



Cisco Active Network Abstraction EventVision User's Guide, 3.5

Corporate 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: 408 526-4100

Text Part Number: OL-8838-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Important Notice

Cisco ANA 3.5 is a carrier-class, multi-vendor network and service management platform which builds a real-time virtual model of the network, serving as a live information base for value-added tools and applications for integration into an existing OSS environment.

Cisco ANA 3.5 is a limited release by Cisco Systems of the existing features and functions of the Sheer DNA 4.0.1 software.

As this is a limited release, the naming of the product in the software and the user documentation remains as Sheer DNA.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

1 877 228-7302

1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
- EMEA: +32 2 704 55 55
- USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

- Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
- Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
- Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://cisoiq.texterity.com/cisoiq/sample/>

Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

About This Guide

This User's Guide describes the events that are logged in the Sheer DNA Gateway and how they can be viewed.

Introducing Sheer EventVision, page 1, overviews the Sheer EventVision application used to view events and describes event categories.

Getting Started with EventVision, page 7, describes how to open the Sheer EventVision window, and the Sheer EventVision window, including its toolbar and menus.

Setting EventVision Viewing Options, page 15, describes how to define the options for displaying events in the Sheer EventVision window.

Viewing Events in EventVision, page 17 describes the EventVision tabs used for viewing system and network events.

Working in EventVision, page 29, 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.

Table of Contents

1	Introducing EventVision.....	1
1.1	About Sheer™ EventVision.....	1
1.2.1	Sheer™ EventVision Overview	1
1.2.2	Basic Concepts and Terms	2
1.2.3	EventVision Categories	5
2	Getting Started with EventVision	7
2.1	Launching EventVision.....	7
2.2	The EventVision Window.....	10
2.2.1	EventVision Menus	11
2.2.2	Color Coding of Events List Severity Icons	14
2.2.3	EventVision Navigation Toolbar	14
2.3	Setting EventVision Viewing Options	15
3	Viewing Events in EventVision.....	17
3.1	All Tab.....	18
3.2	Audit Tab.....	19
3.3	Provisioning Tab	20
3.4	Security Tab	21
3.5	Service Tab	22
3.6	Syslog Tab	23
3.7	System Tab	24
3.8	Ticket Tab.....	25
3.9	V1 Trap Tab.....	26
3.10	V2 Trap Tab.....	27

4	Working in EventVision	29
4.1	Viewing Event Properties	29
4.1.1	Ticket Tab Properties.....	30
4.1.2	Provisioning Tab Properties	40
4.1.3	V1 and V2 Trap Tabs Properties	40
4.2	Refreshing the Events List	42
4.3	Filtering Events	43
4.4	Exporting displayed Data	45
4.5	Logging Out	46

1 Introducing EventVision

Welcome to the *Cisco Active Network Abstraction EventVision User's Guide* that describes the intuitive interface for viewing system events and tickets that are generated within the Sheer DNA system.

1.1 About Sheer™ EventVision

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

You can configure Sheer 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 the Sheer EventVision. In addition, when an event occurs in the Sheer DNA system the details are available in Sheer EventVision.

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

1.1.1 Sheer™ EventVision Overview

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

- Audit
- Provisioning
- Security
- Service
- Syslog

- Ticket
- V1 and V2 Traps
- System Event

1.1.2 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:

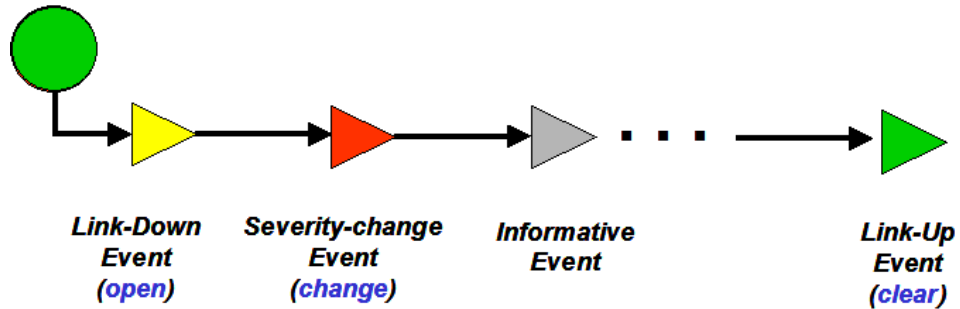
- Port status change
- Route entry drop
- Device reset
- Device becoming reachable
- User acknowledgement of an alarm

Events are written to the DNA 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*.

Link-Down event sequence



Typically, a complete event sequence includes three mandatory events:

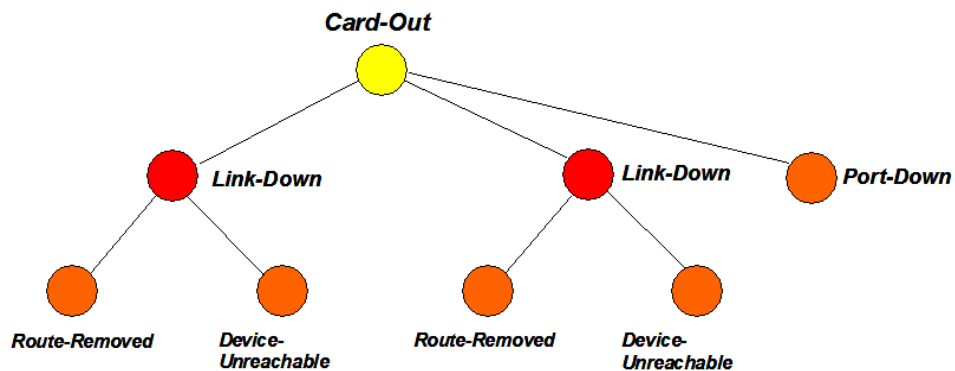
- Alarm Open (in this example, a Link Down event).
- Alarm Clear (in this example, a Link Up event).
- Alarm Acknowledge (not shown in this example)

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).



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. Sheer EventVision’s *Ticket Properties* dialog box displays only tickets, but allows drilling down to view the consequent alarm hierarchy.

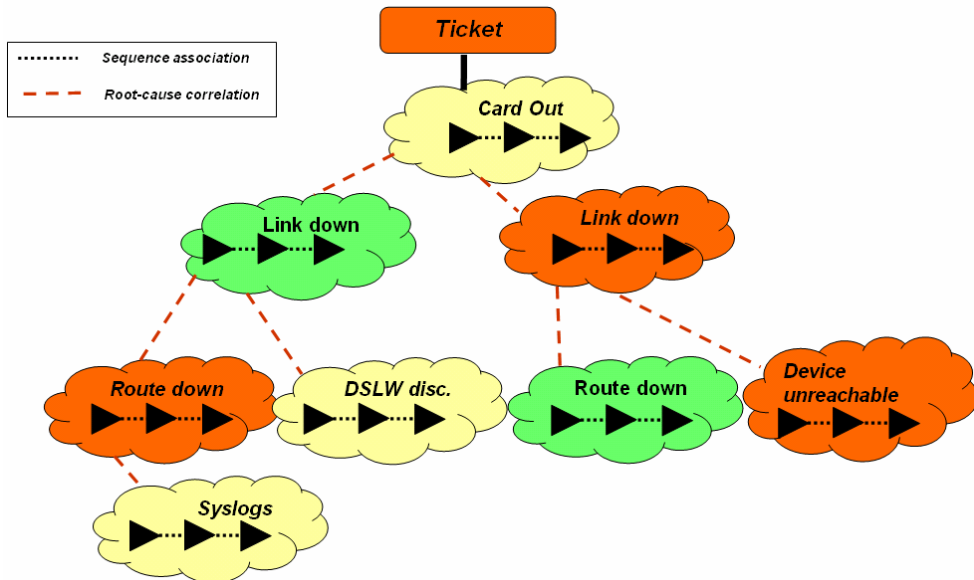
From an operator’s point of view, the managed entity is always a complete ticket. Operations such as Acknowledge, Force-Clear or Remove are always applied to the whole ticket. The ticket also assumes an overall, propagated severity.

Sequence Association vs. Root-Cause Correlation

It is important not to confuse between the two types of relationships in DNA 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:



In the above figure, the “clouds” represent alarms, which are correlated into a hierarchy according to root-cause. Within each alarm is its respective event sequence, representing the lifecycle of the alarm.

1.1.3 EventVision Categories

The EventVision recognizes the following categories of Sheer DNA system events or alarms:

- **Audit:** These events are related to the running of commands in the Sheer DNA Gateway.
- **Provisioning:** These events are related to configuration and provisioning activities.
- **Security:** These events are related to client login and user activity when managing the system and the environment.
- **Service:** These events are related to the alarms that are generated by the Sheer DNA system.
- **Syslog:** 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.
- **System:** These events are related to the everyday working of the internal system and its components. These events may be related to the Sheer DNA and Sheer DNA Gateway resources, representing the system log.
- **Ticket:** These events are related to all of the tickets that were opened in Sheer DNA.
- **V1 Trap:** These events are related to SNMPv1 traps from the devices by the VNEs, which are used to generate the trap events.
- **V2 Trap:** These events are related to SNMPv2 traps from the devices by the VNEs, which are used to generate the trap events.

You can also view all of the events in the **All** tab, if required, refer to page 18 for an example of the **All** tab appearing as one of the EventVision tabs.

2 Getting Started with EventVision

This chapter describes the EventVision application and describes the available viewing options enabling you to view system events and tickets that are generated within the Sheer DNA system.

Note: EventVision is available to Administrators only.

Launching EventVision describes how to launch EventVision.

The EventVision Window, page 10, details the EventVision menu options, including using the toolbar buttons to navigate through the application.

Setting NetworkVision Viewing Options, page 15, explains how to define the amount time constraints for displaying events in the various in the EventVision window.

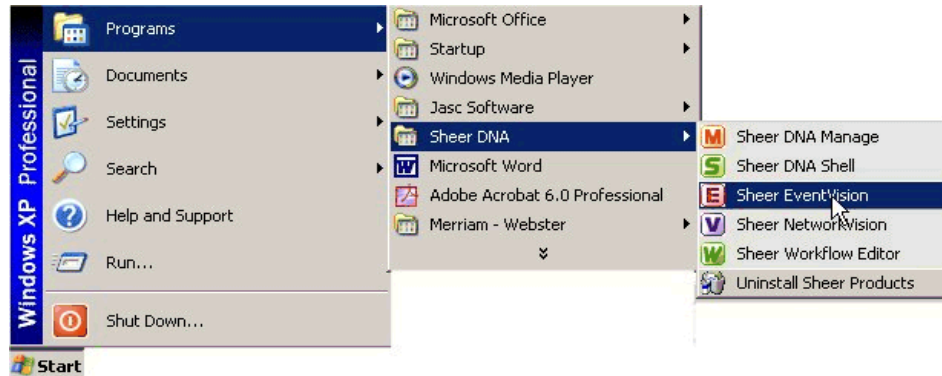
2.1 Launching EventVision

This section provides instructions for launching the Sheer EventVision application. Sheer EventVision is password protected to ensure security. Before you start working with Sheer EventVision make sure you know your user name, password, and the Sheer DNA Gateway IP address or host name that you require.

Note: If a user does not login to the Sheer DNA Manage, NetworkVision or EventVision applications during a specified period of time (the default is 30 days) the user's account will be automatically locked. The default period can be changed in the Sheer DNA 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, Section 10.5*). The period of time is measured from the time the user last logged out of any of the Sheer DNA Client applications.

To start Sheer EventVision

1. From the *Start* menu, select the **Programs** folder, then **Sheer DNA/Sheer EventVision**.



The login dialog box is displayed:

2. Type your **User Name**, and **Password** in the appropriate fields.
3. Enter the required Sheer DNA Gateway's information in the **Host** field, as an IP address or host name,

or

Select a Sheer DNA Gateway from the **Host** dropdown list.

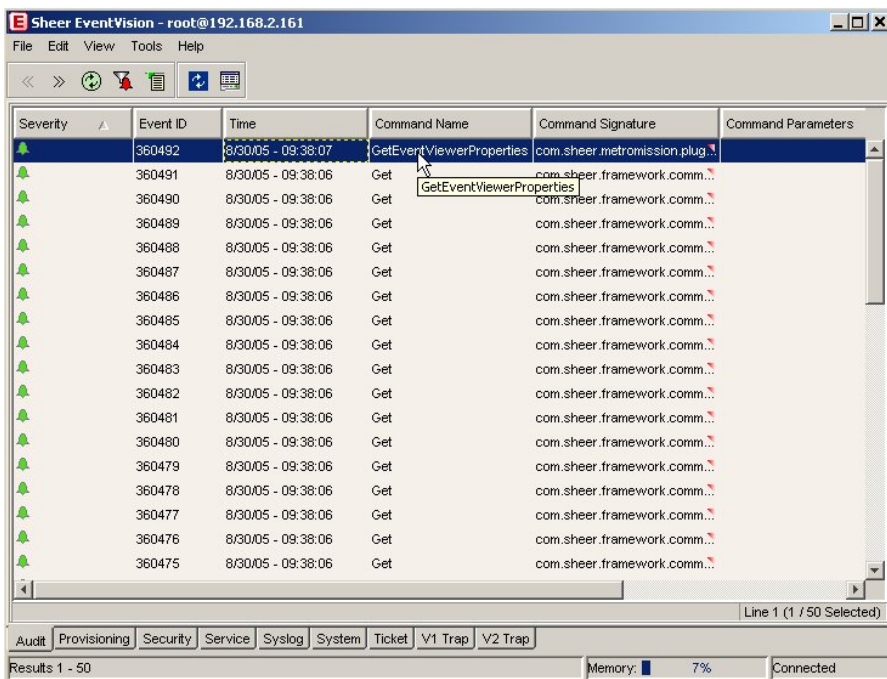
Note: The Sheer DNA Gateway IP address or host name that was used when you last logged in is automatically displayed at the top of the **Host** dropdown list.

Note: Make sure that you use the leading IP address (the IP on which the Sheer DNA Gateway was configured) when logging in to the system.

4. Click **OK**. The *Sheer EventVision* window is displayed (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.



2.2 The EventVision Window

The *Sheer EventVision* window displays the events generated in the Sheer DNA system. An example of the *Sheer EventVision* window is displayed below.

The screenshot shows the Sheer EventVision window with the following components labeled:

- Menu bar:** File, Edit, View, Tools, Help
- Toolbar:** Navigation and action icons (back, forward, refresh, etc.)
- Table pane:** A table with columns: Event ID, Short Description, Location, and Time. The selected event (ID 1138) is highlighted in blue.
- Event Properties pane:** A pane showing details for the selected event, including Alarm, Location, Affected, Acknowledged, Severity (Minor), Time, and Open Alarms.
- EventVision tabs:** Audit, Provisioning, Security, Service, Syslog, System, Ticket, V1 Trap, V2 Trap
- Status bar:** Results 1 - 50, Memory: 6%, Connected

Event ID	Short Description	Location	Time
1146	Agent 10.100.12.190 is reachable: BOS Unit = 192.168.2.181 AVM = 700	DNA Unit 192.168.2.181	01/12/05 - 14:53:13
1145	Agent 10.100.12.185 is reachable: BOS Unit = 192.168.2.181 AVM = 700	DNA Unit 192.168.2.181	01/12/05 - 14:52:53
1144	Agent 10.100.12.182 is reachable: BOS Unit = 192.168.2.181 AVM = 700	DNA Unit 192.168.2.181	01/12/05 - 14:52:53
1139	AVM 192.168.2.181:700 (avm700_-930602184) is reachable	Avm 700	01/12/05 - 14:51:53
1138	Agent 10.100.12.182 is starting.BOS Unit = 192.168.2.181 AVM = 700	PE-West1	01/12/05 - 14:51:47
1137	Agent 10.100.12.185 is starting.BOS Unit = 192.168.2.181 AVM = 700	PE-East1	01/12/05 - 14:51:47
1136	Agent 10.100.12.190 is starting.BOS Unit = 192.168.2.181 AVM = 700	CE-Black-West1	01/12/05 - 14:51:47
1135	AVM 700 started.BOS Unit = 192.168.2.181	Avm 700	01/12/05 - 14:51:45
1085	Agent 10.100.12.185 is unreachable: BOS Unit = 192.168.2.181 AVM = 700	DNA Unit 192.168.2.181	01/12/05 - 14:51:34
1084	Agent 10.100.12.182 is unreachable: BOS Unit = 192.168.2.181 AVM = 700	DNA Unit 192.168.2.181	01/12/05 - 14:51:34

The *Sheer EventVision* window is divided into the following parts:

- **Menu Bar**, described on page 11.
- **Toolbar**, described on page 14.
- The **Events List** and **Properties** pane comprised of tabs, which 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, refer to page 13 for an example.

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

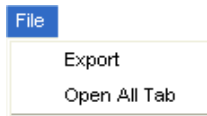
- Define Sheer EventVision display and configuration options, refer to page 15 for more information.
- Display the **All** tab, refer to page 18 for more information.
- Filter dialog box to (filter-in) display selected lines only refer to page 43 for more information.
- Selected event properties in a separate window, refer to page 29.

2.1.1 EventVision Menus

This section provides a description of each option available in the *Sheer 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 *Sheer 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 *Sheer EventVision* window.



Filter

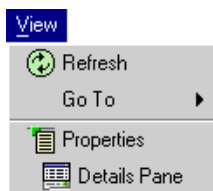
Defines a filter for the events displayed in the *Sheer EventVision* window according to the tab selected. For more information, refer to page 43.

Purge

This option is currently unavailable in this version.

View Menu

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



Refresh

Refreshes the information displayed in the *Sheer EventVision* window.

Go To

Navigates to:

- **Previous Page:** The previous page of events in the *Sheer EventVision* window.
- **Next Page:** The next page of events in the *Sheer EventVision* window.

Properties

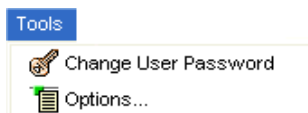
Displays the properties of the selected event, for example, the root cause and source. For more information, refer to the *Viewing Event Properties* section on page 29.

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 *Sheer EventVision* window's *Table* pane.



Change User Password

Enables the user to change the password used when logging in to the Sheer DNA Client application suite. The change will take effect the next time that the user logs in to the application.

Options

Defines the display options for the *Sheer EventVision* window. For more information, refer to the *Setting EventVision Viewing Options* section on page 15.

Help Menu

The *Help* menu provides information about Sheer EventVision.



SheerNetworks.com

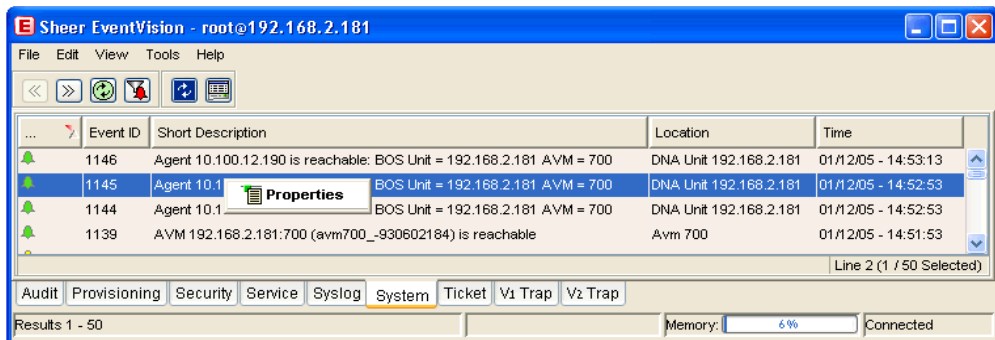
This option is currently unavailable in this version.

About EventVision

Displays application information, for example, the version number.

Shortcut Properties Menu

Displays the properties of an event selected in the Event Properties window, refer to the *Viewing Event Properties* section on page 29 for more information.









2.1.2 Color Coding of Events List Severity Icons

The Events List is color-coded according to the severity of the event. An icon is displayed 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.

2.1.3 EventVision Navigation Toolbar

The *Sheer EventVision* window contains the following tools in the Navigation bar/Toolbar:

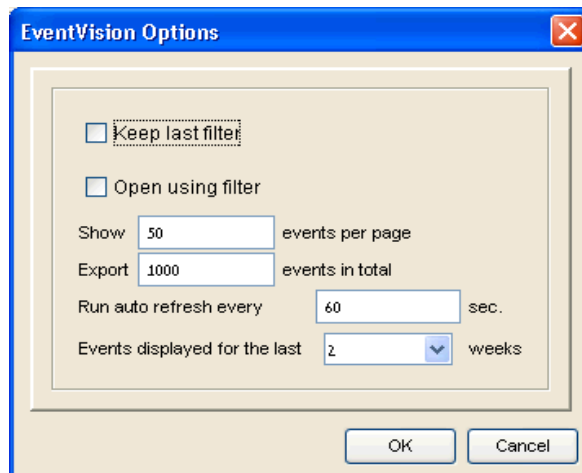
Button	Function
	Goes back to the previous page of events in the <i>Sheer EventVision</i> window.
	Goes forward to the next page of events in the <i>Sheer EventVision</i> window.
	Refreshes the events (if a filter is active, the refresh is done according to the filter) displayed in the log by querying 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, refer to page 40.
	Displays the <i>Sheer EventVision Filter</i> dialog box enabling you to define a filter for the events displayed in the EventVision log. For more information, refer to page 43.
	Toggles automatic refresh of event data on and off. You define the refresh-time period (in seconds) in the <i>EventVision Options</i> dialog box. The default is 60 seconds. If a filter is active, the refresh is done according to the filter. For more information, refer to page 15.
	Displays the properties of the selected event or ticket in the <i>EventVision Properties Details</i> pane, refer to page 13 for an example.

2.3 Setting EventVision Viewing Options

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

To define Sheer EventVision options


1. From the *Tools* menu, select **Options**. The *EventVision Options* dialog box is displayed.



The following fields are displayed in the *EventVision Options* dialog box:

- **Keep last filter:** Saves the filter criteria defined per event type in the *Filter Events* dialog box to the Sheer DNA Registry. The filter criteria are available the next time you login to Sheer EventVision.

Note: Events are not filtered automatically when you next login to Sheer 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 Sheer 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:** Enables the user to set the number of events that are displayed per page.
- **Export ... events in total:** Enables the user to set the maximum number of events to be exported to a file.
- **Run auto refresh every ... sec:** Enables you to configure Sheer 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.
2. Select the required options by checking the appropriate checkbox(es).
 3. Click **OK** to close the dialog box and save your settings.

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 *Sheer EventVision* window:

- **All**, as described on page 18.
- **Audit**, as described on page 19.
- **Provisioning**, as described on page 20.
- **Security**, as described on page 21.
- **Service**, as described on page 22.
- **Syslog**, as described on page 23.
- **System**, as described on page 24.
- **Ticket**, as described on page 25.
- **V1 Trap**, as described on page 26.
- **V2 Trap**, as described on page 27.

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 refer to page 15.

The navigation toolbar enables you to navigate through all the Sheer 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, such as 50, refer to the *Setting EventVision Viewing Options* section on page 15. You can use the **Go To** sub-menu options on the *View* menu or the respective toolbar buttons in the toolbar, to navigate between each displayed page.

3.1 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 Sheer DNA 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.

Severity	Event ID	Short Description	Time	Event Type
Green	8794	Command:InternalGet was executed by root from IP:10.56.20.185	22/02/06 - 14:27:47	Audit
Green	8793	Command:Get was executed by root from IP:10.56.20.185	22/02/06 - 14:27:47	Audit
Green	8792	Command:Get was executed by root from IP:10.56.20.185	22/02/06 - 14:27:47	Audit
Green	8791	Command:Get was executed by root from IP:10.56.20.185	22/02/06 - 14:27:46	Audit
Green	8790	Command:Get was executed by root from IP:10.56.20.185	22/02/06 - 14:27:46	Audit
Green	8789	Command:InternalGet was executed by root from IP:10.56.20.185	22/02/06 - 14:27:45	Audit
Green	8788	Command:CheckApplicationPermission was executed by root from IP:10.56.20.185	22/02/06 - 14:27:45	Audit
Green	8787	Successful login root	22/02/06 - 14:27:43	Security
Red	8781	BGP neighbour loss	22/02/06 - 14:01:31	Service
Red	8781	BGP neighbour loss	22/02/06 - 14:01:31	Ticket
Blue	8775	Enterprise generic trap	22/02/06 - 14:01:14	V1 Trap
Blue	8773	Enterprise generic trap	22/02/06 - 14:00:55	V1 Trap

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 DAY MM/DD HH:MM:SS YYYY.
- **Event Type:** The event type, namely, audit, system, ticket, provisioning, syslog, security, service, and traps.

3.2 Audit Tab

The **Audit** tab displays all of the events generated for each command or request in the Sheer DNA System, for example, opening EventVision displays the following “GetEvent” in the Audit List:

Event ID	Time	Command Name	Command Si...	Command P...	Result	Originating IP	User Name	Short Desc...
1242	04/12/05 - 08:53:51	GetEventViewerPr...	com.sheer.m...			10.56.20.130	root	Command:G...
1241	04/12/05 - 08:53:51	Get	com.sheer.fr...			10.56.20.130	root	Command:G...
1240	04/12/05 - 08:53:51	Get	com.sheer.fr...			10.56.20.130	root	Command:G...
1239	04/12/05 - 08:53:51	Get	com.sheer.fr...			10.56.20.130	root	Command:G...
1238	04/12/05 - 08:53:51	Get	com.sheer.fr...			10.56.20.130	root	Command:G...
1237	04/12/05 - 08:53:51	Get	com.sheer.fr...			10.56.20.130	root	Command:G...
1236	04/12/05 - 08:53:51	Get	com.sheer.fr...			10.56.20.130	root	Command:G...

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

- **Severity:** Displays a severity bell icon, 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)
- **Event ID:** The sequential ID number of the event (generated by Sheer DNA).
- **Time:** Logged and recorded at the time the event happened.
- **Command Name:** The audit specific command name, prefaced by, for example, such as Get..., Update..., Find...
- **Command Signature:** The actual command executed by Sheer DNA, such as com.sheer.framework.
- **Command Parameter:** This column may be empty, depending on the “real” value and a defined audit level.
- **Result:** The result of the command.
- **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 Results 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*.

3.3 Provisioning Tab

Events displayed in the **Provisioning** tab are events triggered during the configuration of a device. The Sheer DNA sends an event explaining the configuration operation, for example, 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 Sheer Command Builder and Sheer Workflow Editor. Additional information specific to this event category can be viewed in the *Events Properties* dialog box. The **Provisioning** tab is displayed below.

Event ID	Short Description	User Name	Time	Status	Source
307391	Execution of script Show succeeded	root	8/28/05 - 10:22:13	Success	PE_South
303440	Execution of script Show succeeded	root	8/28/05 - 09:11:25	Success	PE_South
303388	Script Show has failed.	root	8/28/05 - 09:10:24	Fail	PE_South
302283	Script Show has failed.	root	8/28/05 - 08:50:34	Fail	PE_South
302236	Execution of script Show succeeded	root	8/28/05 - 08:49:38	Success	PE_South
94215	Execution of script Show succeeded	root	8/25/05 - 18:27:32	Success	PE_South
94140	Execution of script Show succeeded	root	8/25/05 - 18:25:57	Success	PE_South

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

- **Severity:** Displays a severity bell icon, 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)
- **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.

3.4 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 **Security** tab is displayed below.

Severity	Event ID	Short Description	Location	Time	Client IP
Green Bell	360595	User root logged off	Avm 11	8/30/05 - 09:52:59	192.168.1.141
Green Bell	360594	Successful login root	Avm 11	8/30/05 - 09:52:59	192.168.1.141
Green Bell	360544	Successful login root	Avm 11	8/30/05 - 09:52:11	192.168.1.141
Green Bell	360493	Successful login root	Avm 11	8/30/05 - 09:51:04	192.168.1.141
Green Bell	360447	Successful login root	Avm 11	8/30/05 - 09:37:53	192.168.1.141
Green Bell	360445	User root logged off	Avm 11	8/30/05 - 09:32:05	192.168.1.46
Green Bell	360345	User root logged off	Avm 11	8/30/05 - 09:31:34	192.168.1.46
Green Bell	360337	Successful login root	Avm 11	8/30/05 - 09:31:27	192.168.1.46
Green Bell	360224	Successful login root	Avm 11	8/30/05 - 09:30:08	192.168.1.46
Green Bell	360223	User root logged off	Avm 11	8/30/05 - 09:14:41	192.168.1.46
Green Bell	360123	User root logged off	Avm 11	8/30/05 - 09:01:42	192.168.1.46
Green Bell	360115	Successful login root	Avm 11	8/30/05 - 09:01:36	192.168.1.46
Green Bell	360114	Polling group Persistence (description: Persistence) was removed		8/30/05 - 08:57:07	192.168.1.131

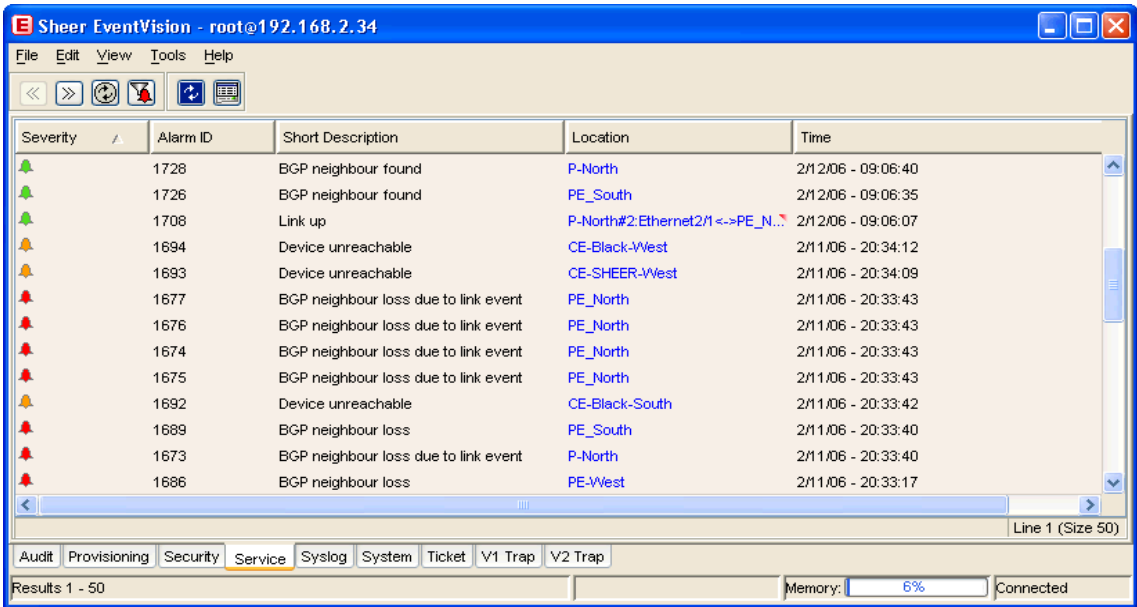
The following additional information is displayed in the **Security** tab:

- **Severity:** Displays a severity bell icon, 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)
- **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.
- **User Name:** The user name of the client.
- **Client Type:** The type of client, for example, NetworkVision or EventVision.

3.5 Service Tab

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



The screenshot shows the Sheer EventVision application window. The title bar reads "Sheer EventVision - root@192.168.2.34". The menu bar includes File, Edit, View, Tools, and Help. Below the menu bar is a toolbar with navigation icons. The main area displays a table of alarms with the following columns: Severity, Alarm ID, Short Description, Location, and Time. The table contains 15 rows of data. At the bottom of the window, there are tabs for Audit, Provisioning, Security, Service (selected), Syslog, System, Ticket, V1 Trap, and V2 Trap. The status bar shows "Results 1 - 50", "Memory: 6%", and "Connected".

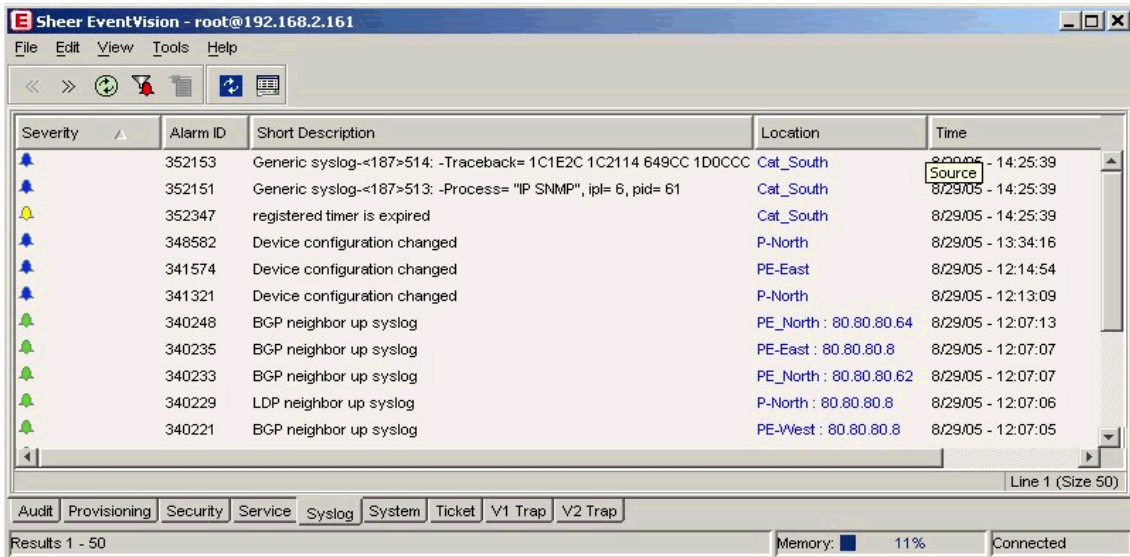
Severity	Alarm ID	Short Description	Location	Time
Green Bell	1728	BGP neighbour found	P-North	2/12/06 - 09:06:40
Green Bell	1726	BGP neighbour found	PE_South	2/12/06 - 09:06:35
Green Bell	1708	Link up	P-North#2:Ethernet2/1 <->PE_N...	2/12/06 - 09:06:07
Yellow Bell	1694	Device unreachable	CE-Black-West	2/11/06 - 20:34:12
Yellow Bell	1693	Device unreachable	CE-SHEER-West	2/11/06 - 20:34:09
Red Bell	1677	BGP neighbour loss due to link event	PE_North	2/11/06 - 20:33:43
Red Bell	1676	BGP neighbour loss due to link event	PE_North	2/11/06 - 20:33:43
Red Bell	1674	BGP neighbour loss due to link event	PE_North	2/11/06 - 20:33:43
Red Bell	1675	BGP neighbour loss due to link event	PE_North	2/11/06 - 20:33:43
Yellow Bell	1692	Device unreachable	CE-Black-South	2/11/06 - 20:33:42
Red Bell	1689	BGP neighbour loss	PE_South	2/11/06 - 20:33:40
Red Bell	1673	BGP neighbour loss due to link event	P-North	2/11/06 - 20:33:40
Red Bell	1686	BGP neighbour loss	PE-West	2/11/06 - 20:33:17

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

- **Severity:** Displays a severity bell icon, 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)
- **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.

3.6 Syslog Tab

The **Syslog** tab displays all of 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 **Syslog** tab is displayed below.



Severity	Alarm ID	Short Description	Location	Time
Blue Bell	352153	Generic syslog-<187>514: -Traceback= 1C1E2C 1C2114 649CC 1D0CCC	Cat_South	8/29/05 - 14:25:39
Blue Bell	352151	Generic syslog-<187>513: -Process= "IP SNMP", ip= 6, pid= 61	Cat_South	8/29/05 - 14:25:39
Yellow Bell	352347	registered timer is expired	Cat_South	8/29/05 - 14:25:39
Blue Bell	348582	Device configuration changed	P-North	8/29/05 - 13:34:16
Blue Bell	341574	Device configuration changed	PE-East	8/29/05 - 12:14:54
Blue Bell	341321	Device configuration changed	P-North	8/29/05 - 12:13:09
Green Bell	340248	BGP neighbor up syslog	PE_North : 80.80.80.64	8/29/05 - 12:07:13
Green Bell	340235	BGP neighbor up syslog	PE-East : 80.80.80.8	8/29/05 - 12:07:07
Green Bell	340233	BGP neighbor up syslog	PE_North : 80.80.80.62	8/29/05 - 12:07:07
Green Bell	340229	LDP neighbor up syslog	P-North : 80.80.80.8	8/29/05 - 12:07:06
Green Bell	340221	BGP neighbor up syslog	PE-West : 80.80.80.8	8/29/05 - 12:07:05

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

- **Severity:** Displays a severity bell icon, 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)
- **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.

3.7 System Tab

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

Severity	Event ID	Short Description	Location	Time
Green	360782	Agent 10.100.12.182 is reachable: BOS Unit = 192.168.2.192 AVM = 333	DNA Unit 192.168.2.192	Source - 14:28:47
Yellow	360761	Agent 10.100.12.182 is starting.BOS Unit = 192.168.2.192 AVM = 333	PE-West1	8/30/05 - 14:28:36
Yellow	360758	Agent 10.100.12.182 is shutting down.BOS Unit = 192.168.2.192 AVM = 333	PE-West1	8/30/05 - 14:26:08
Green	360698	Agent 10.100.12.182 is reachable: BOS Unit = 192.168.2.192 AVM = 333	DNA Unit 192.168.2.192	8/30/05 - 14:18:41
Yellow	360677	Agent 10.100.12.182 is unreachable: BOS Unit = 192.168.2.192 AVM = 333	DNA Unit 192.168.2.192	8/30/05 - 14:18:21
Yellow	360674	Agent 10.100.12.182 is starting.BOS Unit = 192.168.2.192 AVM = 333	PE-West1	8/30/05 - 14:18:12
Green	360669	AVM 192.168.2.192:333 (333) is reachable	Avm 333	8/30/05 - 14:13:41
Yellow	360667	AVM 333 started.BOS Unit = 192.168.2.192	Avm 333	8/30/05 - 14:13:32
Yellow	360666	AVM 333 is starting.BOS Unit = 192.168.2.192	Avm 333	8/30/05 - 14:13:29
Red	360446	Dropped Events Report	Avm 11	8/30/05 - 09:32:38
Green	360444	10 sec period limiter for general event type reached CLEARED threshold	Avm 11	8/30/05 - 09:31:47
Green	360443	10 sec period limiter for default event type reached CLEARED threshold	Avm 11	8/30/05 - 09:31:47
Blue	360419	10 sec period limiter for general event type reached WARNING threshold	Avm 11	8/30/05 - 09:31:37
Blue	360418	10 sec period limiter for default event type reached WARNING threshold	Avm 11	8/30/05 - 09:31:37
Red	360336	Dropped Events Report	Avm 11	8/30/05 - 09:31:21
Green	360332	10 sec period limiter for general event type reached CLEARED threshold	Avm 11	8/30/05 - 09:30:47

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

- **Severity:** Displays a severity bell icon, 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)
- **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.

3.8 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 **Ticket** tab is displayed below.

Sever...	Ticket ID	Short Description	Location	Last Modification Time	Time	Acknow...	Affected D...	Affected	Correlation Co...	Reduction C...	Duplication
🟢	2908199	BGP neighbour found	PE-East	04/12/05 - 10:09:00	04/12/05 - 10:08:00	false	1	41	0	2	1
🟢	2908188	Device reachable	PE-West	04/12/05 - 10:08:52	04/12/05 - 10:04:40	false	1	0	0	2	1
🟢	2908187	Device reachable	PE_South	04/12/05 - 10:08:59	04/12/05 - 10:04:35	false	1	0	0	2	1
🟢	2908182	Device reachable	CE-Black-North	04/12/05 - 10:09:40	04/12/05 - 10:04:10	false	1	0	0	2	1
🟢	2908179	Device reachable	Switch_South	04/12/05 - 10:08:58	04/12/05 - 10:04:08	false	2	0	1	4	1
🟢	2908177	Device reachable	PE-East	04/12/05 - 10:08:18	04/12/05 - 10:04:05	false	1	0	0	2	1
🟢	2908172	Device reachable	CE-SHEER-West	04/12/05 - 10:09:33	04/12/05 - 10:04:03	false	1	0	0	2	1
🟢	2908178	Device reachable	PE_North	04/12/05 - 10:09:38	04/12/05 - 10:04:02	false	1	0	0	2	1
🟢	2908176	Device reachable	CE-Black-West	04/12/05 - 10:09:36	04/12/05 - 10:04:00	false	1	0	0	2	1
🟢	2908170	Device reachable	CE-Black-South	04/12/05 - 10:09:36	04/12/05 - 10:03:53	false	1	0	0	2	1
🟢	2908093	Cold start trap due t...	PE-East	04/12/05 - 10:03:34	04/12/05 - 10:03:34	false	1	0	0	1	0
🟢	2908194	LDP neighbor up sy...	PE-East : 80.80	04/12/05 - 10:08:57	04/12/05 - 10:03:32	false	1	0	0	2	1
🟢	2908089	Reloading device sy...	PE-East	04/12/05 - 10:03:32	04/12/05 - 10:03:32	false	1	0	0	1	0
🟢	2907797	Port up	Test3_up_dow...	04/12/05 - 10:25:08	04/12/05 - 09:54:46	false	1	0	1	4	1
🟢	2905769	Port up	Test3_up_dow...	04/12/05 - 09:25:07	04/12/05 - 08:54:46	false	1	0	1	4	1

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

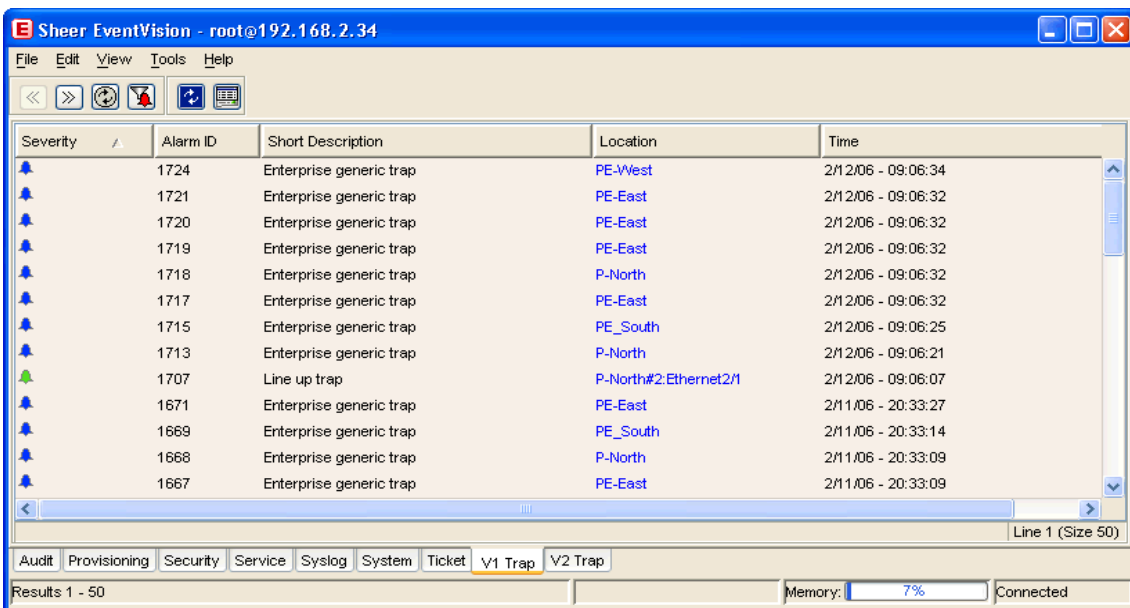
- **Severity:** Displays a severity bell icon, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the *Properties* pane's **Severity** field).
- **Ticket ID:** The sequential ID number of the ticket.
- **Short Description:** A description 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, refer to page 30.

3.9 V1 Trap Tab

This event is triggered when the Network Element sends a trap message to the Sheer DNA 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 **V1 Trap** tab is displayed below.



The screenshot shows the Sheer EventVision interface with the V1 Trap tab selected. The main window displays a table of alarm events with the following columns: Severity, Alarm ID, Short Description, Location, and Time. The table contains 15 rows of data, including several 'Enterprise generic trap' events and one 'Line up trap' event. The interface also shows a menu bar, a toolbar, and a status bar at the bottom indicating 'Results 1 - 50' and 'Memory: 7% Connected'.

Severity	Alarm ID	Short Description	Location	Time
Enterprise generic trap	1724	Enterprise generic trap	PE-West	2/12/06 - 09:06:34
Enterprise generic trap	1721	Enterprise generic trap	PE-East	2/12/06 - 09:06:32
Enterprise generic trap	1720	Enterprise generic trap	PE-East	2/12/06 - 09:06:32
Enterprise generic trap	1719	Enterprise generic trap	PE-East	2/12/06 - 09:06:32
Enterprise generic trap	1718	Enterprise generic trap	P-North	2/12/06 - 09:06:32
Enterprise generic trap	1717	Enterprise generic trap	PE-East	2/12/06 - 09:06:32
Enterprise generic trap	1715	Enterprise generic trap	PE_South	2/12/06 - 09:06:25
Enterprise generic trap	1713	Enterprise generic trap	P-North	2/12/06 - 09:06:21
Line up trap	1707	Line up trap	P-North#2:Ethernet2/1	2/12/06 - 09:06:07
Enterprise generic trap	1671	Enterprise generic trap	PE-East	2/11/06 - 20:33:27
Enterprise generic trap	1669	Enterprise generic trap	PE_South	2/11/06 - 20:33:14
Enterprise generic trap	1668	Enterprise generic trap	P-North	2/11/06 - 20:33:09
Enterprise generic trap	1667	Enterprise generic trap	PE-East	2/11/06 - 20:33:09

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

- **Severity:** Displays a severity bell icon, 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)
- **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.

3.10 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 **V2 Trap** tab is displayed below.

...	Alarm ID	Short Description	Location	Time	Affected
🔔	232830	Enterprise generic trap	R_2	05/12/05 - 15:55:50	0
🔔	232662	Enterprise generic trap	R_2	05/12/05 - 15:49:44	0
🔔	231980	Enterprise generic trap	R_2	05/12/05 - 15:25:50	0
🔔	231748	Enterprise generic trap	R_2	05/12/05 - 15:19:44	0
🔔	230953	Enterprise generic trap	R_2	05/12/05 - 14:55:48	0
🔔	230772	Enterprise generic trap	R_2	05/12/05 - 14:49:44	0
🔔	230456	Enterprise generic trap	R_2	05/12/05 - 14:39:13	0
🔔	230158	Enterprise generic trap	R_2	05/12/05 - 14:29:40	0
🔔	230147	Enterprise generic trap	R_2	05/12/05 - 14:29:18	0
🔔	230177	Line down cisco proprietary trap due to port event	R_2#0:FastEthernet0/0	05/12/05 - 14:29:15	0
🔔	230142	Enterprise generic trap	R_2	05/12/05 - 14:29:13	0
🔔	230128	Enterprise generic trap	R_2	05/12/05 - 14:28:59	0
🔔	230113	Enterprise generic trap	R_2	05/12/05 - 14:28:37	0

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

- **Severity:** Displays a severity bell icon, 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)
- **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.

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, page 29, describes how to properties of a specific event type.

Refreshing the Events List, page 42, describes how to manually and automatically refresh the *Events List*.

Filtering Events, page 43, describes how to define a filter for the events displayed in the *Events List*.

Exporting displayed Data, page 45, describes how to export the currently displayed data from the Sheer EventVision table. In addition, it describes how to import the data and view it at a later stage.

Logging Out, page 46, describes how to log out of *Sheer EventVision*.

4.1 Viewing Event Properties

Sheer 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 of:

- The **Ticket** tab, refer to *Section 4.1.1*.
- The **Provisioning** tab, refer to *Section 4.1.2*.
- The **V1** and **V2 Trap** tabs, refer to *Section 4.1.3*.

To view Event Properties

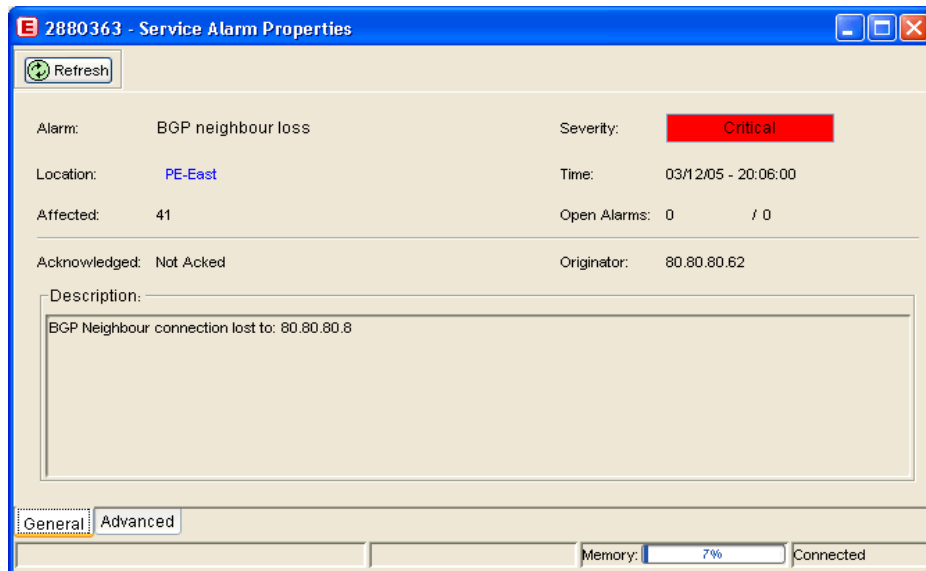
1. Select the required tab for the specific event type and the event in the *Sheer EventVision* window.


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.



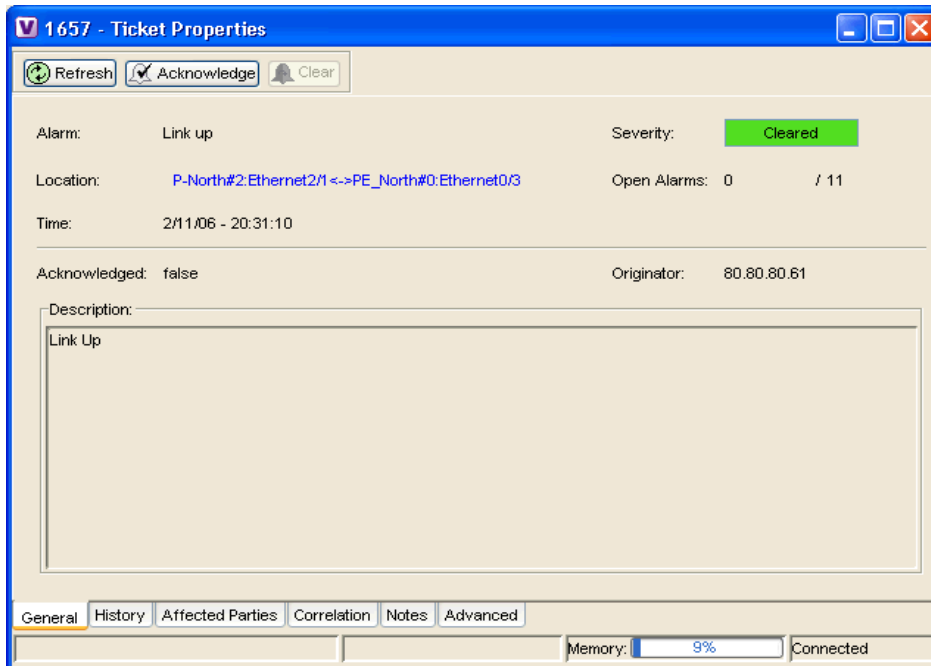
Note: Clicking  in the toolbar displays the properties of the selected ticket or event in the *Properties Details* pane.

The header displays the ID number of the selected event.

4.1.1 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. For more information about the **Ticket** tab, refer to page 25.

For information about opening the *Properties* dialog box, refer to page 29. The *Ticket Properties* dialog box is displayed.



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**, as described below.
- **Toolbar**, as described on page 39.

4.1.1.1 Tabbed Pane

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

- **General:** General information about the selected ticket, as described on page 32.
- **History:** The history of the ticket, as described on page 33.
- **Affected Parties:** The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket, as described on page 34.
- **Correlation:** All of the alarms that are correlated to the selected ticket, as described on page 36.
- **Notes:** Enables you to add notes to the selected ticket, as described on page 37.

- **Advanced:** All of the affected devices, correlation, duplication and reduction counts for the selected ticket. In addition, it provides any other additional information available about the ticket, as described on page 38.

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. For more information, refer to page 14.
- **Time:** The date and time when the initial root-cause alarm was generated. The time is taken from Sheer DNA 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 of the events. The **History** tab is displayed below.

Severity	Alarm ID	Duplication Count	Short Description	Reduction Count	Location	Time
🔴	1674	1	BGP neighbour loss due to link event	1	PE_North	2/11/06 - 20:3...
🔴	1676	1	BGP neighbour loss due to link event	1	PE_North	2/11/06 - 20:3...
🔴	1675	1	BGP neighbour loss due to link event	1	PE_North	2/11/06 - 20:3...
🔴	1673	1	BGP neighbour loss due to link event	1	P-North	2/11/06 - 20:3...
🔴	1672	1	BGP neighbor down syslog due to ...	1	P-North : 80.80.8...	2/11/06 - 20:3...
🔴	1661	1	Line down syslog due to link event	1	P-North#2:Ethern...	2/11/06 - 20:3...
🔴	1660	0	Link down syslog due to link event	1	P-North#2:Ethern...	2/11/06 - 20:3...
🔴	1657	1	Link down	1	P-North#2:Ethern...	2/11/06 - 20:3...
🔴	1658	0	Line down trap due to link event	1	P-North#2:Ethern...	2/11/06 - 20:3...

BGP Neighbour connection lost to: 80.80.80.61

General History Affected Parties Correlation Notes Advanced

Memory: 9% Connected

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 Sheer DNA 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 of the correlated faults. You can view a list of all the end-points that are affected and that have lost connectivity. For more information about **proactive impact analysis**, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide, Viewing Impact Analysis*.

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's Guide, Accumulating Affected Parties*.

The **Affected Parties** tab is displayed below.

The screenshot shows the '1657 - Ticket Properties' window. The 'Affected Parties' tab is active, displaying two tables: 'Source' and 'Destination'.

Source Table:

Location	Key	Name	Type	IP Address	Highest Affected Severity
PE-East VRF Blue		Blue@PE-...			Potential
PE-East VRF MNG_to_CE		MNG_to_...			Potential
PE-East VRF RUBEN		RUBEN@...			Potential
PE-West VRF 123445		123445@...			Potential
PE-West VRF Black		Black@PE...			Potential
PE-West VRF Blue		Blue@PE-...			Potential
PE-West VRF moshe		moshe@P...			Potential

Destination Table:

Location	Key	Name	Type	IP Address	Affected Severity	Alarm Clear State
PE_North VRF Black		Black@PE...			Potential	Cleared
PE_North VRF RUBEN		RUBEN@...			Potential	Cleared

The interface also includes a 'Find' search box, 'Refresh', 'Acknowledge', and 'Clear' buttons at the top. The bottom status bar shows 'Memory: 9%' and 'Connected'.

The **Affected Parties** tab is divided into two areas, namely, **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 sub-interface (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's Guide*.
- **Type:** The business tag type.
- **IP Address:** If the affected element is an IP interface the IP address of the sub-interface (site) is displayed. For more information, refer to the *Cisco Active Network Abstraction Managing MPLS User's 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.

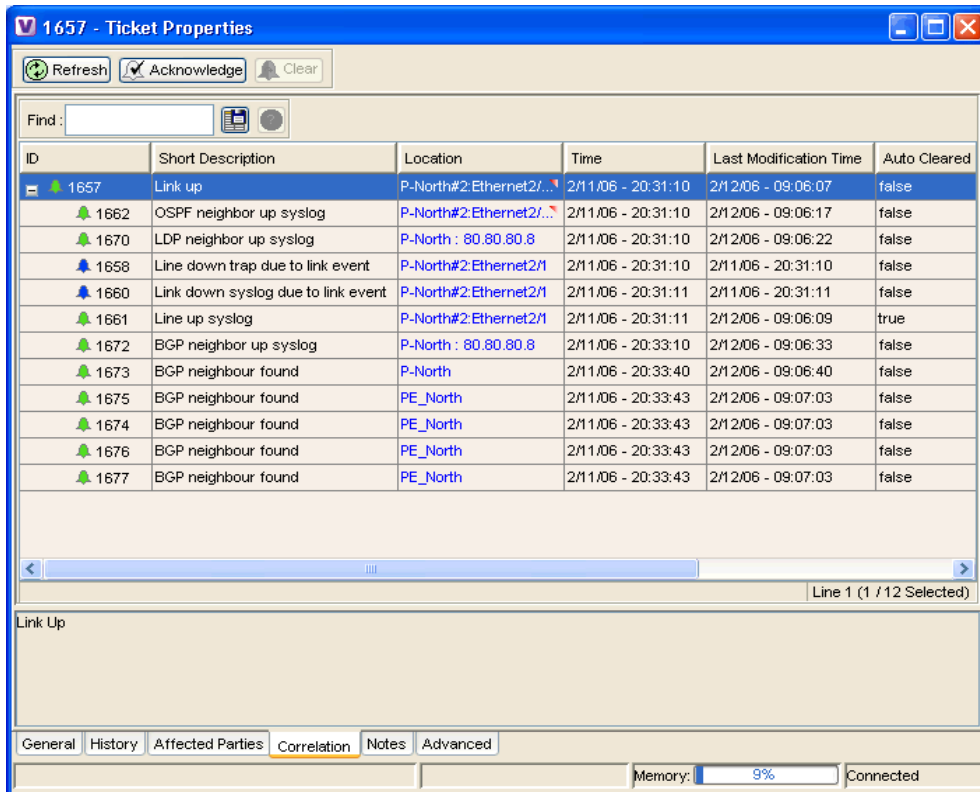
The following additional columns are displayed in the **Destination** area table in the *Ticket Properties* window:

- **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's Guide, Accumulating Affected Parties*.
- **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 of 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's Guide, Viewing a Detailed Report for the Affected Pair*.

Correlation Tab

The **Correlation** tab displays all of 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:

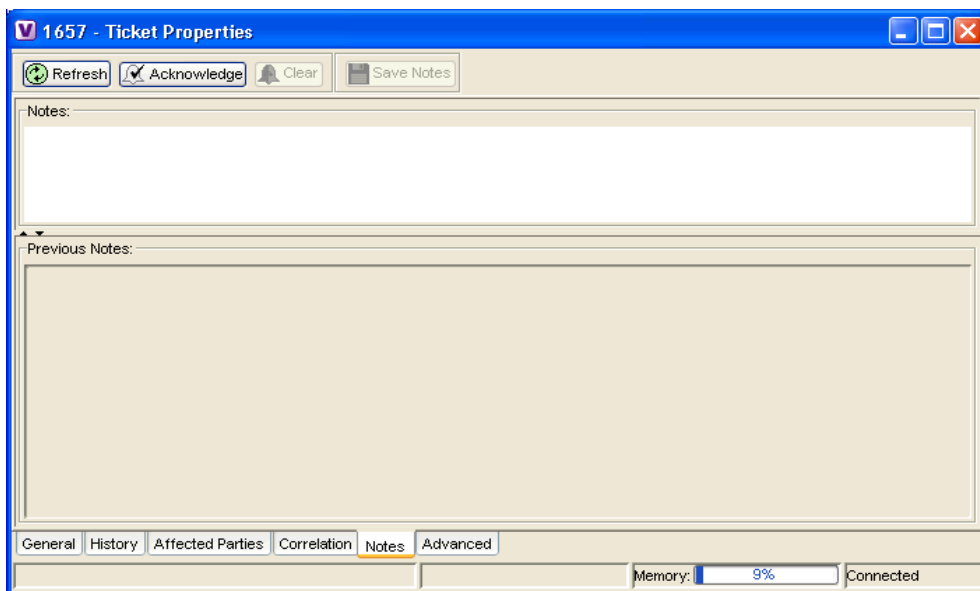
- **ID:** The ID number of the event that changed the ticket. The branches can be expanded and collapsed in order to hide information as needed.
- **Short Description:** A description of the change in the ticket. The full description is displayed in the lower tab area.
- **Location:** A hyperlink that 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 in 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. The **Notes** tab is displayed below.



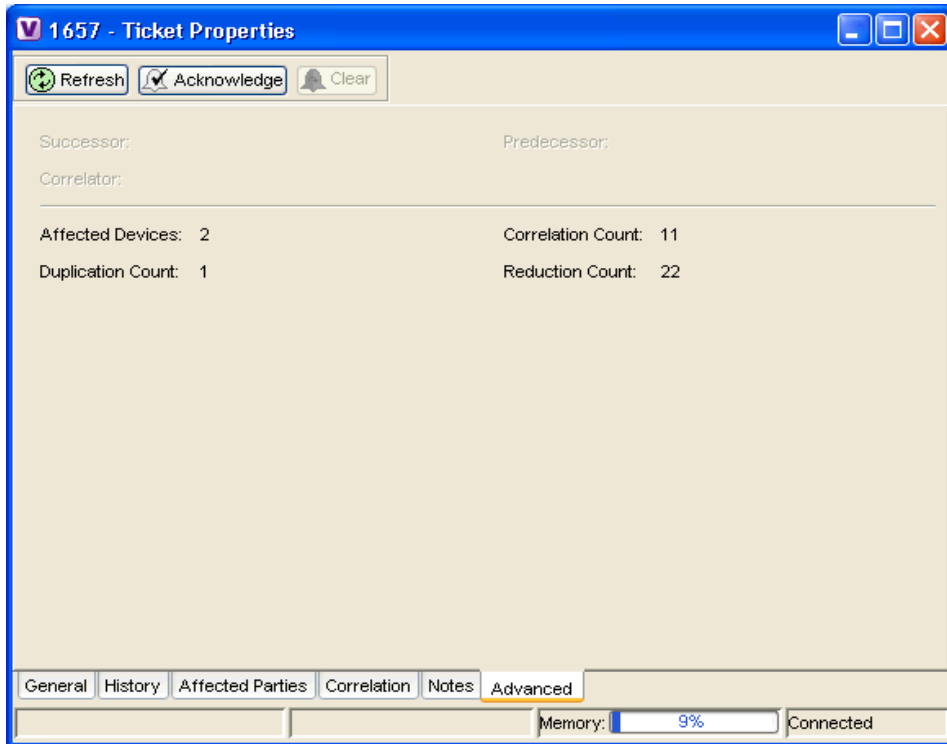
To add text, enter text in the **Notes** field and click **Save Notes**. The new text is added to any previously existing text.

Note:

- **Save Notes** is only enabled when text is entered in the **Notes** field.
- The text cannot be edited or removed once you have saved the notes.

Advanced Tab

The **Advanced** tab enables you to view all of 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 **Advanced** tab is displayed below.



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 source(s) 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 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.

4.1.1.2 Toolbar

The *Ticket Properties* dialog box contains the following tools:



Refresh

Refreshes the information displayed in the *Ticket Properties* dialog box.



Acknowledge

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's Guide*.

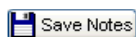
Note: This button is only enabled if the ticket has not yet been acknowledged.



Clear

Clear: Requests the relevant Sheer DNA to remove the faulty Network Element from the Sheer DNA 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's Guide*.

Note: This button is only enabled if the severity of the alarm is higher than Cleared/Normal.



Save Notes

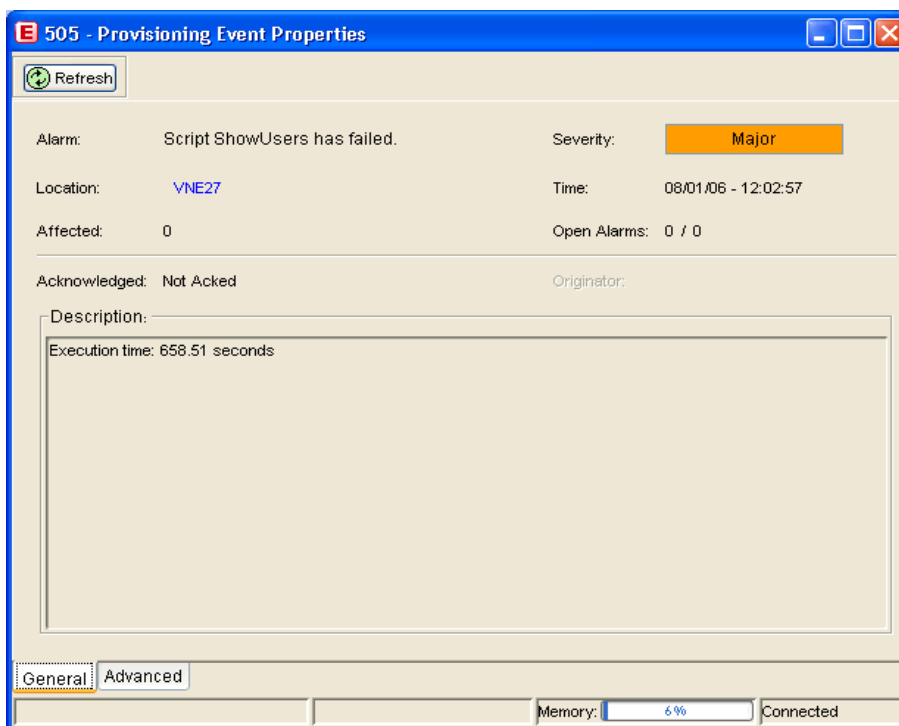
Save Notes: Saves the notes for the selected ticket.

Note: This button is only enabled when text is entered in the **Notes** field of the **Notes** tab.

4.1.2 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, refer to page 29. An example of the *Provisioning Event Properties* dialog box is displayed.



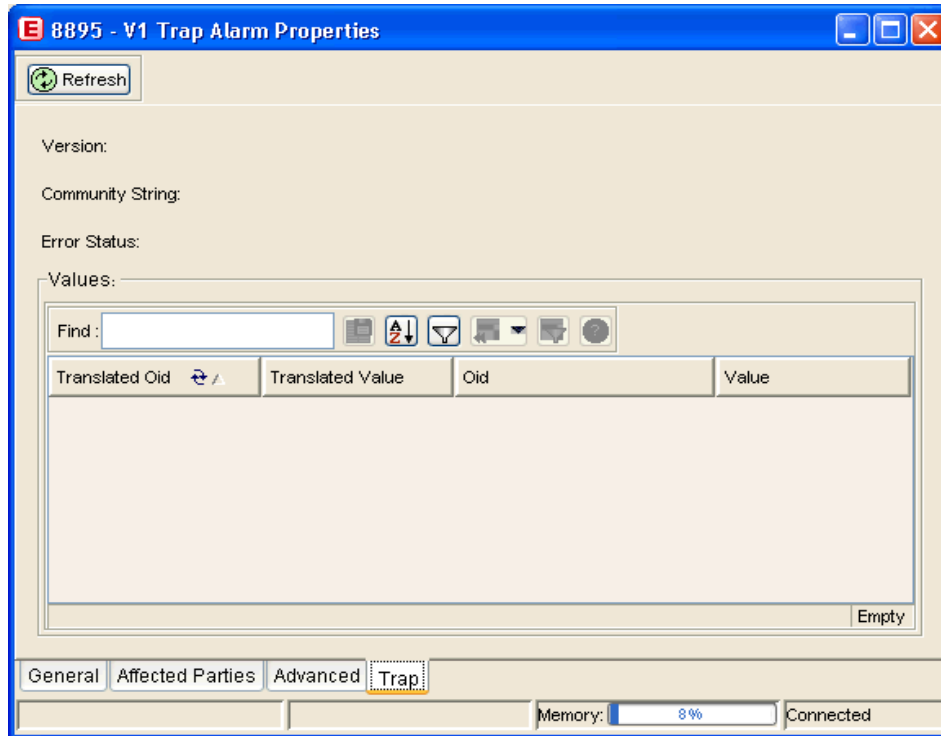
For a detailed description of the information displayed in the **Provisioning** tab, refer to page 20.

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.

4.1.3 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, refer to page 29. An example of the *V1 Trap Alarm Properties* dialog box is displayed below, with the **Trap** tab showing.



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, refer to page 26. For more information about the information displayed in the **V2 Trap** tab, refer to page 27.
- **Affected Parties:** The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. For more information, refer to page 34.
- **Advanced:** All of 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, refer to page 38.
- **Trap:** General description of V1 and V2 trap information. For more information, refer to the section below.

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.

4.2 Refreshing the Events List

Sheer 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  **Automatic Refresh** option, you configure Sheer EventVision to automatically run the refresh option. You define the refresh-time period (in seconds) in the *EventVision Options* dialog box. For more information, refer to page 15.

To manually refresh the Events List


- On the toolbar, click .



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.

To automatically refresh the Events List

- On the toolbar, click . The *Events List* is automatically refreshed, and older information is moved down the list.

Note: When you click  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 .

4.3 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 Sheer DNA database.

Note: Filter fields are enabled/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

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

or


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

2. Select and type in the required filter values.
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 (refer to page 15) saves the currently defined filter settings in the Sheer DNA Registry. The next time that the user logs in to 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 (refer to page 15), the events are continuously filtered according to the defined settings even after logging out of and in to the application.

To remove the filter

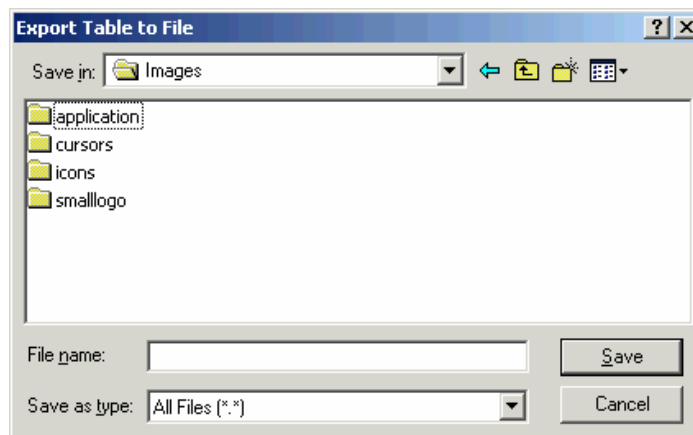
1. In the toolbar, click . The *Filter Events* dialog box is displayed as shown on page 44.
2. Click **Clear**. The selected options in the *Filter Events* dialog box are cleared.
3. Click **OK**. All of the events are displayed in the *Events List*.

4.4 Exporting displayed Data

Sheer EventVision enables you to export the currently displayed data from the Sheer 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

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




2. Browse to the directory where you want to save the list.
3. In the File name field, type a name for the list.
4. Click **Save**. The displayed Events List or row(s) are saved in the selected directory.

4.5 Logging Out

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

To log out of Sheer EventVision

- Click  to close the *Sheer EventVision* window. The *Sheer EventVision* window is closed.