Embedded Support Partner User Guide

Document Number 007-4065-008

CONTRIBUTORS
Written by Darrin Goss
Edited by Allison Gosbin
Production by Karen Jacobson
Engineering contributions by the System and Site Support Tools Group

Embedded Support Partner User Guide
Document Number 007-4065-008

Contents

List of Figures xi

List of Tables xix

What's New in this Document xxi

1. Introduction 1

Distribution 3

Base Package 3

Extended Package 4

Named Groups 6

Full and Light Nodes 7

TCP/IP Protocol 9

Group Management Over Hierarchies 9

Simplified Group Management Configuration 11

Enhanced Configuration for SGM Clients 11

Central Logbook Capability 11

ESP Benefits 12

ESP Architecture 14

Core Software 19

System Support Database (SSDB) 19

ESP and SGM DSOs 19

Monitoring Software 21

Configuration Monitoring 21

Event Monitoring 22

Availability Monitoring 25

Notification Software 26

Console Software 28

Web-based Interface 28

Command Line Interface 29
External Tools 30
Performance Monitoring Tools 30
Diagnostic Tools 31
RAID Monitoring Tools 31
Remote Support Capability 31
Security Features 32
System Performance Impact of ESP 33

2. Accessing ESP 35
Using the Command Line Interface 35
Using the Web-based Interface 42
Accessing the Web-based Interface 44
Configuring Single System Management 48
Configuring Group Management 49

3. Administering ESP 51
Setting Up the Customer Profile 52
Using the Web-based Interface 52
Using the Command Line Interface 55
Setting Up the Network Permissions 56
Using the Web-based Interface 56
Using the Command Line Interface 58
Setting Up the User Permissions 59
Viewing the Current Users 59
Using the Web-based Interface 59
Using the Command Line Interface 60
Adding a User 61
Using the Web-based Interface 61
Using the Command Line Interface 64
Updating a Password 65
Using the Web-based Interface 65
Using the Command Line Interface 67
Updating Permissions for a User 68

Using the Web-based Interface 68
Using the Command Line Interface 71
Deleting a User 73
Using the Web-based Interface 73
Using the Command Line Interface 74
Manipulating Database Archives 75
Using the Web-based Interface 75
Using the Command Line Interface 76

4. Setting Up the ESP Environment 77
Setting Up the System Serial Number (Linux OS Only) 78
Setting the System Serial Number (Single System Manager Mode) 79
Setting the System Serial Number (System Group Manager Mode) 81
Setting Up the Global Configuration Parameters 83
Using the Web-based Interface 83
Using the Command Line Interface 88
Setting Up the System Parameters (Single System Manager Mode Only) 91
Setting Up the System/Client Parameters (System Group Manager Mode Only) 93
Adding a New SGM Client 93
Updating the System or a Client 97
Updating the SGM Server 98
Updating an SGM Client 100
Unsubscribing SGM Clients 104
Setting Up the Authentication Password 106
Adding a Password for a New Server 106
Updating the Password for an Existing Server 107
Using the Command Line Interface to Configure SGM Settings 108
Importing and Exporting ESP Environments 110

5. Configuring ESP 111
Configuring Events 111
Managing Event Profiles 112
Using the Web-based Interface 112

Using the Command Line Interface 115
Viewing Event Classes and Events 117
Adding Events 118
Using the Web-based Interface 118
Using the Command Line Interface 135
Updating Events 136
Using the Web-based Interface 136
Using the Command Line Interface 144
Updating Multiple Events at the Same Time (Batch Updating) 146
Using the Web-based Interface 146
Using the Command Line Interface 150
Deleting Events 151
Using the Web-based Interface 151
Using the Command Line Interface 153
Subscribing Events from SGM Clients 155
Using the Web-based Interface 155
Using the Command Line Interface 158
Configuring Actions 159
Viewing the Existing Actions 159
Adding Actions 160
Using the Web-based Interface 160
Using the Command Line Interface 172
Updating Actions 173
Using the Web-based Interface 173
Using the Command Line Interface 176
Disabling and Enabling Actions 177
Using the Web-based Interface 177
Using the Command Line Interface 178
Configuring Performance Monitoring 179
Using the Web-based Interface 179
Using the Command Line Interface 185

Configuring System Monitoring 186
Using the Web-based Interface (Single System Manager Mode) 186
Using the Web-based Interface (System Group Manager Mode) 190
Using the Command Line Interface 192

6. Viewing Reports 195
About Reports 195
Events Registered Reports 199
Using the Web-based Interface (Single System Manager Mode) 199
Using the Web-based Interface (System Group Manager Mode) 205
Using the Command Line Interface 211
Actions Taken Reports 212
Using the Web-based Interface (Single System Manager Mode) 212
Using the Web-based Interface (System Group Manager Mode) 214
Using the Command Line Interface 216
Availability Reports 217
Using the Web-based Interface (Single System Manager Mode) 217
Using the Web-based Interface (System Group Manager Mode) 220
Using the Command Line Interface 223
Diagnostic Result Reports 224
Using the Web-based Interface (Single System Manager Mode) 224
Using the Web-based Interface (System Group Manager Mode) 226
Using the Command Line Interface 228
Hardware Reports 229
Hardware Inventory Reports 229
Using the Web-based Interface (Single System Manager Mode) 229
Using the Web-based Interface (System Group Manager Mode) 232
Using the Command Line Interface 235
Hardware Changes Reports 236
Using the Web-based Interface (Single System Manager Mode) 236
Using the Web-based Interface (System Group Manager Mode) 238
Using the Command Line Interface 240
Software Reports 241
Software Inventory Reports 241

Using the Web-based Interface (Single System Manager Mode) 241
Using the Web-based Interface (System Group Manager Mode) 245
Using the Command Line Interface 247
Software Changes Reports 248
Using the Web-based Interface (Single System Manager Mode) 248
Using the Web-based Interface (System Group Manager Mode) 250
Using the Command Line Interface 251
System Reports 252
System Inventory Reports 252
Using the Web-based Interface 252
Using the Command Line Interface 255
System Changes Reports 256
Using the Web-based Interface (Single System Manager Mode) 256
Using the Web-based Interface (System Group Manager Mode) 258
Using the Command Line Interface 259
Site Reports (System Group Manager Mode Only) 260
Using the Command Line Interface 262

7. Using the ESP Logbook 263
About the ESP Logbook 263
Viewing Logbook Entries 263
Using the Web-based Interface (Single System Manager Mode) 263
Using the Web-based Interface (System Group Manager Mode) 265
Using the Command Line Interface 267
Adding a Logbook Entry 268
Using the Web-based Interface (Single System Manager Mode) 268
Using the Web-based Interface (System Group Manager Mode) 270
Using the Command Line Interface 273

8. Sending Notifications 275
About the espnotify Tool 275
Command Line Options for Displaying a Message on the Console 275
Displaying a Message on an X Window System Display 276
Sending an E-mail Message 278

Invoking espnotify from ESP 279
Example: Creating an Action to Send an E-mail 279

9. Logging Events from Applications and Scripts 283
Event Classification and Sequence Numbers 283
Using the Event Manager API 284
Using the emgrlogger and esplogger Tools 284
Example 1 286
Example 2 286

10. Default Event Classes and Types 287
Default Event Classes 287
Default Event Types 287

List of Figures

Figure 1-1 ESP Functional Diagram 2
Figure 1-2 System Group Management Block Diagram 5
Figure 1-3 Named Groups 6
Figure 1-4 Full and Light Nodes 8
Figure 1-5 Group Management Over Hierarchies 10
Figure 1-6 ESP Architecture (Using Web Browser) 17
Figure 1-7 ESP Architecture (Using Command Line Interface) 18
Figure 1-8 Sending Event Information to SGI 27
Figure 2-1 ESP Opening Page 44
Figure 2-2 Entering a Username and Password 45
Figure 2-3 ESP Main Page (Single System Manager Mode) 46
Figure 2-4 ESP Main Page (System Group Manager Mode) 47
Figure 3-1 Choosing the System to Update the Customer Profile 52
Figure 3-2 Update Customer Profile Window (Web-based Interface) 53
Figure 3-3 Network Permissions Window (Web-based Interface) 57
Figure 3-4 Current User List (Web-based Interface) 60
Figure 3-5 Add User Window (Web-based Interface) 62
Figure 3-6 Update Password Window (Web-based Interface) 65
Figure 3-7 Update Password for User Window (Web-based Interface) 66
Figure 3-8 Update User's Permissions Window (Web-based Interface) 69
Figure 3-9 Updated Update User Permissions Window (Web-based Interface) 70
Figure 3-10 Delete User Window (Web-based Interface) 73
Figure 3-11 Updated Delete User Window (Web-based Interface) 74
Figure 4-1 Linux System SN Button 78
Figure 4-2 Add Linux System Serial Number Window (Single System Manager Mode) 79
Figure 4-3 Add Linux System Serial Number Verification Window (Single System Manager Mode) 80

Figure 4-4 Linux System SN Window (SGM Server that has One Client without a Serial Number Entered) 81
Figure 4-5 Linux System SN Window (SGM Server that has Multiple Clients without Serial Numbers Entered) 82
Figure 4-6 Choosing the System to Update the Global Parameters 84
Figure 4-7 Global Configuration Window (Web-based Interface) 84
Figure 4-8 Update System Information Window (Single System Manager) 91
Figure 4-9 Add New Client Window (System Group Manager Mode) 93
Figure 4-10 Update System/Client Window (System Group Manager Mode) 97
Figure 4-11 Update System Information Window (SGM Server Selected) 98
Figure 4-12 Update Client Information Window (SGM Client Selected) 100
Figure 4-13 Unsubscribe/Delete Client Window 105
Figure 4-14 Add Password for a New Server Window 106
Figure 4-15 Update Password for an Existing Server Window 107
Figure 5-1 Event Profile Window (System Group Manager) 113
Figure 5-2 Event Profile Window 113
Figure 5-3 Add Event Window (System Group Manager) 118
Figure 5-4 Add Event Window (Single System Manager) 119
Figure 5-5 Add Event Window (Adding Event to Existing Class) 120
Figure 5-6 Add Event Window with Sample Parameters (Adding Event to Existing Class) 122
Figure 5-7 Verification Message for Adding an Event (Adding Event to Existing Class) 123
Figure 5-8 Confirmation Message for Adding an Event (Adding Event to Existing Class) 124
Figure 5-9 Add Event Window (Adding Event to New Class) 125
Figure 5-10 Add Event Window with Example Parameters (Adding Event to New Class) 127
Figure 5-11 Verification Message for Adding an Event (Adding Event to New Class) 128
Figure 5-12 Confirmation Message for Adding an Event (Adding Event to New Class) 129
Figure 5-13 Add Event Window (Adding an Event to a New Class in a New Profile) 130

Figure 5-14 Add Event Window with Example Parameters (Adding an Event to a New Class in a New Profile) 132
Figure 5-15 Verification Message for Adding an Event (Adding an Event to a New Class in a New Profile) 133
Figure 5-16 Confirmation Message for Adding an Event (Adding Event to a New Class in a New Profile) 134
Figure 5-17 Update Event Window (with SGM Clients) 137
Figure 5-18 Update Event Window 138
Figure 5-19 Event List for Updating an Event 139
Figure 5-20 Update Event Window (with Event to Update) 140
Figure 5-21 Verification Message for Updating an Event 142
Figure 5-22 Confirmation Message for Updating an Event 143
Figure 5-23 Batch Events Update Window (with SGM Clients) 146
Figure 5-24 Event Batch Update Window 147
Figure 5-25 Delete User Events Window (with SGM Clients) 151
Figure 5-26 Delete User Events Window (Web-based Interface) 152
Figure 5-27 Verification Message for Deleting an Event 152
Figure 5-28 Confirmation Message for Deleting an Event 153
Figure 5-29 Batch Event Subscription Window 156
Figure 5-30 Events by Subscription Class Window 157
Figure 5-31 Add an Action Window 160
Figure 5-32 Add an Action Window (Using Notification Action Option) 161
Figure 5-33 Add an Action Window (Using Notification Action and E-mail Options) 163
Figure 5-34 Add an Action Window (Using Notification Action and System Console Options) 164
Figure 5-35 Add an Action Window (Using Notification Action and GUI Pop-up Options) 165
Figure 5-36 Verification Message for Adding an Action (Using Notification Action Option) 167
Figure 5-37 Confirmation Message for Adding an Action (Using Notification Action Option) 167
Figure 5-38 Add an Action Window (Using Other Action Option) 168
Figure 5-39 Example Parameters (Add an Action Window Using Other Action Option) 170

Figure 5-40 Verification Message for Adding an Action (Using Other Action Option) 170
Figure 5-41 Confirmation Message for Adding an Action (Using Other Action Option) 171
Figure 5-42 Update Current Actions Window 173
Figure 5-43 Update Action Window 174
Figure 5-44 Verification Message for Updating an Action 174
Figure 5-45 Confirmation Message for Updating an Action 175
Figure 5-46 View Current Actions Window 178
Figure 5-47 Performance Monitoring Window (with SGM Clients) 179
Figure 5-48 Performance Monitoring Window 180
Figure 5-49 System Monitoring Window (Single System Manager Mode) 187
Figure 5-50 System Monitoring Change Verification Screen (Single System Manager Mode) 188
Figure 5-51 Updated System Monitoring Window (Single System Manager Mode) 189
Figure 5-52 System Monitoring Window (System Group Manager Mode) 190
Figure 5-53 Update System Monitoring Window (System Group Manager Mode) 191
Figure 5-54 System Monitoring Change Verification Screen (System Group Manager Mode) 191
Figure 5-55 Updated System Monitoring Window (System Group Manager Mode) 192
Figure 6-1 Example Report (Web-based Interface) 196
Figure 6-2 Example Report (Web-based Interface Printable Format) 197
Figure 6-3 Example Report (Command Line Interface) 199
Figure 6-4 Event Reports Window (Single System Manager Mode) 200
Figure 6-5 Example Events Registered Report (Single System Manager Mode) 201
Figure 6-6 Events Registered in a Specific Class (Single System Manager Mode) 203
Figure 6-7 All Occurrences of a Specific Event (Single System Manager Mode) 204
Figure 6-8 Event Reports for System Group Window (System Group Manager Mode) 205
Figure 6-9 Event Reports Window with List of Classes (System Group Manager Mode) 206

Figure 6-10 Example Events Registered Report (System Group Manager Mode) 207
Figure 6-11 Events Registered in a Specify Class (System Group Manager Mode) 209
Figure 6-12 All Occurrences of a Specific Event (System Group Manager Mode) 210
Figure 6-13 Action Reports Window (Single System Manager Mode) 212
Figure 6-14 Example Actions Taken Report (Single System Manager Mode) 213
Figure 6-15 Actions Report for System Group Window (System Group Manager Mode) 214
Figure 6-16 Example Actions Taken Report (System Group Manager Mode) 215
Figure 6-17 Availability Reports Window (Single System Mode) 217
Figure 6-18 Example Availability Report (Single System Manager Mode) 218
Figure 6-19 Availability Reports for System Group Window (System Group Manager Mode) 220
Figure 6-20 Example Availability Report for a Specific Host (System Group Manager Mode) 221
Figure 6-21 Diagnostic Results Window (Single System Manager Mode) 224
Figure 6-22 Example Diagnostic Results Report (Single System Manager Mode) 225
Figure 6-23 Diagnostic Results Window (System Group Manager Mode) 226
Figure 6-24 Example Diagnostic Results Report (System Group Manager Mode) 227
Figure 6-25 Hardware Inventory Report Window (Single System Manager Mode) 230
Figure 6-26 Example Hardware Inventory Report (Single System Manager Mode) 231
Figure 6-27 Hardware Inventory Reports for System Group Window (System Group Manager Mode) 233
Figure 6-28 Example Hardware Inventory Report (System Group Manager Mode) 234
Figure 6-29 History of Hardware Changes Window (Single System Manager Mode) 236
Figure 6-30 Example Hardware Changes Report (Single System Manager Mode) 237
Figure 6-31 Hardware Changes Reports for System Group Window (System Group Manager Mode) 239

Figure 6-32 Example Hardware Changes Report (Single Group Manager Mode) 239
Figure 6-33 Software Inventory Report Window (Single System Manager Mode) 242
Figure 6-34 Example Software Inventory Report (Single System Manager Mode) 243
Figure 6-35 Software Inventory Reports for System Group Window (System Group Manager Mode) 245
Figure 6-36 Example Software Inventory Report (System Group Manager Mode) 246
Figure 6-37 History of Software Changes Window (Single System Manager Mode) 248
Figure 6-38 Example Software Changes Report (Single System Manager Mode) 249
Figure 6-39 Software Changes for System Group Window (System Group Manager Mode) 250
Figure 6-40 Example Software Changes Report (System Group Manager Mode) 251
Figure 6-41 Example System Inventory Report (Single System Manager Mode) 253
Figure 6-42 Example System Inventory Report (System Group Manager Mode) 254
Figure 6-43 History of System Changes Window (Single System Manager Mode) 256
Figure 6-44 Example System Changes Report (Single System Manager Mode) 257
Figure 6-45 System Changes for System Group Window (System Group Manager Mode) 258
Figure 6-46 Example System Changes Report (System Group Manager Mode) 259
Figure 6-47 Site Reports Window 260
Figure 6-48 Site Information Report 262
Figure 7-1 View Logbook Entries Window (Single System Manager Mode) 264
Figure 7-2 Specified Logbook Entries (Single System Manager Mode) 264
Figure 7-3 Logbook Entry Information (Single System Manager Mode) 265
Figure 7-4 View Logbook Entries Window (System Group Manager Mode) 266
Figure 7-5 Specified Logbook Entries (System Group Manager Mode) 266
Figure 7-6 Logbook Entry Information (System Group Manager Mode) 267
Figure 7-7 Create Log Window (Single System Manager Mode) 268

Figure 7-8 Logbook Entry Confirmation Window (Single System Manager Mode) 269
Figure 7-9 Completed Logbook Entry (Single System Manager Mode) 270
Figure 7-10 Create Log Window (System Group Manager Mode) 271
Figure 7-11 Logbook Entry Confirmation Window (System Group Manager Mode) 272
Figure 7-12 Completed Logbook Entry (System Group Manager Mode) 273
Figure 8-1 Displaying a Message in the Console Window 276
Figure 8-2 Displaying a Message on an X Window System Display 277
Figure 8-3 Sending an E-mail Message 279
Figure 8-4 Example Action Parameters for Sending an E-mail Message 280
Figure 8-5 Example Verification Message for Sending an E-mail Message Action 281
Figure 8-6 Example Confirmation Message for Sending an E-mail Message Action 281

List of Tables

Table 1-1 ESP Benefits 12

Table 2-1 ESP Startup Error Messages 42

Table 3-1 Customer Profile Parameters 53

Table 3-2 Available User Permissions 63

Table 3-3 Command Line Interface User Permission Settings 72

Table 4-1 Global Configuration Parameters 85

Table 4-2 Update System Information Window Parameters (Single System Manager Mode) 92

Table 4-3 Add New Client Window Parameters 94

Table 4-4 Update System Information Window Parameters (SGM Server) 99

Table 4-5 Update Client Information Window Parameters (SGM Client) 101

Table 5-1 Batch Update Options 148

Table 5-2 Notification Action Parameters 166

Table 5-3 espnotify Parameters 169

Table 5-4 PMIE Rules 181

Table 6-1 Report Navigation Controls 197

Table 6-2 Events Registered Report Contents (Single System Manager Mode) 202

Table 6-3 Events Registered Report Contents (System Group Manager Mode) 208

Table 6-4 Actions Taken Report Contents (Single System Manager Mode) 213

Table 6-5 Actions Taken Report Contents (System Group Manager Mode) 215

Table 6-6 Single System Availability Report Contents (Single System Manager Mode) 219

Table 6-7 Single System Availability Report Contents (System Group Manager Mode) 222

Table 6-8 Diagnostic Results Report Contents (Single System Manager Mode) 225

Table 6-9 Diagnostic Results Report Contents (System Group Manager Mode) 228
Table 6-10 Hardware Inventory Report Contents 232
Table 6-11 Hardware Inventory Report Contents (System Group Manager Mode) 235
Table 6-12 Hardware Changes Report Contents (Single System Manager Mode) 238
Table 6-13 Hardware Changes Report Contents (System Group Manager Mode) 240
Table 6-14 Software Inventory Report Contents (Single System Manager Mode) 244
Table 6-15 Software Inventory Report Contents (System Group Manager Mode) 247
Table 6-16 Software Changes Report Contents (Single System Manager Mode) 249
Table 6-17 Software Changes Report Contents (System Group Manager Mode) 251
Table 6-18 System Changes Report Contents (Single System Manager Mode) 257
Table 6-19 System Changes Report Contents (System Group Manager Mode) 259
Table 8-1 Example Action Parameters for Sending an E-mail Notification 280

What's New in this Document

Revision 008 makes the following changes to this document:

- It updates the document to include ESP 3.0 changes from the SGI ProPack 2.3 release.
- It adds to Chapter 1 information about new features included in ESP 3.0 and the new architecture used by ESP 3.0.
- It updates the descriptions of the Web-based interface throughout the document.
- It updates the descriptions of the `espconfig` and `espreport` commands throughout the document.
- It incorporates miscellaneous technical and editorial changes throughout the document.

This revision supports only the Linux operating system version of ESP 3.0 that is included in the SGI ProPack 2.3 release.

Introduction

The SGI product line ranges from desktop workstations to supercomputers, which makes it one of the broadest product lines in the industry. Supporting such a diverse product line creates many challenges.

Embedded Support Partner (ESP) was created to address some of these challenges by automatically detecting system conditions that indicate potential future problems and notifying the appropriate personnel. This enables SGI customers and support personnel to proactively support systems and resolve issues before they develop into actual failures.

ESP integrates monitoring, notifying, and reporting operations. It enables users to monitor one or more systems at a site from a local or remote connection. ESP provides the following functions:

- Monitoring system configuration, events, performance, availability, and services
- Providing proactive notification when specific conditions occur
- Generating reports about system activity (configuration changes, events, availability, etc.)
- Sending event information to SGI for statistical interpretation
- Providing usability enhancements (common interface, remote support, and system group management)

Figure 1-1 provides a functional diagram of ESP.

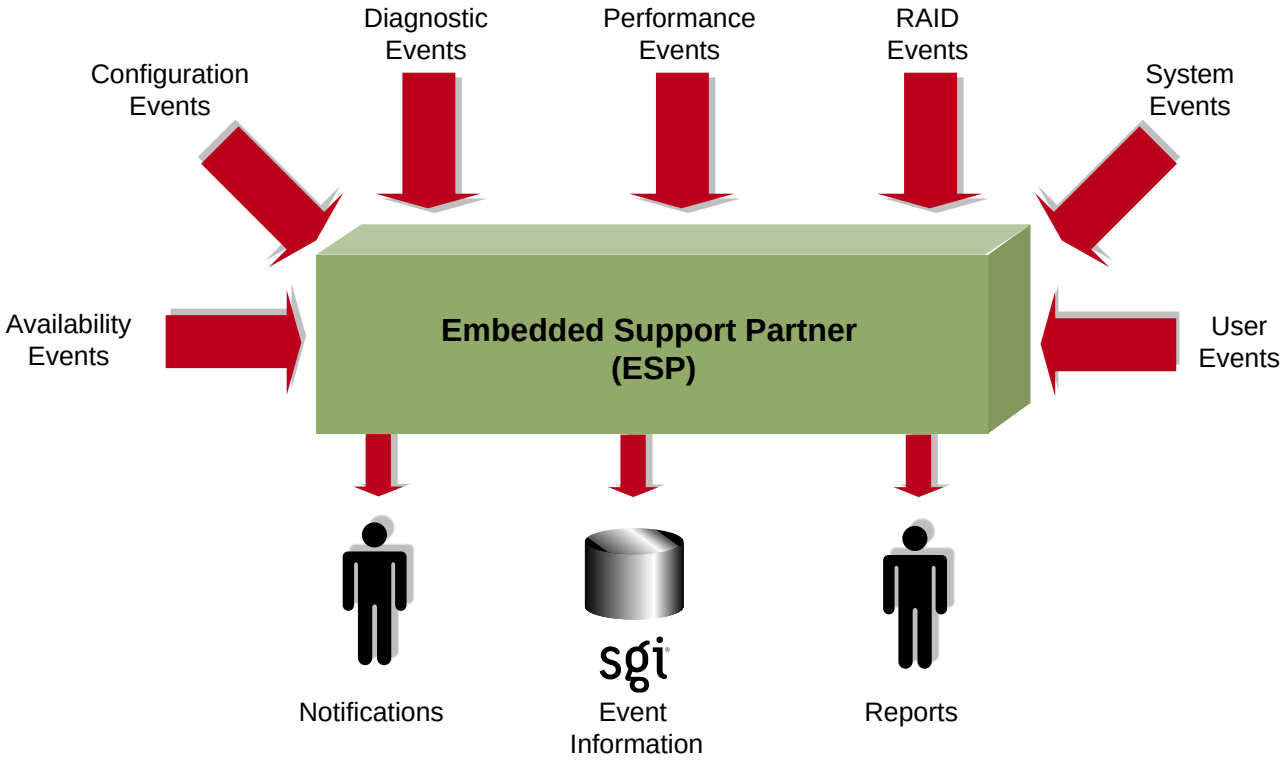


Figure 1-1 ESP Functional Diagram

This document describes the Linux operating system (OS) version of ESP 3.0, which is included in SGI ProPack 2.3.

Distribution

The ESP software is distributed in two levels:

- Base package
- Extended package

Base Package

The base package includes the single system manager, which has the functionality necessary to:

- Configure ESP
- Monitor a single system for system and performance events, configuration changes, and availability
- Notify support personnel when specific events occur
- Generate basic reports

The features in the base package are included at no extra cost. They are installed by default, and ESP begins monitoring the system as soon as the system is booted (if ESP is `chkconfig`'ed on). You can configure the base package to specify what types of events it should monitor and whom it should notify when events occur.

Note: ESP can also monitor events from diagnostic tests and perform actions based on these events. To use these optional features, install the diagnostics from the *Internal Support Tools 2.0* CD or a later release. The *Internal Support Tools* CDs are available only to SGI personnel.

Extended Package

The extended package includes the System Group Manager (SGM), which adds the capabilities to monitor multiple systems at a site. The system selected as the group manager runs the SGM, which manages all systems in the group.

The SGM provides functionality to uniformly manage multiple systems when more than one system is installed at a site. Specifically, it performs the following functions:

- System group event tracking
- System group configuration management
- System group availability monitoring
- Notification (based on the events that occur on systems in the group)
- Enhanced reporting for groups of systems

Any system within a system group can be designated the group manager (it is even possible to have more than one group manager). A system that is designated as the group manager monitors all systems in the group, including itself.

The features in the extended package are not enabled unless the customer acquires a license to use them. (A 90-day free trial license is included; full licenses are included in some service contracts or may be purchased separately.)

Figure 1-2 provides a block diagram of system group management.

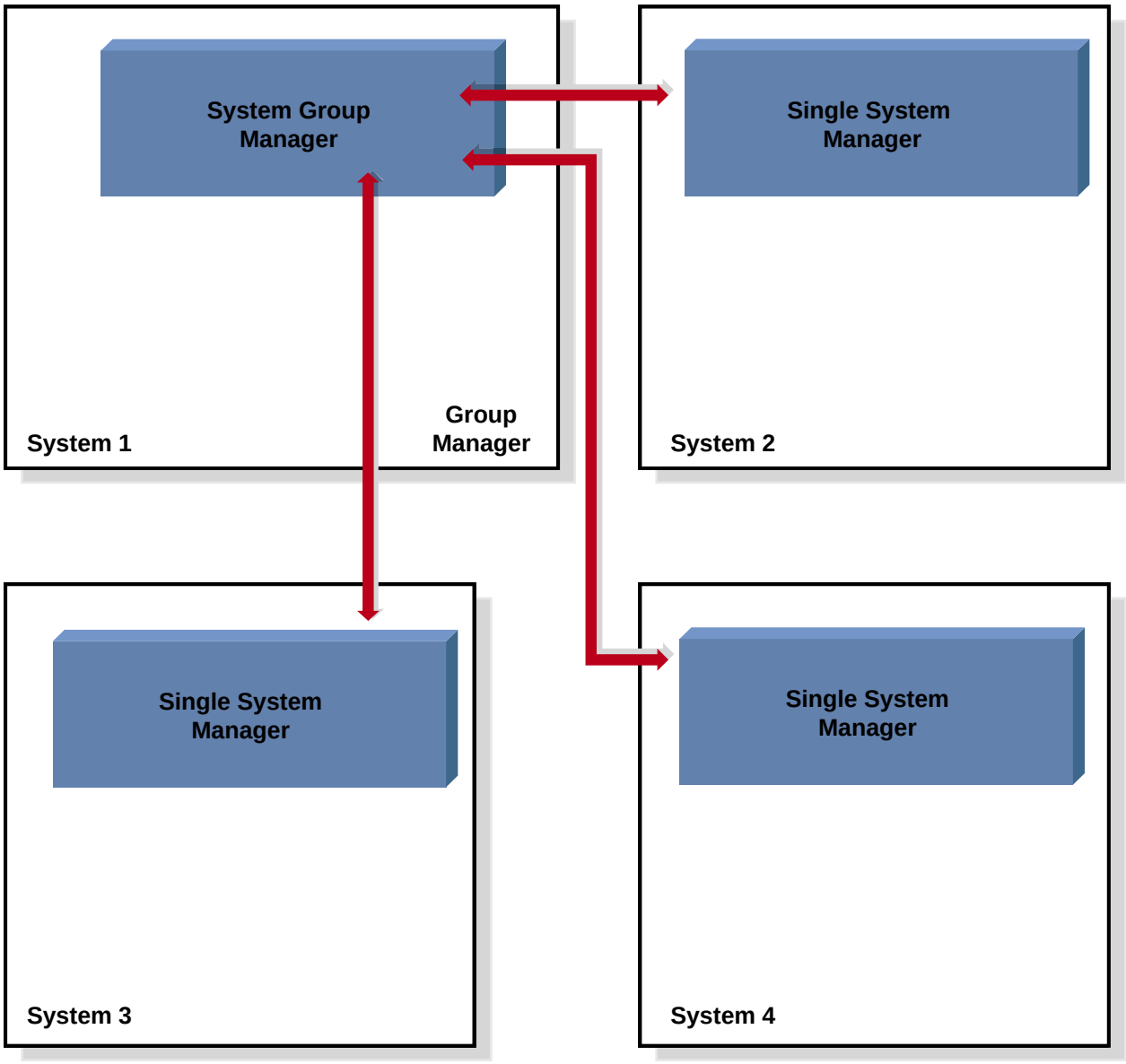


Figure 1-2 System Group Management Block Diagram

ESP 3.0 adds enhanced group management functionality in the extended package, including:

- Support for named groups
- Communication via TCP/IP protocol
- Support for full and light nodes
- Support for group management over hierarchies
- A simplified group management configuration process
- Enhanced configuration for SGM clients
- Central logbook capability

Named Groups

ESP 3.0 enables you to categorize the systems that you monitor by group name. You can use the group names to quickly access statistical information and reports about all systems in a group by generating a site report (through the `Reports` -> `Site` menu options). Example group names include *Server*, *Desktop*, and *Web server*. (Refer to Figure 1-3.)

Figure 1-3 Named Groups

Full and Light Nodes

ESP 3.0 enables SGM clients to be full or light nodes:

- A full node is a client system that stores ESP data in a database on a local disk and also sends the data to a group manager system for storage. In this case, ESP maintains two copies of the data: one copy on the local system and one copy on the group manager system.
- A light node is a client system that sends all ESP data to a group manager system for storage. No ESP data is stored on the client system, which reduces the resources used on the system. In this case, ESP stores all data on the group manager system.

  For light nodes, you can generate reports on the SGM server (by accessing the ESP 3.0 interface from the Web server or by running the `espreport` command on the SGM server).

  Running `espreport` on a light node returns the following message:

  ```
  ****ESPREPORT (EventRprt): This system is a light node. espreport
  cannot be run on light node.
  ```

Note: You can convert a light node to a full node at any time; however, only data that is generated after the conversion completes is stored in the local database. (Data generated before the conversion completes is stored only in the database on the SGM server.)

Figure 1-4 shows an example of a group that contains full and light nodes.

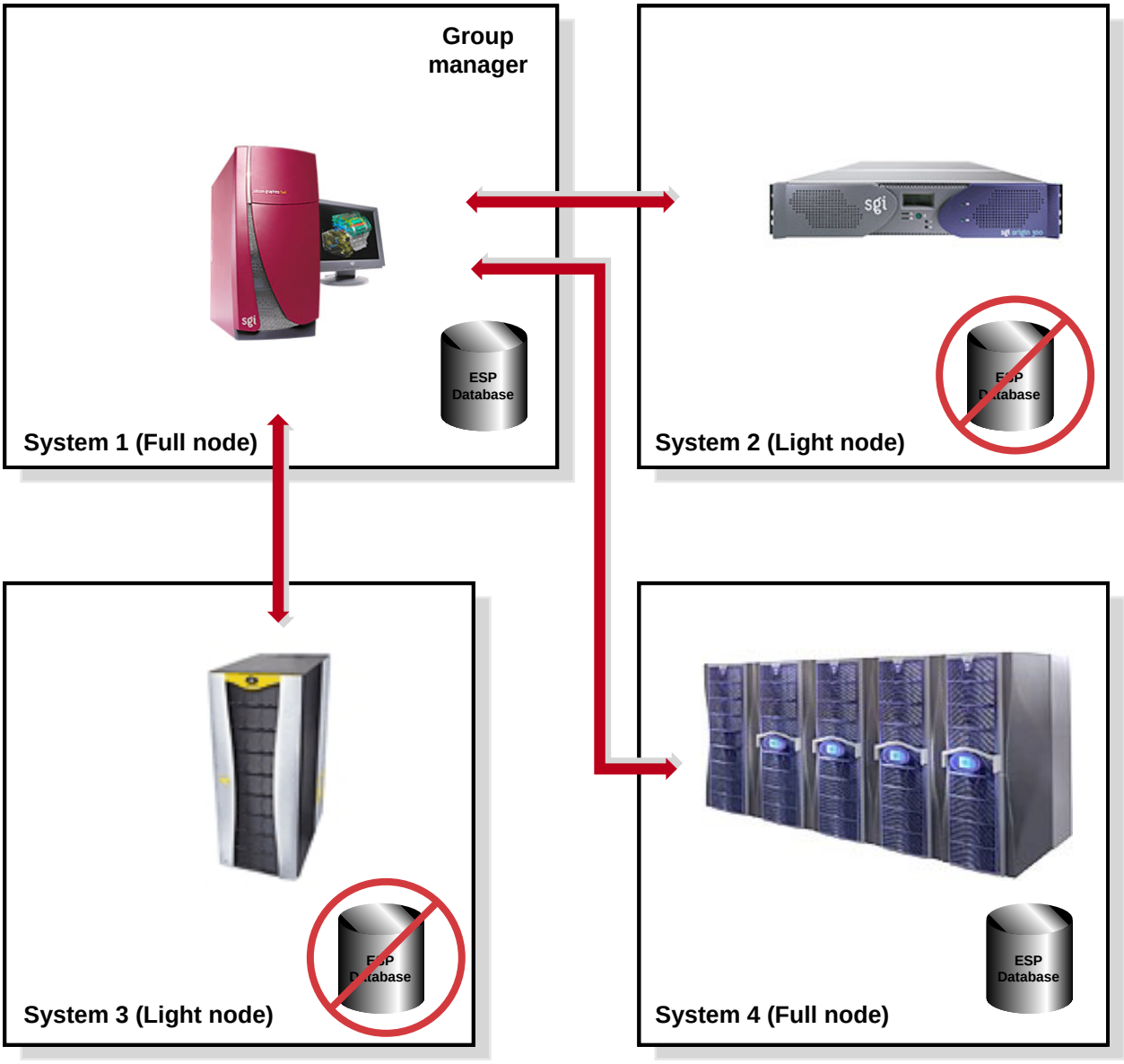


Figure 1-4 Full and Light Nodes

TCP/IP Protocol

ESP 3.0 uses TCP/IP protocol to communicate between a group manager system and its clients. (Previous versions of ESP used RPC protocol over TCP/IP.) Using standard TCP/IP protocol provides the following benefits:

- TCP/IP protocol is easier to configure.
- TCP/IP protocol uses fewer resources.
- TCP/IP protocol enables ESP 3.0 to communicate through a firewall.

Group Management Over Hierarchies

Under ESP 3.0, an SGM server is required to know the hostname but not the IP address of a client system. ESP 3.0 allows intermediate system(s) to know this information. This enables ESP to work through a firewall. (The intermediate systems must have `eventmond` and ESP running. The intermediate systems run an SGM dynamic shared object [DSO] that routes events from host to host. The intermediate systems do not require an SGM license unless they are configured as SGM servers.)

For example, system A is an SGM server and system D is a client, but system A does not know the IP address of system D. However, system B knows the IP addresses of systems A and C, and system C knows the IP addresses of systems B and D. ESP 3.0 allows you to add system D as a client to system A by specifying the connection path as follows:

B>C

This means that events will be forwarded from system D to system A, following the connection path through system C and system B. (Refer to Figure 1-5.)

In this example, an SGM DSO that is running on the client system (system D) forwards the event through the `eventmond` daemons on the intermediate systems (system C and system B) to the SGM server system (system A).

Note: The SGM DSO feature does not require a license; however, you need a license on the SGM system to create SGM clients.

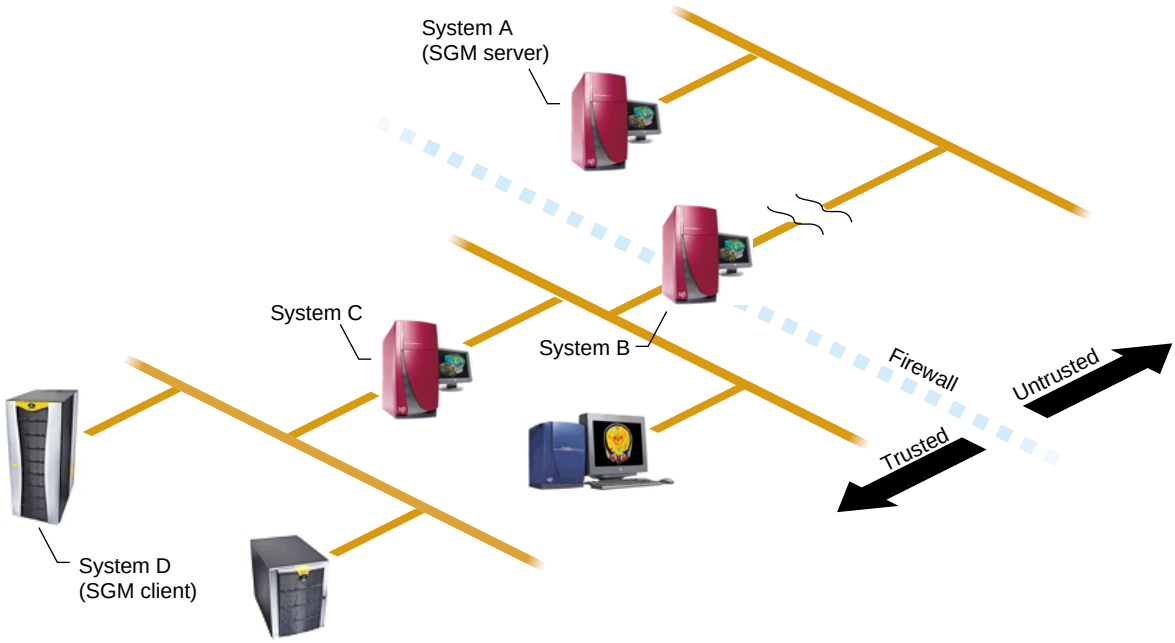


Figure 1-5 Group Management Over Hierarchies

Simplified Group Management Configuration

Under ESP 3.0, you do not need to configure group management on both the server and client sides like you did in earlier versions of ESP. You only need to configure group management from the SGM server side.

Note: No authentication is performed when you use this method to add clients to a server. For increased security, you can add a password that the server and client must exchange before they transfer data. To do this, you must configure the authentication password on the client and then on the server.

Enhanced Configuration for SGM Clients

ESP 3.0 enables you to configure all configuration parameters (including performance monitoring and system monitoring parameters) for remote systems from the SGM server. This enables you to set parameters for multiple systems from one location.

Note: You cannot configure performance monitoring and system monitoring parameters for clients that are connected to a group manager through intermediate systems. The group manager must have a direct connection to the clients to configure these parameters. This restriction is caused by limitations of PMIE.

Central Logbook Capability

ESP 3.0 includes a feature that enables you to create logbook entries for SGM clients on the SGM server. (The logbook entries are stored on the SGM server.) This feature enables you to store all logbook data on a common system, which makes it easier to access information about multiple systems. You can specify which system each logbook entry is for.

ESP Benefits

Table 1-1 lists the benefits that ESP provides for service personnel and customers.

Table 1-1 ESP Benefits

Component	Feature	Benefit to Service Provider	Benefit to Customer
Base Package (Single System Manager)	Single Web-based interface	Increases usability of support tools on a single system	Provides fast and effective service
	Broad and useful support functionality	Provides an integrated set of tools that work in a single framework while increasing support coverage	Provides consistent and wide coverage on systems
	Centralized event processing (single system)	Enables you to collect and display all information from one central location	Provides the entire set of circumstances in one place
	Centralized automated response and notification (single system)	Provides visibility to problems as they occur	Enables proactive support Provides a quick insight to problems
	Remote support	Provides a virtual seat into the site remotely	Provides an effective means of delivering service (which greatly increases system availability with accurate problem diagnosis)

Table 1-1 ESP Benefits **(continued)**

Component	Feature	Benefit to Service Provider	Benefit to Customer
Extended Package (System Group Manager)	Centralized event processing (group management)	Enables you to collect and display all information from one central location (which helps to determine causes of problems on systems within the site)	Provides the entire set of circumstances in one place
	Centralized support administration (group management)	Provides a single location from which all support activities can be performed for a group of systems	Eases administration and service tracking
	Centralized automated response and notification (group management)	Provides visibility to problems as they occur	Provides proactive support Provides a quick insight to problems
	Centralized site reporting	Provides accurate system and site data online	Enables extensive tracking of availability and system performance
	Centralized troubleshooting	Provides the ability to resolve problems from a central location	Provides an efficient mechanism to fix problems on-site

Table 1-1 ESP Benefits **(continued)**

Component	Feature	Benefit to Service Provider	Benefit to Customer
Performance Monitoring Tools	Proactive, automated performance analysis	Assists in diagnosis of system-level performance issues	Identifies performance hotspots and areas where system resource usage could be optimized for improved performance
	Extensible rule evaluation mechanism	Provides an easy method to add site- or system-specific rules to the default set	Enables use of additional software products to extend the range of monitored subsystems (for example, Cisco routers and Web servers)
	Local or remote service failure detection and quality-of-service monitoring	Automates detection of failed services for proactive support	Increases service availability and quality by automating service probing and checking

ESP Architecture

ESP is a modular system that uses a producer/client architecture and receives events from the Event Manager. Each module works independently on a specific function, and no functional overlap exists between the various modules. Some modules run as daemons, some run as dynamic shared objects (DSOs) that can load into the Event Manager, and some run as stand-alone applications that are driven by events.

Note: For more information about the Event Manager and the client/producer architecture, refer to the *Event Manager User Guide*, publication number 007-4661-00x.

The daemon components of ESP are:

- Core software
  - System Support Database (SSDB): `espdbd`
- Monitoring software
  - Event monitor subsystem: `eventmond`

The DSO components of ESP are:

- Core software:
  - ESP DSO
  - SGM DSO
- Monitoring software:
  - `availmon` DSO
  - `syslog` DSO
  - Performance monitoring DSO

The stand-alone components of ESP are:

- Monitoring software
  - Availability monitor: `availmon`
  - Configuration monitor: `configmon`
- Notification software
  - `espnotify`
  - `espcall`
- Console software
  - Configurable Web server: `esphttpd`
  - Web-based interface
  - Report generator core
  - Report generator plugins
- Command line interface
  - Configuration tool: `espconfig`
  - Report tool: `espreport`

If you install the performance metrics inference engine application, `pmie`, which is included in the Performance Co-Pilot Execution Only Environment (`pcp_eoe` subsystem), ESP can receive notification of resource oversubscription, bandwidth saturation, and other adverse performance conditions.

If you install the *Internal Support Tools 2.0* CD or a later release, ESP can receive data from the diagnostic tools included on the CD.)

Note: The *Internal Support Tools* CDs are available only to SGI support personnel (for example, System Support Engineers).

Figure 1-6 shows the ESP architecture when a Web-based interface is used. Figure 1-7 shows the ESP architecture when a command line interface is used. Descriptions of the components follow the figures.

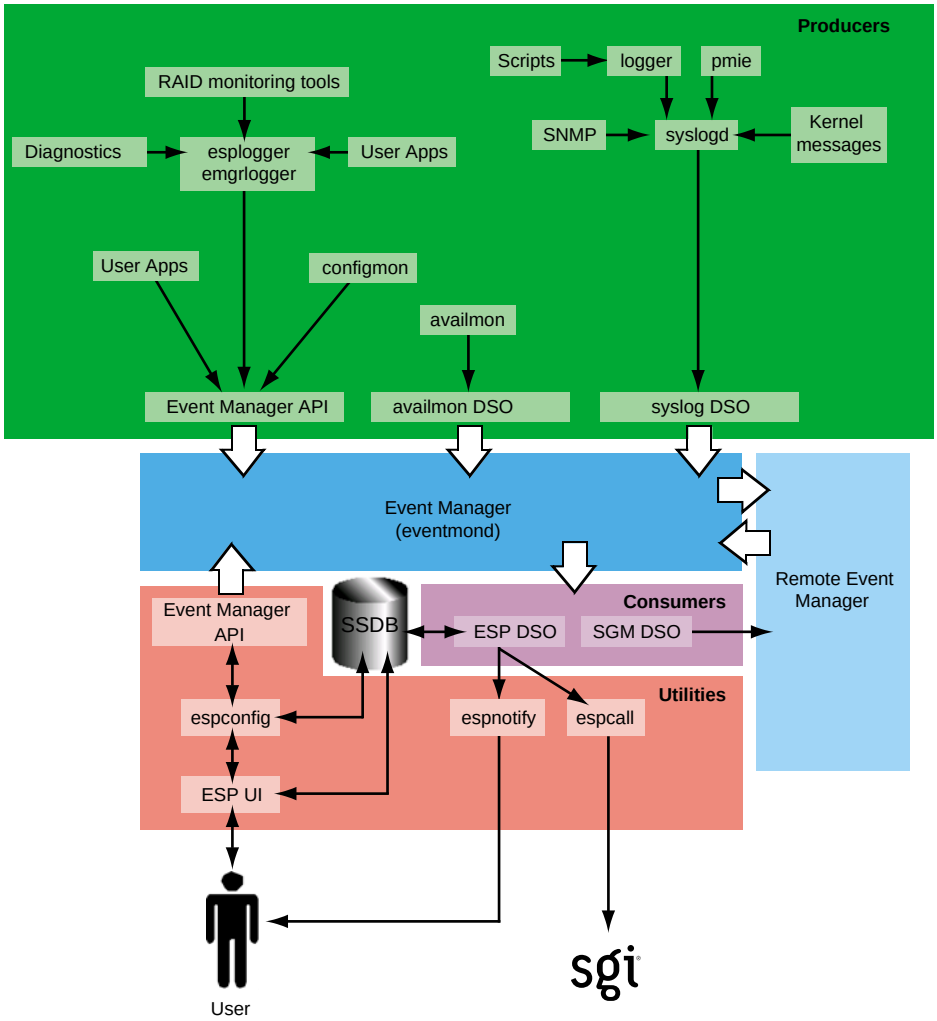


Figure 1-6 ESP Architecture (Using Web Browser)

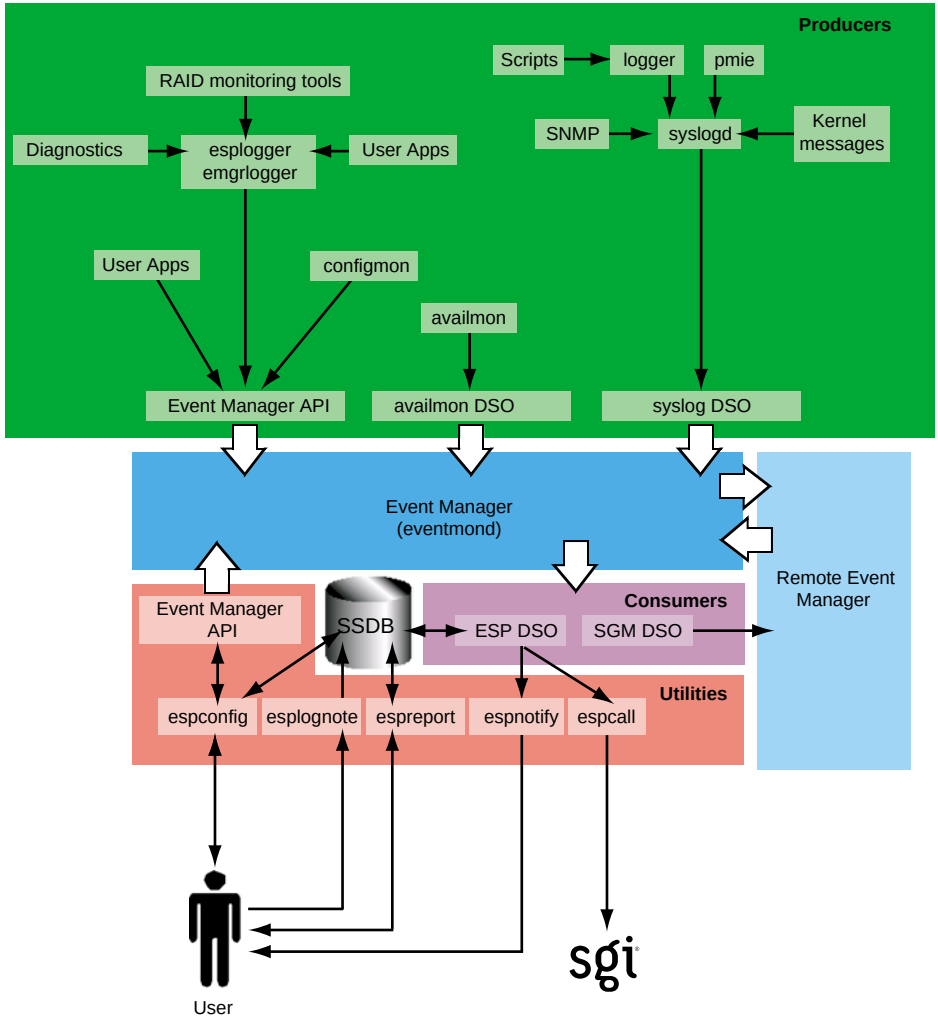


Figure 1-7 ESP Architecture (Using Command Line Interface)

Core Software

The core software includes the functionality that is necessary to process events, to determine the action to perform, and to store data about the system that ESP is monitoring.

The core software includes the following components:

- System Support Database (SSDB)
- ESP and SGM dynamic shared objects (DSOs)

System Support Database (SSDB)

The SSDB is the central repository for all system support data. It contains the following data types:

- System configuration data
- System event data
- System actions for system events
- System availability data
- Diagnostic test data
- Task configuration data

The SSDB includes a server that runs as a daemon, `espdbd`, which starts at boot time.

Note: ESP includes a utility (`esparchive`) that you can use to archive the current SSDB data, which reduces the amount of disk space that is used.

ESP and SGM DSOs

There are two main consumer DSOs that ESP 3.0 uses to subscribe, unsubscribe, and process events:

- The ESP DSO
- The System Group Manager (SGM) DSO

ESP DSO

The ESP DSO is the main ESP processing module. It is the consumer for all ESP events. It receives events from the Event Manager, converts them to the ESP-specific format, saves them in the SSDB, and executes any ESP actions that are assigned to the events. All processing done is based on configuration information from the ESP database.

The ESP startup script starts this DSO as a task of the Event Manager daemon (`eventmond`). The DSO stores event information in the SSDB and uses the `espnotify` utility to generate notifications.

SGM DSO

The SGM DSO provides distributed functionality among a group of ESP systems. The Event Manager loads and executes this DSO when there are SGM-specific events to handle. There is no need to load and execute this DSO during the startup sequence.

The SGM DSO serves as a router/translator for remote ESP configuration requests. When an SGM server needs to configure an SGM client, it sends an ESP SGM event via the Event Manager API. This event has an SGM DSO as a consumer; when an SGM DSO receives these events, it either performs a routing/forwarding (producer) operation if the event needs to go to a remote system or executes the specified operation and sends the result back to the SGM server. SGM DSO functionality requires a license.

Monitoring Software

A key function of ESP is monitoring the system. The ESP base package includes software that enables the following types of monitoring on a system:

- Configuration monitoring
- Event monitoring
- Availability monitoring

Monitoring is performed by tools that run as stand-alone programs or as DSOs and send events to the Event Manager. The Event Manager passes subscribed events to ESP for processing.

Note: Performance monitoring is available through the `pmie` application, which is included in the Performance Co-Pilot Execution Only Environment (`pcp_eoe` subsystem). Refer to "Performance Monitoring Tools" on page 30 for more information.

Configuration Monitoring

The base package includes a configuration monitoring application, `configmon`. `configmon` is a standalone application that monitors the system configuration by performing the following functions when configuration events occur:

- It determines the current software and hardware configuration of a system, gathering as much detail as possible (for example, serial numbers, board revision levels, installed software products, installed patches, installation dates, etc.).
- It verifies that the configuration data in the SSDB is up-to-date by comparing the current system configuration data with the configuration data in the SSDB.
- It updates the SSDB so that it is current (with information about the hardware or software that has changed).
- It provides data for various system configuration reports that the system administrator or field support personnel can use.

The `configmon` application runs at system start-up to gather updated configuration information. `configmon` uses a producer/consumer model. Some functionality is provided by the producer and some is provided by the consumer (which may or may not be on the same system as the producer if SGM servers and clients are used). The `configmon` binary tool handles both functions.

The `configmon` producer gathers information about the hardware and software configuration. Then, it checks a file in the `/var/esp` directory that contains checksums from the last time that `configmon` was run. If the current and old checksums are the same, no action is performed. If the `configmon` producer detects any differences, then the data that differs is sent to the `configmon` consumer via a private `configmon` event.

The `configmon` consumer then checks the SSDB and compares the data received from the producer to the SSDB data. If no differences in the data exist, no action is performed. If differences do exist, `configmon` brings the database up-to-date and moves the old configuration data into the archive tables.

Note: You can use the `-u` (update) and `-f` (force) command-line options to force producer data to go to the consumer.

On non-SGM systems, both the producer and consumer reside on the local system (and the data passes through the Event Manager).

Event Monitoring

ESP is an event-driven system. Events can come from various sources. Examples of events are:

- Configuration events
- Inferred performance events
- Availability events
- System critical events (from the kernel and various device drivers)
- Diagnostic events

Starting with ESP 3.0, event management moves outside of the ESP framework. A new standalone version of the Event Manager daemon (named `eventmond` to maintain compatibility with previous versions of ESP and other tools) performs all event management functions.

The Event Manager daemon collects event information from other applications. It runs independently of all other applications and enables local or remote applications to receive event data from it on a subscription basis. Any application can subscribe to receive event information from the Event Manager; event information availability is not limited to ESP, as it was in earlier releases of ESP and `eventmond`. ESP 3.0 subscribes to the Event Manager daemon to receive information about events that occur on a system.

The new Event Manager daemon provides greater flexibility for applications that submit events. This flexibility provides enhanced monitoring ability for ESP and any other applications that subscribe to receive events from the Event Manager.

Applications that submit events can specify the following information:

- An event class ID number
- An event type ID number that is unique to each application
- Internal flags that indicate how to handle the message
- An event version number that is specific to each application
- The time that the event occurred
- The user ID number of the process that generated the event
- The hostname (including domain name) of the system that generated the event
- The name of the application that owns the event (for example, Kernel or UNIX)
- The name of the application that generated the event (for example, SYSLOG)
- The event data

All events that ESP receives pass to the Event Manager daemon from one of the following paths:

- `syslog DSO`
- `esplogger` or `emgrlogger`
- `logger`
- Event Manager API

syslog DSO

The `syslog` DSO runs as a separate task of the Event Manager daemon and performs the following functions:

- It reads all SYSLOG messages from the `/tmp/.eventmond.events.sock` file.

  Note: The ESP installation script creates a configuration entry in the `/etc/syslogd.conf` file that causes the `syslogd` daemon to write all messages to `/tmp/.eventmond.events.sock` file.

- It converts the messages to Event Manager event format.
- It passes the events to the Event Manager.

The Event Manager sends any subscribed SYSLOG events to the ESP DSO consumer, so ESP can process the events.

The ESP startup script starts the `syslog` DSO by loading it as a task of the Event Manager. The `syslog` DSO continues to run as long as the Event Manager runs.

esplogger and emgrlogger

The `esplogger` and `emgrlogger` applications provide a simple command-line interface to submit events to the Event Manager. `emgrlogger` works with the new Event Manager and replaces `esplogger`, which previous versions of `eventmond` and ESP used. `esplogger` remains available to provide backward compatibility.

Note: `emgrlogger` can produce any type of Event Manager event, including subscription events.

logger

`logger` provides a shell command interface to the `syslog` system log routine. It can log messages specified on the command line, from a specified file, or from the standard input. Each line in the specified file or standard input is logged separately.

Event Manager API

The Event Manager API provides a mechanism that enables tasks to communicate with `eventmond`. The `eventmond` daemon receives information from external monitoring tasks through API function calls. Each command that is sent to `eventmond` returns a status code that indicates successful completion or the reason that a failure occurred.

Availability Monitoring

The base package also includes an availability monitoring application, `availmon`. `availmon` monitors system uptime and differentiates between controlled shutdowns, system panics, power cycles, and power failures. Availability monitoring is useful for high-availability systems, production systems, or other customer sites where monitoring availability information is important.

The `availmon` script runs at system start-up to gather the availability data. Do not manually run the `availmon` script. Manually running the script creates inaccurate availability results.

The `availmon` DSO monitors system uptime. To do this, it updates the `/var/adm/avail/.save/lasttick` file every 5 minutes to indicate that the system is still running. The `/var/adm/avail/.save/lasttick` file contains the current uptime (in seconds since January 1, 1970).

Note: In ESP 3.0, you cannot change the default status interval of last tick (5 minutes) or the default interval for sending status reports (7 days).

You can use the `/usr/sbin/eventmond -T` command to verify that the `availmon` DSO is running. The output from this command lists the `availmon` DSO when it is running. SGI recommends that you do not manually run the `availmon` DSO.

Notification Software

Notification is one of the actions that can be programmed to take place when a particular system event occurs. The notification software provides several types of notifiers, including dialog boxes on the local system, e-mail, paging, and diagnostic reports and other types of reports.

The `espnotify` tool provides the following notification capabilities for ESP:

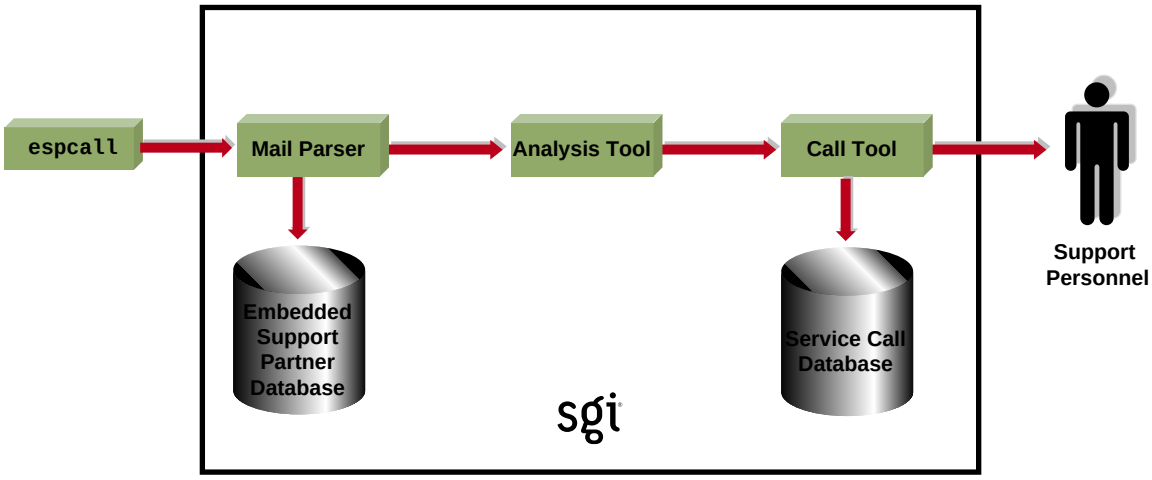
- E-mail notifications
- GUI-based or console text notifications (with audio if the notification is on the local host)
- Program execution for notification
- Alphanumeric and chatty paging through the `Qpage` application

ESP 3.0 for the Linux OS does not include paging by default. SGI does not distribute the `QPage` application for the Linux OS. Paging capabilities are disabled when ESP 3.0 runs under the Linux OS. The ESP 3.0 graphical user interface for the Linux OS does not include the `Paging` menu.

If you obtain the `QPage` application for the Linux OS from another source, you should manually install and configure it and then create an ESP action that calls the `QPage` application.

Typically, the ESP DSO invokes the `espnotify` tool in response to some event. However, you can run the `espnotify` tool as a stand-alone application, if necessary.

The `espcall` tool sends event information from a system to the main ESP database at SGI. Figure 1-8 shows how this information is processed.



1) espcall sends e-mail to SGI with information about the event.
2) A mail parser application running at SGI receives the e-mail and logs the data in the master ESP database.
3) An analysis tool analyzes a set of business rules for the event and determines if a service call should be opened.
4) If a call needs to be opened, the call is created in the service database and the appropriate support personnel are notified.

Figure 1-8 Sending Event Information to SGI

SGI uses the event information to provide faster and more accurate responses to potential system problems. (Any customer can send event information to SGI; however, service calls are automatically opened only for customers whose service contracts include this option.)

The following example message, which was generated by `espcall`, shows the type of information that is returned to SGI for an availability event:

```
Subject: [maui]: System Information

maui.sgi.com 1015961831,1015961831,1015357057,0,7
,NULL,NULL,NULL,NULL,NULL,NULL,0,0,NULL,NULL 03/12/2002 11:37:11
Availability 4000 Status report 2097158 21  B0006011
```

Console Software

The ESP base package includes console software that enables you to interact with it from a Web browser. The console software uses the Configurable Web Server (`esphttpd`) to receive input from the user, send it to the ESP software running on the system, and return the results to the user. (`inetd` invokes `esphttpd` whenever a Web server connection is needed.)

The console software also includes a report generator core and a set of plugins to create various types of reports. These reports are based on the data that ESP tasks provide, such as `configmon`, `availmon`, etc.

In the base package, you can access the following types of reports:

- System, hardware, and software configuration reports (current and historical)
- System event reports
- Event action reports
- Local system metrics (MTBI, availability, etc.)
- ESP configuration

The extended package enables you to generate enhanced site-level reports and reports for any system on the site.

Web-based Interface

If you use a graphical Web browser (for example, Netscape Communicator) to access the Web server, the console software provides a graphical Web-based interface that supports the following functionality:

- Configuring the behavior of ESP
- Configuring the Web server
- Configuring system groups
- Configuring the behavior of tasks
- Setting up monitors and associated thresholds
- Setting up notifiers
- Generating reports for a single system or group of systems

- Accessing system consoles and system controllers
- Remotely controlling a system with the IRISconsole multiserver management system

The ESP GUI uses the `espconfig` command to interact with the Event Manager

Command Line Interface

If you prefer to use a command line interface, the Command Line Application (CLA) software enables you to connect to ESP without using a Web server. This enables ESP to be used at a site where the Web server cannot be used for security reasons. It also enables ESP to be used over slower remote connections because only text is transferred across the connection.

The CLA software comprises three components:

- `espconfig`
- `esplognote`
- `espreport`

The `espconfig` command enables you to configure ESP. `espconfig` is the main ESP configuration utility. It maintains all ESP configuration information in the SSDB and ESP configuration files. It performs ESP-related operations, such as database accesses and Event Manager interactions (for example, subscribing/unsubscribing certain events and producing SGM-related events), based on command-line interface requests.

The `esplognote` command enables you to create logbook entries.

The `espreport` command enables you to generate and view reports.

Note: You must use the root account or an account with root privileges to execute the `espconfig`, `esplognote`, and `espreport` commands.

External Tools

The following external tools can generate events:

- Performance monitoring tools
- Diagnostic tools
- RAID monitoring tools

These tools are not part of the ESP package and must be loaded separately.

Performance Monitoring Tools

The performance metrics inference engine application, `pmie`, which is included in the Performance Co-pilot Execution Only Environment (`pcp_eoe` subsystem), provides ESP with performance monitoring events.

`pmie` is an inference engine for performance metrics: It evaluates a set of performance rules at specified time intervals. You can use a separate utility to customize and extend the rules and their attributes.

Refer to the *Performance Co-Pilot for IA-64 Linux User's and Administrator's Guide*, publication number 007-4580-00*x*, for more information about `pmie` and the `pcp_eoe` subsystem.

ESP 3.0 uses a performance monitoring DSO when you configure performance monitoring settings via the ESP user interface or the `espconfig` command (for example, `/usr/sbin/espconfig -on performance` or `/usr/sbin/espconfig -off performance`).

The performance monitoring DSO enables you to:

- Enable/disable PMIECONF at the global level (performs `chkconfig pmie on` or `chkconfig pmie off`)
- Enable/disable specific PMIE rules

You can use the ESP user interface or the `espconfig` command to configure performance monitoring.

Diagnostic Tools

The support tools included in the *Internal Support Tools 2.0* CD and later releases can also interface with the ESP framework. If you install the *Internal Support Tools 2.0* CD or a later release, ESP collects data from the diagnostic tools that are included on the CD. Refer to the CD booklet for installation instructions for the support tools.

Note: The *Internal Support Tools* CDs are available only to SGI support personnel (for example, System Support Engineers).

RAID Monitoring Tools

Starting with IRIX 6.5.17, ESP receives RAID events from the TP9100 and TP9400 disk subsystems. The following software enables ESP to receive these events:

- The `tpmwatch` application monitors the TP9100 disks and writes RAID events to the `tpmwatch` log.
- The `tpssm7monitor` (for T9400 releases 3 and 4) and `tpssmmonitor` (for TP9400 release 5) daemons monitor the TP9400 disks and write RAID events to the Major Event Log (MEL).
- A script checks the `tpmwatch` log and MEL for new events and uses `esplogger` to send the events to ESP.
- The `Storage_TP9100.esp` and `Storage_TP9400.esp` ESP event profiles specify the RAID events that ESP should register.

Refer to the *tp9100esptool User Guide*, publication number 007-4596-00*x*, for more information about how `tpmwatch` sends events to ESP.

Remote Support Capability

Remote support capability enables you to connect to the console software (with a Web browser) or directly to ESP (with the command line application) from a remote location. This capability enables you to control ESP from the remote location and provides SGI support personnel with a “virtual seat” on the system or systems on which they need to work.

Remote support capability is built into ESP. The only requirement is a communication channel (for example, a network connection) to the site.

Security Features

ESP implements the following security features to prevent unauthorized access to ESP, the data that ESP stores, and the system that is running ESP:

- ESP requires a login/password combination to access the Web server.
- ESP validates user permissions for the accounts that are assigned to execute actions.
- ESP does not permit actions to run as root.
- ESP implements ReverseDNS lookup for Web server and SGM connections.
- ESP uses HMAC-MD5 digital signatures for all data transfers to an SGM server.
- ESP disables login attempts after four unsuccessful attempts. (Users must wait several minutes before attempting to log in again.)
- ESP includes a command-line interface to enable users to use ESP without running the Web server on their system.
- ESP restricts database access to local transactions (external systems cannot directly access the ESP database).
- ESP limits information returned to SGI with the call-logging feature to event-specific information. (ESP does not transmit any customer proprietary information to SGI.)
- ESP can encrypt the e-mail notifications that it sends.

System Performance Impact of ESP

The `eventmond` and `espdbd` daemons that ESP uses are event-driven and consume CPU resources only when events occur. When ESP receives an event, the daemons use less than 2 milliseconds of CPU time to process the event and store it in the ESP database.

The `eventmond` daemon uses approximately 200 KB of memory to run; the `espdbd` daemon uses approximately 500 KB of memory to run. Most of this memory is used to store the system configuration data, so the daemons use more memory on larger systems than they do on smaller systems.

ESP disk utilization depends on the size of the system; larger systems require more disk space than smaller systems. (For example, a 64-processor system with 75 to 125 boards uses less than 30 MB of disk space.) Once a database uses at least 10 MB of disk space, you can use the `esparchive` utility to compress the database to 40 to 60 percent of its original size.

Accessing ESP

This chapter describes how to use the command line interface and Web-based interface to access ESP on your systems. It also describes how to configure single system management and system group management for your systems.

All ESP components are installed on your system by default when you load an operating system release or patch that contains ESP. ESP begins monitoring your system when the system is booted. You can access ESP by using the command line interface or Web-based interface.

Using the Command Line Interface

The command line interface includes three commands: `espconfig`, `espreport`, and `esplognote`. The `espconfig` command configures ESP. The `espreport` command generates and displays ESP reports. The `esplognote` command creates logbook entries.

`espconfig` has the following command line options:

```
system# espconfig -help
Information Commands
--------------------
espconfig -help [ <prototype> ]
espconfig -spec
espconfig -version

Group Configuration
-------------------------
espconfig -add group -name <new group name>
espconfig -delete group -name <group name>
espconfig -list group
espconfig -listmembers group -name <group name>
```

```
Event Configuration
-------------------
espconfig -show evtype {-tid <type id> |-td <type desc>  }
                       [-sgmclient <client alias>]
espconfig -list evtype [-cid <class id>|-cd <class desc>]
                       [-enable|-disable]
                       [-log|-nolog]
                       [-sgmclient <client alias>]
espconfig -add  evtype -td <type desc>
                       {-cid <class id>|-cd <class desc>}
                       [-throttle <value>]
                       [-enable|-disable]
                       [-log|-nolog]
                       [-acfreq <action frequency value>]
                       [-acid <action id>|-acd <action desc>]
                       [-pri <priority>] [-fac <facility>]
                       [-appname <app. name>] [-regexp <reg. expression>]
                       [-prfid <profile id> |-prfn <profile name>]
                       [-sgmclient <client alias>|-sysid <client system id >]
espconfig -update evtype -tid <type id> [-cid <class id>|-cd <class desc>]
                       [-sgmclient <client alias>|-sysid <client system id >]
                       [-td <type desc>]
                       [-throttle <value>]
                       [-enable|-disable]
                       [-log|-nolog]
                       [-acfreq <action frequency value>]
                       [-acid <action id> | -acd <action desc>|
                        -noacid <action id> | -noacd <action desc>]
                       [-pri <priority>] [-fac <facility>]
                       [-appname <app. name>] [-regexp <reg. expression>]
                       [-prfid <profile id> | -prfn <profile name> |
                        -noprfid <profile id> | -noprfn <profile name>]
espconfig -delete evtype {-tid <type id>|-td <type desc>}
                       [-sgmclient <client alias>|-sysid <client system id >]
espconfig -subscribe evtype [-cid <class id>|-cd <class desc>]
                       [-tid <type id>|-td <type desc>]
                       [-pri <priority>] [-fac <facility>]
                       [-appname <application name>]
                       [-sgmclient <client alias>|-sysid <client system id >]
espconfig -unsubscribe evtype [-cid <class id>|-cd <class desc>]
                       [-tid <type id>|-td <type desc>]
                       [-pri <priority>] [-fac <facility>]
                       [-appname <application name>]
                       [-sgmclient <client alias>|-sysid <client system id >]
```

```
espconfig -add evclass [-cid <class id>] -cd <class desc>
                       [-sgmclient <client alias>|-sysid <client system id >]
espconfig -update evclass -cid <class id> -cd <class desc>
                       [-sgmclient <client alias>|-sysid <client system id >]
espconfig -delete evclass {-cid <class id>|-cd <class desc>}
                       [-sgmclient <client alias>|-sysid <client system id >]
espconfig -list evclass

Event Action Configuration
--------------------------
espconfig -show evaction {-acid <action id>|-acd <action desc>}
espconfig -list evaction
espconfig -add  evaction -acd <action desc> -act <action string>
                       [-enable|-disable]
                       [-user <name>]
                       [-tout <timeout value>]
espconfig -update evaction {-acd  <action desc> | -acid <action id>}
                       [-act <action string>]
                       [-enable|-disable]
                       [-user <name>]
                       [-tout <timeout value>]

Exporting and Importing Environment
-----------------------------------
espconfig -add|-load|-merge   eventprofile <profile name>+|allprofiles
                 [-defaults] [-dontsubscribe]
                 [-sgmclient <client alias> | -sysid <system Id>]
espconfig -drop|-unload    eventprofile <profile name>+|allprofiles
                 [-sgmclient <client alias> | -sysid <system Id>]
espconfig -save|-refresh    eventprofile [-defaults] <profile name>+|allprofiles
                 [-sgmclient <client alias> | -sysid <system Id>]
espconfig -list    eventprofile
                 [-sgmclient <client alias> | -sysid <system Id>]
espconfig -showevents    eventprofile <profile name>+
                 [-sgmclient <client alias> | -sysid <system Id>]
espconfig -save    espenv [global][ipaddr][user][site|customer_profile][all] [-to <file
name>]
espconfig -load    espenv [-sysid <client system id >]
                [-chk <check definition file name>]
                -from <data definition file name>

IP Address Configuration
------------------------
espconfig -enable  ipaddr <IP address> ... <IP address>
espconfig -disable ipaddr <IP address> ... <IP address>
```

```
espconfig -delete  ipaddr <IP address> ... <IP address>
espconfig -list    ipaddr <IP address> ... <IP address> [-enabled|-disabled]

User and User Permission Configuration
--------------------------------------
espconfig -add     user  -name <user name> [-p <password>]
espconfig -delete  user  -name <user name> [-p <password>]
espconfig -update  user  -name <user name> [-p <new password>]
espconfig -list    user [-name <user name>]
espconfig -createadmin
espconfig -add     permdesc  -perm <permission name> -desc <permission description>
espconfig -delete  permdesc  -perm <permission name>
espconfig -list    permdesc  [-perm <permission name> .. <permission name>]
espconfig -add     userperm  [-name <user name>] -perm <permission name>
espconfig -delete  userperm  [-name <user name>][-perm <permission name>]
espconfig -list    userperm  [-name <user name>][-perm <permission name>]

ESP Archive Management
----------------------
espconfig -list    archive  [<archive name> .. <archive name>]
espconfig -drop    archive  <archive name>

ESP Customer Profile Configuration
----------------------------------
espconfig -create  customer_profile
              -fname <first name>
              -lname <last name>
              -phone <phone number>
              -email <email address>
              [-street1 <street address (line 1)>]
              [-street2 <street address (line 2)>]
              [-street3 <street address (line 3)>]
              [-city <city name>]
              [-state <state or province>]
              [-post <postal/zip code>]
              -country <country>
              [-site_id <site id>]
              [-host <host name>|-alias <client alias>|-sysid <system id>]
```

```
espconfig -update  customer_profile
              [-fname <first name>]
              [-lname <last name>]
              [-phone <phone number>]
              [-email <email address>]
              [-street1 <street address (line 1)>]
              [-street2 <street address (line 2)>]
              [-street3 <street address (line 3)>]
              [-city <city name>]
              [-state <state or province>]
              [-post <postal/zip code>]
              [-country <country>]
              [-site_id <site id>]
              [-host <host name>|-alias <client alias>|-sysid <system id>]
espconfig -show    customer_profile
              [-host <host name>|-alias <client alias>|-sysid <system id>]

Global Configuration
--------------------
espconfig -enable  call_logging [-text|-comp_encoded]
                       [-sgmclient <client alias> |-sysid <system id>]
espconfig -enable  {event_registration
                   |event_throttling
                   |event_actions
                   |shutdown_reason}
                   [-sgmclient <client alias> |-sysid <system id>]
espconfig -enable  mail -from <email address>
                   [-email1 <email address>]
                   [-email2 <email address>]
espconfig -disable {call_logging
                   |event_registration
                   |event_throttling
                   |event_actions
                   |shutdown_reason}
                   [-sgmclient <client alias> |-sysid <system id>]
espconfig -show {call_logging
                   |event_registration
                   |event_throttling
                   |event_actions
                   |shutdown_reason}
                   [-sgmclient <client alias> |-sysid <system id>]
espconfig -show mail
espconfig -flushdb [-sysid <system id>|-host <host name>]
                   [config|all]
```

```
espconfig -reconstructdb

Performance and System Monitoring  Configuration
-----------------------------------------------
espconfig -on performance
          -off performance
          -list performance [-status|-enable|-disable]
          -enable performance -pd {all|<pmie rule description>}
          -disable performance -pd {all|<pmie rule description}>
espconfig monitor -list     <service name>
          monitor -show     <service name>  [-sgmclient <client alias>]
          monitor -enable   <service name>  [-sgmclient <client alias> ]
          monitor -disable  <service name>  [-sgmclient <client alias> ]

SGM Related Commands
--------------------
espconfig -show systems
espconfig -show sgmclients
espconfig -show sgmservers
espconfig -show system
             -host <host name>|-sgmclient <client alias>|-sysid <system id>
espconfig -set system -host <host name>|-sysid <system id>
                        [-alias <new alias>]
                   [-group <group name> | -gid <group id> ]
espconfig -setnode system -sgmnode|-fullnode
espconfig -check system -sgmlicense|-update
espconfig -add  sgmclient -alias <client alias> -host <client hostname>
             [-path <client reach path>]
             [-group <group descr.>|-gid <group id>]
             [-v2|-v3] [-p <password>]
espconfig -subscribe  sgmclient
             -host <host name>|-alias <client alias>|-sysid <system id>
             [-loadprofiles] [-refreshprofiles] [-lightnode|-fullnode] ] [-force]
espconfig -unsubscribe  sgmclient
             -host <host name>|-alias <client alias>|-sysid <system id>
             [-force]
espconfig -update  sgmclient
             -host <host name>|-alias <client alias>|-sysid <system id>
              [-p <password>] [-path <new path>] [-lightnode|-fullnode]
espconfig -delete  sgmclient
             -host <host name>|-alias <client alias>|-sysid <system id>
espconfig ping
             -sgmclient <client alias>|-sysid <system id>|-path <reach path>
             [-espver]
espconfig -add sgmserver -host <SGM host name> -p <communication password>
```

```
espconfig -update sgmkey -host <host name> -p <comm. password> [-pid <key ID>]
```

Refer to Chapter 3, "Administering ESP," Chapter 4, "Setting Up the ESP Environment," and Chapter 5, "Configuring ESP," for more information about using the `espconfig` command.

`espreport` has the following command line options:

```
system# espreport -help
Information Commands
--------------------
espreport -help [ <prototype> ]
espreport -spec
espreport -version

Report Commands
--------------------
espreport availability [-sysid <system id>|-host <host name>]
                       [-from mm/dd/yyyy] [-to mm/dd/yyyy]
espreport action_taken [-sysid <system id>|-host <host name>]
                       [-from mm/dd/yyyy] [-to mm/dd/yyyy]
espreport events       [-sysid <system id>|-host <host name>]
                       [-from mm/dd/yyyy] [-to mm/dd/yyyy]
                       [-tid <type id>  |-td <type desc>]
                       [-cid <class id> |-cd <class desc>]
espreport hwchanges    [-sysid <system id>|-host <host name>]
                       [-from mm/dd/yyyy] [-to mm/dd/yyyy]
espreport swchanges    [-sysid <system id>|-host <host name>]
                       [-from mm/dd/yyyy] [-to mm/dd/yyyy]
espreport logbook      [-sysid <system id>|-host <host name>]
                       [-from mm/dd/yyyy] [-to mm/dd/yyyy]
espreport summary      [-sysid <system id>|-host <host name>]
                       [-from mm/dd/yyyy] [-to mm/dd/yyyy]
espreport sysinfo      [-sysid <system id>|-host <host name>]
                       [all]
```

Refer to Chapter 6, "Viewing Reports," for more information about using the `espreport` command.

`esplognote` does not have any command line options:

```
system# esplognote
```

Refer to Chapter 7, "Using the ESP Logbook," for more information about using the `esplognote` command.

Using the Web-based Interface

The Web-based interface provides a graphical interface that you can use to access ESP. You can access the Web-based interface via one of the following URLs:

- `http://localhost:5554`
- `http://<systemname>:5554`

Table 2-1 lists error messages that might appear when you attempt to start the Web-based interface. It also lists the cause of each message and the actions you should perform to correct the problems that caused the error messages.

Table 2-1 ESP Startup Error Messages

Error Message	Cause	Solution
`There was no response. The server could be down or is not responding.`	The ESP Web server is not running on the system or the system is down.	Verify that the system is running. Reboot the system, if necessary. Verify that the ESP Web server (`esphttpd`) is running on the system. Restart the ESP Web server if it is not running. If the `esphttpd` server is not running, verify that ESP is chkconfig'ed on.

`Forbidden Request`
 	
`The current request was forbidden. Please check your permissions.`
	Your system does not have permission to access the ESP Web server.	Add your system to the "allow access" list or remove it from the "restrict access" list. (Refer to "Setting Up the Network Permissions" on page 56.)

Table 2-1 ESP Startup Error Messages **(continued)**

Error Message	Cause	Solution

`Forbidden Request`
 	
`The current request was forbidden. Please check your permissions.`
 	
`Unable to verify that the host name matches the address.`
 	
`This may be a transient problem or a botched name server setup.`
	Reverse DNS lookup failed because ESP was not able to verify that your system IP address and hostname matched. Reverse DNS lookup fails if an IP address is "faked" or if the DNS server used by the ESP Web server is not working correctly.	If the DNS server on the system is not working correctly, perform the following actions to disable reverse DNS lookup:
		
		1. Add the following line to the Web server configuration file (`/etc/esphttpd.conf`):
		
		`ReverseDNSLookup : off`
		
		2. Enter the following command to kill the current Web server process:
		
		`killall esphttpd`
		
		3. Restart the `esphttpd` process.
		
		Warning: Disabling the reverse DNS lookup feature increases the possibility of security problems.

`Authorization failed. Retry?`	The username and password that you entered are not valid.	Enter a valid username and password. If you forget your username and password, enter **`espconfig -update user -name <username>`**. ESP will prompt you for a new password.

`Forbidden Request`
 	
`The current request was forbidden. Please check your permissions.`
 	
`Connection was rejected since number of authorization attempts was reached.`
 	
`Please try to connect later.`
	You did not enter a valid username/password combination within four attempts. When this happens, the ESP Web server prevents login attempts for two minutes.	Wait for two minutes and log in with a valid username/password combination.

Accessing the Web-based Interface

Perform the following procedure to access the ESP Web-based graphical interface:

1. If this is the first time that you are using ESP on the system, do the following:
   - Log into the system as root and enter **`espconfig -createadmin`** to create the default user account (administrator).
   - Enter **`espconfig -enable ipaddr 127.0.0.0`** and **`espconfig -enable ipaddr 127.0.0.1`** to enable access to ESP from the local system.
2. Open the appropriate URL (`http://locahost:5554` or `http://`*<systemname>*`:5554`) in a Web browser.

   The Web browser displays the ESP opening page. (Refer to Figure 2-1.)

Figure 2-1 ESP Opening Page

3. Specify the system that you want to access:
   - To connect to the local system, click on the `login` button.
   - To connect to a remote system, enter the system name or IP address in the `hostname` box, and click on the `login` button.
4. Enter a username and password. (Refer to Figure 2-2.)

   The default username is *administrator*; the default password is *partner*.

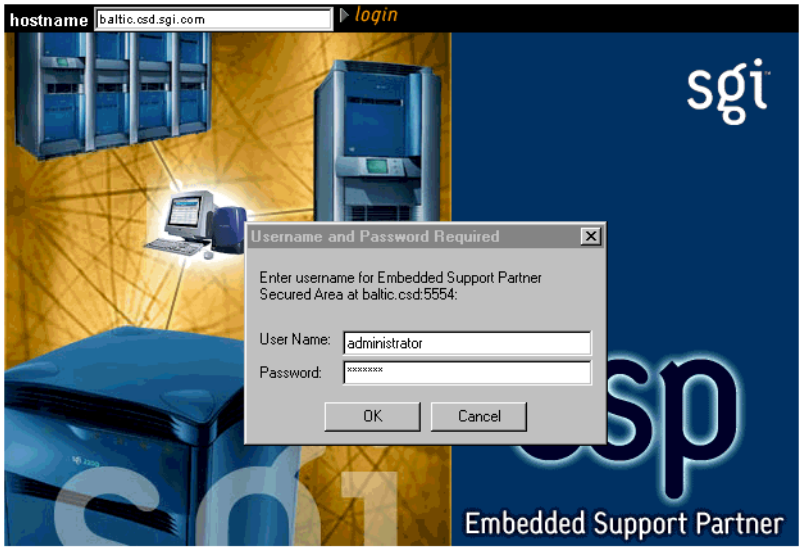


Figure 2-2 Entering a Username and Password

The ESP main page appears. (Figure 2-3 shows the main page in single system manager mode. Figure 2-4 shows the main page in system group manager mode.) The main page shows the current system and ESP configuration information and provides buttons that link to the main ESP functions.

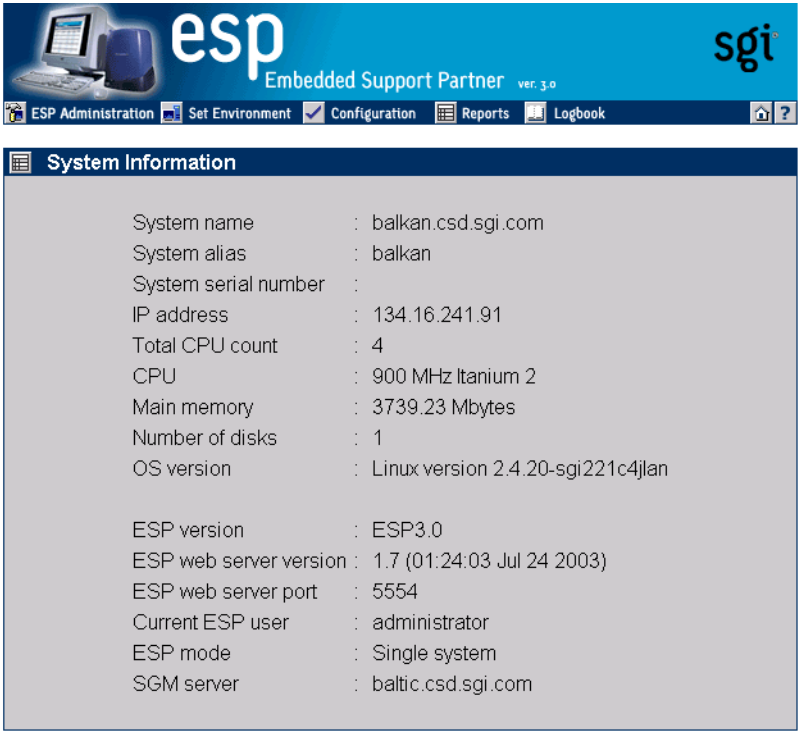


Figure 2-3 ESP Main Page (Single System Manager Mode)

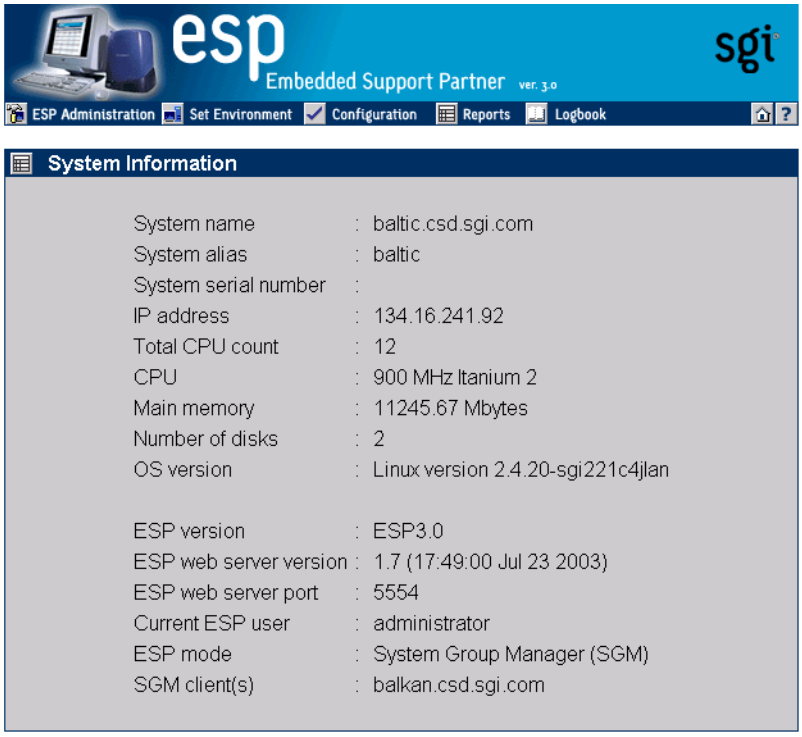


Figure 2-4 ESP Main Page (System Group Manager Mode)

Configuring Single System Management

Perform the following procedure the first time that you use single system manager mode to configure it:

1. Log into the system as root and enter **`espconfig -createadmin`** to create the default user account (administrator).
2. Enter **`espconfig -enable ipaddr 127.0.0.0`** and **`espconfig -enable ipaddr 127.0.0.1`** to enable access to the ESP from the local system.
3. Open the following URL in a Web browser: `http://localhost:5554`

   (Refer to "Using the Web-based Interface" on page 42.)
4. Change the default password to prevent unauthorized access to your system. (Refer to "Updating a Password" on page 65.)
   - The default user name is `administrator`.
   - The default password is `partner`.
5. Set up any user accounts and permissions that you want on your system. (Refer to "Setting Up the User Permissions" on page 59.)
6. Set up the access lists to allow systems to connect to the Configurable Web Server that ESP uses. By default, the Configurable Web Server is configured to refuse connections from all other IP addresses. (Refer to "Setting Up the Network Permissions" on page 56.)
7. Enter the system serial number. (Refer to "Setting Up the System Serial Number (Linux OS Only)" on page 78.)
8. Enter the customer profile information. (Refer to "Setting Up the Customer Profile" on page 52.)
9. Set up the global configuration parameters. (Refer to "Setting Up the Global Configuration Parameters" on page 83.)
10. Modify and/or add actions. (Refer to "Configuring Actions" on page 159.)
11. Modify and/or add events. (Refer to "Configuring Events" on page 111.)

Configuring Group Management

All ESP components necessary for group management are installed on your system by default; however, you need a nodelocked license to enable the system group management (SGM) functionality. You must configure a system to use system group manager (SGM) mode to use the group management functions in ESP.

If you want one system to register events from other systems in a group and perform actions for those events, you must subscribe to those events on the remote systems. When the ESP software on a remote system registers subscribed events, it logs them in its database (if it is a full node; light nodes do not maintain a database), performs any actions assigned to the events, and then forwards the events to the ESP software on the group manager system. Then, the ESP software on the group manager system registers the events, logs the events in its database, and performs any actions assigned to the events. This process creates a central repository of data on the group manager system, which enables you to access information about all of the systems in the group from a single interface.

Be aware of the following requirements as you configure group management:

- Although you can subscribe to any events that are recognized on group member systems, the systems forward only the events that have event registration enabled. (Globally disabling event registration on a group member system disables event forwarding for all events on that system. Disabling an individual event registration on a group member prevents the group member system from forwarding that event to the group manager system.)
- Event forwarding is an internal ESP action, so you must enable ESP actions on group member systems to forward events to the group manager system.
- On a group manager system, ESP stores event settings on a per-host basis. There are separate sets of events for each member of the group. Disabling global or individual event registration on the group manager does not propagate to the group members systems: if a group member attempts to deliver an event that is disabled on the group manager, the event is delivered to the group manager and then the event is discarded. If you no longer need an event from a member system, you should unsubscribe the event rather than disable it on the group manager system. This reduces the overhead caused by unnecessary event delivery.

Perform the following procedure to configure group management:

1. Select the group of systems that you want to monitor. (These systems are called the "group members" or "SGM clients.")

   Each system in a group can be monitored by more then one group manager. Each group manager has an independent set of events that it monitors.

   For the initial release of ESP 3.0, the SGM server and clients must be running the same version of ESP.

2. Select the system that you want to be the group manager. (This system is called the "group manager" or "SGM server.")

   The group manager system can also be a group member for another group manager. In that case, the other group manager treats the system as a single system.

3. Configure the group manager system in SGM mode. (Refer to "Setting Up the System Parameters (Single System Manager Mode Only)" on page 91.)

4. Configure the ESP single system manager on each system in the group. (Refer to "Configuring Single System Management" on page 48.)

   Note: Be sure to enable event registration on the group member system for all events that you want to subscribe.

5. Add the SGM clients on the SGM server. (Refer to "Adding a New SGM Client" on page 93.)

   Note: For greater security, configure an authentication password on the SGM server and clients. You must configure the password on an SGM client first (refer to "Adding a Password for a New Server" on page 106) and then on the SGM server (refer to"Adding a New SGM Client" on page 93 and "Updating the System or a Client" on page 97).

6. Subscribe to the events that you want to receive from the SGM Clients. (Refer to "Subscribing Events from SGM Clients" on page 155.)

Administering ESP

This chapter describes how to administer ESP on your system. ESP administration includes the following components:

- Customer profile
- Network permissions
- User permissions
- Database archives

You must set up the administration components when you first configure ESP on a system. After that, modify specific parameters as needed (for example, add or delete users).

Setting Up the Customer Profile

Customer profiles provide contact information for a system/site. If the service contract for your site includes automatic call logging, ESP sends the name, telephone number, and e-mail address of the contact person to the call logging tool at SGI.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to set up the customer profile for a system:

1. Click on the `ESP Administration` button.

   Note: If the system is an SGM server, choose the system for which you want to set up the customer profile and click on the `Continue` button. (Refer to Figure 3-1.)

   The interface displays the `Create Customer Profile` window. (Refer to Figure 3-2.)

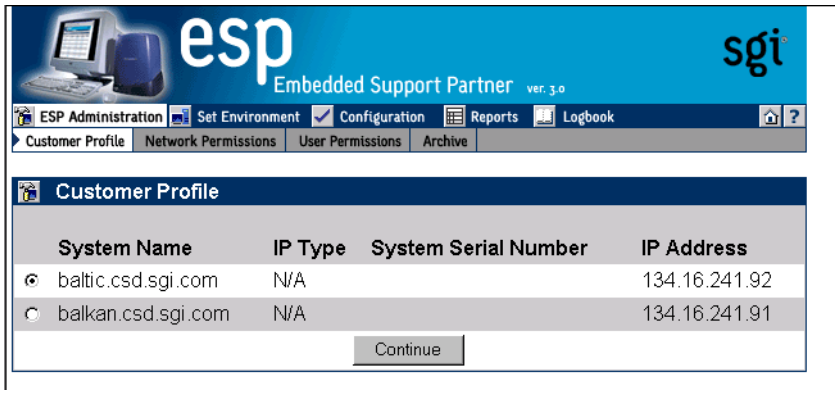


Figure 3-1 Choosing the System to Update the Customer Profile

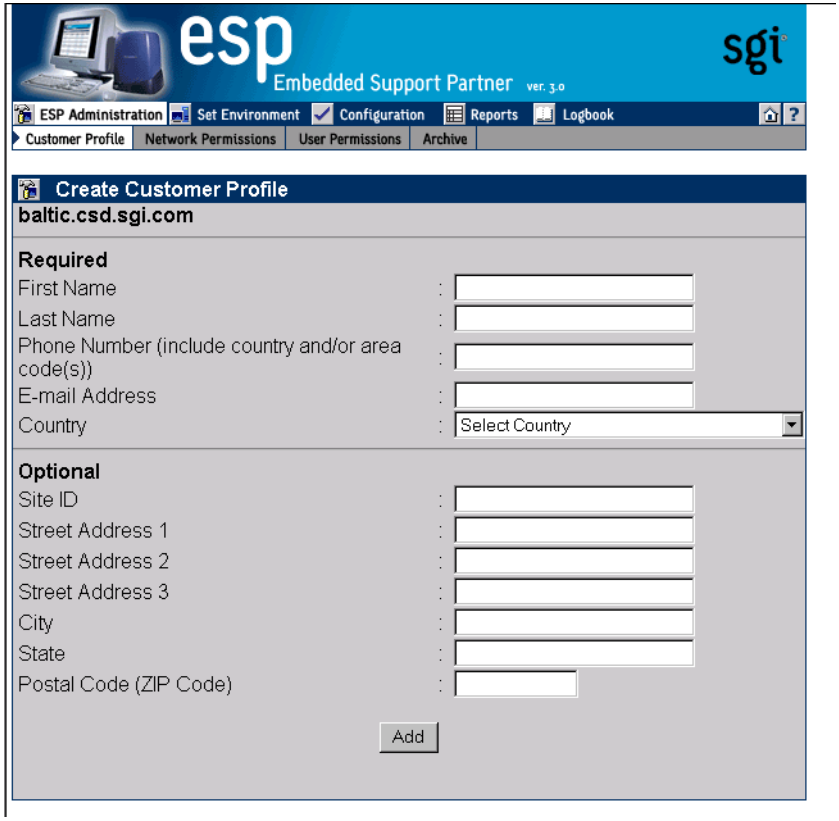


Figure 3-2 Update Customer Profile Window (Web-based Interface)

2. Update the customer profile parameters. (Table 3-1 describes the parameters.)

Table 3-1 Customer Profile Parameters

Parameter	Description
Required Parameters[a]	
`First Name`	First name of the site contact person
`Last Name`	Last name of the site contact person
`Phone Number`	Phone number of the site contact person (include only numbers and dashes; for example: 1-715-123-4567)

Table 3-1 Customer Profile Parameters **(continued)**

Parameter	Description
E-mail Address	E-mail address of the site contact person (ESP sends a copy of any automated e-mail messages to this address)
Country	Country where the site is located
Optional Parameters[b]	
Site ID	Identification number for the site
Street Address 1 Street Address 2 Street Address 3	Street address for the site
City	City where the site is located
State	State where the site is located
Postal Code (Zip Code)	Postal code or zip code of the site location

a. Information in the required fields is necessary to enable automatic call logging. If this information is not provided, automatic call logging is disabled.

b. Although these fields are optional, it is recommended that you provide this information

3. Click on the Add button.

Using the Command Line Interface

You can use the `espconfig` command to view, set up, or modify the customer profile from the command line interface:

- Use the following command syntax to view the current customer profile:

```
/usr/sbin/espconfig -show customer_profile
 [-host <host name>|-alias <client alias>|-sysid <systemid>]
```

- Use the following command syntax to set up the initial customer profile:

```
/usr/sbin/espconfig -create customer_profile
  [-fname   <first name>]
  [-lname   <last name>]
  [-phone   <phone>]
  [-email   <email>]
  [-street1 <street address line1>]
  [-street2 <street address line2>]
  [-street3 <street address line3>]
  [-city    <city>]
  [-state   <state/province>]
  [-post    <postal code>]
  [-country <country>]
  [-site_id <site id>]
 [-host <host name>|-alias <client alias>|-sysid <systemid>]
```

- Use the following command syntax to update an existing customer profile:

```
/usr/sbin/espconfig -update customer_profile
  [-fname   <first name>]
  [-lname   <last name>]
  [-phone   <phone>]
  [-email   <email>]
  [-street1 <street address line1>]
  [-street2 <street address line2>]
  [-street3 <street address line3>]
  [-city    <city>]
  [-state   <state/province>]
  [-post    <postal code>]
  [-country <country>]
  [-site_id <site id>]
 [-host <host name>|-alias <client alias>|-sysid <systemid>]
```

Setting Up the Network Permissions

Network permissions enable you to specify which systems can access the Web server that ESP uses. These permissions provide a layer of security to prevent unauthorized systems from accessing ESP data from your systems.

If you want to restrict access to ESP, you must set up a "restrict access" list and an "allow access" list. (If you do not set up a "restrict access" list, all IP addresses can connect to ESP regardless of the "allow access" list settings because the default configuration allows connections from all IP addresses if no "restrict access" list exists.)

The most secure configuration is to set the "restrict access" list to all hosts (*.*.*.*) and set the "allow access" list to the hosts that you want to have access to ESP. (For example, set the "allow access" list to `197.*.*.*` and the "restrict access" list to `*.*.*.*` if you want only the systems that have IP addresses that begin with 197 to have access to ESP.)

Caution: All changes that you make to the "restrict access" and "allow access" lists immediately take effect. Ensure that you do not set up access lists that prevent your administration system from connecting to ESP.

By default, the "restrict access" list is set to *.*.*.* to restrict all hosts. You must enable access by the local host (127.0.0.0 and 127.0.0.1) before you can access the ESP Web server. To do this, enter the **`espconfig -enable ipaddr 127.0.0.0`** and **`espconfig -enable ipaddr 127.0.0.1`** commands before you attempt to access ESP on a system for the first time.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to set up network permissions:

1. Click on the `ESP Administration` button.
2. Click on the `Network Permissions` button.

   The interface displays the `Network Permissions` window. (Refer to Figure 3-3.)

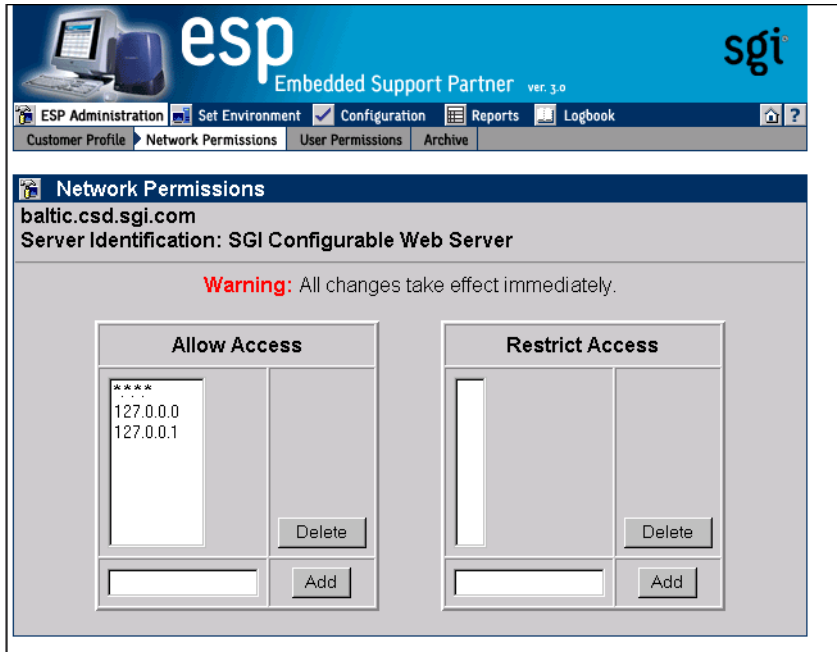


Figure 3-3 Network Permissions Window (Web-based Interface)

3. To modify the `Allow Access` list:
   - To add an address, enter the IP address or IP address mask (using * as a wild card for one or more values in the address) in the box, and click on the `Add` button.
   - To delete an address, click on the address in the `Allow Access` list, and click on the `Delete` button.
4. To modify the `Restrict Access` list:
   - To add an address, enter the IP address or IP address mask (using * as a wild card for one or more values in the address) in the box, and click on the `Add` button.
   - To delete an address, click on the address in the `Restrict Access` list, and click on the `Delete` button.

Using the Command Line Interface

You can use the `espconfig` command to set up the network permissions from the command line interface:

Tip: Use an asterisk as a wild card character in any of the IP addresses that you enter for the `<ip address>` parameter (for example, 123.23.2.*, 123.255.*.*, and *.*.*.*).

- Use the following command syntax to enable IP addresses to access the ESP Web server:

  ```
  /usr/sbin/espconfig -enable ipaddr <ip address> ... <ip address>
  ```

  You must specify at least one IP address. If you specify an IP address that is already enabled, it remains enabled. If you specify an IP address that is disabled, ESP moves it from the "restrict access" list to the "allow access" list to enable it for Web server access. If you specify a new IP address, ESP adds it to the "allow access" list to enable it for access to the Web server.

- Use the following command syntax to restrict IP addresses from accessing the ESP Web server:

  ```
  /usr/sbin/espconfig -disable ipaddr <ip address> ...<ip address>
  ```

  You must specify at least one IP address. If you specify an IP address that is disabled, it remains disabled. If you specify an address that was enabled for Web server access, ESP moves it from the "allow access" list to the "restrict access" list to prevent it from accessing the Web server. If you specify a new IP address, ESP adds it to the "restrict access" list to prevent it from accessing the Web server.

- Use the following command syntax to delete IP addresses from the access lists on the system:

  ```
  /usr/sbin/espconfig -delete ipaddr <ip address> ...<ip address>
  ```

  You must specify at least one IP address.

- Use the following command syntax to list the IP addresses that are contained in the access lists on the system and the current state of the IP addresses:

  ```
  /usr/sbin/espconfig -list ipaddr <ip address>...<ip address>
  [-enabled | -disabled]
  ```

  If you do not specify an IP address, this command lists all IP addresses in the access lists on the system. If you specify the `-enabled` option, this command lists only the IP addresses that are in the "allow access" list. If you specify the `-disabled` option, this command lists only the IP addresses that are included in the "restrict access" list.

Setting Up the User Permissions

User permissions provide an additional security layer by enabling you to create individual user accounts within ESP. Each user account can have access to different areas of ESP (for example, one account could have access only to availability reports and a second account could have access to all reports).

ESP contains one user account by default (login: `administrator`; password: `partner`). The administrator account has full access to all ESP features.

Note: This is no direct correlation between ESP user accounts and "normal" user accounts on a system.

Viewing the Current Users

You can view a list of all ESP user accounts that are currently available.

Using the Web-based Interface

1. Click on the `ESP Administration` button.
2. Click on the `User Permissions` button.

   The interface shows the list of current users. (Refer to Figure 3-4.)

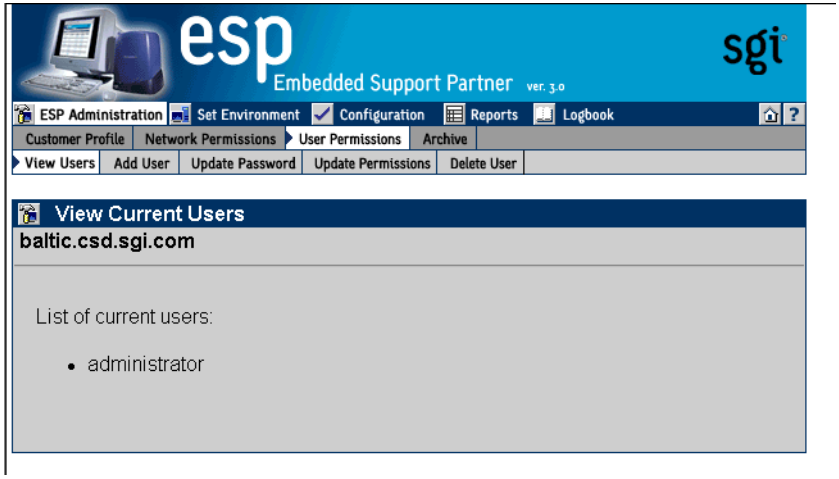


Figure 3-4 Current User List (Web-based Interface)

Using the Command Line Interface

Use the following syntax of the `espconfig` command to view a list of current users:

```
/usr/sbin/espconfig -list user [-name <username>]
```

If you include the `-name` option, this command displays information about a specific user. If you do not include the `-name` option, this command lists all users.

Adding a User

Any user with the "ESP Administration and Set Environment" permission can add new users and configure access permissions for them.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to add a user:

1. Click on the `ESP Administration` button.
2. Click on the `User Permissions` button.
3. Click on the `Add User` button.

   The interface displays the `Add User` window. (Refer to Figure 3-5.)

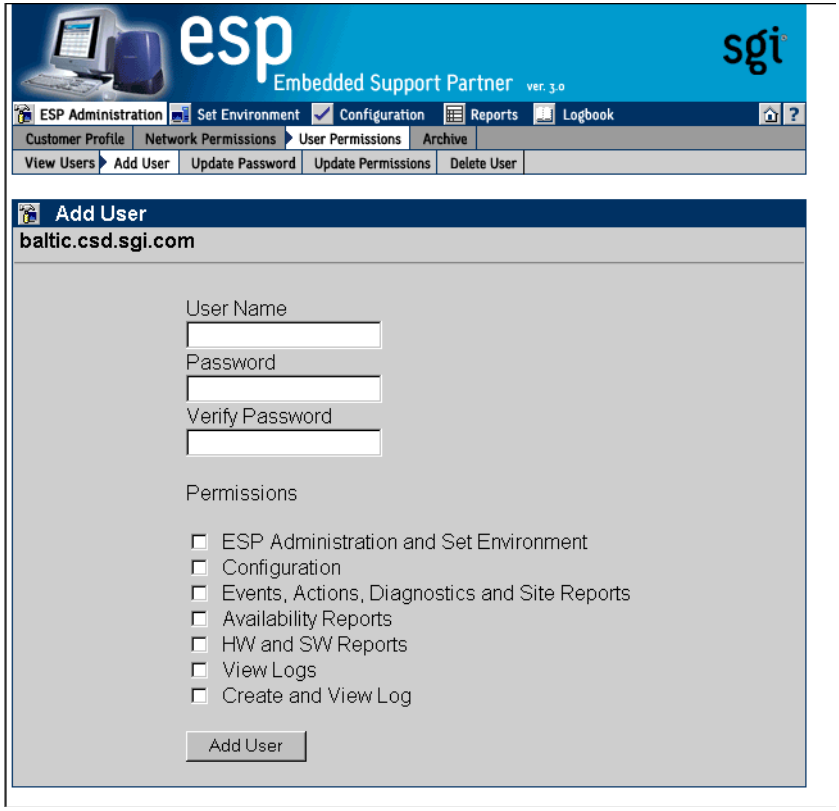


Figure 3-5 Add User Window (Web-based Interface)

4. Enter the login name for the user in the `User Name` field.

   User names have the following restrictions:

   - User names are case sensitive; for example, User is different than USer.
   - User names cannot be more than 126 characters.
   - User names cannot include the following characters: ? & * “ < > %

5. Enter the password for the user in the `Password` field.

   Passwords have the following restrictions:

   - Passwords are case sensitive; for example, Password is different than PAssword.
   - Passwords cannot be more than 126 characters.
   - Passwords cannot include the following characters: ? & * “ < > % <SPACE> <Tab>

6. Re-enter the password for the user in the `Verify Password` field. (You must enter the password twice to ensure that it is entered correctly.)
7. Set the permissions for the user. (Table 3-2 describes the permissions.)

Table 3-2 Available User Permissions

Permission	Description
`ESP Administration and Set Environment`	Enables the user to perform all activities in the `ESP Administration` and `Set Environment` sections of the interface (set up customer profile, network permissions, user permissions, global configuration, paging parameters, archive settings, and SGM settings)
`Configuration`	Enables the user to perform all activities in the `Configuration` section of the interface (configure events, actions, performance monitoring, and system monitoring)
`Events, Actions, Diagnostics and Site Reports`	Enables the user to view all event reports, action reports, diagnostic reports, and site reports
`Availability Reports`	Enables the user to view availability reports
`HW and SW Reports`	Enables the user to view hardware inventory reports, software inventory reports, and system reports
`View Logs`	Enables the user to view logbook entries
`Create Log`	Enables the user to create logbook entries

8. Click on the `Add User` button.

Using the Command Line Interface

Use the following syntax of the `espconfig` command to add a new user:

```
/usr/sbin/espconfig -add user -name <username> [-p <password>]
```

User names have the following restrictions:

- User names are case sensitive; for example, User is different than USer.
- User names cannot be more than 126 characters.
- User names cannot include the following characters: ? & * “ < > %

Passwords have the following restrictions:

- Passwords are case sensitive; for example, Password is different than PAssword.
- Passwords cannot be more than 126 characters.
- Passwords cannot include the following characters: ? & * “ < > % <SPACE> <Tab>

Updating a Password

Any user with the "ESP Administration and Set Environment" permission can update user passwords. (You must know a user's current password to update their password. If a user forgets their password, delete their current user account and create a new account with the same user name.)

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to update a user password:

1. Click on the `ESP Administration` button.
2. Click on the `User Permissions` button.
3. Click on the `Update Password` button.

   The interface displays the `Update Password for User` window. (Refer to Figure 3-6.)

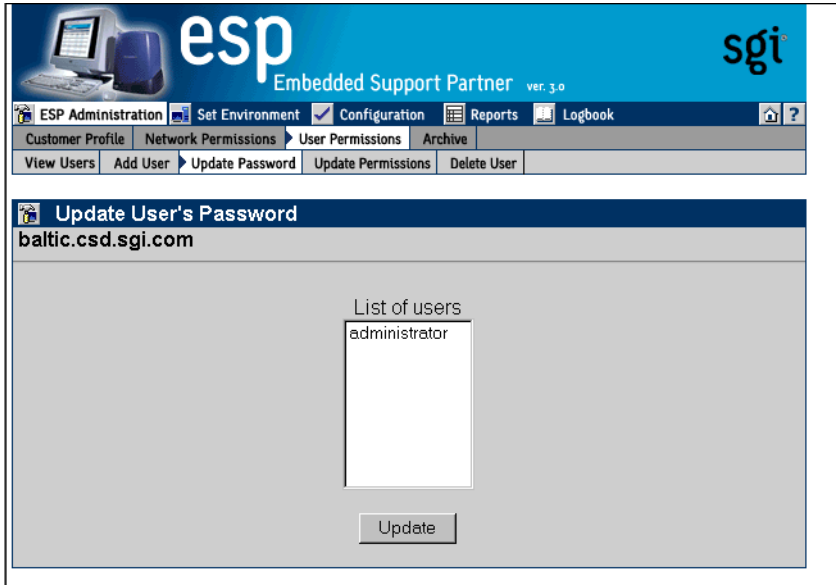


Figure 3-6 Update Password Window (Web-based Interface)

4. Select the user whose password you want to update.
5. Click on the `Update Password` button.

   The interface displays the `Add User` window. (Refer to Figure 3-5.)

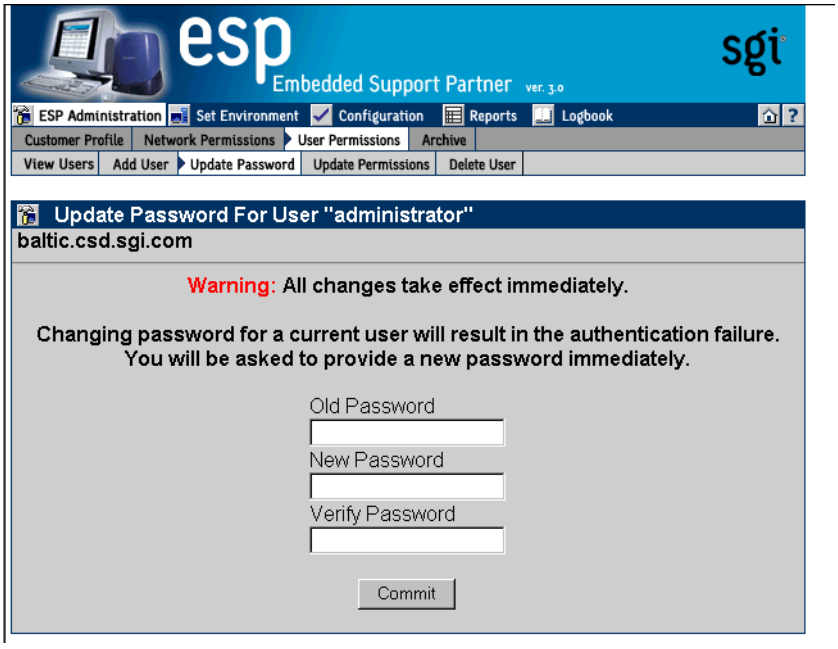


Figure 3-7 Update Password for User Window (Web-based Interface)

6. Enter the old password for the selected user in the `Old Password` field.
7. Enter the new password in the `New Password` field.

   Passwords have the following restrictions:

   - Passwords are case sensitive; for example, Password is different than PAssword.
   - Passwords cannot be more than 126 characters.
   - Passwords cannot include the following characters: ? & * “ < > % <SPACE> <Tab>

8. Re-enter the new password in the `Verify Password` field. (You must enter the password twice to ensure that it is entered correctly.)
9. Click on the `Commit` button.

Note: If you change the password for the account you are currently using, the interface displays an `Authorization Failed` message and prompts you for the new password.

Using the Command Line Interface

Use the following syntax of the `espconfig` command to update a password:

```
/usr/sbin/espconfig -update user -name <username> [-p <new_password>]
```

Passwords have the following restrictions:

- Passwords are case sensitive; for example, Password is different than PAssword.
- Passwords cannot be more than 126 characters.
- Passwords cannot include the following characters: ? & * “ < > % <SPACE> <Tab>

Updating Permissions for a User

Any user with "ESP Administration and Set Environment" permission can update permissions for other users. (Updating permissions enables you to add or remove specific permissions for a user.)

Note: If a user attempts to access a feature for which he/she does not have permission, the interface displays an `Authorization Failed` message and ESP does not perform the requested operation.

Caution: Do not change the permissions for the administrator account. The administrator account is the main ESP account and should always have full permissions.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to update permissions for a user:

1. Click on the `ESP Administration` button.
2. Click on the `User Permissions` button.
3. Click on the `Update Permissions` button.

   The interface displays the `Update User's Permissions` window. (Refer to Figure 3-8.)

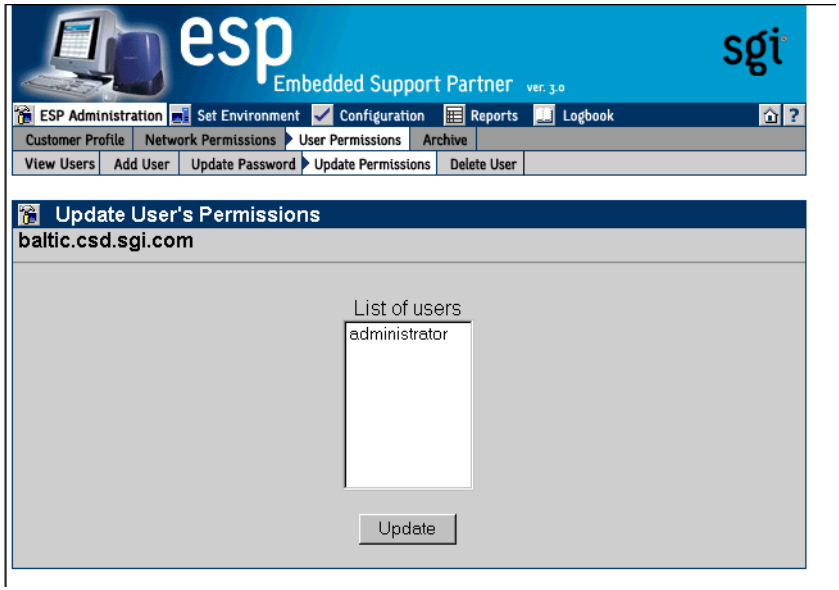


Figure 3-8 Update User's Permissions Window (Web-based Interface)

4. Select the user whose permissions you want to update.
5. Click on the `Update Permissions` button.

   The interface updates the `Update User's Permissions` window. (Refer to Figure 3-9.)

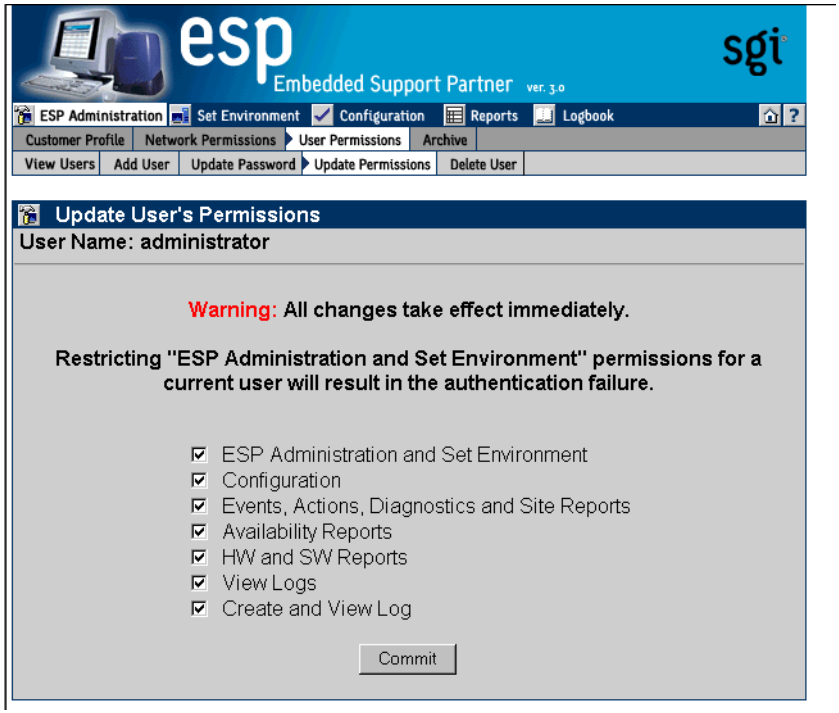


Figure 3-9 Updated Update User Permissions Window (Web-based Interface)

6. Select the permissions that you want the user to have. (Refer again to Table 3-2 on page 63 for descriptions of the permissions.)

   Note: Restricting the "ESP Administration and Set Environment" permission for the current user causes the interface to display an `Authorization Failed` message because the account no longer has access to the `Update Permissions` command.

7. Click on the `Commit` button.

Using the Command Line Interface

You can use the `espconfig` command to list the available permissions on a system and to list, add, or delete user permissions:

- Use the following command syntax to create the default user account and password:

  ```
  /usr/sbin/espconfig -createadmin
  ```

- Use the following command syntax to list the permissions that are available on a system:

  ```
  /usr/sbin/espconfig -list permdesc [-perm <permission
  name>..<permission name>]
  ```

  If you do not specify a specific permission name, this command displays all permissions that are available on the system.

- Use the following command syntax to add a new type of permission to a system:

  ```
  /usr/sbin/espconfig -add permdesc -perm <permission name> -desc
  <permission description>
  ```

- Use the following command syntax to delete a specific type of permission from a system:

  ```
  /usr/sbin/espconfig -delete permdesc -perm <permission name>
  ```

- Use the following command syntax to list permissions for a user:

  ```
  /usr/sbin/espconfig -list userperm [-name <user name>] [-perm
  <permission name>]
  ```

  If you do not specify a user name, this command lists all users. If you do not specify a permission name, this command lists all permissions. If you do not specify a user name or permission name, this command lists all permissions for all users.

- Use the following command syntax to add new permissions for a user:

  ```
  /usr/sbin/espconfig -add userperm [-name <user name>] -perm
  <permission name>
  ```

  Table 3-3 lists the settings for the `<permission name>` parameter.

Table 3-3 Command Line Interface User Permission Settings

Permission	Setting
ESP administration and set environment	`ESPpermission:set_environment`
Configuration	`ESPpermission:configuration`
Event registered, actions taken, diagnostic results, and site reports	`ESPpermission:events_actions_diag_reports`
Availability reports	`ESPpermission:availability_reports`
Hardware and software configuration reports	`ESPpermission:hw_sw_reports`
View logs	`ESPpermission:logbook_view`
Create log	`ESPpermission:logbook`

If you do not specify a user name, this command adds the permission to all users.

- Use the following command syntax to delete permissions from a user:

  ```
  /usr/sbin/espconfig -delete userperm [-name <user name>] [-perm
  <permission name>]
  ```

  If you do not specify a user name, this command deletes the specified permission from all users. If you do not specify a permission name, this command deletes all permissions from the specified user. If you do not specify a permission name or user name, this command deletes all permissions from all users.

Deleting a User

Any user with the "ESP Administration and Set Environment" permission can delete other ESP users. To ensure that security is not compromised, always delete users that no longer need access to ESP on a specific system.

Caution: Do not delete the administrator user account. All systems should have the administrator account.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to delete a user:

1. Click on the `ESP Administration` button.
2. Click on the `User Permissions` button.
3. Click on the `Delete User` button.

   The interface displays the `Delete User` window. (Refer to Figure 3-10.)

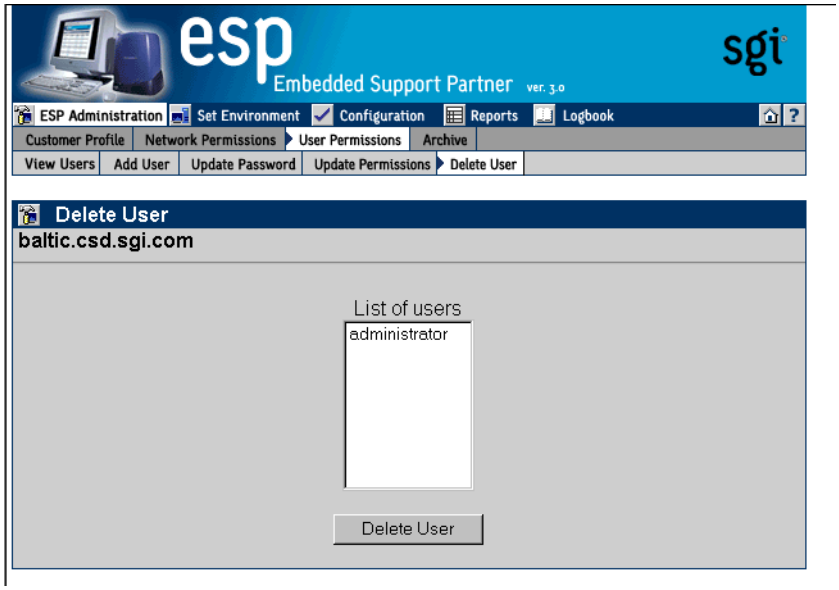


Figure 3-10 Delete User Window (Web-based Interface)

4. Select one or more user accounts to delete.
5. Click on the `Delete User` button.

   The interface updates the `Delete User` window. (Refer to Figure 3-11.)

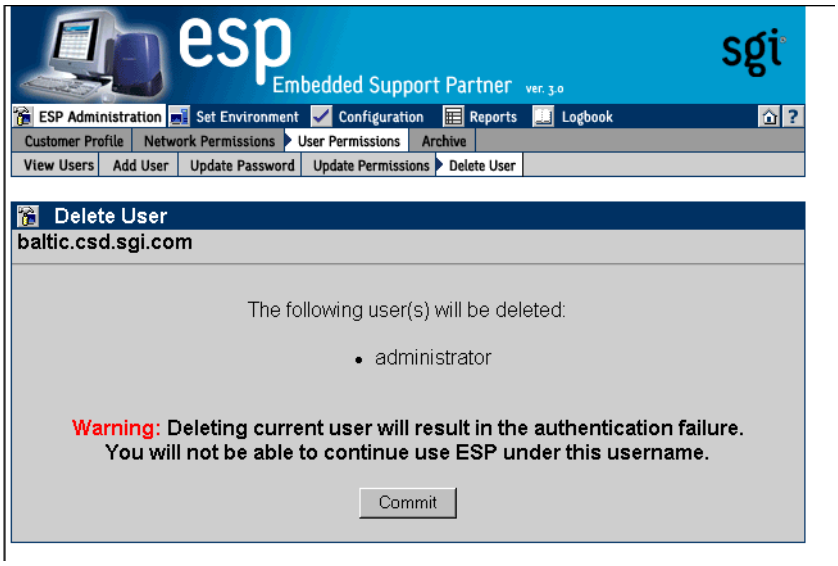


Figure 3-11 Updated Delete User Window (Web-based Interface)

6. Click on the `Commit` button.

Using the Command Line Interface

Use the following syntax of the `espconfig` command to delete a user:

```
espconfig -delete user -name <user name> [-p <user password>]
```

If you do not provide the password for the user account that you want to delete, this command prompts you for the password (but does not display the password on the screen).

Manipulating Database Archives

ESP logs data in a database on the system as it registers events and performs actions. You can archive the current database to reduce the amount of disk space used on the system.

Use the `esparchive` command at a UNIX prompt to archive the current database that ESP is using on a system. The `esparchive` command shuts down ESP momentarily, compresses the current database to save space, opens a new database to receive data from ESP, and restarts ESP. (You must use the root account to execute the `esparchive` command; this command archives the current database only if it is 10 MB or larger.)

You can use the Web-based interface and command line interface to delete database archives that you no longer need.

Warning: When you delete a database archive, the information in the database archive is permanently lost. You will not be able to view any system information that was stored in the database archive.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to delete a database archive:

1. Click on the `ESP Administration` button.
2. Click on the `Archive` button.

   The interface displays the `Delete Archive` window.
3. Click on the check box next to the name of the database archive that you want to delete.
4. Click on the `Delete Archive` button.

   The interface displays a verification screen.
5. Click on the `Commit` button.

Using the Command Line Interface

You can use the `espconfig` command to view information about the available database archives and to delete a specific database archive:

- Use the following command syntax to view the available database archives:

  ```
  /usr/sbin/espconfig -list archive [<archive name> ... <archive name>]
  ```

  This command displays the name and date information for archives. If you specify one or more archive names, this command lists information about those archives. If you do not specify an archive name, this command displays information about all of the archives on the system.

- Use the following command syntax to delete a database archive:

  ```
  /usr/sbin/espconfig -drop archive <archive name>
  ```

The `espconfig` command also enables you to initialize the ESP database on your system.

Warning: Initializing the ESP database on a system deletes all data for that system. If the system is a group manager, initializing the ESP database also deletes information about events on other systems in the group.

- Use the following command syntax to initialize the ESP database on your system to return it to the initial state:

  ```
  /usr/sbin/espconfig -reconstructdb
  ```

- Use the following command syntax to "clean" the ESP database tables on your system:

  ```
  /usr/sbin/espconfig -flushdb [-sysid <system id>|-host <hostname>] [config | all]
  ```

  Use the `-sysid` option to select a system by system ID. Use the `-host` option to select a system by hostname. If you do not specify the `-sysid` or `-host` option, this command "cleans" the database tables on the local system.

  If you do not specify the `config` or `all` option, this command "cleans" the ESP data tables on the selected system. If you specify the `config` option, this command "cleans" only the configuration tables for the local system. If you specify the `all` option, this command "cleans" the configuration tables and the ESP data tables on the selected system.

Setting Up the ESP Environment

This chapter describes how to set up the ESP environment on your system. The ESP environment includes the following components:

- System serial number (Linux OS only)
- Global configuration
- System/client parameters
- System Group Manager (SGM) password parameters

Note: The paging parameters are not included in the ESP 3.0 Web-based interface for the Linux OS. ESP 3.0 for the Linux OS does not include paging by default. SGI does not distribute the `QPage` application for the Linux OS. Paging capabilities are disabled when ESP 3.0 runs under the Linux OS. The ESP 3.0 graphical user interface for the Linux OS does not include the `Paging` menu. If you obtain the `QPage` application for the Linux OS from another source, you should manually install and configure it and then create an ESP action that calls the `QPage` application.

You must set up the environmental components when you first configure ESP on a system. After that, modify specific parameters only when the corresponding environmental component changes.

Setting Up the System Serial Number (Linux OS Only)

The `Linux System SN` button (refer to Figure 4-1) is available only on systems that run the Linux OS. This button enables you to enter the serial number of a system that is running the Linux OS. (ESP cannot automatically detect the system serial number of a system that is running the Linux OS.)

Figure 4-1 Linux System SN Button

The `Linux System SN` button appears under two conditions:

- A local system is running the Linux OS, and ESP cannot detect the system serial number.
- An SGM server has a subscribed client that is running the Linux OS and the system serial number was not detected or entered on the client before you subscribed the client to the SGM server.

Note: You cannot set the `Registration with SGI` global configuration parameter to `Enabled` until you set the system serial number.

On a local system, the `Linux System SN` button disappears after you enter the system serial number. On an SGM system, the `Linux System SN` button disappears after you enter the system serial number for each client system that does not have a system serial number set.

Setting the System Serial Number (Single System Manager Mode)

Perform the following procedure to set the system serial number in single system manager mode:

1. Click on the `Set Environment` button.
2. Click on the `Linux System SN` button.

   The interface displays the `Add Linux System Serial Number` window. (Refer to Figure 4-2.)

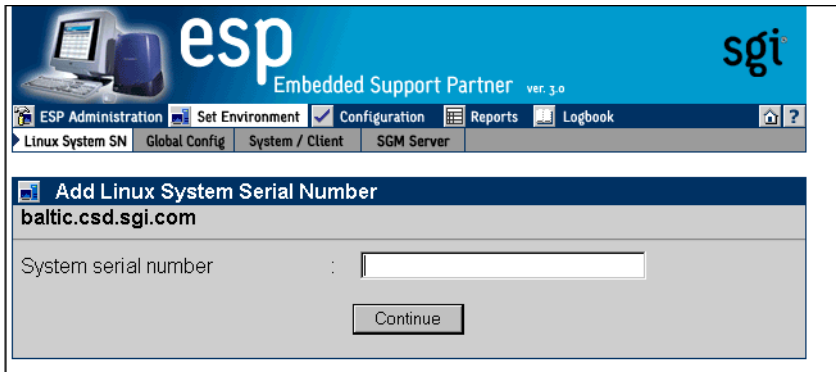


Figure 4-2 Add Linux System Serial Number Window (Single System Manager Mode)

3. Enter the system serial number in the `System serial number` field.
4. Click on the `Continue` button.

   The interface displays a verification window. (Refer to Figure 4-3.)

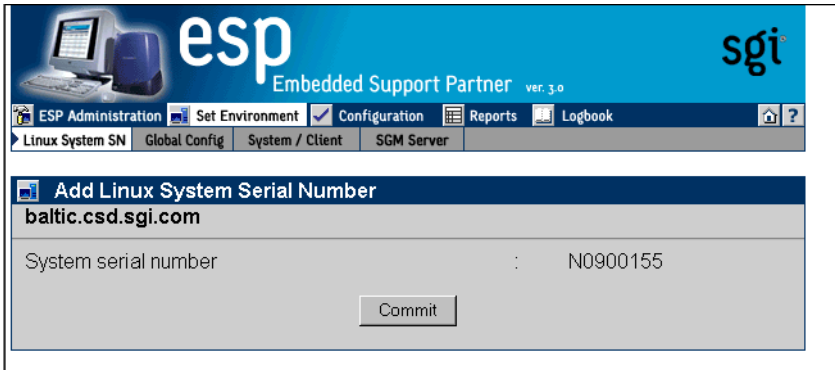


Figure 4-3 Add Linux System Serial Number Verification Window (Single System Manager Mode)

Tip: Verify that you correctly entered the serial number before you click on the `Commit` button. You cannot change the serial number once it has been submitted.

5. Click on the `Commit` button.

Setting the System Serial Number (System Group Manager Mode)

Perform the following procedure to set the system serial number in system group manager mode:

1. Click on the `Set Environment` button.
2. Click on the `Linux System SN` button.

   The interface displays the `Add Linux System Serial Number` window.

One SGM Client without a Serial Number Set

If there is only one SGM client without a serial number, enter the system serial number in the `System serial number` field, and click on the `Continue` button. (Refer to Figure 4-4.) Then, log into ESP on the SGM client, and set the serial number on that system. You must set the serial number on the SGM server and the SGM client.

Tip: Verify that you correctly entered the serial number before you click on the `Commit` button. You cannot change the serial number once it has been submitted.

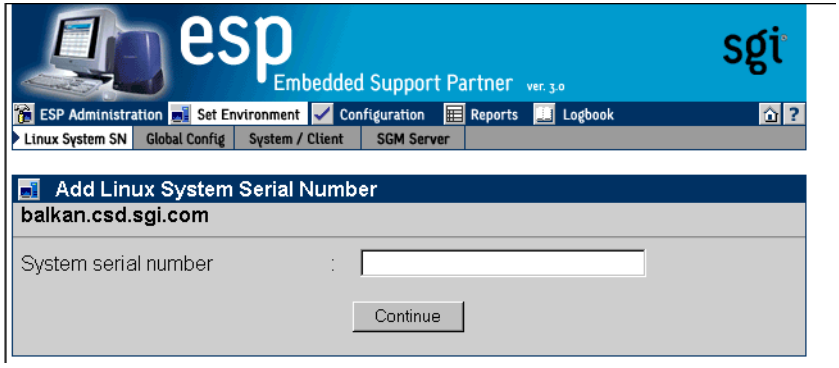


Figure 4-4 Linux System SN Window (SGM Server that has One Client without a Serial Number Entered)

Multiple Clients without a Serial Number Set

If there is more than one SGM client without a serial number, choose the correct system from the pulldown menu, enter the system serial number in the `System serial number` field, and click on the `Continue` button. (Refer to Figure 4-5.) Then, log into ESP on the SGM client, and set the serial number on that system. You must set the serial number on the SGM server and the SGM client.

Tip: Verify that you correctly entered the serial number before you click on the `Commit` button. You cannot change the serial number once it has been submitted.

Figure 4-5 Linux System SN Window (SGM Server that has Multiple Clients without Serial Numbers Entered)

Setting Up the Global Configuration Parameters

The global configuration parameters define global ESP behaviors and are divided into the following categories:

- Global event handling parameters, which determine if ESP should register events, throttle events, and perform any actions
- Global availability parameter, which determines if a reason must be supplied when the system is shutdown
- Global registration parameters, which determine if event information is returned to SGI, the format of the message that contains the event information, and any additional recipients of the message

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to set up the global configuration parameters:

1. Click on the `Set Environment` button.
2. Click on the `Global Config` button.

   Note: If the system is an SGM server, choose the system for which you want to update the global configuration parameters, and click on the `Continue` button. (Refer to Figure 4-6.)

   The interface displays the `Global Configuration` window. (Refer to Figure 4-7.)

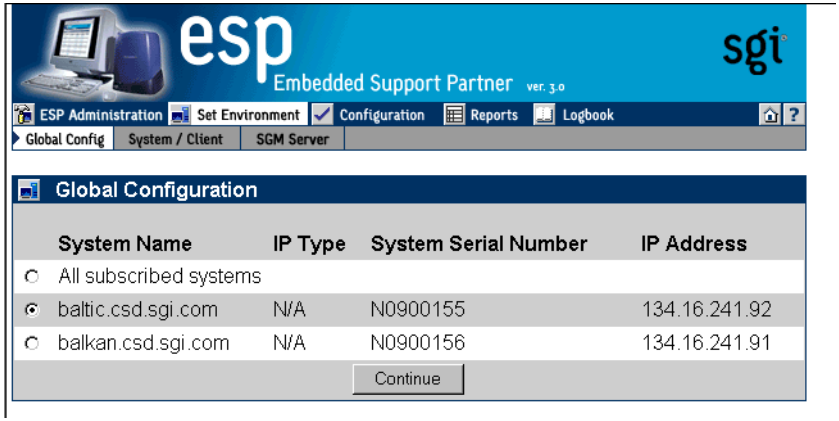


Figure 4-6 Choosing the System to Update the Global Parameters

Figure 4-7 Global Configuration Window (Web-based Interface)

3. Set the parameters. (Table 4-1 describes the global configuration parameters.)

Table 4-1 Global Configuration Parameters

Parameter	Description
`Register events`	Specifies whether or not ESP should register events in the ESP database Set this parameter to `Enabled` if you want to register event information in the ESP database on your system Set this parameter to `Disabled` if you do not want to register event information in the ESP database on your system (if you set this parameter to `Disabled`, it overrides the individual event settings) Recommendation: Always set this parameter to `Enabled` to capture all event information in the ESP database on your system
`Throttle events`	Specifies whether or not ESP should throttle events Set this parameter to `Enabled` to require that a specific number of events must occur before the event is registered in the ESP database on your system Set this parameter to `Disabled` to register every event in the ESP database Recommendation: Set this parameter to `Enabled` and configure the individual throttle values for each event
`Enable actions`	Specifies whether or not ESP should perform actions Set this parameter to `Enabled` to specify that ESP should perform any assigned actions in response to all events that occur Set this parameter to `Disabled` to specify that ESP should not perform actions for any events (if you set this parameter to `Disabled`, it overrides any action settings for individual events) Recommendation: Set this parameter to `Enabled` and assign the desired actions for each event

Table 4-1 Global Configuration Parameters **(continued)**

Parameter	Description
`Shutdown reason`	Specifies whether or not users will be prompted to enter a reason when they shut down the system Set this parameter to `Enabled` to prompt users for a reason whenever they shut down the system Set this parameter to `Disabled` to allow users to shut down the system without providing a reason Recommendation: Always set this parameter to `Enabled` to ensure that ESP generates accurate availability metrics
`Registration with SGI`	Specifies whether or not ESP should send data (system hardware and software information, event information, crash analysis reports, and system availability reports) to SGI at `esp@sgi.com` (under specific service contracts, SGI uses this data to open trouble tickets and respond to problems on your system before the problems affect system availability) Set this parameter to `Enabled` to have ESP send e-mail messages to SGI Set this parameter to `Disabled` to prevent ESP from sending e-mail messages to SGI Recommendation: Always set this parameter to `Enabled` so SGI can provide proactive support for your system (providing this information helps the call center provide quick and accurate responses to problems on your system)
`E-mail format`[a]	Specifies the format for e-mail that ESP sends. ESP can send e-mail in plain text format or compressed and encrypted (uuencoded) format. If e-mail is sent in compressed and encrypted format, recipients should use the `amreceiver` program to decode the e-mail; refer to the `amreceiver` man page for more information. Recommendation: Set this parameter to `Compressed & Encrypted`.

Table 4-1 Global Configuration Parameters **(continued)**

Parameter	Description
`Send e-mail as`[a]	Specifies the name that appears in the "From" portion of the e-mail header. This option affects e-mail messages sent by `espnotify`, `availmon`, and `espcall` (when registration with SGI is enabled).
`E-mail (text format)`[a] `E-mail (specified format)`[a]	Specify e-mail addresses that should receive e-mail from ESP. ESP sends these addresses the same messages that it sends to `esp@sgi.com`. If the `Registration with SGI` parameter is disabled, ESP sends e-mail to these addresses only; it does not send e-mail to `esp@sgi.com`. The `E-mail (text format)` parameter specifies e-mail addresses that should receive the e-mail in plain text format. The `E-mail (specified format)` parameter specifies e-mail addresses that should receive e-mail in the format specified by the `E-mail format` parameter. Each field can hold up to 255 characters; you should separate multiple e-mail addresses with spaces or commas. Recommendation: Enter e-mail addresses of local personnel that are interested in this information (for example, system administrators)

a. Any changes that you make to these parameters from an SGM server affect all SGM clients that are currently subscribed to that server.

4. Click on the `Update` button. The interface displays a confirmation window.
5. Click on the `Commit` button.

Using the Command Line Interface

You can use the `espconfig` command to update the global configuration parameters:

- Use the following command syntax to view the current setting of the event registration parameter:

```
/usr/sbin/espconfig -show event_registration
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to enable event registration by ESP:

```
/usr/sbin/espconfig -enable event_registration
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to disable event registration by ESP:

```
/usr/sbin/espconfig -disable event_registration
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to view the current setting of the event throttling parameter:

```
/usr/sbin/espconfig -show event_throttling
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to enable event throttling:

```
/usr/sbin/espconfig -enable event_throttling
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to disable event throttling:

```
/usr/sbin/espconfig -disable event_throttling
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to view the current setting of the actions parameter:

```
/usr/sbin/espconfig -show event_actions
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to enable actions:

```
/usr/sbin/espconfig -enable event_actions
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to disable actions:

```
/usr/sbin/espconfig -disable event_actions
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to view the current setting of the shutdown description parameter:

```
/usr/sbin/espconfig -show shutdown_reason
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to prompt users for a description when they shut down the system:

```
/usr/sbin/espconfig -enable shutdown_reason
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to allow users to shut down the system without providing a reason:

```
/usr/sbin/espconfig -disable shutdown_reason
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to view the current setting of the call logging parameter:

```
/usr/sbin/espconfig -show call_logging
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to enable call logging (which sends event information to SGI to provide proactive support):

```
/usr/sbin/espconfig -enable call_logging  [-text|-comp_encoded]
                    [-sgmclient <client alias>|-sysid <system id>]
```

  Note: You must set up a customer profile for call logging to work.

  The `-text` option specifies that ESP should send the e-mail message in plain text format; the `-comp_encoded` option specifies that ESP should send the message in uuencoded format. The e-mail address lists can contain up to 255 characters of comma separated e-mail addresses.

- Use the following command syntax to disable call logging:

```
/usr/sbin/espconfig -disable call_logging
                    [-sgmclient <client alias>|-sysid <system id>]
```

- Use the following command syntax to view the current setting of the e-mail parameter:

```
/usr/sbin/espconfig -show mail
```

- Use the following command syntax to enable ESP to send e-mail messages and specify the e-mail account that sends the messages:

```
/usr/sbin/espconfig -enable mail -from <email address>
                    [-email1 <email address>]
                    [-email2 <email address>]
```

- Use the following command syntax to disable ESP from sending e-mail messages:

```
/usr/sbin/espconfig -disable mail
```

Setting Up the System Parameters (Single System Manager Mode Only)

The system parameters enable you to set up an alias name, select the system mode (full or SGM), and add the system to a group.

Perform the following procedure to update the system parameters in single system manager mode:

1. Click on the `Set Environment` button.
2. Click on the `System` button.

   The interface displays the `Update System Information` window. (Refer to Figure 4-8.)

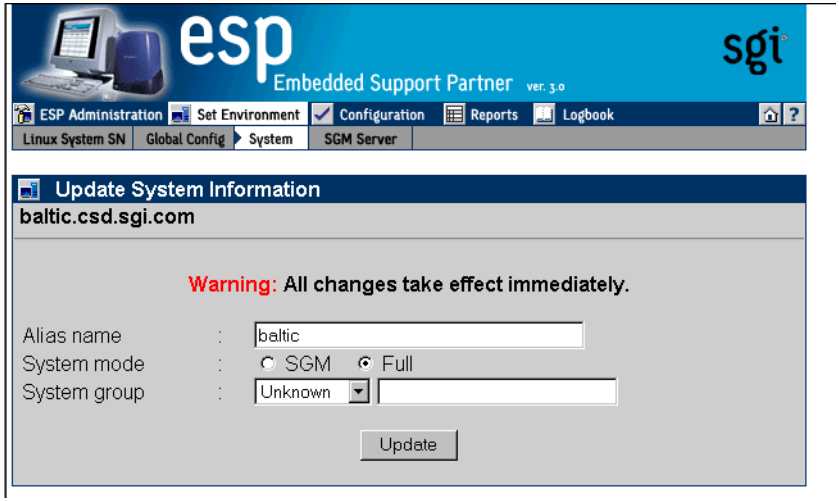


Figure 4-8 Update System Information Window (Single System Manager)

3. Set the parameters. (Table 4-2 describes the parameters that are available.)
4. Click the `Update` button.

Table 4-2 Update System Information Window Parameters (Single System Manager Mode)

Parameter	Description
`Alias`	Specifies an alias that ESP uses to identify the SGM server. This parameter is optional. If you do not set this parameter, ESP uses the hostname of the client (without the domain name). This parameter can contain any non-blank-space character, except for single or double quotes.
`System mode`	Specifies how the system is configured. There are two choices: `SGM` and `Full node` (default) The `SGM` option configures the system to be a system group manager system. The `Full node` option configures the system as a single system manager. The system does not have any clients.
`System group`	Specifies the group to which the system belongs. You can use groups to quickly access information about all systems in a group by generating a site report. Example group names include Server, Desktop, Web Server, and File Server. To create a new group, enter the name in the `System group` field. Once you create one or more group names, ESP displays a menu of the existing groups; to select an existing group, choose it from the menu. **Note:** When you enter group names, the entry in the field takes precedence over the selection in the menu. The proper way to create a new group is to set the menu to `New Group` and enter the group name in the `System Group` field. The following three rules apply for creating group names: 1) The case of characters does not matter. (ESP puts systems hat you enter in the groups named “Web server” and “Web Server” in the same group.) 2) Spacing between characters does matter. (ESP puts systems that you enter in the groups named “Web server” and “Web server” in different groups.) 3) Single and double quotes are not allowed. This parameter is optional.

Setting Up the System/Client Parameters (System Group Manager Mode Only)

The system/client parameters enable you to add a new SGM client to an SGM server, update system parameters for an SGM server or one of its SGM clients, and unsubscribe an SGM client from an SGM server.

Adding a New SGM Client

1. Click on the `Set Environment` button.
2. Click on the `System` button.
3. Click on the Add New Client button.

   The interface displays the `Add New Client` window. (Refer to Figure 4-9.)

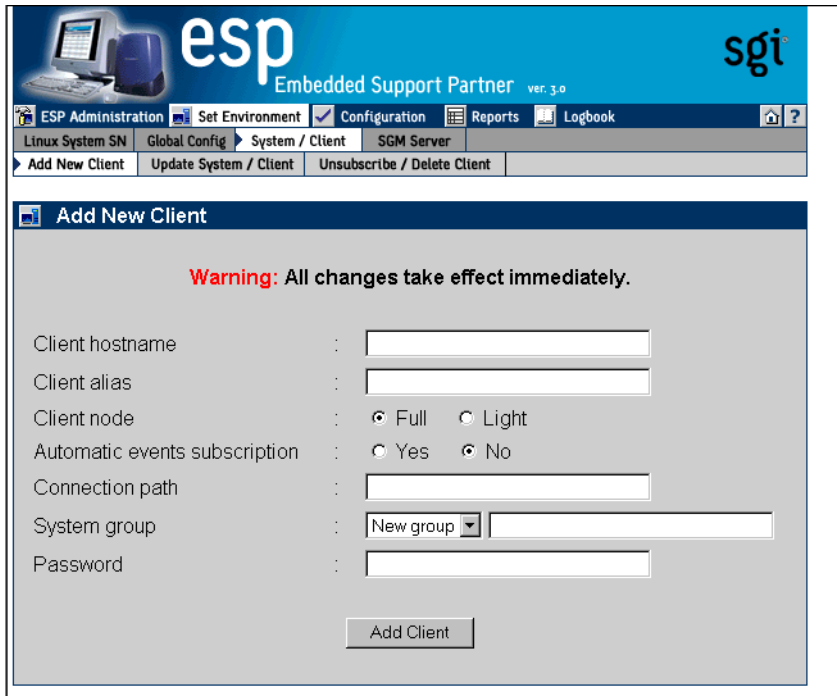


Figure 4-9 Add New Client Window (System Group Manager Mode)

4. Set the parameters for the client. (Table 4-3 describes the parameters that are available.)
5. Click on the `Add Client` button.

Table 4-3 Add New Client Window Parameters

Parameter	Description
`Client hostname`	Specifies the fully qualified hostname of a client system.
`Client alias`	Specifies an alias that ESP uses to identify the client. This parameter is optional. If you do not set this parameter, ESP uses the hostname of the client (without the domain name). This parameter can contain any non-blank-space character, except for single or double quotes.
`Client node`	Specifies how the client is configured. There are two choices: `Full` and `Light` (default). A full node is an SGM client that sends data to an SGM server and also keeps a copy of all data in its own database. Full nodes require more local disk space than light nodes. A light node is an SGM client that sends data to an SGM server but does not keep any data in its own database. You can convert a light node to a full node at any time; however, only data that is generated after the conversion completes is stored in the local database. (Data generated before the conversion completes is stored only in the database on the SGM server.)
`Automatic events subscription`	Specifies whether or not ESP should automatically subscribe events with the Event Manager. If you set this parameter to `Yes`, you do not need to manually subscribe the event (with the `Subscription` button).

Table 4-3 Add New Client Window Parameters **(continued)**

Parameter	Description
`Connection path`	Specifies the connection path between the SGM server and this client. This parameter applies only to ESP 3.0 clients. ESP 2.0 clients ignore this parameter. ESP 3.0 does not require an SGM to know the hostname and IP address information for its clients. ESP 3.0 allows an intermediate system to know this information about the SGM and client systems. This enables ESP to work through a firewall. For example, system A is an SGM server and system D is a client, but system A does not know the hostname or IP address of system D. However, system B knows about systems A and C, and system C knows about systems B and D. ESP 3.0 allows you to add system D as a client to system A by specifying the connection path as follows: B>C This means that events are forwarded from system D to system A, following the connection path through system C and system B. If only one system is intermediate, enter a fully qualified hostname of that system. If a direct connection can be established between SGM server and client systems, leave this field blank. **Note:** A connection path must be specified in the direction from the SGM server towards a client. The SGM server and client hostnames should be omitted. All systems name must be fully qualified hostnames.

Table 4-3 Add New Client Window Parameters **(continued)**

Parameter	Description
`System group`	Specifies the group to which the client belongs. You can use groups to quickly access information about all systems in a group by generating a site report. Example group names include Server, Desktop, Web Server, and File Server. To create a new group, enter the name in the `System group` field. Once you create one or more group names, ESP displays a menu of the existing groups; to select an existing group, choose it from the menu. **Note:** When you enter group names, the entry in the field takes precedence over the selection in the menu. The proper way to create a new group is to set the menu to `New Group` and enter the group name in the `System Group` field. The following three rules apply for creating group names: 1) The case of characters does not matter. (ESP puts systems hat you enter in the groups named "Web server" and "Web Server" in the same group.) 2) Spacing between characters does matter. (ESP puts systems that you enter in the groups named "Web server" and "Web server" in different groups.) 3) Single and double quotes are not allowed. This parameter is optional.
`Password`	Specifies a password that the server and client must exchange before transmitting data (to provide stronger security via authentication) This parameter is optional. If you require a password, you must configure it on the client side first.

After you set the parameters, click on the `Continue` button. For ESP 3.0 clients, ESP immediately subscribes the system without waiting for additional verification. If ESP cannot establish a connection between systems, ESP displays a message that indicates this.

Updating the System or a Client

Perform the following procedure to update the SGM server (system) or an SGM client in system group manager mode:

1. Click on the `Set Environment` button.
2. Click on the `System/Client` button.
3. Click on the `Update System/Client` button.

   The interface displays the `Update System/Client` window. (Refer to Figure 4-10.)

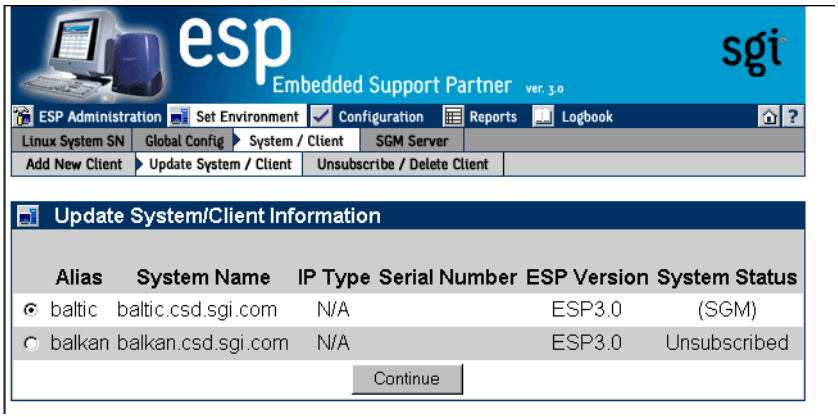


Figure 4-10 Update System/Client Window (System Group Manager Mode)

4. Select the system to update.
5. Click on the `Continue` button.

Updating the SGM Server

If you select the local system (the SGM server), ESP displays the `Update System Information` window. (Refer to Figure 4-11.)

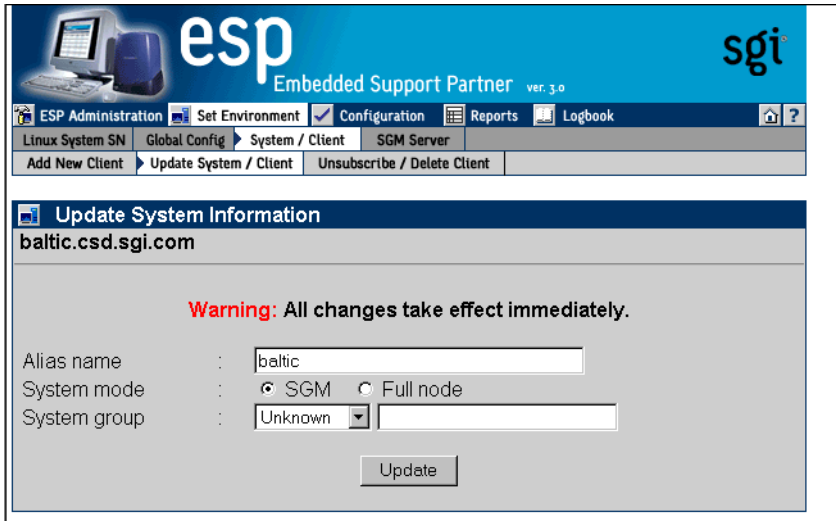


Figure 4-11 Update System Information Window (SGM Server Selected)

1. Set the parameters. (Table 4-4 describes the parameters that are available.)
2. Click the `Update` button.

Table 4-4 Update System Information Window Parameters (SGM Server)

Parameter	Description
`Alias`	Specifies an alias that ESP uses to identify the SGM server. This parameter is optional. If you do not set this parameter, ESP uses the hostname of the client (without the domain name). This parameter can contain any non-blank-space character, except for single or double quotes.
`System mode`	Specifies how the system is configured. There are two choices: `SGM` (default) and `Full node` The `SGM` option configures the system to be a system group manager system. The `Full node` option configures the system as a single system manager. The system does not have any clients.
`System group`	Specifies the group to which the system belongs. You can use groups to quickly access information about all systems in a group by generating a site report. Example group names include Server, Desktop, Web Server, and File Server. To create a new group, enter the name in the `System group` field. Once you create one or more group names, ESP displays a menu of the existing groups; to select an existing group, choose it from the menu. **Note:** When you enter group names, the entry in the field takes precedence over the selection in the menu. The proper way to create a new group is to set the menu to `New Group` and enter the group name in the `System Group` field. The following three rules apply for creating group names: 1) The case of characters does not matter. (ESP puts systems hat you enter in the groups named “Web server” and “Web Server” in the same group.) 2) Spacing between characters does matter. (ESP puts systems that you enter in the groups named “Web server” and “Web server” in different groups.) 3) Single and double quotes are not allowed. This parameter is optional.

Updating an SGM Client

If you select an SGM client, ESP displays the `Update Client Information` window. (Refer to Figure 4-12.)

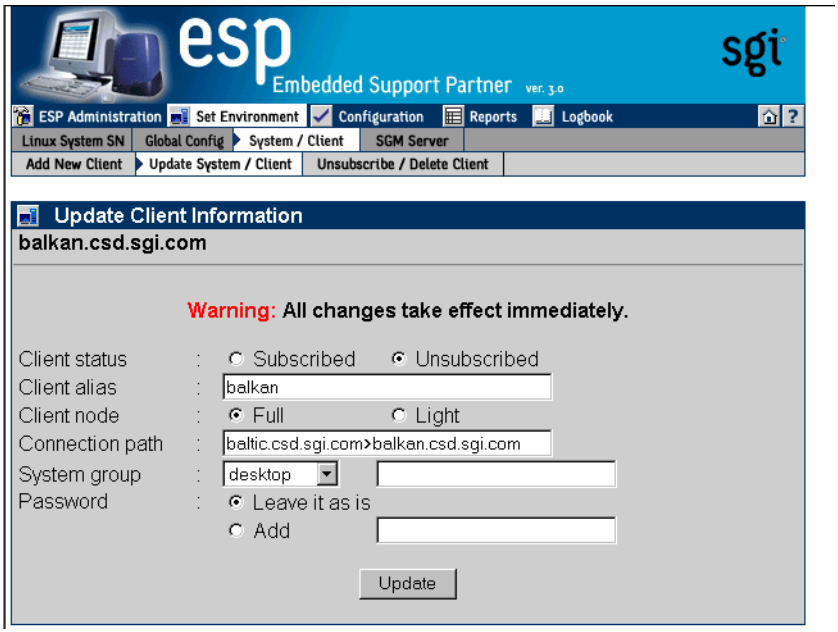


Figure 4-12 Update Client Information Window (SGM Client Selected)

1. Set the parameters. (Table 4-5 describes the parameters that are available.)
2. Click the `Update` button.

Table 4-5 Update Client Information Window Parameters (SGM Client)

Parameter	Description
`Client alias`	Specifies an alias that ESP uses to identify the client. This parameter is optional. If you do not set this parameter, ESP uses the hostname of the client (without the domain name). This parameter can contain any non-blank-space character, except for single or double quotes.
`Client node`	Specifies how the client is configured: `Full` and `Light` A full node is an SGM client that sends data to an SGM server and also keeps a copy of all data in its own database. Full nodes require more local disk space than light nodes. A light node is an SGM client that sends data to an SGM server but does not keep any data in its own database. You can convert a light node to a full node at any time; however, only data that is generated after the conversion completes is stored in the local database. (Data generated before the conversion completes is stored only in the database on the SGM server.) This parameter applies only to ESP 3.0 clients.

Table 4-5 Update Client Information Window Parameters (SGM Client) **(continued)**

Parameter	Description
`Connection path`	Specifies the connection path between the SGM server and this client. This parameter applies only to ESP 3.0 clients. ESP 2.0 clients ignore this parameter. ESP 3.0 does not require an SGM to know the hostname and IP address information for its clients. ESP 3.0 allows an intermediate system to know this information about the SGM and client systems. This enables ESP to work through a firewall. For example, system A is an SGM server and system D is a client, but system A does not know the hostname or IP address of system D. However, system B knows about systems A and C, and system C knows about systems B and D. ESP 3.0 allows you to add system D as a client to system A by specifying the connection path as follows: B>C This means that events are forwarded from system D to system A, following the connection path through system C and system B. If only one system is intermediate, enter a fully qualified hostname of that system. If a direct connection can be established between SGM server and client systems, leave this field blank. **Note:** A connection path must be specified in the direction from the SGM server towards a client. The SGM server and client hostnames should be omitted. All systems name must be fully qualified hostnames.

Table 4-5 Update Client Information Window Parameters (SGM Client) **(continued)**

Parameter	Description
`System group`	Specifies the group to which the client belongs. You can use groups to quickly access information about all systems in a group by generating a site report. Example group names include Server, Desktop, Web Server, and File Server. To create a new group, enter the name in the `System group` field. Once you create one or more group names, ESP displays a menu of the existing groups; to select an existing group, choose it from the menu. **Note:** When you enter group names, the entry in the field takes precedence over the selection in the menu. The proper way to create a new group is to set the menu to `New Group` and enter the group name in the `System Group` field. The following three rules apply for creating group names: 1) The case of characters does not matter. (ESP puts systems hat you enter in the groups named "Web server" and "Web Server" in the same group.) 2) Spacing between characters does matter. (ESP puts systems that you enter in the groups named "Web server" and "Web server" in different groups.) 3) Single and double quotes are not allowed. This parameter is optional.
`Password`	Specifies a password that the server and client must exchange before transmitting data (to provide stronger security via authentication) This parameter is optional. If you require a password, you must configure it on the client side first.

Unsubscribing SGM Clients

If a system is subscribed, you can either unsubscribe a client or unsubscribe and delete it:

- When you unsubscribe a client, the client no longer sends events to the SGM server, and changes occur on the client system. If a client system is a light node and subscribed to only one SGM server, the client system resets to a full node once the unsubscription process completes. If a client system is a full node or is subscribed to two or more SGM servers, the mode for that node remains the same. All information about an unsubscribed client for the period of time that the system was subscribed to the SGM server remains available on the SGM system.
- When unsubscribe a delete a system, the same actions occur, and all information for the system (including reports) is removed from the SGM server.

Tip: If an ESP SGM license expires and you do not plan to renew it, enter the `espconfig -unsubscribe sgmclient` command to unsubscribe the clients.

Perform the following procedure to unsubscribe a system:

1. Click on the `Set Environment` button.
2. Click on the `System/Client` button.
3. Click on the `Unsubscribe/Delete Client` button.

   The interface displays the `Unsubscribe/Delete Client` window. (Refer to Figure 4-13.)

   Note: If more than one client is subscribed to the SGM server, the interface displays a list of clients. Select the client that you want to unsubscribe and click on the `Continue` button.

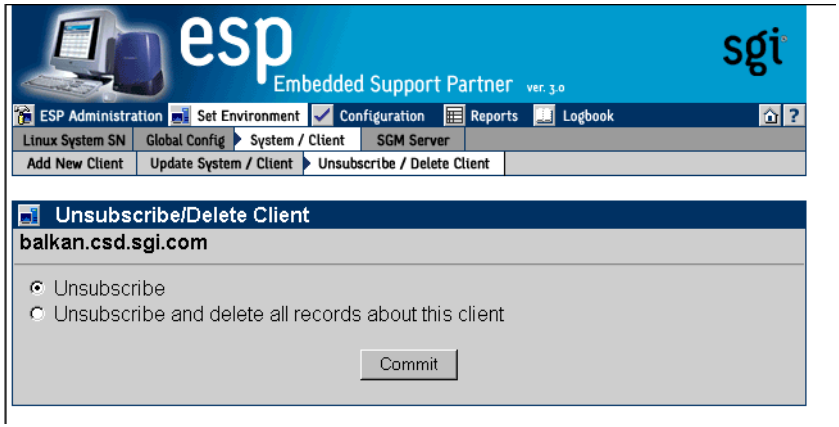


Figure 4-13 Unsubscribe/Delete Client Window

4. Specify if you want to unsubscribe the client or unsubscribe and delete the client. (ESP 2.0 clients are unsubscribed immediately. For ESP 3.0 clients, you must commit the unsubscription on a verification screen before ESP will unsubscribe them.)

   Note: When you unsubscribe an ESP 2.0 client on the server side, SGI recommends that you also unregister the server on the ESP 2.0 client side.

5. Click on the `Commit` button.

Setting Up the Authentication Password

You can use authentication between the SGM server and clients to provide stronger security. Authentication requires the SGM server to exchange and authenticate a password before any data transactions can occur. You must configure the password on the client side and then on the server side.

Adding a Password for a New Server

Perform the following procedure to set up a password on the client side in single system manager mode:

1. Click on the `Set Environment` button.
2. Click on the `SGM Server` button.
3. Click on the `Add Password for a New Server` button.

   The interface displays the `Add Password for a New Server` window. (Refer to Figure 4-14.)

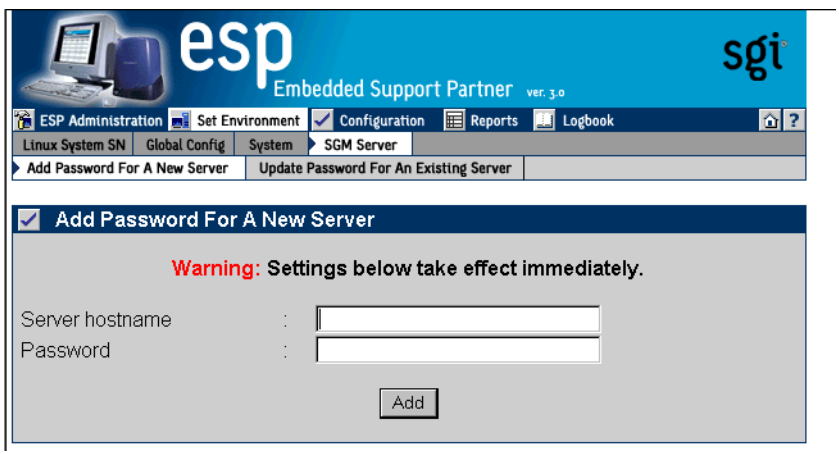


Figure 4-14 Add Password for a New Server Window

4. Enter the fully qualified hostname of the SGM server in the `Server hostname` field.
5. Enter the password in the `Password` field.
6. Click on `the Add` button.

ESP immediately adds the password. Be sure to configure the same password on the SGM server when you add the client to the server. (Refer to "Adding a New SGM Client" on page 93.)

Updating the Password for an Existing Server

Perform the following procedure to update a password that you previously assigned to a server:

1. Click on the `Set Environment` button.
2. Click on the `SGM Server` button.
3. Click on the `Update Password for an Existing Server` button.

   The interface displays the `Update Password for an Existing Server` window. (Refer to Figure 4-15.)

   Note: If the client has more than one SGM server, select the server for which you want to update the password, and click on the `Continue` button.

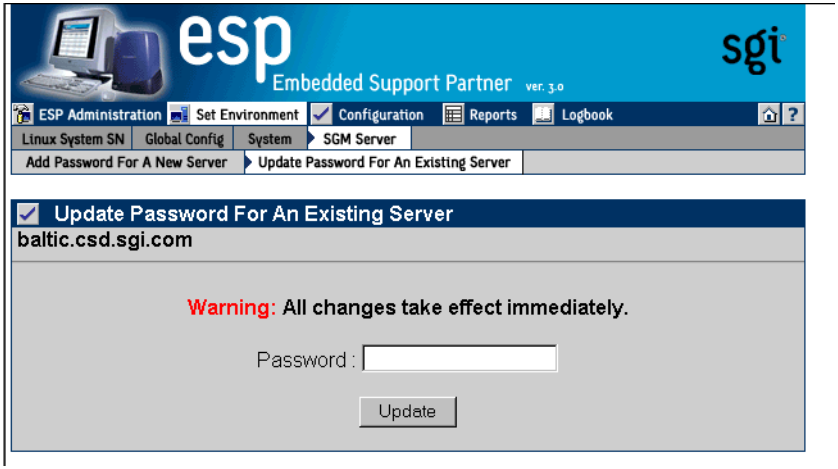


Figure 4-15 Update Password for an Existing Server Window

4. Enter the new password in the `Password` field.

   Tip: To remove a password, leave the `Password` field empty.

5. Click on the `Update` button.

Using the Command Line Interface to Configure SGM Settings

You can use the `espconfig` command to register an SGM server.

- Use the following command syntax to register a server:

  ```
  /usr/sbin/espconfig -add sgmserver -host <SGM host name>
  ```

  The command prompts you for a communication password.

You can use the `espconfig` command to configure SGM clients.

- Use the following command syntax to register a client:

  ```
  /usr/sbin/espconfig -add sgmclient <client alias> <client hostname>
  <server alias>
  ```

  The command prompts you for a communication password.

- Use the following command syntax to add a client:

  ```
  /usr/sbin/espconfig -add  sgmclient -alias <client alias>
              -host <client hostname>
              [-path <client reach path>]
              [-group <group descr.>|-gid <group id>]
              [-v2|-v3] [-p <password>]
  ```

- Use the following command syntax to subscribe a client:

  ```
  /usr/sbin/espconfig -subscribe  sgmclient
            -host <host name>|-alias <client alias>|-sysid <system id>
            [-loadprofiles] [-refreshprofiles] [-lightnode|-fullnode]
            [-force]
  ```

- Use the following command syntax to unsubscribe a client:

  ```
  /usr/sbin/espconfig -unsubscribe  sgmclient
           -host <host name>|-alias <client alias>|-sysid <system id>
          [-force]
  ```

- Use the following command syntax to update a client:

```
/usr/sbin/espconfig -update  sgmclient
          -host <host name>|-alias <client alias>|-sysid <system id>
          [-p <password>] [-path <new path>] [-lightnode|-fullnode]
```

- Use the following command syntax to delete a client:

```
/usr/sbin/espconfig -delete  sgmclient
          -host <host name>|-alias <client alias>|-sysid <system id>
```

- Use the following command syntax to ping a client:

```
/usr/sbin/espconfig ping
     -sgmclient <client alias>|-sysid <system id>|-path <reach path>
    [-espver]
```

You can use the `espconfig` to check and configure general SGM settings.

- Use the following command syntax to show the systems that an SGM knows:

```
/usr/sbin/espconfig -show systems
```

- Use the following command syntax to show an SGM's clients:

```
/usr/sbin/espconfig -show sgmclients
```

- Use the following command syntax to show the SGM servers configured for a system:

```
/usr/sbin/espconfig -show sgmservers
```

- Use the following command syntax to show information about a system:

```
/usr/sbin/espconfig -show system
    -host <host name>|-sgmclient <client alias>|-sysid <system id>
```

- Use the following command syntax to set group management parameters for a system:

```
/usr/sbin/espconfig -set system -host <host name>|-sysid <system id>
             [-alias <new alias>]
             [-group <group name> | -gid <group id> ]
```

- Use the following command syntax to configure a system (node) in SGM or full mode:

```
/usr/sbin/espconfig -setnode system -sgmnode|-fullnode
```

- Use the following command syntax to get information about the SGM license or update it:

```
/usr/sbin/espconfig -check system -sgmlicense|-update
```

- Use the following command syntax to update the SGM license key:

  ```
  /usr/sbin/espconfig -update sgmkey -host <host name> -p <comm.
  password> [-pid <key ID>]
  ```

You can use the `espconfig` command to create and manage named groups.

- Use the following command syntax to create a new group name:

  ```
  espconfig -add group -name <new group name>
  ```

- Use the following command syntax to delete a group name:

  ```
  espconfig -delete group -name <group name>
  ```

- Use the following command syntax to list the groups that are available:

  ```
  espconfig -list group
  ```

- Use the following command syntax to list the members of a group:

  ```
  espconfig -listmembers group -name <group name>
  ```

Importing and Exporting ESP Environments

You can use the `espconfig` command to import and export ESP environments between systems. The `espconfig` command transfers the following environmental information: global configuration parameters, user configuration parameters, and IP address "allow access" and "restrict access" lists. All changes are effective immediately.

- Use the following command syntax to save an ESP environment:

  ```
  /usr/sbin/espconfig -save espenv [global] [ipaddr] [user]
  [site|customer_profile] [all] [-to <filename> ]
  ```

- Use the following command syntax to load an ESP environment:

  ```
  /usr/sbin/espconfig -load espenv [-sysid <client system id>]
      [-chk <check definition filename>]
       -from <data definition filename>
  ```

Configuring ESP

This chapter describes how to configure the following components of ESP:

- Events
- Actions
- Performance monitoring
- System monitoring

Configuring Events

Events are conditions that ESP monitors. ESP includes many default events, and you can add custom events. Example events include panics, high processor utilizations, and nonmaskable interrupts (NMI).

Events are organized into event classes, which enables you to quickly view and update similar events. Example event classes include availability, system configuration, and performance.

Note: Chapter 10, "Default Event Classes and Types," contains lists of all event classes and event types that ESP includes by default.

To manage events on your system, use ESP to perform the following activities:

- Manage event profiles
- View existing event classes and events
- Add events
- Update existing events
- Update multiple events at the same time (batch update)

- Delete events
- Subscribe to events on other system (system group management mode only)

Managing Event Profiles

Event profiles provide an easy way to control which events are being monitored on your system. You can use event profiles to quickly load events that pertain to your system configuration and unload events that do not.

Event profiles are located in the `/var/esp/init/eventprofiles` directory. If you manually edit an event profile, you must save it with a `.esp` extension in this directory.

Note: In the following subsections, the term "ESP event list" refers to the events that are currently loaded in ESP on your system.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to use event profiles:

1. Click on the `Configuration` button.
2. Click on the `Events` button.
3. Click on the `Load Profile` button.

   Note: If the system is an SGM server, the interface displays a list of clients. (Refer to Figure 5-1.) Click on the client that you want to use, and click on the `Continue` button.)

   The interface displays the `Event Profile` window. (Refer to Figure 5-2.)

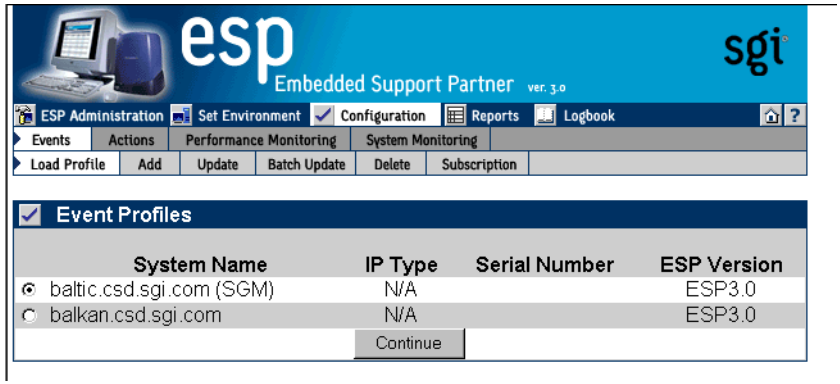


Figure 5-1 Event Profile Window (System Group Manager)

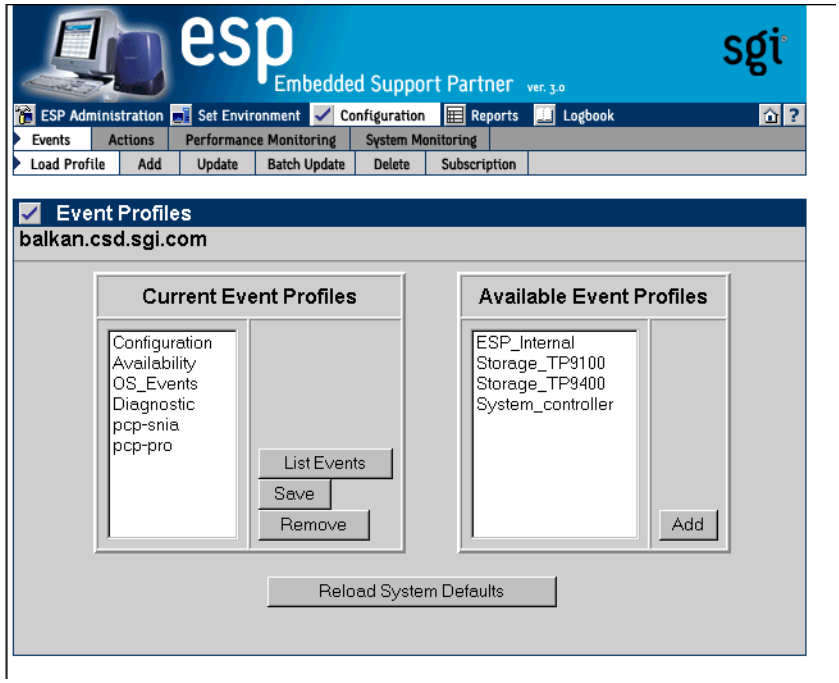


Figure 5-2 Event Profile Window

4. Use this window as follows:
   - To list the events that are contained in a profile, click on the profile in the `Current Event Profile` list, and then click on the `List Events` button.
   - To remove a set of events from the current ESP event list, click on the profile in the `Current Event Profile` list, and then click on the `Remove` button.
   - To save the current ESP event list in an event profile, click on a profile name, and then click on the `Save` button.
   - To refresh the list of profiles (from the SGM client), click on the `Refresh All Profiles` button.
   - To add a set of events from an event profile file to the ESP event list, click on the profile in the `Available Event Profiles` list, and then click on the `Add` button.

     Note: If the selected system is an SGM client, you should click on one of the radio buttons before you click on the `Add` button. Click on the radio button next to `Subscribe` to subscribe the events in the profile to the SGM server when ESP loads the event profile, or click on the radio button next to `Do Not Subscribe` to load the event profile without subscribing the events to the SGM server.
   - To reload the system defaults, click on the `Reload System Defaults` button.

Using the Command Line Interface

You can use the `espconfig` command to manage event profiles:

- Use the following command syntax to list the event profiles that are available on a system and determine which profiles are currently loaded:

  ```
  /usr/sbin/espconfig -list eventprofile [eventprofile name]
    [-sgmclient <client alias> | -sysid <system Id>]
  ```

  If you indicate a specific event profile, ESP lists only information about that event profile.

- Use the following command syntax to clear the current event list and assigned actions and to install the event profile that is stored in a file:

  ```
  /usr/sbin/espconfig -load eventprofile
    <profile name>+|allprofiles [-defaults] [-dontsubscribe]
    [-sgmclient <client alias> | -sysid <system Id>]
  ```

- Use the following command syntax to compare a file of event profile data with the events that are currently installed in ESP and to insert any events in the file that are not already installed:

  ```
  /usr/sbin/espconfig -add eventprofile
    <profile name>+|allprofiles [-defaults] [-dontsubscribe]
    [-sgmclient <client alias> | -sysid <system Id>]
  ```

- Use the following command to compare the events that are currently loaded in ESP with an event profile data file and update the events in ESP that are different in the event profile data file:

  ```
  /usr/sbin/espconfig -merge eventprofile
    <profile name>+|allprofiles [-defaults] [-dontsubscribe]
    [-sgmclient <client alias> | -sysid <system Id>]
  ```

  Note: If the event is not already in the ESP event list, the event is added to the list with the parameters defined for the event.

- Use the following command syntax to remove all events that are in the specified event profile data file from the ESP event list:

  ```
  /usr/sbin/espconfig -drop eventprofile
    <eventprofile name>+|allprofiles
    [-sgmclient <client alias> | -sysid <system Id>]
  ```

  Note: If the event being dropped is part of another event profile, the event is not dropped.

- Use the following command syntax to unload an event profile:

```
/usr/sbin/espconfig -unload eventprofile
  <eventprofile name>+|allprofiles
  [-sgmclient <client alias> | -sysid <system Id>]
```

- Use the following command syntax to save the current ESP event list and assigned actions in an event profile data file:

```
/usr/sbin/espconfig -save eventprofile <profile name>+|allprofiles
[-defaults]
```

- Use the following command syntax to refresh the ESP event list and assigned actions from an event profile data file:

```
/usr/sbin/espconfig -refresh eventprofile <profile
name>+|allprofiles    [-defaults]
```

- Use the following command syntax to show event information from an event profile:

```
/usr/sbin/espconfig -refresh eventprofile <profile name>+
[-sgmclient <client alias> | -sysid <system Id>]
```

Viewing Event Classes and Events

You can use the `espconfig` command to view all events and event classes that are available on your system.

- Use the following command syntax to list the event classes that are loaded on your system.

  ```
  /usr/sbin/espconfig -list evclass
  ```

  The output lists the event class ID and event class description. (Refer to Chapter 10, "Default Event Classes and Types," for a list of the default event classes.)

- Use the following command syntax to view the event types that are loaded on your system:

  ```
  /usr/sbin/espconfig -list evtype [-cid <class id> | -cd <class
  description>] [-enable | -disable] [-log | -nolog] [-sgmclient
  <alias>]
  ```

  Use the `-cid` option to show events with a specific class ID value. Use the `-cd` option to show events with a specific description. If you do not use the `-cid` or `-cd` option, this command lists all event types. (Refer to Chapter 10, "Default Event Classes and Types," for a list of default events.)

- The following command syntax shows all information about an event:

  ```
  /usr/sbin/espconfig -show evtype {-tid <type id> | -td <type
  description>} [-sgmclient <alias>]
  ```

  Use the `-tid` option to show events with a specific type. Use the `-td` option to show events with a specific description. If the type description is not unique, the command displays all matching event types.

  The following example shows output from this command:

  ```
  karma# espconfig -show evtype -tid 4194470
  begin : eventType
              class            : 7001
              type             : 4194470  #(0x4000a6)
              classDescription : "Irix"
              typeDescription  : "unix / * CONFIG-ISSUE*"
              throttleValue    : 1
              actionFrequency  : 0
              eventEnabled     : YES
  end   : eventType
  ```

Adding Events

You can add your own events to ESP on your system to have it monitor and register events that are specific to your system.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to add an event:

1. Click on the `Configuration` button.
2. Click on the `Add` button.

   Note: If the system is an SGM server, the interface displays a list of clients. (Refer to Figure 5-3.) Click on the client that you want to use, and click on the `Continue` button.)

   The interface displays the `Add Event` window. (Refer to Figure 5-4.)

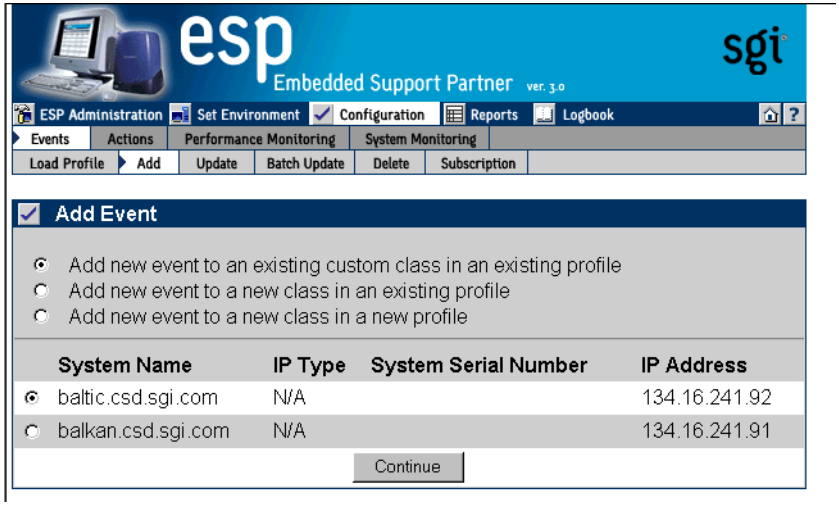


Figure 5-3 Add Event Window (System Group Manager)

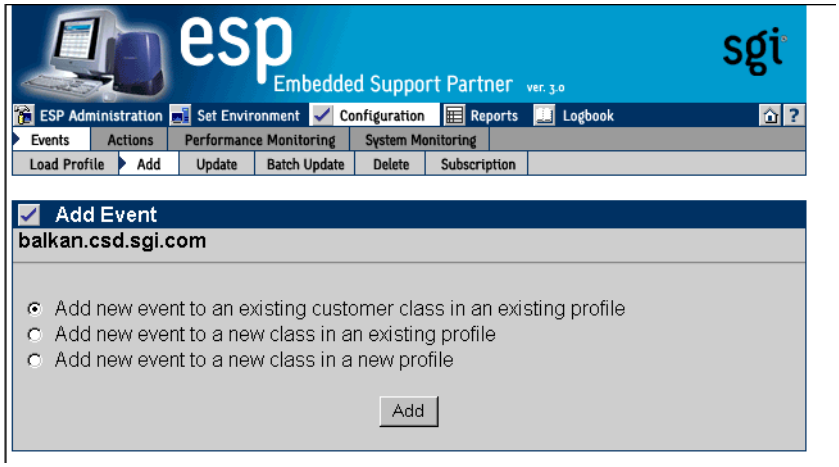


Figure 5-4 Add Event Window (Single System Manager)

Adding an Event to an Existing Event Class in an Existing Profile

Figure 5-5 shows the `Add Event` window when you choose the `Add new event to an existing customer class in an existing profile` option. Use this option to add an event to an event class that you already created. (You can only add events to the event classes that you create; you cannot add events to the default event classes.)

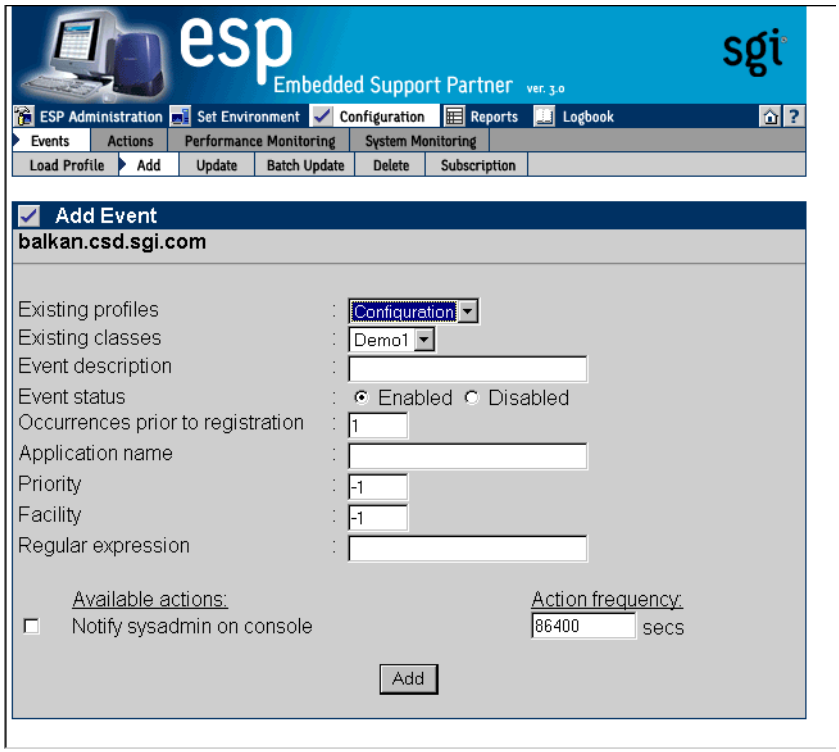


Figure 5-5 Add Event Window (Adding Event to Existing Class)

Perform the following procedure to use this window to add an event to an existing event class:

1. Choose the event profile.
2. Choose the event class.
3. Enter a description of the event in the `Event Description` field. ESP displays this description on other pages of the interface to identify the event.

   Note: The description cannot include the following characters: ‘ <
4. Specify a status for the event:
   - Click on `Enabled` to add the event to the database and to start monitoring it.
   - Click on `Disabled` to add the event to the database but not monitor it.
5. Specify the number of times that the event must occur before ESP registers it (and performs any assigned actions) in the `Occurrences prior to registration` field.
6. Set the following optional parameters to provide more information about the event:
   - Application name
   - Priority value
   - Facility value
   - Regular expression to match
7. Assign an action to the event. (If `Event status` is set to `Enabled`, ESP performs this action when the event is registered.)
8. Specify the number of seconds that ESP should pause between multiple executions of an action in the `Action frequency time` field. (A value of 0 disables the option.)

   For example, if you set this parameter to 5 seconds and ESP registers an event every second, ESP executes the assigned action(s) every 5 seconds.

   Figure 5-6 shows the `Add Event` window with example parameters.

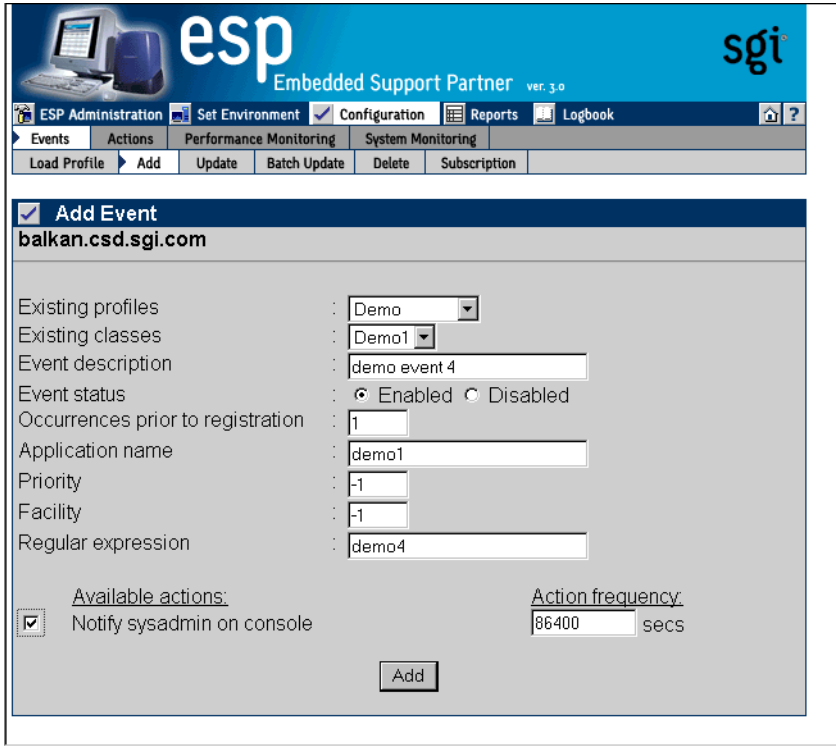


Figure 5-6 Add Event Window with Sample Parameters (Adding Event to Existing Class)

9. Click on the `Add` button.

   The interface displays a verification message. (Refer to Figure 5-7.)

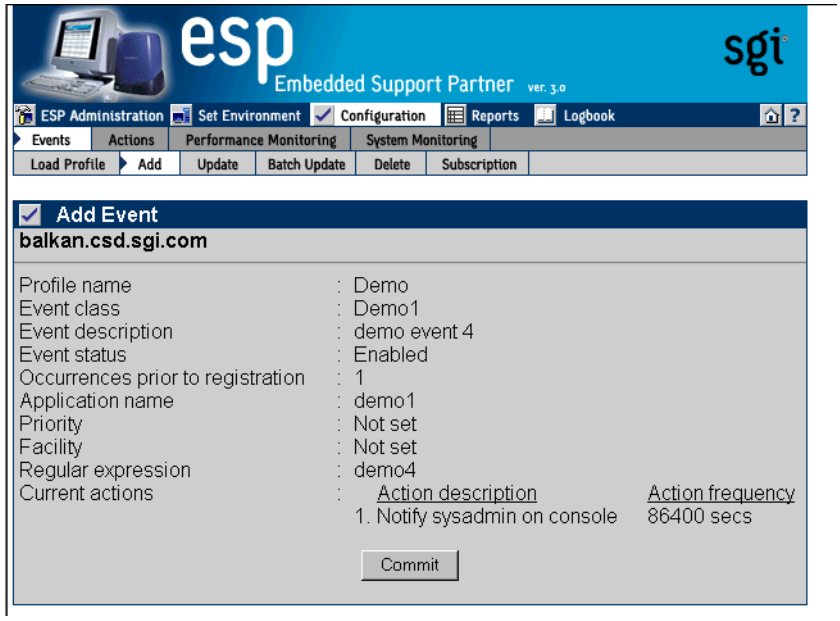


Figure 5-7 Verification Message for Adding an Event (Adding Event to Existing Class)

10. Click on the `Commit` button.

    The interface displays information about the event that was added. (Refer to Figure 5-8.) If you need to update the event, click on the `Update` button.

    Be sure to note the sequence number assigned to the event (located in the event description next to the event name). You need this number to register the event in ESP from an external application. (Refer to Chapter 9, "Logging Events from Applications and Scripts.")

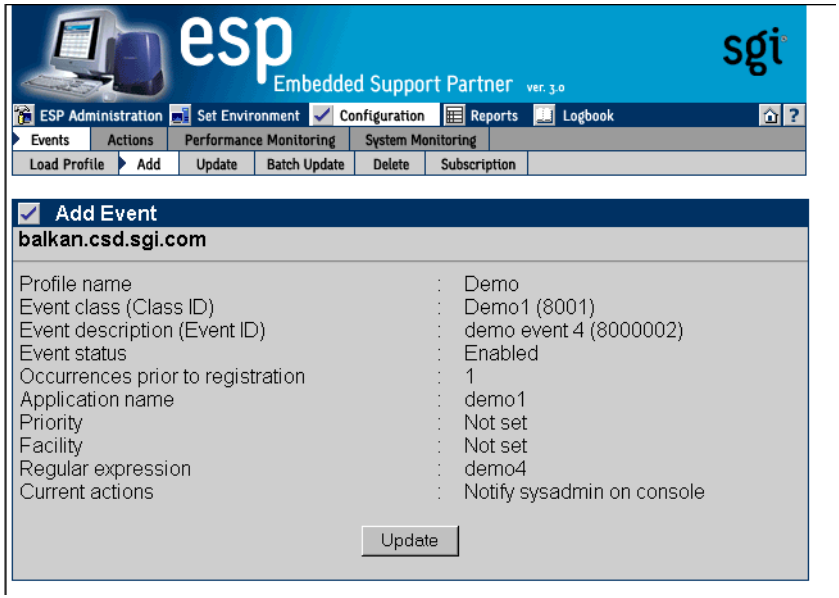


Figure 5-8 Confirmation Message for Adding an Event (Adding Event to Existing Class)

Adding an Event to a New Event Class in an Existing Event Profile

Figure 5-9 shows the `Add Event` window when you choose the `Add new event to a new class in an existing profile` option (refer again to Figure 5-4).

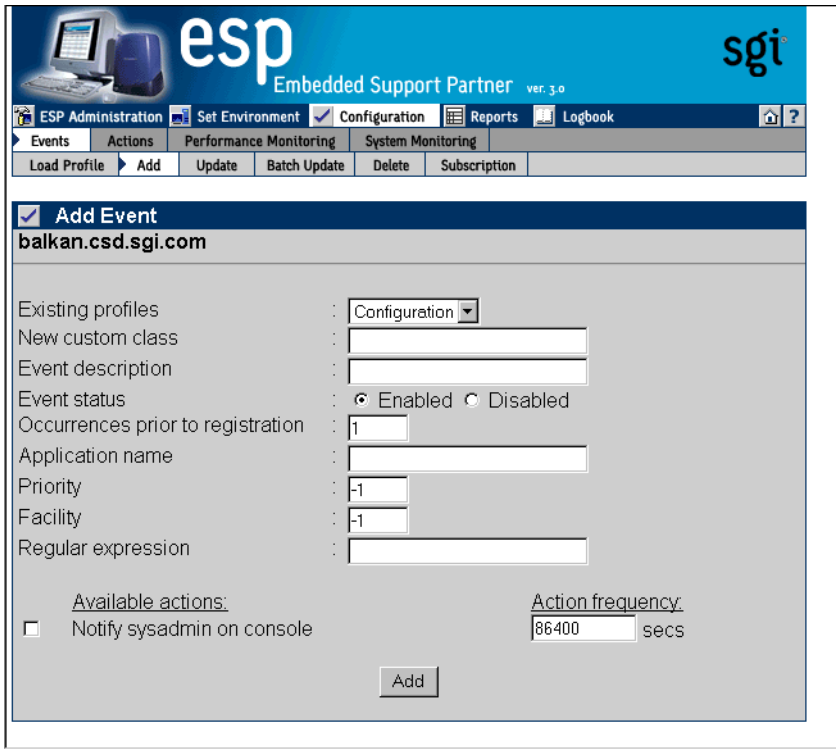


Figure 5-9 Add Event Window (Adding Event to New Class)

Perform the following procedure to use this window to add an event to a new event class:

1. Choose the event profile.
2. Enter the name of the new event class in the `New custom class` field.
3. Enter a description of the event in the `Event description` field. ESP displays this description on other pages of the interface to identify the event.

   Note: The description cannot include the following characters: ‘ <
4. Specify a status for the event:
   - Click on `Enabled` to add the event to the database and to start monitoring it.
   - Click on `Disabled` to add the event to the database but not monitor it.
5. Specify the number of times that the event must occur before ESP registers it (and performs any assigned actions) in the `Occurrences prior to registration` field.
6. Set the following optional parameters to provide more information about the event:
   - Application name
   - Priority value
   - Facility value
   - Regular expression to match
7. Assign an action to the event. (If `Event status` is set to `Enabled`, ESP performs this action when the event is registered.)
8. Specify the number of seconds that ESP should pause between multiple executions of an action in the `Action frequency time` field. (A value of 0 disables the option.)

   For example, if you set this parameter to 5 seconds and ESP registers an event every second, ESP executes the assigned action(s) every 5 seconds.

   Figure 5-10 shows the `Add Event` window with example parameters.

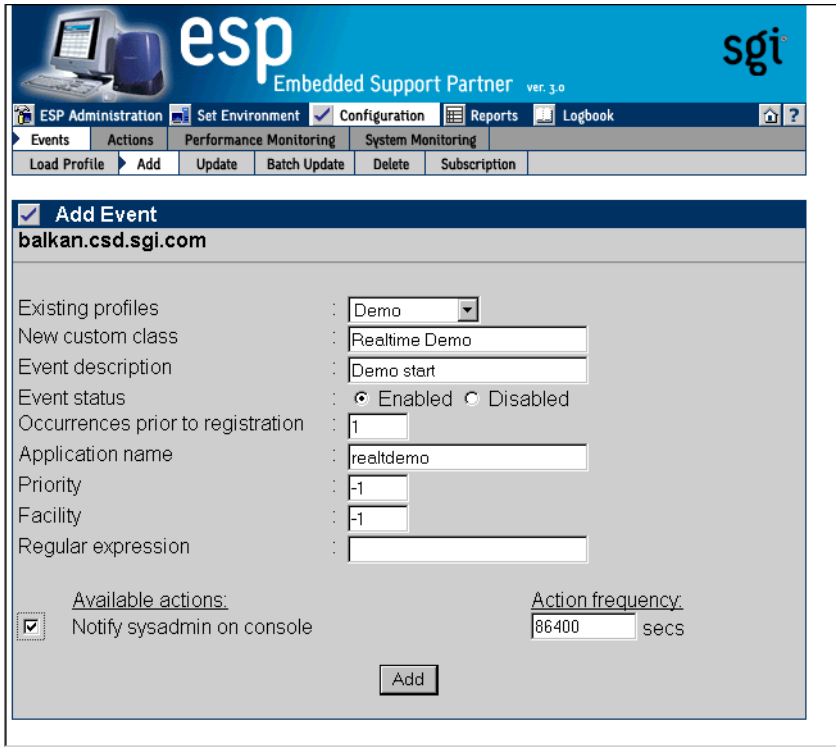


Figure 5-10 Add Event Window with Example Parameters (Adding Event to New Class)

9. Click on the Add button.

   The interface displays a verification message. (Refer to Figure 5-11.)

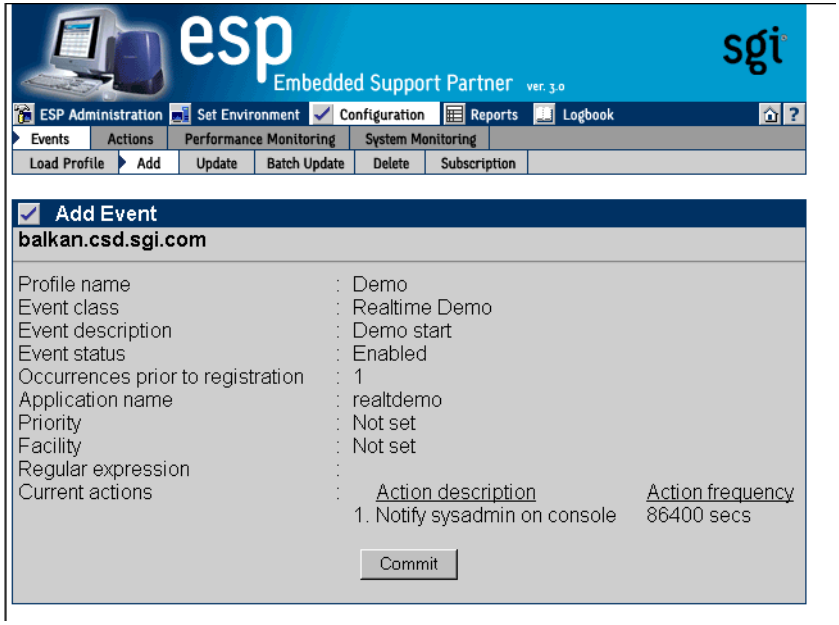


Figure 5-11 Verification Message for Adding an Event (Adding Event to New Class)

10. Click on the `Commit` button.

    The interface displays information about the event that was added. (Refer to Figure 5-12.) If you need to update the event, click on the `Update` button.

    Be sure to note the sequence number assigned to the event (located in the event description next to the event name). You need this number to register the event in ESP from an external application. (Refer to Chapter 9, "Logging Events from Applications and Scripts.")

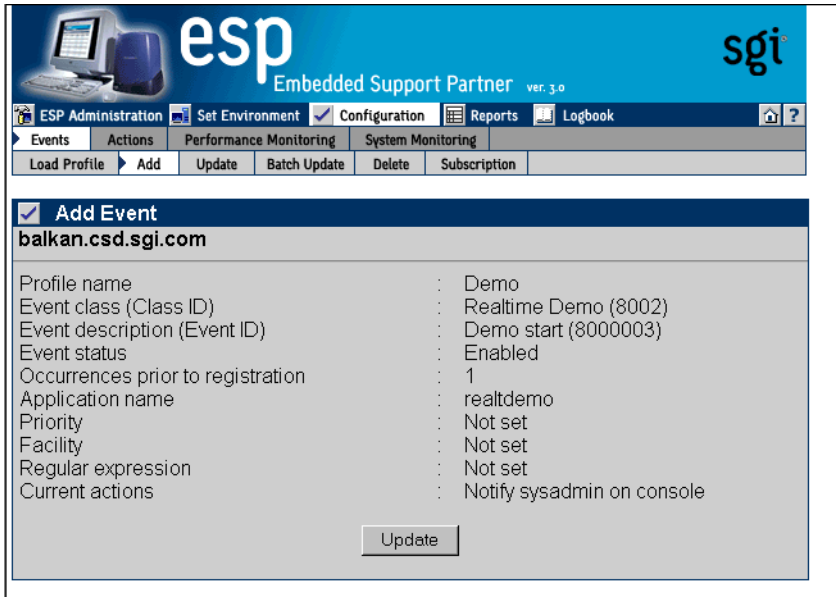


Figure 5-12 Confirmation Message for Adding an Event (Adding Event to New Class)

Adding an Event to a New Event Class in a New Event Profile

Figure 5-13 shows the `Add Event` window when you choose the `Add new event to a new class in a new profile` option (refer again to Figure 5-4).

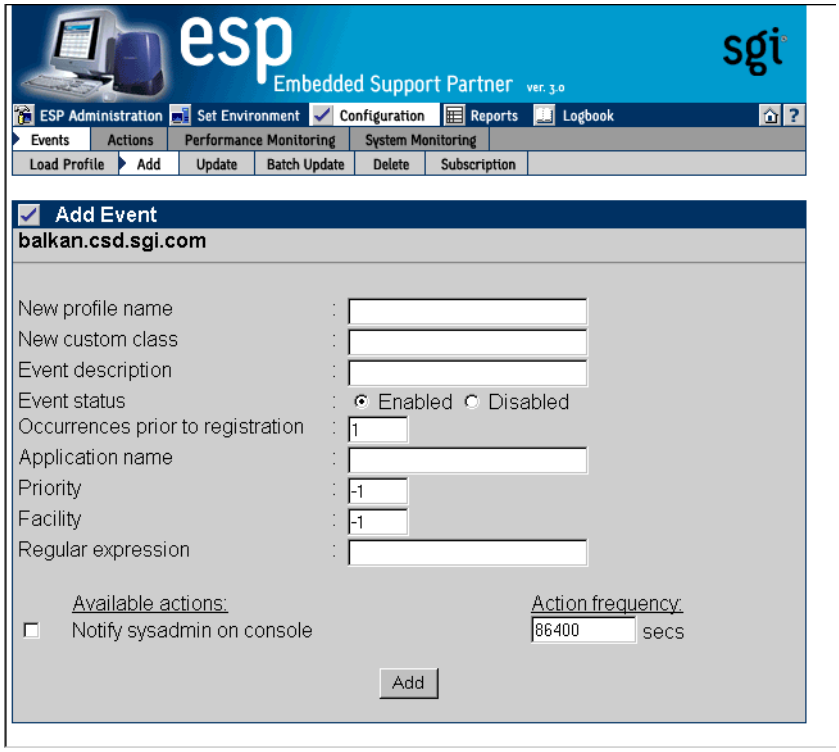


Figure 5-13 Add Event Window (Adding an Event to a New Class in a New Profile)

Perform the following procedure to use this window to add an event to a new event class:

1. Enter the name of the new event profile in the `New profile name` field.
2. Enter the name of the new event class in the `New custom class` field.
3. Enter a description of the event in the `Event description` field. ESP displays this description on other pages of the interface to identify the event.

   Note: The description cannot include the following characters: ‘ <
4. Specify a status for the event:
   - Click on `Enabled` to add the event to the database and to start monitoring it.
   - Click on `Disabled` to add the event to the database but not monitor it.
5. Specify the number of times that the event must occur before ESP registers it (and performs any assigned actions) in the `Occurrences prior to registration` field.
6. Set the following optional parameters to provide more information about the event:
   - Application name
   - Priority value
   - Facility value
   - Regular expression to match
7. Assign an action to the event. (If `Event status` is set to `Enabled`, ESP performs this action when the event is registered.)
8. Specify the number of seconds that ESP should pause between multiple executions of an action in the `Action frequency time` field. (A value of 0 disables the option.)

   For example, if you set this parameter to 5 seconds and ESP registers an event every second, ESP executes the assigned action(s) every 5 seconds.

   Figure 5-14 shows the `Add Event` window with example parameters.

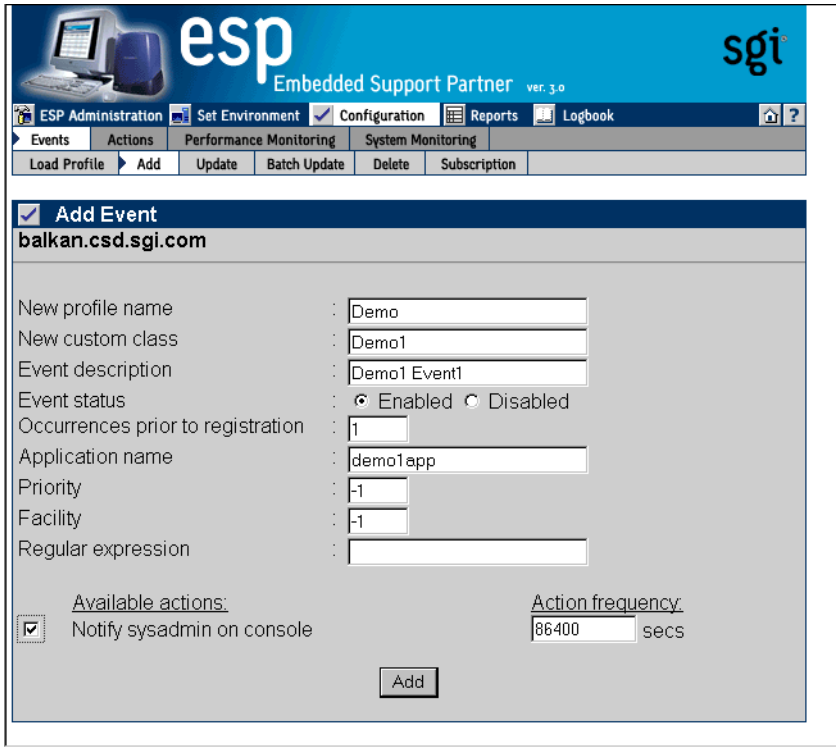


Figure 5-14 Add Event Window with Example Parameters (Adding an Event to a New Class in a New Profile)

9. Click on the Add button.

   The interface displays a verification message. (Refer to Figure 5-15.)

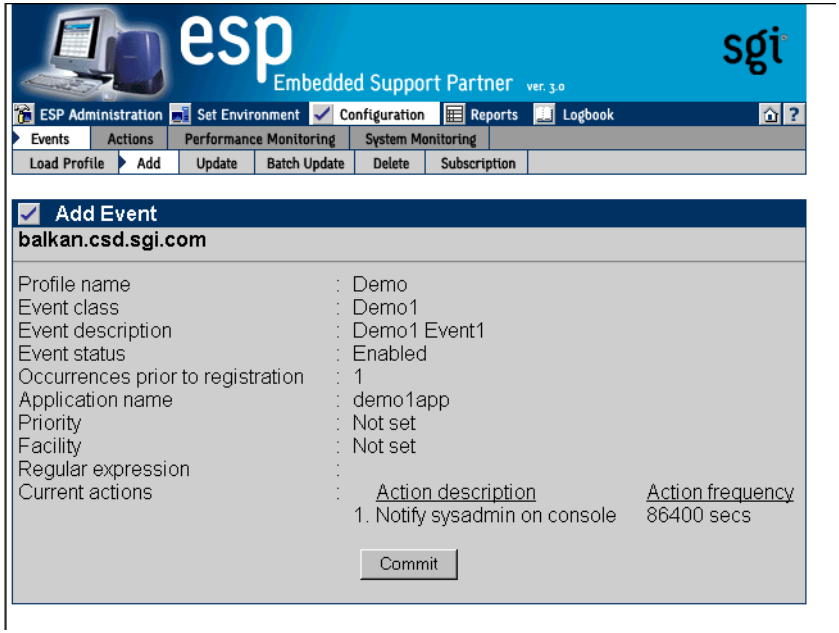


Figure 5-15 Verification Message for Adding an Event (Adding an Event to a New Class in a New Profile)

10. Click on the `Commit` button.

    The interface displays information about the event that was added. (Refer to Figure 5-16.) If you need to update the event, click on the `Update` button.

    Be sure to note the sequence number assigned to the event (located in the event description next to the event name). You need this number to register the event in ESP from an external application. (Refer to Chapter 9, "Logging Events from Applications and Scripts.")

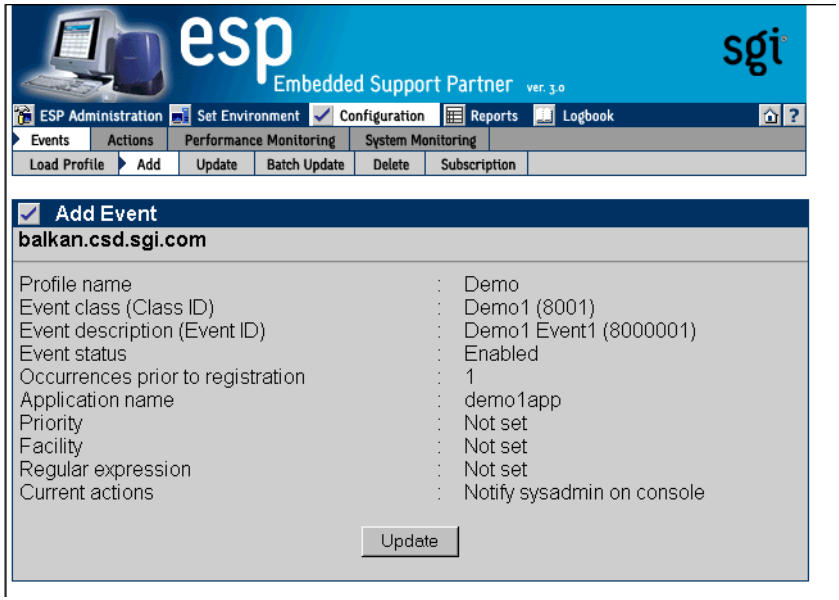


Figure 5-16 Confirmation Message for Adding an Event (Adding Event to a New Class in a New Profile)

Using the Command Line Interface

Use the following `espconfig` command syntax to add an event:

```
/usr/sbin/espconfig -add evtype    -td <type description>
    {-cid <class id> | -cd <class description>}
    [-throttle <throttle value>]
    [-enable | -disable]
    [-log | -nolog]
    [-acfreq <action frequency value>]
    [-acid <action id> | -acd  <action description>]
    [-pri <priority>] [-fac <facility>]
    [-appname <app name>] [-regexp <reg expression>]
    [-prfid <profile id> | -prfn <profile name>]
    [-sgmclient <client alias> | -sysid <client system id>]
```

Use the `-td` option to specify the type description (a string enclosed in quotes that describes the event). Use the `-cid` option to specify an existing event class ID, or use the `-cd` option to provide an existing or new class description (a string enclosed in quotes that describes the class). If the class does not exist, ESP creates a new class.

Use the `-throttle` option to specify the throttling value, which is the number of times the event must occur before ESP registers it. If you do not specify this option, the default value of 1 is used.

Use the `-enable` or `-disable` option to specify whether the event is enabled or disabled. You can specify only one of these options at a time. If you do not specify this option, the event is disabled by default.

Use the `-log` or `-nolog` option to specify if ESP should log the event.

Use the `-acid` option to assign an action to the event by specifying an existing action ID, or use the `-acd` option to assign an action to an event by specifying an action description (a string enclosed in quotes that describes the action). If you do not specify an action, no action is assigned to the event by default.

Use the `-pri`, `-fac`, `-appname`, and `-regexp` options to provide more information about the event (priority, facility, application name, and regular expression).

Use the `-prfid` or `-prfn` option to add the event to an event profile.

Use the `-sgmclient` or `-sysid` to add the event to an SGM client.

Use the following syntax to update add an event class:

```
/usr/sbin/espconfig -add evclass -cid <class id> -cd <class
description> [-sgmclient <client alias> | -sysid <client system id>]
```

Use the `-cid` option to specify the event class by class ID. Use the `-cd` option to specify a new class description (a string enclosed in quotes).

Use the `-sgmclient` or `-sysid` option to select the SGM client on which you want to update the event information.

Updating Events

You can also update the parameters for existing events.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to update an event:

1. Click on the `Configuration` button.
2. Click on the `Events` button.
3. Click on the `Update` button.

   Note: If you are using ESP on a system group manager, the interface displays the `Update Event` window with a list of SGM clients. (Refer to Figure 5-17.) Select the system on which you want to update the event, and click on the `Continue` button.

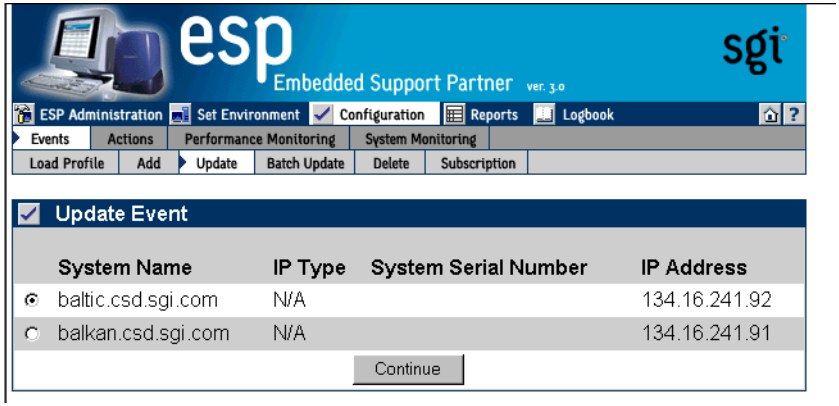


Figure 5-17 Update Event Window (with SGM Clients)

The interface displays the `Update Event` window. (Refer to Figure 5-18.)

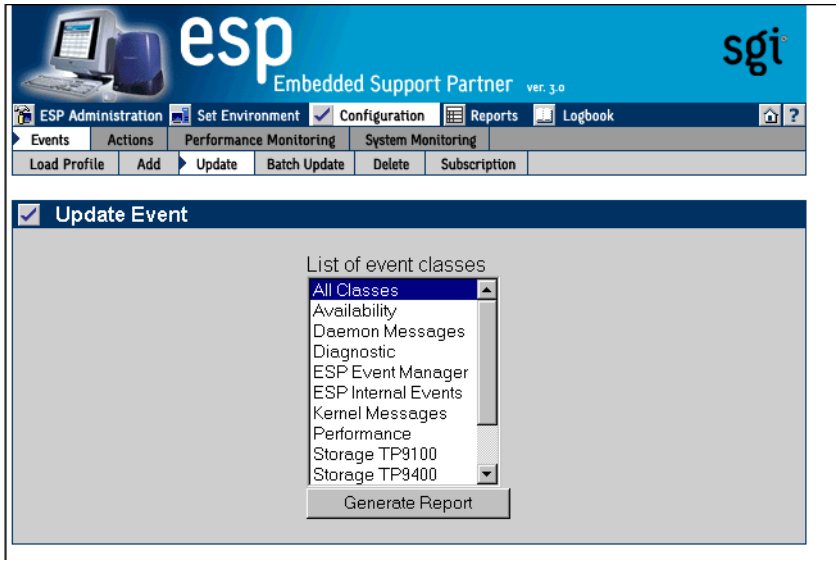


Figure 5-18 Update Event Window

4. Click on the event class that contains the event that you want to update.
5. Click on the `Generate Report` button.

   The interface displays a list of all events in the event class that you selected. (Refer to Figure 5-19.)

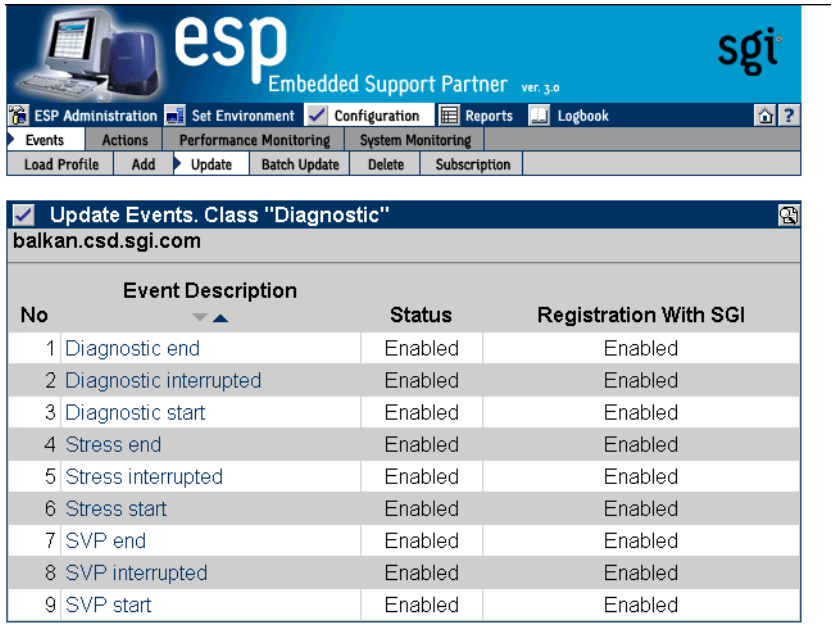


Figure 5-19 Event List for Updating an Event

6. Click on the description of the event that you want to update.

   The interface displays the `Update Event` window with the information for the event that you selected. (Refer to Figure 5-20.)

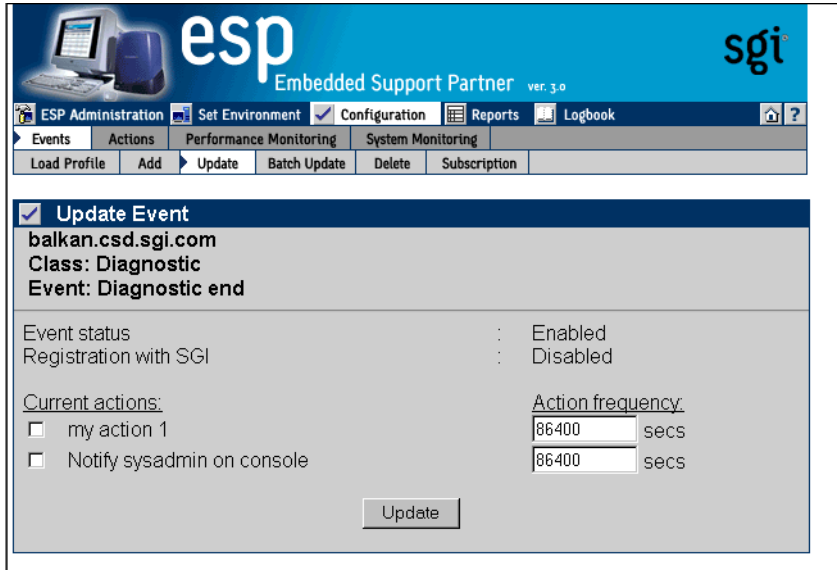


Figure 5-20 Update Event Window (with Event to Update)

You cannot modify the parameters for single events in the availability, configuration, and diagnostics classes. You must use the `Batch Update` command to update these parameters for events in those classes. (The `Live event` in the availability class is the exception; you can modify all parameters for this event.)

You cannot update the `Event Status` parameter for individual events in the availability, system configuration, or diagnostics event classes. Use the `Batch Update` command to update these parameters.

7. Update the `Event Status` parameter:
   - Click on `Enabled` to add the event to the ESP event list on your system and start monitoring it.
   - Click on `Disabled` to add the event to the ESP event list on your system but not monitor it.
8. Update the `Registration with SGI` parameter:
   - Click on `Enabled` to specify that ESP should return information about the event to SGI when the event occurs.
   - Click on `Disabled` to specify that ESP should not return information about the event to SGI when the event occurs.

   The `Registration with SGI` parameter provides individual control over specific events that ESP returns to SGI. To use this parameter, you must also enable the global `Registration with SGI` parameter.

   When the `Registration with SGI` global configuration parameter is enabled in the `Global Configuration` window (refer to Figure 4-7 on page 84), the `Registration with SGI` parameter for each event takes precedence for the individual events. When the `Registration with SGI` global configuration parameter is disabled, the `Registration with SGI` parameter for individual events does not affect ESP operation.

   The `Registration with SGI` parameter is not available for custom events. ESP never returns information about custom events to SGI.
9. Update the `Occurrences prior to registration` parameter.
10. Select the actions to assign to the event.
11. Update the `Action frequency time` parameter for each action.
12. Click on the `Update` button.

    The interface displays a verification message that shows the changes that you selected. (Refer to Figure 5-21.)

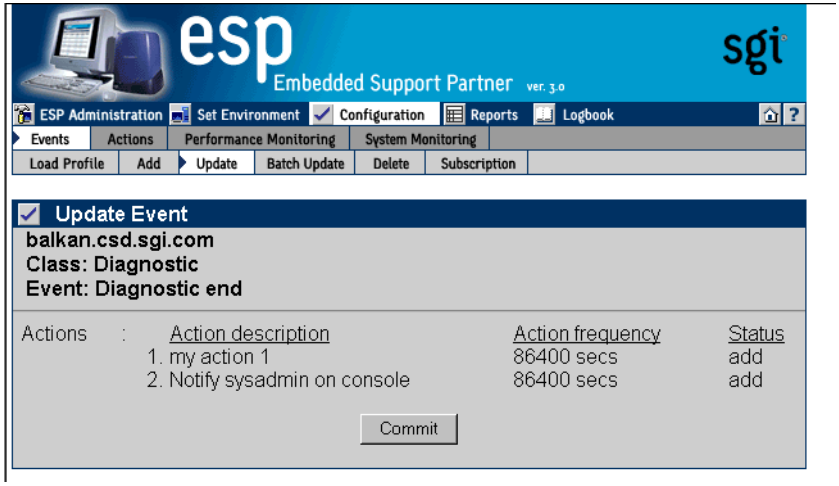


Figure 5-21 Verification Message for Updating an Event

13. Click on the `Commit` button.

    The interface displays a confirmation message that shows the updated event in bold. (Refer to Figure 5-22.)

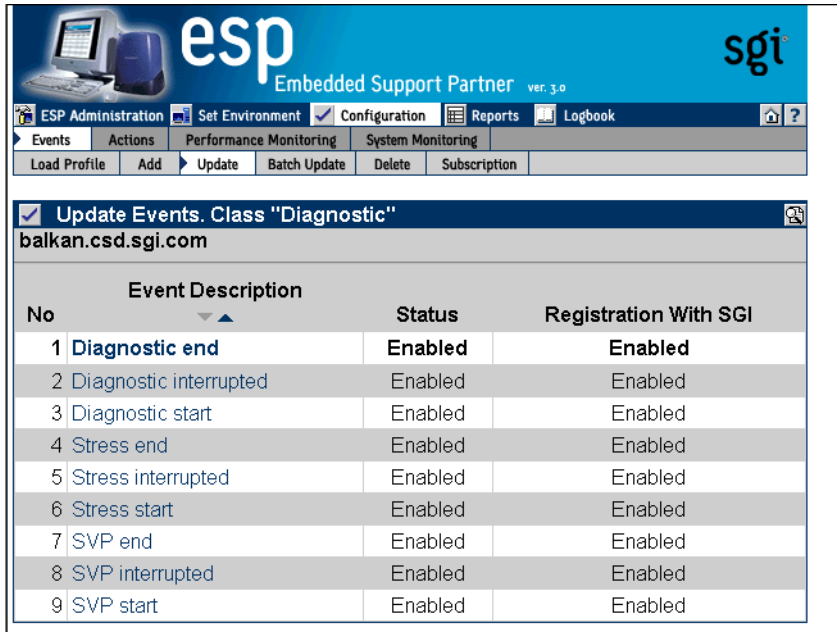


Figure 5-22 Confirmation Message for Updating an Event

Using the Command Line Interface

You can use the `espconfig` command to update event information:

- Use the following command syntax to update an event:

```
/usr/sbin/espconfig -update evtype -tid <type id>
     [-cid <class id> | -cd <class description>]
     [-sgmclient <client alias> | -sysid <client system id>]
     [-td <type description>]
     [-throttle <throttle value>]
     [-enable | -disable]
     [-log | -nolog]
     [-acfreq <action frequency value>]
     [-acid <action id> | -acd  <action description> |
     -noacid <action id> | -noacd  <action description>]
    [-acid <action id> | -acd  <action description>]
    [-pri <priority>] [-fac <facility>]
    [-appname <app name>] [-regexp <reg expression>]
    [-prfid <profile id> | -prfn <profile name> |
    -noprfid <profile id> | -noprfn <profile name>]
```

  Use the `-cid` option to specify an existing event class ID, or use the `-cd` option to provide a class description (a string enclosed in quotes that describes the class).

  Use the `-sgmclient` or `-sysid` option to select the SGM client on which you want to update the event information.

  Use the `-tid` option to specify the event to update. (You must provide a unique event type ID.)

  Use the `-td` option to update the event description. (You can only update custom event descriptions. You must provide a string enclosed in quotes.)

  Use the `-throttle` option to update the throttling value, which specifies the number of times that the event must occur before ESP registers it.

  Use the `-enable` option to enable registration of the event, or use the `-disable` option to disable registration of the event.

  Use the `-log` or `-nolog` option to specify if ESP should log the event.

  Use the `-acid` and `-acd` options to assign actions to the event. (This command can add only one action at a time; if you want to assign more than one action to an event, you must enter the command multiple times.) Specify an action ID with the `-acid` option. Specify a string enclosed in quotes with the `-acd` option.

Use the `-noacid` and `-noacd` options to remove an action that is already assigned to the event. Specify an action ID with the `-noacid` option. Specify a string enclosed in quotes with the `-noacd` option.

Use the `-pri`, `-fac`, `-appname`, and `-regexp` options to provide more information about the event (priority, facility, application name, and regular expression).

Use the `-prfid` or `-prfn` option to add the event to an event profile.

Use the `-noprfid` or `-noprfn` to remove the event from an event profile.

- Use the following syntax to update a custom class description:

  ```
  /usr/sbin/espconfig -update evclass -cid <class id> -cd <class
  description> [-sgmclient <client alias> | -sysid <client system id>]
  ```

  Use the `-cid` option to select the event class by class ID. Use the `-cd` option to specify a new class description (a string enclosed in quotes).

  Use the `-sgmclient` or `-sysid` option to select the SGM client on which you want to update the event information.

Updating Multiple Events at the Same Time (Batch Updating)

You can update multiple events at the same time by using the "batch update" feature. The "batch update" feature enables you to select more than one event at a time and apply parameter changes to all of the selected events.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to update multiple events at the same time:

1. Click on the `Configuration` button.
2. Click on the `Events` button.
3. Click on the `Batch Update` button.
4. If you are using ESP on a system group manager, the interface displays the `Update Event` window with a list of SGM clients. (Refer to Figure 5-23.) Select the system on which you want to update events, and click on the `Continue` button.

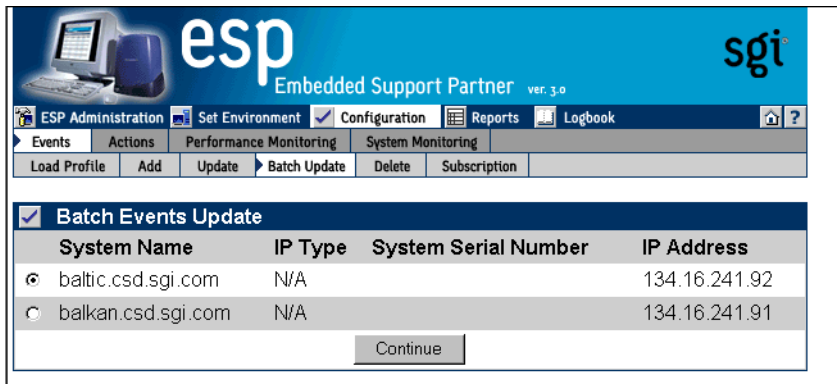


Figure 5-23 Batch Events Update Window (with SGM Clients)

The interface displays the `Event Batch Update` window. (Refer to Figure 5-24.)

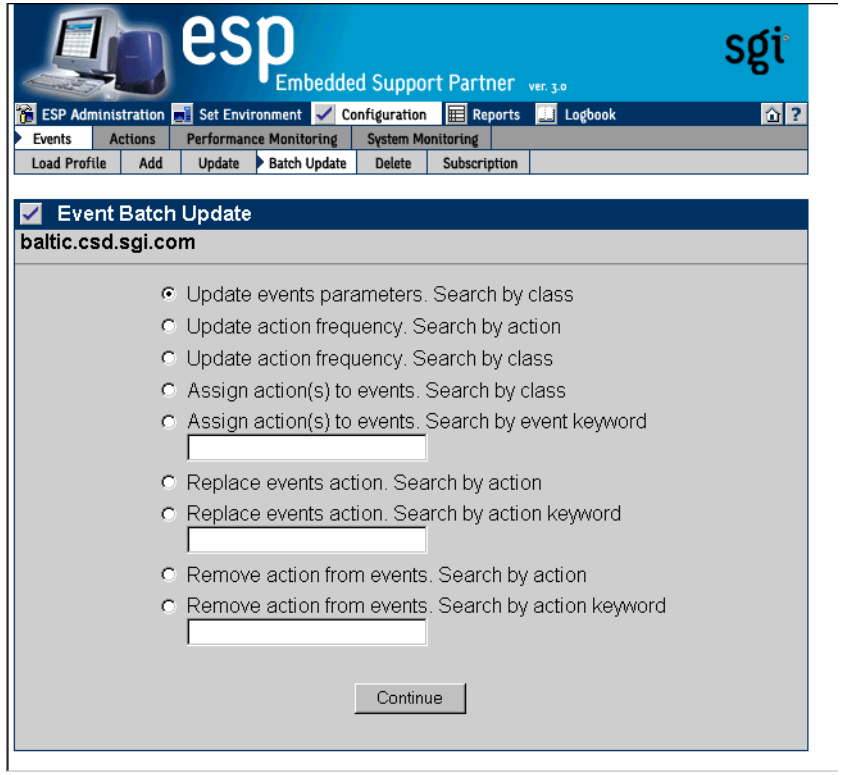


Figure 5-24 Event Batch Update Window

5. Click on the radio button next to the batch operation you want to perform. (Table 5-1 describes the batch operations and the procedure to use each operation.)

Table 5-1 Batch Update Options

Option	Description
`Update events parameters. Search by class`	Updates the event parameters for an entire class of events Perform the following procedure: 1. Click on the `Continue` button 2. Choose the class of events that you want to update 3. Click on the `Update` button 4. Update the `Event Status` and `Registration with SGI` values 5. Click on the `Update` button 6. Click on the `Commit` button
`Update action frequency. Search by action`	Updates the action frequency for multiple events Perform the following procedure: 1. Click on the `Continue` button 2. Click on the action that you want to update 3. Click on the `Continue` button 4. Uncheck the checkmark for any event classes that you do not want to update, or click on a class description to update actions assigned to individual events in the class 5. Update the `Action Frequency` values 6. Click on the `Update` button
`Update action frequency. Search by class`	Updates the action frequency for multiple events Perform the following procedure: 1. Click on the `Continue` button 2. Choose the class of events that you want to update 3. Click on the `Continue` button 4. Update the `Action Frequency` values 5. Click on the `Update` button

Table 5-1 Batch Update Options **(continued)**

Option	Description
`Assign action(s) to events. Search events by class`	Assigns an action to an entire class of events Perform the following procedure: 1. Click on the `Continue` button 2. Choose one or more classes of events 3. Choose one or more actions 4. Click on the `Assign Action` button 5. If you selected only one event class, select the check box for any events for which you do not want to assign the action 6. Click on the `Commit` button
`Assign action(s) to events. Search by event keyword`	Assigns an action to events that match a specific keyword Perform the following procedure: 1. Enter the keyword in the box 2. Click on the `Continue` button 3. Select the events to which you want to assign the action 4. Click on the `Assign Action` button 5. Select one or more actions 6. Click on the `Assign Action` button 7. Deselect the check box for any events for which you do not want to assign the action 8. Click on the `Commit` button
`Replace events action. Search events by action`	Replaces the assigned action for an event Perform the following procedure: 1. Click on the `Continue` button 2. Select the actions to replace 3. Select the new action 4. Click on the `Replace Action` button 5. Deselect the check box for any events for which you do not want to replace the action 6. Click on the `Commit` button

Table 5-1 Batch Update Options **(continued)**

Option	Description
`Replace events action. Search by action keyword`	Replaces the assigned action for an event Perform the following procedure: 1. Enter the keyword in the box 2. Click on the `Continue` button 3. Select the actions to replace 4. Select the new action 5. Click on the `Replace Action` button
`Remove action from events. Search action`	Removes an assigned action from an event Perform the following procedure: 1. Click on the `Continue` button 2. Select the action to remove 3. Click on the `Remove Action` button 4. Deselect the check box for any events for which you do not want to delete the action 5. Click on the `Commit` button.
`Remove action from events. Search by action keyword`	Removes an assigned action from an event (finds event-action combination by searching for an action) Perform the following procedure: 1. Enter the keyword in the box 2. Click on the `Continue` button 3. Select the action to remove 4. Click on the `Remove Action` button 5. Deselect the check mark for any events for which you do not want to delete the action 6. Click on the `Commit` button

Using the Command Line Interface

Batch updating is not available from the command line interface.

Deleting Events

You can delete custom events that you added to ESP on your system.

Warning: Deleting an event removes all records that are associated with the event from the database. After you delete an event, you will not be able to retrieve information about any occurrences of the event on your system.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to delete an event:

1. Click on the `Configuration` button.
2. Click on the `Events` button.
3. Click on the `Delete` button.

   Note: If the system is an SGM server, the interface displays a list of clients. (Refer to Figure 5-25.) Click on the client that you want to use, and click on the `Continue` button.)

   The interface displays the `Delete User Events` window. (Refer to Figure 5-26.)

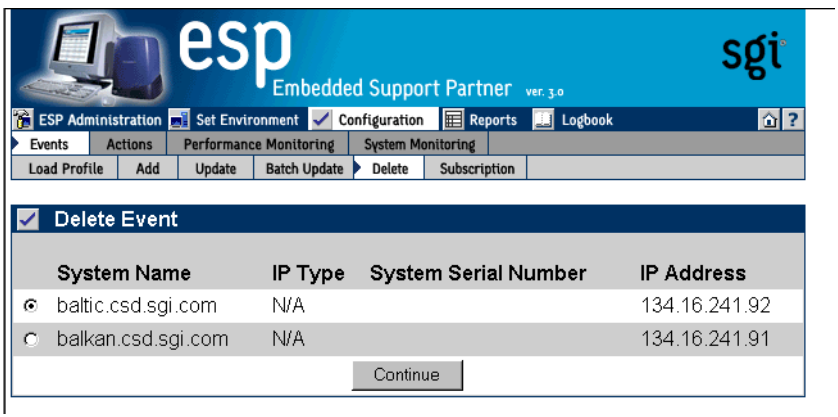


Figure 5-25 Delete User Events Window (with SGM Clients)

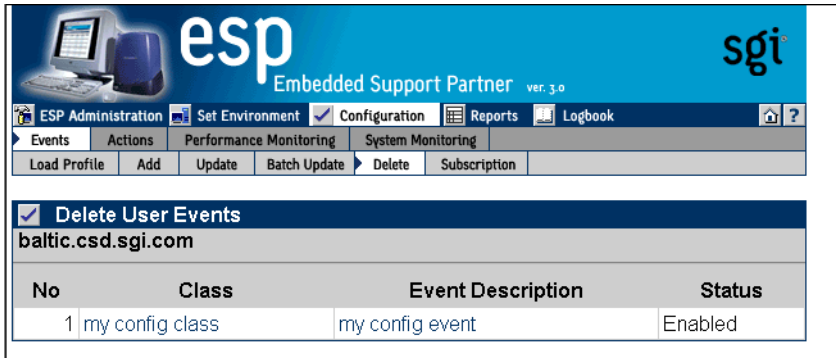


Figure 5-26 Delete User Events Window (Web-based Interface)

4. Click on the description of the event that you want to delete, or click the name of event class to delete an entire class of events.

   The interface displays a verification message. (Refer to Figure 5-27.)

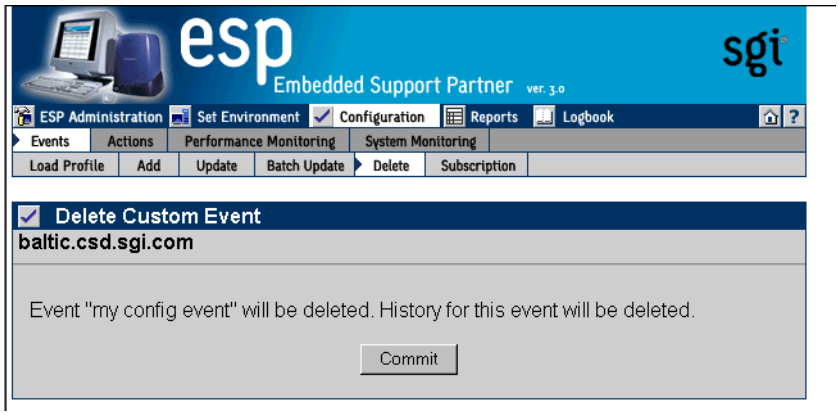


Figure 5-27 Verification Message for Deleting an Event

5. Click on the `Commit` button.

   The interface displays a confirmation message. (Refer to Figure 5-28.)

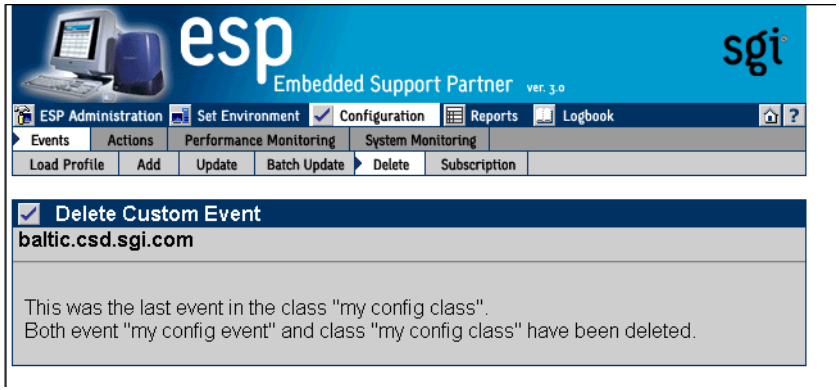


Figure 5-28 Confirmation Message for Deleting an Event

Using the Command Line Interface

You can use the `espconfig` command to delete events and event classes:

- Use the following command syntax to delete an existing custom event:

  ```
  /usr/sbin/espconfig -delete evtype {-tid <type id> | -td <type
  description>} [-sgmclient <client alias> | -sysid <client system
  id>]
  ```

  Use the `-tid` option to specify an event ID, or use the `-td` option to specify an event description (a string enclosed in quotes).

  Use the `-sgmclient` or `-sysid` option to specify an SGM client.

  Note: If the event description is not unique, the command displays a table of matching events and event IDs. When this occurs, use an event ID from the table with the `-td` option to delete an event.

  If the event to delete is the last event in a custom class, this command also deletes the event class.

- Use the following command syntax to delete an entire custom event class:

  ```
  /usr/sbin/espconfig -delete evclass {-cid <class id>|-cd <class
  description>} [-sgmclient <client alias> | -sysid <client system
  id>]
  ```

  Use the `-cid` option to specify an event class ID, or use the `-cd` option to specify an event class description (a string enclosed in quotes).

  Use the `-sgmclient` or `-sysid` option to select the SGM client on which you want to update the event information.

- Use the following command syntax to delete all event-related data structures (types, classes, actions, and so on) in the system support database:

  ```
  /usr/bin/espconfig -delete events [-sysid <system id> | -host <host
  name>]
  ```

  Use the `-sysid` option to select a system by system ID. Use the `-host` option to select a system by hostname. If you do not specify the `-sysid` or `-host` option, this command deletes data from the database tables on the local system.

Subscribing Events from SGM Clients

You can select which events to subscribe from the SGM clients.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to subscribe to events:

1. Click on the `Configuration` button.
2. Click on the `Events` button.
3. Click on the `Subscription` button.

   Note: If the system is an SGM server, the interface displays a list of clients. (Refer to Figure 5-29.) Click on the client that you want to use, and click on the `Continue` button.

   The interface displays the `Events Subscription by Class` window. (Refer to Figure 5-30.)

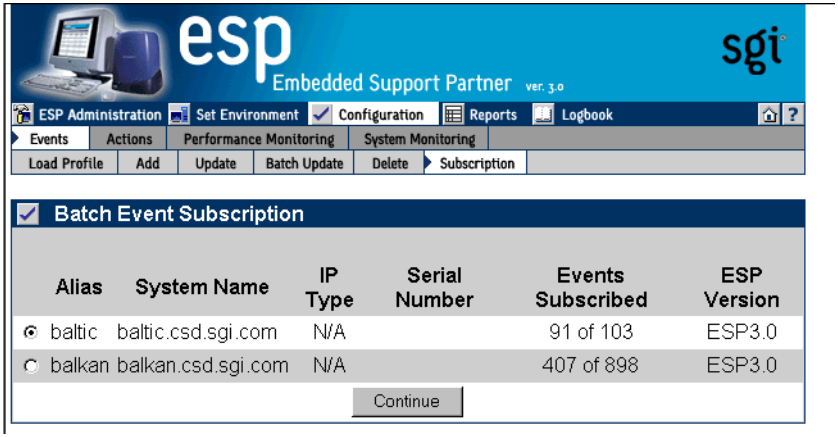


Figure 5-29 Batch Event Subscription Window

Figure 5-30 Events by Subscription Class Window

This window displays all event classes available on the selected client.

- Set the check mark to select an entire class for subscription or unsubscription.
- Click on a class description to access the individual events in a class. The interface displays the current status of all events in the class.
- Click on the `Subscribe` button to subscribe all events in a class. (ESP subscribes all events in the class that have event registration enabled on the SGM client.)
- Click on the `Unsubscribe` button to unsubscribe all events in a class. (ESP unsubscribes all events in the class.)

Using the Command Line Interface

You can use the `espconfig` command to subscribe and unsubscribe events:

- Use the following command syntax to subscribe events:

```
/usr/sbin/espconfig -subscribe evtype
     [-cid <class id>|-cd <class desc>]
     [-tid <type id>|-td <type desc>]
     [-pri <priority>] [-fac <facility>]
     [-appname <application name>]
     [-sgmclient <client alias>|-sysid <client system id >]
```

- Use the following command syntax to unsubscribe events:

```
/usr/sbin/espconfig -unsubscribe evtype
     [-cid <class id>|-cd <class desc>]
     [-tid <type id>|-td <type desc>]
     [-pri <priority>] [-fac <facility>]
     [-appname <application name>]
     [-sgmclient <client alias>|-sysid <client system id >]
```

Configuring Actions

Actions are commands that ESP performs in response to events if you set up event/action assignments. An event/action assignment specifies the action that ESP should perform for a specific event when it registers a specific number of events. Example actions include sending an e-mail message and sending a page.

Use ESP to perform the following activities to manage actions on your system:

- View existing actions
- Add actions
- Update existing actions
- Disable actions

Viewing the Existing Actions

You can use the `espconfig` command to view the existing actions.

- Use the following command syntax to list event actions. It lists the action IDs and action descriptions from the event action fields.

  ```
  /usr/sbin/espconfig -list evaction
  ```

- Use the following command syntax to view all parameters for an action:

  ```
  /usr/sbin/espconfig -show evaction {-acid <action id> | -acd <action
  description>}
  ```

  This command shows the fields in the following format:

  ```
  begin : eventAction
      actionId          : 4
      throttle          : 1
      action            : "/usr/bin/espnotify -A \"%D\""
      retryCount        : 0
      timeout           : 10
      user              : "root"
      actionDescription : "Notify sysadmin on console"
      disabled          : "NO"
  end   : eventAction
  ```

  Use the `-acid` option to specify an action ID, or use the `-acd` option to specify an action description (a string enclosed in quotes).

Adding Actions

You can customize ESP by adding new actions.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to add actions:

1. Click on the `Configuration` button.
2. Click on the `Actions` button.

   The interface displays the `Add an Action` window. (Refer to Figure 5-31.)

Figure 5-31 Add an Action Window

3. Specify how you want to create the action string:
   - To have ESP build a notification action string from menu options that you select, click on the radio button next to `Notification action`. (Use this option if you do not know the appropriate syntax of the `espnotify` command for the notification that you want to create.)
   - To manually enter the action string, click on the radio button next to `Other action`. (Use this option if you know the syntax of the `espnotify` command for the notification that you want to create or if you want to create an action that is not a notification.)
4. Click on the `Continue` button.

The interface updates the `Add An Action` window. The following subsections describe how to use this window.

Using the Notification Action Option

Figure 5-32 shows the `Add an Action` window when you choose the `Notification Action` option.

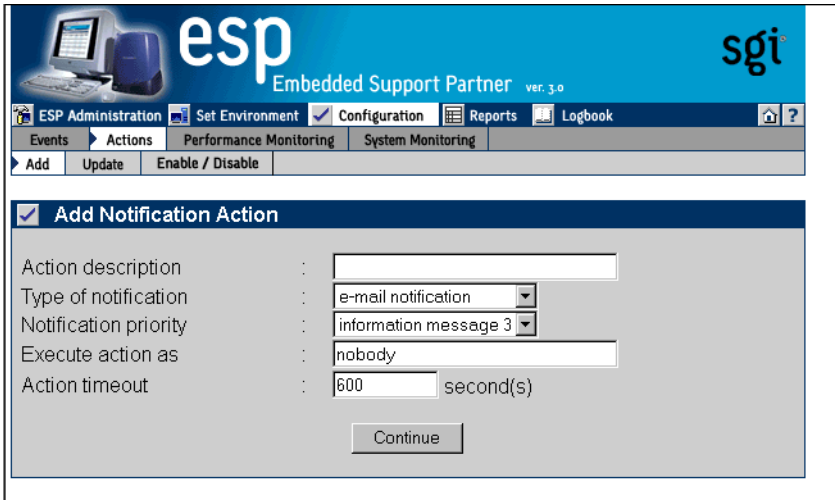


Figure 5-32 Add an Action Window (Using Notification Action Option)

Perform the following procedure to use this window to create an action:

1. Enter a description for the action. ESP displays this description on other pages of the interface.
2. Select the type of notification that you want to create (e-mail notification, system console notification, or GUI pop-up notification).
3. Select the priority of the notification.
4. Enter the user account that will execute the command. (The default is the `nobody` account.)
5. Enter the amount of time that ESP should wait for the action to execute (timeout value). If the action does complete within this period of time, ESP kills the action.
6. Click on the `Continue` button.
   - If you selected `e-mail notification`, ESP displays the window shown in Figure 5-33.
   - If you selected `notify on console`, ESP displays the window shown in Figure 5-34.
   - If you selected `GUI pop-up notification`, ESP displays the window shown in Figure 5-35.

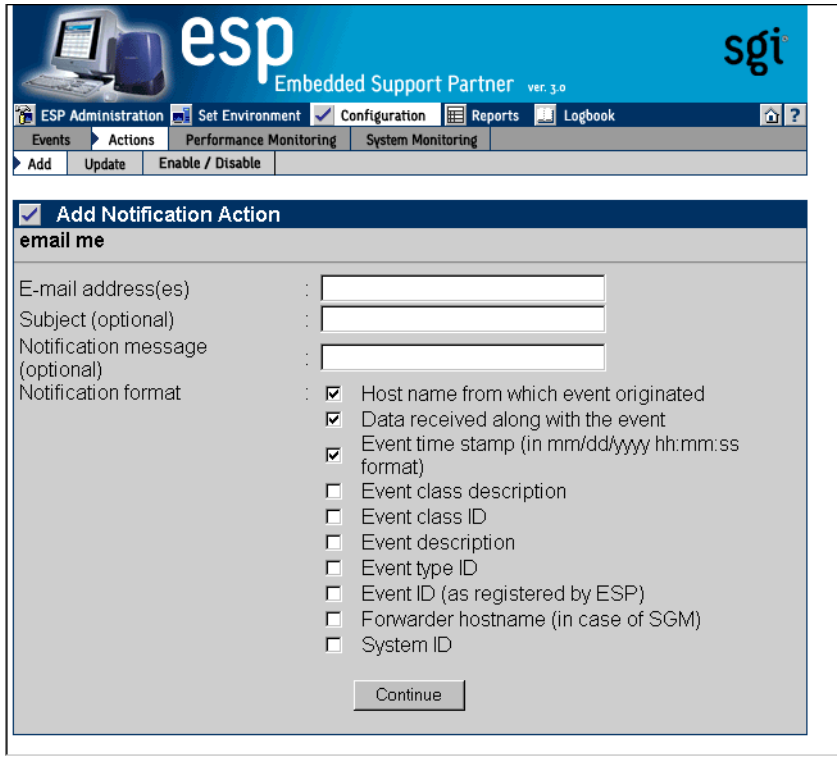


Figure 5-33 Add an Action Window (Using Notification Action and E-mail Options)

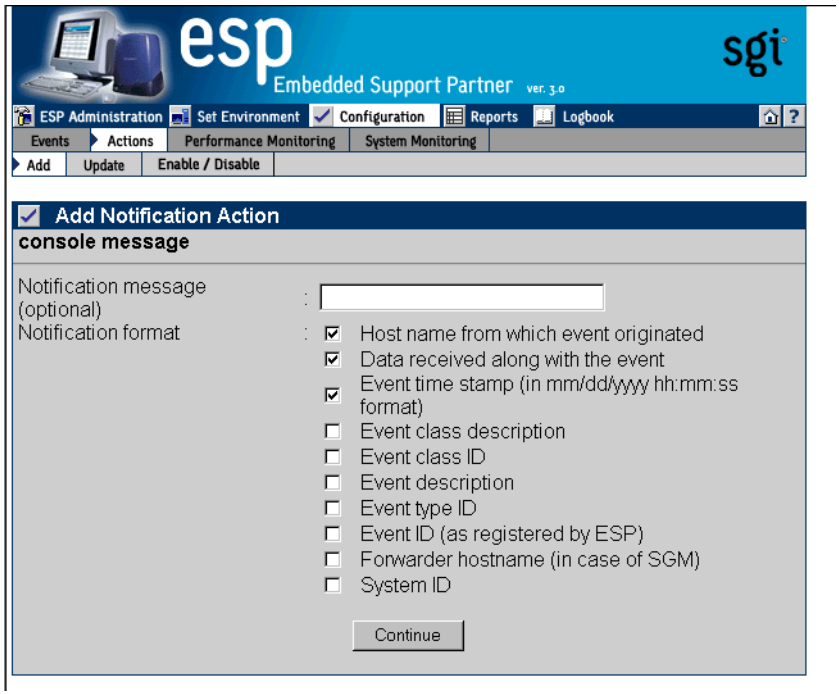


Figure 5-34 Add an Action Window (Using Notification Action and System Console Options)

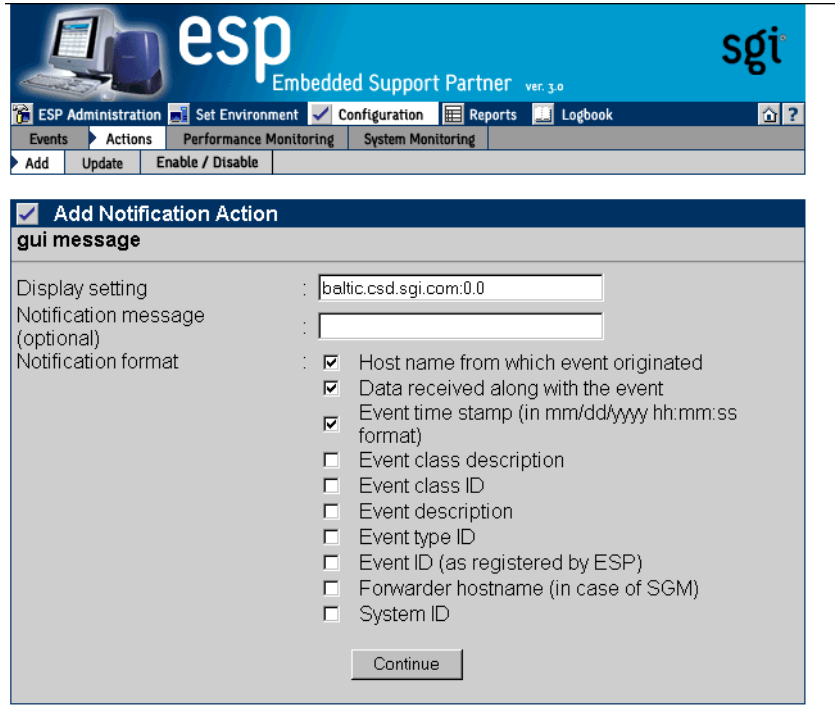


Figure 5-35 Add an Action Window (Using Notification Action and GUI Pop-up Options)

7. Set the parameters for the action.

   Table 5-2 describes the parameters that are available for each type of notification.

Table 5-2 Notification Action Parameters

Notification Type	Parameter	Description
E-mail notification	`E-mail address(es)`	Specifies the e-mail address(es) that receive an e-mail notification **Tip:** Separate multiple e-mail addresses with a space, a comma, or a semicolon.
	`Subject`	Specifies the subject of the e-mail notification **Tip:** The message cannot include quotation marks (single or double).
	`Notification message`	Specifies a message to add to the end of the notification **Tip:** The message cannot include quotation marks (single or double).
	`Notification format`	Specifies event information to include in the notification
Console Notification	`Notification message`	Specifies a message to add to the end of the notification **Tip:** The message cannot include quotation marks (single or double).
	`Notification format`	Specifies event information to include in the notification
GUI pop-up notification	`Display setting`	Specifies the X Window System display to use
	`Notification message`	Specifies a message to add to the end of the notification **Tip:** The message cannot include quotation marks (single or double).
	`Notification format`	Specifies event information to include in the notification

8. Click on the `Continue` button.

   The interface displays a verification message. (Refer to Figure 5-36.)

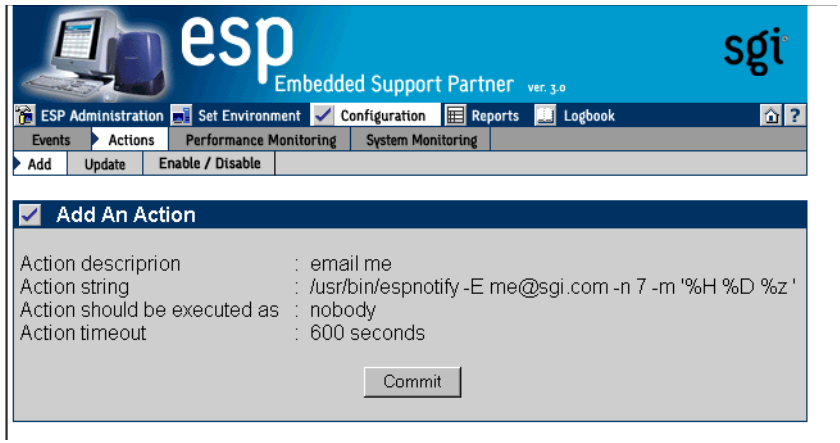


Figure 5-36 Verification Message for Adding an Action (Using Notification Action Option)

9. Click on the `Commit` button.

   The interface displays a confirmation message. (Refer to Figure 5-37.) If you need to update the action parameters, click on the `Update` button.

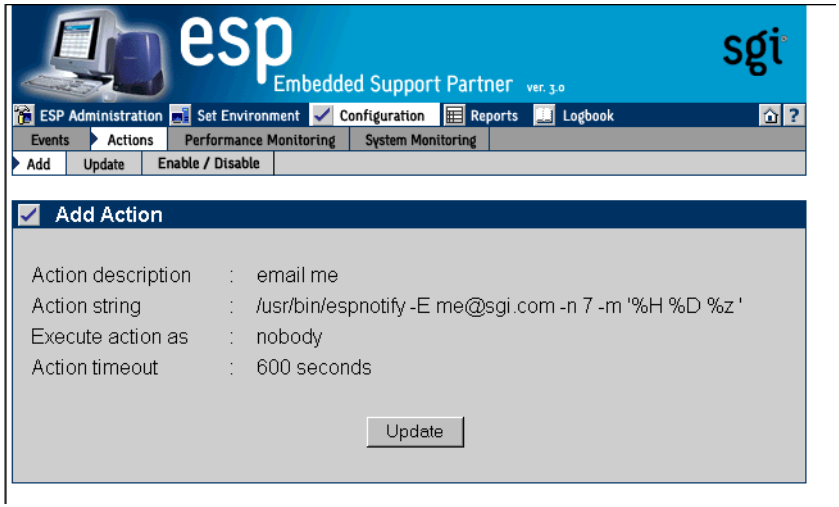


Figure 5-37 Confirmation Message for Adding an Action (Using Notification Action Option)

Using the Other Action Option

Figure 5-38 shows the `Add An Action` window when you choose the `Other Action` option.

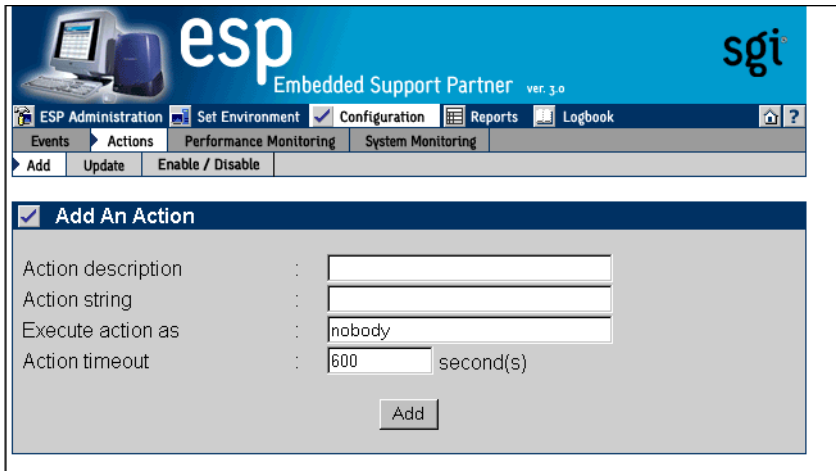


Figure 5-38 Add an Action Window (Using Other Action Option)

Perform the following procedure to use this window to create an action:

1. Enter a description for the action. ESP displays this description on other pages of the interface.
2. Enter a command to execute as a action. (For example, you could use the `espnotify` command to send an e-mail. Refer to Chapter 8, "Sending Notifications," for more information about using the `espnotify` command to send notifications.)

   Note: If you want to create a standard notification, it is easiest to use the `Notification Action` option in the `Add An Action` window. (Refer to Figure 5-31.)

Tip: When you use the `espnotify` command, you can include several variables in the `<message>` parameter. (Table 5-3 describes the variables.)

Table 5-3 espnotify Parameters

Variable	Description
`%C`	Event class
`%T`	Event type
`%D`	Event data
`%H`	Host where the event originated
`%S`	Time when the event occurred (in seconds since 00:00:00 UTC on January 1, 1970)
`%F`	Host that forwarded the event
`%I`	System ID
`%t`	Current time string
`%s`	Current time (in seconds since 00:00:00 UTC on January 1, 1970)
`%m`	Current minute of the hour
`%M`	Current month of the year
`%h`	Current hour of the day
`%y`	Current year
`%d`	Current day of the month

3. Enter the user account that will execute the command. (The default is the `nobody` account.)
4. Enter the amount of time that ESP should wait for the action to execute (timeout value). If the action does complete within this period of time, ESP kills the action.

   Figure 5-39 shows the `Add an Action` window with example parameters.

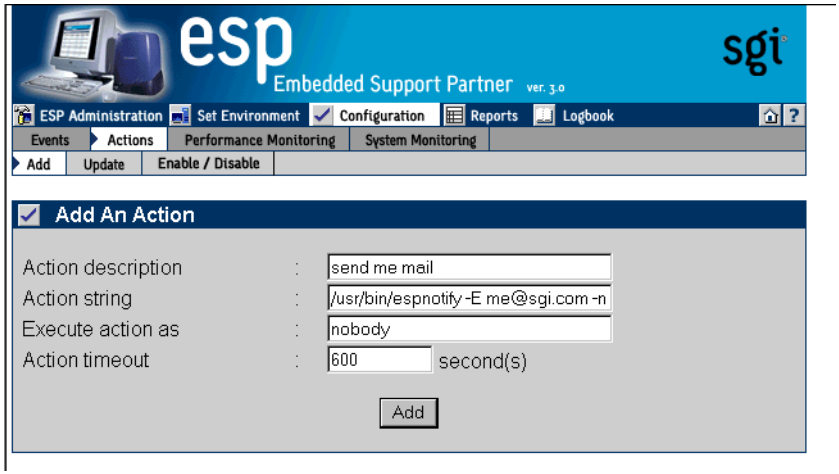


Figure 5-39 Example Parameters (Add an Action Window Using Other Action Option)

5. Click on the `Add` button.

   The interface displays a verification page. (Refer to Figure 5-40.)

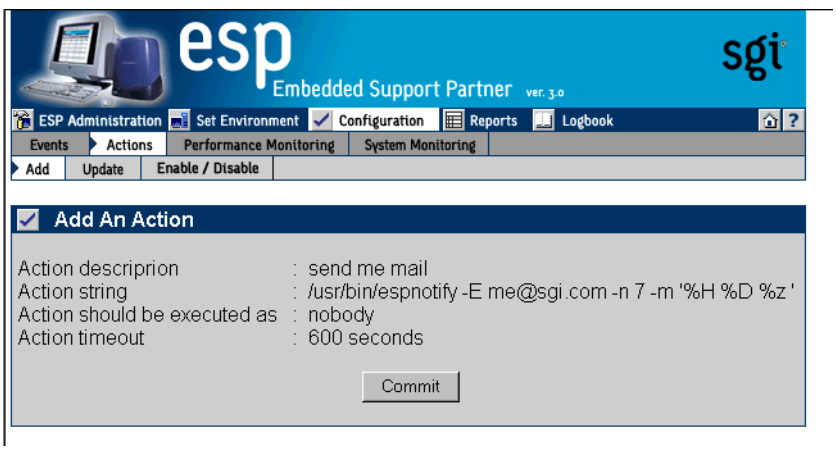


Figure 5-40 Verification Message for Adding an Action (Using Other Action Option)

6. Click on the `Commit` button.

The interface displays a confirmation message. (Refer to Figure 5-41.) If you need to update the action parameters, click on the `Update` button.

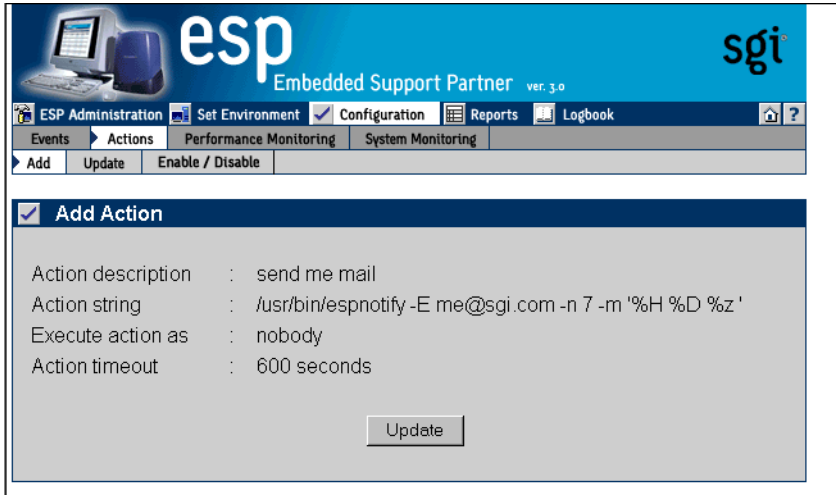


Figure 5-41 Confirmation Message for Adding an Action (Using Other Action Option)

Using the Command Line Interface

Use the following `espconfig` command syntax to add an action:

```
/usr/sbin/espconfig -add evaction  -acd <action description>
          -act <action string>
          [-user <name>]
          [-retry <count>]
          [-tout <timeout value>]
          [-throttle <throttle value>]
          [-enable | -disable]
```

Use the `-acd` option to specify a description of the action (a string enclosed in quotes).

Use the `-act` option to specify the command (a string enclosed in quotes) that the action performs.

Use the `-user` option to specify the UNIX user that executes the action. If you do not specify a user, ESP uses the default user `nobody`.

Use the `-retry` option to specify the number of times that ESP should perform the action before stopping. If you do not specify a value, ESP uses the default value 0.

Use the `-tout` option to specify the amount of time (in seconds) that ESP should wait for the action to execute. If the action does not complete before the timeout period expires, ESP kills the action command. If you do not specify a value, ESP uses the default value 0.

Use the `-throttle` option to specify the throttling value for the action, which specifies the number of times an event must occur before ESP performs the action. If you do not specify a value, ESP uses the default value 1.

Use the `-enable` option to enable the action, or use the `-disable` option to disable the action.

Updating Actions

You can update actions to customize them for your site.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to update an action:

1. Click on the `Configuration` button.
2. Click on the `Actions` button.
3. Click on the `Update` button.

   The interface displays the `Update Current Actions` window. (Refer to Figure 5-42.)

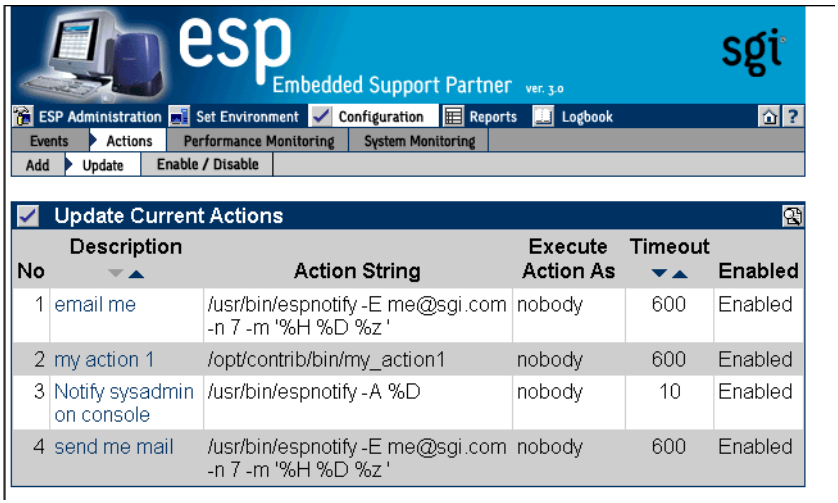


Figure 5-42 Update Current Actions Window

4. Click on the description of the action that you want to update.

   The interface displays the `Update Action` window. (Refer to Figure 5-43.)

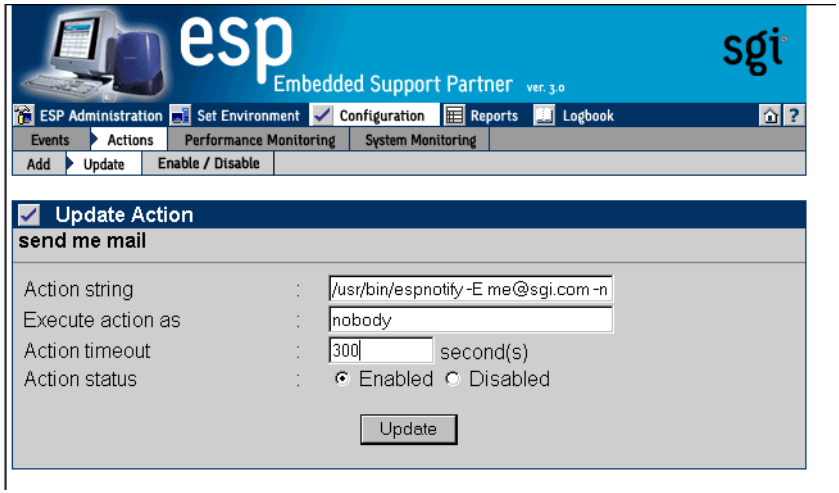


Figure 5-43 Update Action Window

5. Update the parameters.
6. Click on the `Update` button.

   The interface displays a verification window. (Refer to Figure 5-44.)

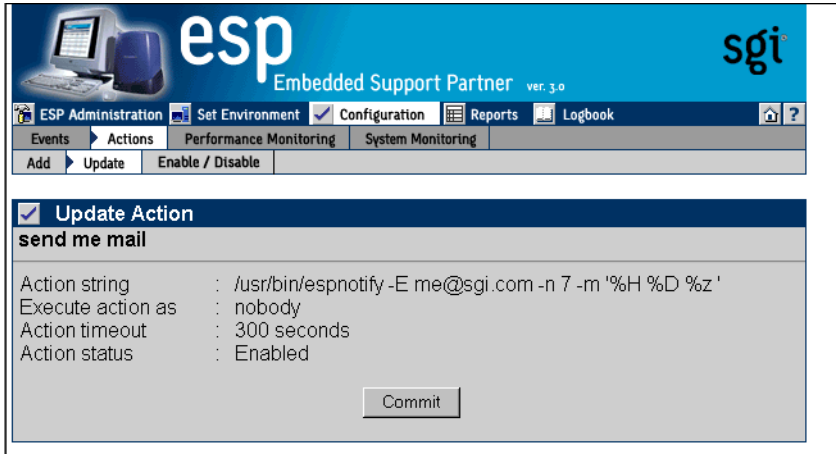


Figure 5-44 Verification Message for Updating an Action

7. Click on the `Commit` button.

   The interface displays a confirmation message. (Refer to Figure 5-45.) If you need to update the parameters again, click on the description of the action.

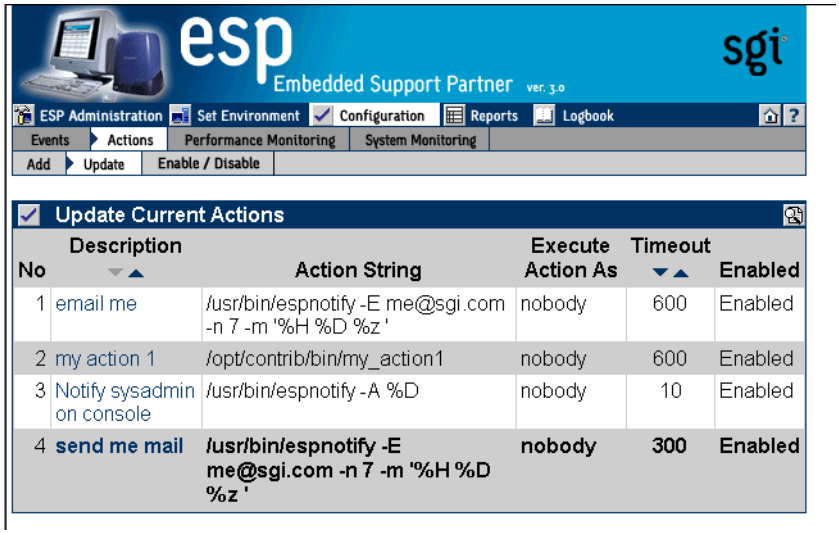


Figure 5-45 Confirmation Message for Updating an Action

Using the Command Line Interface

Use the following `espconfig` command syntax to update an action:

```
/usr/sbin/espconfig -update evaction
         {-acid <action id> [-acd <new action description>] |
         -acd <action description>}
         [-act <action string>]
         [-user <name>]
         [-retry <count>]
         [-tout <timeout value>]
         [-throttle <throttle value>]
         [-enable | -disable]
```

Use the `-acid` option to select an action by action ID. If you use the `-acd` option with the `-acid` option, this command updates the action description.

Use the `-acd` option to select an action by description (a string enclosed in quotes).

Note: If you do not specify any of the following options, ESP does not update the related action parameters.

Use the `-act` option to update the command (a string enclosed in quotes) that the action performs.

Use the `-user` option to update the UNIX user that executes the action.

Use the `-retry` option to update the number of times that ESP should perform the action before stopping.

Use the `-tout` option to update the amount of time (in seconds) that ESP should wait for the action to execute. If the action does not complete execution before the timeout period expires, ESP kills the action command.

Use the `-throttle` option to update the throttling value for the action, which specifies the number of times an event must occur before ESP performs the action.

Use the `-enable` option to enable the action, or use the `-disable` option to disable the action.

Disabling and Enabling Actions

You can disable actions that you no longer need to use. When you disable an action, ESP does not execute it when the events to which it is assigned are registered. Disabling an action allows you to prevent a specific action from occurring without modifying the individual event-action assignments. (You can also re-enable any actions that you disable.)

Note: ESP does not allow you to delete actions because deleting an action removes the historical data for the action from the ESP database.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to disable an action:

1. Click on the `Configuration` button.
2. Click on the `Actions` button.
3. Click on the `Enable/Disable` button.

   The interface displays the `View Current Actions` window. (Refer to Figure 5-46.)

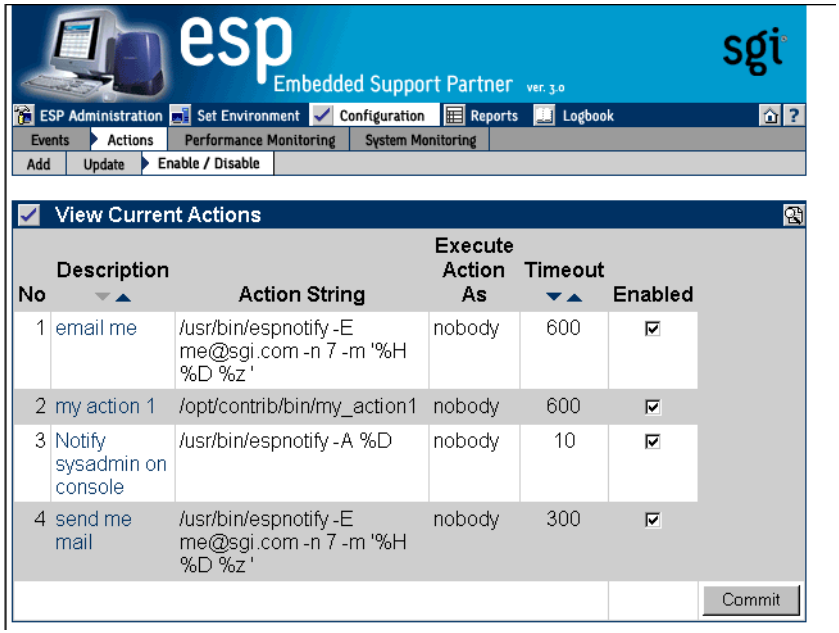


Figure 5-46 View Current Actions Window

4. Deselect the `Enabled` check mark.
5. Click on the `Commit` button.

Tip: To re-enable the action, perform the same procedure with the following difference: Set the `Enabled` check mark.

Using the Command Line Interface

Actions cannot be disabled from the command line interface.

Configuring Performance Monitoring

ESP monitors the performance of a system by evaluating a set of performance rules at specified time intervals. Performance monitoring is disabled by default.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to configure performance monitoring:

1. Click on the `Configuration` button.
2. Click on the `Performance Monitoring` button.

   Note: If the system is an SGM server, the interface displays a list of clients. (Refer to Figure 5-47.) Click on the client that you want to use, and click on the `Continue` button.

   The interface displays the `Performance Monitoring` window.

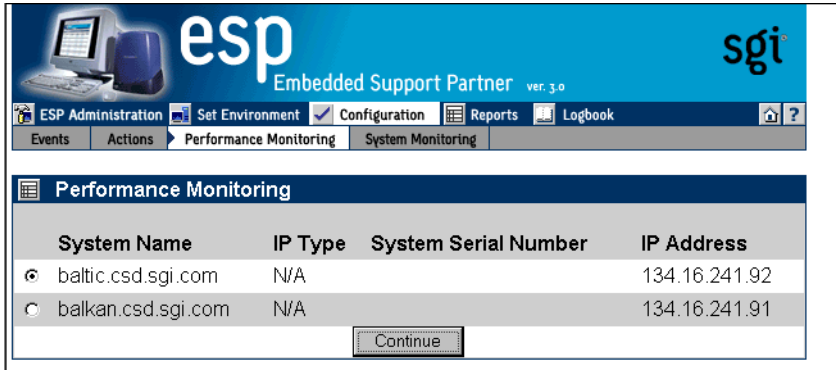


Figure 5-47 Performance Monitoring Window (with SGM Clients)

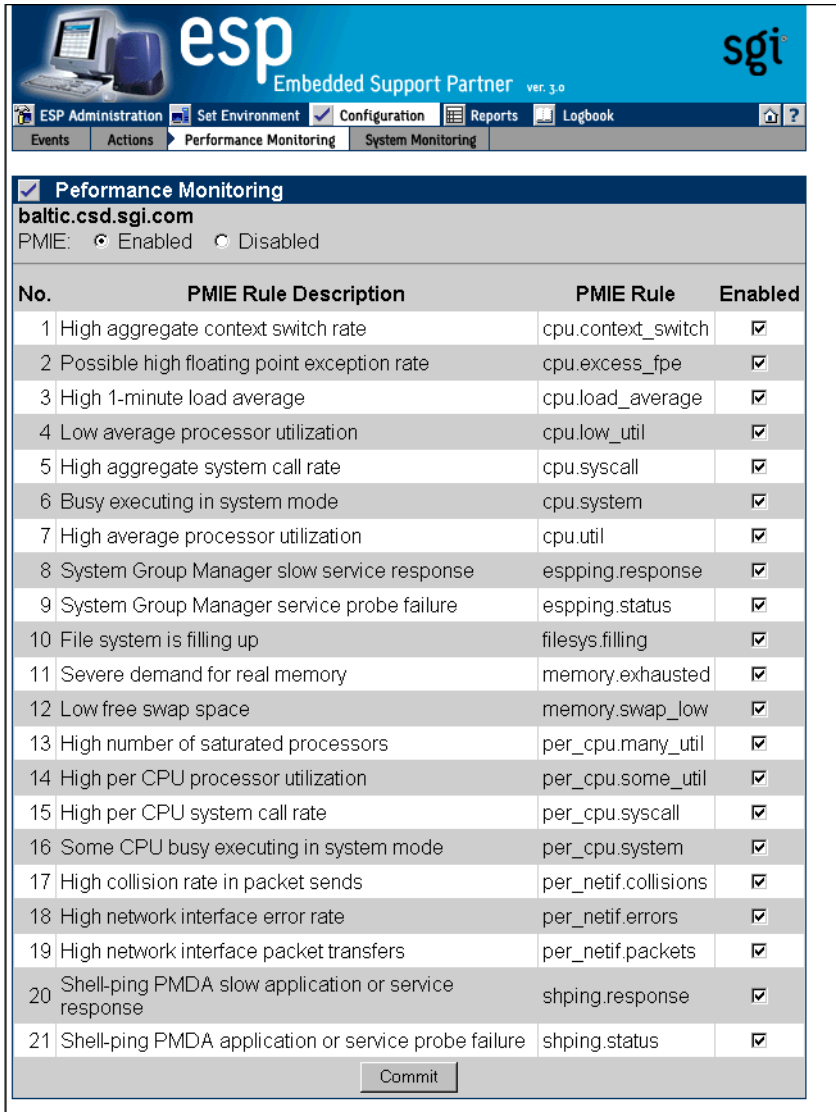


Figure 5-48 Performance Monitoring Window

3. Click on the `Enabled` radio button to enable performance monitoring or click on the `Disabled` radio button to disable performance monitoring.
4. Set the `Enabled` check marks for the PMIE rules that you want to enable.
5. Click on the `Update` button.

Table 5-4 describes the PMIE rules that are available and the performance issues that they detect. Refer to the *Performance Co-Pilot for IA-64 Linux User's and Administrator's Guide*, publication number 007-4580-00*x*, for more information about PMIE rules.

Table 5-4 PMIE Rules

Rule	Description	Performance Issue
cpu.context_switch	High aggregate context switch rate	The average number of context switches per CPU per second exceeded a threshold value.
cpu.excess_fpe	Possible high floating-point exception rate	Processes generating large numbers of floating-point exceptions (FPEs) were detected. Typically, this occurs when heavy system time is coupled with low system call rates. (Exceptions are delivered through the kernel to the process, taking some system time, but no system calls are serviced for the application.)
cpu.load_average	High 1-minute load average	The current 1-minute load average exceeded a threshold value. The load average measures the number of processes that are running, executable, or soon to be executed (for example, processes in short term sleep).
cpu.low_util	Low average processor utilization	The average processor utilization across all CPUs was below a threshold percentage. This rule is effectively the opposite of cpu.util and is disabled by default; it is useful only in specialized environments where, for example, processing is batch-oriented and low processor utilization is indicative of poor use of system resources. In such a situation, you should enable the cpu.low_util rule and disable the cpu.util rule.
cpu.syscall	High aggregate system call rate	The average number of system calls per CPU per second exceeded a threshold value.

Table 5-4 PMIE Rules **(continued)**

Rule	Description	Performance Issue
cpu.system	Busy executing in system mode	The average utilization per CPU exceeded a threshold value, and the ratio of system time to busy time exceeded a threshold value.
cpu.util	High average processor utilization	The average processor utilization across all CPUs exceeded a threshold value.
espping.response	System Group Manager slow service response	The amount of time required for a monitored service to complete exceeded a threshold value.
espping.status	System Group Manager service probe failure	A service that was being monitored by a group manager system failed or did not respond within a timeout period.
filesys.filling	File system is filling up	The amount of data in the filesystem exceeded a threshold value, and the remaining space in the filesystem is filling at a rate that exceeded a threshold value.
memory.exhausted	Severe demand for real memory	The rate at which the system is swapping modified pages out of main memory to the swap partitions exceeded a threshold value.
memory.swap_low	Low free swap space	The amount of swap space remaining reached a threshold value. Reduce the number and size of the running programs, or add more swap(1) space before it completely runs out.
per_cpu.many_util	High number of saturated processors	The processor utilization for a minimum number of CPUs exceeded a threshold value. This rule applies only to multiprocessor systems that have more than min_cpu_count processors. For single-processor systems, refer to the cpu.util rule. For multiprocessor systems with less than min_cpu_count processors, refer to the per_cpu.some_util rule.

Table 5-4 PMIE Rules **(continued)**

Rule	Description	Performance Issue
per_cpu.some_util	High per CPU processor utilization	The processor utilization for at least one CPU exceeded a threshold value. This rule applies only to multiprocessor systems with less than max_cpu_count processors. For single-processor systems, refer to the cpu.util rule. For multiprocessor systems with more than max_cpu_count processors, refer to the cpu.many_util rule.
per_cpu.syscall	High per CPU system call rate	The number of system calls per second for at least one CPU exceeded a threshold value. This rule applies only to multiprocessor systems. For single-processor systems, refer to the cpu.syscall rule.
per_cpu.system	Some CPU busy executing in system mode	At least one CPU was busy, and the ratio of system time to busy time exceeded a threshold value. This rule applies only to multiprocessor systems. For single-processor systems refer to the cpu.system rule.
per_netif.collisions	High collision rate in packet sends	The number of packets that are being sent across an interface and causing collisions exceeded a threshold value. Ethernet interfaces expect a certain number of packet collisions, but a high ratio of collisions to packet sends indicates a saturated network.
per_netif.errors	High network interface error rate	For at least one network interface, the error rate exceeded a threshold value.

Table 5-4 PMIE Rules **(continued)**

Rule	Description	Performance Issue
per_netif.packets	High network interface packet transfers	For at least one network interface, the average rate of packet transfers (in and/or out) exceeded a threshold value. This rule is disabled by default; the per_netif.util rule is more useful because it considers the reported bandwidth of each network interface. However, in some situations this value is zero; in that case, an absolute threshold-based rule like this one is more useful (for this reason it should be applied to some network interfaces, but not others; use the *interfaces* variable to filter this).
shping.response	Shell-ping PMDA slow application or service response	A response came from a shell-ping PMDA application or service probe
shping.status	Shell-ping PMDA application or service probe failure	A failure occurred in a shell-ping PMDA application or service probe

Using the Command Line Interface

You can use the `espconfig` command to configure performance monitoring.

- Use the following command syntax to enable performance monitoring:

  ```
  /usr/sbin/espconfig -on performance
  ```

- Use the following command syntax to disable performance monitoring:

  ```
  /usr/sbin/espconfig -off performance
  ```

- Use the following command syntax to list the current performance monitoring settings and PMIE rule settings:

  ```
  /usr/sbin/espconfig -list performance [-status|-enable|-disable]
  ```

  Use the `-status` option to list the current status (on or off) of performance monitoring on a system.

  Use the `-enable` option to list all PMIE that are currently enabled.

  Use the `-disable` option to list all PMIE that are currently disabled.

- Use the following command syntax to enable PMIE rules:

  ```
  /usr/sbin/espconfig -enable performance -pd {all|<pmie rule
  description>}
  ```

  Use the `all` option to enable all PMIE rules.

  Use the `<pmie rule description>` parameter to enable specific PMIE rules.

- Use the following command syntax to disable PMIE rules:

  ```
  /usr/sbin/espconfig -disable performance -pd {all|<pmie rule
  description}>
  ```

  Use the `all` option to disable all PMIE rules.

  Use the `<pmie rule description>` parameter to disable specific PMIE rules.

Configuring System Monitoring

You can configure ESP to monitor ICMP, DNS, X Window System server, RPCBIND, SMTP, NNTP, and PMCD services on the local system or on other systems in a group.

ESP uses Performance Co-Pilot software tools to monitor the services and to register any events in the Embedded Support Partner database. (The events belong to the `Performance` class; possible events include `System Group Manager service probe failure` and `System Group Manager slow service response`.)

System monitoring is disabled by default.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to configure system monitoring in single system manager mode:

1. Click on the `Configuration` button.
2. Click on the `System Monitoring` button.

   The interface displays the `System Monitoring` window. (Refer to Figure 5-49.)

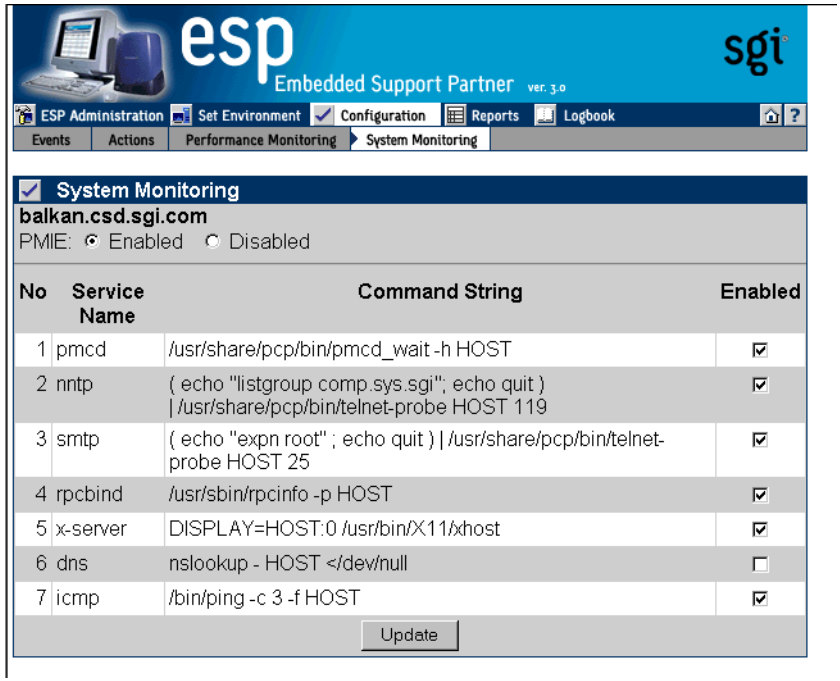


Figure 5-49 System Monitoring Window (Single System Manager Mode)

3. Click on the `Enabled` radio button to enable performance monitoring or click on the `Disabled` radio button to disable performance monitoring.
4. Click on the `Enabled` checkbox for each service that you want to monitor.
5. Click on the `Update` button.

   The interface displays a verification screen. (Refer to Figure 5-50.)

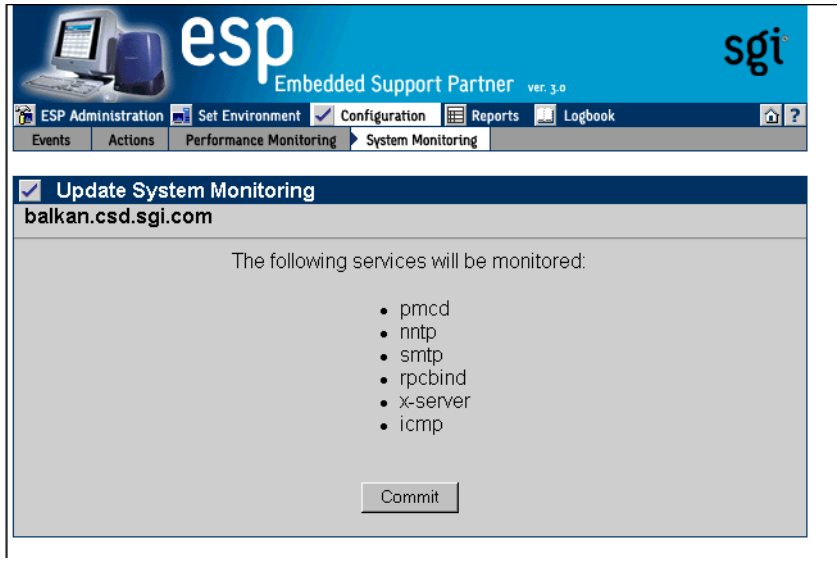


Figure 5-50 System Monitoring Change Verification Screen (Single System Manager Mode)

6. Click on the `Commit` button.

Figure 5-51 Updated System Monitoring Window (Single System Manager Mode)

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to configure system monitoring in system group manager mode:

1. Click on the `Configuration` button.
2. Click on the `System Monitoring` button.

   The interface displays the `System Monitoring` window. (Refer to Figure 5-52.)

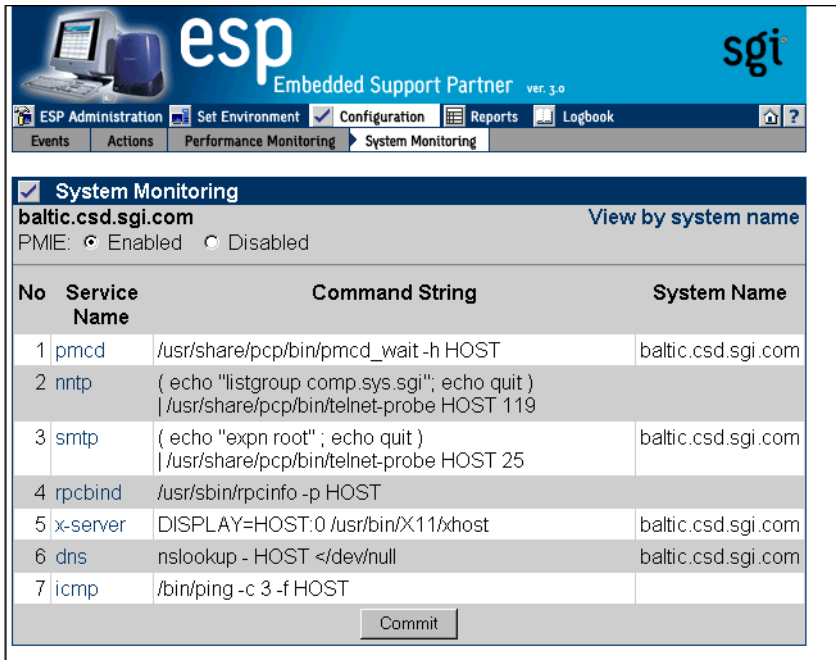


Figure 5-52 System Monitoring Window (System Group Manager Mode)

Note: To change the performance monitoring status, click on the `Enabled` radio button to enable performance monitoring or click on the `Disabled` radio button to disable performance monitoring, and click on the `Commit` button. (To perform system monitoring, performance monitoring must be enabled.)

3. Click on the name of the service that you want to monitor.

   The interface displays the `Update System Monitoring` window. (Refer to Figure 5-53.)

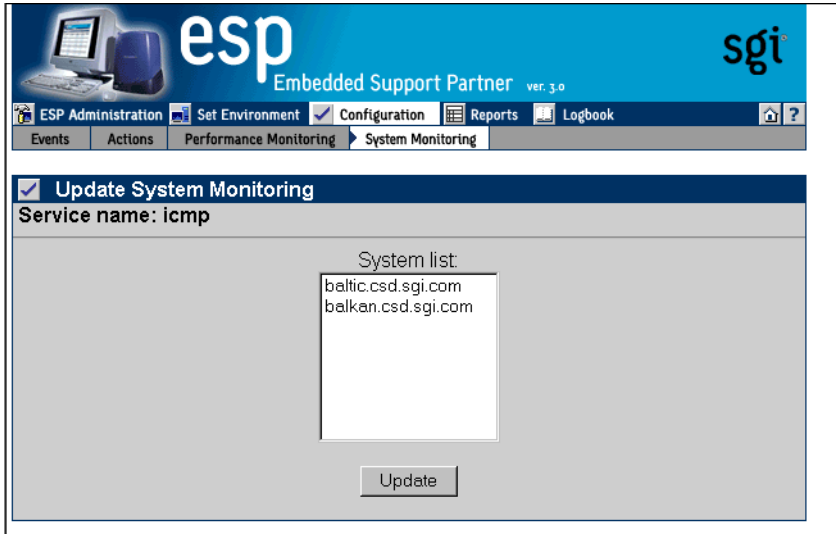


Figure 5-53 Update System Monitoring Window (System Group Manager Mode)

4. Click on the systems(s) that you want to monitor.
5. Click on the `Update` button.

   The interface displays a verification screen. (Refer to Figure 5-54.)

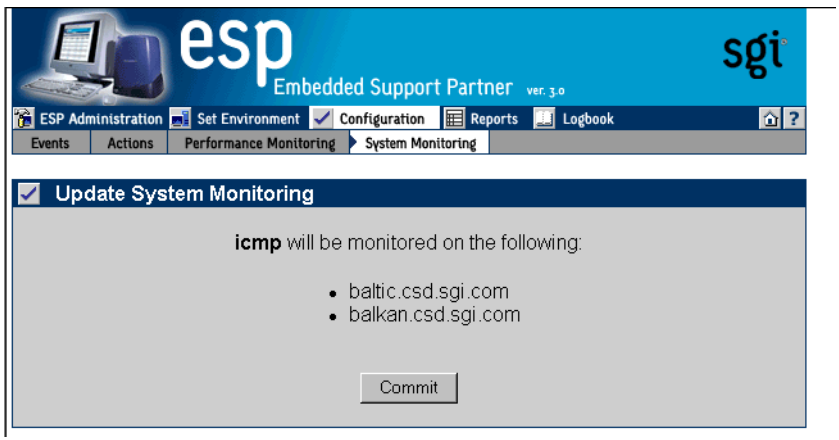


Figure 5-54 System Monitoring Change Verification Screen (System Group Manager Mode)

6. Click on the `Commit` button.

   The interface displays an updated `System Monitoring` window. (Refer to Figure 5-55.)

Figure 5-55 Updated System Monitoring Window (System Group Manager Mode)

Using the Command Line Interface

You can use the `espconfig` command to configure system monitoring.

- Use the following command syntax to list descriptions of services that are available for monitoring:

  ```
  /usr/sbin/espconfig monitor -list [<service list>]
  ```

  Use the `<service list>` parameter to specify which services to show. If you do not use the `<service list>` parameter, this command lists all services that are available on the system.

- Use the following the command syntax to show the hosts that are being monitored for selected services:

  ```
  /usr/sbin/espconfig monitor -show [<service list>] [-sgmclient <host list>]
  ```

  Use the `<service list>` parameter to specify which services to show. If you do not use the `<service list>` parameter, this command lists all services that are available on the system.

  Use the `-sgmclient` option to display services on one or more SGM clients. Use the `<host list>` parameter to specify the SGM clients to view.

- Use the following command syntax to enable monitoring of specific services:

  ```
  /usr/sbin/espconfig monitor -enable [<service list>] [-sgmclient [all|<host list>]]
  ```

  Use the `<service list>` parameter to specify which services to show. If you do not use the `<service list>` parameter, this command lists all services that are available on the system.

  Use the `-sgmclient` option to display services on one or more SGM clients. Use the `all` parameter to list services on all SGM clients. Use the `<host list>` parameter to list services on specific SGM clients.

- Use the following command syntax to disable monitoring of specific services:

  ```
  /usr/sbin/espconfig monitor -disable [<service list>] [-sgmclient [all|<host list>]]
  ```

  Use the `<service list>` parameter to specify which services to stop monitoring. If you do not use the `<service list>` parameter, this command disables all services that are currently monitored on the system.

  Use the `-sgmclient` option to display services on one or more SGM clients. Use the `all` parameter to list services on all SGM clients. Use the `<host list>` parameter to list services on specific SGM clients.

Viewing Reports

This chapter describes how to generate and view the following reports:

- Events registered reports
- Actions taken reports
- Availability reports
- Diagnostic reports
- Hardware reports
- Software reports
- System reports
- Site reports

About Reports

ESP generates reports based on parameters that you specify through the Web-based interface or command line interface.

In single system manager mode, ESP generates reports from the data that is stored in the ESP database on the local system. In system group manager mode, ESP generates reports from the information that is stored in the ESP database on the group manager system.

Figure 6-1 shows an example report generated by the Web-based interface. Figure 6-2 shows an example report generated by the Web-based interface in printable format.

No	Event Description	First Occurrence	Last Occurrence	Event Count	Syslog message
1	Daemon Error	08/13/2003 06:23:55	08/13/2003 06:23:55	1	warning: can't get client address: Transport endpoint is not connected
2	Daemon Error	08/13/2003 06:35:31	08/13/2003 06:35:31	1	warning: can't get client address: Transport endpoint is not connected
3	Daemon Error	08/13/2003 09:03:03	08/13/2003 09:03:03	1	warning: can't get client address: Transport endpoint is not connected
4	Daemon Error	08/13/2003 09:09:04	08/13/2003 09:09:04	1	warning: can't get client address: Transport endpoint is not connected

Figure 6-1 Example Report (Web-based Interface)

Event report for "Daemon Messages" class
From 08/13/2003 to 08/13/2003
System: baltic.csd.sgi.com

No.	Event Description	First Occurrence	Last Occurrence	Ev. Cnt	Syslog message
1	Daemon Error	08/13/2003 06:23:55	08/13/2003 06:23:55	1	warning: can't get client address: Transport endpoint is not connected
2	Daemon Error	08/13/2003 06:35:31	08/13/2003 06:35:31	1	warning: can't get client address: Transport endpoint is not connected
3	Daemon Error	08/13/2003 09:03:03	08/13/2003 09:03:03	1	warning: can't get client address: Transport endpoint is not connected
4	Daemon Error	08/13/2003 09:09:04	08/13/2003 09:09:04	1	warning: can't get client address: Transport endpoint is not connected

Figure 6-2 Example Report (Web-based Interface Printable Format)

If you use the Web-based interface to generate and view reports, there are several controls that you can use to navigate the reports. (Refer to Table 6-1.)

Table 6-1 Report Navigation Controls

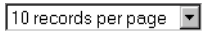
Control	Function
	Select the number of report entries (records) to show on a page
	Select the software application to view in a software inventory report
	Activate the selected menu options.
	Display the report in the printable format that shows an ASCII table with all report entries
	Expand all rows in the table to show subcomponents of each row

Table 6-1 Report Navigation Controls **(continued)**

Control	Function
	Contract all rows in the table to show only the top-level components
	Contract the current row
	Expand the current row to show all subcomponents of the component shown in the row
	Go to the last page of report
	Go to the next page of the report
	Go to the previous page of the report
	Go to the first page of the report
	Sort by this column ascending.
	Sort by this column descending.

Figure 6-3 shows an example report generated by the command line interface.

```
[root@baltic root]# espreport events -cid 7130 -from 08/13/2003 -to 08/13/2003

Event report by class for system "baltic.csd.sgi.com"
Class: (7130) - "Daemon Messages"
+----+------------------+------------+------------+---+--------------------------+
| ## | Type             |   First    |    Last    | # | Syslog message           |
+----+------------------+------------+------------+---+--------------------------+
| 1. | Daemon Error     | 08/13/2003 | 08/13/2003 | 1 | warning: can't get client |
|    |                  |  06:23:55  |  06:23:55  |   | address: Transport       |
|    |                  |            |            |   | endpoint is not connected |
+----+------------------+------------+------------+---+--------------------------+
| 2. | Daemon Error     | 08/13/2003 | 08/13/2003 | 1 | warning: can't get client |
|    |                  |  06:35:31  |  06:35:31  |   | address: Transport       |
|    |                  |            |            |   | endpoint is not connected |
+----+------------------+------------+------------+---+--------------------------+
| 3. | Daemon Error     | 08/13/2003 | 08/13/2003 | 1 | warning: can't get client |
|    |                  |  09:03:03  |  09:03:03  |   | address: Transport       |
|    |                  |            |            |   | endpoint is not connected |
+----+------------------+------------+------------+---+--------------------------+
| 4. | Daemon Error     | 08/13/2003 | 08/13/2003 | 1 | warning: can't get client |
|    |                  |  09:09:04  |  09:09:04  |   | address: Transport       |
|    |                  |            |            |   | endpoint is not connected |
+----+------------------+------------+------------+---+--------------------------+
[root@baltic root]#
```

Figure 6-3 Example Report (Command Line Interface)

Events Registered Reports

Event registered reports show all events that ESP has registered within a specific time period.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate an events registered report in single system manager mode:

1. Click on the `Reports` button.
2. Click on the `Events` button.

   The interface displays the `Event Reports` window. (Refer to Figure 6-4.)

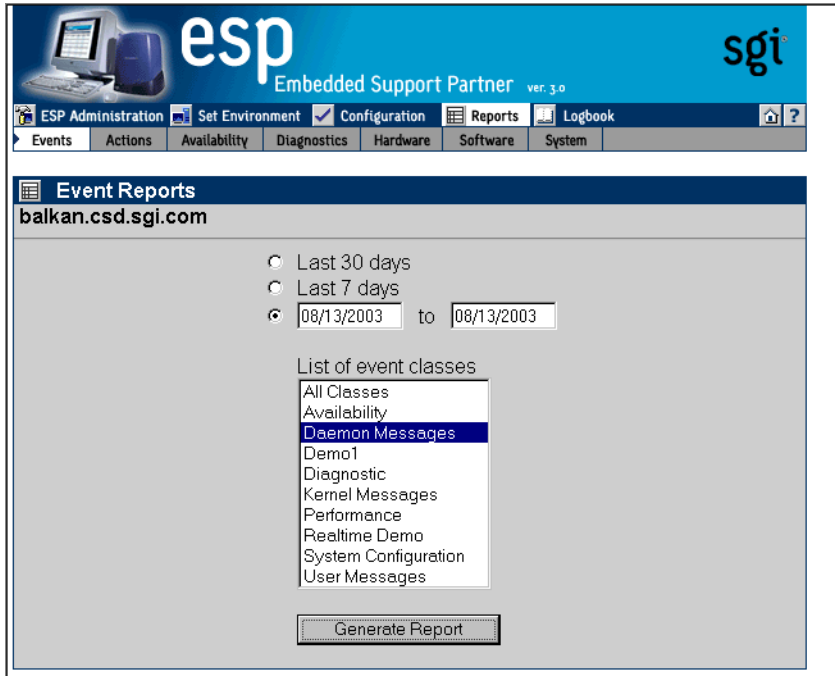
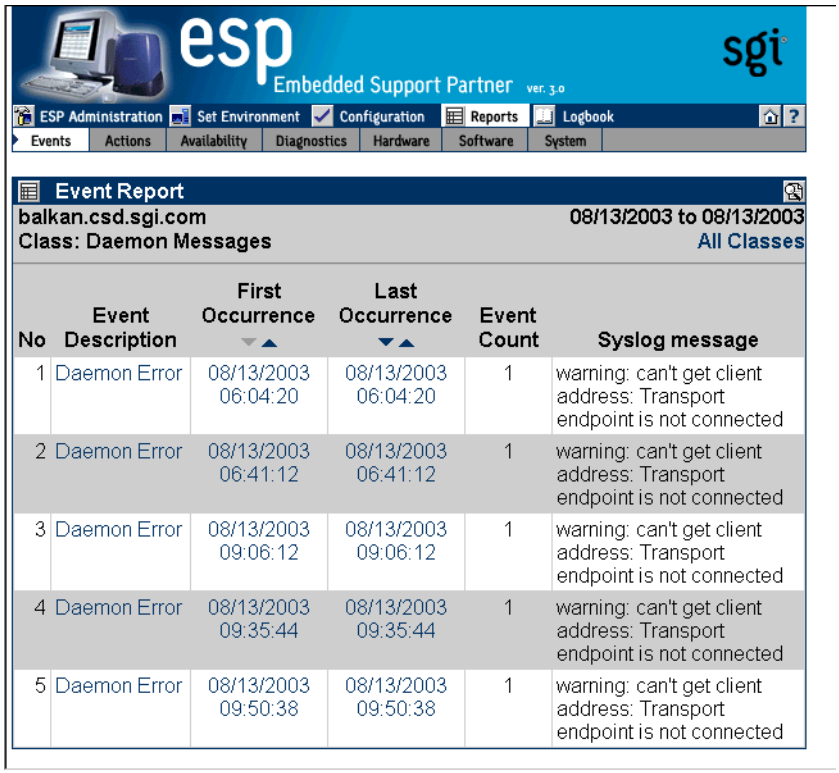


Figure 6-4 Event Reports Window (Single System Manager Mode)

3. Specify the range of dates for the report.
4. Select the event classes that the report should include.
5. Click on the `Generate Report` button.

Figure 6-5 shows an example event report.



No	Event Description	First Occurrence	Last Occurrence	Event Count	Syslog message
1	Daemon Error	08/13/2003 06:04:20	08/13/2003 06:04:20	1	warning: can't get client address: Transport endpoint is not connected
2	Daemon Error	08/13/2003 06:41:12	08/13/2003 06:41:12	1	warning: can't get client address: Transport endpoint is not connected
3	Daemon Error	08/13/2003 09:06:12	08/13/2003 09:06:12	1	warning: can't get client address: Transport endpoint is not connected
4	Daemon Error	08/13/2003 09:35:44	08/13/2003 09:35:44	1	warning: can't get client address: Transport endpoint is not connected
5	Daemon Error	08/13/2003 09:50:38	08/13/2003 09:50:38	1	warning: can't get client address: Transport endpoint is not connected

Figure 6-5 Example Events Registered Report (Single System Manager Mode)

Table 6-2 describes the information that the report contains.

Table 6-2 Events Registered Report Contents (Single System Manager Mode)

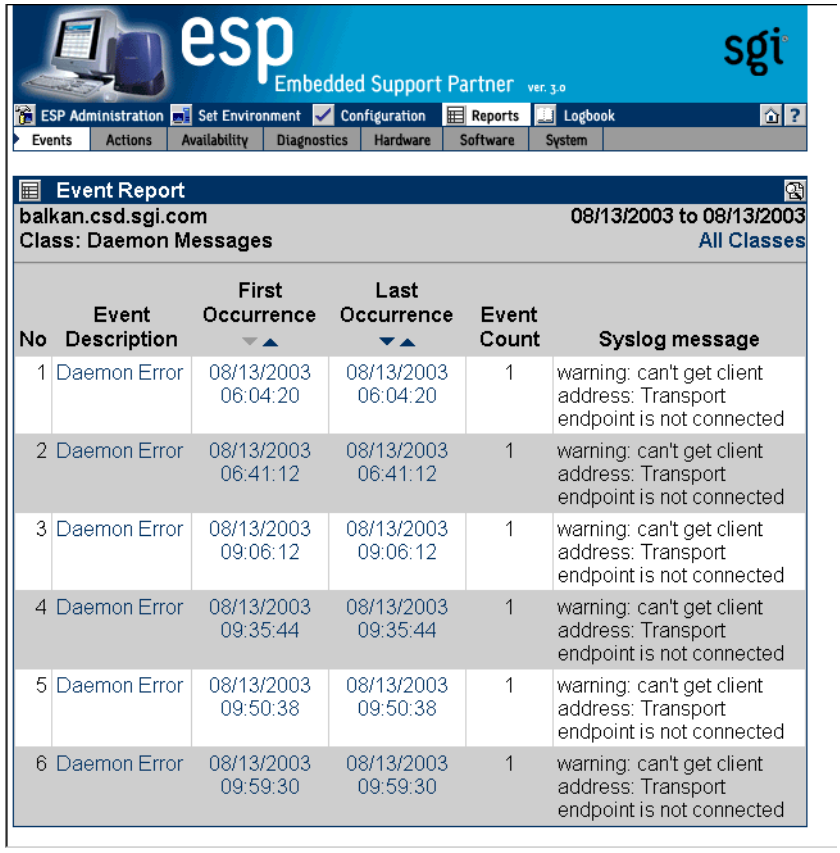
Column Heading	Description
`No.`	Index number within the table
`Class`[a]	The class that contains the event **Tip:** Click on an event class to view a report of all occurrences of events in that class.
`Event Description`	Brief description of the event **Tip:** Click on an event description to view a report of all occurrences of that event.
`First Occurrence`	Date and time at which the event was first registered **Tip:** Click on the occurrence date to view the logbook entry for that date.
`Last Occurrence`	Date and time at which the event was last registered **Tip:** Click on the occurrence date to view the logbook entry for that date.
`Event Count`	Number of times that the event occurred
`Syslog message`	Message from SYSLOG that generated the event

a. This column appears only if a report shows events from more than one class.

To "drill down" a report that contains events from multiple classes to find specific information about an event, perform the following procedure:

1. Click on the `Class` name.

   The interface displays information about events from the class that were registered. (Refer to Figure 6-6.)

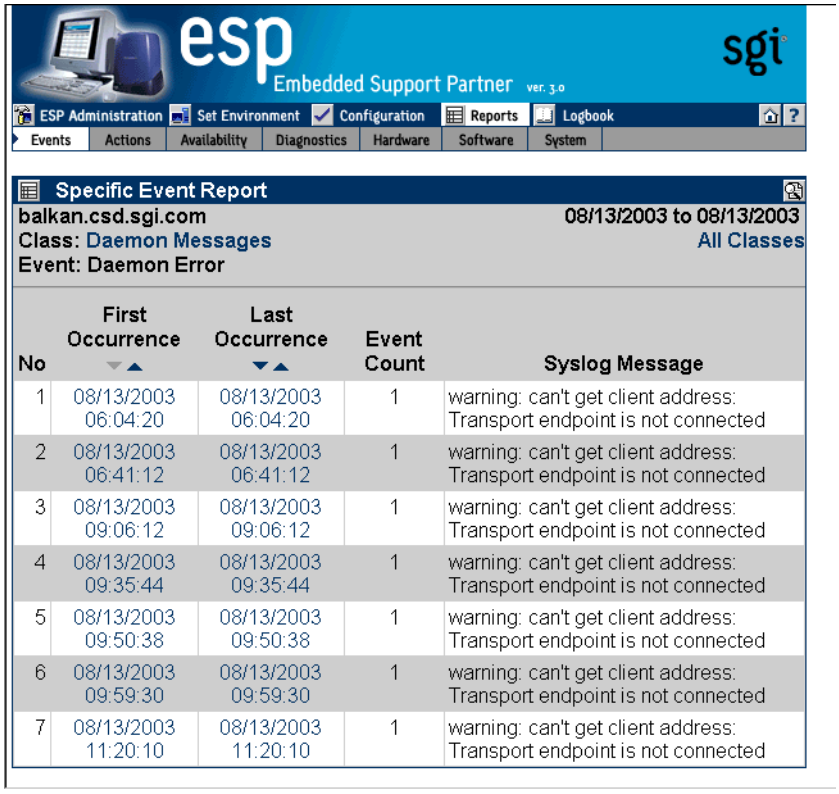


No	Event Description	First Occurrence	Last Occurrence	Event Count	Syslog message
1	Daemon Error	08/13/2003 06:04:20	08/13/2003 06:04:20	1	warning: can't get client address: Transport endpoint is not connected
2	Daemon Error	08/13/2003 06:41:12	08/13/2003 06:41:12	1	warning: can't get client address: Transport endpoint is not connected
3	Daemon Error	08/13/2003 09:06:12	08/13/2003 09:06:12	1	warning: can't get client address: Transport endpoint is not connected
4	Daemon Error	08/13/2003 09:35:44	08/13/2003 09:35:44	1	warning: can't get client address: Transport endpoint is not connected
5	Daemon Error	08/13/2003 09:50:38	08/13/2003 09:50:38	1	warning: can't get client address: Transport endpoint is not connected
6	Daemon Error	08/13/2003 09:59:30	08/13/2003 09:59:30	1	warning: can't get client address: Transport endpoint is not connected

Figure 6-6 Events Registered in a Specific Class (Single System Manager Mode)

2. Click on the `Event Description` for the event.

   The interface displays all occurrences of the event. (Refer to Figure 6-7.)



No	First Occurrence	Last Occurrence	Event Count	Syslog Message
1	08/13/2003 06:04:20	08/13/2003 06:04:20	1	warning: can't get client address: Transport endpoint is not connected
2	08/13/2003 06:41:12	08/13/2003 06:41:12	1	warning: can't get client address: Transport endpoint is not connected
3	08/13/2003 09:06:12	08/13/2003 09:06:12	1	warning: can't get client address: Transport endpoint is not connected
4	08/13/2003 09:35:44	08/13/2003 09:35:44	1	warning: can't get client address: Transport endpoint is not connected
5	08/13/2003 09:50:38	08/13/2003 09:50:38	1	warning: can't get client address: Transport endpoint is not connected
6	08/13/2003 09:59:30	08/13/2003 09:59:30	1	warning: can't get client address: Transport endpoint is not connected
7	08/13/2003 11:20:10	08/13/2003 11:20:10	1	warning: can't get client address: Transport endpoint is not connected

Figure 6-7 All Occurrences of a Specific Event (Single System Manager Mode)

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate an events registered report in system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Events` button.

   The interface displays the `Event Reports For System Group` window. (Refer to Figure 6-8.)

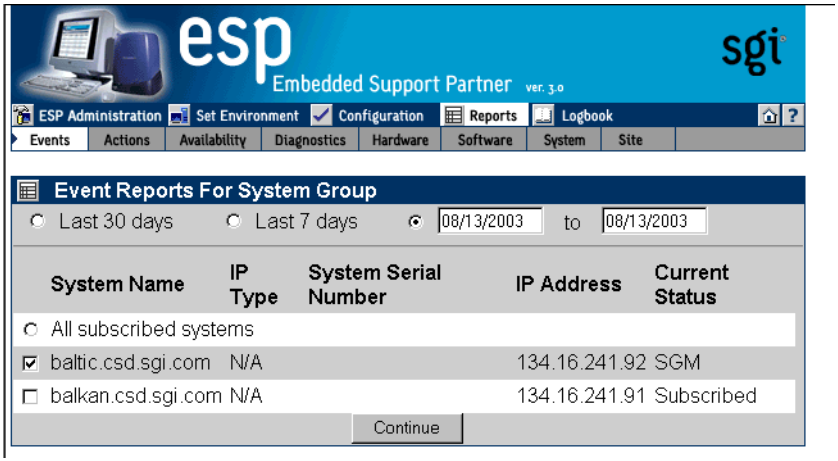


Figure 6-8 Event Reports for System Group Window (System Group Manager Mode)

3. Specify the range of dates for the report.
4. Select the systems to include in the report.
5. Click on the `Continue` button.

   The interface displays the list of classes. (Refer to Figure 6-9.)

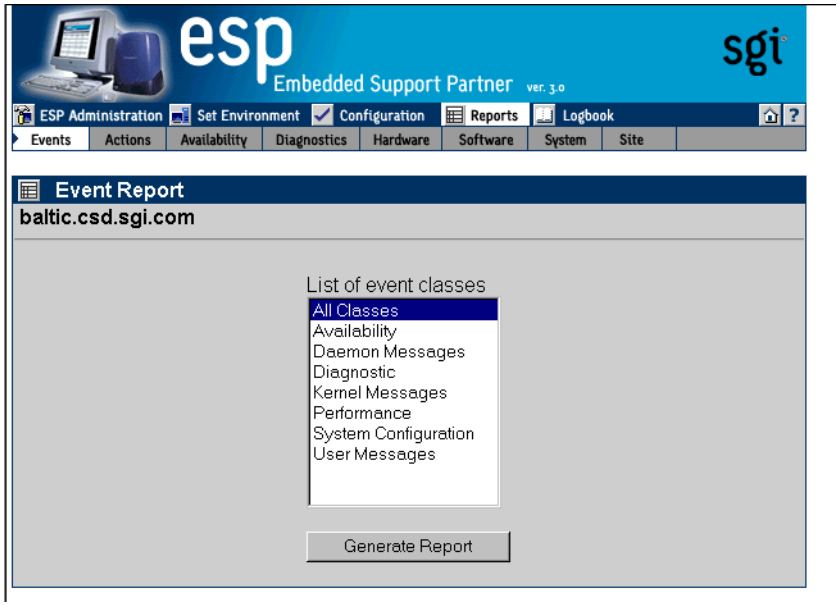
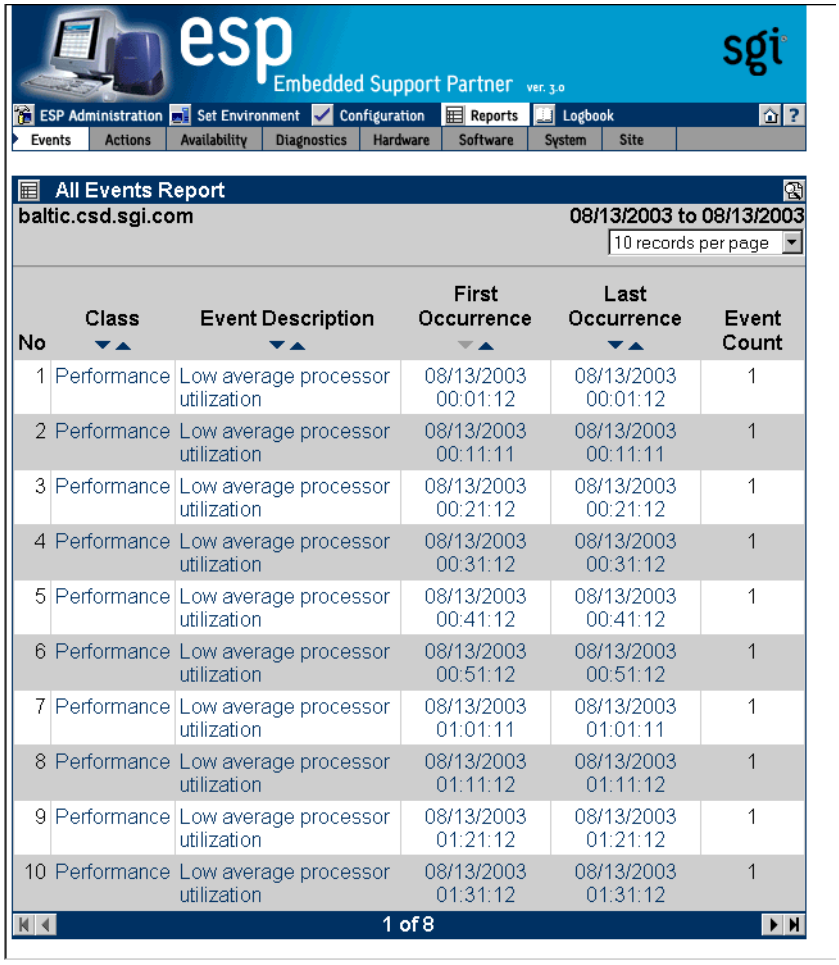


Figure 6-9 Event Reports Window with List of Classes (System Group Manager Mode)

6. Select the event classes to include in the report.
7. Click on the `Generate Report` button.

Figure 6-10 shows an example events registered report.



No	Class	Event Description	First Occurrence	Last Occurrence	Event Count
1	Performance	Low average processor utilization	08/13/2003 00:01:12	08/13/2003 00:01:12	1
2	Performance	Low average processor utilization	08/13/2003 00:11:11	08/13/2003 00:11:11	1
3	Performance	Low average processor utilization	08/13/2003 00:21:12	08/13/2003 00:21:12	1
4	Performance	Low average processor utilization	08/13/2003 00:31:12	08/13/2003 00:31:12	1
5	Performance	Low average processor utilization	08/13/2003 00:41:12	08/13/2003 00:41:12	1
6	Performance	Low average processor utilization	08/13/2003 00:51:12	08/13/2003 00:51:12	1
7	Performance	Low average processor utilization	08/13/2003 01:01:11	08/13/2003 01:01:11	1
8	Performance	Low average processor utilization	08/13/2003 01:11:12	08/13/2003 01:11:12	1
9	Performance	Low average processor utilization	08/13/2003 01:21:12	08/13/2003 01:21:12	1
10	Performance	Low average processor utilization	08/13/2003 01:31:12	08/13/2003 01:31:12	1

Figure 6-10 Example Events Registered Report (System Group Manager Mode)

Table 6-3 describes the information that the report contains.

Table 6-3 Events Registered Report Contents (System Group Manager Mode)

Column Heading	Description
`No.`	Index number within the table
`Class`[a]	The class that contains the event **Tip:** Click on an event class to view a report of all occurrences of events in that class.
`Event Description`	Brief description of the event **Tip:** Click on an event description to view a report of all occurrences of that event.
`First Occurrence`	Date and time at which the event was first registered **Tip:** Click on the occurrence date to view the logbook entry for that date.
`Last Occurrence`	Date and time at which the event was last registered **Tip:** Click on the occurrence date to view the logbook entry for that date.
`Event Count`	Number of times that the event occurred
`System Name`[b]	Client system on which the event occurred

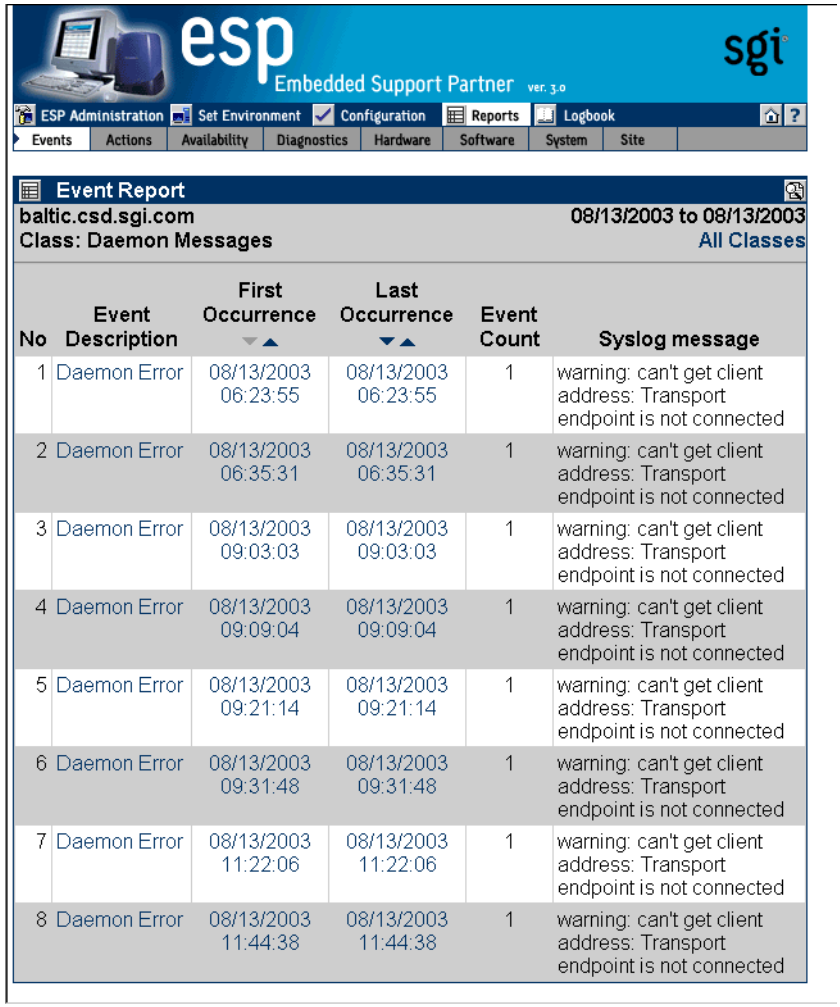
a. This column appears only when reports contain more than one event class.

b. This column appears only on SGM systems when reports contain more than one system.

To “drill down” a report to find specific information about an event, perform the following procedure:

1. Click on the `Class` name.

   The interface displays information about events from the class that were registered. (Refer to Figure 6-11.)



No	Event Description	First Occurrence	Last Occurrence	Event Count	Syslog message
1	Daemon Error	08/13/2003 06:23:55	08/13/2003 06:23:55	1	warning: can't get client address: Transport endpoint is not connected
2	Daemon Error	08/13/2003 06:35:31	08/13/2003 06:35:31	1	warning: can't get client address: Transport endpoint is not connected
3	Daemon Error	08/13/2003 09:03:03	08/13/2003 09:03:03	1	warning: can't get client address: Transport endpoint is not connected
4	Daemon Error	08/13/2003 09:09:04	08/13/2003 09:09:04	1	warning: can't get client address: Transport endpoint is not connected
5	Daemon Error	08/13/2003 09:21:14	08/13/2003 09:21:14	1	warning: can't get client address: Transport endpoint is not connected
6	Daemon Error	08/13/2003 09:31:48	08/13/2003 09:31:48	1	warning: can't get client address: Transport endpoint is not connected
7	Daemon Error	08/13/2003 11:22:06	08/13/2003 11:22:06	1	warning: can't get client address: Transport endpoint is not connected
8	Daemon Error	08/13/2003 11:44:38	08/13/2003 11:44:38	1	warning: can't get client address: Transport endpoint is not connected

Figure 6-11 Events Registered in a Specify Class (System Group Manager Mode)

2. Click on the `Event Description` for the event.

   The interface displays all occurrences of the event. (Refer to Figure 6-12.)

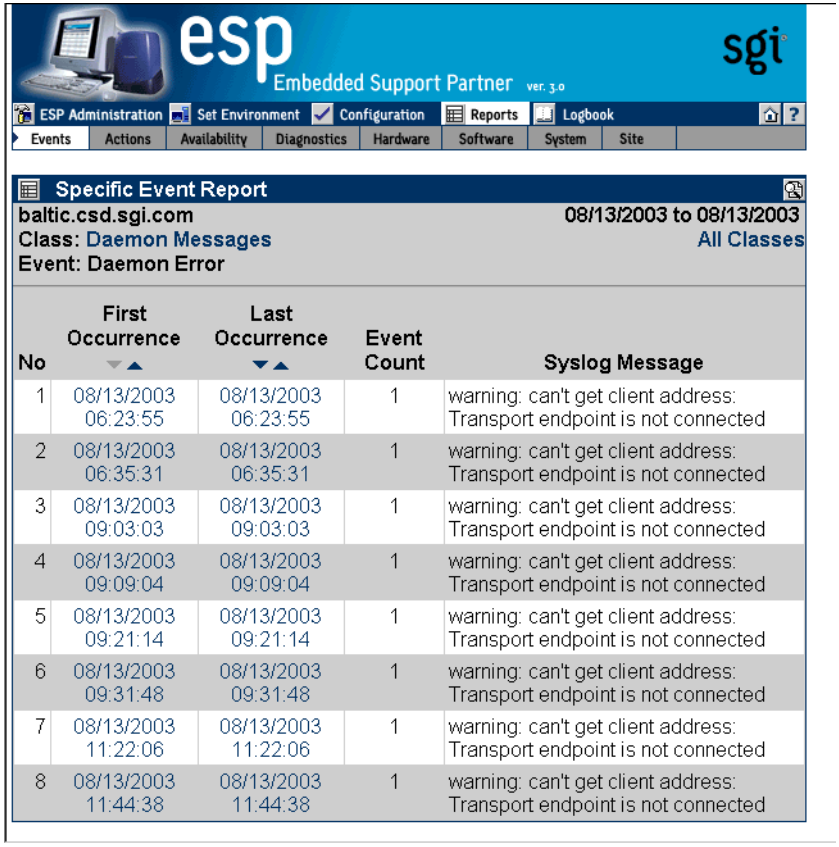


Figure 6-12 All Occurrences of a Specific Event (System Group Manager Mode)

Using the Command Line Interface

Use the following syntax of the `espreport` command to view an events registered report:

```
/usr/sbin/espreport events  [-sysid <system id>| -host <hostname>]
                            [-from mm/dd/yyyy] [-to mm/dd/yyyy]
                            [-tid <type id>  | -td <type desc>]
                            [-cid <class id>  | -cd <class desc>]
```

On group manager systems, use the `-sysid` or `-host` options to select a specific system to include in the report. If you do not specify a system, the report contains events from the local host.

Note: Enter **`/usr/sbin/esreport sysinfo all`** to determine the `<system id>` value.

Use the `-from` and `-to` options to select the range of dates for the report. If you do not specify a range of dates, the report, the report contains all events that have been registered.

Use the `-tid` and `-td` options to select a specific event type. If you do not specify an event type, the report includes all events.

Actions Taken Reports

Actions taken reports show all actions that ESP performed within a specific time period.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate an actions taken report in single system manager mode.

1. Click on the `Reports` button.
2. Click on the `Actions` button.

   The interface displays the `Action Reports` window. (Refer to Figure 6-13.)

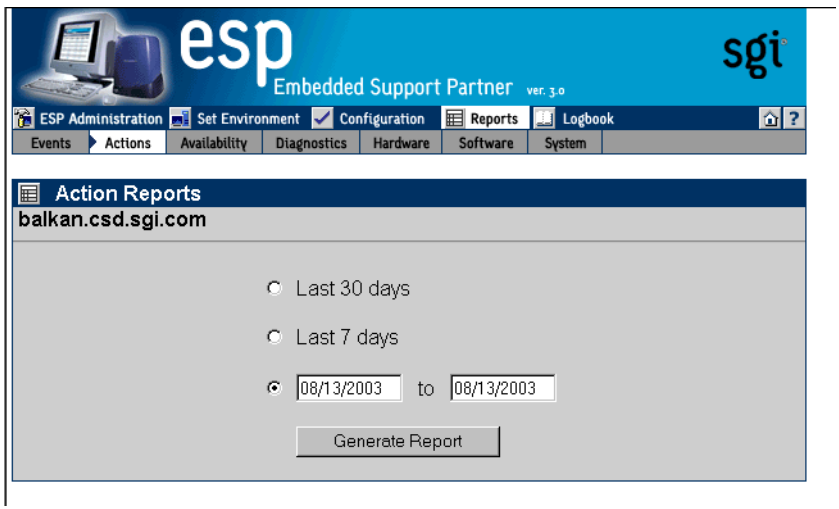


Figure 6-13 Action Reports Window (Single System Manager Mode)

3. Specify the range of dates for the report.
4. Click on the `Generate Report` button.

   Figure 6-14 shows an example actions taken report.

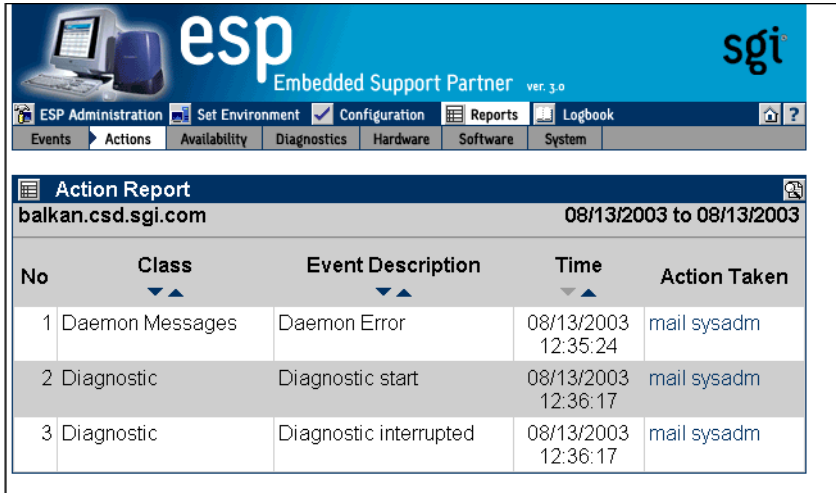


Figure 6-14 Example Actions Taken Report (Single System Manager Mode)

Table 6-4 describes the information that the report contains.

Table 6-4 Actions Taken Report Contents (Single System Manager Mode)

Column	Description
`No.`	Index number in the table
`Class`	Class of the event to which the action is assigned
`Event Description`	Description of the event to which the action is assigned
`Time`	Time and date at that the action was taken
`Action Taken`	Description of the command that the action performed **Tip:** Click on an action to view the parameter settings for the action.

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate an actions taken report in system group manager mode.

1. Click on the `Reports` button.
2. Click on the `Actions` button.

   The interface displays the `Actions Report For System Group` window. (Refer to Figure 6-15.)

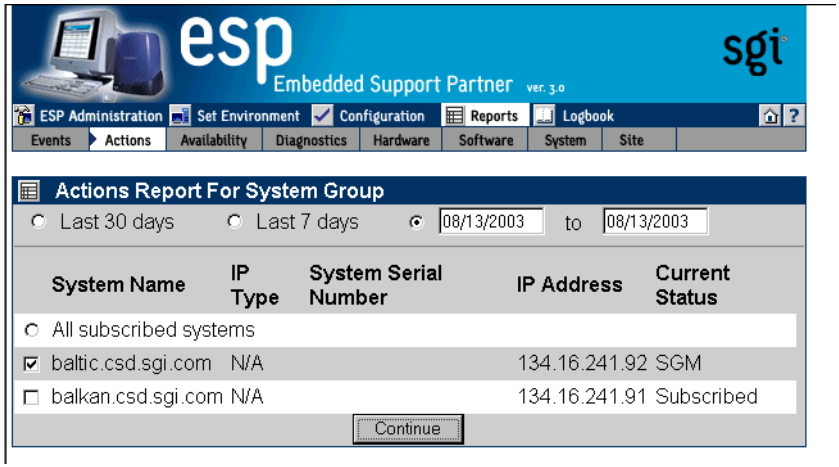


Figure 6-15 Actions Report for System Group Window (System Group Manager Mode)

3. Specify the range of dates for the report.
4. Select the systems to include in the report.
5. Click on the `Generate Report` button.

Figure 6-16 shows an example actions taken report.

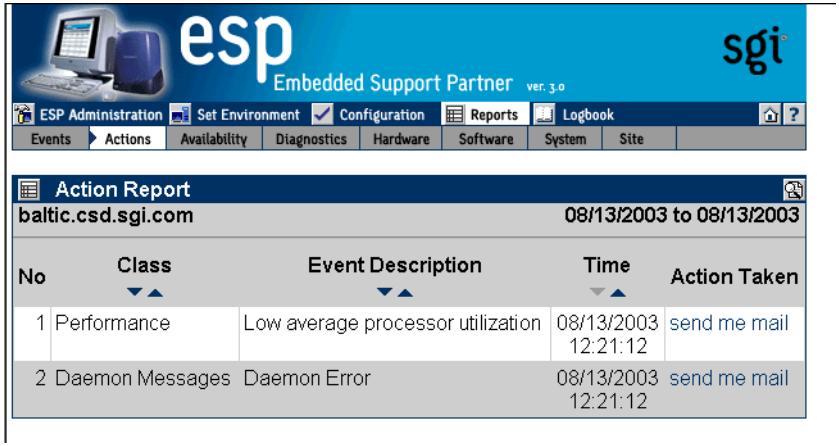


Figure 6-16 Example Actions Taken Report (System Group Manager Mode)

Table 6-5 describes the information that the report contains.

Table 6-5 Actions Taken Report Contents (System Group Manager Mode)

Column	Description
`No.`	Index number in the table
`Class`[a]	Class of the event to which the action is assigned
`Event Description`	Description of the event to which the action is assigned
`Time`	Time and date at that the action was taken
`Action Taken`	Description of the command that the action performed **Tip:** Click on an action to view the parameter settings for the action.
`System Name`[b]	Client system on which the event occurred

a. This column appears only when reports contain more than one event class.

b. This column appears only on SGM systems when reports contain more than one system.

Using the Command Line Interface

Use the following syntax of the `espreport` command to view an actions taken report:

```
/usr/sbin/espreport action_taken
                    [-sysid <system id> | -host <hostname>]
                    [-from mm/dd/yyyy] [-to mm/dd/yyyy]
```

Use the `-sysid` or `-host` options to select a specific system to include in the report. If you do not specify a system, the report contains actions from the local host.

Note: Enter **`/usr/sbin/esreport sysinfo all`** to determine the `<system id>` value.

Use the `-from` and `-to` options to select the range of dates for the report. If you do not specify a range of dates, the report displays all actions that have been taken.

Availability Reports

Availability reports provide statistics about system availability from a specified time period.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate availability reports in single system manager mode:

1. Click on the `Reports` button.
2. Click on the `Availability` button.

   The interface displays the `Availability Reports` window. (Refer to Figure 6-17.)

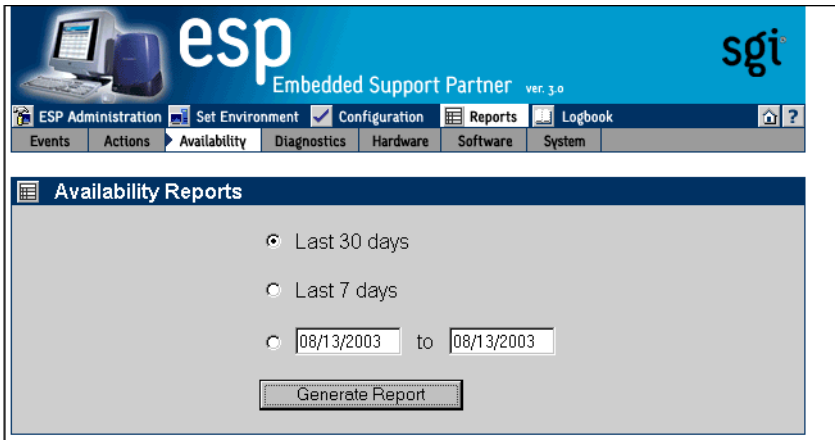


Figure 6-17 Availability Reports Window (Single System Mode)

3. Specify the range of dates for the report.
4. Click on the `Generate Report` button.

   Figure 6-18 shows an example availability report.

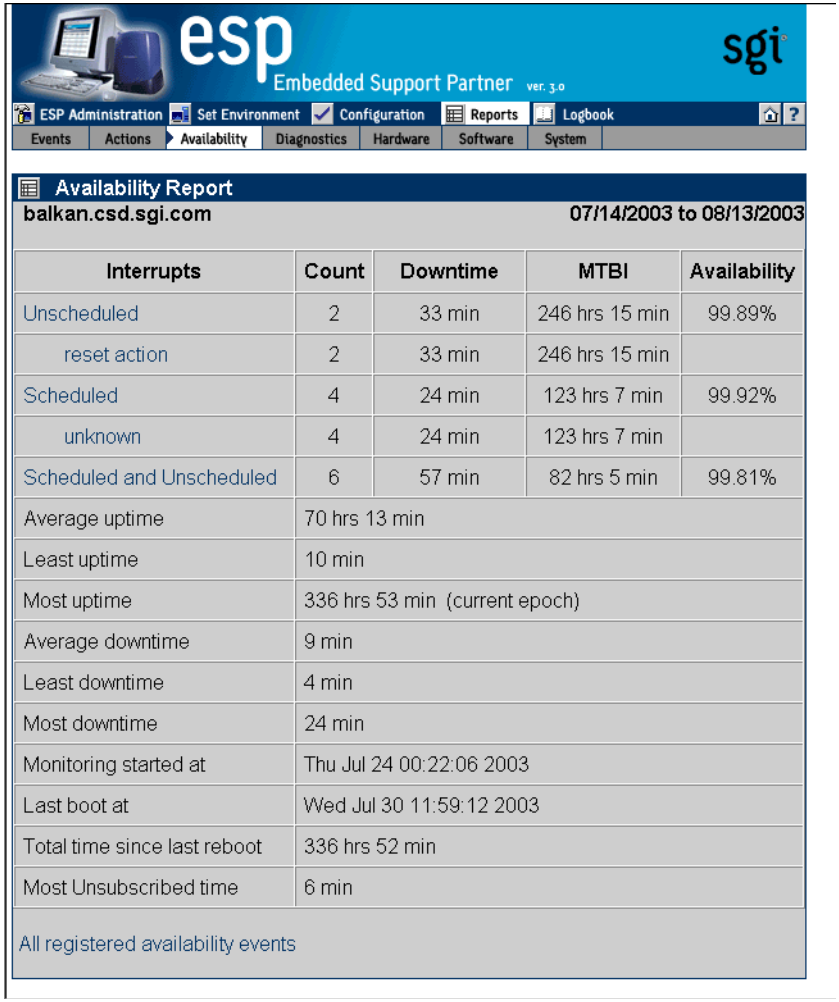


Figure 6-18 Example Availability Report (Single System Manager Mode)

Table 6-6 describes the contents of the report.

Table 6-6 Single System Availability Report Contents (Single System Manager Mode)

Row	Description
`Unscheduled`	Information about any unscheduled downtime events: count, downtime due to the event (in minutes), mean time between interrupts (in minutes), and availability percentage
`Scheduled`	Information about scheduled downtime events: count, downtime caused by the service action (in minutes), mean time between interrupts (in minutes), and availability percentage **Tip:** Click on the link to view a report of all scheduled availability events that ESP registered during the time period.
`Scheduled and Unscheduled`	Information about the total downtime for scheduled and unscheduled downtime: count, downtime (in minutes) caused by the action, mean time between interrupts (in minutes), and availability percentage **Tip:** Click on the link to view a report of all scheduled and unscheduled availability events that ESP registered during the time period.
`Average uptime`	Average uptime between availability events
`Least uptime`	Shortest uptime between availability events
`Most uptime`	Longest uptime between availability events
`Average downtime`	Average downtime
`Least downtime`	Shortest downtime
`Most downtime`	Longest downtime
`Logging started at`	Date and time that ESP began monitoring availability events
`Last boot at`	Date and time of last system boot
`System has been up for`	Length of time that system has been powered up since last system boot
`All registered availability events`	Link to a table of all availability events that ESP registered during the specified time period

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate availability reports in system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Availability` button.

   The interface displays the `Availability Reports For System Group` window. (Refer to Figure 6-19.)

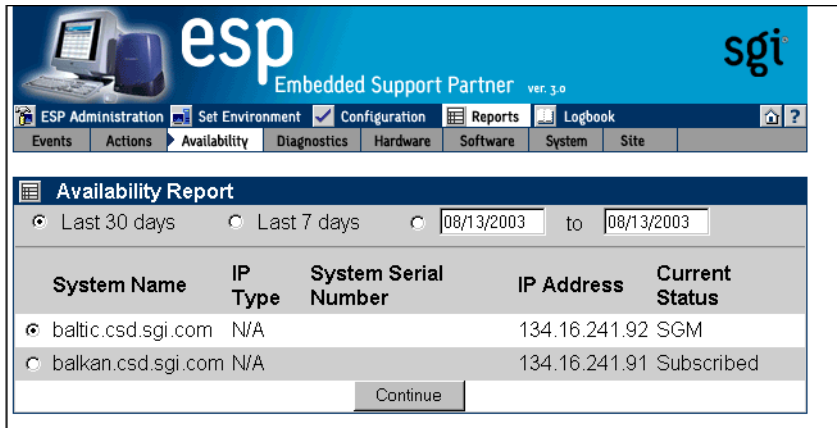
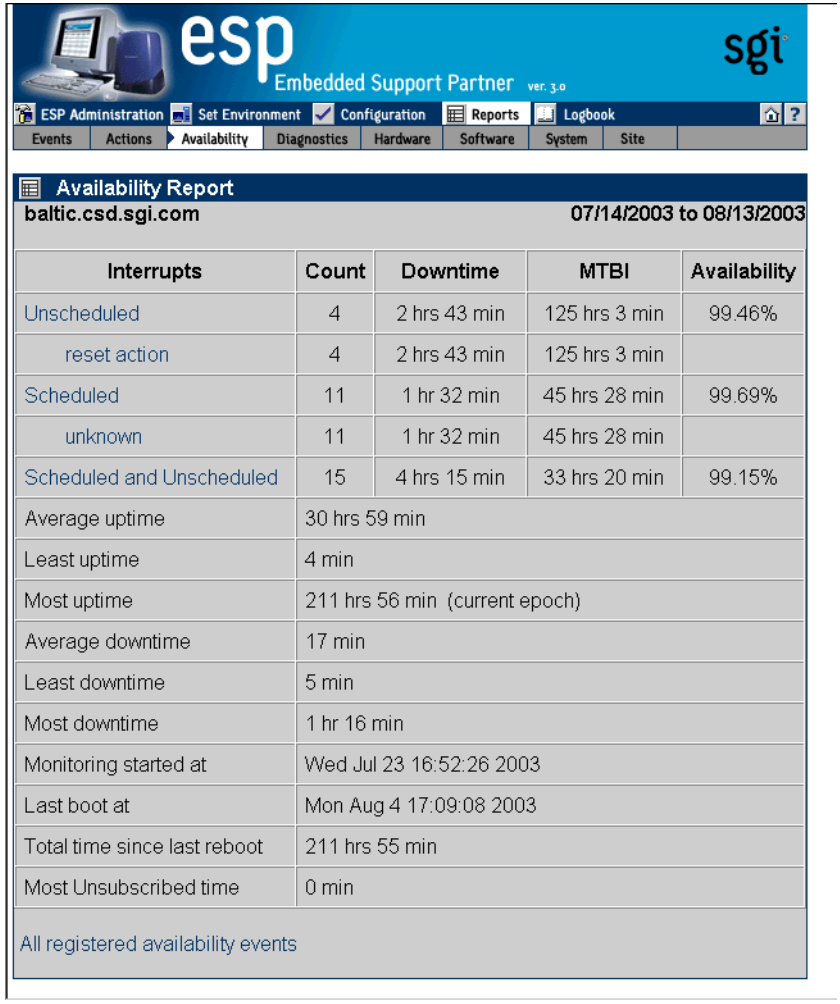


Figure 6-19 Availability Reports for System Group Window (System Group Manager Mode)

3. Specify the range of dates for the report.
4. Select the systems to include in the report.
5. Click on the `Generate Report` button.

   Figure 6-20 shows an example availability report for a specific host.



Interrupts	Count	Downtime	MTBI	Availability
Unscheduled	4	2 hrs 43 min	125 hrs 3 min	99.46%
reset action	4	2 hrs 43 min	125 hrs 3 min	
Scheduled	11	1 hr 32 min	45 hrs 28 min	99.69%
unknown	11	1 hr 32 min	45 hrs 28 min	
Scheduled and Unscheduled	15	4 hrs 15 min	33 hrs 20 min	99.15%
Average uptime	30 hrs 59 min			
Least uptime	4 min			
Most uptime	211 hrs 56 min (current epoch)			
Average downtime	17 min			
Least downtime	5 min			
Most downtime	1 hr 16 min			
Monitoring started at	Wed Jul 23 16:52:26 2003			
Last boot at	Mon Aug 4 17:09:08 2003			
Total time since last reboot	211 hrs 55 min			
Most Unsubscribed time	0 min			

All registered availability events

Figure 6-20 Example Availability Report for a Specific Host (System Group Manager Mode)

Table 6-7 describes the contents of the report.

Table 6-7 Single System Availability Report Contents (System Group Manager Mode)

Row	Description
`Unscheduled`	Information about any unscheduled downtime events: count, downtime due to the event (in minutes), mean time between interrupts (in minutes), and availability percentage
`Scheduled`	Information about scheduled downtime events: count, downtime caused by the service action (in minutes), mean time between interrupts (in minutes), and availability percentage **Tip:** Click on the link to view a report of all scheduled availability events that ESP registered during the time period.
`Scheduled and Unscheduled`	Information about the total downtime for scheduled and unscheduled downtime: count, downtime (in minutes) caused by the action, mean time between interrupts (in minutes), and availability percentage **Tip:** Click on the link to view a report of all scheduled and unscheduled availability events that ESP registered during the time period.
`Average uptime`	Average uptime between availability events
`Least uptime`	Shortest uptime between availability events
`Most uptime`	Longest uptime between availability events
`Average downtime`	Average downtime
`Least downtime`	Shortest downtime
`Most downtime`	Longest downtime
`Logging started at`	Date and time that ESP began monitoring availability events
`Last boot at`	Date and time of last system boot
`System has been up for`	Length of time that system has been powered up since last system boot
`All registered availability events`	Link to a table of all availability events that ESP registered during the specified time period

Using the Command Line Interface

Use the following syntax of the `espreport` command to view an availability report:

```
/usr/sbin/espreport availability
                        [-sysid <system id>|-host <hostname>]
                        [-from mm/dd/yyyy] [-to mm/dd/yyyy]
```

Use the `-sysid` or `-host` options to select a specific system to include in the report. If you do not specify a system, the report contains availability information from the local host.

Use the `-from` and `-to` options to select the range of dates for the report. If you do not specify a range of dates, the report contains all information up to the current date.

Diagnostic Result Reports

If you use the diagnostics that are included in the *Internal Support Tools* 2.0 or later releases, ESP generates diagnostic results reports.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate a diagnostic results report in single system manager mode:

1. Click on the `Reports` button.
2. Click on the `Diagnostics` button.

   The interface displays the `Diagnostic Results` window. (Refer to Figure 6-21.)

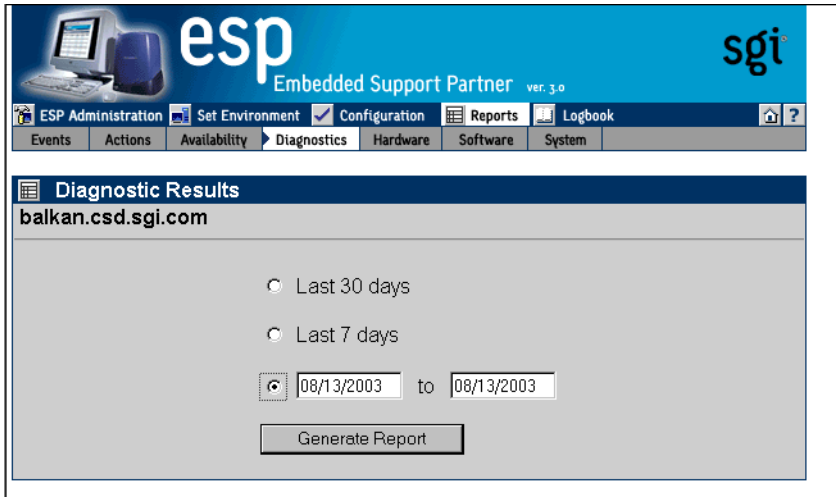


Figure 6-21 Diagnostic Results Window (Single System Manager Mode)

3. Specify the range of dates for the report.
4. If you are using system group manager mode, select the systems to include in the report.
5. Click on the `Generate Report` button.

   Figure 6-22 shows an example diagnostic results report.

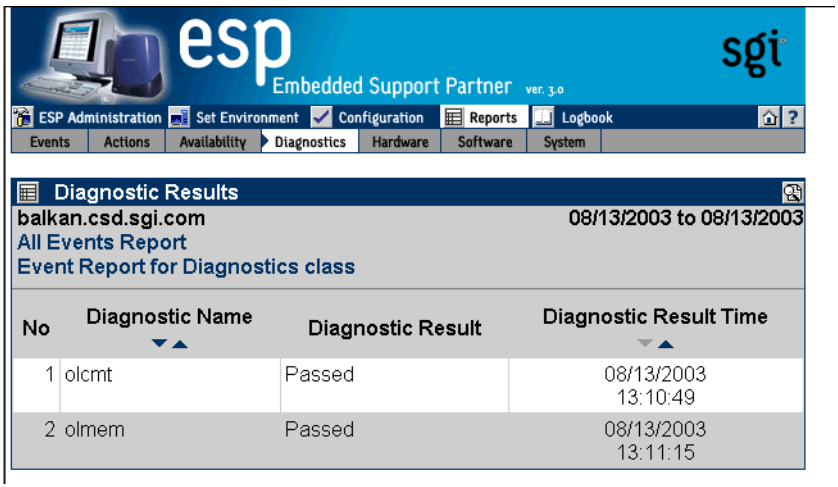


Figure 6-22 Example Diagnostic Results Report (Single System Manager Mode)

Table 6-8 describes the contents of the report.

Table 6-8 Diagnostic Results Report Contents (Single System Manager Mode)

Column Heading	Description
`No.`	Index number within the table
`Diagnostic Name`	Name of the diagnostic When one or more tests run as a group under one program (for example, SVP), the total number of tests run is shown in parentheses next to the diagnostic name; for example: `SVP (86)` indicates that 86 tests ran under SVP

Table 6-8 Diagnostic Results Report Contents (Single System Manager Mode) **(continued)**

Column Heading	Description
`Diagnostic Result`	Result of the diagnostic: `PASS`, `FAIL`, or `COMPLETE` `PASS` indicates that the diagnostic completed successfully `FAIL` indicates that the diagnostic failed `COMPLETE` indicates that multiple tests ran and one or more of them failed and the others passed
`Diagnostic Result Time`	Time at which the diagnostic completed testing When multiple tests run under one diagnostic (for example, SVP), this column indicates the time at which all tests completed

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate a diagnostic results report in system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Diagnostics` button.

   The interface displays the `Diagnostic Results` window. (Refer to Figure 6-23.)

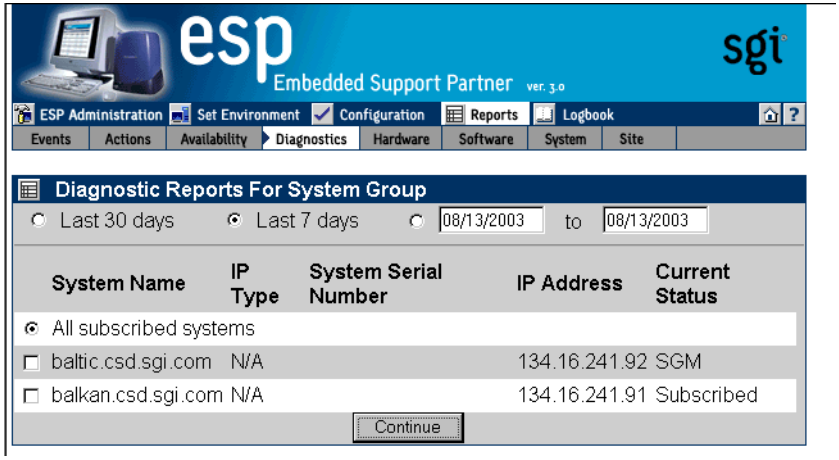


Figure 6-23 Diagnostic Results Window (System Group Manager Mode)

3. Specify the range of dates for the report.
4. Specify the systems to include in the report.
5. Click on the `Generate Report` button.

   Figure 6-24 shows an example diagnostic results report.

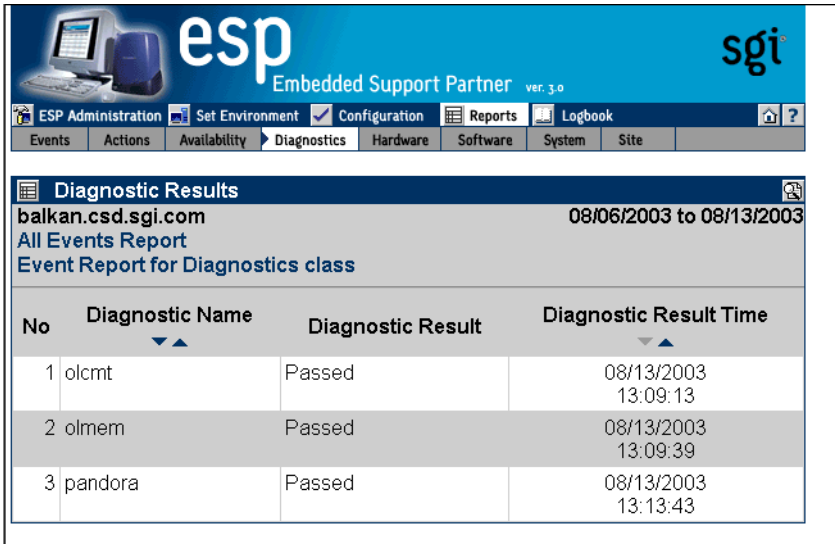


Figure 6-24 Example Diagnostic Results Report (System Group Manager Mode)

Table 6-9 describes the contents of the report.

Table 6-9 Diagnostic Results Report Contents (System Group Manager Mode)

Column Heading	Description
`No.`	Index number within the table
`Diagnostic Name`	Name of the diagnostic When one or more tests run as a group under one program (for example, SVP), the total number of tests run is shown in parentheses next to the diagnostic name; for example: `SVP (86)` indicates that 86 tests ran under SVP
`Diagnostic Result`	Result of the diagnostic: `PASS`, `FAIL`, or `COMPLETE` `PASS` indicates that the diagnostic completed successfully `FAIL` indicates that the diagnostic failed `COMPLETE` indicates that multiple tests ran and one or more of them failed and the others passed
`Diagnostic Result Time`	Time at which the diagnostic completed testing When multiple tests run under one diagnostic (for example, SVP), this column indicates the time at which all tests completed
`System Name`	Client system on which the action was taken

Using the Command Line Interface

Diagnostic reports are not available from the command line interface.

Hardware Reports

There are two types of hardware reports:

- Hardware inventory reports
- Hardware changes reports

Hardware Inventory Reports

Hardware inventory reports show all hardware installed in a system at a specific date and time.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate a hardware inventory report in single system manager mode:

1. Click on the `Reports` button.
2. Click on the `Hardware` button.

   The interface displays the `Hardware Inventory Report` window. (Refer to Figure 6-25.)

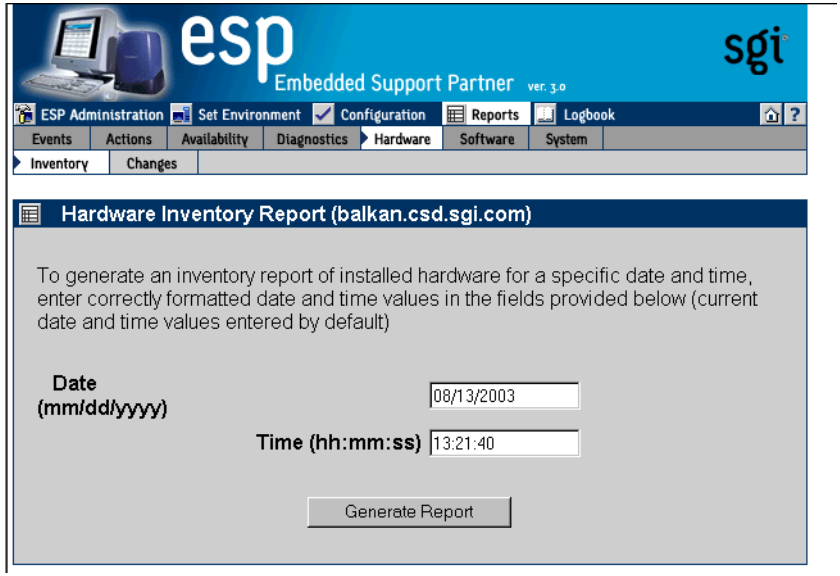
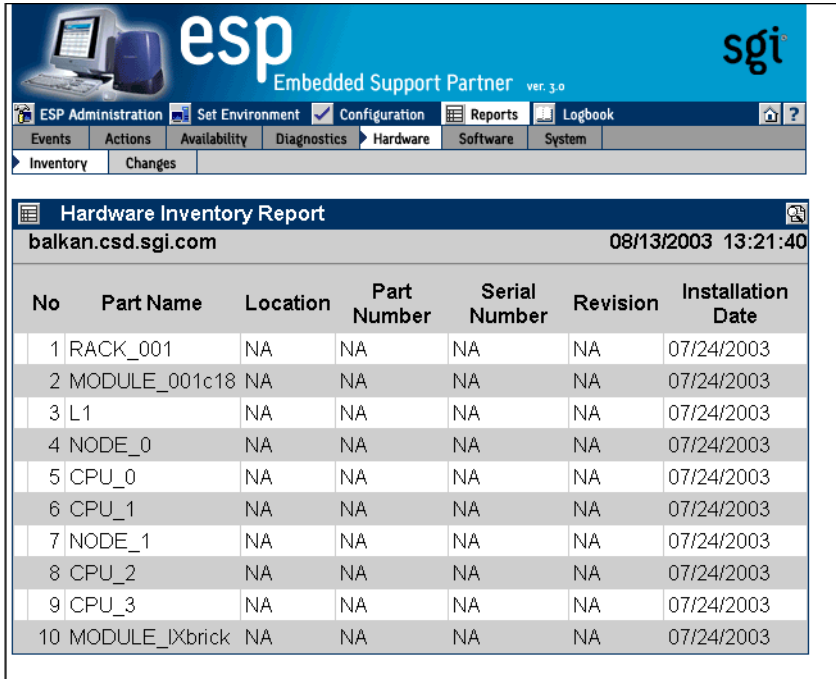


Figure 6-25 Hardware Inventory Report Window (Single System Manager Mode)

3. Specify the date and time of the hardware inventory that you want to view.
4. Click on the `Generate Report` button.

   Figure 6-26 shows an example hardware inventory report.



No	Part Name	Location	Part Number	Serial Number	Revision	Installation Date
1	RACK_001	NA	NA	NA	NA	07/24/2003
2	MODULE_001c18	NA	NA	NA	NA	07/24/2003
3	L1	NA	NA	NA	NA	07/24/2003
4	NODE_0	NA	NA	NA	NA	07/24/2003
5	CPU_0	NA	NA	NA	NA	07/24/2003
6	CPU_1	NA	NA	NA	NA	07/24/2003
7	NODE_1	NA	NA	NA	NA	07/24/2003
8	CPU_2	NA	NA	NA	NA	07/24/2003
9	CPU_3	NA	NA	NA	NA	07/24/2003
10	MODULE_IXbrick	NA	NA	NA	NA	07/24/2003

Figure 6-26 Example Hardware Inventory Report (Single System Manager Mode)

Table 6-10 describes the contents of the report.

Table 6-10 Hardware Inventory Report Contents

Column Heading	Description
`No.`	Index number within the table
`Part Name`	Name of the part
`Location`	Location where the part is installed
`Part Number`	Part number for the part
`Serial Number`	Serial number of the part
`Revision`	Revision level of the part
`Installation Date`	Date that the part was installed

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate a hardware inventory report in system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Hardware` button.

   The interface displays the `Hardware Inventory Reports for System Group` window. (Refer to Figure 6-27.)

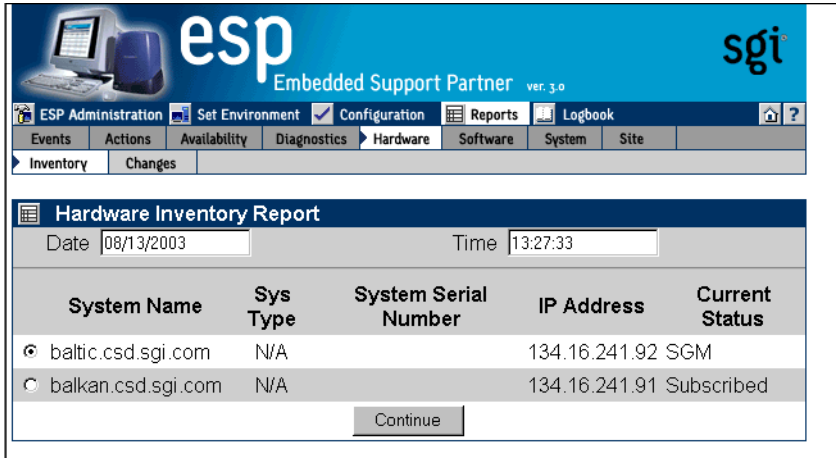
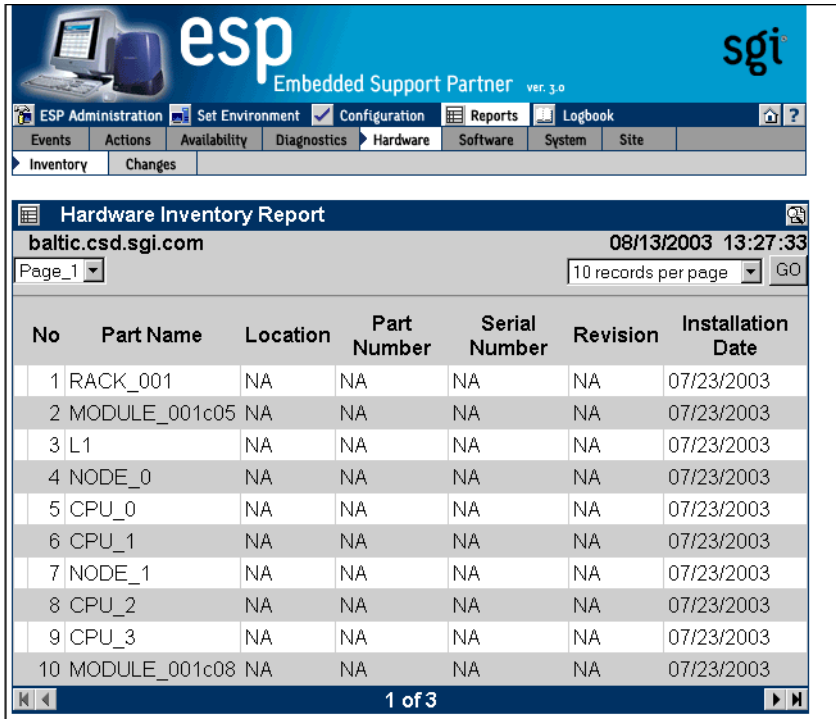


Figure 6-27 Hardware Inventory Reports for System Group Window (System Group Manager Mode)

3. Specify the date and time of the hardware inventory that you want to view.
4. Specify the system for the hardware inventory that you want to view.
5. Click on the `Generate Report` button.

   Figure 6-28 shows an example hardware inventory report.



No	Part Name	Location	Part Number	Serial Number	Revision	Installation Date
1	RACK_001	NA	NA	NA	NA	07/23/2003
2	MODULE_001c05	NA	NA	NA	NA	07/23/2003
3	L1	NA	NA	NA	NA	07/23/2003
4	NODE_0	NA	NA	NA	NA	07/23/2003
5	CPU_0	NA	NA	NA	NA	07/23/2003
6	CPU_1	NA	NA	NA	NA	07/23/2003
7	NODE_1	NA	NA	NA	NA	07/23/2003
8	CPU_2	NA	NA	NA	NA	07/23/2003
9	CPU_3	NA	NA	NA	NA	07/23/2003
10	MODULE_001c08	NA	NA	NA	NA	07/23/2003

Figure 6-28 Example Hardware Inventory Report (System Group Manager Mode)

Table 6-11 describes the contents of the report.

Table 6-11 Hardware Inventory Report Contents (System Group Manager Mode)

Column Heading	Description
`No.`	Index number within the table
`Part Name`	Name of the part
`Location`	Location where the part is installed
`Part Number`	Part number for the part
`Serial Number`	Serial number of the part
`Revision`	Revision level of the part
`Installation Date`	Date that the part was installed

Using the Command Line Interface

Use the following command to view a hardware inventory report:

```
configmon -h
```

Hardware Changes Reports

Hardware changes reports show all hardware that has been installed or deinstalled with a specified time period.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate a hardware changes report from single system manager mode:

1. Click on the `Reports` button.
2. Click on the `Hardware` button.
3. Click on the `Changes` button.

   The interface displays the `History of Hardware` window. (Refer to Figure 6-29.)

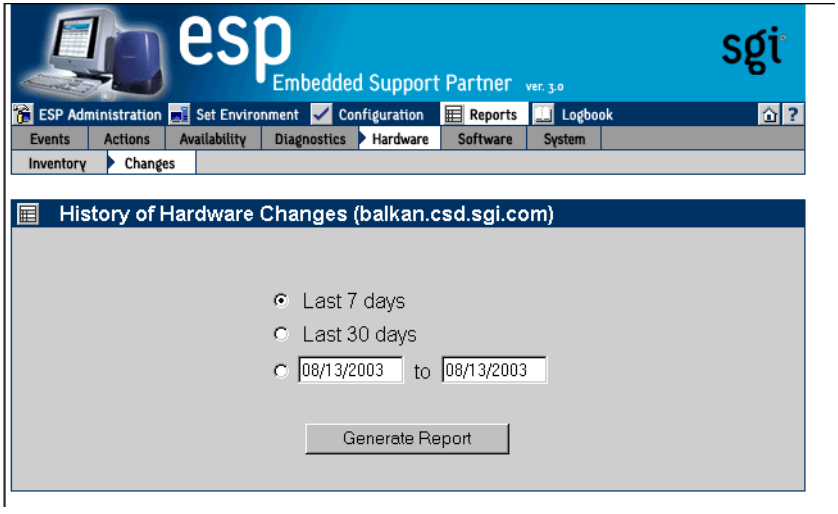


Figure 6-29 History of Hardware Changes Window (Single System Manager Mode)

4. Specify the range of dates for the report.
5. Click on the `Generate Report` button.

   Figure 6-30 shows an example hardware changes report.

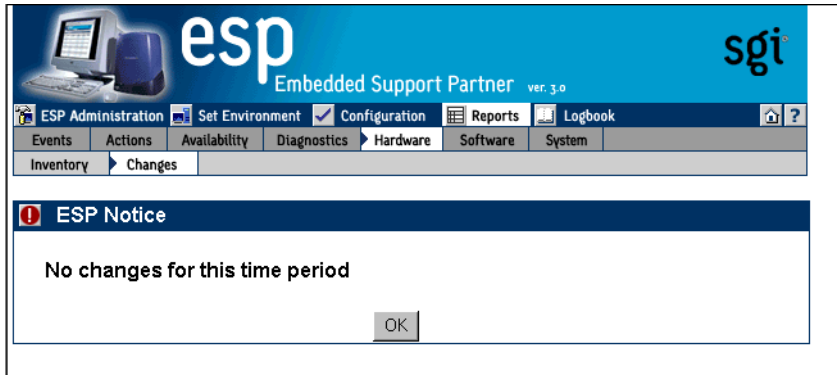


Figure 6-30 Example Hardware Changes Report (Single System Manager Mode)

Table 6-12 describes the contents of the report.

Table 6-12 Hardware Changes Report Contents (Single System Manager Mode)

Column Heading	Description
`No.`	Index number in the table
`Part Name`	Name of the part
`Location`	Location of the part
`Serial Number`	Serial number of the part
`Part Number`	Part number of the part
`Revision`	Revision level of the part
`Install Date/Time`	Date and time that the part was installed in the location
`Removal Date/Time`	Date and time that the part was removed from the location

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate a hardware changes report from system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Hardware` button.
3. Click on the `Changes` button.

   The interface displays the `Hardware Changes Report For System` window. (Refer to Figure 6-31.)

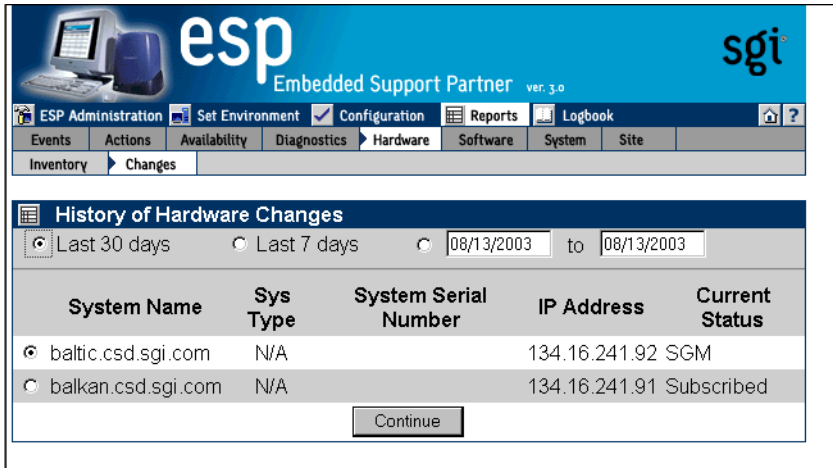


Figure 6-31 Hardware Changes Reports for System Group Window (System Group Manager Mode)

4. Specify the range of dates for the report.
5. Click on the `Generate Report` button.

   Figure 6-32 shows an example hardware changes report.

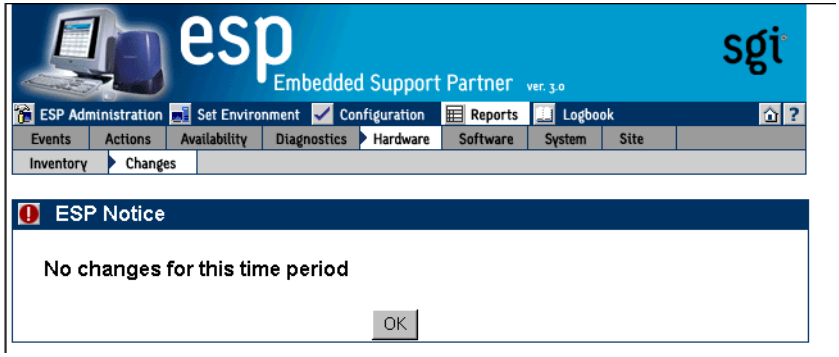


Figure 6-32 Example Hardware Changes Report (Single Group Manager Mode)

Table 6-13 describes the contents of the report.

Table 6-13 Hardware Changes Report Contents (System Group Manager Mode)

Column Heading	Description
`No.`	Index number in the table
`Part Name`	Name of the part
`Location`	Location of the part
`Serial Number`	Serial number of the part
`Part Number`	Part number of the part
`Revision`	Revision level of the part
`System Name`	System on which the part is located
`Install Date/Time`	Date and time that the part was installed in the location
`Remove Date/Time`	Date and time the part was removed from the location

Using the Command Line Interface

Use the following syntax of the `espreport` command to view a hardware changes report:

```
/usr/sbin/espreport hwchanges
                        [-sysid <system id> | -host <host name>]
                        [-from <mm/dd/yyyy>] [-to <mm/dd/yyyy>]
```

Use the `-from` and `-to` options to specify a range of dates. If you do not use these options, the report includes all available data.

Software Reports

There are two types of software reports:

- System inventory reports
- System changes reports

Software Inventory Reports

Software inventory reports show all software installed on a system at a specific date and time.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate a software inventory report from single system manager mode:

1. Click on the `Reports` button.
2. Click on the `Software` button.
3. Click on the `Inventory` button.

   The interface displays the `Software Inventory Report` window. (Refer to Figure 6-33.)

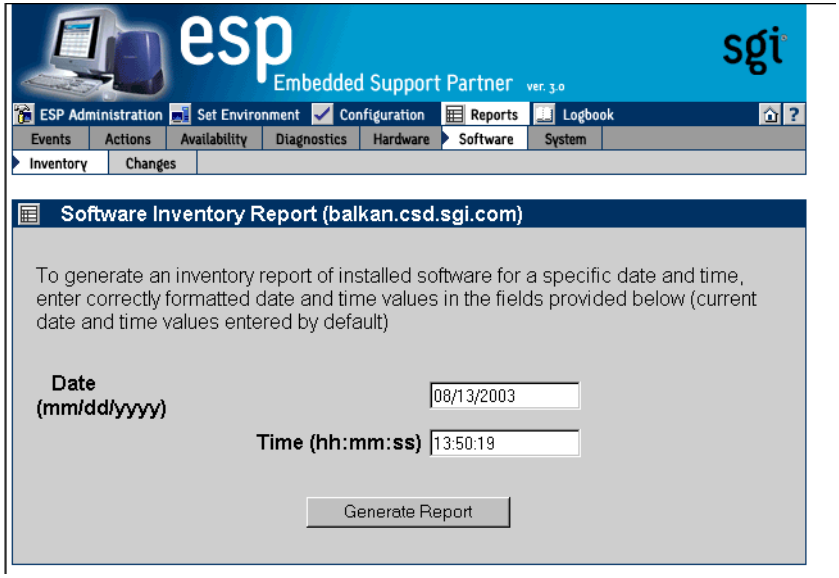
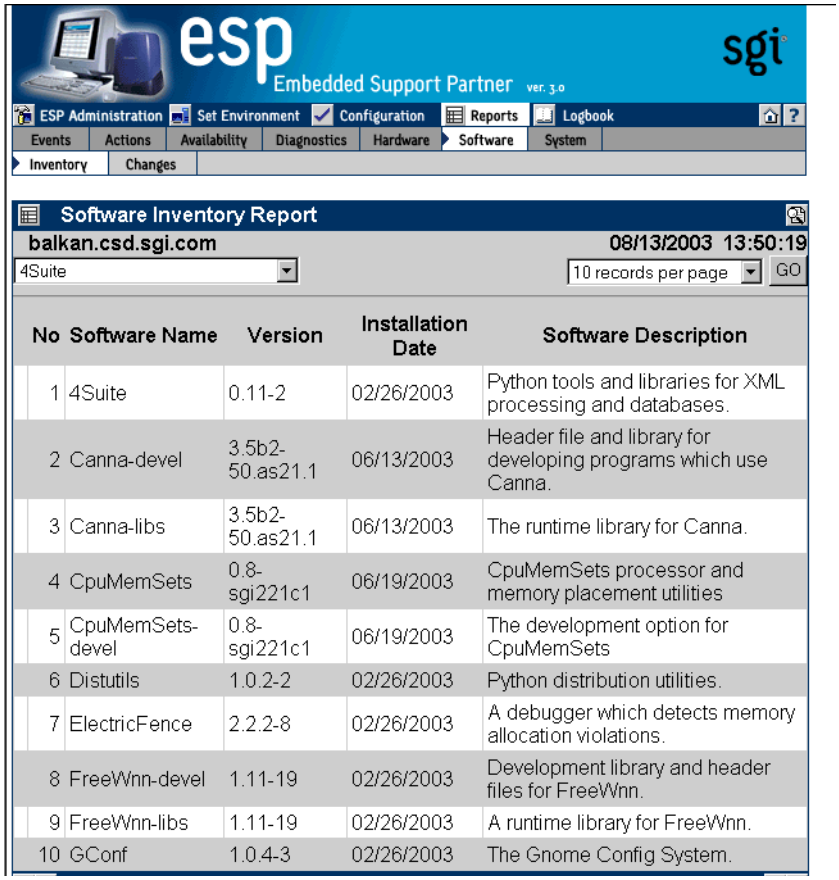


Figure 6-33 Software Inventory Report Window (Single System Manager Mode)

4. Specify the date and time of the software inventory that you want to view.
5. Click on the `Generate Report` button.

   Figure 6-34 shows an example software inventory report.



No	Software Name	Version	Installation Date	Software Description
1	4Suite	0.11-2	02/26/2003	Python tools and libraries for XML processing and databases.
2	Canna-devel	3.5b2-50.as21.1	06/13/2003	Header file and library for developing programs which use Canna.
3	Canna-libs	3.5b2-50.as21.1	06/13/2003	The runtime library for Canna.
4	CpuMemSets	0.8-sgi221c1	06/19/2003	CpuMemSets processor and memory placement utilities
5	CpuMemSets-devel	0.8-sgi221c1	06/19/2003	The development option for CpuMemSets
6	Distutils	1.0.2-2	02/26/2003	Python distribution utilities.
7	ElectricFence	2.2.2-8	02/26/2003	A debugger which detects memory allocation violations.
8	FreeWnn-devel	1.11-19	02/26/2003	Development library and header files for FreeWnn.
9	FreeWnn-libs	1.11-19	02/26/2003	A runtime library for FreeWnn.
10	GConf	1.0.4-3	02/26/2003	The Gnome Config System.

Figure 6-34 Example Software Inventory Report (Single System Manager Mode)

Table 6-14 describes the contents of the report.

Table 6-14 Software Inventory Report Contents (Single System Manager Mode)

Column Heading	Description
`No.`	Index number within the table
`Software Name`	Name of the software application
`Version`	Version number of the software application
`Installation Date`	Date on which the software application was installed
`Software Description`	Brief description of the software

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate a software inventory report from system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Software` button.
3. Click on the `Inventory` button.

   The interface displays the `Software Inventory Reports for System Group` window. (Refer to Figure 6-35.)

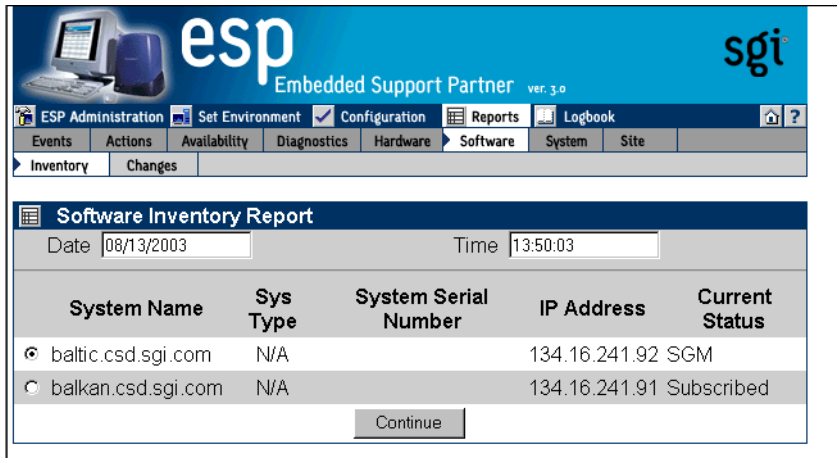
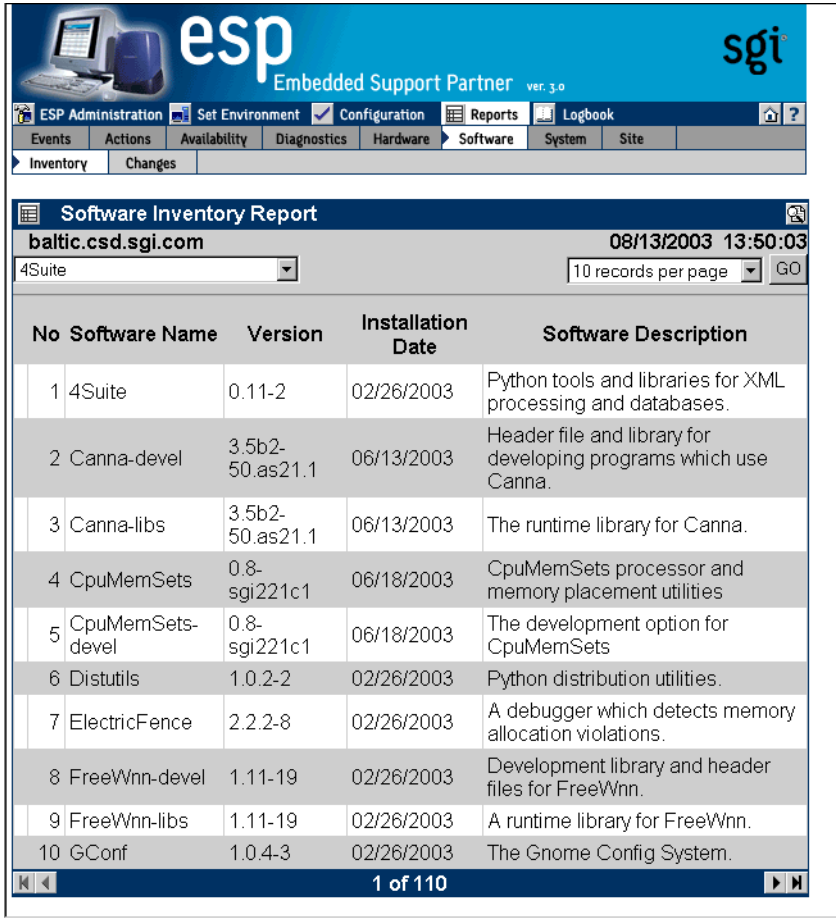


Figure 6-35 Software Inventory Reports for System Group Window (System Group Manager Mode)

4. Specify the date and time of the software inventory that you want to view.
5. Click on the `Generate Report` button.

   Figure 6-36 shows an example software inventory report.



No	Software Name	Version	Installation Date	Software Description
1	4Suite	0.11-2	02/26/2003	Python tools and libraries for XML processing and databases.
2	Canna-devel	3.5b2-50.as21.1	06/13/2003	Header file and library for developing programs which use Canna.
3	Canna-libs	3.5b2-50.as21.1	06/13/2003	The runtime library for Canna.
4	CpuMemSets	0.8-sgi221c1	06/18/2003	CpuMemSets processor and memory placement utilities
5	CpuMemSets-devel	0.8-sgi221c1	06/18/2003	The development option for CpuMemSets
6	Distutils	1.0.2-2	02/26/2003	Python distribution utilities.
7	ElectricFence	2.2.2-8	02/26/2003	A debugger which detects memory allocation violations.
8	FreeWnn-devel	1.11-19	02/26/2003	Development library and header files for FreeWnn.
9	FreeWnn-libs	1.11-19	02/26/2003	A runtime library for FreeWnn.
10	GConf	1.0.4-3	02/26/2003	The Gnome Config System.

Figure 6-36 Example Software Inventory Report (System Group Manager Mode)

Table 6-15 describes the contents of the report.

Table 6-15 Software Inventory Report Contents (System Group Manager Mode)

Column Heading	Description
`No.`	Index number within the table
`Software Name`	Name of the software application
`Version`	Version number of the software application
`Installation Date`	Date on which the software application was installed
`Software Description`	Brief description of the software

Using the Command Line Interface

Use the following command to view a software inventory report:

```
configmon -s
```

Software Changes Reports

Software changes reports show all software that has been added to or removed from a system within a specific time period.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate a software changes report from single system manager mode:

1. Click on the `Reports` button.
2. Click on the `Software` button.
3. Click on the `Changes` button.

   The interface displays the `History of Software Changes` window. (Refer to Figure 6-37.)

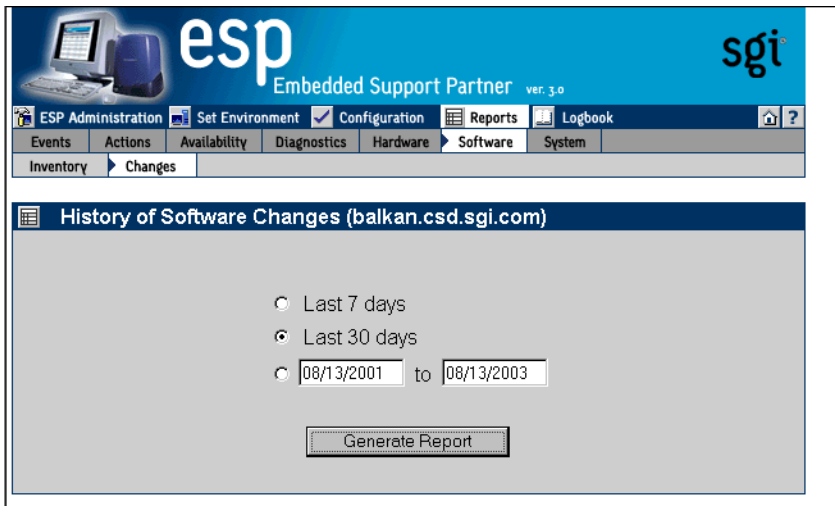


Figure 6-37 History of Software Changes Window (Single System Manager Mode)

4. Specify the range of dates for the report.
5. Click on the `Generate Report` button.

Figure 6-38 shows an example software changes report.

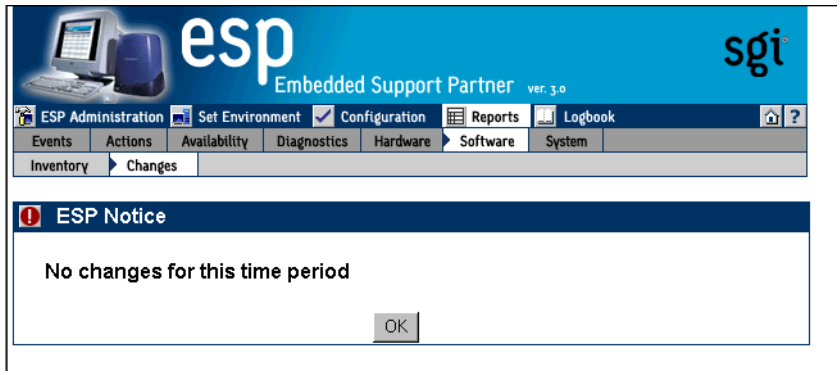


Figure 6-38 Example Software Changes Report (Single System Manager Mode)

Table 6-16 describes the contents of the report.

Table 6-16 Software Changes Report Contents (Single System Manager Mode)

Column Heading	Description
`No.`	Index number in the table
`Software Name`	Name of the software application
`Software Version`	Version number of the software application
`Installation Date`	Date that the software application was installed on the system
`Removal Date/Time`	Date that the software application was removed from the system
`Description`	Description of the software application

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate a software changes report from system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Software` button.
3. Click on the `Changes` button.

   The interface displays the `History of Software Changes For System Group` window. (Refer to Figure 6-39.)

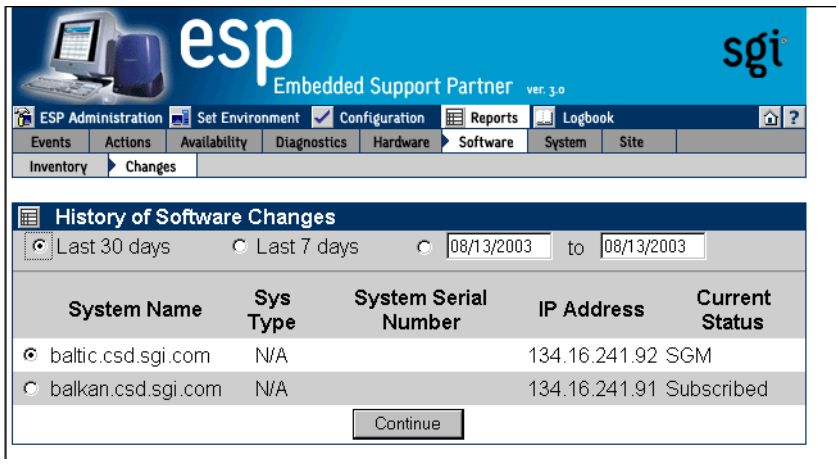


Figure 6-39 Software Changes for System Group Window (System Group Manager Mode)

4. Specify the range of dates for the report.
5. Select the system to include in the report.
6. Click on the `Generate Report` button.

   Figure 6-40 shows an example software changes report.

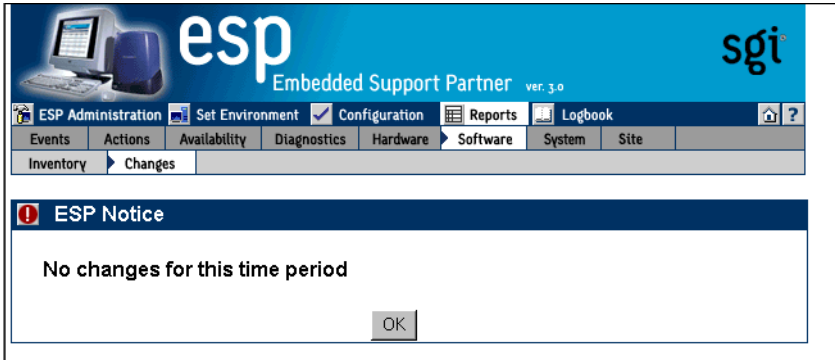


Figure 6-40 Example Software Changes Report (System Group Manager Mode)

Table 6-17 describes the contents of the report.

Table 6-17 Software Changes Report Contents (System Group Manager Mode)

Column Heading	Description
`No.`	Index number in the table
`Software Name`	Name of the software application
`Software Version`	Version number of the software application
`Installation Date`	Date that the software application was installed on the system
`Removal Date/Time`	Date that the software application was removed from the system
`Description`	Description of the software application

Using the Command Line Interface

Use the following syntax of the `espreport` command to view a software changes report:

```
/usr/sbin/espreport swchanges
                    [-sysid <system id> | -host <host name>]
                    [-from <mm/dd/yyyy>] [-to <mm/dd/yyyy>]
```

Use the `-from` and `-to` options to specify a range of dates. If you do not use these options, the report includes all available data.

System Reports

There are two types of system reports:

- System inventory reports
- System changes reports

System Inventory Reports

System inventory reports show the current system and ESP information.

Using the Web-based Interface

Perform the following procedure to use the Web-based interface to generate a system inventory report:

1. Click on the `Reports` button.
2. Click on the `System` button.
3. Click on the `Inventory` button.

   The interface displays the `System` window. (Figure 6-41 shows an example system inventory report in single system manager mode. Figure 6-42 shows an example system inventory report in system group manager mode.)

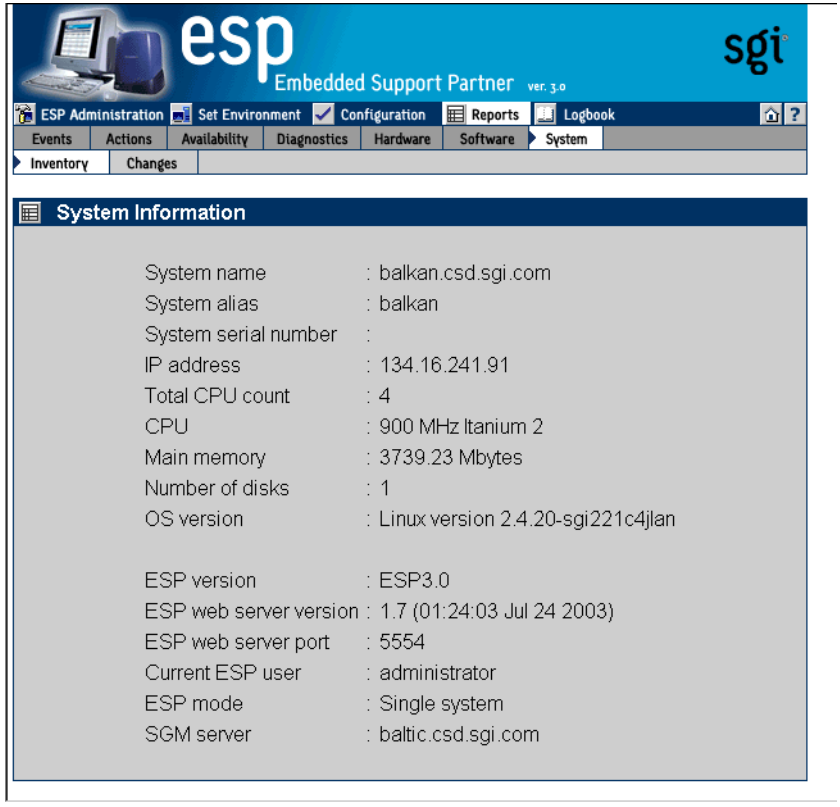


Figure 6-41 Example System Inventory Report (Single System Manager Mode)

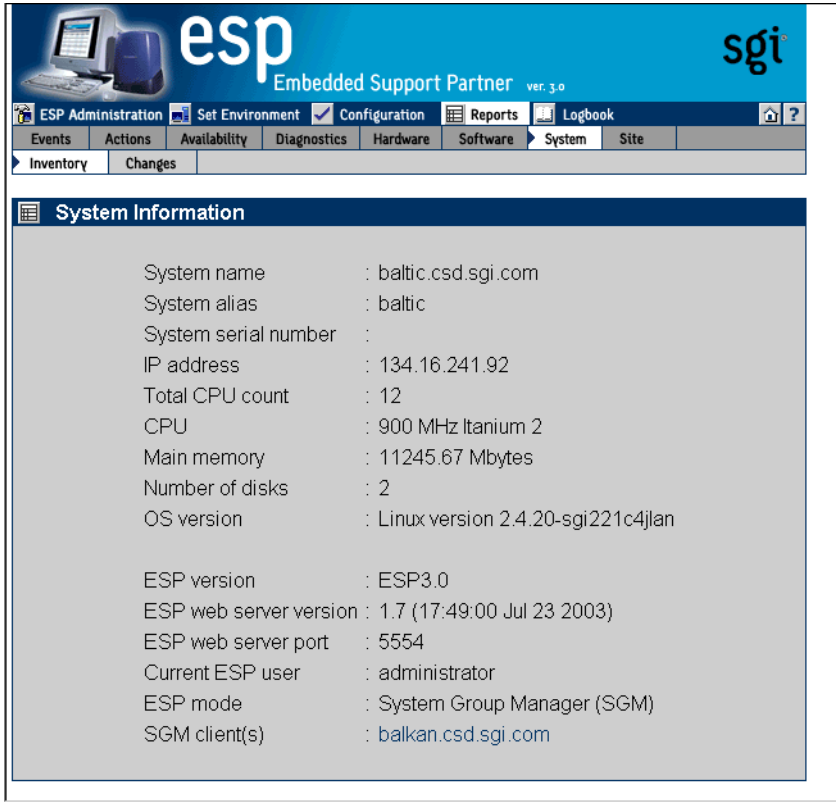


Figure 6-42 Example System Inventory Report (System Group Manager Mode)

Using the Command Line Interface

Use the following syntax of the `espreport` command to generate a system information report:

```
/usr/sbin/espreport sysinfo
                    [-sysid <system id> | -host <host name>]
                    [all]
```

If you specify the `all` option, the command displays the system name, serial number, type, IP address, and system ID. If you do not specify the `all` option, this command displays only the system serial number.

Use the following syntax of the `espreport` command to view a summary report that includes system information, events, hardware and software changes, logbook information, availability overview, and local system disk usage:

```
/usr/sbin/espreport summary
                    [-sysid <system id> | -host <host name>]
                    [-from <mm/dd/yyyy>] [-to <mm/dd/yyyy>]
```

Use the `-from` and `-to` options to specify a range of dates. If you do not use these options, the report includes all available data.

System Changes Reports

System change reports show any system changes (system name, IP address, etc.) that occur within a specific time period.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to generate a system inventory report from single system manager mode:

1. Click on the `Reports` button.
2. Click on the `System` button.
3. Click on the `Changes` button.

   The interface displays the `History of System Changes` window. (Refer to Figure 6-43.)

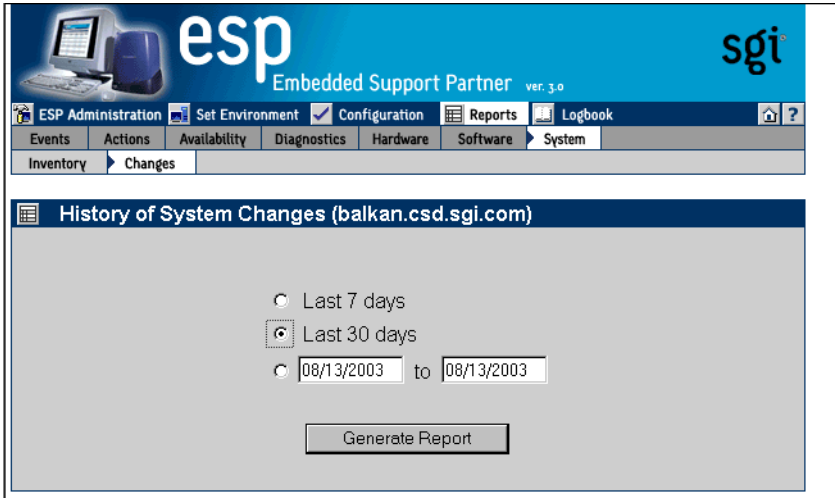


Figure 6-43 History of System Changes Window (Single System Manager Mode)

4. Specify the range of dates for the report.
5. Click on the `Generate Report` button.

Figure 6-44 shows an example system changes report.

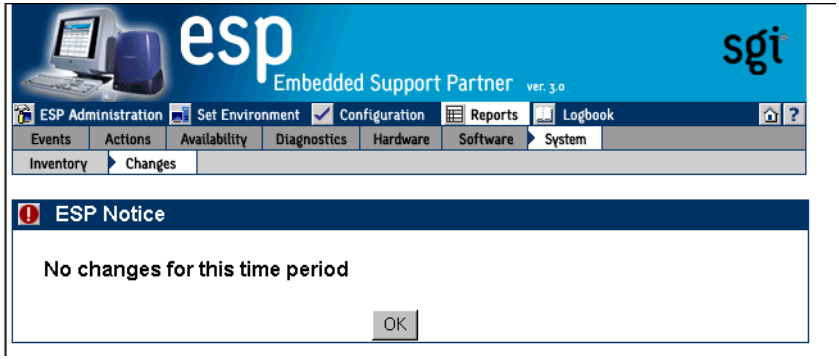


Figure 6-44 Example System Changes Report (Single System Manager Mode)

Table 6-18 describes the contents of the report.

Table 6-18 System Changes Report Contents (Single System Manager Mode)

Column Name	Description
`SysId`	System identification number
`System type`	Processor that the system uses
`System serial number`	Serial number of the system
`Hostname`	Hostname of the system
`IP address`	IP address of the system
`Date/Time`	Date and time of the change

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to generate a system inventory report from system group manager mode:

1. Click on the `Reports` button.
2. Click on the `System` button.
3. Click on the `Changes` button.

   The interface displays the `System Changes For System Group` window. (Refer to Figure 6-45.)

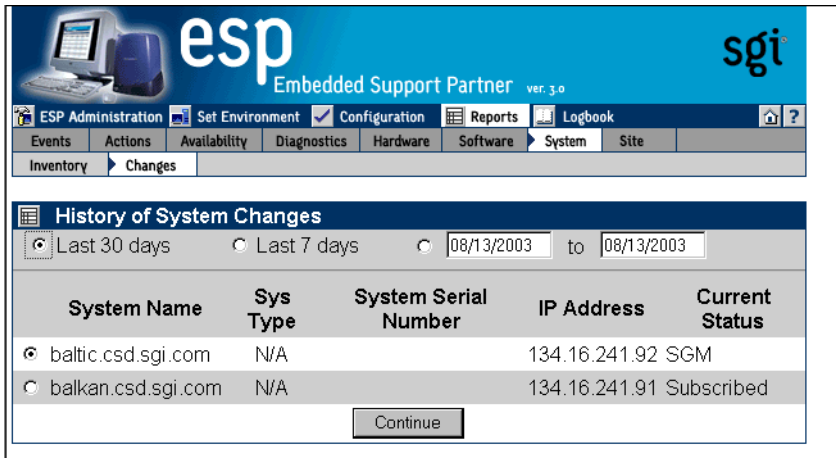


Figure 6-45 System Changes for System Group Window (System Group Manager Mode)

4. Specify the range of dates for the report.
5. Specify the systems to include in the report.
6. Click on the `Generate Report` button.

Figure 6-46 shows an example system changes report.

Figure 6-46 Example System Changes Report (System Group Manager Mode)

Table 6-19 describes the contents of the report.

Table 6-19 System Changes Report Contents (System Group Manager Mode)

Column Name	Description
`SysId`	System identification number
`System type`	Processor that the system uses
`System serial number`	Serial number of the system
`Hostname`	Hostname of the system
`IP address`	IP address of the system
`Date/Time`	Date and time of the change

Using the Command Line Interface

System change reports are not available from the command line interface.

Site Reports (System Group Manager Mode Only)

Site reports show information for various combinations of systems at a site. ESP limits site reports to include only systems that meet specific criteria, including:

- Systems that are in a specific group
- Systems that run a specific operating system version
- Systems that have a specific processor type

Site reports can contain system information, all available events, or specific events by class for the selected systems. Site reports are available only from SGM servers.

Perform the following procedure to use the Web-based interface to generate a site inventory report from system group manager mode:

1. Click on the `Reports` button.
2. Click on the `Site` button.

   The interface displays the Site Reports window. (Refer to Figure 6-47.)

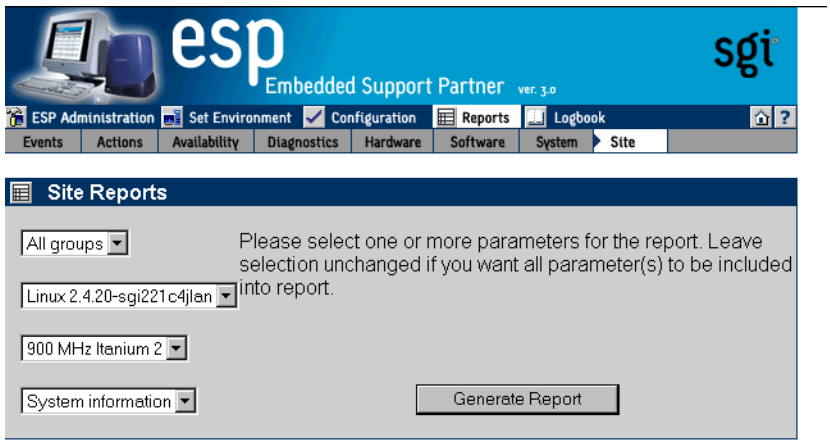


Figure 6-47 Site Reports Window

3. Select the items to include in the report:
    - Choose the groups that you want to include in the report. The pulldown menu includes the names of all groups that are available. When you choose a group name from the menu, the report contains only the systems in the group that you select. Choose `All groups` to include all systems in the report.
    - Choose the operating system that you want to include in the report. The pulldown menu includes the name of all operating systems that ESP detected on the systems. When you choose an operating system from the menu, the report contains only systems that are running that operating system.
    - Choose a processor type. The pulldown menu includes all processor types that ESP detected in the systems. When you choose a processor type from the menu, the report contains only systems that contain that type of processor.
    - Choose the type of site report to generate. The following options are available:

      The `System information` option generates a site information report, which includes the following information: system name, IP type (if applicable), processor type, OS version, the group that includes the system, the system activation date (the date when system was added to the group for the first time), and system deactivation date (the date when system was unsubscribed).

      The `All events` option generates a report of all available events.

      The `Events by class` generates a report of events from specific classes.
4. Click on the `Generate Report` button.

The interface displays the report. (Figure 6-48 shows an example of a site information report.)

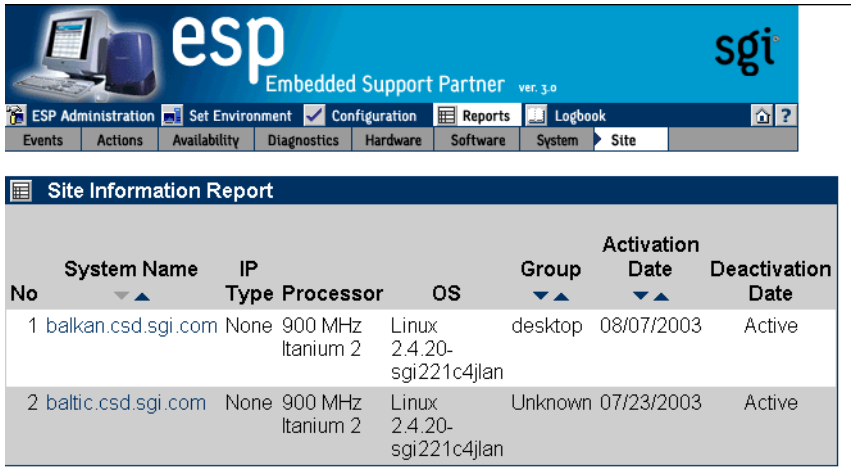


Figure 6-48 Site Information Report

Using the Command Line Interface

Site reports are not available from the command line interface.

Using the ESP Logbook

This chapter describes the ESP logbook, how to view it, and how to add entries to it.

About the ESP Logbook

Use the ESP logbook to record changes that you make to a system: Create a logbook entry each time that you perform a service-related activity on a system. Then, if necessary, any ESP user with the "view logbook" permission can view the entries to review the activities at a later time.

Viewing Logbook Entries

You can view any logbook entries to review previous system activities.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to view logbook entries in single system manager mode:

1. Click on the `Logbook` button.
2. Click on the `View Log` button.

   The interface displays the `View Logbook Entries` window. (Refer to Figure 7-1.)

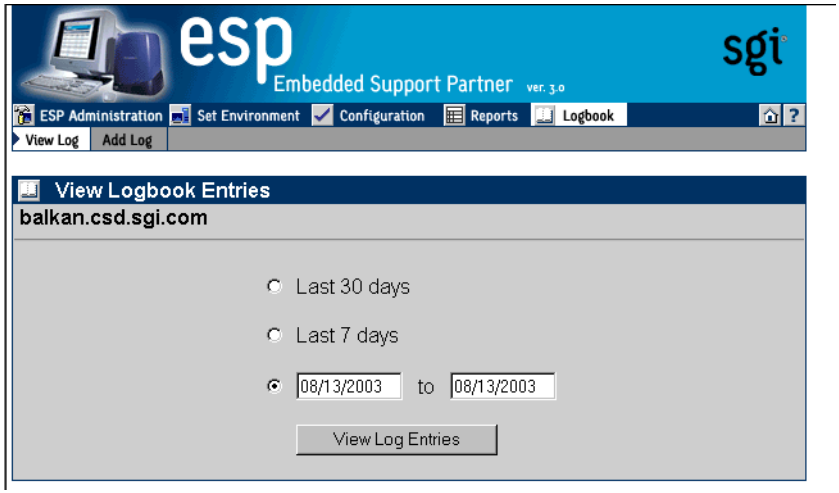


Figure 7-1 View Logbook Entries Window (Single System Manager Mode)

3. Specify the range of dates to view.
4. Click on the `View Log Entries` button.

   The interface displays the specified logbook entries. (Refer to Figure 7-2.)

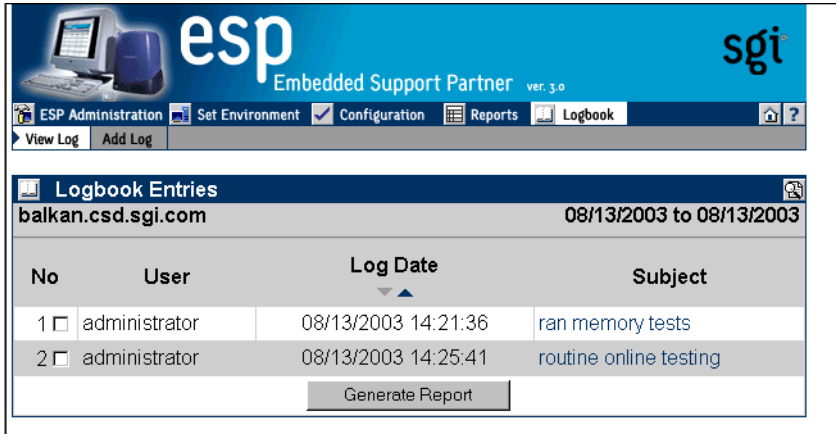


Figure 7-2 Specified Logbook Entries (Single System Manager Mode)

5. Perform one the following actions to view a log entry:
   - Set the check mark next to entry number, and click on the `Generate Report` button.
   - Click on the subject link for the entry.

   The interface displays the logbook entry information. (Refer to Figure 7-3.)

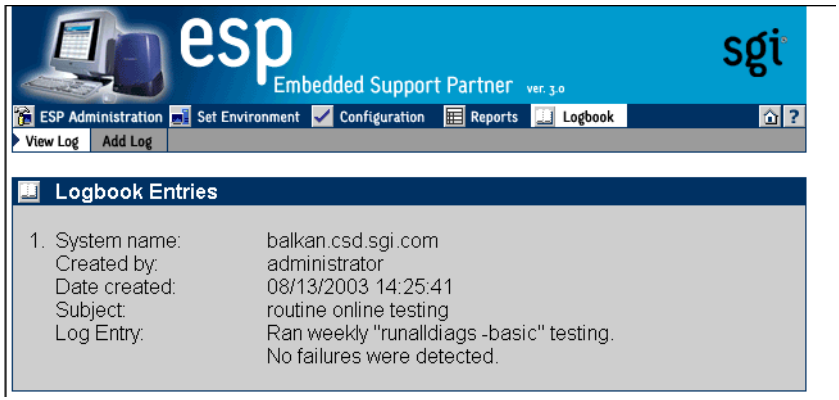


Figure 7-3 Logbook Entry Information (Single System Manager Mode)

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to view logbook entries in system group manager mode:

1. Click on the `Logbook` button.
2. Click on the `View Log` button.

   The interface displays the `View Logbook Entries` window. (Refer to Figure 7-4.)

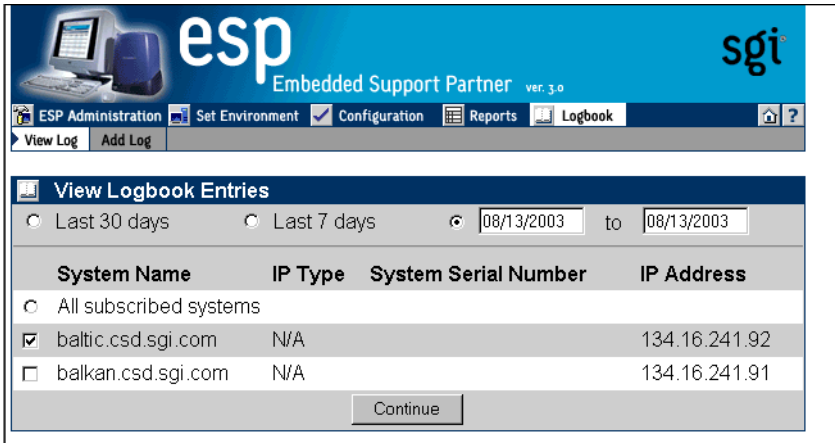


Figure 7-4 View Logbook Entries Window (System Group Manager Mode)

3. Specify the range of dates to view.
4. Select the systems to view.
5. Click on the `View Log Entries` button.

   The interface displays the specified logbook entries. (Refer to Figure 7-5.)

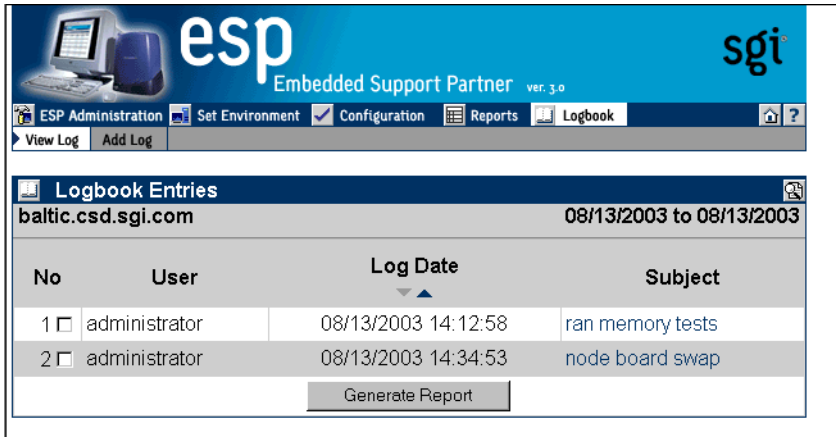


Figure 7-5 Specified Logbook Entries (System Group Manager Mode)

6. Perform one the following actions to view a log entry:
   - Set the check mark next to entry number, and click on the `Generate Report` button.
   - Click on the subject link for the entry.

   The interface displays the logbook entry information. (Refer to Figure 7-6.)

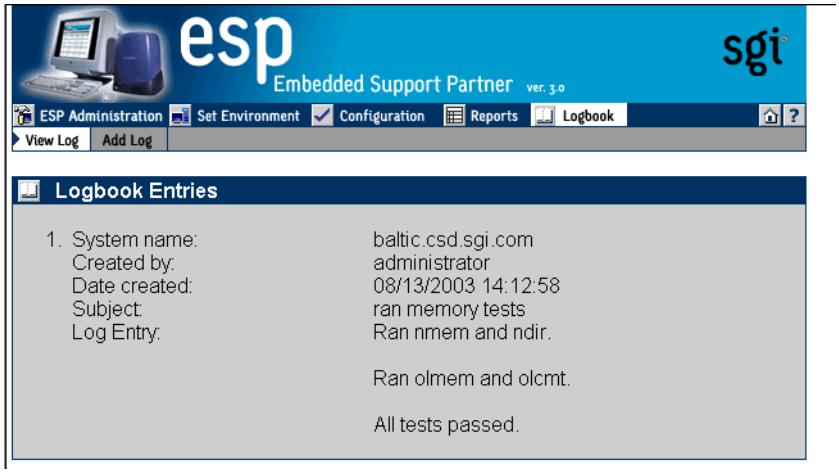


Figure 7-6 Logbook Entry Information (System Group Manager Mode)

Using the Command Line Interface

Use the following syntax of the `espreport` command to view logbook entries:

```
/usr/sbin/espreport logbook  [-sysid <system id>|-host <host name>]
                             [-from mm/dd/yyyy] [-to mm/dd/yyyy]
```

Use the `-sysid` and `-host` options to select a system. Use the `-from` and `-to` options to specify a range of dates. If you do not use these options, the report includes all available data.

Adding a Logbook Entry

You should add logbook entries any time that you modify a system.

Using the Web-based Interface (Single System Manager Mode)

Perform the following procedure to use the Web-based interface to add a logbook entry in single system manager mode:

1. Click on the `Logbook` button.
2. Click on the `Add Log` button.

   The interface displays the `Create Log` window. (Refer to Figure 7-7.)

Figure 7-7 Create Log Window (Single System Manager Mode)

Note: ESP automatically sets the `User` field to the user account that you are using.

3. Enter a subject for the entry. (This required field can hold up to 128 characters.)
4. Enter a log entry. (This required field can hold up to 4 Kbytes of data.)
5. Click on the `Submit Log` button.

   The interface displays the information that you entered. (Refer to Figure 7-8.)

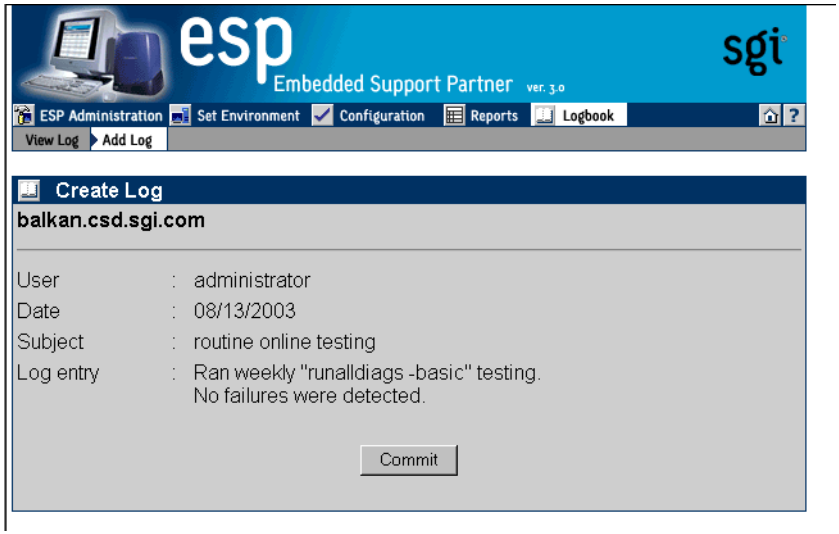


Figure 7-8 Logbook Entry Confirmation Window (Single System Manager Mode)

6. Click on the `Commit` button to create the entry.

   The interface displays the information that was added to the logbook. (Refer to Figure 7-9.)

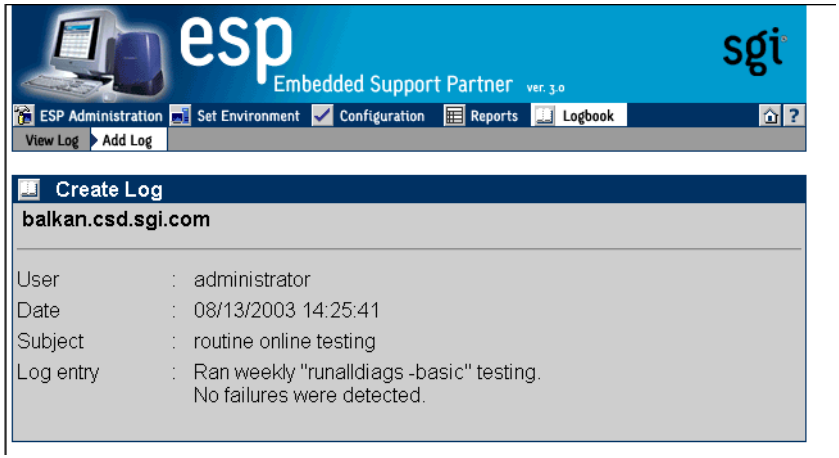


Figure 7-9 Completed Logbook Entry (Single System Manager Mode)

Using the Web-based Interface (System Group Manager Mode)

Perform the following procedure to use the Web-based interface to add a logbook entry in system group manager mode:

1. Click on the `Logbook` button.
2. Click on the `Add Log` button.

   The interface displays the `Create Log` window. (Refer to Figure 7-10.)

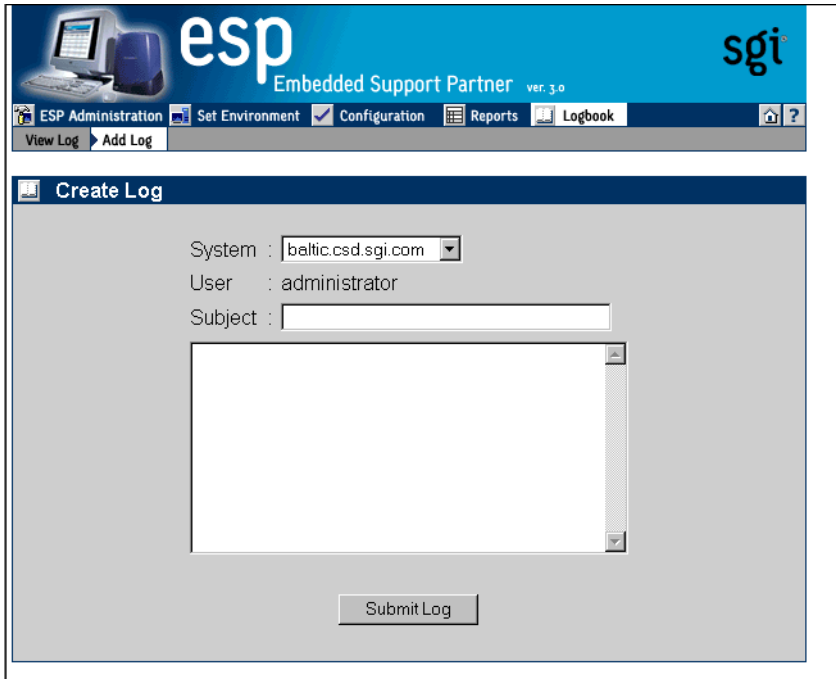


Figure 7-10 Create Log Window (System Group Manager Mode)

Note: ESP automatically sets the `User` field to the user account that you are using.

3. Select the system that the log entry is for.
4. Enter a subject for the entry. (This required field can hold up to 128 characters.)
5. Enter a log entry. (This required field can hold up to 4 Kbytes of data.)
6. Click on the `Submit Log` button.

   The interface displays the information that you entered. (Refer to Figure 7-11.)

Figure 7-11 Logbook Entry Confirmation Window (System Group Manager Mode)

7. Click on the `Commit` button to create the entry.

   The interface displays the information that was added to the logbook. (Refer to Figure 7-12.)

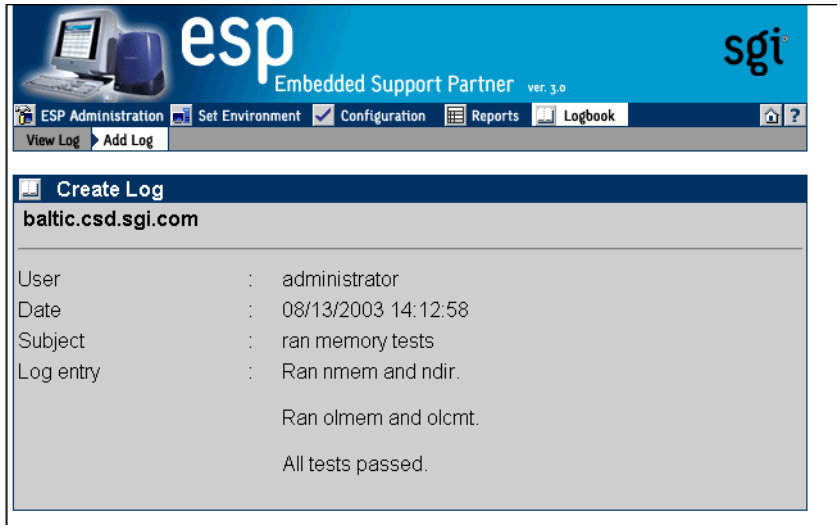


Figure 7-12 Completed Logbook Entry (System Group Manager Mode)

Using the Command Line Interface

Use the `/usr/sbin/esplognote` command to add a logbook entry. This command prompts you for the information that is required in a logbook entry.

Sending Notifications

About the espnotify Tool

The ESP software suite includes the `espnotify` tool, which you can use to perform the following types of notification:

- Display a message on the system console
- Display a message on a local or remote X Window System display
- Send an e-mail message

Note: This chapter describes how to use the `espnotify` command to create notifications. ESP can also automatically generate the `espnotify` command line from options that you select from the graphical user interface (when you use the `Notification Action` option in the `Add Action` window). The information in this chapter simply provides examples of how you can create command lines as actions. If you need to create standard notification actions, it is easiest to use the automated method.

Command Line Options for Displaying a Message on the Console

Use the following format of the `espnotify` command to display a message on the system console:

```
/usr/bin/espnotify -A <message> [-n <number>]
```

This format of the `espnotify` command has the following command line options:

`-A`	Specifies that the message should be displayed in the console window
`<message>`	Specifies the message that the window should display Enclose `<message>` in single quotes (‘ ’) if the message contains more than one word.

`-n <number>` Specifies an optional priority message, which is determined by the value that you specify for `<number>`

The `<number>` parameter can be a value from 1 to 7. `espnotify` attaches a label to the message based on the value of `<number>`: 1 or 2 (`Critical System Error`), 3 (`System Error`), 4 (`System Warning`), or 5 to 7 (`System Information`)

For example, the following command displays the message `This is the message to display.` on the console (refer to Figure 8-1):

```
/usr/bin/espnotify -A 'This is the message to display.'
```

Figure 8-1 Displaying a Message in the Console Window

Displaying a Message on an X Window System Display

Use the following format of the `espnotify` command to display a message on a local or remote X Window System display:

```
/usr/bin/espnotify -c <message> [-a] [-D <display>] [-g <geometry>]
[-i <icon>] -n <number>] [-t <title>]
```

This format of the `espnotify` command has the following command line options:

`-c <message>` Specifies the message that the window should display

Enclose `<message>` in double quotes (" ") if the message contains more than one word.

`-a` Specifies that an audio file should be played

The `/usr/bin/ssplay` application plays the audio file. Audio notification cannot be performed without graphical notification. Audio notification can be performed only on the local host.

`-D <display>` Specifies the display to use. (If you do not specify a display, the window is displayed on the host specified by the `$DISPLAY` environment variable.)

`-g <geometry>` Specifies an optional X Window System geometry string for the window (in the standard WIDTHxHEIGHTxXOFFxYOFF format)

For example, `-g 120x80x50x100` specifies a window that is 120 pixels wide by 80 pixels high and is located 50 pixels from the left edge of the screen and 100 pixels from the top edge of the screen. (Refer to the x(1) man page for more information.)

`-i <icon>` Specifies an optional image to display as an icon for the window

`-n <number>` Specifies an optional priority message, which is determined by the value that you specify for `<number>`

The `<number>` parameter can be a value from 1 to 7. `espnotify` attaches a label to the message based on the value of `<number>`: 1 or 2 (`Critical System Error`), 3 (`System Error`), 4 (`System Warning`), or 5 to 7 (`System Information`)

`-t <title>` Specifies an optional title of the window.

Enclose `<title>` in double quotes (“ “) if the title contains more than one word.

For example, the following command displays a window on the local host (refer to Figure 8-2):

```
/usr/bin/espnotify -c "This is the message to display." -D localhost:0
-t "This is the title."
```

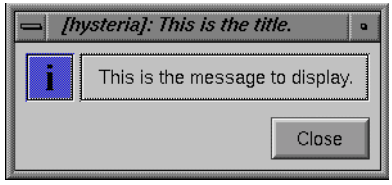


Figure 8-2 Displaying a Message on an X Window System Display

Sending an E-mail Message

Use the following format of the `espnotify` command to send an e-mail message:

```
/usr/bin/espnotify -E <address> { -f <filename> | -m <message> }
[-n <number>] [-o <options>] [-s <subject>]
```

This format of the `espnotify` command has the following command line options:

`-E <address>` Specifies the e-mail addresses that should receive the message

Enclose <address> in single quotes (‘ ‘) if the list contains more than one address.

`-f <filename>` Specifies a text file to use as content for the message

You cannot use the `-f` and `-m` options at the same time.

`-m <message>` Specifies text to use as content for the message

Enclose `<message>` in single quotes (‘ ‘) if the message contains more than one word.

You cannot use the `-f` and `-m` options at the same time.

`-n <number>` Specifies an optional priority message, which is determined by the value that you specify for `<number>`

The <number> parameter can be a value from 1 to 7. `espnotify` attaches a label to the message based on the value of <number>: 1 or 2 (`Critical System Error`), 3 (`System Error`), 4 (`System Warning`), or 5 to 7 (`System Information`)

`-o <options>` Specifies processing options for the message

Two options are available: `-o COMP` (compress and uuencode the message) and `-o ENCO` (uuencode the message). These options are valid only if you also use the `-f` option.

`-s <subject>` Specifies the subject of the message

The format of the default subject is `[HOSTNAME]: <text>`, where `HOSTNAME` is replaced with the name of the host and `<text>` is replaced with a priority message (for example, `Critical System Error`).

If you use the `-n` and `-s` options, the `-s` option overrides the `-n` option.

For example, the following command sends a message to dtg@sgi.com (refer to Figure 8-3):

```
/usr/bin/espnotify -E dtg@sgi.com -m 'This is the text of the message.'
-n 1
```

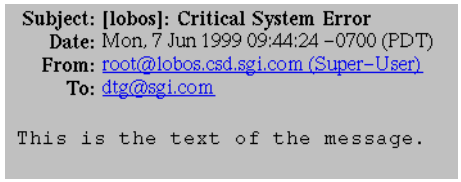


Figure 8-3 Sending an E-mail Message

Invoking espnotify from ESP

Because `espnotify` is a command line utility, you can configure it as an ESP action. To do this, create a new action or update an existing action with a command string that uses the `/usr/bin/espnotify` command. This section shows an example of how to create ESP actions that use `espnotify`.

Note: ESP automatically generates the proper `espnotify` command line when you choose the `Notification` option in the `Add Action` window.

Example: Creating an Action to Send an E-mail

The first example shows how to set up an ESP action to send notification by E-mail.

1. Click on the `Configuration` button.
2. Click on the `Actions` button.
3. Click on the `Add` button.
4. Click on the radio button next to `Other action`.
5. Click on the `Continue` button.

6. Update the parameters. (Table 8-1 lists the parameters for this example.)

Table 8-1 Example Action Parameters for Sending an E-mail Notification

Field	Setting
`Action description`	`Send notification via e-mail to abc123@sgi.com`
`Action string`	`/usr/bin/espnotify -E abc123@sgi.com -m %D -s 'An event was just registered.'`
`Execute action as`	`nobody`
`Action timeout`	`600`

Figure 8-4 shows an interface page with the proper settings for this example.

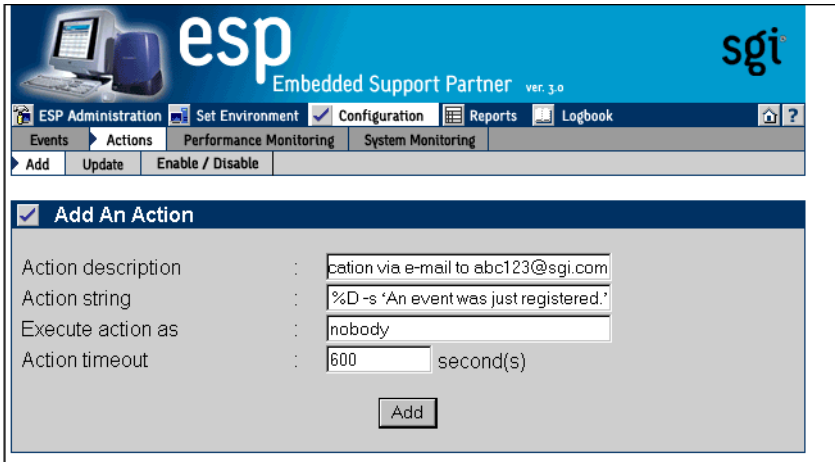


Figure 8-4 Example Action Parameters for Sending an E-mail Message

7. Click on the `Add` button. (Figure 8-5 shows the verification message for this example.)

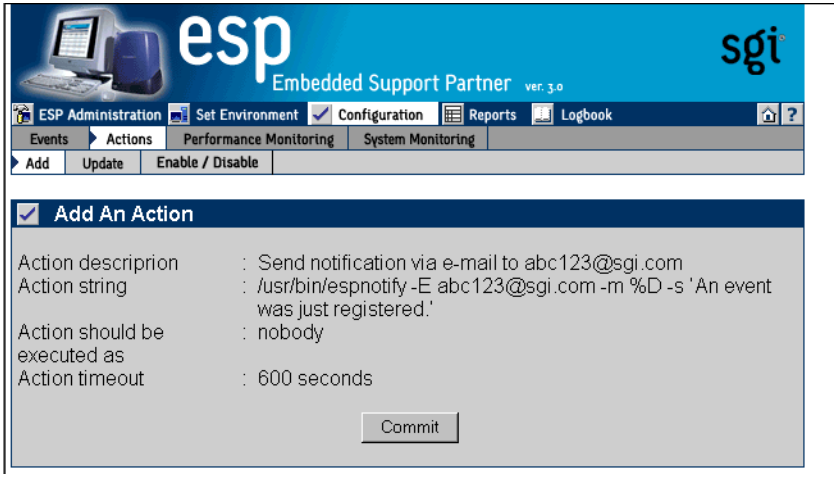


Figure 8-5 Example Verification Message for Sending an E-mail Message Action

8. Click on the `Commit` button. (Figure 8-6 shows the confirmation message for this example.)

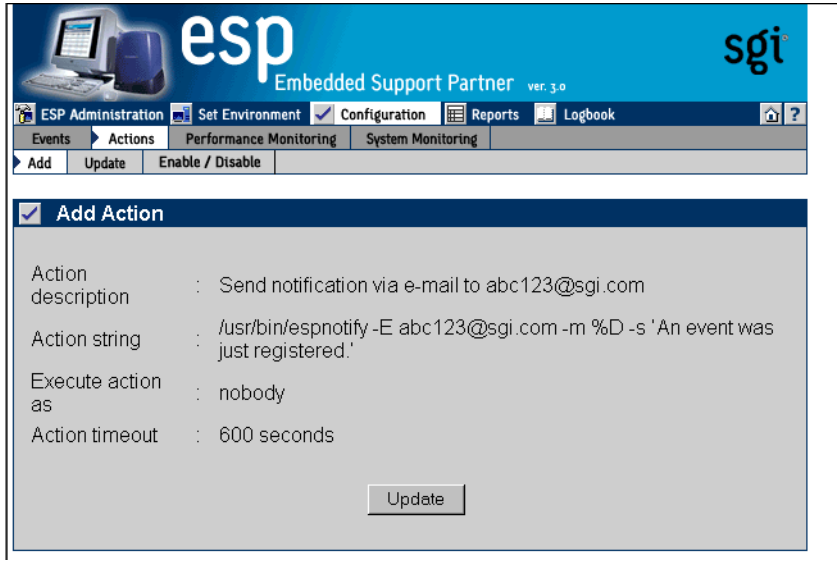


Figure 8-6 Example Confirmation Message for Sending an E-mail Message Action

Logging Events from Applications and Scripts

The ESP framework provides two ways for you to send events from your local applications and scripts to ESP:

- By using the Event Manager Application Programming Interface (API)
- By using the `emgrlogger` and `esplogger` tools

Note: You can also use the `openlog`, `syslog`, and `closelog` SYSLOG functions to send event information through SYSLOG. Refer to the syslog(3c) man page for more information.

Event Classification and Sequence Numbers

The ESP framework uses a standardized event classification scheme for the events that it registers. This classification scheme was implemented to:

- Provide a meaningful representation of the events that have occurred so that users can easily interpret them
- Provide an easy way to locate the source of an error by providing a general category and more specific information

In this scheme, events are categorized by class and type. An event class describes a general area that ESP monitors (for example, SCSI). An event type provides greater detail about individual events (for example, a SCSI controller initialization failure).

ESP automatically generates event class and type numbers when you create custom events and classes. You can use these numbers with your local applications and scripts to send event information to the ESP framework through the Event Manager API and `esplogger` and `emgrlogger` tools.

The ESP framework also uses unique sequence numbers for system messages. These sequence numbers provide a mechanism that enables ESP to isolate problems at the source code level.

Using the Event Manager API

The Event Manager API contains a set of functions that you can call from your local C or C++ programs to send event information to the Event Manager daemon (`eventmond`). The Event Manager forwards events to ESP on a subscription basis.

Refer to the *Event Manager User Guide*, publication number 007-4661-00*x*, for more information about the Event Manager API functions and how to use them.

Using the emgrlogger and esplogger Tools

The `esplogger` and `emgrlogger` tools provide a simple command-line interface to submit events to the Event Manager. `emgrlogger` works with the new Event Manager and replaces `esplogger`, which was used with previous versions of `eventmond` and ESP. `esplogger` remains available to provide backward compatibility. `emgrlogger` can produce any type of Event Manager event, including subscription events.

Use the `emgrlogger` and `esplogger` tools to pass event information from your local scripts to the event monitoring component of ESP (`eventmond`). You can run `esplogger` from a UNIX prompt or from a UNIX shell script. `emgrlogger` and `esplogger` use the following command syntax:

emgrlogger:

```
emgrlogger -h
emgrlogger [-S | -U | -Q | -UQ | -RS]
        [-c <class>] [-t <type>] [-a <appname>] [-s <source host>]
        [-o <origin>] [-p <priority>] [-f <facility>]
        [-P <path to remote host>] [ -is [<tag>]=[<value>]   |
          -if [<tag>]=<file path> |
          -id [<tag>]=<hex data>
        ]*
```

Note: Options related to creating subscription events are not typically used and are not described in this document.

where:

- The `-S` option makes a subscription request.
- The `-U` option makes an unsubscription request.

- The `-Q` option makes a subscription query.
- The `-UQ` option makes an unsubscription by query result request.
- The `-RS` option makes a remote subscription request.
- The `-c` option specifies the event class.
- The `-t` option specifies the event type.
- The `-a` option specifies the name of the application.
- The `-s` option specifies the source (hostname) of the event.
- The `-o` option specifies the origin of the event.
- The `-p` option specifies the priority value of the event.
- The `-f` option specifies the facility value of the event.
- The `-P` option specifies the delivery path for a remote subscription event.
- The `-is` option specifies string data.
- The `-if` option specifies file data.
- The `-id` option specifies digital (binary) data in hexadecimal format.

esplogger:

```
esplogger -s <sequence_number> {-f <filename> | -m "<message>"}
[-p <priority>] [-t <time>]
esplogger -h
esplogger -V
```

where:

- The `-s <sequence_number>` option specifies the sequence number (in decimal or hexadecimal). You must use this option with the `-t` option and the `-f` or `-m` options.
- The `-f <filename>` option specifies the file that contains data to log in the ESP framework. You must include the `-s` option with this option. You cannot use this option with the `-m` option.
- The `-m <message >` option specifies a message to log in the ESP framework. You must include the `-s` option with this option. You cannot use this option with the `-f` option.

- The `-p <priority>` option specifies the priority (for example, local0.notice). Refer to the syslog(3C) man page for descriptions of the priority values. If you do not specify a priority value, `esplogger` sets the priority to local0.info. You must use this option with the `-s` option and the `-f` or `-m` option.
- The `-t <time>` option specifies the time that the event occurred. You must specify the time in seconds since 00:00:00 UTC on January 1, 1970 (in decimal notation). If you do not specify the time, `esplogger` defaults the time to the time that it received the event. You must use this option with the `-s` option and the `-f` or `-m` option.
- The `-h` option prints the usage information.
- The `-V` option prints the `esplogger` version number.

Note: You can also use `logger` to send event information through SYSLOG. Refer to the logger(1) man page for more information.

Example 1

```
emgrlogger -t 200356 -if FILE=availmon.dat
esplogger -s 200356 -f availmon.dat
```

This example sets the sequence number to 200356, the priority to local0.info (1030), and the time to the time that `esplogger` received the event. Then, it passes this information and the data in the `availmon.dat` file to `eventmond`.

Example 2

```
emgrlogger -t 0x00200000 -p syslog -f warning -is MSG="Start SVP"
emgrlogger -s 0x00200000 -p syslog.warning -m "Start SVP"
```

This example sets the sequence number to 0x00200000, the priority to syslog.warning (324), and the time to the time that `emgrlogger` or `esplogger` received the event. Then, it passes this information and the message to `eventmond`.

Default Event Classes and Types

This chapter lists the default event classes and events that ESP includes.

Default Event Classes

The following output from the `espconfig` command shows the default event classes that ESP includes on a system running the Linux OS:

```
system# espconfig -list evclass
ClassId  Class description
-------  -----------------
   4000  "Availability"
   4001  "Performance"
   4002  "System Configuration"
   4005  "Diagnostic"
   7100  "Kernel Messages"
   7110  "User Messages"
   7130  "Daemon Messages"
```

Default Event Types

The following output from the `espconfig` command shows the default event types that ESP includes on a system running the Linux OS:

```
system# espconfig -list evtype
Event types for 8006913E029:
+----------+-----------+------------------------------+---------+-------------+
| Class Id |  Type Id  |        Type Description      | Enabled | Log Enabled |
+----------+-----------+------------------------------+---------+-------------+
|      4002|    2097408|                Configmon init|      Yes|          Yes|
|      4002|    2097409|               Sysinfo changed|      Yes|          Yes|
|      4002|    2097410|            Hardware installed|      Yes|          Yes|
|      4002|    2097411|         Harwdare de-installed|      Yes|          Yes|
|      4002|    2097412|            Software installed|      Yes|          Yes|
```

4002	2097413	Software de-installed	Yes	Yes
4002	2097414	System change	Yes	Yes
4002	2097415	Configuration error	Yes	Yes
4002	2097416	ESP registered with SGI	Yes	Yes
4002	2097417	ESP deregistered with SGI	Yes	Yes
4002	2097418	ESP package updated	Yes	No
4002	2097419	ESP package uninstalled	Yes	No
4002	2097420	ESP system information change	Yes	No
4002	2097421	ESP profile(s) update	Yes	No
4002	340	Customer information is updated	Yes	No
4000	2097152	Live event	No	No
4000	2097153	System ID change	Yes	Yes
4000	2097154	Power cycle	Yes	Yes
4000	2097155	System reset	Yes	Yes
4000	2097156	NMI	Yes	Yes
4000	2097157	Panic (S/W)	Yes	Yes
4000	2097158	Status report	Yes	Yes
4000	2097159	Software error	Yes	Yes
4000	2097160	Hardware error	Yes	Yes
4000	2097161	No error	Yes	Yes
4000	2097162	Registration	Yes	Yes
4000	2097163	Deregistration	Yes	Yes
4000	2097164	Power failure	Yes	Yes
4000	2097165	System off	Yes	Yes
4000	2097166	Interrupt	Yes	Yes
4000	2097167	Panic (H/W)	Yes	Yes
4000	2097168	Panic	Yes	Yes
4000	2097169	Controlled shutdown (unknown)	Yes	Yes
4000	2097170	Controlled shutdown (timeout)	Yes	Yes
4000	2097171	Controlled shutdown(1) (unknown)	Yes	Yes
		)		
4000	2097182	Controlled shutdown (1)	Yes	Yes
4000	2097183	Controlled shutdown (2)	Yes	Yes
4000	2097184	Controlled shutdown (3)	Yes	Yes
4000	2097185	Controlled shutdown (4)	Yes	Yes
4000	2097186	Controlled shutdown (5)	Yes	Yes
4000	2097187	Controlled shutdown (6)	Yes	Yes
4000	2097190	Singleuser shutdown (unknown)	Yes	Yes
4000	2097191	Singleuser shutdown(1)(unknown)	Yes	Yes
4000	2097192	Singleuser shutdown (1)	Yes	Yes
4000	2097193	Singleuser shutdown (2)	Yes	Yes
4000	2097194	Singleuser shutdown (3)	Yes	Yes
4000	2097195	Singleuser shutdown (4)	Yes	Yes
4000	2097196	Singleuser shutdown (5)	Yes	Yes
4000	2097197	Singleuser shutdown (6)	Yes	Yes

4000	3761	Subscribe availability events	Yes	Yes
4000	3762	Unsubscribe availability events	Yes	Yes
7100	7000100	Kernel Emergency	Yes	No
7100	7000101	Kernel Alert	Yes	No
7100	7000102	Kernel Critical	Yes	No
7100	7000103	Kernel Error	Yes	No
7100	7000104	Kernel Warning	Yes	No
7100	7000105	Kernel Notice	No	No
7100	7000106	Kernel Info	No	No
7100	7000107	Kernel Debug	No	No
7110	7000110	User Emergency	Yes	No
7110	7000111	User Alert	Yes	No
7110	7000112	User Critical	Yes	No
7110	7000113	User Error	Yes	No
7110	7000114	User Warning	No	No
7110	7000115	User Notice	No	No
7110	7000116	User Info	No	No
7110	7000117	User Debug	No	No
7130	7000130	Daemon Emergency	Yes	No
7130	7000131	Daemon Alert	Yes	No
7130	7000132	Daemon Critical	Yes	No
7130	7000133	Daemon Error	Yes	No
7130	7000134	Daemon Warning	No	No
7130	7000135	Daemon Notice	No	No
7130	7000136	Daemon Info	No	No
7130	7000137	Daemon Debug	No	No
4005	2098176	Diagnostic start	Yes	Yes
4005	2098177	Diagnostic interrupted	Yes	Yes
4005	2098178	Diagnostic end	Yes	Yes
4005	2098179	Stress start	Yes	Yes
4005	2098180	Stress end	Yes	Yes
4005	2098181	SVP start	Yes	Yes
4005	2098182	SVP end	Yes	Yes
4005	2098183	SVP interrupted	Yes	Yes
4005	2098184	Stress interrupted	Yes	Yes
4001	2097244	High aggregate context switch rate	Yes	Yes
4001	2097217	Possible high floating point exception rate	Yes	Yes
4001	2097218	High 1-minute load average	Yes	Yes
4001	2097246	Low average processor utilization	Yes	Yes
4001	2097219	High aggregate system call rate	Yes	Yes
4001	2097220	Busy executing in system mode	Yes	Yes
4001	2097221	High average processor utilizat	Yes	Yes

		ion		
4001	2097249	System Group Manager slow servi	Yes	Yes
		ce response		
4001	2097248	System Group Manager service pr	Yes	Yes
		obe failure		
4001	2097226	File system is filling up	Yes	Yes
4001	2097227	Severe demand for real memory	Yes	Yes
4001	2097228	Low free swap space	Yes	Yes
4001	2097247	High number of saturated proces	Yes	Yes
		sors		
4001	2097241	High per CPU processor utilizat	Yes	Yes
		ion		
4001	2097239	High per CPU system call rate	Yes	Yes
4001	2097240	Some CPU busy executing in syst	Yes	Yes
		em mode		
4001	2097230	High collision rate in packet s	Yes	Yes
		ends		
4001	2097231	High network interface error ra	Yes	Yes
		te		
4001	2097232	High network interface packet t	Yes	Yes
		ransfers		