



## Events

An *event* is any significant occurrence within or affecting the VPN 3000 Concentrator, such as an alarm, trap (an event message sent to an SNMP system is called a “trap”), error condition, network problem, task completion, threshold breach, or status change. The VPN Concentrator records events in an event log, which is stored in nonvolatile memory. You can also specify that certain events trigger a console message, a UNIX syslog record, an e-mail message, or an SNMP management system trap.

Event attributes include *class* and *severity level*.

## Event Class

*Event class* denotes the source of the event and refers to a specific hardware or software subsystem within the VPN Concentrator. [Table 9-1](#) lists the event classes.

**Table 9-1** VPN Concentrator Event Classes

Class Name	Class Description (Event Source)	Cisco-Specific Event Class?
AUTH	Authentication	N
AUTHDBG	Authentication debugging	Y
AUTHDECODE	Authentication protocol decoding	Y
AUTOUPDATE	Autoupdate subsystem	N
BMGT	Bandwidth management subsystem	Y
BMGTDBG	Bandwidth management debugging	Y
CAPI	Cryptography subsystem	N
CERT	Digital certificates subsystem including SCEP	N
CIFS	CIF file access	Y
CIFSDBG	Cif file access debugging	Y
CONFIG	Configuration subsystem	N
DHCP	DHCP subsystem	N
DHCPDBG	DHCP debugging	Y
DHCPDECODE	DHCP decoding	Y
DM	Data Movement subsystem	N

**Table 9-1** VPN Concentrator Event Classes (continued)

<b>Class Name</b>	<b>Class Description (Event Source)</b>	<b>Cisco-Specific Event Class?</b>
DNS	DNS subsystem	N
DNSDBG	DNS debugging	Y
DNSDECODE	DNS decoding	Y
EAP	EAP subsystem	Y
EAPPOUDP	EAP over UDP subsystem	Y
EVENT	Event subsystem	N
EVENTDBG	Event subsystem debugging	Y
EVENTMIB	Event MIB changes	Y
EXPANSIONCARD	Expansion card (module) subsystem	N
FILTER	Filter subsystem	N
FILTERDBG	Filter debugging	Y
FSM	Finite State Machine subsystem (for debugging)	Y
FTPD	FTP daemon subsystem	N
GENERAL	NTP subsystem and other general events	N
GRE	GRE subsystem	N
GREDBG	GRE debugging	Y
GREDECODE	GRE decoding	Y
HARDWAREMON	Hardware monitoring (fans, temperature, voltages, etc.)	N
HTTP	HTTP subsystem	N
IKE	ISAKMP/Oakley (IKE) subsystem	N
IKEDBG	ISAKMP/Oakley (IKE) debugging	Y
IKEDECODE	ISAKMP/Oakley (IKE) decoding	Y
IP	IP router subsystem	N
IPDBG	IP router debugging	Y
IPDECODE	IP packet decoding	Y
IPSEC	IP Security subsystem	N
IPSECDBG	IP Security debugging	Y
IPSECDECODE	IP Security decoding	Y
L2TP	L2TP subsystem	N
L2TPDBG	L2TP debugging	Y
L2TPDECODE	L2TP decoding	Y
LBSSF	Load Balancing subsystem	N
MIB2TRAP	MIB-II trap subsystem: SNMP MIB-II traps	N
NAC	NAC subsystem	Y
OSPF	OSPF subsystem	N

**Table 9-1** VPN Concentrator Event Classes (continued)

Class Name	Class Description (Event Source)	Cisco-Specific Event Class?
PPP	PPP subsystem	N
PPPDBG	PPP debugging	Y
PPPDECODE	PPP decoding	Y
PPTP	PPTP subsystem	N
PPTPDBG	PPTP debugging	Y
PPTPDECODE	PPTP decoding	Y
PSH	Operating system command shell	N
PSOS	Embedded real-time operating system	N
QUEUE	System queue	N
REBOOT	System rebooting	N
RM	Resource Manager subsystem	N
SMTP	SMTP event handling	N
SNMP	SNMP trap subsystem	N
SSH	SSH subsystem	N
SSL	SSL subsystem	N
SYSTEM	Buffer, heap, and other system utilities	N
TCP	TCP subsystem	N
TELNET	Telnet subsystem	N
TELNETDBG	Telnet debugging	Y
TELNETDECODE	Telnet decoding	Y
TIME	System time (clock)	N
VRRP	VRRP subsystem	N
WebVPN	SSL over VPN sessions	Y
XML	XML	N

**Note**

The Cisco-specific event classes provide information that is meaningful only to Cisco engineering or support personnel. Also, the DBG and DECODE events require significant system resources and might seriously degrade performance. We recommend that you avoid logging these events unless Cisco requests it.

# Event Severity Level

*Severity level* indicates how serious or significant the event is,. It indicates how likely it is to cause unstable operation of the VPN concentrator, whether it represents a high-level or low-level operation, or whether it returns little or great detail. Level 1 is most significant. [Table 9-2](#) describes the severity levels.

**Table 9-2** VPN Concentrator Event Severity Levels

Level	Category	Description
1	Fault	A crash or non-recoverable error.
2	Warning	A pending crash or severe problem that requires user intervention.
3	Warning	A potentially serious problem that might require user action.
4	Information	An information-only event with few details.
5	Information	An information-only event with moderate detail.
6	Information	An information-only event with greatest detail.
7	Debug	Least amount of debugging detail.
8	Debug	Moderate amount of debugging detail.
9	Debug	Greatest amount of debugging detail.
10	Packet Decode	High-level packet header decoding
11	Packet Decode	Low-level packet header decoding
12	Packet Decode	Hex dump of header
13	Packet Decode	Hex dump of packet

Within a severity level category, higher-numbered events provide more details than lower-numbered events, without necessarily duplicating the lower-level details. For example, within the Information category, Level 6 provides greater detail than Level 4, but does not necessarily include the same information as Level 4.

Logging higher-numbered severity levels causes performance to deteriorate, since more system resources are used to log and handle these events.



**Note**

The Debug (7–9) and Packet Decode (10–13) severity levels are intended for use by Cisco engineering and support personnel. We recommend that you avoid logging these events unless Cisco requests it.

The VPN Concentrator, by default, displays all events of severity level 1 through 3 on the console. It writes all events of severity level 1 through 5 to the event log. You can change these defaults on the System | Events | [General](#) screen, and you can configure specific events for special handling on the System | Events | [Classes](#) screens.

# Event Log

The VPN Concentrator records events in an event log, which is stored in nonvolatile memory. Thus the event log persists even if the system is powered off. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events. The log wraps when it is full; that is, newer events overwrite older events when the log is full.

For the event log, you can configure:

- Which event classes and severity levels to log.
- Whether to save the event log to a file in Flash memory when it is full (when it wraps). And if so:
  - The format of the information in the saved log file.
  - Whether to automatically send a copy of the saved log file via FTP to a remote system.

## Event Log Data

Each entry (record) in the event log consists of several fields including:

- A sequence number
- Date and time
- Event severity level
- Event class and number
- Event repetition count
- Event IP address (only for certain events)
- Description string

For more information, see the Monitoring | Filterable Event Log screen.

## Syslog Data and Formats

Two formats are available for all events sent to syslog servers:

- Original — Original VPN Concentrator event format with information on one line.
- Cisco IOS Compatible — Event format that is compatible with Cisco syslog management applications. Each entry in the event log is one line.

### Original Log Format

Each entry in the event log consists of the following fields:

*Sequence Date Time SEV=Severity Class/Number RPT=RepeatCount String*

- *Sequence*: The sequence number of the event.
- *Date*: The date the event occurred. The date is in the following format: MM/DD/YYYY.
- *Time*: The time the event occurred. The time is in the following format: hh:mm:ss.ttt.

- *Severity*: The severity of the event (1-13). To see how this original severity level maps to Cisco IOS severity levels, see [Table 9-3](#).
- *Class/Number*: The event class and event number. For a list of event classes, see [Table 9-1](#).
- *RepeatCount*: The number of times this particular event has occurred since the VPN Concentrator was last booted.
- *String*: The description of the event. The string sometimes includes the IP address of the user whose session generated the event.

For example:

```
3 11/04/2004 14:37:06.680 SEV=4 HTTP/47 RPT=17 10.10.1.35 New administrator login:
admin.
```

## Cisco IOS Compatible Log Format

Each entry in the event log is one line consisting of the following fields. The field values are in different order but contain the same data as Original log format, except as noted below:

*Sequence: Date Time TimeZone TimeZoneOffset %Class-Severity-Number: RPT=RepeatCount: String*

- *Date*: The date is in the following format: YYYY MMM DD.
- *TimeZone*: The time zone in which the event occurred.
- *TimeZoneOffset*: The offset of the time zone from GMT.
- *Severity*: The Cisco IOS severity of the event (0-7). [Table 9-3](#) shows the mapping between Cisco IOS format severity levels and Original format severity levels.

For example:

```
3 2004 Nov 04 14:37:06.680 EDT -4:00 %HTTP-5-47:RPT=17 10.10.1.35: New administrator
login: admin.
```

The Original severities and the Cisco IOS severities differ. Original severities number from 1-13. (For the meaning of each Original severity, see [Table 9-2 on page 9-4](#).) Cisco IOS severities number from 0-7. [Table 9-3](#) shows the meaning of Cisco IOS severities and how they map to Original severities.

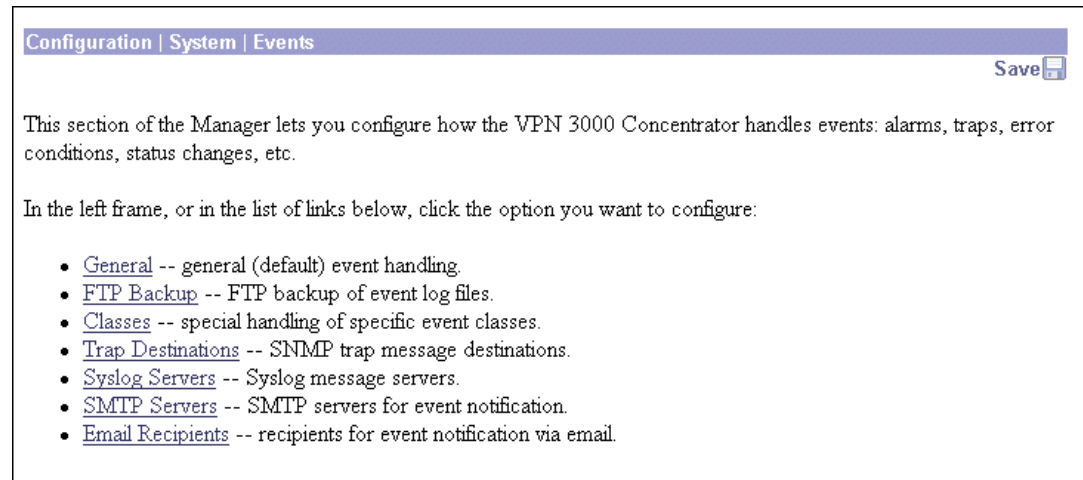
**Table 9-3 Cisco IOS Severities**

Cisco IOS Severity	Meaning	Original Severity
0	Emergencies	1
1	Alerts	Not used
2	Critical	2
3	Errors	Not used
4	Warning	3
5	Notification	4
6	Informational	5, 6
7	Debugging	7-13

# Configuration | System | Events

This section of the Manager lets you configure how the VPN Concentrator handles events. Events provide information for system monitoring, auditing, management, accounting, and troubleshooting.

**Figure 9-1** Configuration | System | Events Screen



## General

This Manager screen lets you configure the general, or default, handling of all events. These defaults apply to all event classes.

You can override these default settings by configuring specific events for special handling on the System | Events | [Classes](#) screens.

Figure 9-2 Configuration | System | Events | General Screen

Configuration | System | Events | General

This section lets you configure default event handling.

<b>Save Log on Wrap</b> <input type="checkbox"/>	Check to save the event log to a file on wrap.
<b>Save Log Format</b> <span style="border: 1px solid black; padding: 2px;">Multiline</span>	Select the format of the saved log files.
<b>FTP Saved Log on Wrap</b> <input type="checkbox"/>	Check to automatically FTP the saved log to a remote destination.
<b>Email Source Address</b> <span style="border: 1px solid black; padding: 2px;"> </span>	Enter the email address that appears in the <b>From:</b> field.
<b>Syslog Format</b> <span style="border: 1px solid black; padding: 2px;">Original</span>	Select the format of Syslog messages.
<b>Events to Log</b> <span style="border: 1px solid black; padding: 2px;">Severities 1-5</span>	Select the events to enter in the log.
<b>Events to Console</b> <span style="border: 1px solid black; padding: 2px;">Severities 1-3</span>	Select the events to display on the console.
<b>Events to Syslog</b> <span style="border: 1px solid black; padding: 2px;">None</span>	Select the events to send to a Syslog Server.
<b>Events to Email</b> <span style="border: 1px solid black; padding: 2px;">None</span>	Select the events to send to an Email Recipient.
<b>Events to Trap</b> <span style="border: 1px solid black; padding: 2px;">None</span>	Select the events to send to an SNMP Trap Destination.

---

**Event List**  
*Enter as:* Event Class/List of Event IDs, SEV(#)  
*Example:* IKE/ 1, 13-45, SEV(3)

Apply
Cancel

- Set the *Event Class* to any of the predefined event classes or **ALL** for all event classes
- Set the *List of Event IDs* to:
  - a range of numbers
  - a comma-separated list of numbers
  - or a combination of both  
(e.g. 2,5,8,13-45)
- Set Event Severities to *SEV(levels)* where *levels* can be a single number or a range of numbers

9/19/11

## Screen Elements

- **Save Log on Wrap** — Check this box to automatically save the event log when it is full. (The box is unchecked by default.) The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events. When the log is full, newer events overwrite older events; that is, entry 2049 overwrites entry 1, etc.

If you select automatic save, the system saves the log file to a file in Flash memory with the filename LOGnnnnn.TXT, where *nnnnn* is an increasing sequence number that starts with 00001 and restarts after 99999. The sequence numbers continue through reboots. For example, if four log files have already been saved, the next one saved after a reboot is LOG00005.TXT.

If Flash memory has less than 2.56 MB of free space, the system deletes the oldest log file(s) to make room for the newest saved log file. It also generates an event that notes the deletion. If there are no old log files to delete, the save function fails, and the system generates an event that notes the failure.

Each saved log file requires about 334 KB. To conserve space in Flash memory, we recommend that you periodically remove the saved log files. Keeping more than 10 to 12 files wastes space. The Administration | File Management | Files screen shows total, used, and free space in Flash memory.



### Note

The VPN Concentrator automatically saves the log file if it crashes, and when it is rebooted, regardless of this Save Log on Wrap setting. This log file is named SAVELOG.TXT, and it overwrites any existing file with that name. The SAVELOG.TXT file is useful for debugging.

You can manage saved log files with options on this screen and on the Administration | File Management screens.

- **Save Log Format** — Click this drop-down menu button to specify the format of the saved log files.
  - **Multiline:** Entries are ASCII text and appear on multiple 80-character lines (default). Choose this format for easiest reading and printing.
  - **Comma Delimited:** Each entry is a single record with fields separated by commas. Choose this format for subsequent processing by an application program such as a spreadsheet or accounting system.
  - **Tab Delimited:** Each entry is a single record with fields separated by tab characters. Choose this format for subsequent processing by an application program such as a spreadsheet or accounting system.

Refer to the section on Monitoring | Filterable Event Log in *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* for details on event log fields.

- **FTP Saved Log on Wrap** — Check this box to automatically send the saved event log file, when it wraps, via FTP to a remote computer. (The box is unchecked by default.) This option *copies* the log file but does not delete it from the VPN Concentrator. If you check this box, you must also configure FTP destination system parameters on the System | Events | [FTP Backup](#) screen.
- **E-mail Source Address** — Enter the address to put in the From: field of an e-mailed event message. Enter up to 48 alphanumeric characters with no spaces, for example: cisco@cisco.com. You should configure this field if you configure any Severity to E-mail events; if you leave it blank, the From: field has the same address as the To: field (the recipient's e-mail address).
- **Syslog Format** — Click this drop-down menu button and choose the format for all events sent to syslog servers. Choices are:
  - **Original:** Original VPN Concentrator event format.
  - **Cisco IOS Compatible:** Event format that is compatible with Cisco syslog management applications.

See [Syslog Data and Formats](#) above for a description of the differences between the two log formats.

- **Events to Log / Console / Syslog** — Click these drop-down menu buttons and choose the range of event severity levels to enter in the event log, display on the console, or send to a syslog server respectively. The choices are: None, Severity 1, Severities 1-2, Severities 1-3, Severities 1-4, Severities 1-5 and Use Event List. The defaults are:
  - **Log:** Severities 1-5
  - **Console:** Severities 1-3
  - **Syslog:** None

Using the default means that all events in the specified range are captured; for example, severity level 1 through severity level 5 are entered in the event log. If you choose Use Event List, configure the Event List to specify the event types to log, display, or send.

If you select any severity levels to send, you must also configure the syslog server(s) on the System | Events | [Syslog Servers](#) screens.

- **Events to E-mail** — Click this drop-down menu button and choose the range of event severity levels to e-mail to recipients by default. The choices are: None, Severity 1, Severities 1-2, Severities 1-3, and Use Event List. The default is None. Using the default means that no events are sent via e-mail. If you choose Use Event List, configure the Event List to specify the event types to e-mail.

If you select any severity levels events to e-mail, you must also configure an SMTP server on the System | Events | [SMTP Servers](#) screens, and you must configure e-mail recipients on the System | Events | [E-mail Recipients](#) screens. You should also configure the preceding E-mail Source Address.

- **Events toTrap** — Click this drop-down menu button and choose the range of event severity levels to send to an SNMP network management system by default. Event messages sent to SNMP systems are called “traps.” The choices are: None, Severity 1, Severities 1-2, Severities 1-3, and Use Event List. The default is None: no events are sent as SNMP traps. If you choose Use Event List, configure the Event List to specify the event types to trap.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the System | Events | [Trap Destinations](#) screens.

The VPN Concentrator can send the standard, or “well-known,” SNMP traps listed in [Table 9-4](#). To have an SNMP NMS receive them, you must configure the events as in the table, and configure a trap destination.

**Table 9-4** Configuring “Well-Known” SNMP Traps

To Send this “Well-Known” SNMP Trap	Configure Either General Event Handling or this Event Class	With this Severity to Trap
coldStart	EVENT	1 or higher
linkDown	IP	1-3 or higher
linkUp	IP	1-3 or higher
authFailure (This trap is SNMP authentication failure, not tunnel authentication failure.)	SNMP	1-3 or higher

- **Event List** — Use the Event List text box to define particular events that you want to track. This feature allows you to pare down the event log to contain just the events that interest you. You can track events by class, severity, or event ID. See [Event List](#) below for details.

## Event List

You can use this feature in two ways. You can set *global* defaults to track this customized list, sending the results to your preferred event destination (log, console, syslog, e-mail, or trap). Or, you can override global defaults to track this customized list for an *individual* event class.

To set global defaults to track this customized list of events:

- Define the event list, including the event classes, event severities, or particular event IDs to track.
- Choose **Use Event List** from one or more of the following drop-down menus on the System | Events | [General](#) page (this page): Events to Log, Events to Console, Events to Syslog, Events to E-mail, Events to Trap.

To override any global defaults for a particular event class to track these events only, within that class:

- Define the event list, including the event severities or particular events within the event classes that you want to track.
- On the System | Events | [Classes](#) page, select the event class you want to modify or add a new one.

- On the System | Events | [Classes | Add or Modify](#) page, choose **Use Event List** from one or more of the following drop-down menus: Events to Log, Events to Console, Events to Syslog, Events to E-mail, Events to Trap.

## Event List Syntax

Each line in the Event List represents one entry. Each entry has the following format: *<Event Class> / <List of Event IDs or Severity Numbers>* where:

Variable	Can be...	Syntax	For example
<i>Event Class</i>	Any predefined event class	Use event class name	IKE
	All event classes	Use keyword "ALL" <sup>1</sup>	ALL
<i>Event IDs</i>	A single event number	Use event number	123
	A range of event numbers	Use hyphen to indicate range	13-45
<i>Severity Numbers</i>	An event severity level or a range of event severity levels.	Use "SEV(L)" where L is the event severity level or the range of event severity levels	SEV(1) SEV(1-3)
	A combination of single events, a range of events, or event severities		IKE/1,13-45,SEV(3)

1. For the ALL event class, you can specify only event severities, not particular event numbers. For example, ALL/SEV(1) is a valid entry; ALL/123 is not.

Note the following rules:

- Separate each entry by a carriage return.
- An event class can appear multiple times on the list. For example:  
IKE/SEV(1), SEV(3)  
IKE/1, 13-45
- You can use spaces and tabs. The VPN Concentrator ignores all white space in the entry.
- Unknown event classes are not treated as errors, so you can use the same Event List across VPN Concentrators running different versions of the software.

The following lines are examples of valid event list entries:

```
ALL/SEV(1)
AUTH/1, 3-8, 22, SEV(2)
IKE/SEV(5-6)
```

# FTP Backup

This screen lets you configure parameters for using FTP to automatically back up saved event log files on a remote computer. If you enable FTP Saved Log on Wrap on the System | Events | [General](#) screen, you must configure the FTP parameters on this screen.

The VPN Concentrator acts as an FTP client when executing this function.



## Note

Another way to back up saved event log files on a remote computer is to enable an external Syslog server.

**Figure 9-3** Configuration | System | Events | FTP Backup Screen

Configuration | System | Events | FTP Backup

This screen lets you configure FTP backup options for the log.

**FTP Server**  Enter the IP address or hostname of the destination FTP server.

**FTP Directory**  Enter the directory pathname for files on the FTP server.

**FTP Username**  Enter the username to log on to the FTP server.

**FTP Password**  Enter the password to log on to the FTP server.

**Verify**  Re-enter the password to verify it.

Apply Cancel

67173

## Screen Elements

- **FTP Server** — Enter the IP address or host name of the destination computer to receive copies of saved event log files via FTP. (If you have configured a DNS server, you can enter a host name; otherwise enter an IP address.)
- **FTP Directory** — Enter the complete directory path name on the destination computer to receive copies of saved event log files. For example, c:\vpn\logfiles.
- **FTP Username** — Enter the username for FTP login on the destination computer.
- **FTP Password** — Enter the password to use with the FTP username. The field displays only asterisks.
- **Verify** — Re-enter the FTP password to verify it. The field displays only asterisks.

## Reminder:

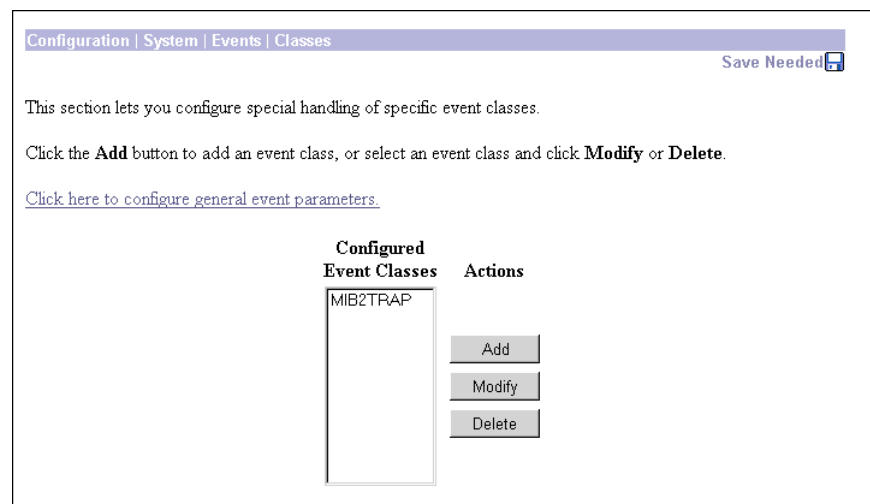
After you apply changes, the Manager returns to the [Configuration | System | Events](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# Classes

This section of the Manager lets you add, configure, modify, and delete specific event classes for special handling. You can thus override the general, or default, handling of event classes. For example, you might want to send e-mail for HARDWAREMON events of severity 1 and 2, whereas default event handling does not send any e-mail.

Event classes denote the source of an event and refer to a specific hardware or software subsystem within the VPN Concentrator. [Table 9-1](#) describes the event classes.

**Figure 9-4** Configuration | System | Events | Classes Screen



To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*”

## Screen Elements

- **Configured Event Classes** — The Configured Event Classes list shows the event classes that have been configured for special handling. The initial default entry is MIB2TRAP, which are SNMP MIB-II events, or “traps,” that you might want to monitor with an SNMP network management system. Other configured event classes are listed in order by class number and name. If no classes have been configured for special handling, the list shows --Empty--.
- **Add** — Click to configure and add a new event class for special handling. See System | Events | Classes | [Add or Modify](#).
- **Modify** — To modify an event class that has been configured for special handling, select the event class from the list and click **Modify**. See System | Events | [Classes | Add or Modify](#).
- **Delete** — To remove an event class that has been configured for special handling, select the event class from the list and click **Delete**.



### Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the list.

# Classes | Add or Modify

These screens let you:

- Add and configure the special handling of a specific event class.
- Modify the special handling of a specific event class.

If you chose **Use Event List** for any of the fields on the System | Events | **General** screen, that default will appear for the same field on this screen. For example, if you chose **Use Event List** for the **Events to Trap** field on the System | Events | **General** screen, the **Events to Trap** field on this screen defaults to **Use Event List** as well.

**Figure 9-5** Configuration | System | Events | Classes | Add or Modify Screen

Configuration | System | Events | Classes | Add

This screen lets you add and configure an event class for special handling.

Class Name  Select the event class to configure.

Enable  Check to enable special handling of this class.

---

If one of the following values has been set to *Use Event List*, the Event List can be seen by viewing **Configuration | System | Events | General**.

Changing a value set to *Use Event List* will override the sections of the Event List referring to this event class.

Events to Log  Select the events to enter in the log.

Events to Console  Select the events to display on the console.

Events to Syslog  Select the events to send to a Syslog Server.

Events to Email  Select the events to send to an Email Recipient.

Events to Trap  Select the events to send to an SNMP Trap Destination.

83864

## Screen Elements

- **Class Name** — Click the drop-down menu button and choose the event class you want to add and configure for special handling. (Please note that Select Class is an instruction reminder, not a class.) [Table 9-1](#) describes the event classes.

On the **Modify** screen, the field shows the configured event class you are modifying. You cannot change this field.

All subsequent parameters on this screen apply to this event class only.

- **Enable** — Check this box to enable the special handling of this event class. (The box is checked by default.)

Unchecking this box lets you set up the parameters for the event class but activate it later, or temporarily disable special handling without deleting the entry. The Configured Event Classes list on the System | Events | **Classes** screen indicates disabled event classes. Disabled event classes are handled in accordance with the default parameters for all event classes.

- **Events to Log / Console / Syslog** — Click these drop-down menu buttons and choose the range of event severity levels to enter in the event log, display on the console, or send to a syslog server respectively. The choices are: None, Severity 1, Severities 1-2, Severities 1-3, ..., Severities 1-13, and Use Event List. The defaults are:

- **Log:** Severities 1-5
- **Console:** Severities 1-3
- **Syslog:** None

Using the default means that all events in the specified range are captured; for example, severity level 1 through severity level 5 are entered in the event log. If you choose Use Event List, configure the Event List on the System | Events | [General](#) screen to specify which of the particular events in this class you want to log, display, or send.

If you select any severity levels to send, you must also configure the syslog server(s) on the System | Events | [Syslog Servers](#) screens, and you should configure the Syslog Format on the System | Events | [General](#) screen.


**Note**

Sending events to a syslog server generates IP packets, which can generate new events if this setting is above level 9. We strongly recommend that you keep this setting at or below level 6. Avoid setting this parameter above level 9.

- **Events to E-mail** — Click this drop-down menu button and choose the range of event severity levels to send to recipients via e-mail. The choices are: None, Severity 1, Severities 1-2, Severities 1-3, and Use Event List. The default is None: no events are sent via e-mail.

If you select any event severity levels to e-mail, you must also configure an SMTP server on the System | Events | [SMTP Servers](#) screen, and you must configure e-mail recipients on the System | Events | [E-mail Recipients](#) screens. You should also configure the E-mail Source Address on the System | Events | [General](#) screen.

If you choose Use Event List, configure the Event List on the System | Events | [General](#) page to specify which of the particular events in this class you want to send.

- **Events toTrap** — Click this drop-down menu button and choose the range of event severity levels to send to an SNMP network management system. Event messages sent to SNMP systems are called “traps.” The choices are: None, Severity 1, Severities 1-2, Severities 1-3, Severities 1-4, Severities 1-5, and Use Event List. The default is None. Using the default means that no events are sent as SNMP traps.

If you select any event severity levels to send, you must also configure SNMP destination system parameters on the System | Events | [Trap Destinations](#) screens.

To configure “well-known” SNMP traps, see [Table 9-4](#) under Events to Trap for System | Events | [General](#).

- **Add or Apply / Cancel** — To add this event class to the list of those with special handling, click **Add**. Or to apply your changes to this configured event class, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the System | Events | [Classes](#) screen. Any new event class appears in the Configured Event Classes list. To discard your settings, click **Cancel**.

**Reminder:**

After you apply changes, the Manager returns to the System | Events | [Classes](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# Trap Destinations

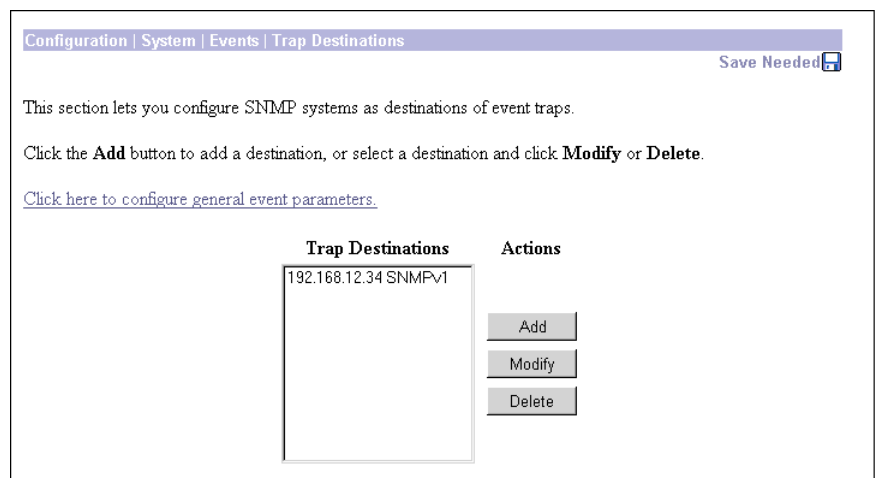
This section of the Manager lets you configure SNMP network management systems as destinations of event traps. Event messages sent to SNMP systems are called “traps.” If you configure any event handling—default or special—with values in **Events to Trap** fields, you must configure trap destinations in this section.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the System | Events | [Classes](#) screens.

To configure well-known SNMP traps, see [Table 9-4](#).

To have an SNMP-based network management system (NMS) receive any events, you must also configure the NMS to see the VPN Concentrator as a managed device or agent in the NMS domain.

**Figure 9-6** Configuration | System | Events | Trap Destinations Screen



## Screen Elements

- **Trap Destinations** — The Trap Destinations list shows the SNMP network management systems that have been configured as destinations for event trap messages, and the SNMP protocol version associated with each destination. If no trap destinations have been configured, the list shows --Empty--.
- **Add** — Click to configure a new SNMP trap destination. See System | Events | [Trap Destinations | Add or Modify](#).
- **Modify** — To modify an SNMP trap destination that has been configured, select the destination from the list and click **Modify**. See System | Events | [Trap Destinations | Add or Modify](#).
- **Delete** — To remove an SNMP trap destination that has been configured, select the destination from the list and click **Delete**.



### Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the list.

# Trap Destinations | Add or Modify

These screens let you:

- Add an SNMP destination system for event trap messages.
- Modify a configured SNMP destination system for event trap messages.

**Figure 9-7** Configuration | System | Events | Trap Destinations | Add or Modify Screen

Configuration | System | Events | Trap Destinations | Add

Add a trap destination.

**Destination**  Enter the IP address or hostname of the trap destination.

**SNMP Version**  Select the SNMP version of the trap to send to this destination.

**Community**  Enter the community string to use in the trap. Default is "public".

**Port**  Enter the destination port for the trap.

67165

## Screen Elements

- **Destination** — Enter the IP address or host name of the SNMP network management system that is a destination for event trap messages. (If you have configured a DNS server, you can enter a host name; otherwise enter an IP address.)
- **SNMP Version** — Click this drop-down menu button and choose the SNMP protocol version to use when formatting traps to this destination. Choices are SNMPv1 (version 1; the default) and SNMPv2 (version 2).
- **Community** — Enter the community string to use in identifying traps from the VPN Concentrator to this destination. The community string is like a password: it validates messages between the VPN Concentrator and this NMS destination. If you leave this field blank, the default community string is public.
- **Port** — Enter the UDP port number by which you access the destination SNMP server. Use a decimal number from 0 to 65535. The default value is 162, which is the well-known port number for SNMP traps.
- **Add or Apply / Cancel** — To add this system to the list of SNMP trap destinations, click **Add**. Or to apply your changes to this trap destination, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the System | Events | [Trap Destinations](#) screen. Any new destination system appears in the Trap Destinations list. To discard your settings, click **Cancel**.

### Reminder:

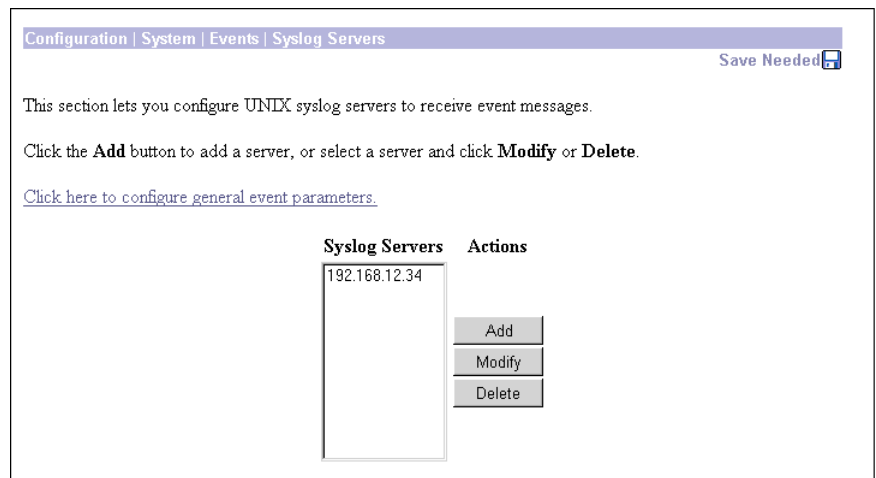
After you apply changes, the Manager returns to the System | Events | [Trap Destinations](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# Syslog Servers

This section of the Manager lets you configure syslog servers as recipients of event messages. Syslog is a daemon, or background process, that records events. The VPN Concentrator can send event messages in two syslog formats to configured syslog systems. If you configure any event handling—default or special—with values in **Events to Syslog** fields, you must configure syslog servers in this section.

To configure default event handling and syslog formats, click the highlighted link that says “Click here to configure general event parameters.” To configure special event handling, see the System | Events | [Classes](#) screens.

**Figure 9-8** Configuration | System | Events | Syslog Servers Screen



## Screen Elements

- **Syslog Servers** — The Syslog Servers list shows the syslog servers that have been configured as recipients of event messages. You can configure a maximum of five syslog servers. If no syslog servers have been configured, the list shows --Empty--.
- **Add** — Click to configure a new syslog server. See System | Events | [Syslog Servers | Add or Modify](#).
- **Modify** — To modify a syslog server that has been configured, select the server from the list and click **Modify**. See System | Events | [Syslog Servers | Add or Modify](#).
- **Delete** — To remove a syslog server that has been configured, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

### Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# Syslog Servers | Add or Modify

These screens let you:

- Add a syslog server as a recipient of event messages. You can configure a maximum of five syslog servers.
- Modify a configured syslog server that is a recipient of event messages.

**Figure 9-9** Configuration | System | Events | Syslog Servers | Add or Modify Screen

## Screen Elements

- **Syslog Server** — Enter the IP address or host name of the syslog server to receive event messages. (If you have configured a DNS server, you can enter a host name; otherwise, enter an IP address.)
- **Port** — Enter the UDP port number by which you access the syslog server. Use a decimal number from 0 to 65535. The default value is 514, which is the well-known port number.
- **Facility** — Click this drop-down menu button and choose the syslog facility tag for events sent to this server. The facility tag lets the syslog server sort messages into different files or destinations. The choices are:
  - User = Random user-process messages.
  - Mail = Mail system.
  - Daemon = System daemons.
  - Auth = Security or authorization messages.
  - Syslog = Internal syslogd-generated messages.
  - LPR = Line printer subsystem.
  - News = Network news subsystem.
  - UUCP = UUCP (UNIX-to-UNIX Copy Program) subsystem.
  - Reserved (9) through Reserved (14) = Outside the Local range, with no name or assignment yet, but usable.
  - CRON = Clock daemon.
  - Local 0 through Local 7 (default) = User defined.
- **Add or Apply / Cancel** — To add this server to the list of syslog servers, click **Add**. Or to apply your changes to this syslog server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the System | Events | [Syslog Servers](#) screen. Any new server appears in the Syslog Servers list. To discard your entries, click **Cancel**.

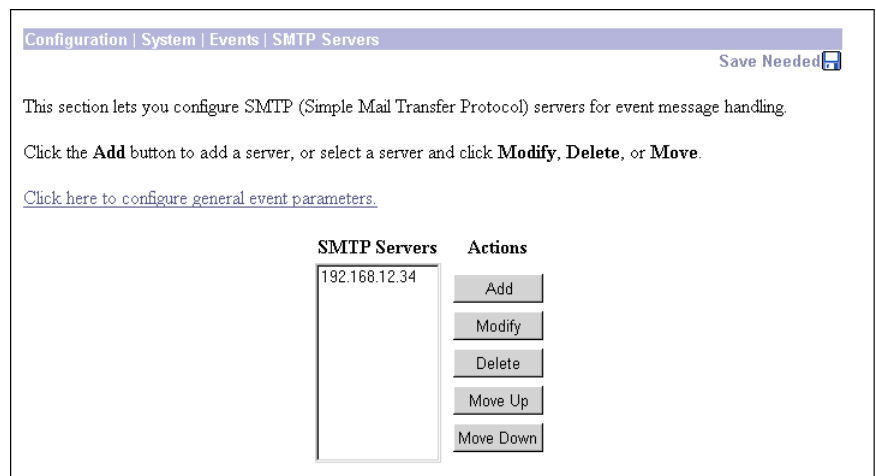
# SMTP Servers

This section of the Manager lets you configure SMTP servers that you use to e-mail event messages to e-mail recipients. If you configure any event handling—default or special—with values in **Events to E-mail** fields, you must identify at least one SMTP server to handle the outgoing e-mail, and you must name at least one e-mail recipient to receive the event messages. You can configure two SMTP servers: one primary and one backup in case the primary is unavailable.

To configure e-mail recipients, see the System | Events | [E-mail Recipients](#) screen.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the System | Events | [Classes](#) screens.

**Figure 9-10** Configuration | System | Events | SMTP Servers Screen



## Screen Elements

- **SMTP Servers** — The SMTP Servers list shows the configured SMTP servers in the order in which the system accesses them. You can configure two prioritized SMTP servers so that you have a backup server in case the primary server is offline, congested, etc. If no SMTP servers have been configured, the list shows --Empty--.
- **Add** — Click to configure a new SMTP server. See System | Events | [SMTP Servers | Add or Modify](#).
- **Modify** — To modify a configured SMTP server, select the server from the list and click **Modify**. See System | Events | [SMTP Servers | Add or Modify](#).
- **Delete** — To remove a configured SMTP server, select the server from the list and click **Delete**.



### Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the SMTP Servers list.

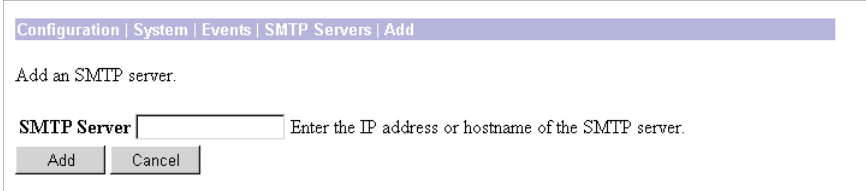
- **Move** — To change the order in which the system accesses configured SMTP servers, select the server from the list and click **Move Up** or **Move Down**. The Manager refreshes the screen and shows the reordered SMTP Servers list.

# SMTP Servers | Add or Modify

These screens let you:

- Add an SMTP server to the list of configured SMTP servers. You can configure two SMTP servers: a primary and a backup.
- Modify the IP address or host name of a configured SMTP server.

**Figure 9-11** Configuration | System | Events | SMTP Servers | Add or Modify Screen



Configuration | System | Events | SMTP Servers | Add

Add an SMTP server.

SMTP Server  Enter the IP address or hostname of the SMTP server.

Add Cancel

67163

## Screen Elements

- **SMTP Server** — Enter the IP address or host name of the SMTP server. (If you have configured a DNS server, you can enter a host name; otherwise, enter an IP address.)
- **Add or Apply / Cancel** — To add this server to the list of SMTP servers, click **Add**. Or to apply your changes to this SMTP server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the System | Events | [SMTP Servers](#) screen. Any new server appears in the SMTP Servers list. To discard your entry, click **Cancel**.

### Reminder:

After you apply changes, the Manager returns to the System | Events | [SMTP Servers](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# E-mail Recipients

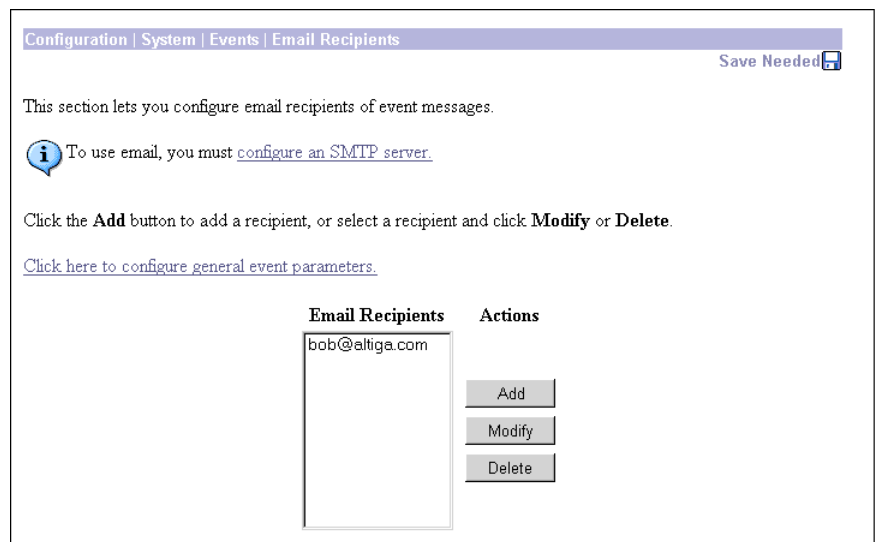
This section of the Manager lets you configure e-mail recipients of event messages. You can configure a maximum of five e-mail recipients, and you can customize the event message severity levels for each recipient.

If you configure any event handling (either default or special) with values in **Events to E-mail** fields, you must name at least one e-mail recipient to receive the event messages, and you must identify at least one SMTP server to handle the outgoing e-mail. You should also configure the **E-mail Source Address** on the System | Events | [General](#) screen.

To configure SMTP servers, see the System | Events | [SMTP Servers](#) screen, or click the highlighted link that says “*configure an SMTP server.*”

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the System | Events | [Classes](#) screens.

**Figure 9-12** Configuration | System | Events | E-mail Recipients Screen



## Screen Elements

- **E-mail Recipients** — This list shows configured event message e-mail recipients in the order they were configured. You can configure a maximum of five e-mail recipients. If no e-mail recipients have been configured, the list shows --Empty--.
- **Add** — Click to configure a new e-mail recipient. See System | Events | [E-mail Recipients | Add or Modify](#).
- **Modify** — To modify an e-mail recipient who has been configured, select the recipient from the list and click **Modify**. See System | Events | [E-mail Recipients | Add or Modify](#).
- **Delete** — To remove an e-mail recipient who has been configured, select the recipient from the list and click **Delete**.



### Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining recipients in the E-mail Recipients list.

## E-mail Recipients | Add or Modify

These screens let you:

- Add and configure an event message e-mail recipient. You can configure a maximum of five e-mail recipients.
- Modify the parameters for a configured e-mail recipient.

**Figure 9-13** Configuration | System | Events | E-mail Recipients | Add or Modify Screen

### Screen Elements

- **E-mail Address** — Enter the recipient's complete e-mail address, for example: cisco@cisco.com.
- **Max Severity** — Click this drop-down menu button and choose the range of event severity levels to send to this recipient via e-mail. The choices are: None, 1, 1-2, 1-3. The default value is 1-3: configured events of severity level 1 through severity level 3 are sent to this recipient.

The event levels e-mailed to this recipient are the *lesser of* the **Events to E-mail** setting for a customized event class, or this **Max Severity** setting. If an event class has not been customized, the events e-mailed are the *lesser of* this setting or the *default Events to E-mail* setting. For example, if you configure IPSEC events with severity levels 1-3 to e-mail, all other events with no severity to e-mail, and cisco@cisco.com to receive e-mail events of severity levels 1-2, cisco will receive only IPSEC events of severity levels 1-2.

- **Add or Apply / Cancel** — To add this recipient to the list of e-mail recipients, click **Add**. Or to apply your changes to this e-mail recipient, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the System | Events | [E-mail Recipients](#) screen. Any new recipient appears at the bottom of the E-mail Recipients list. To discard your entry, click **Cancel**.

### Reminder:

After you apply changes, the Manager returns to the System | Events | [E-mail Recipients](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

