poll all the data or selective data in the SEB II. Selective polling requires that the SEB II is programmed with a regular application program of 4.5.X or above or an SCL application of 5.2.X or above.

To poll the SEB II

1 Do one of the following:

- Choose Action > Polling.
- Right-click a remote agent; then, select Polling from the pop-up menu.
- Click the Polling icon ( ]↔[ ).

IRISnGEN displays the Remote Agent Poll window, shown below.



2 Click a **Type of Poll** radio button to select the type of polling you want to perform.

Button	Description
Destructive Poll	As the Remote Agent Manager receives and acknowledges each block of data, the SEBea clears the data from its memory.
Non-Destructive Poll	As the Remote Agent Manager receives and acknowledges each block of data, the SEBea does not clear the data from its memory.

3 Click a **Polling Data Storage Options** radio button to select the polling storage options.

Button	Description
Save polled data to file only	Select this radio button to store the polled data in the field specified in File Options (File Name textbox).
Save polled data to IRISnGEN's Database	Select this radio button to store data in the IRISnGEN database. To use this option, the alarms polling application must be assigned in the Host record.
Save polled data to file and IRISnGEN Database	Choose this radio button to store data in both the file and the database. The Alarms polling application must be assigned in the Host record.

4 Type the name of your poll storage file in the **File Name** field; then select a save option radio button.

Button	Description
Append	Keep the existing data in a file and save polled data to the end of the file.
Replace	Clear the file before saving the polled data.

5 Click ***OK***.

Polling Password Options

The Password Options only apply when polling a Host. Select a radio button to poll using a password. Your options are:

- Use the remote agent's password.
- Use the host's password.

The polling process is completely automatic. When you click the OK button, Remote Agent Manager contacts the remote agent or host you selected. You can follow the progress of the poll in the History pane.



To perform a selective poll

1. Select a host from the IRISnGEN tree view
2. Click the]↔[icon.
3. Select the appropriate Polling Password Options for your operation from the choices at the bottom of the Remote Agent Poll window.

To cancel polling

- Click ***Cancel***.

Manual Poll

When you select Manual Poll from the IRIS menu the system displays the Manual Poll dialog (shown below) from which you can submit manual polls of an SEB remote agent. The system places your request in the communications queue for processing.

To poll an SEB II device manually

1. Choose Customers folder > Customer > Site > SEB II Remote Agent.
2. Do one of the following:
   - Right-click a host; then, select Manual Poll from the popup menu.
   - Right-click the SEB II remote agent; then, select Manual Poll from the popup menu.



3. Type your polling options in the Manual Poll dialog; then, click ***OK***.

SEBea and NET-PATH Polling - Quick Setup

If you are familiar with the IRISnGEN system and polling, but you need a little help getting started, use the following quick steps to poll your SEBea or NET-PATH. Should you need more information about polling, you can find it at the beginning of this chapter.

Security Setup (for command line polling, only)

1. Choose Remote Agent Libraries > Security Libraries.
2. Create an access group for polling and select the access rights for the DPOLL, NDPOLL, LOGIN, LOGOUT, and STATUS commands.
3. Create a User with the desired username and password and assign this user the access group for polling.



Host setup

1. Choose Customer > Site > Host > Polling tab (for the host you want to poll).
2. Click inside the SEBea (NET-PATH) Options table; then, select a file type and application from the drop lists.
3. Save your record.

Remote Agent Setup

1. Choose Customer > Site > SEBea (NET-PATH) (for the SEBea or NET-PATH you want to poll).
2. On the Remote Agent (SEBea or NET-PATH) tab, select a user name and a password. This can be the same user name assigned to the host for polling. However, this user should have full access permissions to allow administration of the remote agent.



Note *Assigning a user here gives that user access rights to all hosts.*

Storage Setup

1. Choose Remote Agent Libraries > Event Libraries > Action > Actions > Store.
2. Fill in the fields on the Store Action tab.
3. Select a file type from the **File Type** drop list.
4. Assign the action used in the SEBea or NET-PATH database. For example, assign it to a filter, assign the filter to a host library, and then assign the host library to your host.

Manual Polling (not RA Manager)

Confirm that you can successfully send the database to the SEBea or NET-PATH and store data.

To perform a selective poll

- Highlight the host in the tree view, and then right-click and select Manual Poll. Check or uncheck the Destructive flag, as appropriate, and then click ***OK***.

The IRISnGEN system calls the SEBea or NET-PATH via a modem and logs in using the remote agent's system user name and password. It then retrieves all data for that host. IRISnGEN places the host's data in the database or in a file, depending on the application specified in the Polling tab of that host.

Troubleshooting Tips

Problem: I get an error when I try to poll saying my remote agent is empty.

Possible cause:

- You are attempting to poll shared data.

Check the Store Action associated with your host.

Problem: I get an authentication error when I try to poll.

Possible cause:

- Your user name does not have sufficient permissions to poll.
- Your password is incorrect.
- You may not be using the user name you expect, depending on where your data is stored (shared or non-shared).
- You are using the correct user name and password but the user name is not in IRISnGEN, then the system cannot confirm the permissions and the poll will fail.

Double-check your user name, password, and access group.



11

Generic Output

Overview

Today's complex data environments often require systems that integrate seamlessly. The IRISnGEN Generic Output module provides an easy way to send alarm data to dissimilar systems. You can set up the IRISnGEN system to send the alarm information to its Export or Trouble Ticket table. From there, the Generic Output module takes control, formatting the information according to user-specified parameters, then sending it to a destination of your choosing. You can send alarms to one file, send them to individual files for each alarm, or send the alarms to a serial port.

The system receiving the alarm output needs only to access the alarm output files, or receive the alarms via a serial port. Many network management systems provide utilities that allow you to monitor an existing file for new data – a process commonly referred to as "tailing."

You can define all parameters used by the Generic Output module, such as the output format and destination, in a configuration file. The information is in an ASCII text format that you can modify using most any editing or word processing software. The file updates dynamically, so any changes take effect the instant the editing is complete.

Implementation

The Generic Output application runs every sixty seconds (default), but you can change this by editing the TimeToWait parameter in the Configuration file.

If it does not already exist, you must create a new processing application entry in IRISnGEN for the genOutput executable program. We recommend that you name the process GENOUTPUT. You must enter the filename genOutput in the Filename field and check the Auto-startup checkbox. Do not mark the Enable Export checkbox.

To implement the Generic Output application

1. Type a name for the processing application that you are defining in the **Name** field. This name is for your own benefit, so choose something meaningful.
2. Type any description or comments about the application, such as why you created it, when, and its purpose in the **Notes** field. This field is optional. Maximum of 256 characters.
3. Type the name of the application—as referenced by the IRISnGEN system—in the **Filename** field.
4. Select the **Auto-startup** checkbox to automatically start this application when the system loads.
5. Select the **Write to Database** checkbox to have the application write directly to the database.

6 Select the **Write to File** checkbox to have the application write directly to a file.

7 When the Write to **f**ile checkbox is selected, type the location of the file used in the **Directory** field.

Generic output fields from Export table

The genOutput application extracts alarms from either IRISnGEN's Export or Trouble Ticket table and places them in a program structure. The application reads and processes each new pending alarm one at a time, and then marks each record to indicate that it was processed. The alarm record remains in the Trouble Ticket table until deleted though system aging as defined in the AGE_QUEUE system parameter.

The application extracts data for each new pending alarm and stores it in a structure. You can select any combination of these fields for use in the output string. The order of output fields in the configuration file will be the order in the output string. The available output fields in the structure are as follows:

- hostName
- hostAddress
- hostType
- cdName
- cdPort
- cdPhoneNumber
- cdType
- cdModemSpeed
- siteName
- customerName
- siteAddress1
- siteAddress2
- siteAddress3
- city
- state
- zip
- country
- timeReceived
- cdTime
- optionalText
- classCode
- alarmText
- alarmID
- alarmDesc
- alarmKeyword
- status
- severity
- escalationLevel
- equipmentName
- controlElement



The formatted output is an ASCII character string containing a set of user-defined output fields. Each field has a delimiting character, which must be something not normally seen in a typical data string. A pipe symbol (|) is the default delimiting character, but you can change it using the fieldSep parameter. The following shows a sample string.

severity|customerName|siteName|cdName|cdPort|hostName|hostAddress|timeReceived|keyword|alarmText

Program Parameters

The following list represents the program parameters that you control. You can change any of these parameters by including the parameter name and the appropriate value in the configuration file. The user can use the default by leaving out the parameter from the configuration file.

Parameter	Default Value	Possible Values
timeToWait	60 seconds	Any number of seconds
outputDest	1	1=output alarms to a single file 2=output alarms out a serial port 3=output alarms to individual files
outputFilename	genOutput.txt	Any valid DOS filename
serialPort	1	Any valid port number
baudRate	9600	Any valid baud rate
parity	N	N=None, O=Odd, E=Even M=Mark, S=Space
dataBits	8	4, 5, 6, 7, or 8
stopBits	1	1, 1.5, 2
fieldSep	|	(pipe symbol)
source	E	E or T, Export or Trouble Ticket
trimtrailcrlf	Y	Y or 1 to enable trimming N or 0 (zero) to disable trimming

Configuration File

The configuration file genOutput.cfg is found in the $IRISHOME\bin directory. The installation process copies a default configuration file into this directory, which you can change at any time. You do not need to stop and restart the application if you only change the configuration file. You can enter both the program parameters and the output string fields in the configuration file, which the genOutput application reads. The order of the output fields in the configuration file will determine the order in the output string.

The outputDest program variable determines which other program variables you need. If the outputDest value is 1 (write output for each exported alarm to a single output file), you can name the output file by using the outputFilename program variable. The output file is created in $IRISHOME\genOutput.

If the outputDest value is 2 (output is sent out a serial port), you may want to include the serialPort, baudRate, parity, dataBits, and stopBits program variables in the configuration file. If the outputDest value is 3 (write output for each exported alarm to a separate file), the program creates output files in the $IRISHOME\genOutput directory. The program names these output files N.txt, where N is the alarm ID found in the Alarm table, for example, 12345.txt. Since the alarm ID is unique, the file name will also be unique.



Configuration File Examples

Suppose you want the program to check the Export table every 120 seconds (2 minutes) and you want the output format to look like the following.

severity|customerName|siteName|cdName|cdPort|hostName|hostAddress|timeReceived|alarmKeyword|alarmText

The configuration file is set up as follows:

- timeToWait 120
- fieldSep | (could omit this line, because this is the default value)
- outputDest 1 (could omit this line, because this is the default value)
- outputFilename myOutput.txt
- severity
- customerName
- siteName
- cdName
- cdPort
- hostName
- hostAddress
- timeReceived
- alarmKeyword
- alarmText

When the output lines go to serial port 2 with a baud rate of 19200 and N/8/1, the configuration file is set up as follows:

- timeToWait 120
- fieldSep | (could omit this line, because this is the default value)
- outputDest 2
- serialPort 2
- baudRate 19200
- parity N (could omit this line, because this is the default value)
- dataBits 8 (could omit this line, because this is the default value)
- stopBits 1 (could omit this line, because this is the default value)
- severity
- customerName
- siteName
- cdName
- cdPort
- hostName
- hostAddress
- timeReceived
- alarmKeyword
- alarmText

When the output lines for each exported alarm go to individual output files, the configuration file is set up as follows:

- timeToWait 120
- fieldSep |(could omit this line, because this is the default value)
- outputDest 3
- severity



- customerName
- siteName
- cdName
- cdPort
- hostName
- hostAddress
- timeReceived
- alarmKeyword
- alarmText

BOR and EOR Configuration

GenOutput supports user-defined beginning of record (BOR) and end of record (EOR) characters.

The GenOutput.cfg file supports a BOR and EOR character sequence definition. The entry format will be:

BOR beginning_of_record

EOR end_of_record.

Insert BOR/EOR character sequences at the beginning and end of the record, respectively. BOR and EOR are not mandatory entries, so you must remove the hard-coded default for EOR. The default entry in the GenOutput.cfg file does not include BOR and the default EOR is “\r\n” as the last entry in the configuration file.

The BOR entry supports the list of special characters shown below.

Character	Description
\a	Bell
\b	Backspace
\f	Form Feed
\n	New Line
\r	Carriage Return
\t	Horizontal Tab
\v	Vertical Tab
\?	Literal Quotation Mark
\"	Double Quotation Mark
\\	Backslash
\0	Null
\x	Hexadecimal value (for example "\x0A")

Sample *GenOutput.cfg* file

- outputDest 1
- fieldSep |
- outputFilename genOutput.txt
- serialPort 1
- baudRate 9600
- dataBits 8
- stopBits 1
- parity None
- timeToWait 60
- severity
- alarmID
- customerName
- siteName
- hostName
- cdName
- cdPort
- alarmKeyword
- timeReceived
- alarmText
- EOR END OF RECORD\r\n

This entry results with the text “END OF RECORD” followed by carriage return and line feed characters appended to the output record.

Output Directory

If it does not already exist, the genOutput program creates the following directory:

$IRISHOME\genOutput.

The output files will reside in this directory.



Index

A

abandon changes 1-13
AC power 7-31
  lost 8-11
  restored 8-11
access alarm details 9-7
access groups 6-113, 6-118, 10-5
accessing Remote Agent Manager 7-1
action 6-58
Action Group 6-51
Action Libraries 6-28
Action View 9-43
action window 6-29, 6-30, 6-33, 6-34, 6-35, 6-38, 6-40, 6-43, 6-44, 6-48, 6-49, 6-50, 6-52, 6-75, 6-88, 6-103, 6-116
Action Window Definition Table 8-17
Action Window Libraries 6-52
Active Bridge Transparency 7-13, 7-15
active contact sensors 7-31
active toolbar 7-6
activity reporting 2-43
activity state 6-38
add
  alarm entry record 5-37
  comments to alarms 9-11
  contact record 5-44
  contacts to nodes 5-62
  destination 5-25
  dialout override strings 5-68
  email record 5-20
  escalation group record 5-8
  fax record 5-21
  filter action record 5-9
  filter schedule record 5-10
  filters to host type 5-67
  forward schedule record 5-22
  forward selector record 5-23
  forward set record 5-24
  grid lines 9-5
  keyword filter records 5-12
  keyword template 5-34
  message library 5-36
  new alarm 9-19
  object to access list 3-27
  pager record 5-27
  scheduled timed filter record 4-44
  severity filter set record 5-17
  shortcuts 1-3
  superscript 5-39
  threshold and correlations 5-66
  users to host type 5-66
add filter set 5-13
adding
  configuration flags 2-43
  contacts 2-11
  correlations 2-20
  foreign remote agent information 2-44
  groups 2-23
  hosts from different sites 2-33
  layout group 2-39
  layouts 2-40
  modem information 2-42
  SEB II information 2-41
  thresholds 2-20
  users 2-23
Address Lookup 9-26
alarm 6-113, 9-30
  Alarm History display 9-19
  alarm state 9-38
  description 5-38
  export 9-12
  history 9-17
  ID 9-29
  severity 9-30
  status 9-6, 9-30
  text 9-29
  threshold stages 5-40
Alarm List View 9-2
Alarm Viewer 9-3, 9-12
always assert DTR 6-22
append if maximum length 6-67, 6-70
append if timeout 6-68
application (ASP) 2-42
ASM activity 2-43
ASP 2-42, 7-31, 7-38, 7-42, 7-43, 8-2, 8-6, 8-11, 8-13
attachment status 9-17
audit trail 8-11
authentication 2-22, 6-45, 10-16
authentication password 2-22, 5-30
auto-learn 5-37
automated site management 2-25
auto-transparent port 8-27
available hosts 2-32, 2-33
AWSee action window 8-17

B

bad data 4-15
balloonSee information balloon 9-24
batch
  status 9-15

Battery Device Library 6-3
baud rate 6-19
beep 6-113
Beginning of Line 6-68
Beginning of Record 6-65
BOLSee Beginning of Line 6-68
BORSee Beginning of Record 6-65
Busy Response String 6-11
buzzer action 6-29

C

calibration offset 6-6, 6-24
call back 6-113
cancel polling 7-36
capture to log file 7-18
change
  modes in Equipment Explorer 9-36
  selectivity 9-38
  system parameters 3-24
class code 5-36, 9-29
clear
  History Detail Pane 7-4
  mass memory 7-38
client username 2-17
close
  alarm 9-6
  information balloon 9-24
collapse
  tree view 1-9
column
  position 6-76
column offset 5-36, 5-38
command
  buttons 1-14
  command line polling SEBea 10-6
  line interface 7-16
  string 9-45
commandline 6-113
comments 2-10, 9-11
Comments tab 2-10
commercial power 6-16
communication operations 3-2
Communication Queue 1-10
communications 3-2
Communications Queue 5-32
community name for traps 5-30
Compression Translation Definition Table 8-25
compulsory flag 6-66, 6-68
configuration flags 2-43, 2-45
configure
  access group record 10-5
  file type records 6-87
  layout record 10-3
  store actions 10-2
  user record 10-4
configure a trap 5-30
configuring
  V1 security settings 2-21
  V3 security settings 2-22
connect
  string 6-11
  to remote agent 7-7
connection information 7-5
connection method 2-44, 5-67
Contact Device Library 6-4
contacts
  sensors 7-33
Contacts tab 2-11
context
  name 6-46
context ID 2-22, 5-30
context name 2-22, 5-30
control element 5-51, 9-42, 9-44, 9-45
controlled shutdown of commercial power 6-16
copy and paste text 7-18
Correlation Libraries 6-55
correlations 2-20, 5-2, 6-56
  actions 6-58
Correlations Data Table 5-2, 5-4
create 5-13
  contact types record 5-43
  day/night mode record 3-10
  equipment action record 5-50
  equipment record 5-47
  equipment type record 5-55
  holiday record 5-65
  inter host correlation 5-2, 5-3
  map selectivity record 9-28
  modem type record 3-3
  port groups 3-5
  port record 3-7
  printer 5-29
  processing application record 3-23
  remote agent type 5-67
  shortcuts 1-7
  speed buttons 9-5
  string filter set record 5-18
  threshold record 5-41
  user group record 3-26
  user record 3-27
create a customer record 2-2
create a host record 2-16
creating
  daylight saving records 2-14
  equipment records 2-18
  polling records 2-19
  SEBea/NET-PATH records 2-23
  site records 2-13



SNMP Settings records 2-21
time zone records 2-14
user records 2-22
CTSee compression translation 8-25
customer 9-7, 9-28
Customer Library 1-5
customers 2-1
Customers folder 2-3
customizing
Alarm History display 9-19
cut and paste nodes and objects 5-64

D

daily self-check 8-10
data bits 6-20
data tables 1-7, 3-25, 5-66, 5-67
database command 1-14
database command buttons 1-14
Clear 1-14
Close 1-15
Copy 1-14
Delete 1-15
Retrieve 1-14
database debug flag 2-29
database debut flag 2-31
Database Upload dialog 7-39
database utilities 2-27
date and time 7-25
Day/Night Forward Selectors 3-9
Day/Night mode 3-10
daylight saving 2-14
daylight savings 2-43
DC Voltage Device Library 6-5
default daylight savings 2-14
default gateway 2-33
define
map settings 9-31
new fields 3-25
special procedures record 5-38
values of user-defined fields 3-26
define new fields for a customer record 2-5
delay the delivery of actions 2-38
delete
contacts from nodes 5-62
equipment record 5-48
equipment type record 5-56
forwarding destination 5-25
nodes and objects 5-61
object from access list 3-27
delete a customer record 2-3
delete customer 2-3
denial of service 2-34
destination file 2-29, 2-31
destructive poll 7-11, 7-35, 10-8, 10-13
Detail View 9-40
Device Connection 6-31, 6-36, 6-41
Device Libraries 6-2
Devices & Hosts tab 2-32
Dial Tone Response String 6-12
disable
scripts 7-38
disable factory access 2-25
discard
lines less than 6-69
records less than 6-66
disconnect from remote agent 7-7
dispatch
an alarm 9-11
status 9-17
display
Detail View 9-40
effective information 7-44
Effective Information pop-up 7-8
Equipment View window 9-39
Event View 9-42
history detail 7-4
I/O port status 7-38
information balloon 9-24
menu for tree view object 1-6
Remote Agent View 9-45
several Equipment Explorer windows 9-37
shortcut bar 1-4
site information on Map Viewer 9-23
Site View 9-37, 9-38
toolbar 9-20
tree view pane 7-3
Where Used 5-50
displaying
tree view objects 1-6
disposition 9-7
Download Application dialog 7-22, 7-23
Download Database dialog 7-21
Download Utility dialog 2-30
downloading
files using Telnet 2-28
DPOLL command 10-7
drag and drop nodes and objects 5-62
DST
change 8-12
duplicate
equipment record 5-49
equipment type record 5-56
hierarchy 5-64
icon record 5-53
duplicate a customer record 2-4

E

edit

SEB II database 7-28
Edit dialog 7-41
Edit Pane 1-1
Edit pane 1-7
editing data 1-7
editing
Network Properties dialog 2-33, 2-37
EEPROM type 7-34
effective information 7-8, 7-29, 7-44
displaying 7-44
override foreign agent 7-44
overriding 7-29
embedded
remote agent ID 7-31
Embedded Name 4-17
embedded name 2-23, 2-41, 2-44
EMSee external modem 8-28
enable
scripts 7-38
enable polling 2-25, 2-43
encryption 2-22, 5-30, 6-45
encryption password 2-22, 5-30
End of Line 6-68
End of Record 6-66
end transparency 7-17
Enhanced Action Delivery 2-38
enhanced action delivery 2-38
Enhanced Action Delivery tab 2-38
Enhanced Authentication 2-28
enhanced authentication 2-28
enhanced keyword template 5-38
EOLSee End of Line 6-68
EORSee End of Record 6-66
equipment and control elements 2-17
Equipment Explorer 1-10
Equipment Type 5-55, 5-56
equipment type 2-18
Equipment View 9-39
escalate alarms 9-10
escalation 9-29
Ethereal protocol analyzer 5-32
Event Detection Groups 6-73
Event Detection Libraries 6-60
Event History Viewer 9-48
Event Libraries menu 6-27
Event List Viewer 9-47
Event Match Group 6-84
Event Match Tab
Data 6-74
Fixed 6-83
SNMP 6-80
Event Matches 6-74, 6-109
Event View 9-41
exact number of lines 6-69
Exclude from Activity Reporting 2-45
exclude from activity reporting 2-25, 2-45
execute
menu command 1-6
script 7-38
expand and collapse
contact fields 7-9
tree view 1-5
Expect 6-85
Expect Groups 6-86
export alarms 9-12
Expression Builder 5-12
extended hierarchy i-xiv

F

failed action group 6-107
Fax Action 6-30
FESee fixed event 8-10
file types 6-87, 10-2
files
sending and retrieving 7-26
filter actions 5-9
Filter Groups 6-89
filter sets 2-9
filters 6-88
Filters and Forwarding tab 2-7
find entire cells 1-11
find results 1-13
find what 1-11
Fixed Event Definition Table 8-10
fixed event defintion 6-6
Fixed Event Groups 6-91
Fixed Event Match Tab 6-83
Fixed Event Message Definition Table 8-16
Fixed Event Sequence Definition Table 8-13
fixed events 6-90
flow control 8-21
FMSee fixed event definition 8-16
foreign agent 7-44
functions 7-44
overriding effective information 7-44
toolbar 7-7
Foreign Remote Agent tab 2-44
Foreign remote agent tab 2-44
Foreign Remote Agnet tab 2-44
forward
alarms 9-8
Forward Selectors 2-9
forward sets 2-9
FS table 8-12
FSSee fixed event sequence 8-13
FTP 2-34
FTP idle timeout 2-34
FTP port 2-34



FTP server 2-34
FTP server attributes 2-34

G

General tab (for SEB II) 7-30
Geographical viewer 1-10
get
    and view database 7-26
    database 7-39
    status 7-9, 7-30, 9-41
GETPM 6-113
GFI Fax 5-21
go transparent 9-14
    host device 7-45
    to host 7-14
    to host device 7-39
    to host port 7-38
    to SEB II 7-37
    to SEBea 7-14
GoldFax NT 5-21
grid lines 9-5

H

hang-up command 8-28
hide shortcut bar 1-4
hierarchy 5-59, 9-29
    expanding structure 1-5
    extended i-xiv
hierarchy tree 5-60
high speed external modem 2-43
History Detail Pane 7-4
History View 9-44
History viewer 1-10
Holiday Libraries 6-92
host 9-7, 9-28
    address 9-29
    login 7-19
    password 7-19
    ports 7-34
    setup 10-15
    transparency 7-14
host address 2-16, 4-17, 4-31, 4-39, 9-3, 9-29, 9-34
Host dialogue failure 8-11
Host Libraries 6-108
Host Library Group 6-110
Host Type 9-29
Host-Equipment tab 2-17
hosts 2-1
HTTP port 6-15

I

identify sites assigned to a customer 2-4
Idle Line Input Timeout 6-10
Idle Line Output Timeout 6-10
idle time 5-8
idle timeout 6-15
ignore
    alarms 9-12
Include Event List in Threshold Summary Event (XT) 6-107
information balloon 9-24
initialization command string 8-28
insert
    schedule forward selector 4-44
    scheduled timed filter 4-45
Inter-Host Correlations 5-2
internal diagnostic failure 8-11
IP address 2-30, 5-29
IRIS Administration Library 1-5
IRISnGEN
    architecture i-xii
    main window 1-1
    overview i-xii
iterations 5-8

K

keyboard shortcuts 1-6
keyword 5-3, 5-4, 5-37, 9-18, 9-29

L

last download 7-32
last memory clear 7-32
last poll 7-31
Last Status tab 2-40
launching Equipment Explorer 9-32
layout components 6-93
layout group 2-39
Layout Groups 6-97
layout record 2-39
layouts 6-93, 6-99, 10-3
Layouts tab 2-39
LCD Action 6-33
LED Action 6-34
Libraries
    Customer 1-5
    IRIS 1-5
    IRIS Administration 1-5
    Remote Agent 1-5
library name 5-36, 6-5
license key 2-24
line
    lengths 6-70
linked alarms 9-7
loader 7-24
local baud 7-34
local echo 7-20
local IP address 2-33
lock
    SEBea 7-28



log
raw input data 6-22
log file size 2-24
log media 2-24
login failure 8-11
logout 7-38

M

manual polling 10-14, 10-15
manual polling SEBea 10-6
manually escalate alarms 9-10
manually forward alarms 9-8
map
selectivity 9-27
settings 9-31
Map Viewer 9-21, 9-23, 9-27
Map Viewer pop-up menu 9-25
Map Viewer speed buttons 9-30
mass
edit 1-10
mass edit 1-10, 1-11
match case 1-11
max FTP connections 2-34
Max Telnet Connections 6-15
maximum
line length 6-69
log file size 6-22
record length 6-67
threshold 8-7, 8-14
maximum FTP connections 2-34
memory
threshold exceeded 8-10
used 7-32
Memory Device Library 6-8
menu bar 1-8
menu command 1-6
Message Library 5-36, 5-38, 9-18, 9-42
message library 5-36
Microsoft Exchange 5-21
Microsoft MapPoint 2002 9-23
Miscellaneous Tab 7-33
model 6-120
Model Libraries 6-111
modem
baud 7-34
connect speed 6-10
type 3-3, 3-8
Modem Device Library 6-9
modem information 2-42, 2-45
modem speed 2-42, 2-45
Multi-Drop Alarm Delivery and Control System i-xi
my shortcuts 1-3

N

Navigate History 1-13
navigating tree view 1-5
navigation bar 1-13
Navigator 1-13
NDPOLL command 10-7
NET-PATH remote agent tab 2-44
Network Device Library 6-14
network properties 2-33
Network Properties dialog 2-33, 2-37
network protocol analyzer 5-32
new comments 2-10
new password 2-41
NIC parameters 2-33
No Carrier Response String 6-12
No Dial Tone Response String 6-12
node 9-29
non-destructive poll 7-11, 7-35, 10-8, 10-13
number of retries 6-42, 6-47
NVRAM type 7-34

O

offset column 5-36, 5-38
OK Response String 6-11
open an alarm 9-6
operating system 7-23
OptTextMsg 9-18
override
SEB II effective information 7-29
SEBea effective information 7-8
override layout 6-107
override terminal type 7-16
overriding 7-16

P

Packet Size 2-31
packet size 2-31
padding characters 6-95
Pager Action 6-35
Pager Service tab 5-26
Pagers/Pager Services 5-26
parity 3-8, 6-20
Passive Transparency 7-13, 7-14
password 2-41, 2-44, 3-27, 6-116, 8-26
index 7-34
paste and copy text 7-18
Personality module 7-34
Phone Number Definition Table 8-18
phone prefix 2-42, 2-45
phone suffix 2-42, 2-45
phoneprefix 2-42
physical sensors 8-12
PNSee phone number 8-18
poll host if full 2-19
poll if full 2-43
poll schedule 2-19, 2-25, 2-42
poll SEBea 7-10, 7-12, 7-13



polling 7-10
layouts 6-97
methods for SEBea 10-6
password options 7-36, 10-13
schedule 10-6
SEB II 10-12
SEB II manually 10-14
selective 7-36
polling data storage options 10-8, 10-13
Polling Options dialog 10-8
polling password 2-19
Polling tab 2-19
port 6-44
connectivity 7-32
groups 3-4, 3-8
SEB II status 7-32
signals 7-32
Port Activity 7-33
Port Parameter Definition Table 8-20
Ports Connected 7-31
post-processing 6-72
Power Device Library 6-16
PPSee port parameter 8-20
prepend if maximum length 6-67
prepend if timeout 6-68
pre-processing 6-70
pre-processing sequence 6-71, 6-73
Primary DNS Server 6-15
primary DNS server 2-34
processing
applications 3-23
processing application 2-19
Procomm 6-112
protocol 6-45, 8-18
PSTNSee Public Switched Telephone Network i-xi
Public Switched Telephone Network i-xi
Python script code 6-98

Q

qualification
time 6-6
qualification time 6-6
queue overflow 8-11
quick setup 10-14

R

RAM 7-34
raw hardware 7-34
read mass memory 7-37
reassign any sites or hosts to another customer 2-3
receive buffer size 6-21
Record Definition 6-61
record timeout 6-67
refresh
time 9-5
Regular Expression Characters 5-14
Regular Expression Filter Set record 5-13
Regular Expression Filter Sets 5-13
Relay Action 6-38
Relay Device Library 6-17
remote access subnet 2-34
remote agent
model 7-34
setup 10-15
Remote Agent Libraries 1-5
Remote Agent Manager 7-1, 7-6
active toolbar 7-6
drop-down menus 7-5
polling SEBea 10-7
Remote Agent Type 5-67, 5-68
remote agent type 2-24, 2-44
remote maintenance i-xi
remove
alarms 9-12
contact assignment 5-46
shortcut 1-4
removing
contacts 2-11
rename shortcut 1-4
replace with 1-11
Report Queue 1-10
Reports
formats 4-42
Reprocess Threshold Summary Event (XT) 6-107
retry
period 6-42, 6-47
revert changes 1-9
Revert toolbar button 1-8
ring count 3-8
Ring Response String 6-11
RJ45 output relay jack 6-17
RLOGIN 2-17

S

sample interval 6-5
sample trigger words 6-77
save changes 1-13
Save icon 1-8
save polled data to file 7-11, 7-36
save polled data to IRISnGEN database 7-11
save setting 9-6
saving
data in Edit pane 1-8
scheduled
polling SEBea 10-6
script 6-98
status by port 7-38
Script Action 6-43
Script Groups 6-99



search and replace with mass edit 1-11
search every column 1-11
search mass memory 7-37
SEB II 10-12
  functions 7-28
  General tab 7-30
  get status 7-30
  go transparent 7-37
  Miscellaneous tab 7-33
  override effective information 7-29
  toolbar 7-7
SEB II Remote Agent tab 2-41
SEB II remote agent tab 2-41
SEB II tab 2-41
SEB model 2-41
SEBea 10-1
  functions 7-8
  gettting and viewing database 7-26
  manual polling 10-6
  Polling Options dialog 7-10
  polling with Remote Agent Manager 10-7
  pollng quick setup 10-14
  retrieving files from 7-27
  send application 7-22
  send loader 7-24
  sending database to 7-20
  sending date and time to 7-25
  sending files to 7-26
  sending operating system to 7-23
  toolbar 7-6
  transparency 7-14
SEBea/NET-PATH database utilities 2-27
SEBea/NET-PATH records 2-23
Secondary DNS Server 6-15
Secondary DNS server 2-34
secondary DNS server 2-34
security
  setup 10-14
Security Definition Table 8-26
security ID 2-22, 5-30
Security Libraries 6-112
security name 5-30
select database for editing 8-3
selective polling 7-36, 10-14, 10-15
selectivity 9-3, 9-4, 9-28, 9-38
self-check 8-10
self-check time 2-25, 2-42, 7-40, 7-41
send
  application 7-22
  break command 7-19
  database 7-20
  database and application 7-23
  date and time 7-25
  date and time to SEB II 7-43
  host password 7-19
  loader 7-24
  operating system 7-23
send and retrieve files 7-26
send test trap 5-32
sending a test trap 5-32
sensor type 6-5
sensors 7-34
Serial Device Library 6-10
serial device name 6-49
Serial Port Device Library 6-19
Server time 9-20
server username 2-17
SESee security definition 8-26
setting
  refresh time 9-5
severity 5-17, 9-18, 9-38, 9-42
shortcut
  add 1-3
  creating 1-7
  remove or rename 1-4
shortcut bar 1-1, 1-3, 1-4, 1-7, 9-20
  change icon size 1-3
  display or hide 1-4
simple record 6-62
Single Host Correlation 5-3
site 9-7, 9-28
Site View 9-37
sites 2-1, 2-12
size 6-95
SNMP
  action 6-44
  Event Match tab 6-80
  layouts 6-99
  port 6-15
SNMP data size 5-32
SNMP Download Utility 2-30
SNMP download utility 2-30
SNMP managers 5-29
SNMP Settings tab 2-21
SNMP target 5-29
SNMP Targets 5-29
source file 2-31
source filename 2-29
SP table 7-37
special procedure 5-38
speed 2-17
speed buttons 9-5, 9-30
SPSee system parameter 8-22
starting Map Viewer 9-21, 9-32
status bar 7-5
status report 7-37
stop bits 6-20
Store Action 6-48



store actions 10-2
subnet mask 2-33, 6-14
subnet
emote access 2-34
Superscripts 5-39
System Device Library 6-23
System Parameter Definition Table 8-22
System Parameters 3-24

T

tab 3-7
tabs
- Access Group 6-113, 6-118
- Action Group 6-51
- Action Window 6-52
- Battery Device Library 6-3
- Buzzer Action 6-29
- Contact Device Library 6-4
- Correlation 6-56
- Correlation Actions 6-58
- Day/Night Forward Selectors 3-9
- DC Voltage Device Library 6-5
- Device Connection 6-31, 6-36, 6-41
- Event Detection Group 6-73
- Event Match Data 6-74
- Event Match Fixed 6-83
- Event Match Group 6-84
- Event Match SNMP 6-80
- Event Matches 6-109
- Expect 6-85
- Expect Groups 6-86
- Fax Action 6-30
- File Types 6-87
- Filter 6-88
- Filter Groups 6-89
- Fixed Event 6-90
- Fixed Event Groups 6-91
- General (for SEB II) 7-30
- Hierarchy 5-59
- Holiday Library 6-92
- Host Library Group 6-110
- Inter Host Correlation 5-2
- layout groups 6-97
- Layouts 6-93
- LCD Action 6-33
- LED Action 6-34
- Model Libraries 6-111
- Modem Device Library 6-9
- Modem Type 3-3
- Momory Device Library 6-8
- Network Device Library 6-14
- Pager Action 6-35
- Port (for SEB II) 7-32
- Port Groups 3-4
- Ports 3-7
- Post Processing 6-72
- Power Device Library 6-16
- Pre-Processing 6-70
- Processing Applications 3-23
- Record Definition 6-61
- Relay Action 6-38
- Relay Device Library 6-17
- Script 6-98
- Script Action 6-43
- Script Groups 6-99
- Serial Port Device Library 6-19
- Single Host Correlation 5-3
- SNMP Action 6-44
- SNMP Layouts 6-99
- Store Action 6-48
- System Device Library 6-23
- System Parameters 3-24
- Task Groups 6-102
- Temperature Device Library 6-24
- Template 6-120
- Threshold 6-103
- Threshold Action 6-106
- Threshold Group 6-107
- Time Zone & Daylight Saving 6-54
- Triggered Event Action 6-50
- User Defined Fields 3-24
- User Group 6-118
- User Groups 3-26
- User Interface Device Library 6-25
- Users 3-27, 6-116

Task Detail Pane 7-4
task groups 6-102
tasks 6-100
TCP/IP port 5-30
Telnet 2-30
telnet 6-15
Telnet connection 2-30
Telnet Download Utility 2-28
telnet idle 6-15
Telnet Idle Timeout 6-15
Telnet port 6-15
Temperature Device Library 6-24
Template Libraries 6-120
terminal 2-17
terminal type 7-16
terminate script 7-38
test trap 5-32
text and variable components 6-95
threshold
- exceeded 8-10
- period 8-7, 8-14

Threshold Action 6-106
Threshold Group 6-107



thresholds 2-20, 6-103
Thresholds and Correlations tab 2-20
ticket alarms 9-11
time zone 6-54
Time Zone & Daylight Saving tab 2-14
Time Zone and Daylight Saving 6-54
timed comments 2-10
timeout 6-15
timeslot 6-52
TMSee trigger messages 8-9
toggle
  Shortcut window 1-9
toolbar 1-7, 1-8, 1-12, 3-26, 3-27, 5-18, 5-25, 5-45, 5-46, 7-3, 7-6, 7-7, 7-39, 7-45
  foreign agent 7-7
  SEB II 7-7
  SEBea 7-6
  Transparency window 7-17
toolbar icons 1-8
trace scripts 7-38
transfer progress 2-29, 2-31
translate parity in transparency 8-21
translate parity on transparency 6-21
transmit buffer size 6-20
Transparency
  Active Bridge 7-15
  normal 7-14
  passive 7-14
transparency 7-13, 7-37, 7-45
  end 7-17
  overriding terminal type 7-16
  status 7-20
Transparency window toolbar 7-17
transparent
  access 8-27
  going transparent to SEB II 7-37
  on answer 8-23
  to host 7-14
  to SEBea 7-14
trap size limit 5-30
traps 5-29
tree order 1-5
tree view 1-1, 1-3, 1-4, 1-5, 1-6, 1-7, 1-8, 1-9, 1-11, 3-27, 5-48, 5-49, 5-50, 5-51, 5-52, 5-53, 5-54, 5-56, 5-57, 5-68, 7-1, 7-3, 7-14, 7-30, 7-42, 10-6, 10-14, 10-15
  expand and collapse 1-5
  navigating 1-5
Trigger Messages Definition Table 8-9
Triggered Event Action 6-50
TS 8-6
TSSee trigger sequences 8-6

U

UI password 2-24
unlock SEBea 7-28
use compression 2-29
Used dialog 7-41
user defined fields 3-24
User Fields tab 2-5
user groups 3-26, 6-118
User Interface Device Library 6-25
user-defined field 2-7
user-defined fields 3-25, 3-26
users 3-27, 6-116, 10-4
Users tab 2-22
using
  Equipment Explorer with Map Viewer 9-24
  Map Viewer speed buttons 9-30
  Mass Edit 1-11
  navigation buttons 9-32
  Navigator tool 1-12
  tree view menus 1-5, 1-6

V

V1 security settings 2-21
V3
  settings 6-45
V3 security settings 2-22
validating
  data in Edit pane 1-8
variable expression 6-105
variable extraction 6-76, 6-77
variables 9-7
view
  attachment 9-8
  communication operations record 3-2
  detail 9-7
  SEBea status 7-9
  server time 9-20
  transparency status 7-20
View dialog 7-41

W

wildcards 6-75, 8-23

