Cisco Active Network Abstraction EventVision User Guide Version 3.6

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12503-01

Cisco Active Network Abstraction EventVision User's Guide, Version 3.6

CONTENTS

Preface

This guide describes the events that are logged in the Cisco ANA Gateway and how they can be viewed.

- Chapter 1, "Introducing EventVision"—Overviews the Cisco ANA EventVision application used to view events and describes event categories.
- Chapter 2, "Getting Started with EventVision"—Describes how to open the Cisco ANA EventVision window, and the Cisco ANA EventVision window, including its toolbar and menus.
- Chapter 3, "Viewing Events in EventVision"—Describes the EventVision tabs used for viewing system and network events.
- Chapter 4, "Working in EventVision"—Describes how to filter and display view the properties of specific events, refresh and export events.

Note Changes to the registry should only be carried out with the support of Cisco Professional Services.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Introducing EventVision

Cisco ANA EventVision is the intuitive interface used by administrators for viewing system events and tickets that are generated within the Cisco ANA system.

About EventVision

EventVision is a GUI application that serves as a browser for viewing and retrieving detailed information about the different types of system events and tickets that are generated within the Cisco ANA system. Monitoring EventVision helps predict and identify the sources of system problems, which in turn assists in preventing future problems.

You can configure EventVision to display the following information:

- Number of events per page (default 50 events).
- Amount of events to be exported to a file.
- Display previous dated events (in weeks).
- Filter options.
- What information appears in EventVision tabs, such as the **Audit** tab.

System managers or administrators periodically review and manage the events list using EventVision. In addition, when an event occurs in the Cisco ANA system the details are available in EventVision.

All administrator activities in Cisco ANA Manage are logged and available in EventVision. For more information on Cisco ANA Manage, refer to the *Cisco Active Network Abstraction ANA Administrator's Guide*.

EventVision Overview

Every event that occurs in the Cisco ANA system and the Cisco ANA Gateway is logged. This includes all events that are performed as part of the normal operation of the Cisco ANA system, as well as events that may need further attention. Events are categorized and any of these log entries can be viewed in EventVision events list tabs as follows:

- Audit
- Provisioning
- Security
- Service

- Syslog
- System
- Ticket
- V1 Trap
- V2 Trap

Basic Concepts and Terms

Alarm

An alarm represents a fault scenario that occurs in the network or management system. Alarms represent the complete fault lifecycle, from the time that the alarm is opened (when the fault is first detected) until it is closed and acknowledged. Examples of alarms include:

- Link down
- Device unreachable
- Card out
- An alarm is composed of a sequence of events, each representing a specific point in the alarm's lifecycle.

Event

An event is an indication of a distinct "activity" that occurred at a specific point in time. Events are derived from incoming traps or notifications and from detected status changes. Examples of events include:

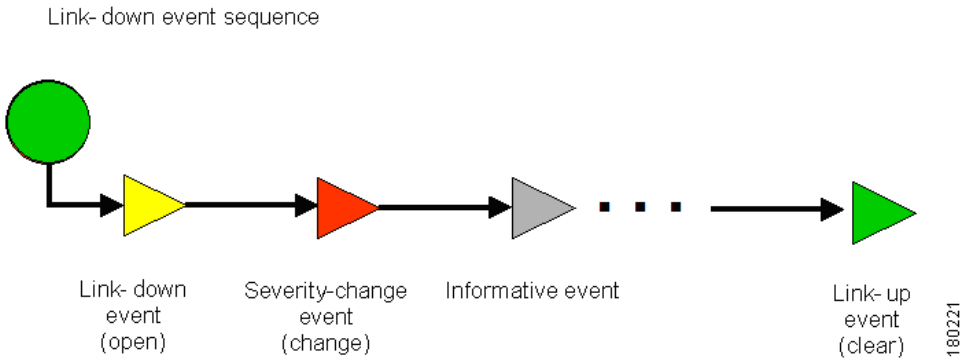
- Port status change
- Route entry drop
- Device reset
- Device becoming reachable
- User acknowledgement of an alarm

Events are written to the Cisco ANA database once and never change.

Event Sequence

An event sequence is the set of related events, which composes a single alarm. For example, Link down – Ack – Link up.

Figure 1-1 Link Down Example



Typically, a complete event sequence includes three mandatory events:

- Alarm Open (in this example, a Link Down event).
- Alarm Clear (in this example, a Link Up event).
- Alarm Acknowledge (not shown in this example).

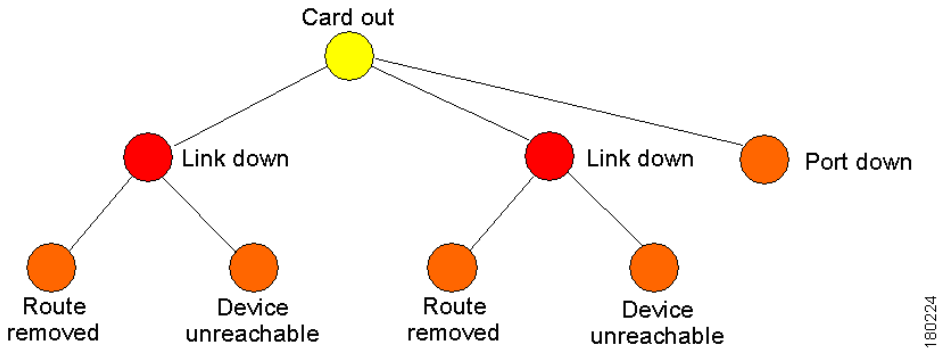
Optionally, there can be any number of alarm change events, which can be triggered by new severity events, affected services update events, and so on.

Correlation by Root Cause

Root-cause correlation is determined between alarms (namely, between event sequences). It represents a causal relationship between an alarm and the consequent alarms that originate from it.

For example, a card-out alarm can be the root cause of several link-down alarms, which in turn can be the root cause of multiple route lost and device unreachable alarms, and so on (a consequent alarm can serve as the root cause of other consequent alarms).

Figure 1-2 Card-Out Example



Ticket

A ticket represents the complete alarm correlation tree of a specific fault scenario. It can be also identified by the topmost (“root of all roots”) alarm. EventVision’s Ticket Properties dialog box displays only tickets, but allows drilling down to view the consequent alarm hierarchy.

From an operator's point of view, the managed entity is always a complete ticket. Operations such as Acknowledge, Force-Clear or Remove are always applied to the whole ticket. The ticket also assumes an overall, propagated severity.

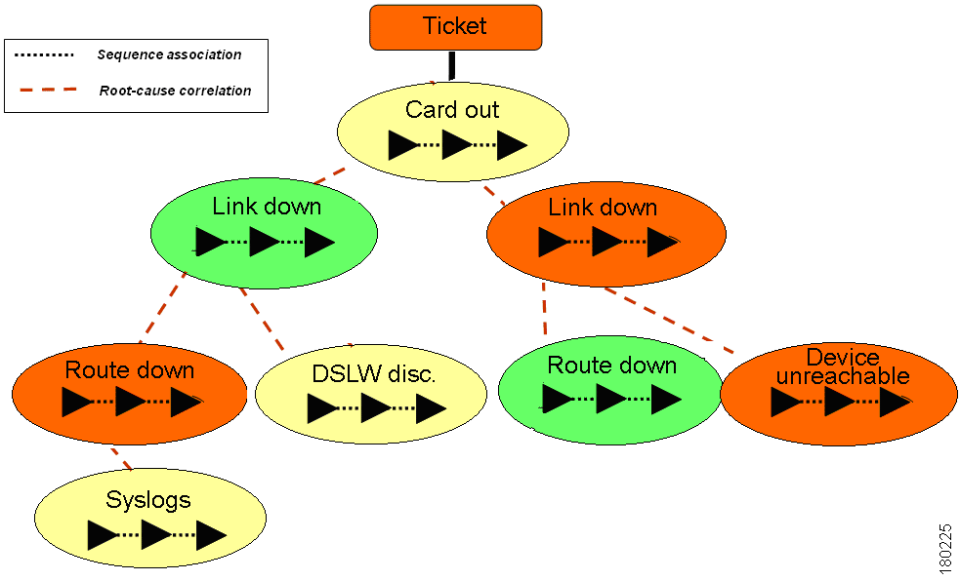
Sequence Association vs. Root-Cause Correlation

It is important not to confuse between the two types of relationships in Cisco ANA alarm management:

- **Sequence Association—**The association between events, which creates the event sequences (namely, alarms). It implements either built-in or user-defined relations (namely, specification of the event types composing each sequence).
- **Root-Cause Correlation—**The association between alarms (event sequences), which represents the root cause relationship.

The following figure shows how both types of relations are implemented in the ticket hierarchy. The alarms are correlated into a hierarchy according to root cause. Within each alarm is its respective event sequence, representing the lifecycle of the alarm.

Figure 1-3 Sequence Association and Root-Cause Correlation



EventVision Categories

EventVision recognizes the following categories of events:

- **Audit—**Related to the running of commands in the Cisco ANA Gateway.
- **Provisioning—**Related to configuration and provisioning activities.
- **Security—**Related to client login and user activity when managing the system and the environment.
- **Service—**Related to the alarms that are generated by the Cisco ANA system.
- **Syslog—**Related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events.

- **System—**Related to the everyday working of the internal system and its components. These events may be related to Cisco ANA and Cisco ANA Gateway resources, representing the system log.
- **Ticket—**Related to all the tickets that were opened in Cisco ANA.
- **V1 Trap—**Related to SNMPv1 traps from the devices by the VNEs, which are used to generate the trap events.
- **V2 Trap—**Related to SNMPv2 traps from the devices by the VNEs, which are used to generate the trap events.

You can also view all the events in the **All** tab, if required. For more information about the **All** tab, see All Tab, page 3-1.

CHAPTER 2

Getting Started with EventVision

This chapter describes the EventVision application and the options you can use to view system events and tickets that are generated within the Cisco ANA system.

Note EventVision is available only to administrators.

- Launching EventVision—Describes how to launch EventVision.
- The EventVision Window—Details the EventVision menu options, including using the toolbar buttons to navigate through the application.
- Setting EventVision Viewing Options—Explains how to define the constraints for displaying events in the EventVision window.

Launching EventVision

This section provides instructions for launching EventVision. EventVision is password protected to ensure security. Before you start working with EventVision make sure you know your username, password, and the Cisco ANA Gateway IP address or hostname that you require.

Note If a user does not log into the Cisco ANA Manage, NetworkVision or EventVision applications during a specified period of time (the default is 30 days) the account will be automatically locked. The default period can be changed in the Cisco ANA Manage per user in the Properties dialog box. (For more information about changing the default period and unlocking an account, refer to the *Cisco Active Network Abstraction Administrator's Guide.*) The period of time is measured from the time the user last logged out of any of the Cisco ANA Client applications.

To start EventVision:

Step 1 From the Start menu, select the **Programs** folder, then **Cisco ANA/Cisco ANA EventVision**.

The login dialog box appears.

Step 2 Enter your username and password.

Step 3 Enter the required Cisco ANA Gateway's information in the **Host** field, as an IP address or hostname,

or

Select a Cisco ANA Gateway from the **Host** list.

Note The Cisco ANA Gateway IP address or hostname that was used when you last logged in is automatically displayed at the top of the Host list.

Note Make sure that you use the leading IP address (the IP on which the Cisco ANA Gateway was configured) when logging into the system.

Step 4 Click **OK**. The EventVision window appears (The Event Properties detail pane is not displayed by default).

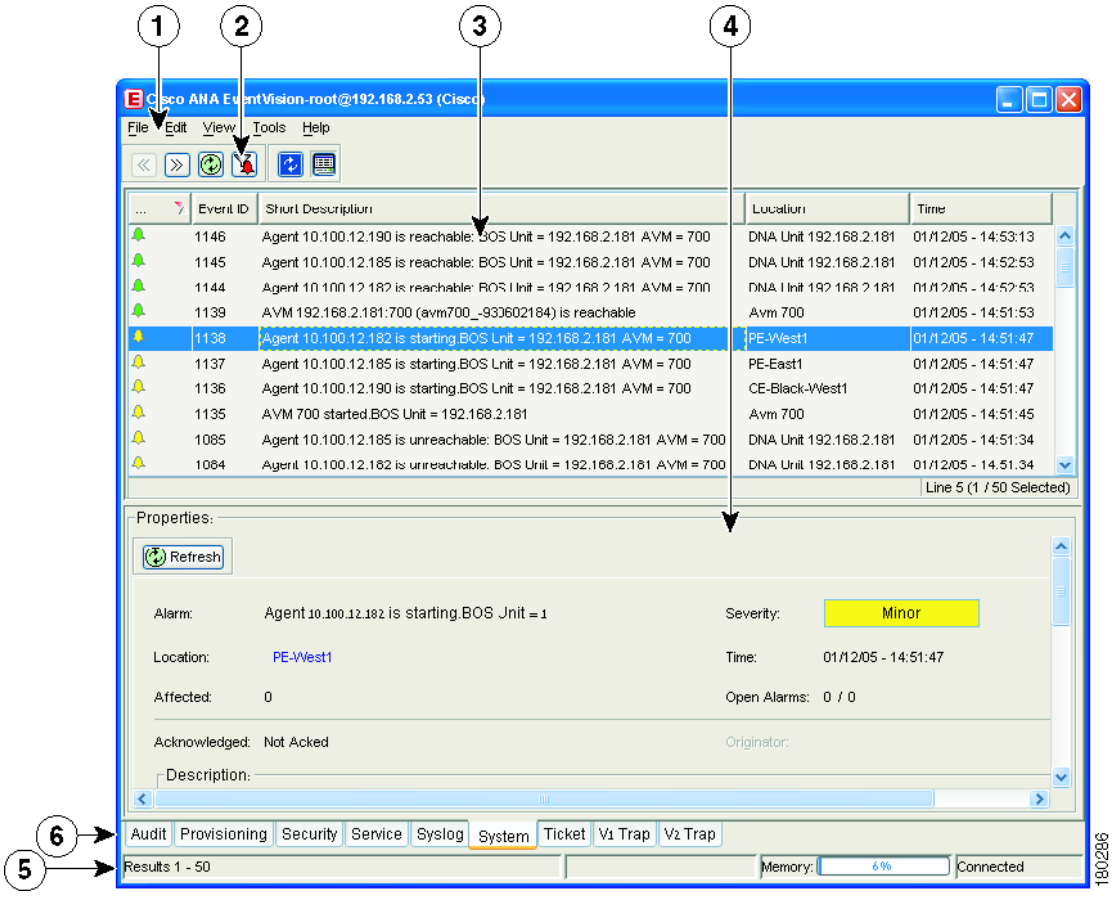
If this is the first time you have logged on, you will see the **Ticket** tab.

If you are logging in again, you will see the tab that was visible when you logged out of the application.

The EventVision Window

The EventVision window displays the events generated in the system. The following figure shows an example of the EventVision window.

Figure 2-1 EventVision Window



1	Menu bar
2	Toolbar
3	Table pane
4	Event Properties pane
5	Status bar
6	EventVision tabs

The EventVision window is divided into the following parts:

- EventVision Menus
- EventVision Navigation Toolbar.
- The **Events List** and **Properties** pane includes tabs that enable you to view the specific events described on the selected page.

You can display the Events List only (without the Event Properties pane), and select the required tab to display events, such as **Provisioning** events only, see Shortcut Properties Menu for an example.

You can also display the following information using the EventVision window toolbar and menu options:

- Define EventVision display and configuration options. See Setting EventVision Viewing Options, page 2-5.
- Display the **All** tab. See All Tab, page 3-1.
- Filter dialog box to (filter-in) display selected lines only. See Filtering Events, page 4-8.
- Selected event properties in a separate window. See Viewing Event Properties, page 4-1.

EventVision Menus

This section provides a description of each option available in the EventVision menus and shortcut menus.

File Menu

The File menu enables you to export the information displayed and to exit the application:

- **Export**—Exports the log event information displayed in the EventVision window according to the criteria defined in the EventVision Options dialog box.
- **Open All Tab**—Opens the **All** tab.

Edit Menu

The Edit menu enables you to define a filter for events displayed in the EventVision window:

- **Filter**—Defines a filter for the events displayed in the EventVision window according to the tab selected. See Filtering Events, page 4-8.
- **Purge**—This option is currently unavailable in this version.

View Menu

The View menu enables you to refresh and navigate through the EventVision window as well as view event properties:

- **Refresh**—Refreshes the information displayed in the EventVision window.
- **Go To**—Navigates to:
  - **Previous Page**—The previous page of events in the EventVision window.
  - **Next Page**—The next page of events in the EventVision window.
- **Properties**—Displays the properties of the selected event, for example, the root cause and source. For more information. See Viewing Event Properties, page 4-1.
- **Details Pane**—Displays or hides the Details pane. If an event is selected then the properties of the selected event are displayed in the Details pane.

Tools Menu

The Tools menu enables you to define various options for displaying events in the EventVision window's Table pane:

- **Change User Password**—Allows you to change the password used when logging into the Cisco ANA Client application suite. The change will take effect the next time you log into the application.
- **Options**—Defines the display options for the EventVision window. For more information, see Setting EventVision Viewing Options, page 2-5.

Help Menu

The Help menu provides information about EventVision:

- **Cisco ANA EventVision Help**—Opens the online help for EventVision.
- **Cisco.com**—This option is currently unavailable in this version.
- **About Cisco ANA EventVision**—Displays application information, for example, the version number.

Shortcut Properties Menu

Displays the properties of an event selected in the Event Properties window. See Viewing Event Properties, page 4-1.

Color Coding of Events List Severity Icons

The Events List is color coded according to the severity of the event. An icon appears for each event (ticket/event) in the EventVision tabs (based on its severity) as follows:

- **Red—**Critical
- **Orange—**Major
- **Yellow—**Minor
- **Sky Blue—**Warning

- **Green—**Cleared/Normal/OK
- **Dark Blue—**Information

EventVision Navigation Toolbar

The EventVision window contains the following tools in the navigation bar/toolbar:

Table 2-1 EventVision Tools

Button	Function
	Goes back to the previous page of events in the EventVision window.
	Goes forward to the next page of events in the EventVision window.
	Refreshes the events (if a filter is active, the refresh is done according to the filter) displayed in the log by querying the database. The log returns to the beginning of the list, displaying the events in ascending or descending order depending on the order of the current list. Descending order means that the last event is displayed first. For more information, see Refreshing the Events List, page 4-8.
	Displays the EventVision Filter dialog box enabling you to define a filter for the events displayed in the EventVision log. For more information, see Filtering Events, page 4-8.
	Toggles automatic refresh of event data on and off. You define the refresh-time period (in seconds) in the EventVision Options dialog box. The default is 60 seconds. If a filter is active, the refresh is done according to the filter. For more information, see Setting EventVision Viewing Options, page 2-5.
	Displays the properties of the selected event or ticket in the EventVision Properties Details pane.

Setting EventVision Viewing Options

The EventVision Options dialog box enables you to define the options for displaying events in the EventVision window.

To define EventVision options:

Step 1 From the Tools menu, select **Options.** The EventVision Options dialog box appears.

The following fields are displayed:

- **Keep last filter—**Saves the filter criteria defined per event type in the Filter Events dialog box to the registry. The filter criteria are available the next time you log into EventVision.

Note Events are not filtered automatically when you next log into EventVision unless the Open using filter option is selected as well.

- **Open using filter—**If the **Keep last filter** option is selected, this option applies the previously defined filter to the events from the time when EventVision is opened (the events are continuously filtered according to the defined settings even after closing and starting a new session).
- **Show … events per page—**Allows you to set the number of events that are displayed per page.
- **Export … events in total—**Allows you to set the maximum number of events to be exported to a file.
- **Run auto refresh every … sec—**Allows you to configure EventVision to run **Automatic Refresh** according to the defined number of seconds.

Note Selecting this option displays a warning message asking you to confirm your selection, as this option uses rapid refresh on the database, which could slow down other vital database options.

- **Events displayed for the last selected number of weeks—**Enables you to configure which past events to display from the database according to the defined number of weeks.

Step 2 Select the required options by checking the appropriate checkbox(es).

Step 3 Click **OK** to close the dialog box and save your settings.

CHAPTER 3

Viewing Events in EventVision

The events are displayed in an Events List log for each tab. These tabs reflect the different event categories and display event information related to the specific event category. The following tabs may be selected in the EventVision window:

- All Tab
- Audit Tab
- Provisioning Tab
- Security Tab
- Service Tab
- Syslog Tab
- System Tab
- Ticket Tab
- V1 Trap Tab
- V2 Trap Tab

The events are sorted according to date, where the latest event is displayed first and the oldest event is displayed last. You can define the filter to be used as well as the number of events to be displayed in the Events List using the EventVision Options dialog box. For more information see Setting EventVision Viewing Options, page 2-5.

The navigation toolbar enables you to navigate through all the EventVision log record pages.

Each page of the Events List displays the selected amount of events per page as defined in the EventVision Options dialog box. See Setting EventVision Viewing Options, page 2-5. You can use the **Go To** sub-menu options on the View menu or the respective toolbar buttons on the toolbar, to navigate between each displayed page.

All Tab

When you launch EventVision, the **All** tab is not displayed.

You can open this tab, as required, using the **Open All Tab** option on the File menu.

Note Opening the **All** tab may take some time to retrieve information from the Cisco ANA database for all category events.

The **All** tab displays information about all the events. Additional information specific to the event category can be viewed in the Events Properties dialog box or individual category tabs.

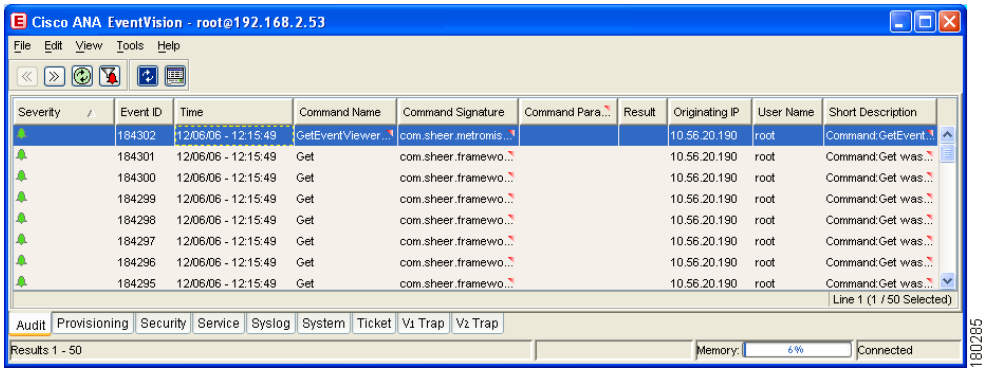
The following columns are displayed in the **All** tab:

- **Severity**—The severity of the ticket.
- **Event ID—**The sequential ID number of the event.
- **Short Description—**A description of the event, for example, device unreachable.
- **Time—**The date and time when the event occurred. The time is displayed in the following format MM/DD/YY HH:MM:SS.
- **Event Type—**The event type, namely, audit, system, ticket, provisioning, syslog, security, service, and traps.

Audit Tab

The **Audit** tab displays all the events generated for each command or request in Cisco ANA, for example, opening EventVision displays the following "GetEvent" in the Audit List:

Figure 3-1 Audit Tab



The following information is displayed in the **Audit** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the event (generated by Cisco ANA).
- **Time—**Logged and recorded at the time the event happened.
- **Command Name—**The audit specific command name, prefaced by, for example, Get…, Update…, Find…
- **Command Signature—**The actual command run by Cisco ANA, such as com.sheer.framework.
- **Command Parameter—**This parameter is currently unavailable in this version.
- **Result—**This parameter is currently unavailable in this version.
- **Originating IP—**The IP address of the client that issued the command.
- **User Name—**The name of the user who initiated the command.
- **Short Description—**An aggregation of portions of the same fields in the Audit Command fields.

The type of information displayed in the **Audit** tab can be audited by defining the appropriate registry keys and their values. The audit service enables you to audit all the commands executed in the system, for example, the Get command can be audited. The **Audit** tab then displays this information.

The following parameters can be controlled through the registry :

- Override the default auditing details level
- All or specific users
- Display only specific commands

The available values for these parameters are:

- **Concise—**Displays all (default) events besides the Command Parameters and Result column values.
- **Disable—**The commands will not be logged in the **Audit** tab events list.

For more information about the Registry Editor, refer to the *Cisco Active Network Abstraction Registry Editor Guide*.

Provisioning Tab

Events displayed in the **Provisioning** tab are events triggered during the configuration of a device. Cisco ANA sends an event explaining the configuration operation, for example, to configure the cross connect table in a device. The **Provisioning** tab displays detailed information specific to this event category. It contains events both from the Cisco ANA Command Builder and Cisco ANA Workflow Editor. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Provisioning** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the event.
- **Short Description—**A description of the event, for example, Script Show has failed.
- **User Name—**The name of the user who performed the provisioning operation.
- **Time—**Logged and recorded at the time the event happened.
- **Status—**The status, for example, success or fail.
- **Source—**The VNE key on which the provisioning operation succeeded or failed.

Security Tab

The **Security** tab displays detailed information specific to this event category. Security events are related to client login and user activity when managing the system and the environment. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Security** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the event.

- **Short Description—**A description of the event, for example, Successful login by root.
- **Location—**The entity that triggered the event, as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the event happened.
- **Client IP**—The IP address of the client where the event was triggered.
- **User Name**—The user name of the client where the event was triggered.
- **Client Type**—The type of client, namely, NetworkVision, EventVision, Cisco ANA Manage or Unknown (for example,BQL, Registry Editor and so on).
- **Auto Cleared**—Indicates whether the alarm is cleared automatically. The alarm is cleared when it is correlated to an alarm which has been cleared. If the alarm is cleared automatically it is defined as true.

Service Tab

The **Service** tab displays all the alarms generated by Cisco ANA, for example, link down. Service events are related to the alarms that are generated by the Cisco ANA system. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Service** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event, for example, Route entry restored.
- **Location—**The entity that triggered the alarm, as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the event happened.

Syslog Tab

The **Syslog** tab displays all the syslog events. These events are related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Syslog** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the alarm, for example, Device configuration changed.
- **Location—**The entity that triggered the alarm, as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the alarm happened.

System Tab

The **System** tab displays all the system events related to the everyday working of the internal system and its components. These events may be related to the Cisco ANA and Cisco ANA Gateway resources, representing the system log. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **System** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event, for example, Dropped Events Report.
- **Location—**The entity that triggered the event.
- **Time—**Logged and recorded at the time the event happened.

Ticket Tab

The **Ticket** tab displays detailed information specific to this event category. A **ticket** event contains a single root alarm (the root-cause alarm can be of any alarm type, for example, syslog, service and so on), and all its subsequent correlated alarms. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The maximum number of open tickets (other tickets can be correlated to them) for the system is 5000.

This number is configurable in the registry, however we do not recommend increasing it.

Note Changes to the registry should only be carried out with the support of Cisco Professional Services.

A "`tickets capacity overflow, red threshold reached`" system alarm is generated when this number is exceeded. The alarm severity is defined as critical.

The following additional information is displayed in the **Ticket** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Ticket ID—**The sequential ID number of the ticket.
- **Short Description—**A description of the event, for example, Link Down.
- **Location—**The entity that triggered the ticket, as a hyperlink that opens the relevant location.
- **Last Modification Time—**The date and time when the ticket was last modified.
- **Time—**Logged and recorded at the time the first event happened.
- **Acknowledged—**The status of the ticket that is being handled, namely, true (acknowledged) or false (not acknowledged).
- **Affected Devices Count—**The number of devices affected by the ticket (the source(s) of the alarm and their subsequent alarms).

- **Correlation Count—**Displays the number of correlated alarms included in the ticket. For example, if in the **Correlation** tab of the Ticket Properties, there are 3 alarms correlated to the root-cause alarm, then the counter displays the number 3. If there are 2 alarms correlated to the root-cause alarm, and each alarm in turn has 2 alarms correlated to it, then the counter displays the number 4.
- **Reduction Count—**Displays the number of alarms included in the ticket. For example, nine alarms can be viewed in the **History** tab of the Ticket Properties window, but only a single ticket is displayed in the Ticket pane.
- **Duplication Count—**Displays the number of occurrences of the original root-cause alarm included in the ticket. For example, if the ticket was created by a link down root-cause alarm, and then the link goes up and down again quickly so that it is included in the same ticket, then the duplication counter displays the number 2, as the root-cause alarm occurred twice.

For information about viewing ticket properties, see Ticket Tab Properties, page 4-2.

V1 Trap Tab

This event is triggered when the network element sends a trap message to Cisco ANA because of a network event, for example, Link Down. The **V1 Trap** tab displays detailed information specific to this event category. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional is displayed in the **V1 Trap** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event, for example, enterprise generic trap.
- **Time—**Logged and recorded at the time the event happened.
- **Location—**The entity that triggered the trap, as a hyperlink that opens the relevant location.

V2 Trap Tab

The **V2 Trap** tab displays detailed information specific to this event category. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **V2 Trap** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event.
- **Location—**The entity that triggered the trap, such as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the event happened.

CHAPTER 4

Working in EventVision

This chapter describes how to view, filter and display the properties of specific events, and how to refresh and export events:

- Viewing Event Properties—Describes how to view the properties of a specific event type.
- Refreshing the Events List—Describes how to manually and automatically refresh the Events List.
- Filtering Events—Describes how to define a filter for the events displayed in the Events List.
- Exporting Displayed Data—Describes how to export the currently displayed data from the EventVision table. In addition, it describes how to import the data and view it at a later stage.
- Logging Out—Describes how to log out of EventVision.

Viewing Event Properties

EventVision enables you to view the properties of a specific event type. The Event Properties dialog box displays detailed information about the event, for example, the severity and the number of affected parties.

For a detailed description of the properties refer to:

- Ticket Tab Properties
- Audit Tab Properties
- Security Tab Properties
- Provisioning Tab Properties
- V1 and V2 Trap Tabs Properties

To view Event Properties:

Step 1 Select the required tab for the specific event type and the event in the EventVision window.

Step 2 Double-click on the event in the Events List or on the View menu, click **Properties**, or right-click the event, and select **Properties** from the shortcut menu.

The Properties tabbed window is displayed for the selected event.

Note Clicking **Details Pane** on the toolbar displays the properties of the selected ticket or event in the Properties Details pane.

The header displays the ID number of the selected event.

Ticket Tab Properties

The properties of a selected ticket can be viewed by displaying the Ticket Properties dialog box. For example, you can view alarm severity, correlated alarms, active alarms, alarm history or the source of the alarm. See Ticket Tab, page 3-5.

For information about opening the Properties dialog box, see Viewing Event Properties, page 4-1.

The information displayed in the Ticket Properties dialog box corresponds with the information displayed in the Ticket pane of the NetworkVision window. The ID number displayed in the header corresponds to the ID number of the ticket selected in the EventVision window.

The Ticket Properties dialog box is divided into the following areas:

- Tabbed Pane
- Toolbar

Tabbed Pane

The Ticket Properties dialog box is divided into the following tabs:

- **General—**General information about the selected ticket. See General Tab, page 4-2.
- **History**—The history of the ticket. See History Tab, page 4-3.
- **Affected Parties**—The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. See Affected Parties Tab, page 4-3.
- **Correlation—**All the alarms that are correlated to the selected ticket. See Correlation Tab, page 4-4.
- **Notes—**Enables you to add notes to the selected ticket. See Notes Tab, page 4-5.
- **Advanced—**All the affected devices, correlation, duplication and reduction counts for the selected ticket. In addition, it provides any other additional information available about the ticket. See Advanced Tab, page 4-5.

General Tab

The following fields are displayed in the **General** tab providing information about the compiled alarm:

- **Alarm—**The supported root-cause alarm name, for example, Link Down.
- **Location—**The entity that triggered the root-cause alarm, as a hyperlink that opens the relevant location.
- **Severity—**Displays the severity that was propagated from all the correlated alarms. See Color Coding of Events List Severity Icons, page 2-4.
- **Time—**The date and time when the initial root-cause alarm was generated. The time is taken from Cisco ANA and is displayed in the following format MM/DD/YY – HH:MM:SS.

- **Open Alarms—**The number of correlated alarms for the ticket that are open. For example, 3 / 4. Four relates to the total number of correlated alarms for the ticket. Three indicates the number of alarms that have not been cleared, and therefore there is one alarm that is closed.
- **Acknowledged—**The status of the ticket that is being handled, namely, acknowledged (true) and unacknowledged (false).
- **Description—**The description from the message field.

History Tab

The **History** tab enables you to display the history of the ticket, including all the events.

The following columns are displayed in the **History** tab providing information about the compiled alarm:

- **Severity—**Displays a severity bell icon, which is colored according to the severity of the alarm on the event.
- **Alarm ID—**The ID number of the alarm that changed the ticket.
- **Duplication Count—**Displays the number of occurrences of the original root-cause alarm included in the ticket. For example, if the ticket was created by a link down root-cause alarm, and then the link goes up and down again quickly so that it is included in the same ticket, then the duplication counter displays the number 2, as the root-cause alarm occurred twice.
- **Short Description—**A description of the change in the ticket.
- **Reduction Count—**Displays the number of alarms included in the ticket. For example, nine alarms can be viewed in the **History** tab of the Ticket Properties window, but only a single ticket is displayed in the Ticket pane.
- **Location—**The entity that triggered the alarm, as a hyperlink that opens the relevant location.
- **Time—**The date and time when the ticket changed.

Affected Parties Tab

When a fault occurs, Cisco ANA automatically calculates the affected parties (automatic impact analysis). For example, when a link goes down, and embeds this information in the ticket along with all the correlated faults. You can view a list of all the endpoints that are affected and that have lost connectivity. For more information about proactive impact analysis, refer to the *Cisco Active Network Abstraction NetworkVision User Guide*.

The **Affected Parties** tab displays the services (affected pairs) that are affected (automatic impact analysis) by the ticket. For more information about accumulating affected parties, refer to the *Cisco Active Network Abstraction NetworkVision User Guide*.

The **Affected Parties** tab is divided into two areas, **Source** and **Destination**. The **Source** area displays the set of affected elements (A side and Z side). The following columns are displayed in the **Affected Parties** tab providing information about the affected parties:

- **Location—**A hyperlink that opens the Inventory window, highlighting the port with the affected parties.
- **Key—**The unique value taken from the affected element's business tag key (if it exists).
- **Name—**The subinterface (site) name or business tag name of the affected element (if it exists). For more information, refer to the *Cisco Active Network Abstraction Managing MPLS User Guide*.
- **Type—**The business tag type.

- **IP Address—**If the affected element is an IP interface the IP address of the subinterface (site) is displayed. For more information, refer to the *Cisco Active Network Abstraction Managing MPLS User Guide*.
- **Highest Affected Severity—**The same source can be part of multiple pairs, and therefore each pair can have different affected severities. The highest affected severity is the highest severity of these affected pairs. The affected pair can have one of the following severities:
  - **Potential—**The service may be affected but its real state is not known.
  - **Real—**The service is affected.
  - **Recovered—**The service was recovered after the network fault. This state only applies to affected pairs that were previously marked as **Potentially Affected** or **Real Affected**.
  - **N/A—**From Links view this indicates not relevant.

When an affected side (a row) is selected in the **Source** area the selected element's related affected pairs are displayed in the **Destination** area.

The following additional columns are displayed in the **Destination** area table in the Ticket Properties window:

- **Affected Severity—**The severity of the affected pair as calculated by the client according to the rules defined in the *Cisco Active Network Abstraction NetworkVision User Guide*.
- **Alarm Clear State—**An indication for each pair of the clear state of the alarm. The following states exist:
  - **Not Cleared—**There are one or more alarms that have not been cleared for this pair.
  - **Cleared—**All the related alarms for this pair have been cleared.

In addition, you can view a detailed report for every affected pair that includes a list of the events that contributed to this affected pair. For more information about viewing a detailed report, refer to the *Cisco Active Network Abstraction NetworkVision User Guide*.

Correlation Tab

The **Correlation** tab displays all the alarms that are correlated to the selected ticket.

Each branch provides a short description of the alarm, a severity icon, ID, location and time of the alarm.

The following columns are displayed in the **Correlation** tab providing information about the alarm as follows:

- **ID—**The ID number of the event that changed the ticket. The branches can be expanded and collapsed in order to hide information as needed.
- **Short Description—**A description of the change in the ticket. The full description is displayed in the lower tab area.
- **Location—**A hyperlink that opens the Alarm Properties window, highlighting the port with the affected parties.
- **Time—**The date and time the ticket was issued.
- **Last Modification Time—**The date and time when the ticket changed.
- **Reduction Count—**Displays the number of alarms included in the ticket. For example, nine alarms can be viewed in the **History** tab of the Ticket Properties window, but only a single ticket is displayed in the Ticket pane.

- **Duplication Count—**Displays the number of occurrences of the original root-cause alarm included in the ticket. For example, if the ticket was created by a link down root-cause alarm, and then the link goes up and down again quickly so that it is included in the same ticket, then the duplication counter displays the number 2, as the root-cause alarm occurred twice.

The **Find** field on the toolbar enables you to search for information in the **Ticket Properties** table.

Notes Tab

The **Notes** tab enables you to add and save notes for the selected ticket.

To add text, enter text in the **Notes** field and click **Save Notes**. The new text is added to any previously existing text.

Note **Save Notes** is enabled only when text is entered in the **Notes** field.

Note The text cannot be edited or removed after you have saved the notes.

Advanced Tab

The **Advanced** tab enables you to view all the affected devices, correlation, duplication and reduction counts for the selected ticket. In addition, it provides any other additional information available about the ticket.

The following fields are displayed in the **Advanced** tab providing information about the compiled alarm:

- **Successor—**A hyperlink to the successor event, for example, port up.
- **Correlator—**A hyperlink to the correlator alarm.
- **Predecessor—**A hyperlink to the predecessor event, for example, port down.
- **Affected Devices—**The number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).
- **Duplication Count—**Displays the number of occurrences of the original root-cause alarm included in the ticket. For example, if the ticket was created by a link down root-cause alarm, and then the link goes up and down again quickly so that it is included in the same ticket, then the duplication counter displays the number 2, as the root-cause alarm occurred twice.
- **Correlation Count—**Displays the number of correlated alarms included in the ticket. For example, if in the **Correlation** tab of the Ticket Properties, there are three alarms correlated to the root-cause alarm, then the counter displays the number 3. If there are two alarms correlated to the root-cause alarm, and each alarm in turn has two alarms correlated to it, then the counter displays the number 4.
- **Reduction Count—**Displays the number of alarms included in the ticket. For example, nine alarms can be viewed in the **History** tab of the Ticket Properties window, but only a single ticket is displayed in the Ticket pane.

Toolbar

The Ticket Properties dialog box contains the following tools:

Table 4-1 Tools in Ticket Properties Dialog Box

Refresh	Refreshes the information displayed in the Ticket Properties dialog box.
Acknowledge	Acknowledges that the ticket is being handled and the status of the ticket is displayed as **true** in the Ticket pane and in the Ticket Properties dialog box. For more information, refer to the *Cisco Active Network Abstraction NetworkVision User Guide*. **Note** This button is enabled only if the ticket has not yet been acknowledged.
Clear	Requests the relevant Cisco ANA to remove the faulty network element from the Cisco ANA networking inventory. In addition, it sets the ticket to Cleared severity/status (the icon is displayed in green) and automatically changes the acknowledged status of the ticket to **true**. For more information, refer to the *Cisco Active Network Abstraction NetworkVision User Guide*. **Note** This button is enabled only if the severity of the alarm is higher than Cleared/Normal.
Save Notes	Saves the notes for the selected ticket. **Note** This button is enabled only when text is entered in the **Notes** field of the **Notes** tab.

Audit Tab Properties

The properties of a selected auditing event can be viewed in detail by displaying the Audit Event Properties dialog box. For information about opening the Properties dialog box, see Viewing Event Properties, page 4-1.

The Audit Event Properties dialog box is divided into the following tabs:

- General—General information about the selected event. For a detailed description of the information displayed in the **Audit** tab, see Audit Tab, page 3-2.
- Advanced—This tab is not relevant for auditing events.
- Audit—Detailed information specific to auditing events. For a detailed description of the information displayed in the **Audit** tab, see Audit Tab, page 3-2.

Security Tab Properties

The properties of a selected security event can be viewed in detail by displaying the Security Event Properties dialog box. For information about opening the Properties dialog box, see Viewing Event Properties, page 4-1.

The Security Event Properties dialog box is divided into the following tabs:

- General—General information about the selected event. For a detailed description of the information displayed in the **Security** tab, see Security Tab, page 3-3.
- Affected Parties—This tab is not relevant for security events.

- Advanced—This tab is not relevant for security events.
- Security—Detailed information specific to security events. For a detailed description of the information displayed in the **Security** tab, see Security Tab, page 3-3.

Provisioning Tab Properties

The properties of a selected provisioning event can be viewed by displaying the Provisioning Event Properties dialog box. For example, you can view a detailed description of the provisioning event.

For information about opening the Properties dialog box, see Viewing Event Properties, page 4-1.

For a detailed description of the information displayed in the **Provisioning** tab, see Provisioning Tab, page 3-3.

The **Description** area of the Provisioning Event Properties dialog box details all the content of the workflow output or the command. If it is a workflow the description includes the execution sequence of the workflow and log messages. The execution sequence includes the output of all the scripts executed by the workflow and also indicates if workflow rollback has occurred. If it is a command, the description includes the output of the script.

V1 and V2 Trap Tabs Properties

The properties of a selected V1 Trap and/or V2 Trap alarm can be viewed by displaying the V1/V2 Trap Alarm Properties dialog box. For example, you can view the translated Oid and value.

For information about opening the Properties dialog box, see Viewing Event Properties, page 4-1.

The V1/V2 Trap Alarm Properties dialog box is divided into the following tabs:

- **General—**General information about the selected event. For more information about the information displayed in the **V1 Trap** tab, see V1 Trap Tab, page 3-6. For more information about the information displayed in the **V2 Trap** tab, see V2 Trap Tab, page 3-6.
- **Affected Parties—**The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. See Affected Parties Tab, page 4-3.
- **Advanced—**All the affected devices, correlation, duplication and reduction counts for the selected ticket. In addition, it provides any other additional information available about the ticket. For more information, see Advanced Tab, page 4-5.
- **Trap—**General description of V1 and V2 trap information. See Trap Tab, page 4-7.

Trap Tab

The **Trap** tab enables you to view V1 and V2 trap information.

The following fields are displayed in the **Trap** tab:

- **Version—**The SNMP version, namely, **version-1** or **version-2c**.
- **Community String—**The community that the device sends to in the PDU.
- **Error Status—**The error status, namely, **No Error**, **Too Big**, **No Such Name**, **Bad Value**, **Read Only**, and **Gen Err**.

The following columns are displayed in the **Values** table:

- **Translated Oid—**A string representation of the Oid. For example, 1.3.6 is translated into iso(1).org(3).dod(6).
- **Translated Value—**A string representation of the Oid value. For example, 1.3 is translated to iso(1).org.10.
- **Oid—**The Oid that is not translated, that is, it is a dot notation representation of the oid, for example, 1.3.6.1.4.1.9.
- **Value—**The value that is not translated, that is, it is not represented by string values.

Refreshing the Events List

EventVision displays current event information in the log. While viewing the log, this information is not updated unless you:

- Refresh the list manually.
- Use the Auto Refresh option.

Note Be sure that when you use the **Auto Refresh** option, you configure EventVision to automatically run the refresh option. You define the refresh time period (in seconds) in the EventVision Options dialog box. See Setting EventVision Viewing Options, page 2-5.

Step 1 To manually refresh the Events List, on the toolbar, click **Refresh**.

or

From the View menu, select **Refresh**. The Events List is refreshed.

Note Click **Refresh** to redisplay the first page of information, namely, the most recent events.

Step 2 To automatically refresh the Events List, on the toolbar, click **Refresh Table**. The Events List is automatically refreshed, and older information is moved down the list.

Note When you click **Refresh Table** the Events List continues to be repeatedly refreshed after the defined refresh time period. The previous setting is maintained, for example, if the order in the Events List is ascending and the Events List is refreshed the order will remain ascending. To cancel automatic refresh, click **Refresh Table**.

Filtering Events

The Filter dialog box allows you to filter events according to:

- Severity
- ID

- Date and Time
- Text in the description field

The **Filter** button toggles to indicate that a filter has been applied.

You may also use the filter to search for information in the database.

Note Filter fields are enabled or disabled according to the event type. For example, if a filter is applied to a ticket, all the fields are enabled.

To define a filter:

Step 1 From Edit menu, select **Filter**,

or

On the toolbar, click **Filter**. The Filter Events dialog box is displayed.

Step 2 Select and type in the required filter values.

Step 3 Click **OK** to save your filter settings and apply the filter. The filtered events are displayed in the Events List according to the defined criteria.

Note Selecting **Keep last filter** in the EventVision Options dialog box (see Setting EventVision Viewing Options, page 2-5) saves the currently defined filter settings in the registry. The next time you log into the application, these filter settings are displayed in the Filter Events dialog box. In addition, the events are filtered repeatedly for the current session according to the defined settings.

Note Selecting **Open using filter** in the EventVision Options dialog box (see Setting EventVision Viewing Options, page 2-5), the events are continuously filtered according to the defined settings even after logging out of and into the application.

To remove the filter:

Step 1 On the toolbar, click **Filter**. The Filter Events dialog box is displayed.

Step 2 Click **Clear**. The selected options in the Filter Events dialog box are cleared.

Step 3 Click **OK**. All the events are displayed in the Events List.

Exporting Displayed Data

EventVision enables you to export the currently displayed data from the EventVision table according to the criteria (total quantity of events) defined in the EventVision Options dialog box. The data can then be imported and viewed at a later stage.

To export the table to a file:

Step 1 Select **Export** from the File menu. The Export Table to File dialog box is displayed.

Step 2 Browse to the directory where you want to save the list.

Step 3 In the File name field, type a name for the list.

Step 4 Click **Save**. The displayed Events List or row(s) are saved in the selected directory.

Logging Out

When you have finished working with EventVision you can log out of the application.

To log out of EventVision, click to close the EventVision window. The EventVision window is closed.

INDEX

L

N

O

P

R

S

T

V