



Sentriant NG Manager User Guide

Software Version 2.5

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
<http://www.extremenetworks.com>

Published: January 2008
Part number: 100289-00 Rev 01



AccessAdapt, Alpine, Altitude, BlackDiamond, EPICenter, ESRP, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodriven, Extreme Velocity, ExtremeWare, ExtremeWorks, Essentials, ExtremeXOS, the Go Purple Extreme Solution, ScreenPlay, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodriven logo, the Summit logos, the Powered by ExtremeXOS logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

Adobe, Flash, and Macromedia are registered trademarks of Adobe Systems Incorporated in the U.S. and/or other countries. AutoCell is a trademark of AutoCell. Avaya is a trademark of Avaya, Inc. Internet Explorer is a registered trademark of Microsoft Corporation. Mozilla Firefox is a registered trademark of the Mozilla Foundation. sFlow is a registered trademark of sFlow.org. Solaris and Java are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2007-2008 Extreme Networks, Inc. All Rights Reserved.



Table of Contents

Chapter 1: Introduction.....	7
Installing Sentriant NG Manager.....	7
Getting Started	7
Running Sentriant NG Manager	8
Log In to Sentriant NG Manager	8
Using the Online Help System	9
Chapter 2: Overview	11
Navigating the Sentriant NG Manager	11
Menu Bar	11
Status Bar	12
General Status Bar	13
Tab and Folder List	14
Information Panel	15
Panel Navigation Bar	16
Customizing the Screen	17
Sorting Data	17
Showing and Hiding Status Bar	18
Showing and Hiding General Status Bar	19
Getting Help	19
Messages and Tool Tips	20
Context-Sensitive Help.....	20
Sentriant NG Manager Version Information	21
Icon Legend	21
Contacting Support	22
Chapter 3: Monitor	23
Status Bar	23
Action Bar	26
Network Activity.....	27
Using the Sources Panel	28
Using the Targets Panel	59
Trend Chart	73
Address Space Panel	74
View IP Addresses	75
Viewing Address Space Details	76
Querying Address Space	78
Address Space Actions	79
Access Activity.....	86
Chapter 4: Events	89
Appliance Events	89
Audit Events	91

Network Activity Events	93
View Network Activity Events	93
Network Activity Details	95
Network Activity Events Actions	102
Chapter 5: Reports	111
System Overview Report	111
Enhanced Reporting	115
Threat Report	116
Audit Report	117
Chapter 6: View Configuration	119
Access	119
Alerts	121
Destinations	121
Sources	122
Deception	124
Personalities	125
Personality Sets	125
Named Items	125
IP Sets	126
Port Sets	126
Traffic Sets	126
Network	127
Segments	127
Segment Sets	127
Appliance	128
Policy	128
Rules	128
Rule Sets	129
Chapter 7: Edit Sentriant NG Configuration Settings	131
Access	138
Creating User Accounts	139
Deleting User Accounts	140
Creating Clients	141
Deleting Clients	142
Alerts	143
Creating SMTP Destinations	144
Deleting E-mail Destinations	147
Creating SNMP Destinations	148
Deleting SNMP Destinations	149
Creating Syslog Destinations	150
Deleting Syslog Destinations	151
Setting Up Sources	152
Deception	153
Creating Personalities	154
Deleting Personalities	157
Creating Personality Sets	158
Deleting Personality Sets	161

Named Items.....	162
Creating IP Sets	162
Deleting IP Sets	164
Creating Port Sets	166
Deleting Port Sets	168
Creating Traffic Sets.....	170
Deleting Traffic Sets	174
Network	176
Runtime.....	177
Segments	198
Segment Sets	236
Switch Information.....	251
Policy	255
Rules	255
Rule Sets	290
Save/Load Configuration Settings.....	293
Save Configuration From File Menu.....	294
Save Configuration From the Configuration Changes Dialog	295
Save Configuration From Navigation Bar	297
Load Configuration Settings	299
Chapter 8: Appliance.....	301
Date and Time	301
Maintenance.....	304
Edit Appliance Name.....	305
Edit Appliance IP Configuration	307
Maintenance Actions	308
Health.....	322
Glossary	329
Index	339

1 Introduction

Welcome to the *Sentriant NG Manager User Guide*. This user guide gives complete instructions for using Sentriant™ NG Manager. Included are user instructions for everyday tasks and administrator instructions for configuring and customizing Sentriant NG Manager.

This documentation uses the following conventions:

Menu tabs and subtabs used to access screens are shown in **bold** separated by a greater than symbol. For example instructions for how to get to the Monitoring Sources Panel, which is accessed by first clicking the Monitoring tab, then the Network subtab, and then selecting Sources will be shown as **Monitoring > Network > Sources** in the documentation.

Installing Sentriant NG Manager

You must install the Sentriant NG Manager either from the CD that was shipped with your Sentriant NG, or by logging in to the Extreme Networks® support site and downloading the Sentriant NG Manager software.

To install the Sentriant NG Manager:

Insert the CD and follow the on-screen instructions for installing the Sentriant NG Manager.

or

Bring up a web browser and enter the URL for the Extreme Networks Support site. Follow the instructions for downloading and installing the Sentriant NG Manager.



NOTE

You can download the installer, save it locally and perform the install to reduce network traffic. After downloading, double-click `ExtremeConsole_windows_Installer.exe`



NOTE

You do not need to install any other software. A Java virtual machine is included with this download.

Follow the on-screen instructions.

Getting Started

Extreme Networks provides an online help system where you can find information for using Sentriant NG Manager.

Running Sentriant NG Manager

You start Sentriant NG Manager just as you would any software application.

To start Sentriant NG in Windows:

Choose **Start > Programs > Sentriant Manager > Sentriant Manager**.

Log In to Sentriant NG Manager

To login to Sentriant NG Manager, you will need to be a user of the system and have the IP Address of a Sentriant NG which you will be connecting to.

To login to Sentriant NG Manager:

From the Sentriant NG Manager Login screen, do the following.

- Type in the Sentriant NG IP Address and port number separated by a colon.
Example: http://192.168.65.2:22



NOTE

If the Sentriant NG resides in a Network Address Translation (NAT) environment, the NAT port assigned to the Sentriant NG must be specified when logging in. By default the port number is 22 and may be excluded in non-NAT environments.

- Type in admin as the user name
Example: admin
- Enter the admin password
Example: *****
- Select the **Remember Settings** radio button and click **Login**.

**NOTE**

Selecting Remember Settings will save the Sentriant NG IP Address, username, and password.

Using the Online Help System

Sentriant NG Manager also includes complete documentation in a Java-based help system. The Sentriant NG Manager Help system includes all of the information in this User Guide.

Online Help provides three ways of locating information. The Contents and Index links let you find general information, and the Search link lets you look up specific words or phrases.

To start online Help:

From the File Menu, choose **Help > Sentriant Help**.

Overview

This chapter provides information about the Sentriant NG Manager interface and its tools for locating, organizing, and displaying information. Consult the topics in this section to find out more about Sentriant NG Manager's Menu Bar, Status Bar, General Status Bar, the Folder List, the Information Panel and the Navigation Bar. This section also includes topics on customizing elements of the interface.

Navigating the Sentriant NG Manager

The Sentriant NG Manager provides a variety of standard navigation tools for finding your way around and locating information you need quickly. You can customize views to suit your need or hide them to save space.

The first time you start the Sentriant NG Manager, you will see the Configure Overview screen, which displays a quick-start procedure on creating and saving a segment configuration. You will also see the screen components and navigation tools as follows:

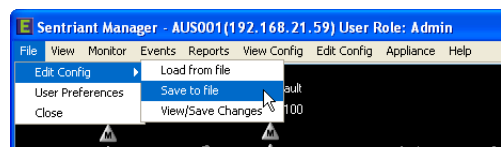
- Menu Bar
- Status Bar
- General Status Bar
- Folder List
- Information Panel
- Navigation Bar

Menu Bar

Clicking an item on the Menu Bar opens a drop-down menu of commands. Clicking a menu command either carries out the command or opens a sub-menu or dialog box with additional choices. An arrow symbol next to a command signifies a sub-menu; an ellipsis (...) signifies a dialog box.

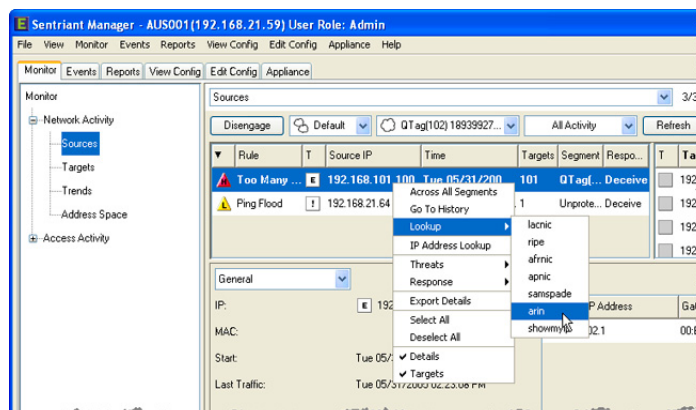


Some menu commands turn a view off and on. A check mark next to the menu command indicates that the setting is currently active.



In addition to the pull-down menus on the Menu Bar, shortcut menus are available on certain screens which give you quick access to common commands for a particular context.

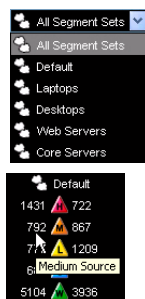
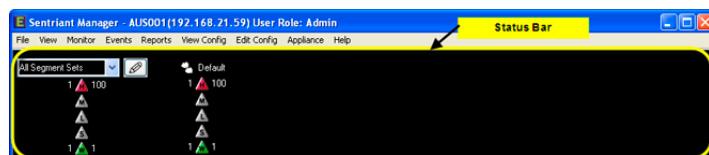
Shortcut menus are activated by clicking the right mouse button when the mouse pointer is positioned over an item in a list or in a particular area of the screen. Clicking a command on a shortcut menu will apply to the currently selected list item or the part of the screen where the pointer is resting.



Status Bar

The Status Bar at the top of the screen provides real-time status information about current network threats and potential threats, and it alerts you to network security issues that require attention. The Sentiari NG appliance supports up to 32 network segments. A scroll bar appears if there are additional network segments that are out of view in the Status Bar.

The Status Bar is always active while the user is logged into the Sentiari NG Manager. Each status object contains active statistics displaying the number of sources and targets that are currently being tracked as threats, suspects and watches in each network segment. The statistics also reflect each Threat priority level and Network Segment status, as shown in the following Status Bar graphic.



Select a Segment Set to be displayed in the Status Bar. The Segment Set's segments will be displayed in the Status Bar. Selecting All Segment Sets displays all Segment Sets with threat counts summed for each Segment Set.

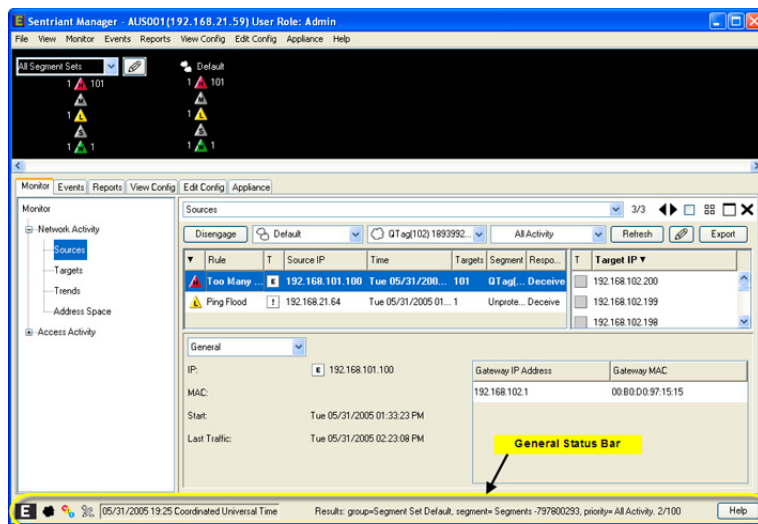
In the Status Bar, selecting a Source from one of the threat trees will display the **Monitoring > Network Activity > Sources** Panel filtered to the selected segment and threat priority.



In the Status Bar, selecting a Target from one of the threat trees will display the **Monitoring > Network Activity > Targets** Panel filtered to the selected segment and threat priority.

General Status Bar

The General Status Bar displays the status and activities for the appliance health, segments, and events.



The icons will change based on the type of current activity described below:













The Sentriant NG appliance icon represents the rolled-up operating status for all Sentriant NG appliance(s) within the Fabric. If an error or warning is encountered with an appliance, the icon will change accordingly displaying the highest severity. For example, a fabric is made up of four (4) appliances. One has an error and another has a warning. The icon displayed in the panel will show that there is an appliance with an error since it is a higher severity. Clicking on the icon will take you to the **Fabric > Health** page which displays all appliances within the fabric. The appliance states are described below:

- E** normal The Sentriant NG appliance is operating normally
- E** warning There is a warning with the Sentriant NG appliance
- E** error There is an error with the Sentriant NG appliance
- E** off The Sentriant NG appliance is off

The Segment icon represents the rolled-up operating status for all segments within the Fabric. If a status change occurs with a segment, the icon will change accordingly displaying the highest severity. For example, a segment has been blocked. The icon displayed in the panel will show that there has been a change in status to a segment. Clicking on the icon will open a dialog with the affected segments. Clicking a segment in the list will take you to the **Edit Config > Network > Segments** page.

The segment states are described below:

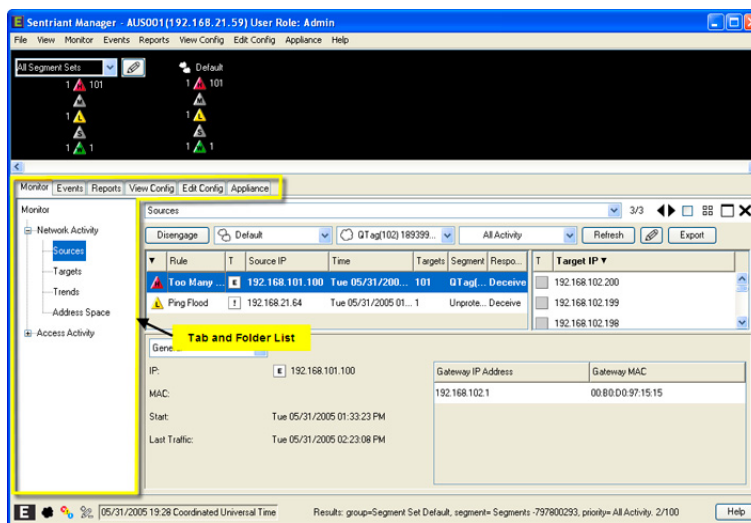
- The segment is operating normally and configured

-  There is a conflict with segment configuration
-  The segment is disengaged
-  The segment is disengaged and has a conflict
-  The segment is blocked
-  The segment is blocked and has a conflict
-  The segment is disabled
-  The segment is disabled and has a conflict
-  The segment is unconfigured
-  The segment is unconfigured and has a conflict
-  Clicking on the Events icon takes the user to the Events Panel.
-  Indicates a configuration change is pending. Configuration changes are kept locally until an administrator persists the changes to the Sentiariant NG appliance.
-  No pending configuration changes.

Additional items in the General Status Bar are the [General Status Messages](#) text and [Context-Sensitive Help](#) button. The General Status Message displays a textual representation of the filtering done by the Action Bar located in the Information Panel. For the example below, a query or filter on Laptops group, Laptops0 segment and All Threats were selected as the priority. At the end of the message is the number of threat sources and targets from the Status Bar. Clicking the Help button brings up context-sensitive help screens for the displayed panel.

Tab and Folder List

The **Tab and Folder List** is a tabular list with a hierarchical structure graphically representing the categories of Sentiariant NG Manager data. When you select a tab and open a folder, the [Information Panel](#) displays the folder contents. For Windows, a plus sign (+) next to a folder icon indicates a closed folder; a minus sign (-) indicates an open folder.

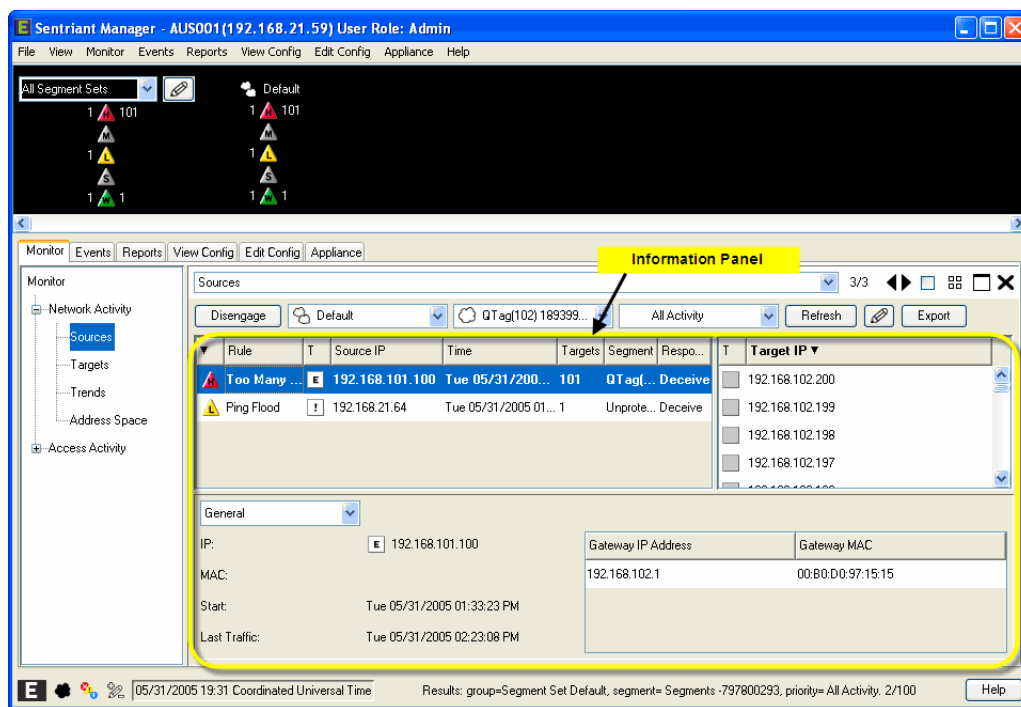


Information Panel

The large area that occupies most of the program window is the **Information Panel** which displays the contents of an open folder. Each folder has a corresponding panel that provides menus and tools specific to the tasks that you may need to perform while working in that panel.

Selecting a tab and then clicking a folder in the Folder List displays one of the following panels:

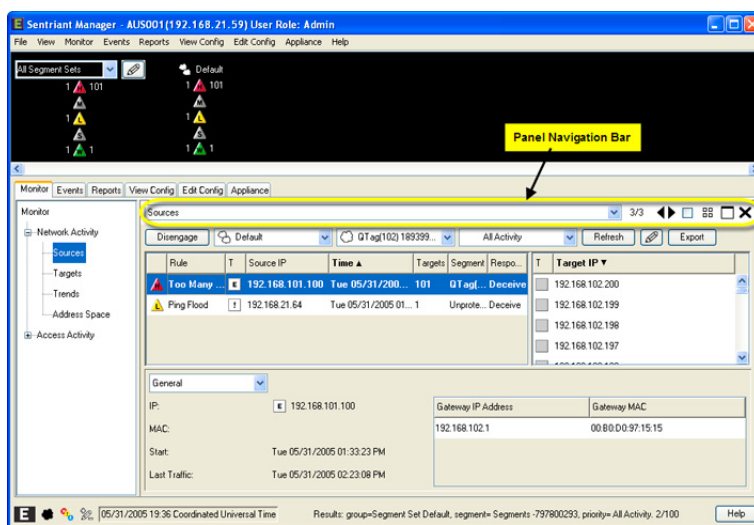
- **Monitoring** - displays threats and address space information. From this panel you can manage/mitigate the threats detected on configured segments within groups.
- **Events** - displays a log of events over time for the SentiNG appliance, Audit or configuration activities, Grid such as new appliance added, and Threat Sources events such as source start and end times and threat escalations.
- **Reports** - displays a daily or weekly **System Overview Report** of activity on one or all network segments over a specified time period.
- **Configure** - displays configuration capabilities and allows administrators of the Extreme SentiNG appliance to perform the following configuration services access, alerts, deception, create and configure groups, and create rules.
- **Appliance** - displays information about the SentiNG appliance's health and working status. Maintenance activities can be performed from this panel to include, disengage and engage, delete the appliance (connectively, not physically) from the network, and restore default configuration.



Each view summarizes the major properties of the items shown. Since the views are dynamic, they are updated to reflect any changes in an item's status, response, or other properties.

Panel Navigation Bar

The Panel Navigation Bar provides a means of changing the way panels are displayed within the Information Panel. A drop-down list keeps track of opened category panels. Controls for changing information panels are provided and determine how the panels are displayed. Panels can be turned off, tiled or displayed singularly.



Targets

Drop-down list of opened panels. Selecting a panel from the drop-down list will display that panel.

2/3 Indicates the logical ordering of panels under the current top-level node.

◀▶ Click the right or left arrow to scroll forward or backward through the panels.

☑ Keeps the current panel active when you navigate to another panel. When selecting Tile, the panel marked as 'keep' will be displayed in the panel workspace.

☐ Click the Tile icon to tile all panels that have been opened. The tile panels button is used mainly when you are reviewing charts across multiple segments. By tiling the trend charts, you will see activity across multiple segments on the screen at once.

☐ Click the icon to maximize or minimize the panel.

✕ Click the icon to close the panel.

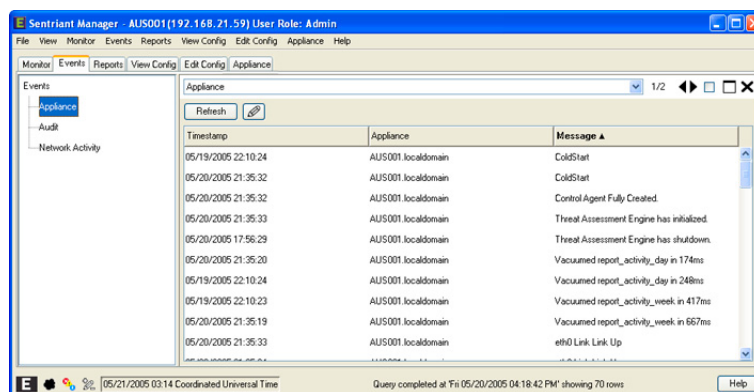
Customizing the Screen

Sentriant NG Manager displays information in the **Information Panel** as a tabular list of items, along with their major properties. These properties are arranged in columns that you can sort, hide, resize and rearrange. Click the links below to learn about:

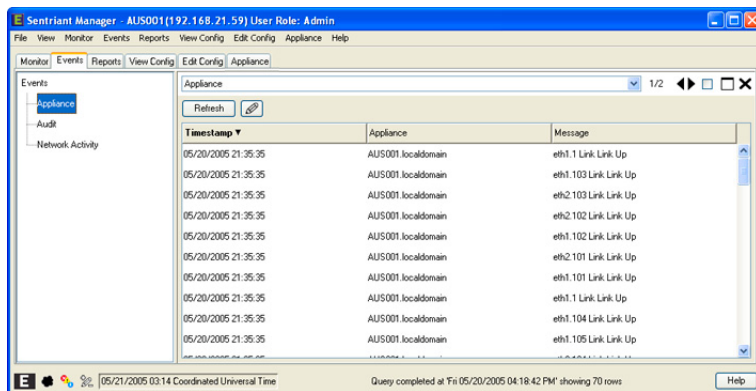
- [Sorting Data](#)
- [Showing and Hiding Status Bar](#)
- [Showing and Hiding General Status Bar](#)

Sorting Data

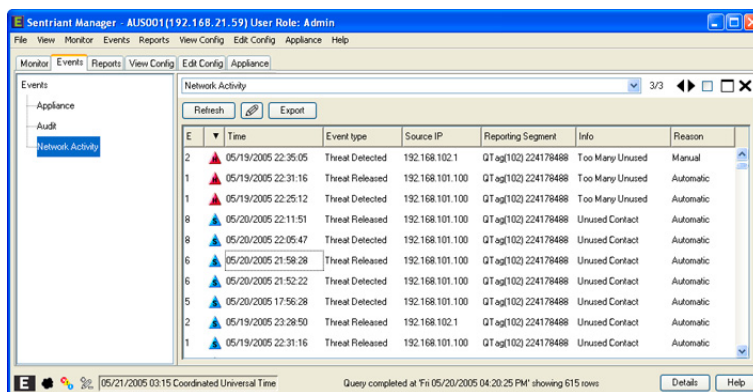
Sorting arranges data in a list sequentially according to data values. Data can either be sorted in an ascending order, for example alphabetical sorts are A to Z and numerical sorts from lowest to highest.



Descending sorts are the opposite result with numerical sorts from highest to lowest.

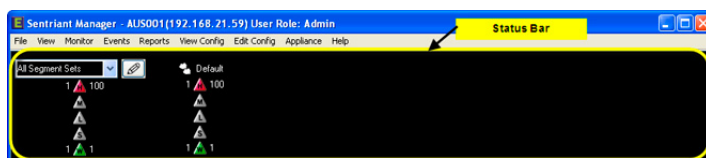


This can be useful if you wish to group Threat priorities together. For example, by clicking on the Threat Priority column, all High level threats will be grouped together then Medium, Low, Warning and so on.



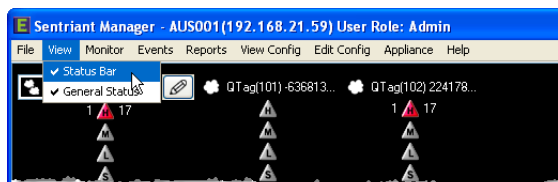
Showing and Hiding Status Bar

The **Status Bar** at the top of the screen provides real-time status information about current network threats and potential threats, and it alerts you to network security issues that require attention. You can hide and show the Status Bar as needed while you work.



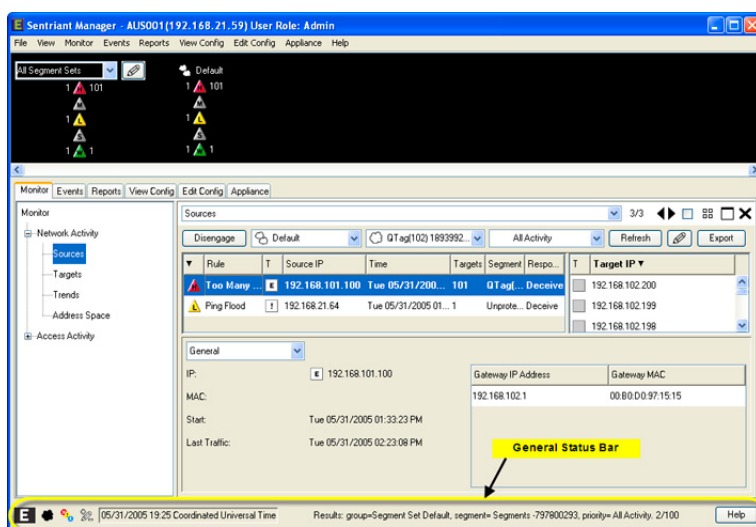
To show or hide the Status Bar:

- 1 From the **View** menu, select **Status Bar** to hide.



Showing and Hiding General Status Bar

The General Status Bar displays the status of activities for the appliance health, segments, and events. You can hide and show the General Status Bar as needed while you work.



To show or hide the General Status Bar:

- 1 From the **View** menu, select **General Status** to hide.



Getting Help

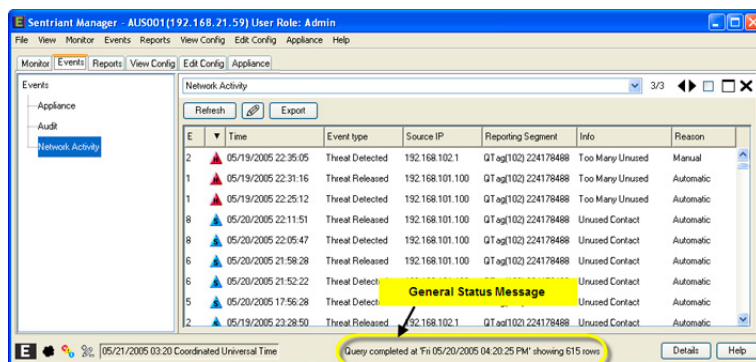
Sentriant NG Manager provides the following options for obtaining on-screen assistance:

- [Messages and Tool Tips](#)
- [Context-Sensitive Help](#)

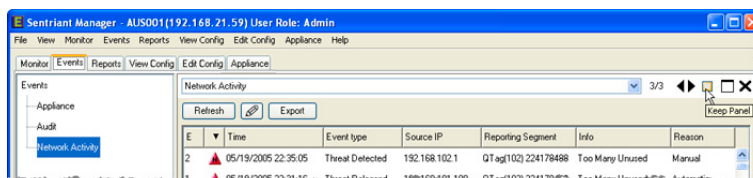
- Sentriant NG Manager Version Information
- Icon Legend

Messages and Tool Tips

Sentriant NG Manager provides brief descriptive messages that indicate what a command will do before you select the command. One kind of message is the **General Status Message**, which appears in the General Status Bar at the bottom of the screen. When you perform a command, the General Status Message is constructed based on the command. For example, from the **Monitor > Network > Sources** panel, a filter on Medium Priority Threats is performed, the General Status Message displays the syntax of the filter.

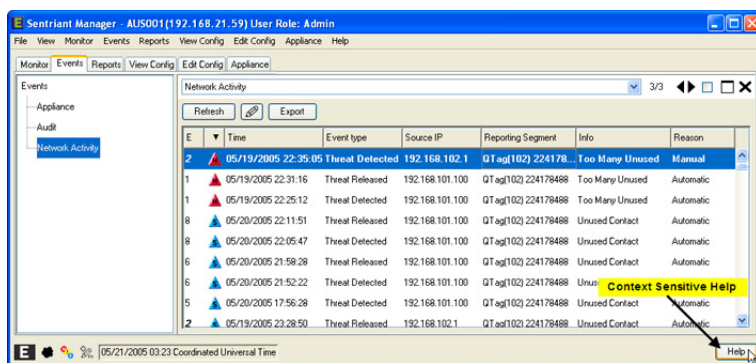


Another type of message is a **Tool Tip**, a text label describing the function of a toolbar button. Tool Tips appears when you place the pointer over a button, table field or other type of command or control.



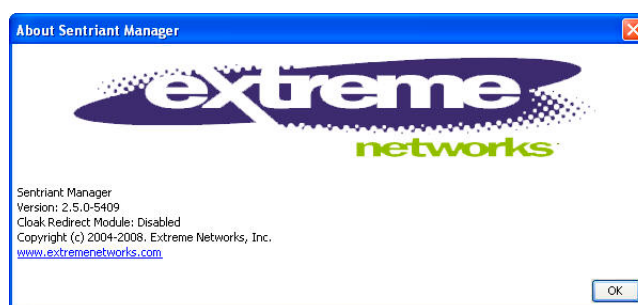
Context-Sensitive Help

Context-sensitive help is also available for most of Sentriant NG Manager's Information Panels. The corresponding Help topic displays when you press the Help button located at the bottom right of the General Status Bar.



Sentriant NG Manager Version Information

The About command on the Help menu displays the **About Sentriant Manager** dialog which shows the version of Sentriant NG Manager that you are using in the title bar of the dialog.

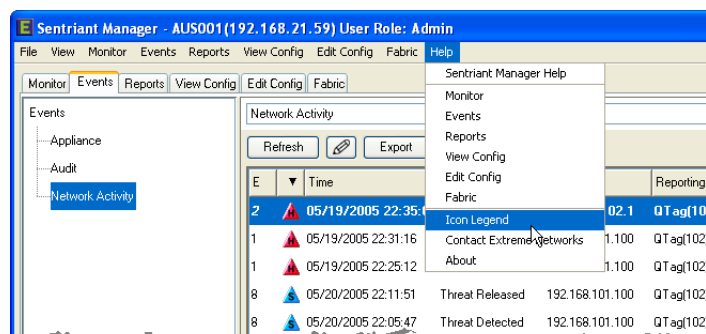


Icon Legend

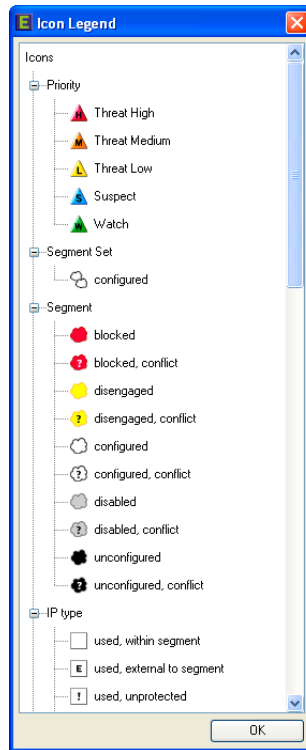
An Icon Legend is provided that groups icons relative to their usage (for example, threat priority, group, configure). A short description follows each icon. You may collapse or expand each group as needed.

To view the Icon Legend:

- 1 From the Menu Bar, select Help then Icon Legend.



- 2 Scroll down the list to see the icon categories.



Contacting Support

Please contact Extreme Networks Support by logging in to our **Technical Support Portal** at <https://esupport.extremenetworks.com/>. The portal allows you to search the Extreme Networks knowledgebase, submit a support incident, and track incidents that your organization has submitted. If you wish to speak with support representative, call toll free at (800)-998-2408. Before calling, please create a support incident through the portal and reference the incident number.

If you report an incident with Sentriant NG Manager, please include the following information:

- Your name, E-mail, phone and fax number
- A description of the incident and what you were trying to do
- Sentriant NG Manager Software version number
- The make and model of the Sentriant NG appliance
- The make and model of the switch connected to the Sentriant NG appliance

Monitor

The Sentriant NG appliance's Monitor functions let you monitor, track, and manually mitigate suspicious and potentially threatening network behavior across one or more network segments that are under the protection of the Sentriant NG appliance. Threat behavior can be monitored whether it originates from a source inside or outside of the Sentriant NG appliance's protected range.

Clicking the Sentriant NG appliance's **Monitor Tab** gives you access to **Network Activity**, a **Trend Chart**, **Address Space Panel**, and **Active Sessions**. These panels contain information about network source and target traffic currently being monitored on selected network segments. From these panels, you can perform specific actions to assess and mitigate potentially threatening network behavior. These panels are:

Sources - Selecting a Source IP Address displays detailed information about the IP Address, including a history of any threat and mitigation taken as well as a list of its target IP Addresses within the Sentriant NG appliance's protected range.

Targets - The Targets panel provides a list of Target IP Addresses for the selected network segment. Choosing a target displays a list of source IP Addresses that have contacted the target.

Trend Chart - A visual representation of historical network traffic for all Segment Sets or segments over time. The information can be used to determine threat patterns.

Address Space - The Address Space panel provides a set of detailed state information for a list of IP Addresses in the selected network segment. You can use this state information to verify that used and virtual IP Addresses for a segment are allocated as expected. You can also take action from this panel to add an IP Address as a gateway or to exclude an IP Address from being virtualized.

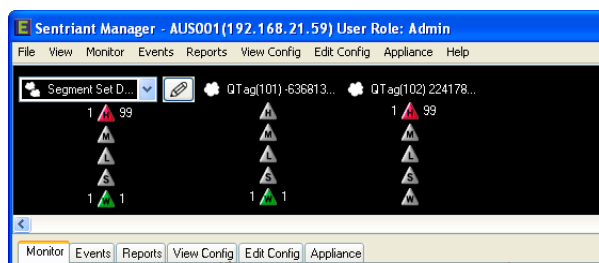
Active Sessions - Displays a list of active users connected to the Sentriant NG appliance through the Sentriant NG Manager. Active Session data displayed includes the user's login ID, a time stamp showing date, time and time zone, and the IP Address of the client connected to the Sentriant NG appliance.

Status Bar - The Status Bar displays a visual representation of traffic. The view can show all Segment Sets with segment totals rolled up for each threat priority or by Segment Set with each segment represented.

Panel Action Bar - Directly above the Sources, Targets, and Address Space panels provides controls for filtering and modifying actions on currently selected Threats, Suspects, and Watches.

Status Bar

The real-time Status Bar at the top of the Sentriant NG Manager shows currently active Threats, Suspects, and Watches for all configured network segments contained within Segment Sets and provides tools and resources that let you monitor and quickly determine the nature of any malicious network behavior.



The **Status** area, which is always active but can be hidden, displays sets of status objects. Status objects represent network Segment Sets or individual segments that have been configured within the protection range of the Sentriant NG appliance. Each set of status objects contains active statistics that displays the number of sources and targets currently being tracked. The statistics also indicate Threat priority levels and the status of network segments.

The Sentriant NG appliance supports up to sixty-four (64) network segments. The network administrator can combine the segments to form a Segment Set containing functionally-related segments usually grouped by VLANs. Segment Sets are represented by the following icon:



The illustration above displays Segment Sets Qtag(101) and Qtag(102). On initial configuration a Segment Set named Default is created where discovered segments will be placed. The segments can be moved according to their functionality. For example, laptops are contained within a Segment Set called Laptops. Creating Segment Sets that have similar configurations makes threat monitoring and mitigation more manageable.

Priority Levels

Threat sources that have triggered rules, or that communicate with a target monitored by Sentriant NG are assigned a priority level. Priority levels are governed by Sentriant NG appliance policies, rules, and response modes that can be modified or configured as needed to meet network requirements.

The Sentriant NG appliance supports five priority levels:

-  Threat High
-  Threat Medium
-  Threat Low
-  Suspect
-  Watch

Each object in the Status area includes counters representing the number of hosts that are active at a given priority level within the network segment that the status object represents. For a given status object, the left side of the priority level displays the number of sources within that segment at that priority level. The right side of the status object displays the targets contacted by one or more source(s)

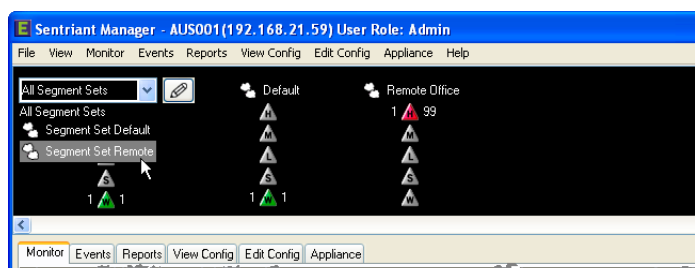
at the corresponding priority level. A target is displayed only once and is determined by the source that triggered the highest priority level. For example, a target has traffic from two sources, one source triggers a medium threat while the other triggers a high threat. The target will only be displayed in the high threat priority level.



You can obtain more information about sources or targets by clicking on the counter or the Priority Level Icon. Clicking the sources counter or Priority Level Icon displays sources information while clicking on the targets counter displays information for targets. This action loads data about the status objects represented.

View Segments

A drop-down menu at the upper left of the Status Bar contains the list of Segment Sets. Here you can select to view all Segment Sets or select a specific Segment Set to be displayed in the Status bar. The segments contained in the Segment Set will be displayed individually. A scroll bar across the bottom appears if there are additional segments that are out of view in the Status area.




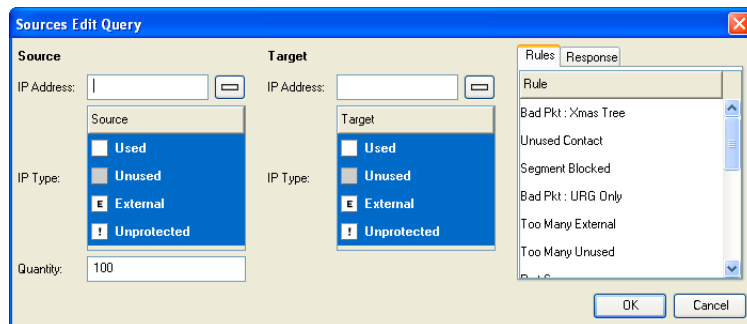
Querying IP Types

The Status Bar by default displays all IP Types from sources and targets. IP Types are:

- ☐ Used - IP Address used by host within the protected range
- ☒ Unused - IP Address within the protected range that is not used by a host
- ☐ External - IP Address used by host external to the protected range
- ☐ Unprotected - IP Address not in the protected range

It may become necessary to display only certain IP Types for sources and targets to track down a specific threat pattern.

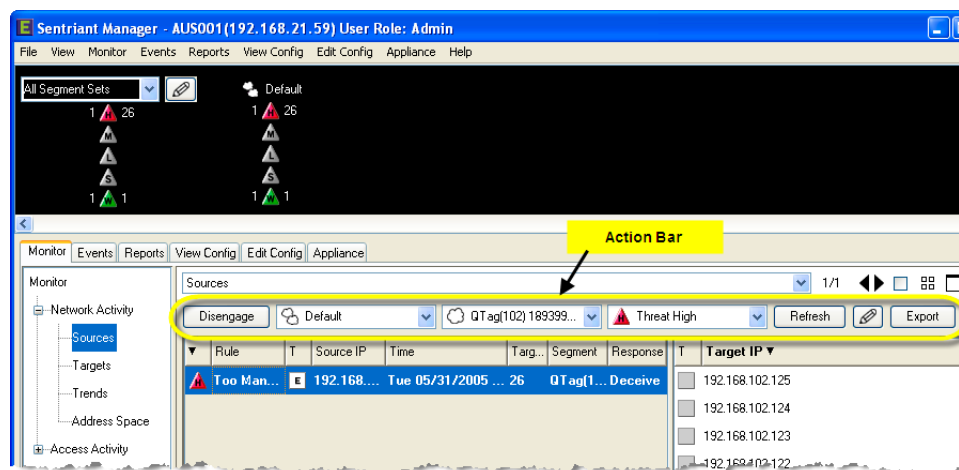
Clicking the **Edit Query**  button in the Status Bar will bring up the Threat Status Bar Edit Query dialog.



Select or unselect the IP Types for sources and targets. For example, to show sources external to the monitored segment with traffic on all IP Addresses within the segment, select External (external to segment) for sources and select all of the types for targets.

Action Bar

The **Action Bar** at the top of the Information Panel contains buttons and drop-down lists that allow you to perform specific actions on current Threats, Suspects, and Watches.



The **Disengage** button has two states **Disengage** and **Engage**. In Disengage mode, it disables all monitoring and threat mitigation for the selected network segment or all network segments. In Engage mode, it re-enables all Sentriant NG appliance monitoring and threat mitigation for the selected network segment or all network segments. At some times it may become necessary to disengage the Sentriant NG appliance from the network to perform administrative tasks such as network reconfiguration.



NOTE

It is recommended to Disengage the Sentriant NG appliance rather than shutting down to prevent loss of critical data.

The selected network segment remains disengaged until one of the following events occurs:

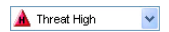
- The Engage button is invoked
- The Sentriant NG appliance is rebooted



The Segment Sets menu lets you select specific Segment Sets for monitoring or for mitigation action.



The Segment menu lets you select a specific network segment for monitoring or for mitigation action.



The Threat Type menu lets you select a specific priority level for monitoring or for mitigation action.



Refreshes the Sources Panel when filtering on Segment Sets, segments or threats.



Clicking the **Edit Query** button opens an advanced query dialog where queries can be performed on Sources, Targets, and Address Space tables. These queries are used in conjunction with the Segment Select and Priority Select menus to filter information and help you discover threat-related usage patterns and trends in a network segment or segments. The data fields that are available in the advanced query menu differ depending on the current panel, however most functionality remains the same for each.



Data coming from the Sentriant NG appliance is 'live' or streaming data. As threats are detected, they may be contained and removed based on the rule timeout value.

Clicking the **Export** button opens a dialog where you can export data from the Sources, Targets, and Address Space panels. The purpose of the exported data is to keep a log of network activity and also used as a report to help update rules and identify new threats that have been detected. The exported data can be saved either as a formatted text file, HTML page or to a Microsoft Excel spreadsheet.

Network Activity

When a source violates a rule, the source and target IP Address pair is added as a threat. Sources are displayed in the Sources Panel and Targets displayed in the Targets Panel. Additional information can be displayed in the Details Panel.

All traffic to and from a monitored host is considered for suspect or threat activity. The Sentriant NG appliance considers all network traffic it monitors to be a bidirectional communication stream. A single TCP session between two hosts is considered as a single distinct communication stream within the Sentriant NG appliance. If the source of the communication stream is suspect or deemed as threatening behavior based on configured rules, the source is considered a threat to the target and both are monitored via the Status Bar. Clicking on a source or target in the Status Bar will bring up the Sources or Targets Panel respectively.

The Sources Panel displays source IP Addresses along with additional information about the rule that was triggered, the type of IP Address and a date/time stamp when the communication stream was started. More detailed information can be accessed by activating the Details Panel. You may also access a list of targets, within the segment, with which the source has communicated.

**NOTE**

The Sources Panel shows information for only one segment. In some cases, a source may be contacting targets across multiple segments. The Details Panel provides a view of targets across all segments.

The Targets Panel displays target IP Addresses along with additional information along with the date/time stamp and the segment where the target resides. Additional information can be accessed by activating the Details Panel for targets. You may also access a list of sources that have communicated to the target and perform mitigation actions.

A Trend Chart provides visual representations of network traffic over time for each Segment Set and is broken down into each threat priority.

Using the Sources Panel

The **Sources Panel** displays a list of source IP Addresses that have triggered a threat. Choosing an individual source gives you the source's IP Address and MAC Address when placing the mouse over the source. Selecting the source displays a list of the IP Addresses for all of its targets in the Targets list on the right of the screen.

**NOTE**

To view source IP Addresses in the Sources Panel, MAC Validation must be turned on for the segment. Turning MAC Validation on validates the sources MAC address and retrieves the IP Address. If MAC Validation is turned off for the segment, the source IP Address and MAC address will not be displayed in the Sources Panel. The Sources Panel will show the source as masked.

The purpose of this panel is to provide detailed information on a source IP Address to determine the cause of threats. This is accomplished by the following:

- Integrating low-level information such as IP, Port, Packet, and Comm streams into the Detail Views
- Providing a cross-segment view of the threat source spanning all segments
- Providing an ease of use navigation to view detailed data efficiently

From the Sources Panel, you can:

- [View Source IP Addresses](#)
- [View Affected Targets](#)
- [View Source Details](#)
- [Query Sources](#)
- [Perform Mitigation Actions](#)

View Source IP Addresses

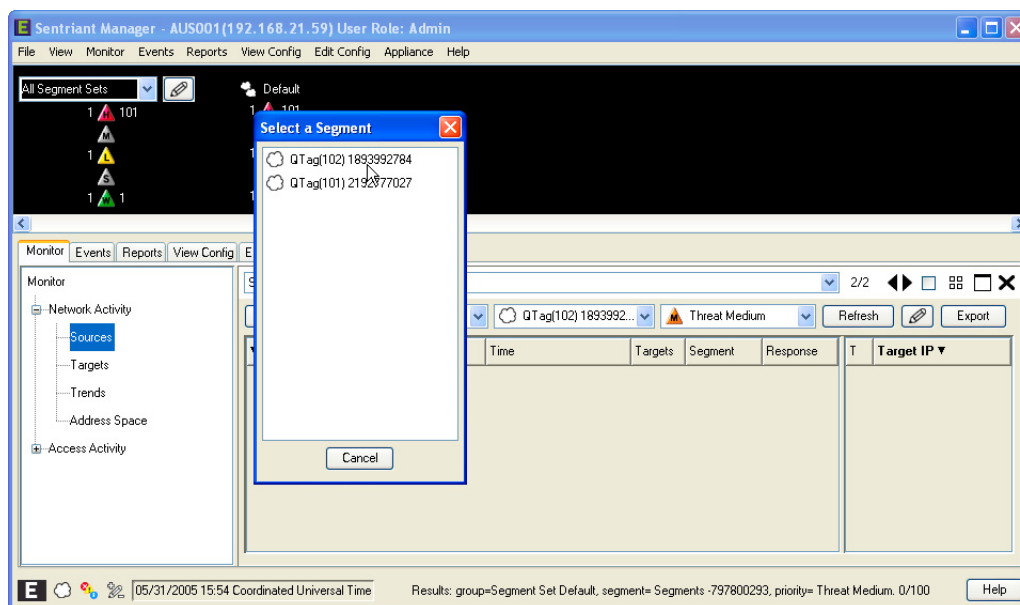
To display information about Source IP Addresses:

- 1 Select one of the Segment Sets displayed in the **Status Bar**.
- 2 Click on the **Segment Name** to display a list of active **Segments**.

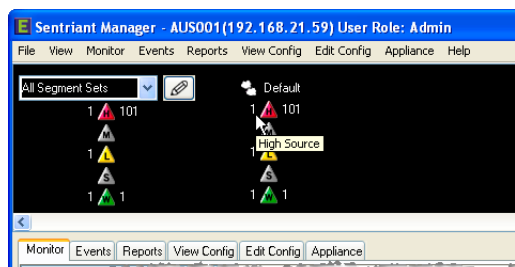
- 3 Select a **Segment** to display the traffic on the segment in the **Sources Information Panel**.

NOTE

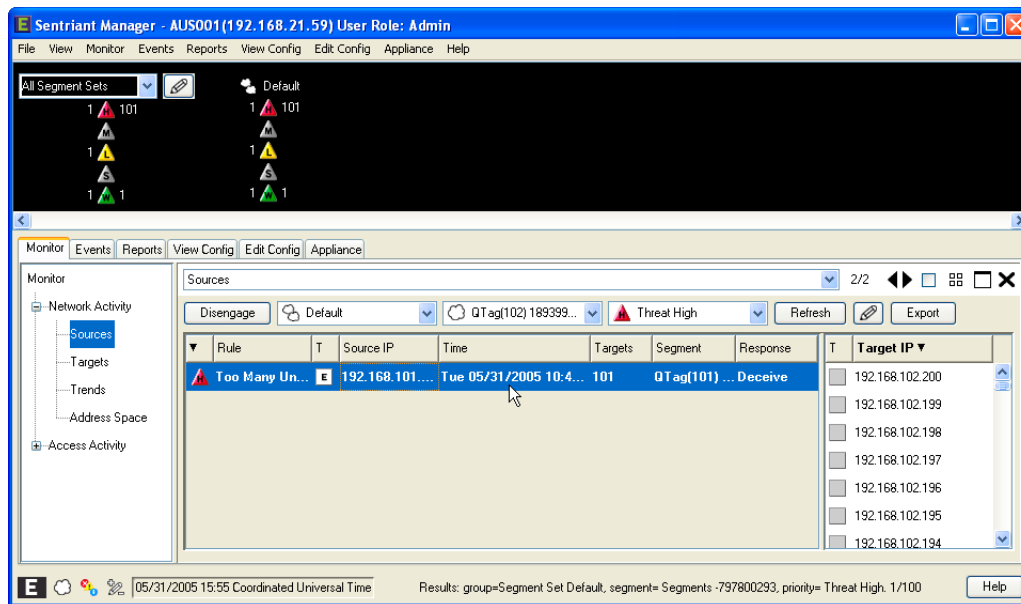
You may also use the Navigation Bar on the left of the screen by selecting Sources and using the Action Bar segment selectors.



- 4 To view only the Sources for a **Threat Priority**, click the **Threat Value** to the right of the threat.



For each **Source**, the following information is displayed:



- Priority level - Values are High, Medium, Low, Suspect or Watch (see “Status Bar” on page 23 for more information)
- Rule Name - The threat rule name that was triggered
- Source State - An icon representing the state or type of Source IP. The states of a source IP are:
 - ☐ Used - IP Address used by host within the protected range
 - ☒ Unused - IP Address within the protected range that is not used by a host
 - ☐ External - IP Address used by host external to the protected range
 - ☐ Unprotected - IP Address not in the protected range
 - ☐ All - All IP Addresses
- Source IP Address - **NOTE:** The MAC address can be viewed by placing the mouse cursor over the source



NOTE

To view source IP Addresses in the Sources Panel, MAC Validation must be turned on for the segment. Turning MAC Validation on validates the source's MAC address and retrieves the IP Address. If MAC Validation is turned off for the segment, the source IP Address and MAC address will not be displayed in the Sources Panel. The Sources Panel will show the source as masked.

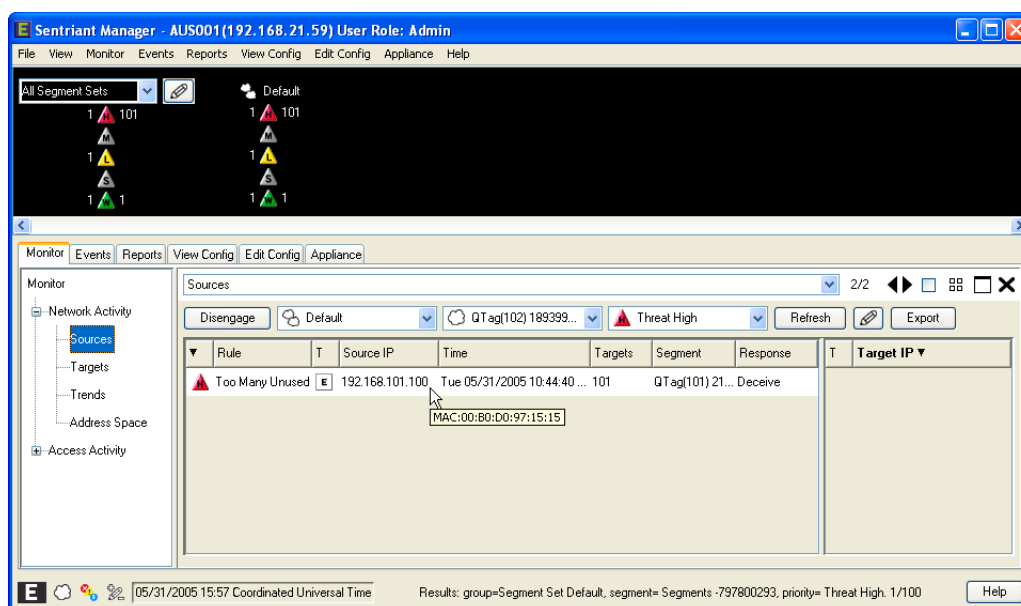
- Date and start time of the event
- Number of targets contacted
- The Network Segment of the IP Address
- Response currently in effect for the source. Response can be one of the following:
 - Cloak - Stops the communication stream to the external host effectively hiding targets from attacks

- Snare - Ties up an attack thread so it cannot move to another computer.
- Slow Scan - Increases the time it takes for an external host to scan the monitored network, causing the attacker to consume time and resources.
- Deceive - Misleads the external host by providing false data about a target
- Track - Monitors the external host but does not take action

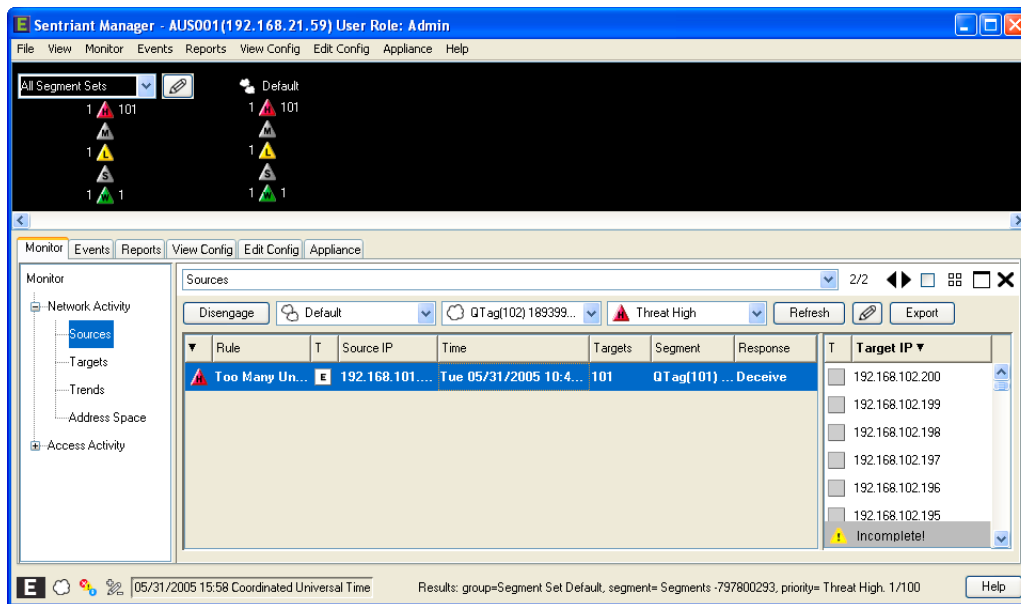
View Affected Targets

To view the IP Addresses of targets affected by the source:

- 1 From the Sources Panel, select the row of any **Source IP Address**.
- 2 Click on the Source.

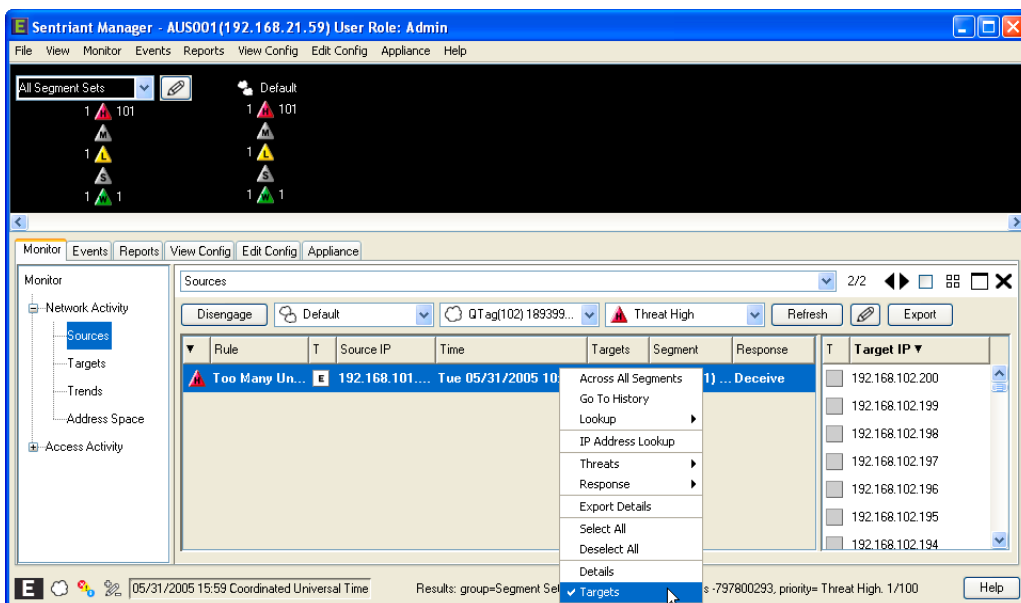


A list of Targets is shown in the Targets List on the right of the panel.

**NOTE**

An *Incomplete!* warning is displayed at the bottom of the Targets List if there are more than 3,500 Target IP Addresses and it may be necessary to use the Query function to view all Target IP Addresses in groups.

To hide the list of Targets, double-click on a Source and deselect Targets from the popup menu.



View Source Details

The Source Details views contain detailed source information to assist in processing source/target threat information. The Source Details views is grouped by the type of data displayed. The groups are:

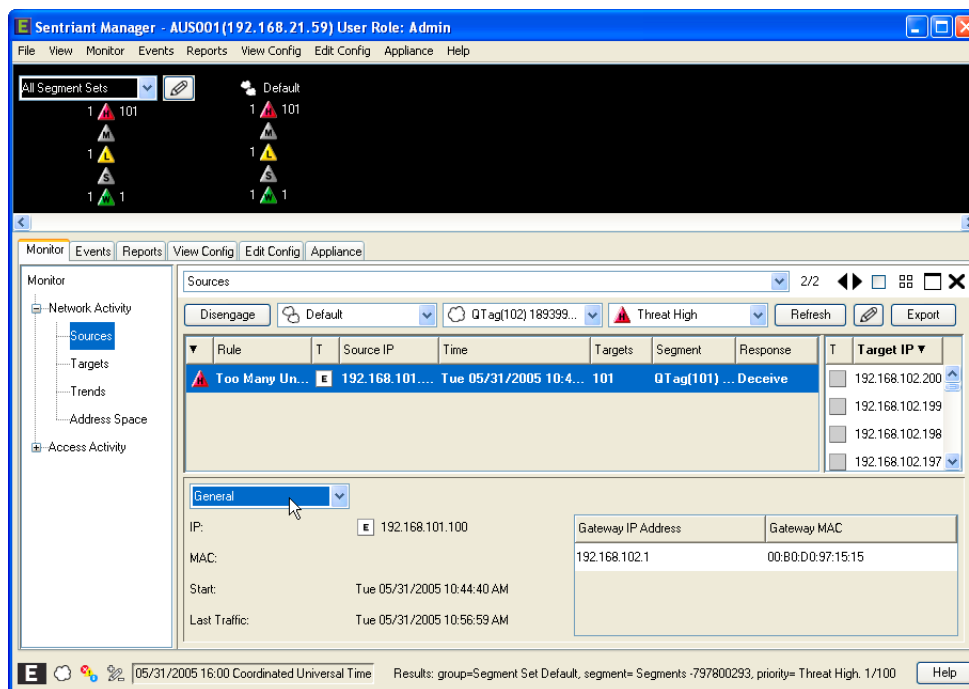
- **General** - High level source information including gateways, current and active target counts
- **IP** - Displays Spoofed As information for source IP Addresses
- **Port** - Displays Port information that sources and targets utilized
- **Packet** - Displays detailed packet information
- **Threats** - Displays all triggered rules
- **Responses** - Displays responses taken against a source threat
- **Across All Segments** - Displays a list of targets across all segments contacted by the source threat

General. The General view contains high-level information for a selected source. This information is:

- IP Address of the source
- MAC address of the source
- Start Activity - Time the source monitoring began
- Last Traffic - the last time the source communicated with a Target IP Address
- General Table - Displays the Gateway IP Addresses and MAC address where the source originated from if external or unprotected

To view a source's general information:

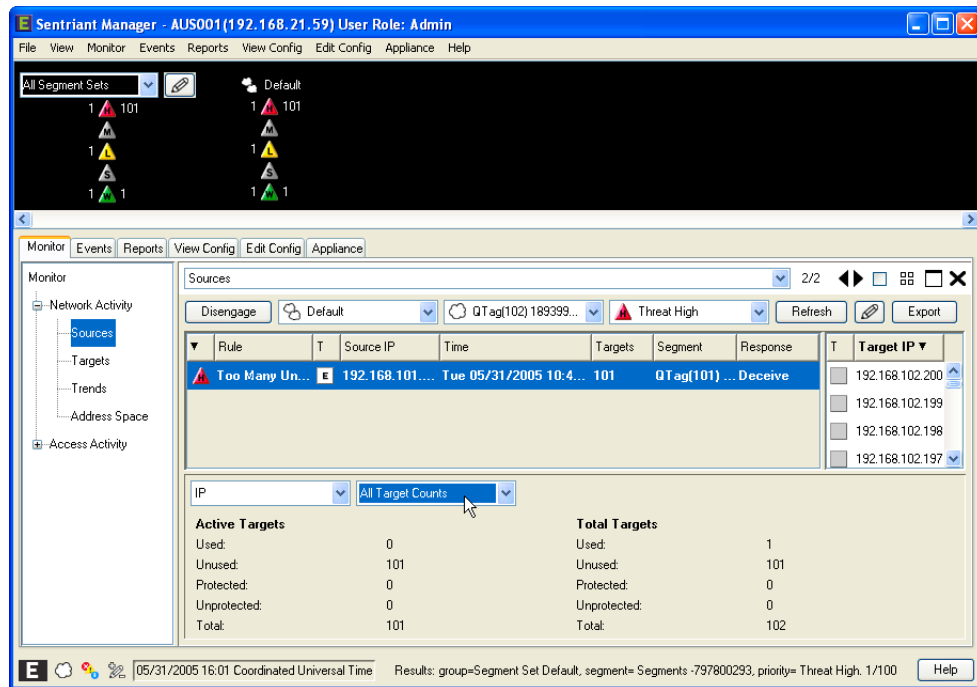
- 1 Select a source from the Source Panel. (The General Tab is default for the Details view)



IP. The IP view contains information specific to the number of active and total targets that the source has communicated with as well as if the source was a spoof IP Address and what IP Addresses were spoofed as and its origins.

To view a source's All Target Counts:

- 1 Select a source from the Source Panel.
- 2 Select IP from the Details view drop-down list. The first view that displays is All Targets Count.

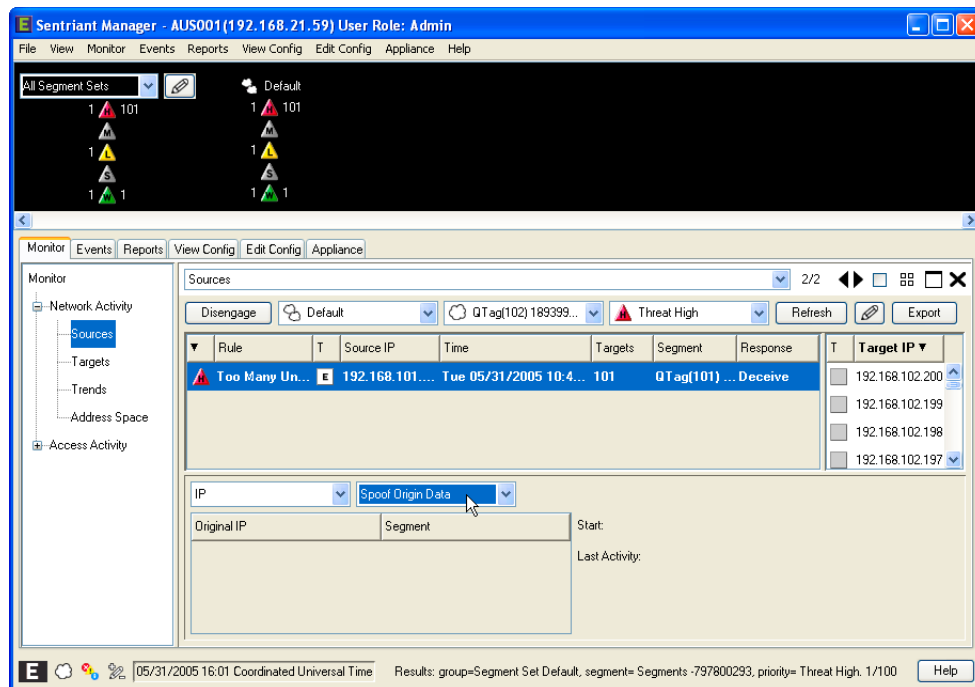


On the left side of the view is a list of all **Active Targets**. Active Targets are sources that are currently communicating with targets. Each type of target, used, unused, protected, and unprotected quantity is displayed along with a total of active targets.

On the right side of the view is the **Total Targets**. The total targets represents the total targets communicated with by the source since it was first identified.

To view a source's Spoof Origin Data:

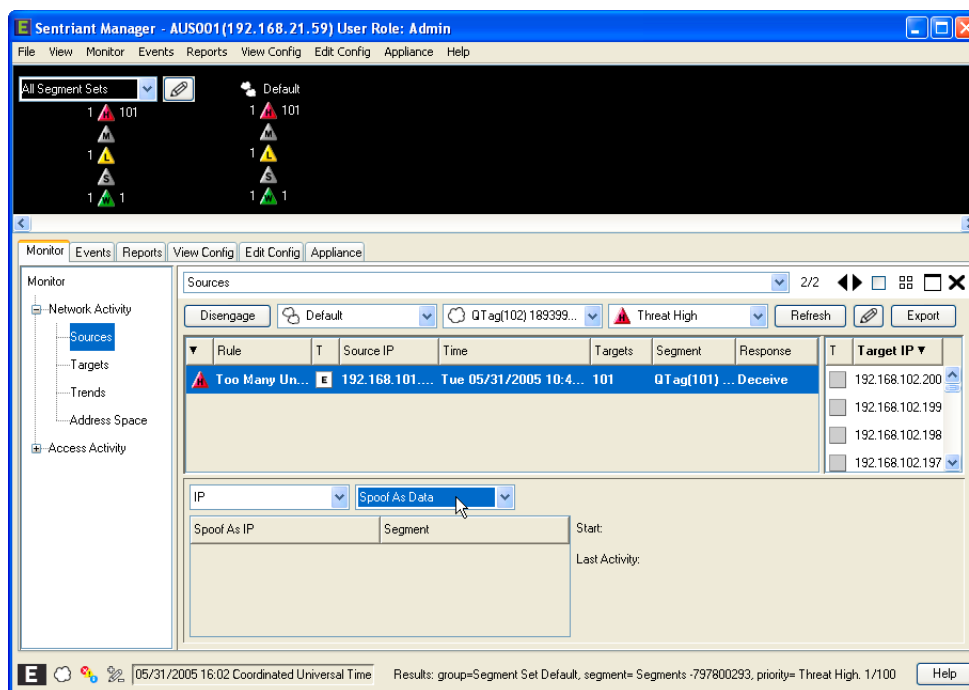
- 1 Select a source from the Source's Panel.
- 2 Select IP from the Details view drop-down list.
- 3 Select **Spoof Origin Data** from the IP drop-down list.
- 4 Select an **Original IP** from the list.



Spoofed IP Addresses' origins are displayed in the table along with the segment that was contacted. Selecting the spoofed IP Address will display the start day, date and time it first contacted a target and the last activity. One source IP Address may have many origins contacting across multiple groups and segments. Using this view, you can see where the spoofed IP Address has contacted targets.

To view a source's Spoof As Data:

- 1 Select a source from the Source's Panel.
- 2 Select **IP** from the Details view drop-down list.
- 3 Select **Spoof As Data** from the IP drop-down list.
- 4 Select a **Spoof As IP** from the list. Select a **Spoof As IP** from the list.

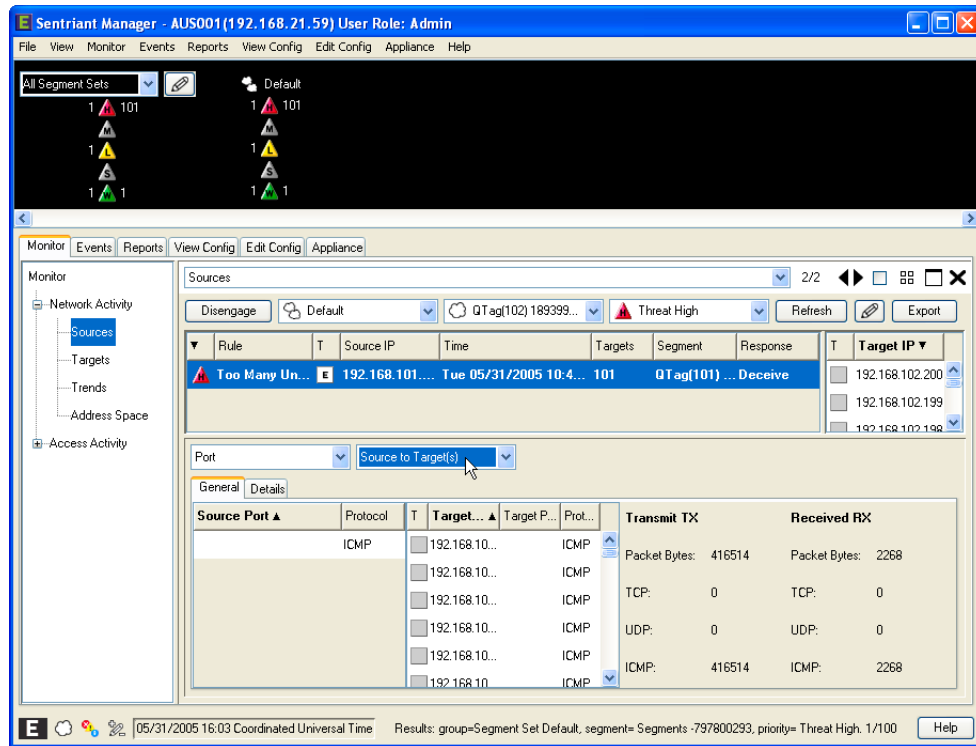


When an IP Address is spoofed, it may have multiple IP Addresses it spoofed as. For example, a source IP Address of 1.1.1.2 has spoofed IP Addresses of 2.2.2.1, 2.2.2.2, 2.2.2.3 and 2.2.2.4. By selecting Spoof As Data from the IP Details view, each spoofed as IP Address is displayed for that source IP Address along with the segment contacted. By selecting an IP Address from the Spoof As IP table will display the start day, date and time it first contacted a target and last activity.

Port. The Port view contains information specific to the number of ports and the type of port that the source has communicated with including total number of packets and bytes transmitted and received to the responding targets.

To view the Ports that a source communicated with:

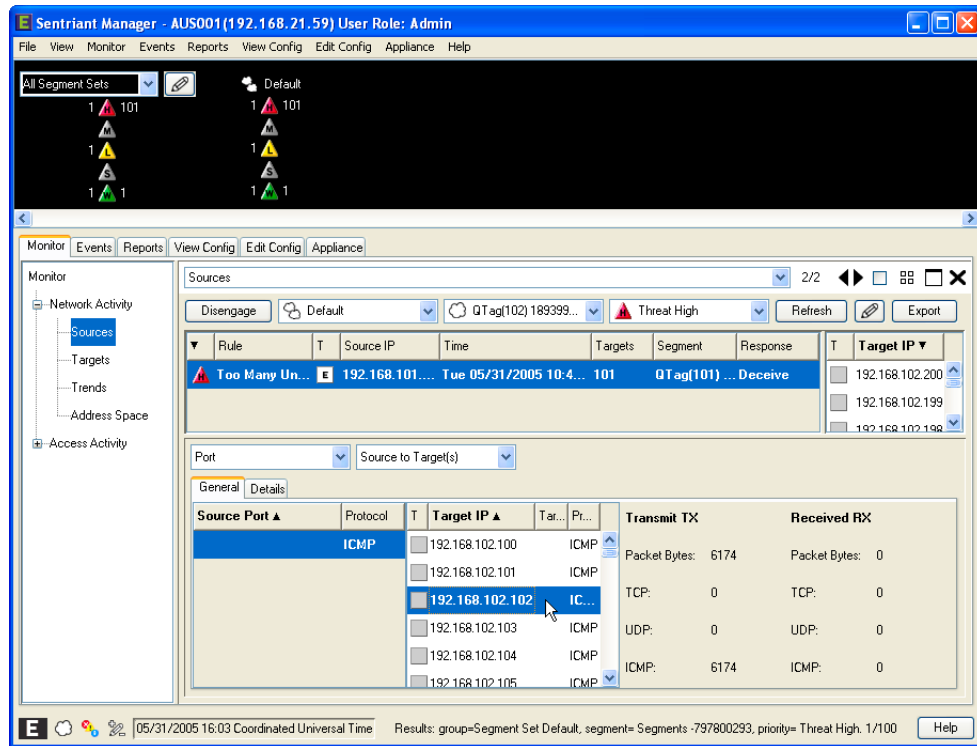
- 1 Select a source from the Source Panel.
- 2 Select Port from the Details drop-down list.
- 3 Select a source from the Source Panel.
- 4 Select **Port** from the Details drop-down list.



The port and the port's protocol type is displayed in the left-most table for the source IP Address. Selecting a Source Port displays the Packet Bytes transmitted and received. In addition, the bytes are broken down into the TCP, UDP and ICMP communication layers.

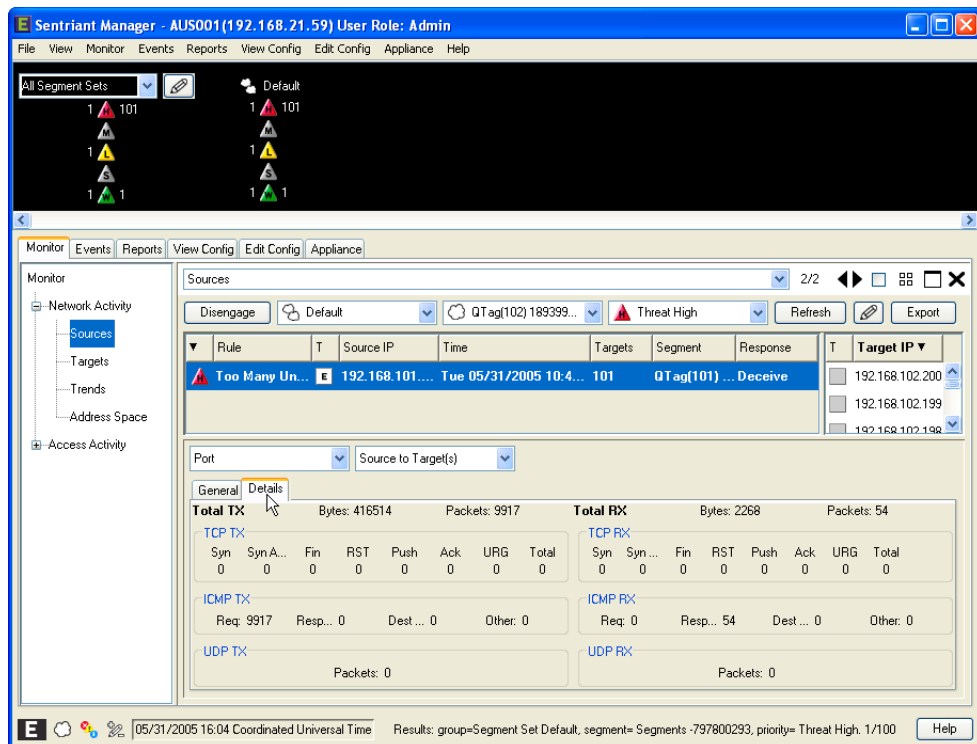
Selecting a row from the Source Ports table filters the target table.

Selecting a row from the Source Ports table, then selecting a row from the Target Ports table filters the TX and RX info.



To view Port Details:

- 1 Click the **Details** tab.

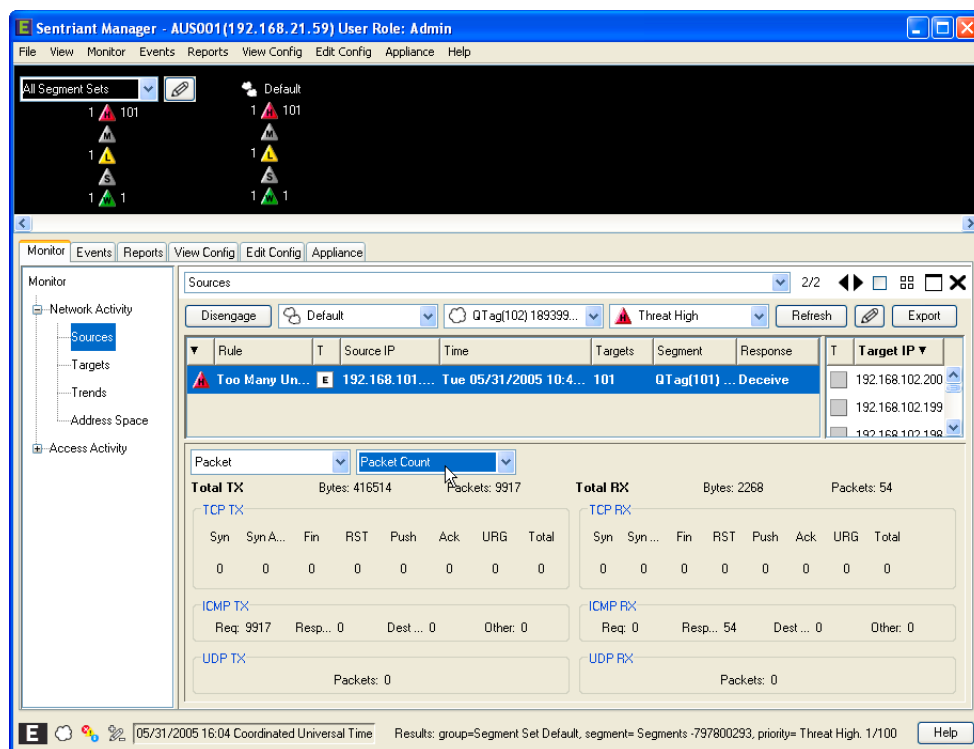


The traffic between the selected source and target are displayed showing the count of packet and bytes transmitted and received. In addition, the bytes are broken down into the TCP, ICMP and UDP communication layers.

Packet. The Packet view contains specific packet information for the selected Source IP Address. The total packet count for transmitted and received packet bytes is displayed and the packet count pair for each port type.

To view Packet Count:

- 1 Select a source from the Source Panel.
- 2 Select **Packet** from the Details view drop-down list. The first view that displays is Packet Count.



The information displayed is the count of how many packets were sent from that selected Source IP to the selected Target IP. The information is displayed showing each packet relative to the communication layer where it was sent and received.

Totals are displayed across the top of the view for the number of bytes and packets transmitted and received and UDP.

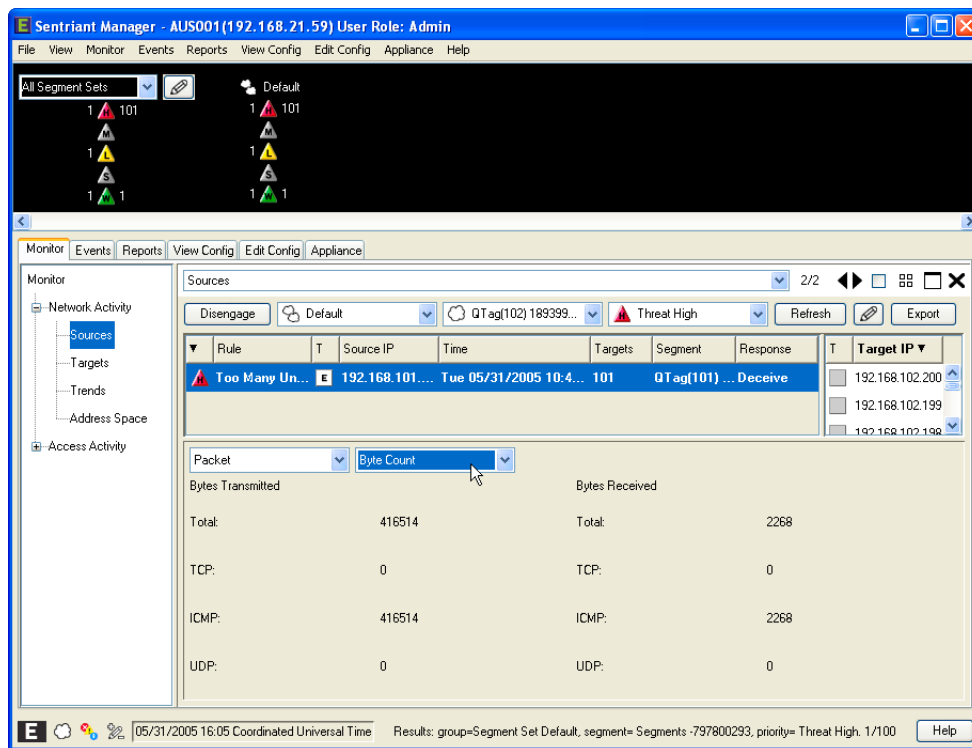
The second row of data shows the number of packets sent and received to the TCP header fields and a roll-up total for each.

The third row of data shows the number of packets sent and received to the ICMP layer for Requested, Response and Unread Destination packets and a roll-up total for each.

The last row of data shows the number of packets sent and received to the UDP header.

To view Byte Count:

- 1 Select a source from the Source Panel.
- 2 Select **Byte Count** from the Details view drop-down list.



The information displayed is the count of how many bytes were sent from that selected Source IP to the selected Target IP. The information is displayed showing each byte relative to the communication layer where it was sent and received.

Totals are displayed across the top of the panel view for the number of bytes transmitted and received.

The second row of data shows the number of bytes sent and received to the TCP header.

The third row of data shows the number of bytes sent and received to the ICMP header.

The bottom row of data shows the number of bytes sent and received to the UDP layer.

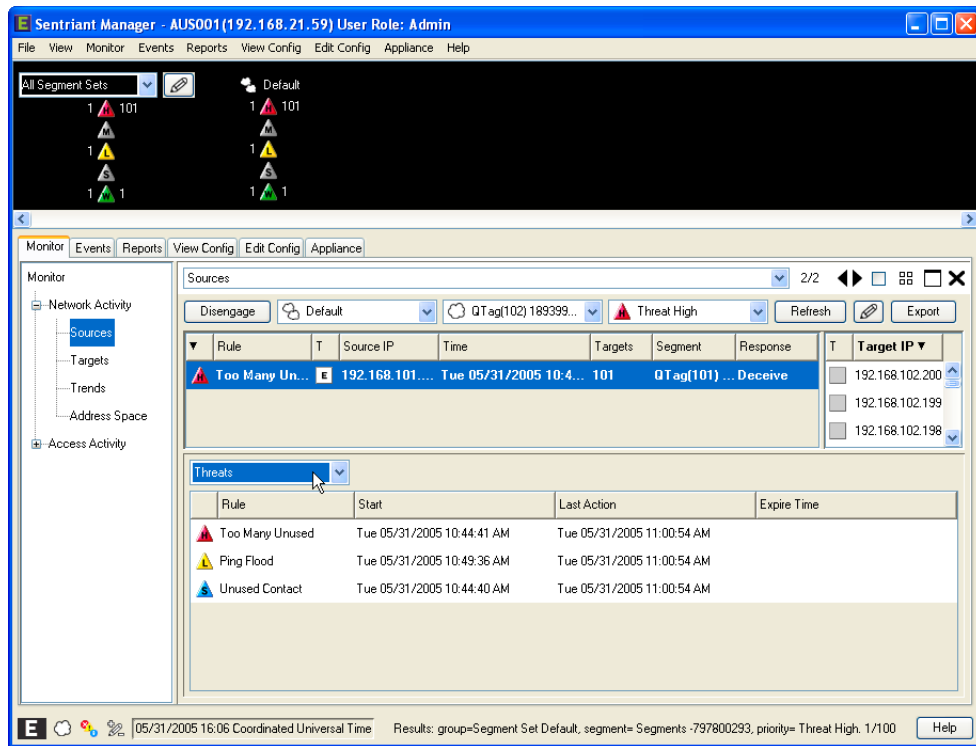
Threats. In the Sources Panel, a threat is displayed only once and is determined by the source that triggered the highest priority level. For example, a source triggers a medium threat and a high threat. The Source Panel will only display the highest threat priority level. The Threats Detail View displays all rules and threat type categories that have been triggered by the source.

The administrator has the choice of dismissing threats using two methods. The first is from the Sources Panel where when selecting a source and right-clicking **Threats > Dismiss**, all threats for the source are dismissed. The other method is from the Threats Detail Panel where the administrator can dismiss each threat singularly.

To view a source's threats:

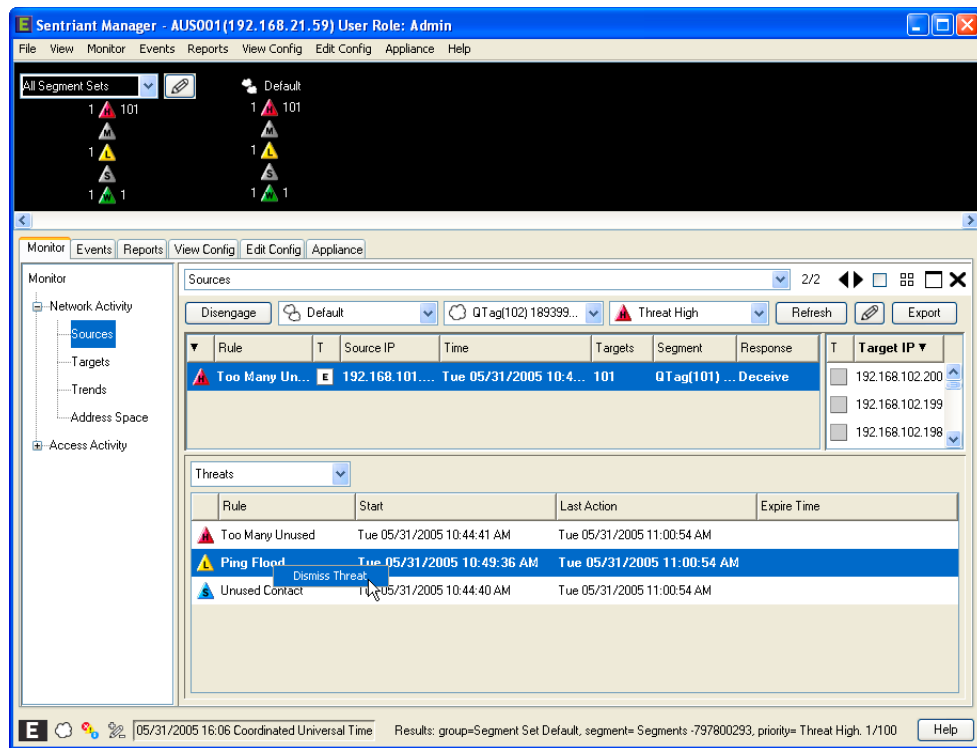
- 1 Select a source from the Source Panel.
- 2 Select **Threats** from the Details panel drop-down list.

All Threat Priorities, High, Medium, Low, and Suspect are displayed for the selected source.



To dismiss a threat from the Threats Detail Panel:

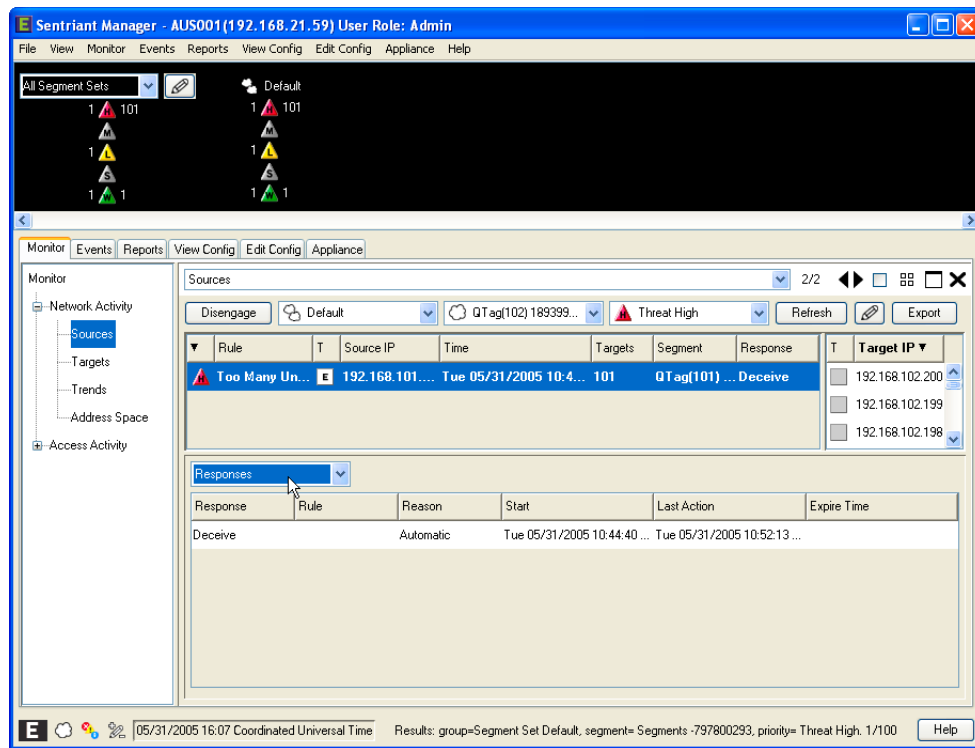
- 1 Select a threat from the list in the Threats Detail Panel.
- 2 Right-click and select **Dismiss Threat**.



Responses. This view displays the type of responses to known source threats that have triggered a rule. For example, a Too Many Unused rule was triggered. The response for this type of rule was set to Cloak the source threat.

To view the responses to source threats:

- 1 Select a source from the Source Panel.
- 2 Select **Responses** from the Details view drop-down list.

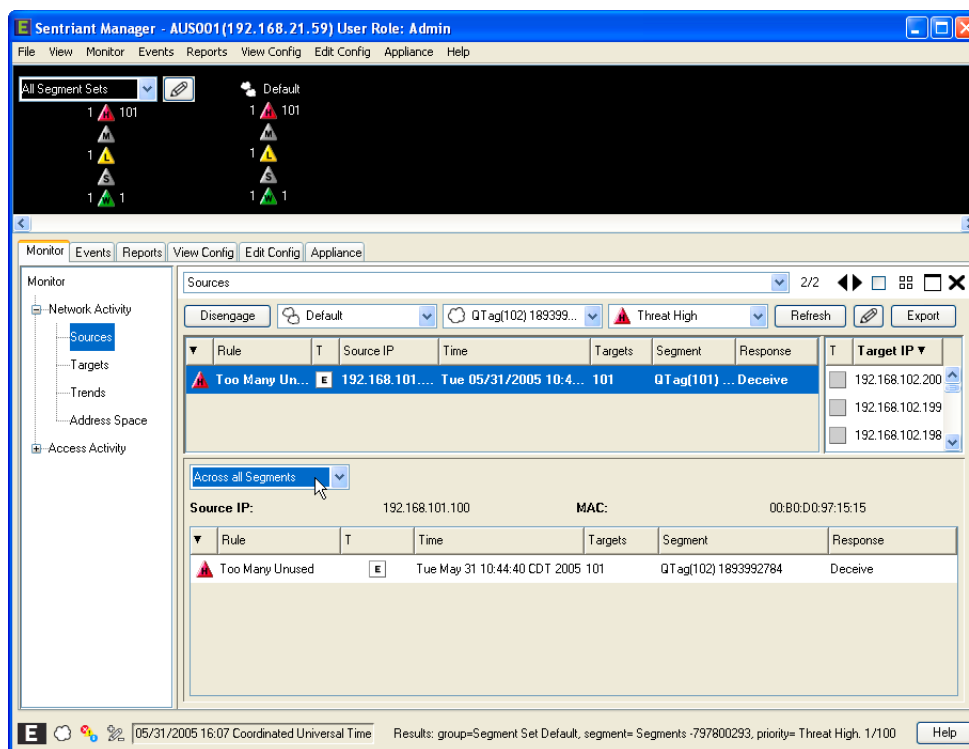


The Details view displays the type of response, the rule that triggered, how the rule was triggered (that is, automatically), when the response was started, the date and time the last action was taken against the threat and the remaining date and time a triggered rule stays active.

Across all Segments. This view displays sources affecting all configured network segments being monitored within the Sentriant NG appliance. The user will be able to see the sources impact across all other segments by selecting a source from the Source Panel.

To view a source across all segments:

- 1 Select a source from the Source Panel.
- 2 Select **Across all Segments** from the Details view drop-down list.



The Details view displays the source IP and MAC address. The table is populated with rules that have been triggered, the time the rule triggered, number of targets, the segments containing targets and the response.

Source Actions

The following actions can be performed within the Sources panel. From the Action Bar, you can:

- [Engage and Disengage](#) a segment
- [Query](#) segment details

A right-click pop up menu contains the following:

- [Across All Segments](#) - Opens the Details view with source information spanning across all segments
- [History](#) - Opens the Events Viewer Panel with history for the selected source
- [Lookup IP Address on the Web](#) - Opens a web browser to the various IP lookup providers
- [IP Address Lookup](#) - A tool that returns the host name and IP Address of a source using the client's DNS
- [Threat - Escalate and Dismiss](#) - Manually escalate or dismiss a suspect to a threat
- [Response - Cloak or Uncloak](#) - Cloaks or Uncloaks a source from the communication paths to protected targets
- [Select/Deselect All](#) - Selects/Deselects All source IP Addresses in the source workspace

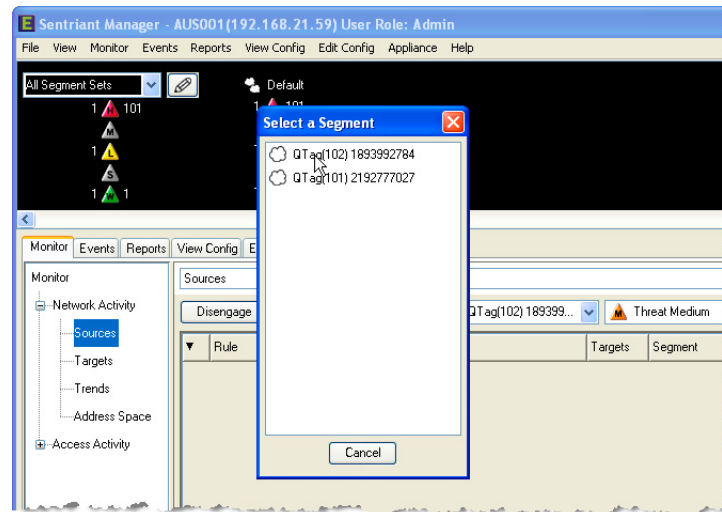
Disengage and Engage. Upon configuration of a group and segments, the Sentriant NG appliance is engaged and monitoring all traffic within the protected segment ranges IP Addresses. In some circumstances it may become necessary to stop monitoring or disengage from a specific segment

without completely shutting down the Sentriant NG appliance. For example, network reconfiguration. The administrator can quickly suspend all monitoring and policy enforcement on individual segments and maintain monitoring and mitigation on other configured segments.

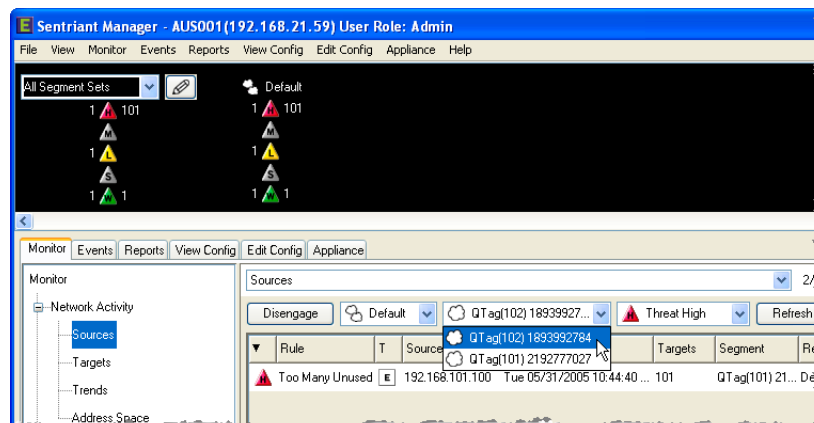
The Sentriant NG appliance defense mechanisms remain disengaged until the administrator clicks the **Engage** button, clicks the **Block** button, or reboots the system. While disengaged, the Sentriant NG appliance will not generate any traffic on the selected segment.

To disengage a segment:

- 1 Select a Segment using the Status Bar by clicking on a Segment Set and then selecting a Segment.

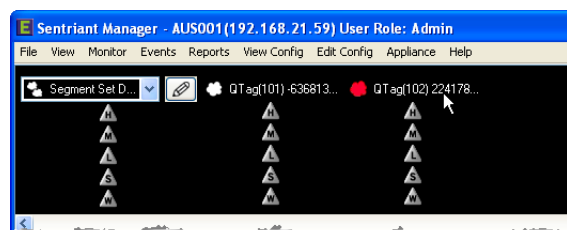


- 2 Select a segment using the Action Bar selectors.



- 3 Click the **Disengage** button.
- 4 Click **Yes** to disengage the segment.

The segment is now disengaged and the icon in the status bar changes from white to red.



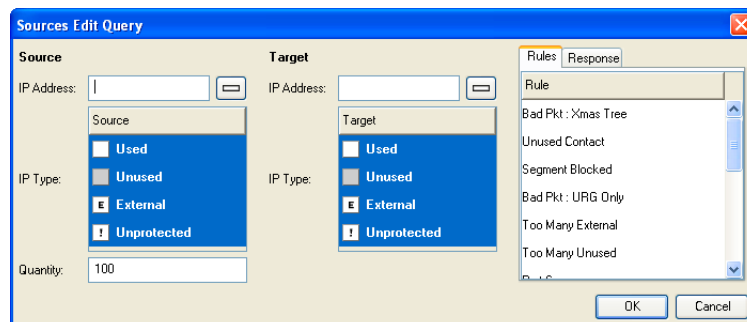
To Engage a segment:

- 1 Select the segment that you wish to engage from the Status Bar or using the Action Bar selectors.
- 2 Click the **Engage** button.
- 3 Click **Yes** to engage the segment.

Querying Sources.

To perform a query in the Sources Panel:

- 1 From the Sources Panel, click the **Edit Query** button to open the Sources Edit Query dialog.



- 2 Select parameters for the query. The **Sources Edit Query** dialog contains fields for querying on **Source**, **Target**, **Rules**, and **Response** attributes. The attributes for each field are:

Source:

- IP Address - A single or range of IP Addresses can be entered. If no IP Address is entered all IP Addresses will be returned.
- IP Type Status - Select an IP Type from the list. Options are Used, Unused, External, and Unprotected.
- Quantity - Enter a number for the maximum number of IP Addresses to be returned. One (1) to a thousand (1000) may be entered.

Target:

- IP Address - A single or range of IP Addresses that the source must target in order to include this source in the query list. If no IP Address is entered all IP Addresses will be returned.
- IP Type - Select an IP Type from the list. Options are Used, Unused, External, and Unprotected.

Rules:

- Rule Type - Select the rule from the list.

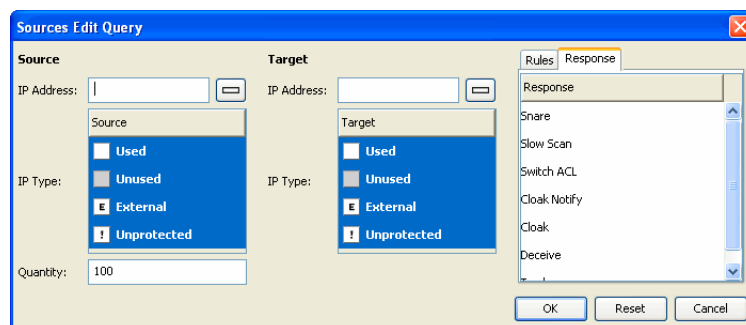


NOTE

In the Rule Type list is a pick called Segment Block which is not a rule but a query filter used to view IP Addresses of a segment which has been blocked.

Response:

- Click the Response Tab and select the Response Type from the drop-down list. Options are Cloak, Deceive, Snare, Slow Scan, and Track.



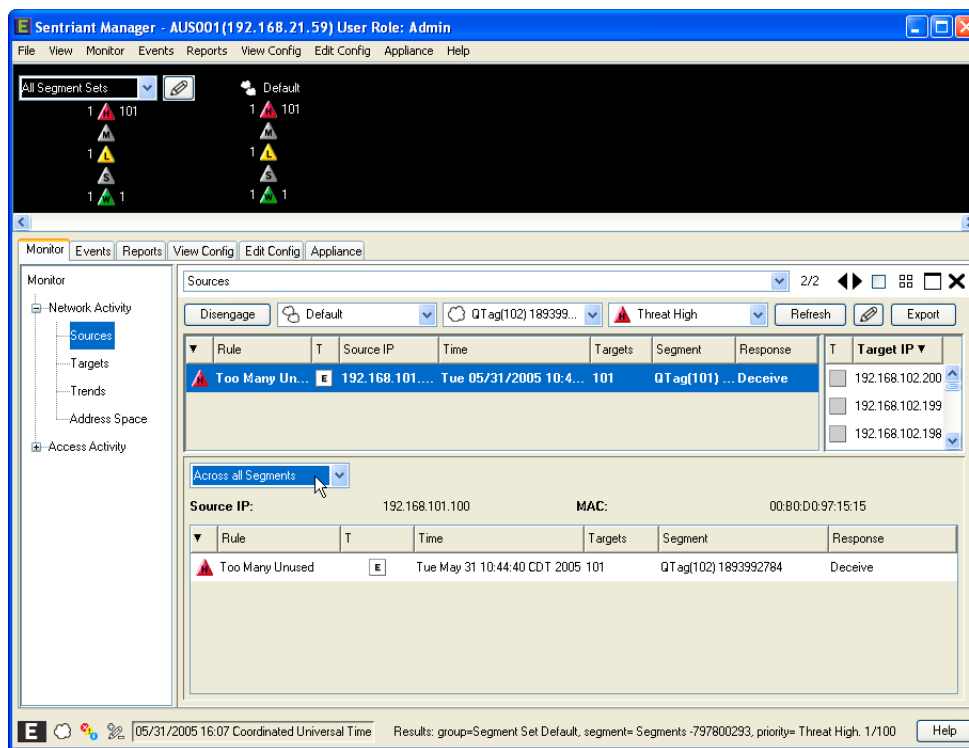
- 3 Click **OK** to return to the Sources Panel.
- 4 Click **Refresh** to run the query and display the results.

Across All Segments Action. This view displays sources affecting all configured network segments being monitored within the Sentiang NG appliance. The user will be able to see the sources impact across all other segments by selecting a source from the Sources Panel.

To view a source across all segments:

- 1 Right-click a source.
- 2 Select **Across all Segments** from the pop-up menu.

The Details view displays the source's IP and MAC Address. The table is populated with rules that have been triggered, the time the rule triggered, number of targets, the segments containing targets and the response.



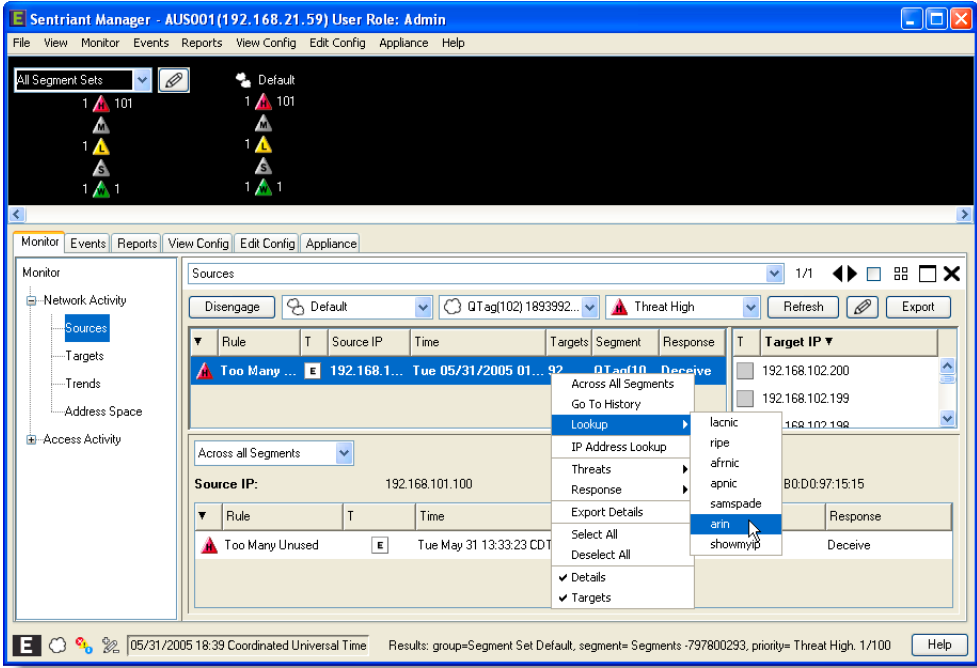
Look up an IP Address on the Web. It may become necessary to look up the location of an IP Address to understand where it is coming from. Sentiari NG Manager's Lookup IP Address on the web tool contains all of the regional internet registry services. The Internet Registry services are:

- APNIC represents the Asia Pacific region, comprising 62 economies
- AfriNIC represents the African community
- ARIN represents the American Registry for Internet Numbers managing the Internet numbering resources for North America, a portion of the Caribbean, and subequatorial Africa
- RIPE represents a membership base of around 3,500 members. The RIPE NCC service region consists of more than 90 countries across Europe, the Middle East, Central Asia and African countries located north of the equator
- LACNIC represents the Latin American and Caribbean Internet Addresses Registry, is the organization that administrates IP Addresses space, Autonomous System Numbers (ASN), reverse resolution and other resources of the Latin American and Caribbean region (LAC), on behalf of the Internet community.

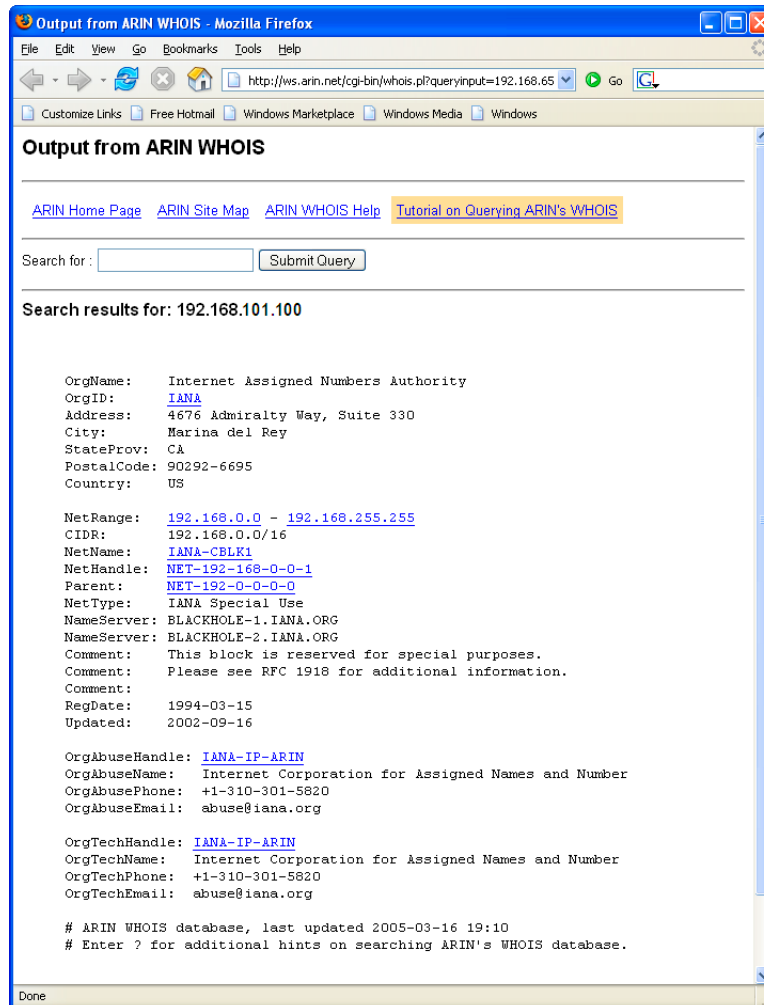
The tool will direct you to the correct internet page and start the search of the IP Addresses location.

To look up an IP Address on the web:

- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Lookup** and then one of the registry services from the list.



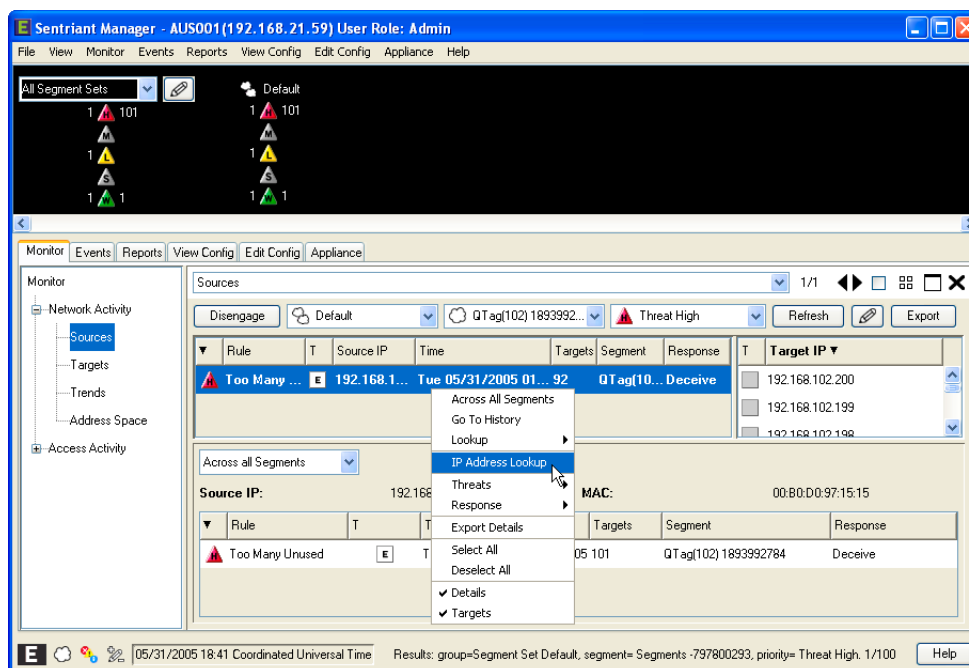
The selected IP Address is populated in the 'who is' section of the registry service. Search results are displayed for the selected IP Address. Each registry service displays results differently so review carefully.



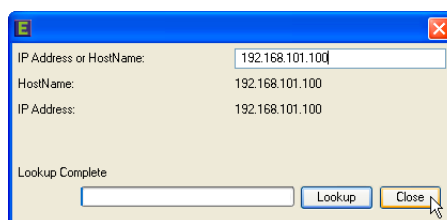
Look up a Source IP Address. The IP Address Lookup tool will display the IP Address of a source and the HostName returned by the client's DNS.

To look up a source's IP Address and HostName:

- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **IP Lookup**.



The HostName is displayed along with the IP Address. You may enter another IP Address or HostName in the IP Address or HostName field and click the Lookup button.



Threat - Escalate and Dismiss. Threat hosts listed in the Sources Panel can be escalated or dismissed manually. For example, an external source is slow scanning a protected range but has not triggered a rule, however the source has a watch priority. You may escalate the watch priority to a higher priority by assigning a rule to the source. You may also escalate a lower priority threat to a higher one shown in the table below:

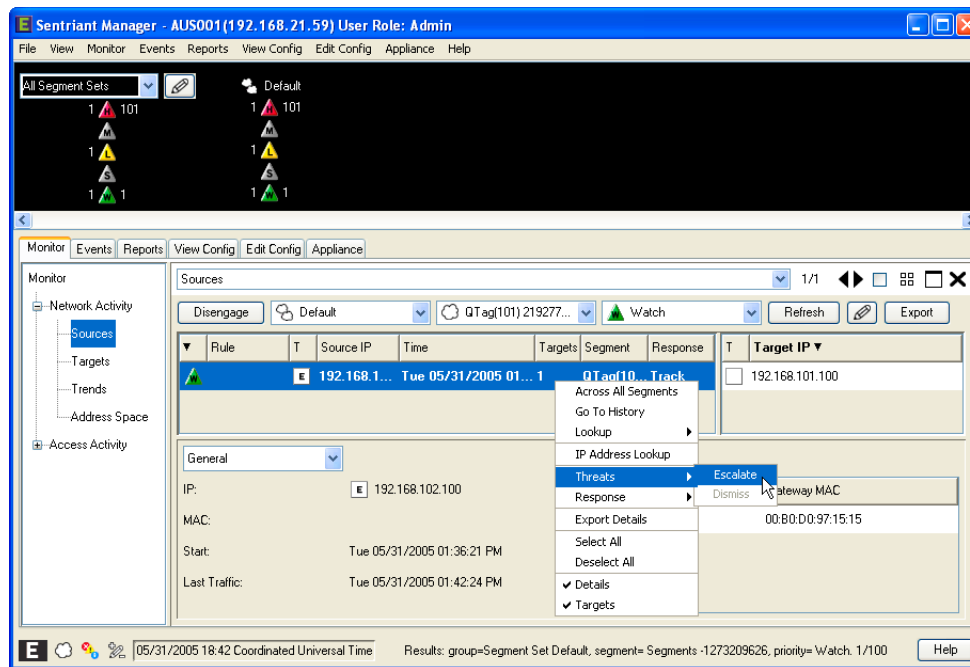
Table 1: Threat Escalation

Current Priority	Escalate Priority To:
watch	suspect, low, medium, high
suspect	low, medium, high
low	medium, high
medium	high

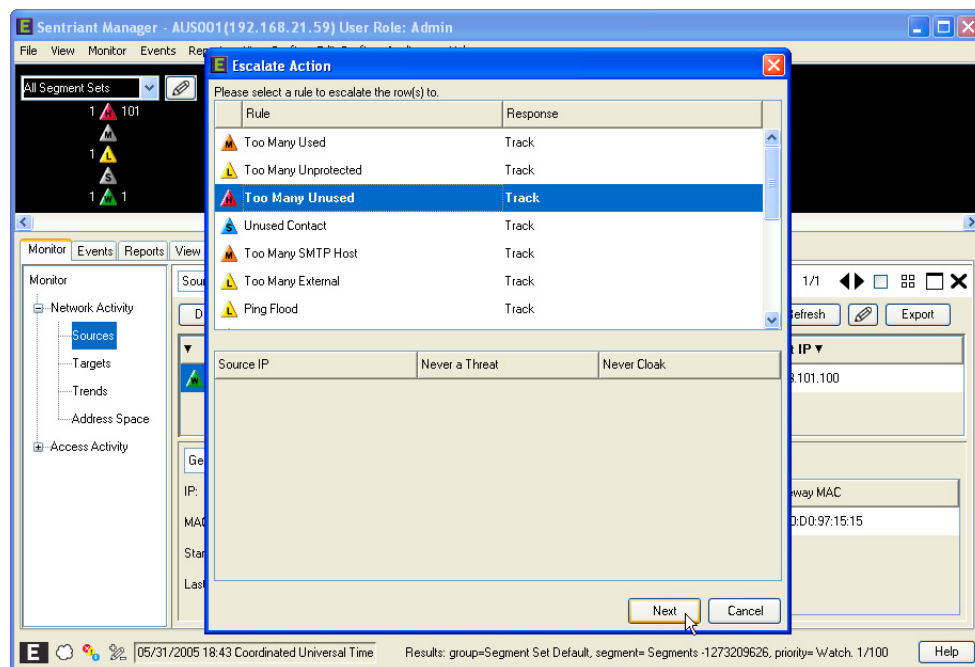
Threats may also be dismissed if it is determined that the source is not a threat. Threat hosts that are dismissed are given a watch priority.

To escalate a watch:

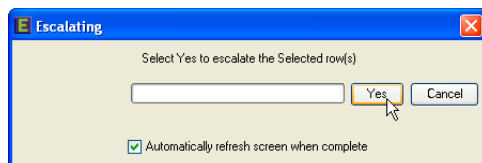
- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Escalate** from **Threats**.



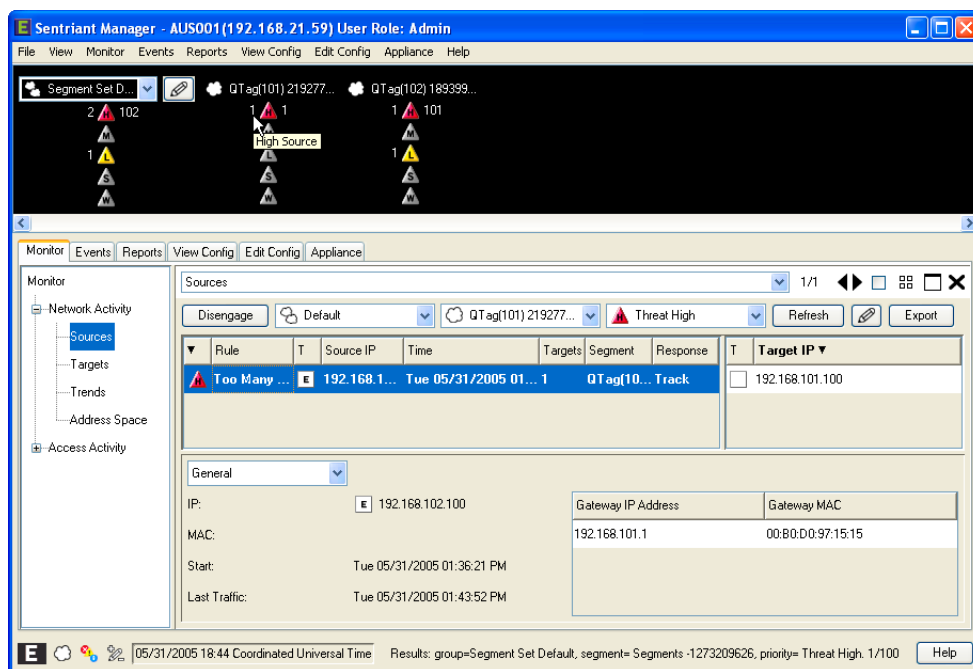
- 4 Select a rule from the Escalate Watch(s) Action table to apply to the source.
- 5 Click **Next**.



6 Click **Yes**.

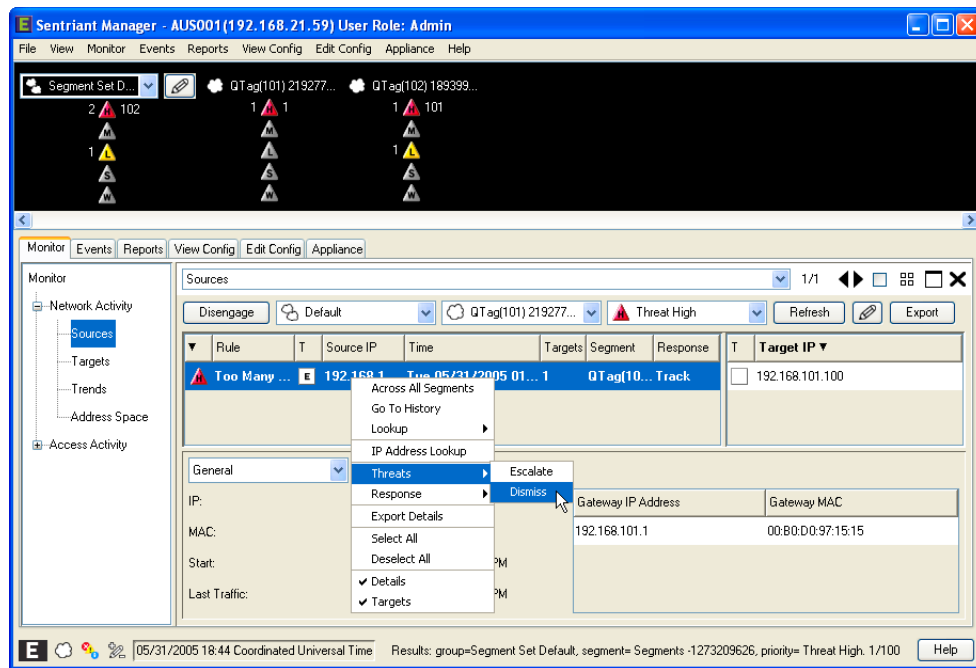


The source is escalated to the priority level set by the rule.

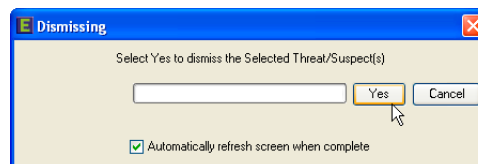


To dismiss a threat:

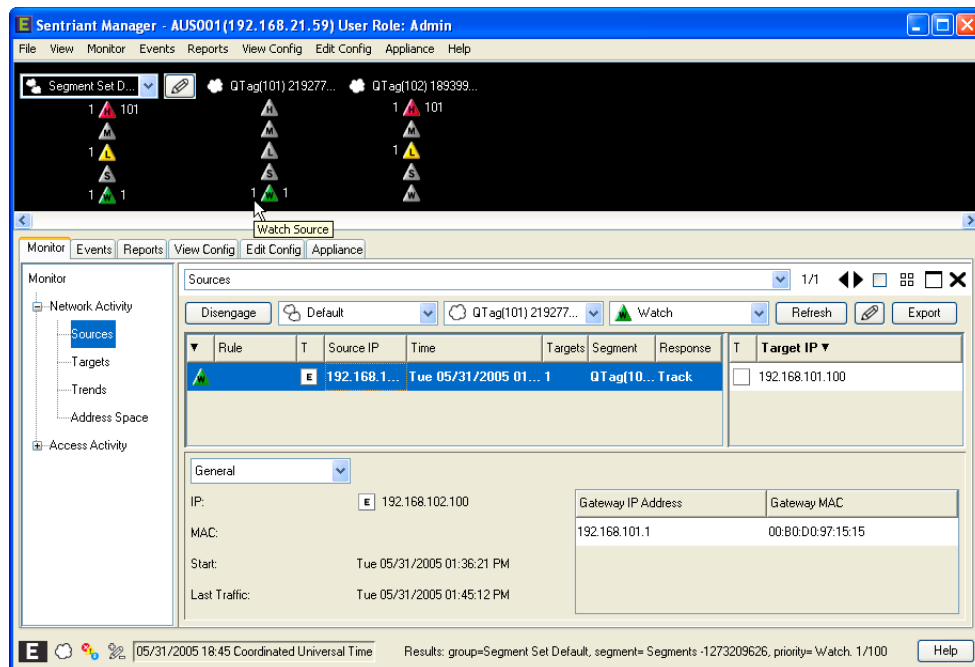
- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Dismiss** from **Threats**.



- Click **Yes** to dismiss the source as a threat. (This sets the priority to Watch.)



- Click **Close**.
The threat is set to Watch priority.



Response - Cloak and Uncloak. When Cloak is selected as the response to a threat, the Sentriant NG appliance initially inserts itself into communication paths for only the devices that have communicated with the threat. The Sentriant NG appliance also inserts itself into all new communication paths as they occur. At the point in which the Sentriant NG appliance has inserted itself into the communication path, all traffic to/from the threat source will be surgically removed. Traffic to/from other (non-threat) hosts will be permitted. Once it is determined that the threat source is no longer a threat it can be uncloaked so that communication is permitted within the Sentriant NG appliance's protected segments.



NOTE

The cloak will remain active until active traffic stops being generated from the selected source.

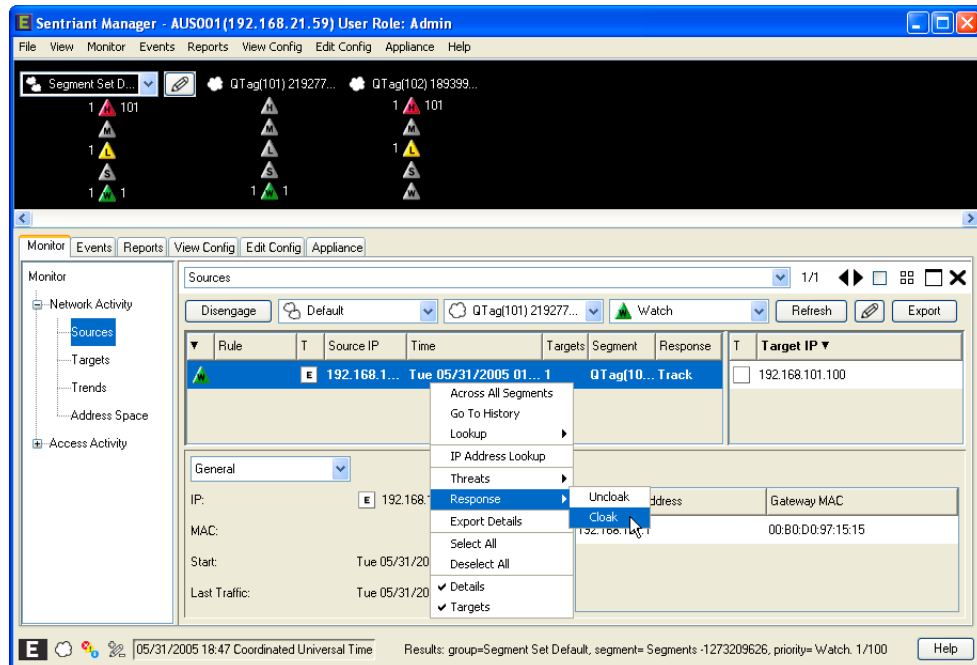


NOTE

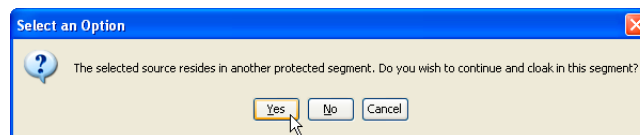
Cloaking a switch is not allowed. If a switch is inadvertently selected, a warning dialog will be displayed.

To cloak a source:

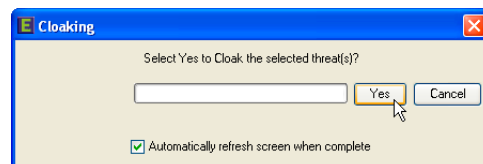
- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Cloak** from **Response**.



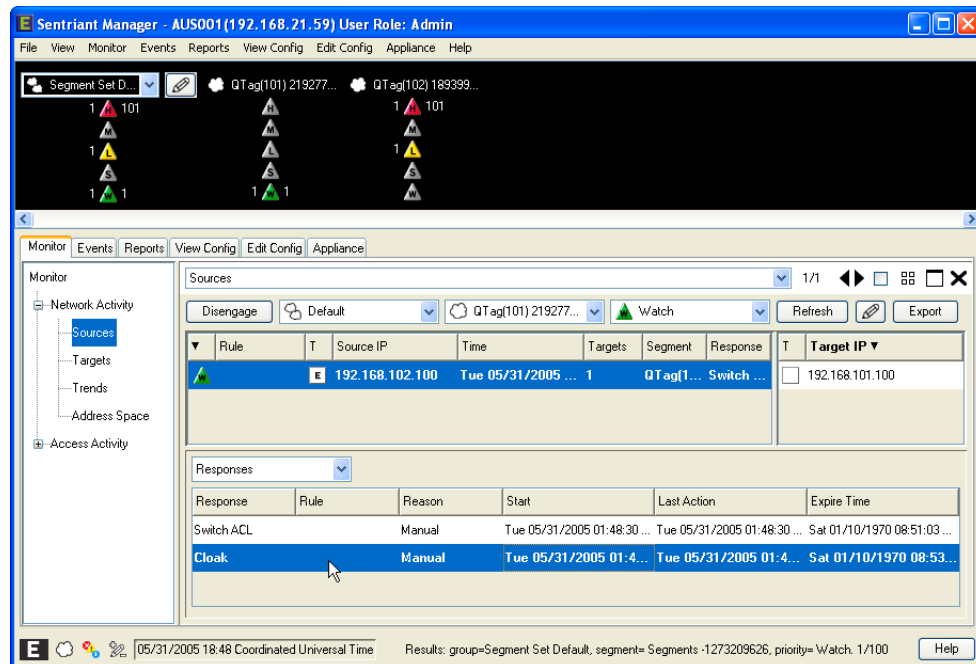
4 Click **Yes** to cloak the source.



5 Click **Close** to close the dialog.

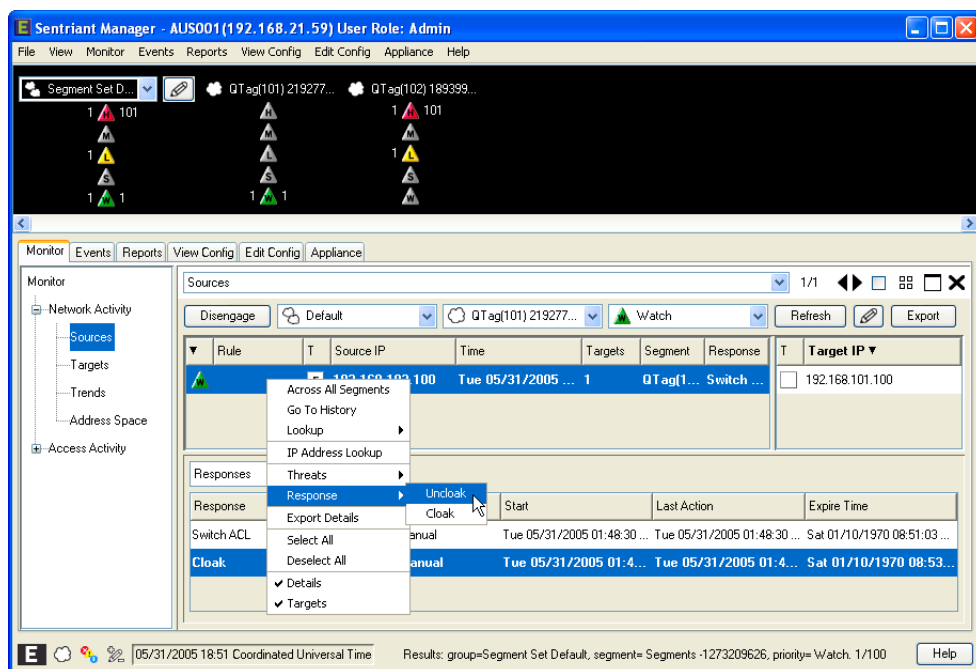


To verify that the source was cloaked, from the **Details Panel** select **Responses**. You should see a response for Cloak in the list.

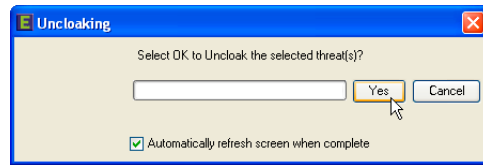


To uncloak a cloaked source:

- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Uncloak** from **Response**.



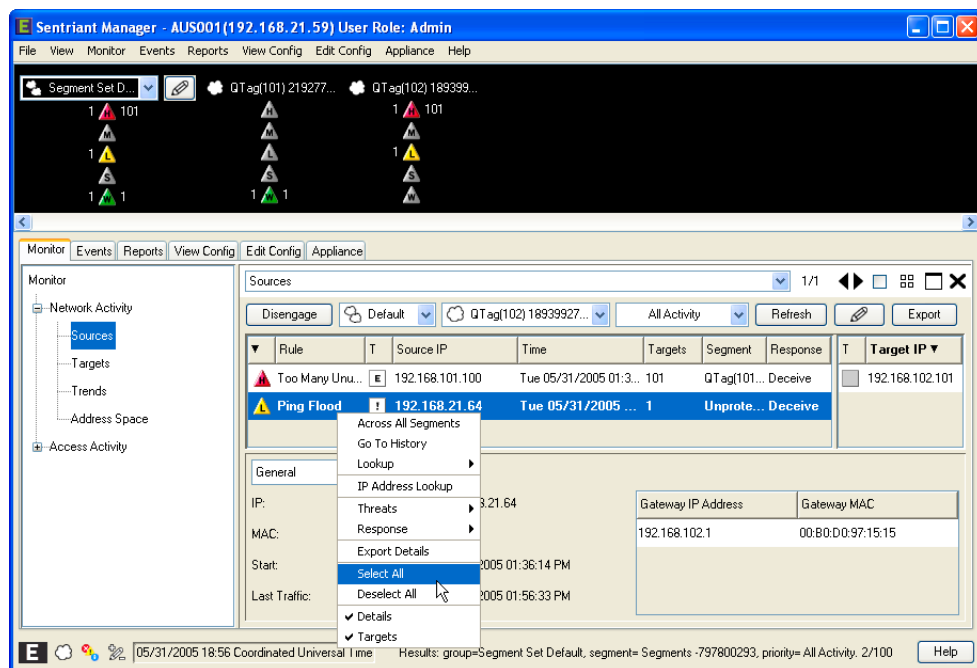
- 4 Click **Yes** to uncloak the source.



Selecting and Deselecting Sources.

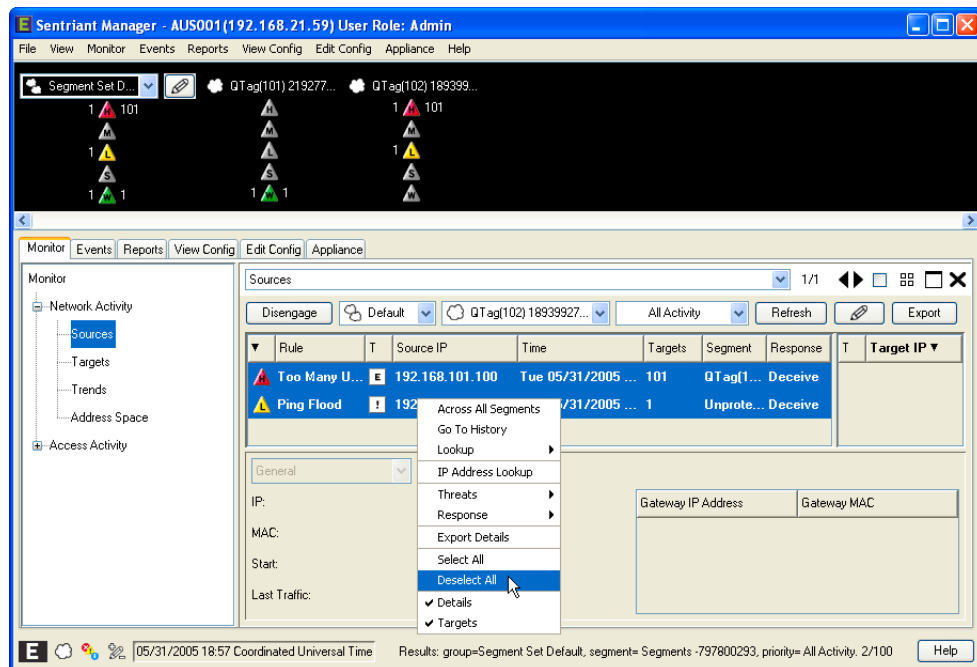
To select all sources in the Sources Panel:

- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Choose **Select All**.



To deselect sources in the Sources Panel:

- 1 Right-click in the sources panel to bring up the pop-up menu.
- 2 Select **Deselect All**.



Using the Targets Panel

The **Targets Panel** displays a list of IP Addresses targeted by traffic for a segment. Choosing an individual target IP Address displays its information including a list of the source IP Addresses that has made contact with the target. The purpose of this panel is to provide information to help the user determine the threat source and appropriate mitigation action.

From the Targets Panel, you can:

- [View Target IP Addresses](#)
- [View Target Details](#)
- [View Source IP List](#)
- [Query Targets](#)
- [Look up Target IP Address](#)

Viewing Target IP Addresses

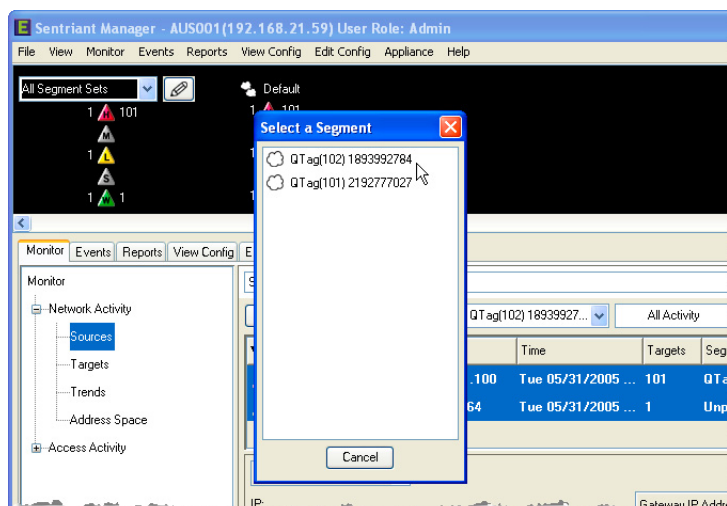
The Targets Panel provides a list of Target IP Addresses for a selected network segment. Selecting an individual target provides additional details, including a list of the IP Addresses of all of its sources.

To display information about Target IP Addresses:

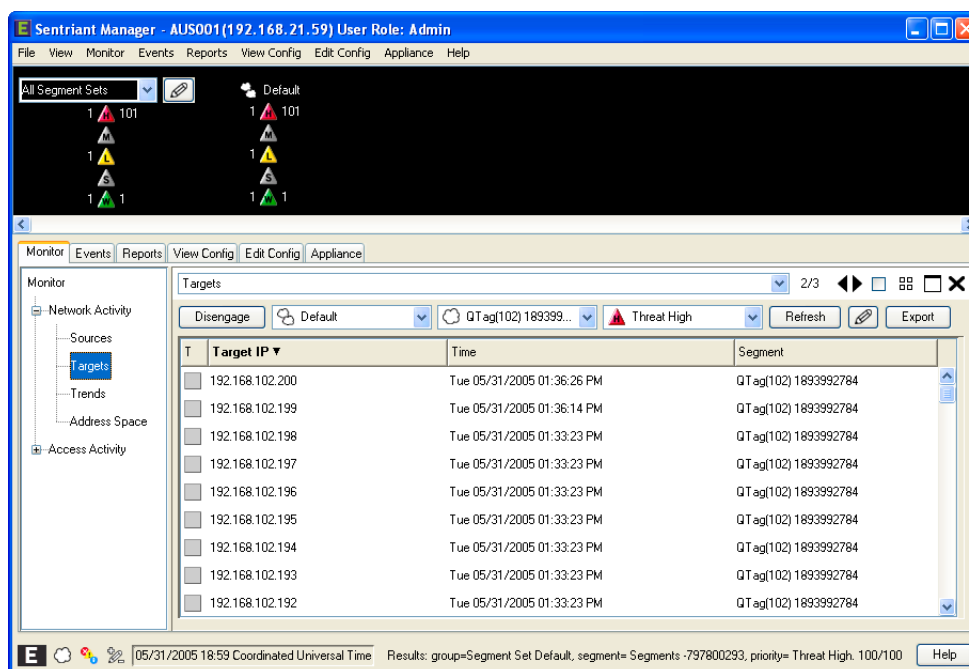
- 1 From the Monitor Panel, select Target from Network Activity, or...
- 2 From the **Status Bar** click a Target from the priority list. This will display all targets for that segment.

**NOTE**

A target is displayed only once and is determined by the source that triggered the highest priority level. For example, a source triggers a medium threat and a high threat. The Source Panel will only display the highest threat priority level for that target.



For each Target, the following information is displayed:



- Source State - An icon representing the state or type of Source IP. The states of a source IP are:
 - ☐ Used - IP Address used by host within the protected range
 - ☒ Unused - IP Address within the protected range that is not used by a host

- ☐ External - IP Address used by host external to the protected range
- ☐ Unprotected - IP Address not in the protected range
- ☐ All - All IP Addresses

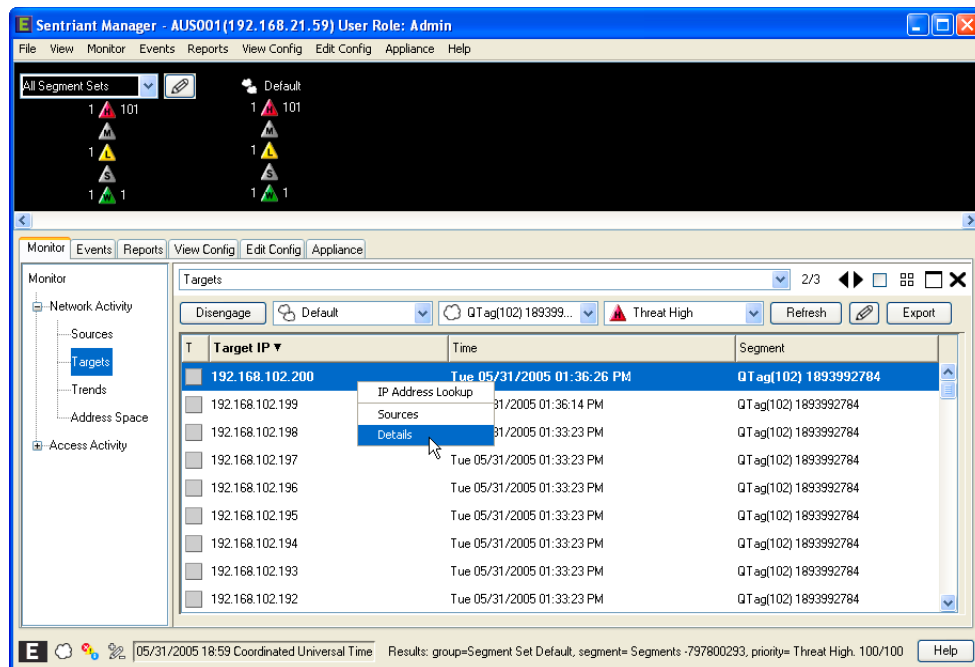
- Target IP Address
- Date and time the target was communicated to by a source
- The network segment name where the target resides

Targets Details

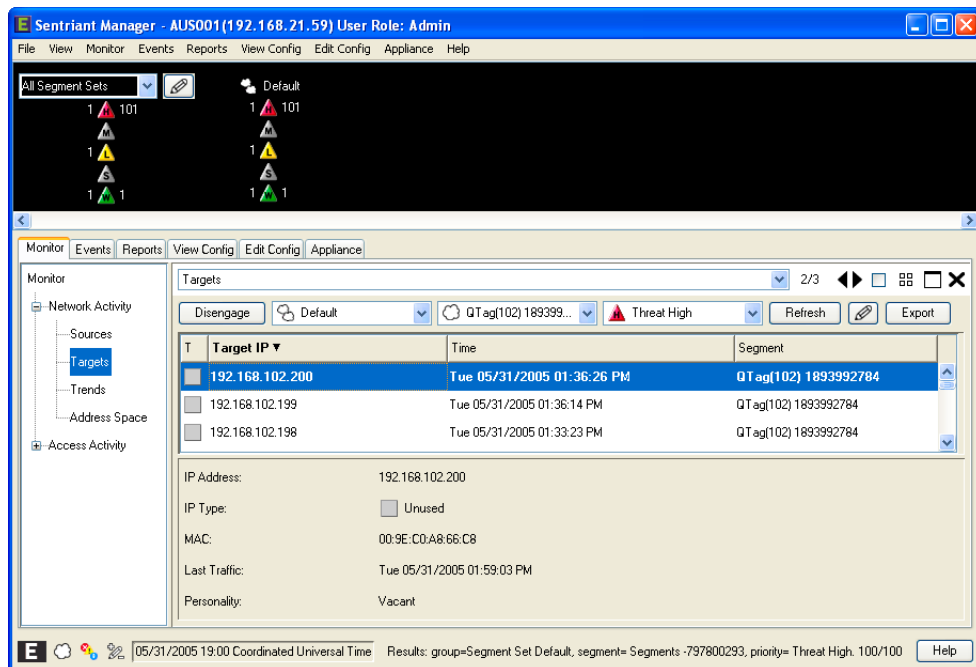
Details about Target IP are displayed in the Targets Details View.

To see Target details and display the list of Source IPs:

- 1 Select Details by right-clicking on the Target in the Target Panel.



The Targets Details View is displayed.



For the selected Target IP, the following information is displayed in the Details area.

- Target IP - The IP Address of the targeted system
- IP Type - The IP Type of the target. The IP Types are:
 - ☐ Used - IP Address used by host within the protected range
 - ☒ Unused - IP Address within the protected range that is not used by a host
 - ☐ External - IP Address used by host external to the protected range
 - ☐ Unprotected - IP Address not in the protected range
 - ☐ All - All IP Addresses
- MAC Address - The hardware address of the targeted system
- Last Traffic - The last activity from a source on the target
- Personality - Customized, Virtual Personality, or Vacant

View Source IP List

The **View Source IP List** displays a list of source IP Addresses that are actively communicating with target IP Addresses. Choosing an individual target IP Address displays a list of source IP Addresses that are currently communicating with the target. From the Source IP List, you can perform IP Look Up, threat and response activities.

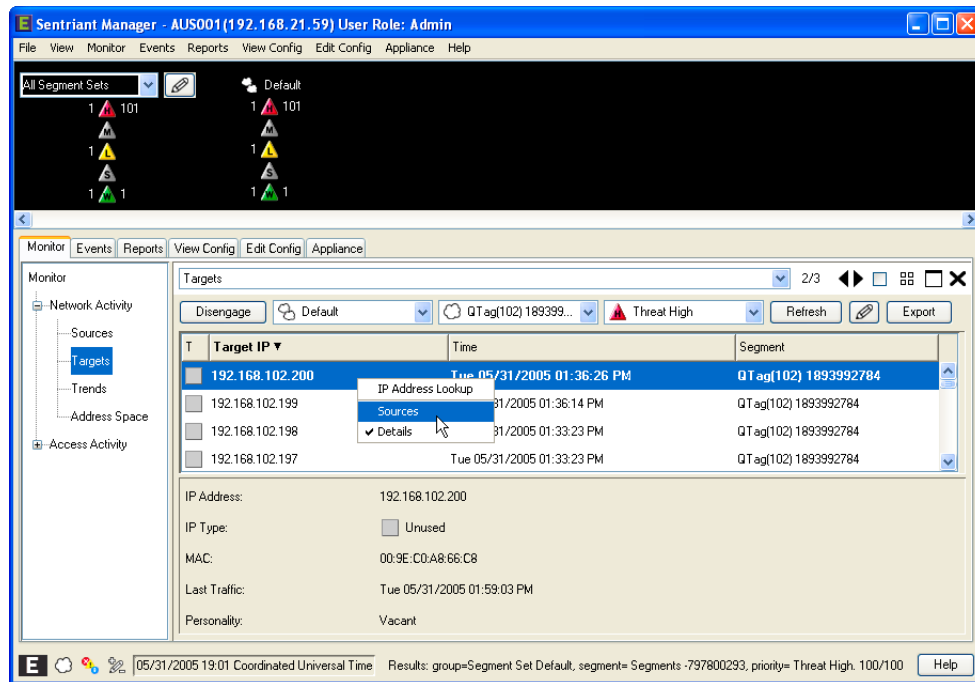
From the Source IP List, you can:

- [View source IP Addresses](#) for each selected target
- [IP Address Lookup](#) - A tool that returns the host name and IP Address of a source

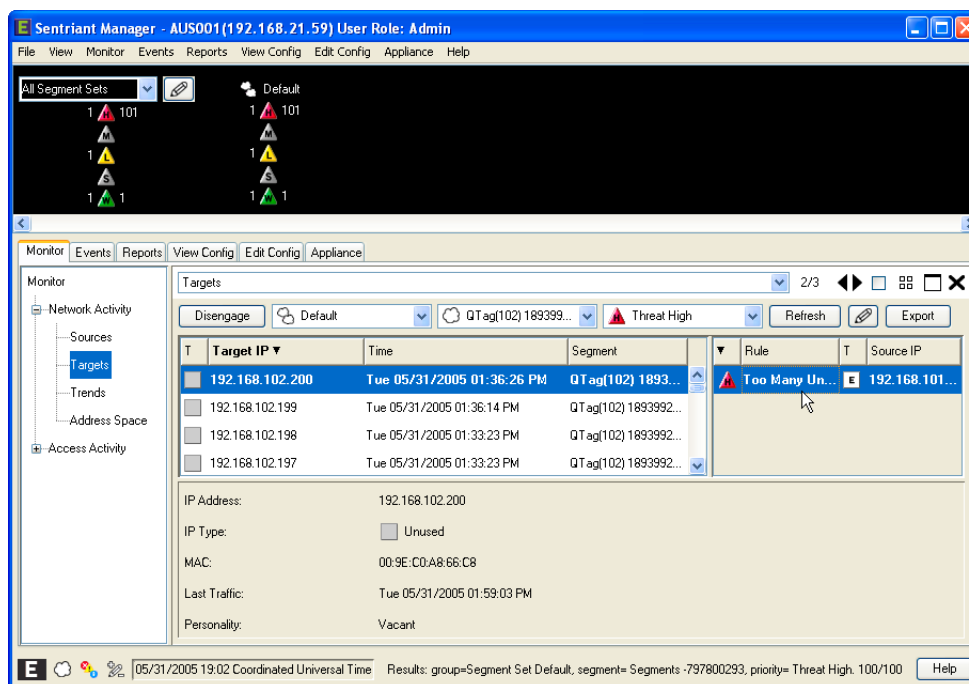
- **Threat - Escalate and Dismiss** - Manually escalate or dismiss a suspect to a threat
- **Response - Cloak or Uncloak** - Cloaks or Uncloaks a source from the communication paths to protected targets

To view the IP Addresses of sources communicating with targets:

- 1 Select the row of any Target IP Address.
- 2 Right-click to bring up the pop up menu.
- 3 Select **Sources**.



The Sources table is displayed containing all sources that have communicated with the selected target.

**NOTE**

A target is displayed only once and is determined by the source that triggered the highest priority level. For example, a source triggers a medium threat and a high threat. The Sources Panel will only display the highest threat priority level for that target.

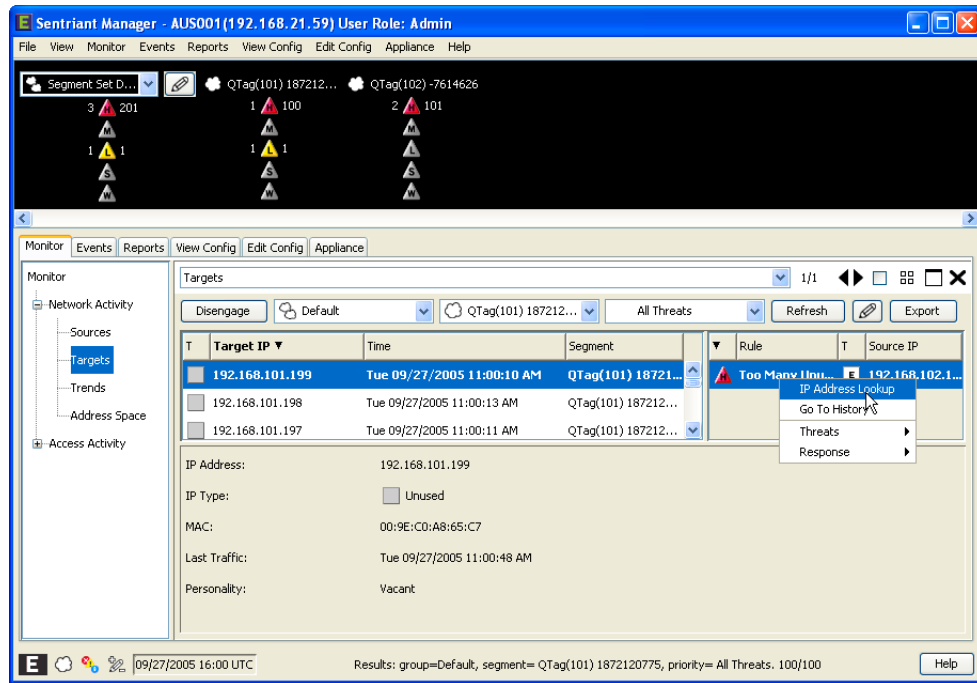
Source IP List - IP Lookup. It may become necessary to look up the location of an IP Address to understand where it is coming from. Sentries NG Manager's Lookup IP Address on the web tool contains all of the regional internet registry services. The Internet Registry services are:

- APNIC represents the Asia Pacific region, comprising 62 economies
- RIPE represents a membership base of around 3,500 members. The RIPE NCC service region consists of more than 90 countries across Europe, the Middle East, Central Asia and African countries located north of the equator
- SHOWMYIP

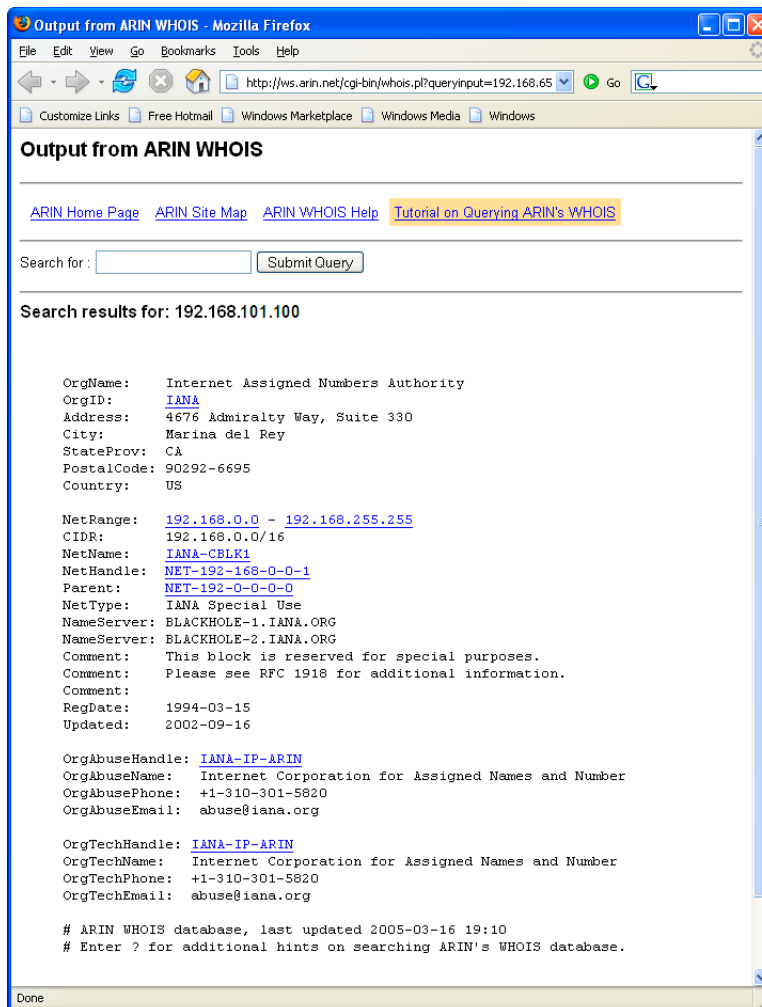
The tool will direct you to the correct page and start the search of the IP Addresses location.

To look up an IP Address on the web:

- 1 From the Targets Panel, select a source from the Sources IP List.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Lookup** and then one of the registry services from the list.



The selected IP Address is populated in the “who is” section of the registry service. Search results are displayed for the selected IP Address. Each registry service displays results differently so review carefully.

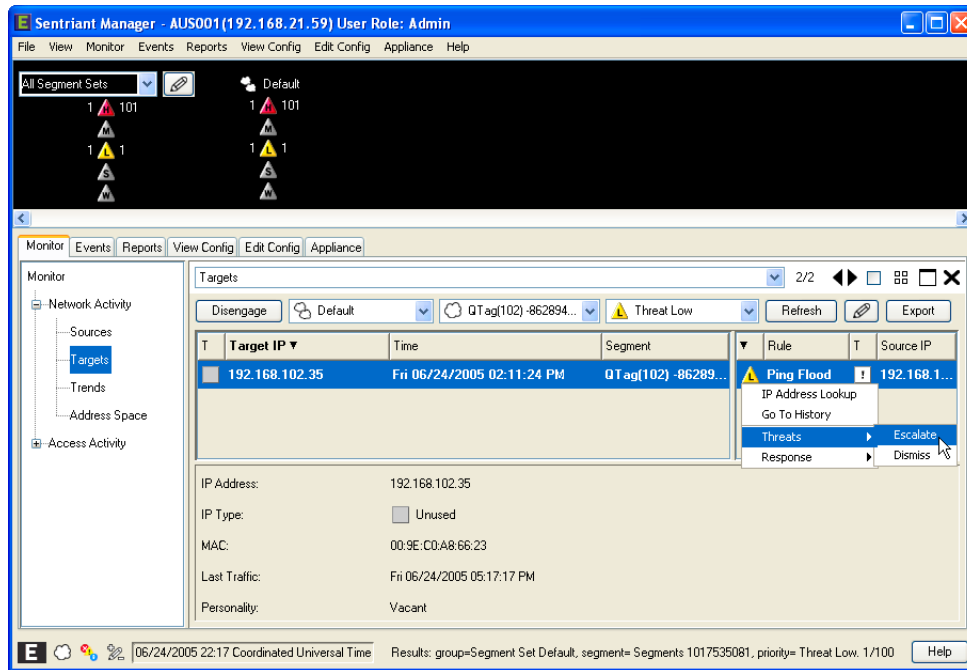


Source IP List - Threat. Sources that are listed can be escalated as a threat. In some cases, sources may need to be escalated manually. For example, an external source is slow scanning a protected range but has not triggered a rule. You may escalate from Watch to any other priority which in turn will trigger the rule responses to cloak the source.

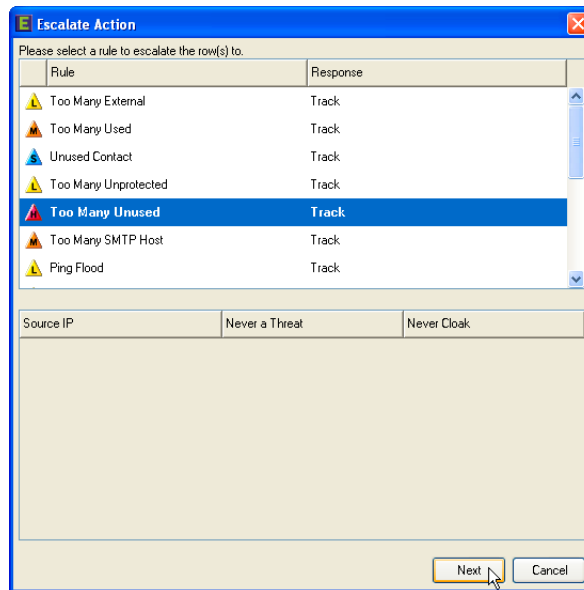
If it is determined that the source is not a threat, you may dismiss the source and return it to a Watch priority.

To escalate a threat:

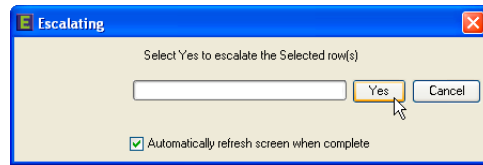
- 1 From the Targets Panel, select a source from the Sources IP List.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Escalate** from **Threats**.



- 4 Select a rule from the Escalate Watch(s) Action table to apply to the source.
- 5 Click **OK**.



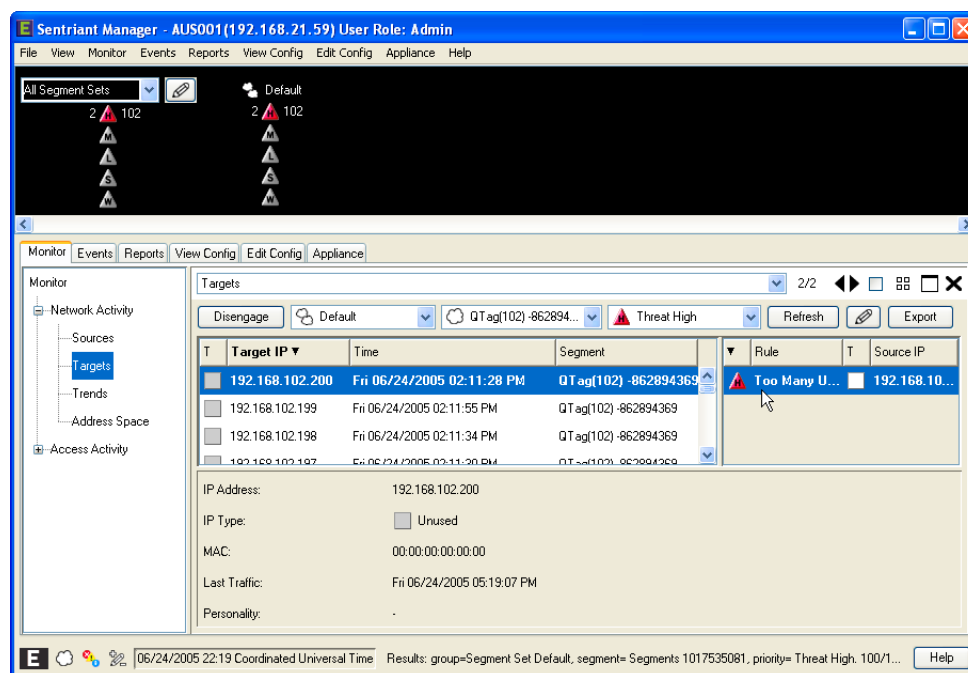
- 6 Click **Yes**.
- 7 Click **Close** to close the dialog.



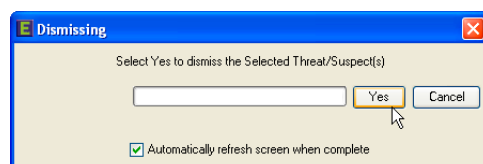
The source is escalated to the priority level set by the rule.

To dismiss a threat:

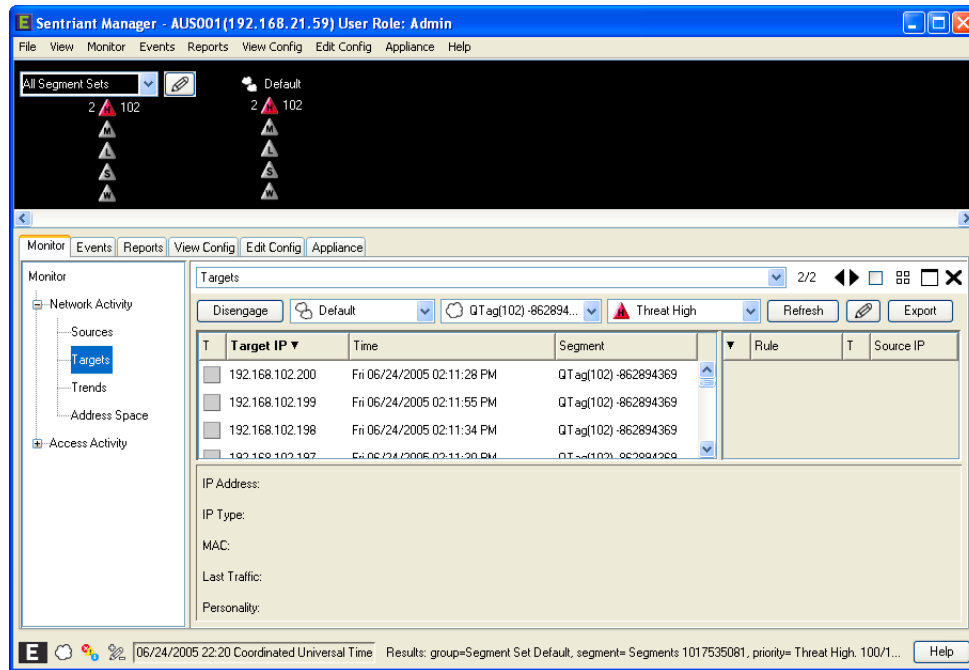
- 1 From the Targets Panel, select a source from the Sources IP List.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Dismiss from Threats**.



- 4 Click **Yes** to dismiss the source as a threat.



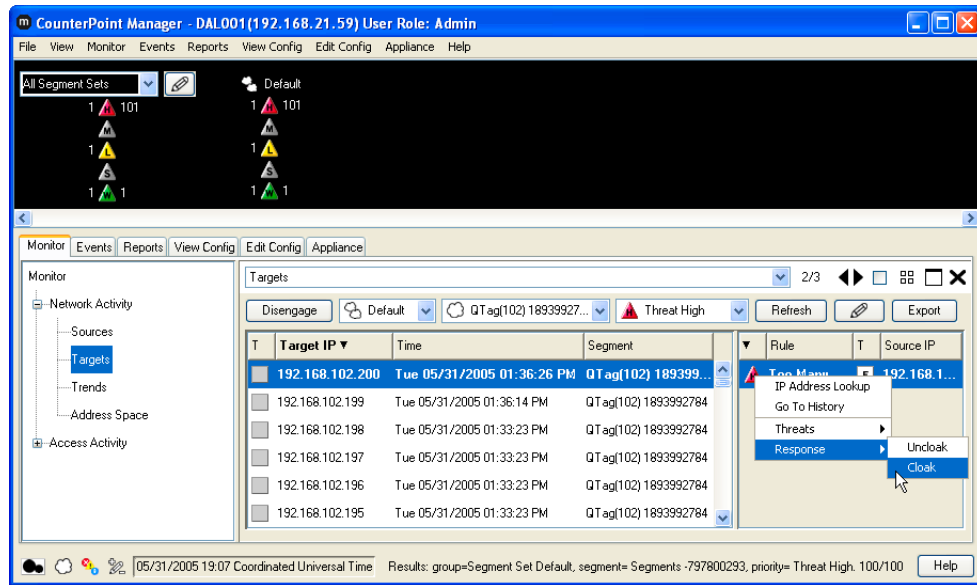
The threat is dismissed and the Source list is refreshed.



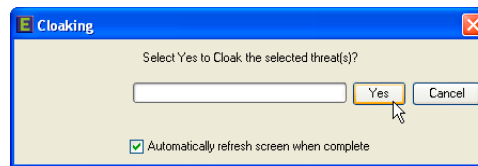
Source IP List - Response. When Cloak is selected as the response to a threat, the Sentriant NG appliance initially inserts itself into communication paths for only the devices that have communicated with the threat. The Sentriant NG appliance also inserts itself into all new communication paths as they occur. At the point in which the Sentriant NG appliance has inserted itself into the communication path, all traffic to/from the threat source will be surgically removed. Traffic to/from other (non-threat) hosts will be permitted. Once determined that the threat source is no longer a threat it can be uncloaked so that communication is permitted within the Sentriant NG appliance's protected segments.

To cloak a source:

- 1 From the Targets Panel, select a source from the Sources IP List.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Cloak** from **Response**.

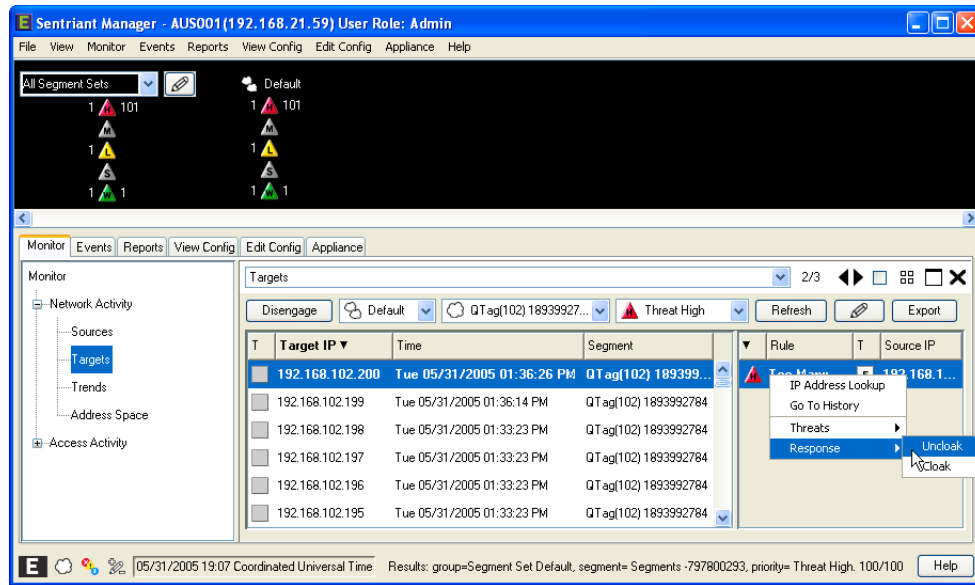


4 Click **Yes** to cloak the source.

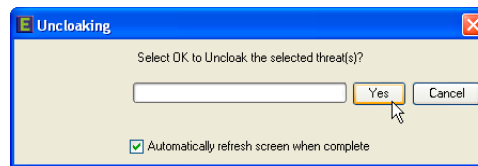


To uncloak a cloaked source:

- 1 From the Targets Panel, select a source from the Sources IP List.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Uncloak** from **Response**.



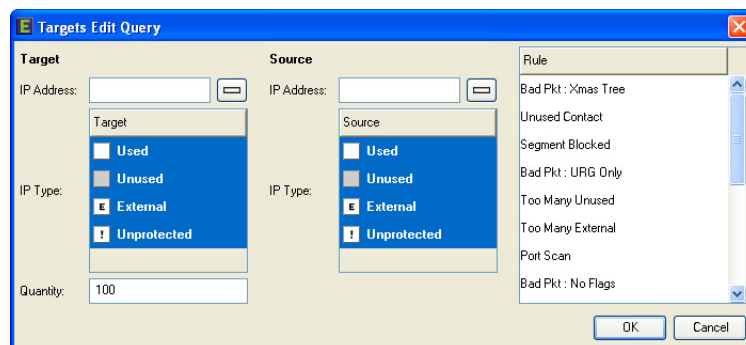
- 4 Click **Yes** to uncloak the source.



Querying Targets

To perform a query in the Targets Panel:

- 1 From the Targets Panel, click the Edit Query button to open the Targets Edit Query dialog.



- 2 Select parameters for the query. The **Targets Edit Query** dialog contains fields for filtering on **Target**, **Source**, and **Rules** attributes. The attributes for each field are:

Target

- IP Address - A single or range of IP Addresses can be entered. If no IP Address is entered all IP Addresses will be returned. To clear the IP Address field, click the Delete button.
- IP Type - Select an IP Type from the list. Options are Used, Unused, External, and Unprotected.
- Quantity - Enter a number for the maximum number of IP Addresses to be returned. One (1) to a thousand (1000) may be entered.

Source

- IP Address - A single or range of IP Addresses that the source must target in order to include this source in the query list. If no IP Address is entered all IP Addresses will be returned.
- IP Type - Select an IP Type from the list. Options are Used, Unused, External, and Unprotected.
- IP Type Status - Select an IP Type. Options are All, Used, Unused, External, and Unprotected.

Rules

- Rules - Select the rule from the list.

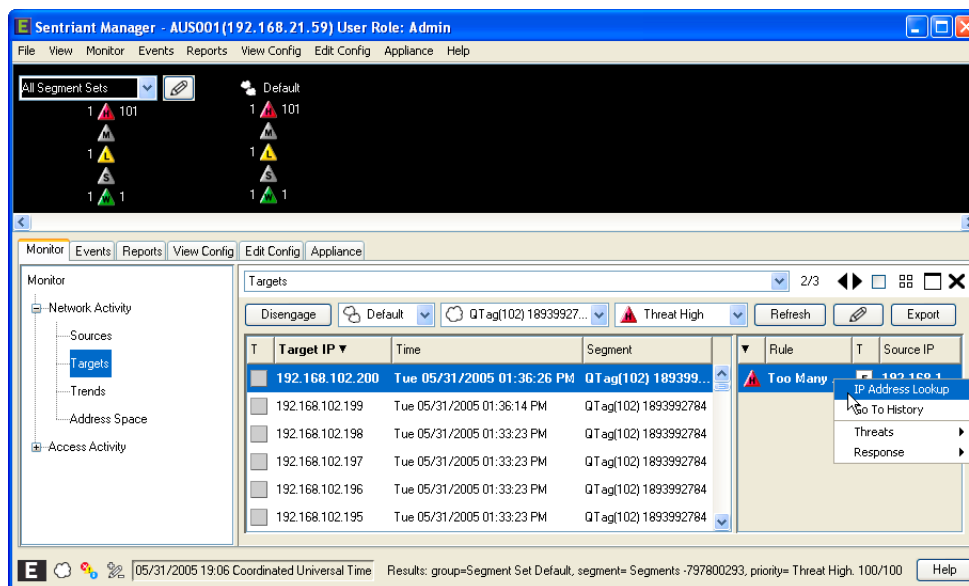
- 3 Click **OK** to return to the Sources Panel.
- 4 Click **Refresh** to run the query and display the results.

Looking Up Target IP Addresses

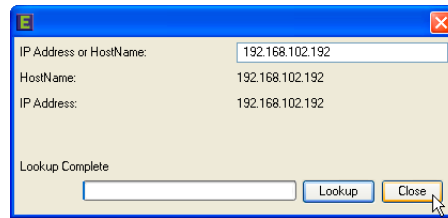
The IP Address Lookup tool will display the IP Address of a target and the HostName returned by the client's DNS.

To look up a Target IP Address and HostName:

- 1 Select a Target IP from the Targets panel.
- 2 Right-click to open the pop-up menu.
- 3 Select **IP Address Lookup**.



The HostName is displayed along with the IP Address. You may enter another IP Address or HostName in the IP Address or HostName field and click the **Lookup** button.



Trend Chart

The Trend Chart provides two visual representations of network traffic. The Trend Chart consists of two charts, the Line Chart and the Dial Chart.

The Line Chart shows network traffic over time and begins collecting data once the Sentriant NG Manager is started. Network traffic data from the Status Bar is represented in the Line Chart by the color of each threat priority and watch. Trend Chart data differs from the Status Bar data in that network traffic is continuously updated in the Status Bar while the Trend Chart is historical and updates periodically.



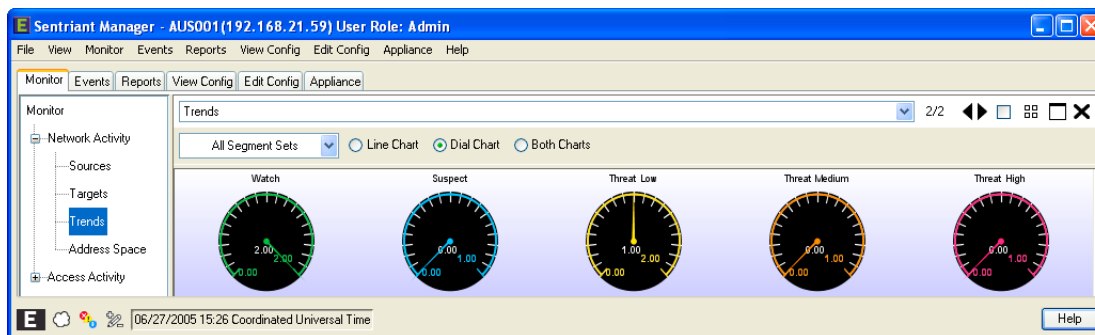
The Line Chart's horizontal axis indicates the time duration that the network traffic has been collected. The chart's vertical axis indicates number of network traffic packets sent to the group being monitored for each of threat priority and watch. As the trend data is collected, the chart resizes automatically as time goes by and the number of network traffic packets increases.



NOTE

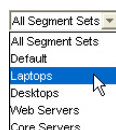
Trend data is collected for active sessions only. Once the Sentriant NG Manager is closed, the collection is time and quantity is reset.

The Dial Charts show a count of the highest number of threats during a session. As threats are mitigated, you will see the number decrease or the dial swing towards zero.



To change the Segment Set:

- 1 From the Monitor Tab, select Network Activity and then Trend Chart.
- 2 Select a **Segment Set** from the drop-down list.



To change chart view:

- 1 From the Monitor Tab, select Network Activity and then Trend Chart.
- 2 Click a button to toggle between Line Chart, Dial Chart or Both Charts.



Address Space Panel

The **Address Space** panel provides a set of state information for IP Addresses that reside in the selected network segment that are actively being contacted or have been contacted by a source host. You can use the state information to verify that used and unused IP Addresses for a segment are allocated as expected. You can take action from this view to add an IP Address as a gateway, to exclude an IP Address from becoming a decoy, and to diagnose unexpected network behaviors



NOTE

The Address Space Panel can provide information about data with common configuration issues. For example, IP Addresses that have a large spoof count are indicative of a possible gateway. IP Addresses that act as both used candidates and deception candidates may be IP Addresses that should be excluded from deception.

From the Address Space Panel, you can:

- [View IP Addresses](#)

- View Address Space Details
- Query Address Space
- Perform Action on IP Addresses

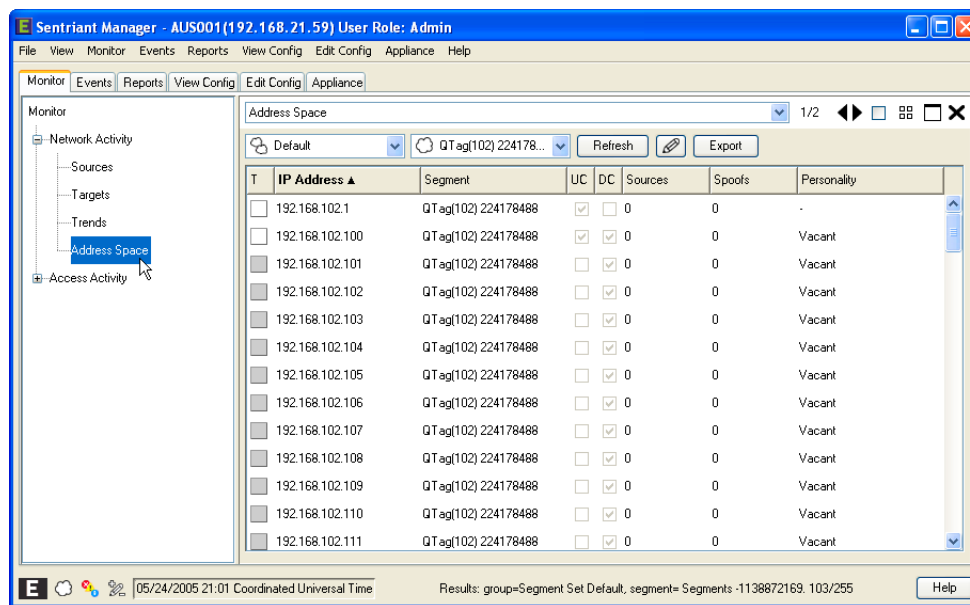
View IP Addresses

The **Address Space Panel** provides a set of state information for IP Addresses that reside in the selected network segment that are actively being contacted or have been contacted by a source host. You can use the state information to verify that used and unused IP Addresses for a segment are allocated as expected. You can take action from this view to add an IP Address as a gateway, to exclude an IP Address from becoming a decoy, and to diagnose unexpected network behaviors.



NOTE

The list of IP Addresses represent past and present activity. Refreshing the panel will not remove inactive IP Addresses. To remove the list of IP Addresses, you must restart the SentiNG appliance.



For each active IP Address, the following information is displayed:

- IP Types:
 - ☐ Used - IP Address used by host within the protected range
 - ☒ Unused - IP Address within the protected range that is not used by a host
 - ☐ External - IP Address used by host external to the protected range
 - ☐ Unprotected - IP Address not in the protected range
 - ☐ All - All IP Addresses

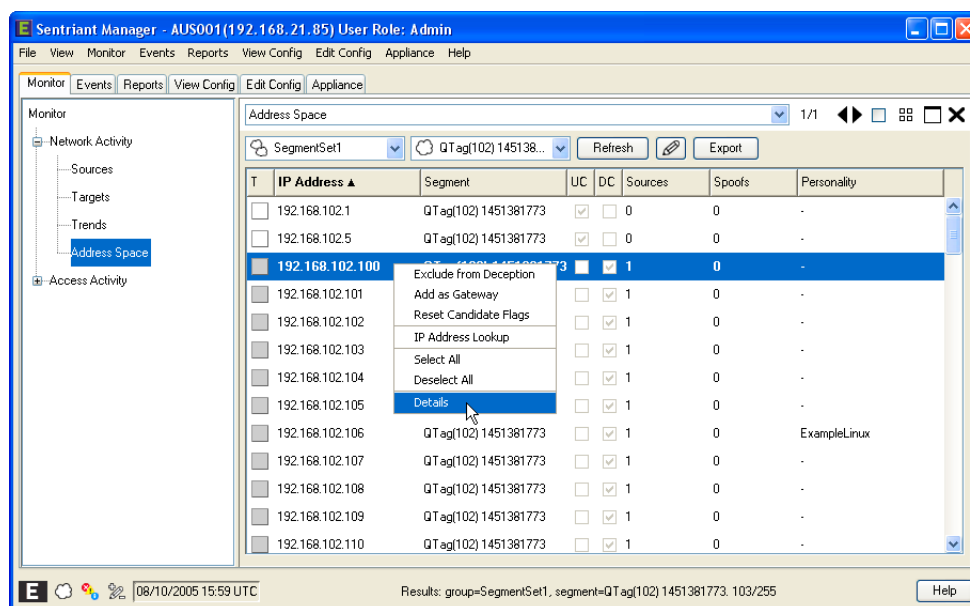
- IP Address
- Network Segment
- Used Candidate (UC) - A check mark in this field indicates that traffic has been detected from this IP since the Sentriant NG appliance was started.
- Deception Candidate (DC) - A check mark in this field indicates that the IP Address has been used as a decoy since the Sentriant NG appliance was started.
- Sources - Number of sources contacting the address
- Spoofs - Number of spoofed as addresses from this IP Address
- Personality - Indicates the current decoy personality assigned, if applicable

Viewing Address Space Details

The **Address Space Details View** identifies specific attributes of the selected IP Address.

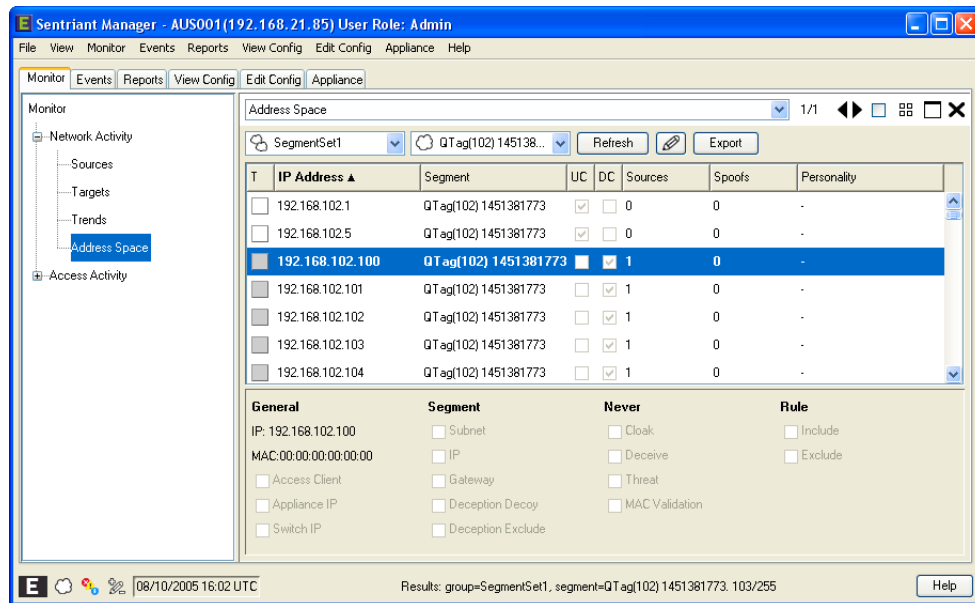
To view Address Space Details:

- 1 Select Details by right-clicking on an IP Address in the Address Space Panel.



The Address Space Details view is displayed.

A check mark beside an attribute indicates that the attribute is in effect for the selected IP Address.



The Address Space attributes are:

General

- IP - IP Address that has received communication from another source
- MAC - MAC address of the workstation assigned to the IP Address
- Access Client - A check indicates the IP Address is configured as an Access Client
- Appliance IP - A check indicates the IP Address is a Sentriant NG appliance

Segment

- Subnet - Indicates the IP Address is within a Segment Subnet
- IP - Indicates the IP Address is within a Segment IP
- Gateway - Indicates the IP Address is configured as a Segment Gateway
- Deception Decoy - Indicates the IP Address is configured as a Deception Decoy
- Deception Exclude - Indicates the IP Address is configured to exclude the IP Address from deception

Never

- Cloak - The IP Address is configured to never be Cloaked
- Deceive - The IP Address is configured to never be a Deception Decoy
- Threat - The IP Address is configured to never be considered a Threat
- MAC Validation - The IP Address is configured to never validate the MAC address of the host

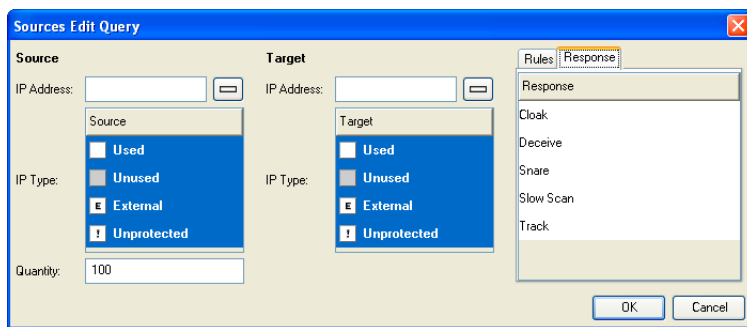
Rule

- Include - The IP Address is configured for Rule Inclusion
- Exclude - The IP Address is configured for Rule Exclusion

Querying Address Space

To perform a query in the Address Space Panel:

- 1 From the **Address Space Panel**, click the Edit Query button to open the **Address Space Edit Query** dialog.



The **Address Space Edit Query** dialog contains fields for filtering on **IP Address**, **IP Type**, **Range**, **Quantity**, and **Type** attributes as described below.

Address

- **Source IP Address** - Enter an IP Address or a range of IP Addresses. If no IP Address is entered all IP Addresses will be returned. To clear the Source IP Address field, click the delete button.
- **IP Type** - Select an IP Type from the list. Options are Used and Unused.
- **Range** - Select either **Seen so far** to include only hosts that have sent or received traffic on a segment or **All** to list all IP Addresses in the protected range regardless of traffic.
- **Quantity** - Enter a value for the maximum number of IP Addresses to be returned. One (1) to One Thousand (1000) may be entered.

Type

- The default setting is to retrieve all Types of address space data. However, you have the option of selecting specific types of data or customizing the Type query. A default set of Types has been identified and are:
- **All** - returns all address space types based on the Address query selection.
- **Gateway/Router** - Display all IP Addresses that have a high spoof count.



NOTE

IP Addresses that have a large spoof count may be an indication of a gateway that has not been configured as a gateway within Sentriant NG or a rogue unknown device acting as a gateway.

- **Deception Conflict** - Display all IP Addresses that have been both used candidates and virtual candidates.
- **Targeted Unused** - Display all IP Addresses that have a large number of sources targeting them.
- **Custom** - Gives the user the ability to set individual Type values which are:
- **Deception Candidate (DC)** - Setting to **All** returns all IP Addresses that have Deception Candidate marked as **Yes** or **No**. Selecting **Yes** returns only IP Addresses marked as DC, selecting **No** returns IP Addresses not marked.

- Deception Exclude (DE) - Setting to **All** returns all IP Addresses that have Deception Exclude marked as **Yes** or **No**. Selecting **Yes** returns only IP Addresses marked as DE, selecting **No** returns IP Addresses not marked.
- Used Candidate (UC) - Setting to **All** returns all IP Addresses that have Used Candidate marked as **Yes** or **No**. Selecting **Yes** returns only IP Addresses marked as UC, selecting **No** returns IP Addresses not marked.
- Gateway/Router - Setting to **All** returns all IP Addresses that are configured as either a gateway or router. Selecting **Yes** returns only IP Addresses configured as gateways/routers, selecting **No** returns IP Addresses not configured.
- Sources Count - Enter a value to filter on the number of separate threat sources per IP Address.
- Spoof Count - Enter a value to filter on IP Addresses that have a high spoof count.

Address Space Actions

From the **Pop up Menu**, the following configuration actions on IP Addresses can be performed:

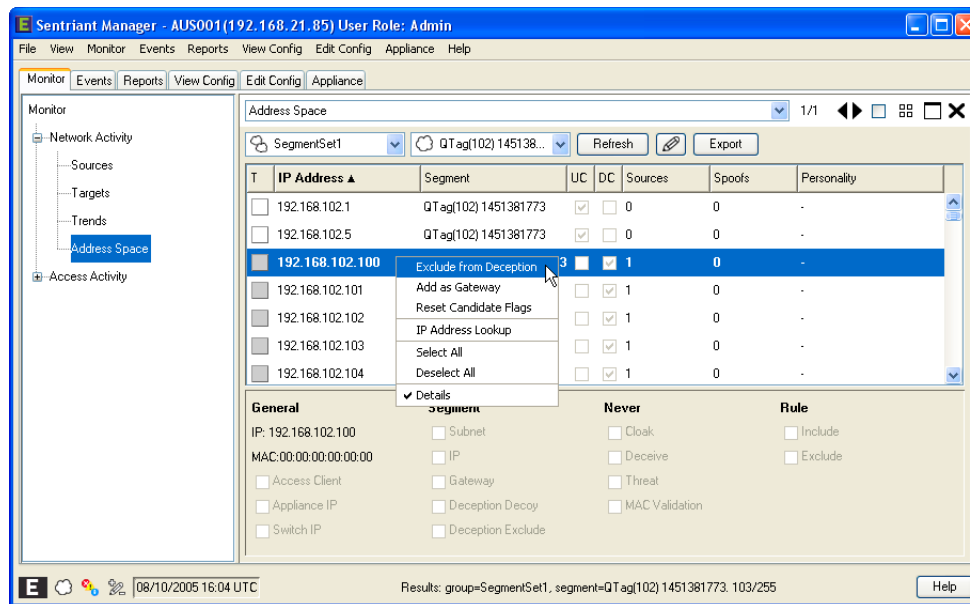
- **Exclude** - Excludes the selected IP Address from being virtualized
- **Add as Gateway** - Sets the selected IP Address as a gateway
- **Reset candidate flags** - Resets the Used and Deception flags for selected IP Addresses
- **IP Address Lookup** - A tool that returns the host name and IP Address of a source
- **Select/Deselect All** - Selects/Deselects All source IP Addresses in the source workspace
- **Show/Hide the Details Panel** - Turns the Details Panel on or off for selected IP Addresses

Exclude IP Address

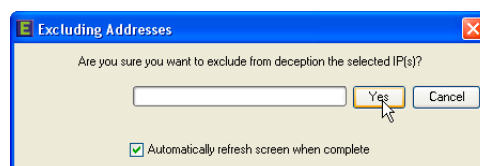
The Address Space Panel can provide information about data with common configuration issues. For example, IP Addresses that have a large spoof count are indicative of a possible gateway. IP Addresses that act as both used candidates and deception candidates may be IP Addresses that should be excluded from deception.

To exclude an IP Address:

- 1 Select an IP Address from the Address Space Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Exclude from Deception**.



4 Click OK.



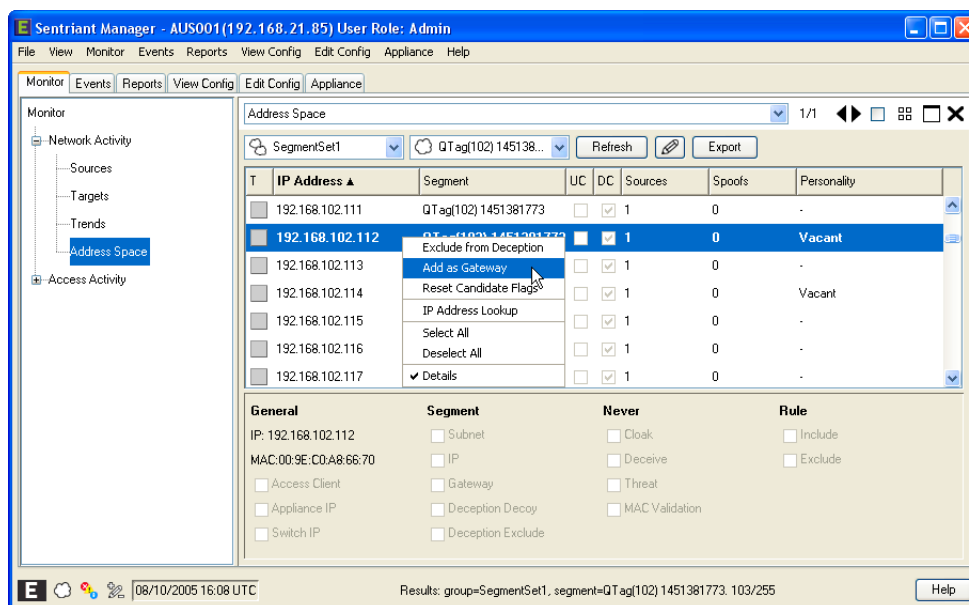
The IP Address will no longer be monitored; however, it will remain in the Address Space Panel.

Add as Gateway

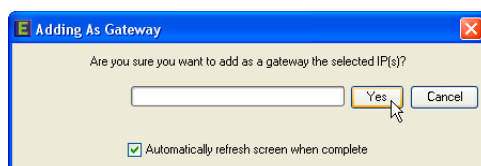
All Gateways that reside within the Fabric of Sentriant NG appliance monitoring must be identified. This is accomplished by setting the IP Address in the Address Space Panel to a Gateway.

To set an IP Address as a gateway:

- 1 Select an IP Address from the Address Space Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Add as Gateway**.



4 Click Yes.



NOTE

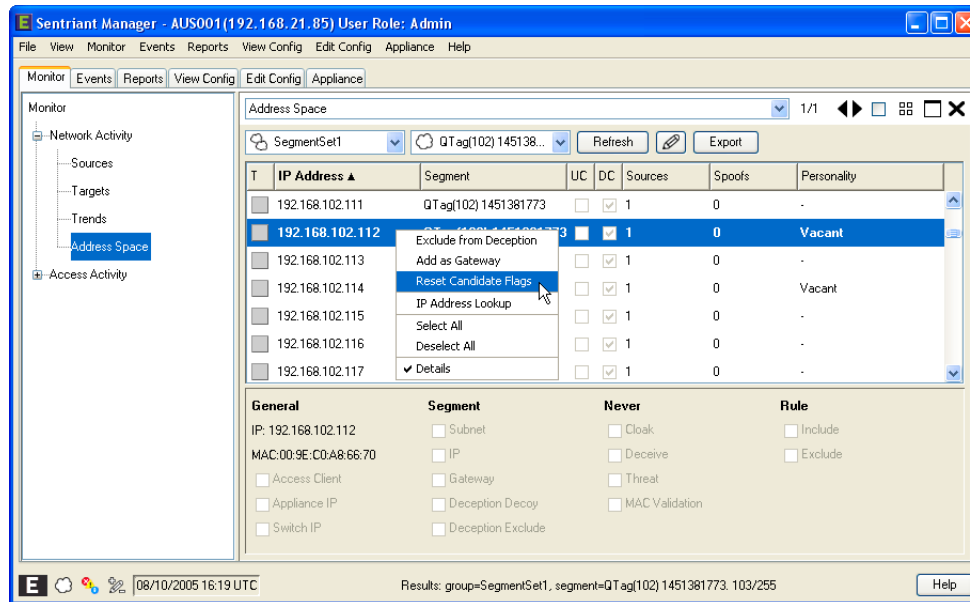
The IP Address must be within the range of the protected network segment in order for it to be added as gateway.

Reset Candidate Flags

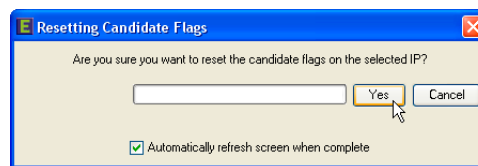
After mitigation activities have taken place on a target, it may become necessary to reset the used and/or deception flags.

To reset candidate flags:

- 1 Select an IP Address from the Address Space Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Reset Candidate Flags**.



4 Click Yes.

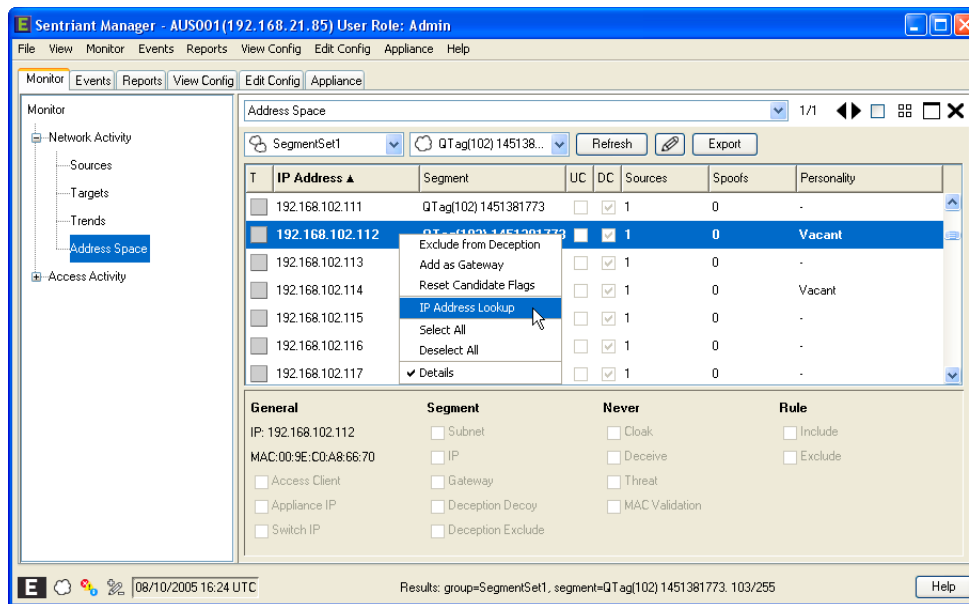


IP Address Lookup

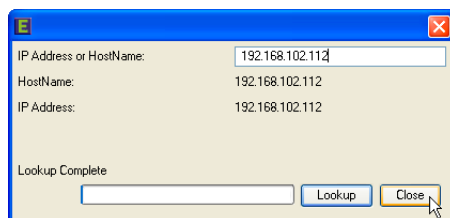
The IP Address Lookup tool will display the IP Address of a source and the hostname.

To look up an IP Address and hostname:

- 1 Select a source from the Sources Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **IP Address Lookup**.



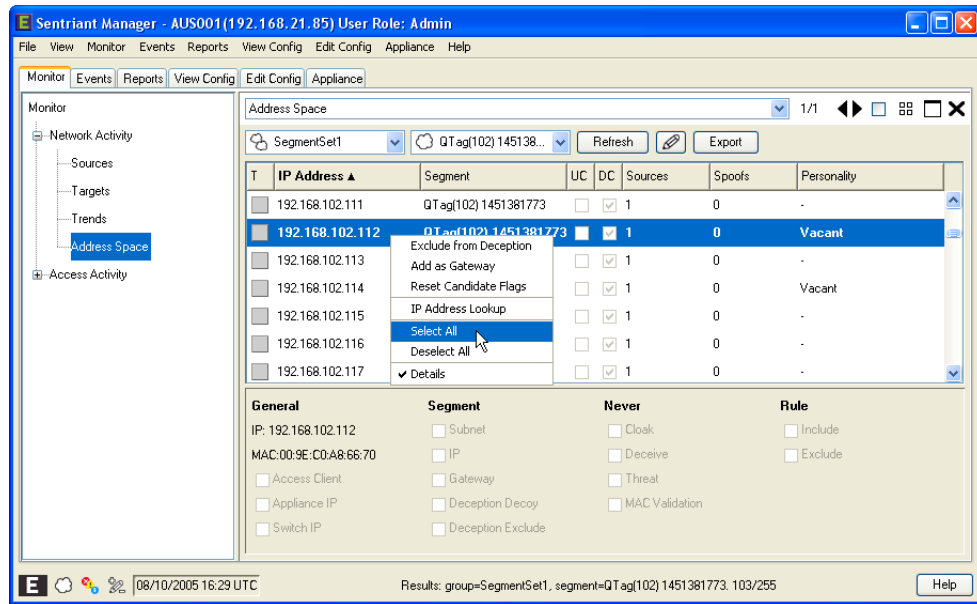
The HostName is displayed along with the IP Address. You may enter another IP Address or HostName in the IP Address or HostName field and click the Lookup button.



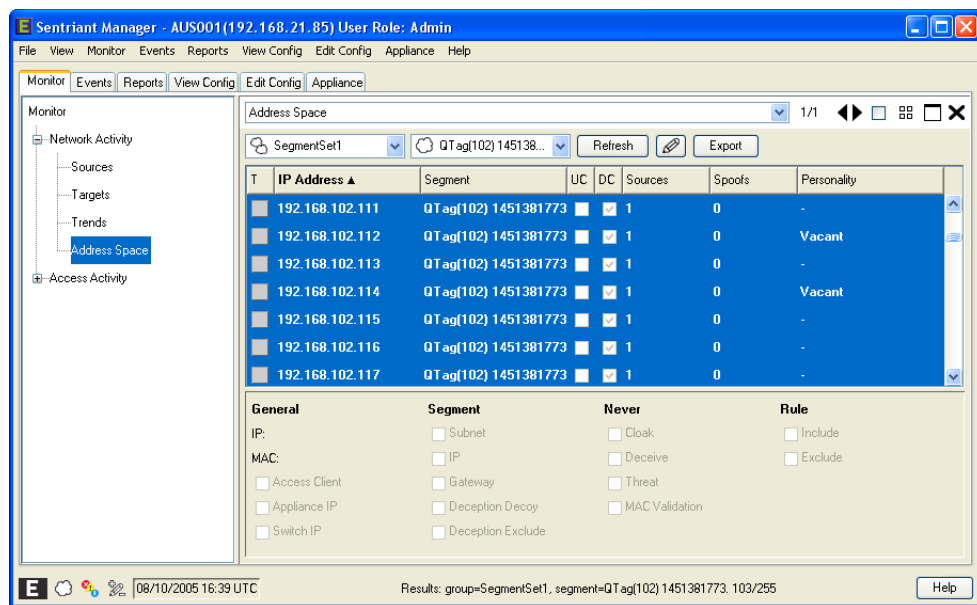
IP Address Select/Deselect All

To select all sources in the Address Space Panel:

- 1 Select an IP Address from the Address Space Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Choose **Select All**.

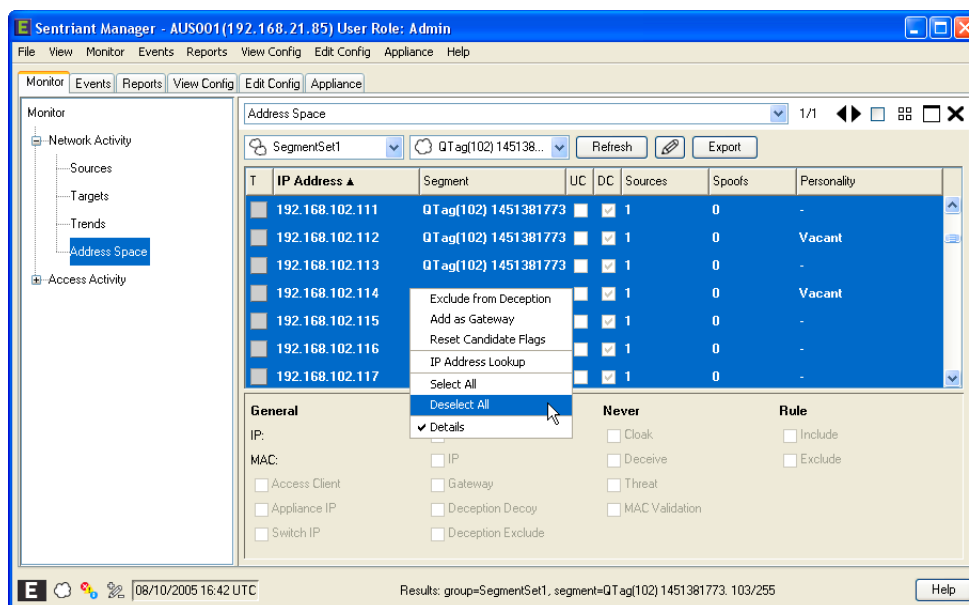


All IP Addresses are selected.



To deselect IP Addresses in the Address Space Panel:

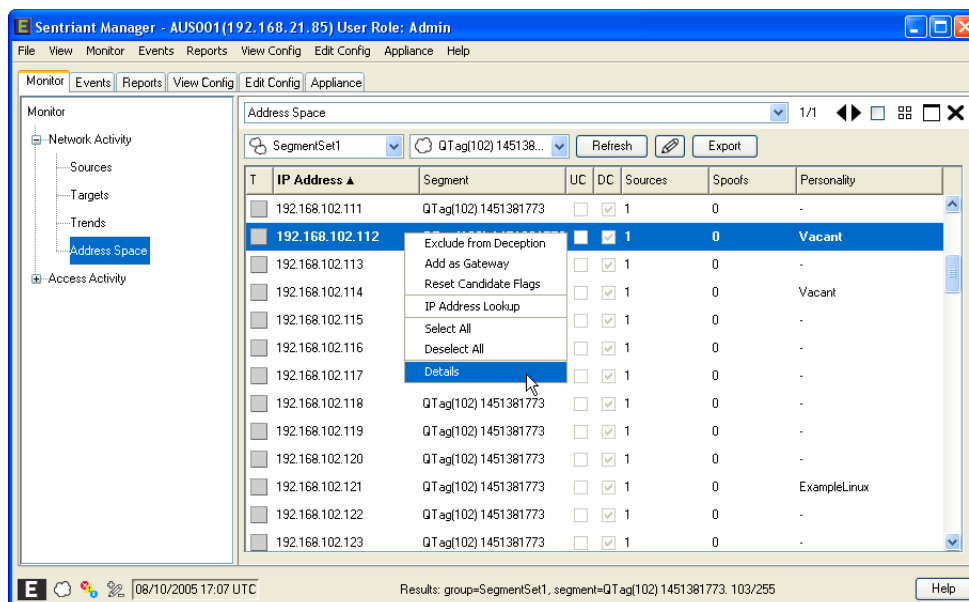
- 1 Right-click in the Address Space Panel to bring up the pop-up menu.
- 2 Choose **Deselect All**.



Show/Hide Details Panel

To display the Details Panel:

- 1 Right-click in the Address Space Panel.
- 2 Select **Details**.

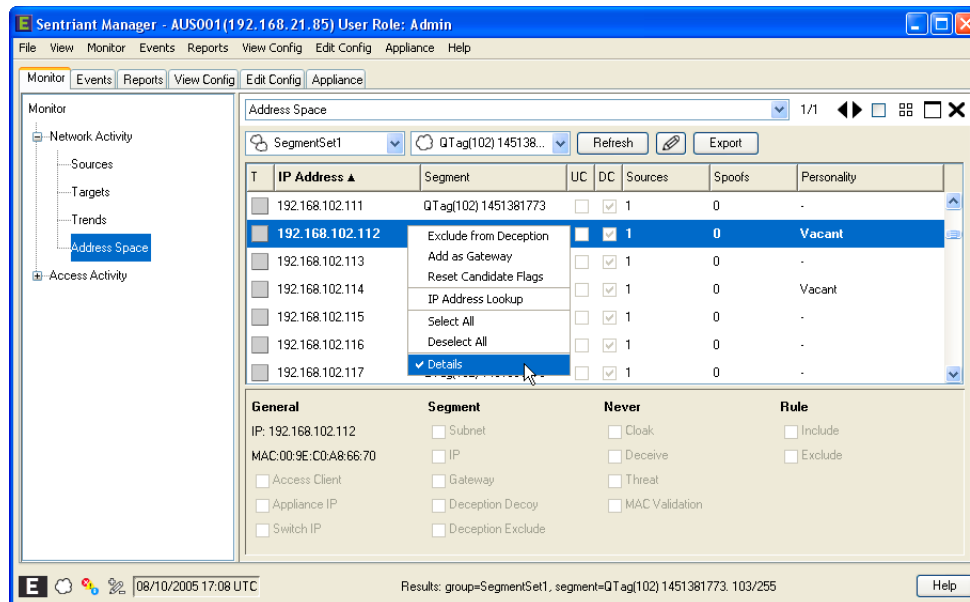


To hide the Details Panel:

- 1 Right-click in the Address Space Panel.
- 2 Select **Details**.

**NOTE**

You may also double-click an IP Address to hide/open the Details Panel.



Access Activity

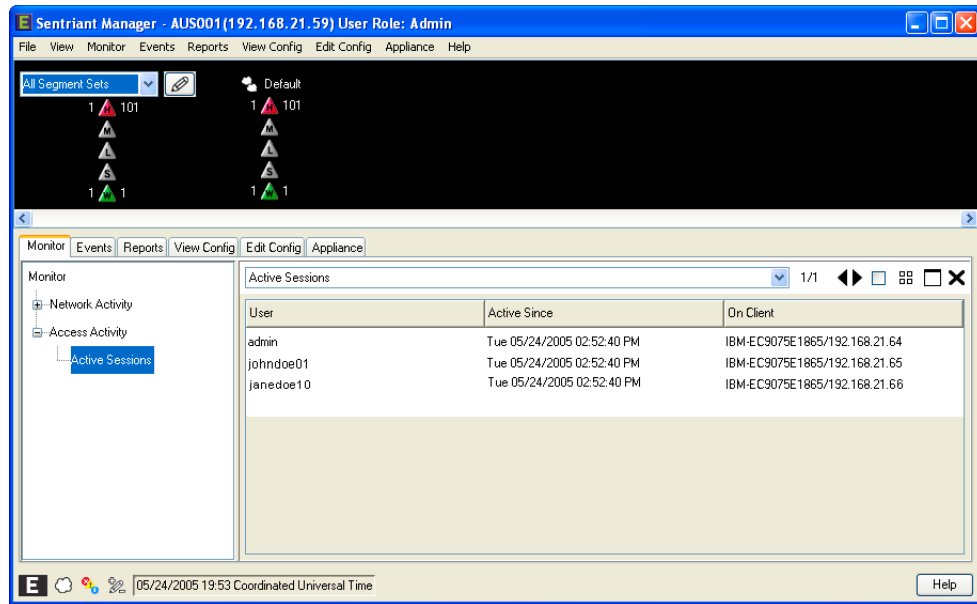
The purpose of the Access Activity Panel is to determine who is currently connected to the Sentriant NG appliance. When you make changes to the Sentriant NG appliance's configuration setting, the Sentriant NG appliance will automatically notify the user of upcoming changes therefore mitigating lost or conflicting configuration changes.

Active Sessions

To view Active Sessions:

- 1 From **Monitor > Access Activity**, select **Active Sessions**.

A list of all users currently logged into the Sentriant NG appliance is displayed.



Events

The Sentries NG appliance captures event logs that can be used to gather information about threats, hardware and software.

Appliance - Appliance events panel contains events logged by the Sentries NG appliance. For example, the database manager has started the database or a physical port on a Sentries NG appliance has gone down.

Audit - Audit events panel contains events such as log in attempts as well as events related to resource use such as creating, or deleting new users.

Network Activity - Network Activity events panel contains events logged by the Sentries NG appliance. For example, an activity started, a threat was detected, an activity has stopped. The Network Activity can be used for troubleshooting threats.

Events are automatically captured once the Sentries NG appliance is started. All users can view Appliance, Audit and Network Activity events. Only administrators can perform actions on an event.

Appliance Events

The Appliance events panel contains events logged by the Sentries NG appliance. For example, the database manager has started the database or a physical port on an Sentries NG appliance has gone down.

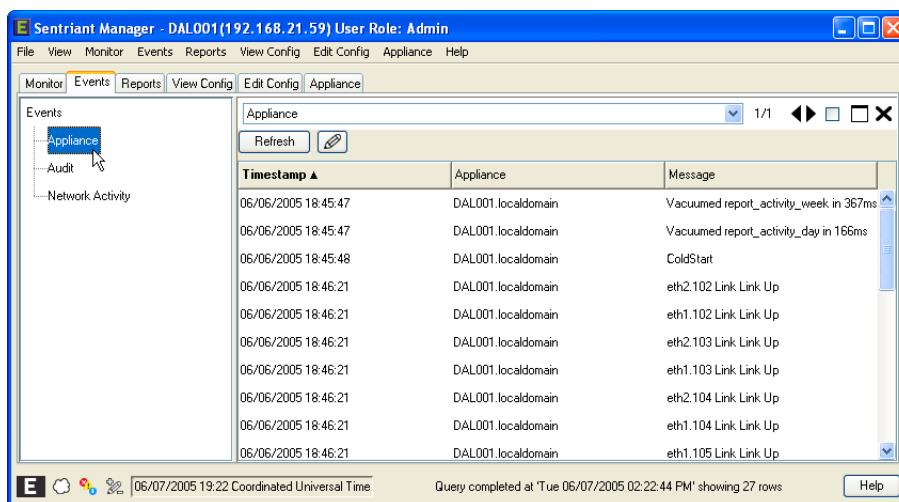
The Appliance Event Panel List contains the following information:

Table 2: Appliance Event Information

Information	Meaning
Timestamp	The date and time when the event occurred.
Appliance	The IP Address of the Sentries NG appliance.
Message	A message describing the event.

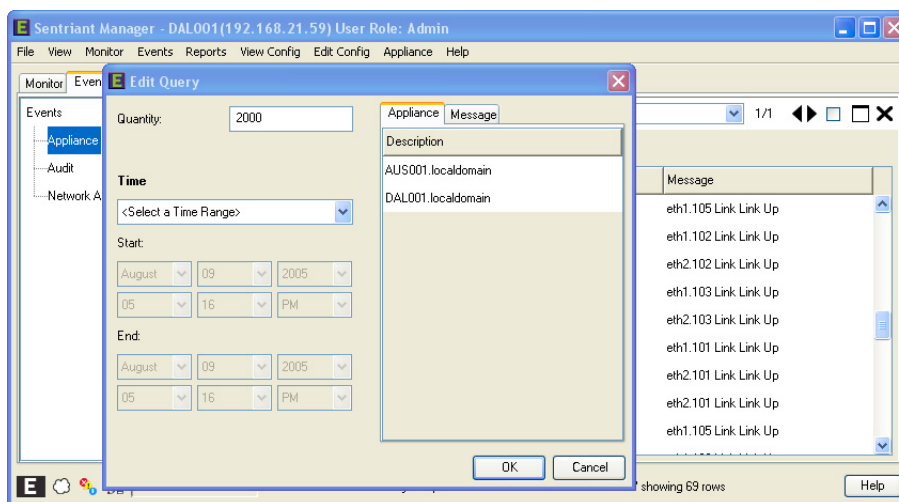
To view Appliance Events:

- 1 From **Events Tab**, select **Appliance** from the list.



To query the Appliance Events list:

- 1 Click the **Query** button.
- 2 The **Edit Query** dialog opens.



You can query appliance event parameters by the following:

- **Quantity** - The default events record quantity returned is 2000. This value may be changed from 1 to 9999.



NOTE

Entering a value that is less than the total amount of records that exist will return the events with the oldest timestamps. For example, if you select a start and end range that contains 250 records and you enter a Quantity of 200, you will not see 50 records with the latest timestamps.

- **Time**

- Select a Time Range - You may enter a custom timestamp or select one of the following:
 - Last Minute
 - Last 5 Minutes
 - Last Hour
 - Last Day
 - Last Week
 - Start - Enter a specific date and time when events occurred
 - End - Enter a specific date and time when events concluded
- Appliance - You may select from the list of appliances
- Message - You may select from the list of messages

Audit Events

The Audit events panel contains events such as log in attempts as well as events related to resource use such as creating, or deleting new users.



NOTE

When a user logs in to the Sentriant NG Manager, two connections are made resulting in two login events. One login event is for the connection to the Sentriant NG Manager and another is generated once the user has logged into the Sentriant NG itself.

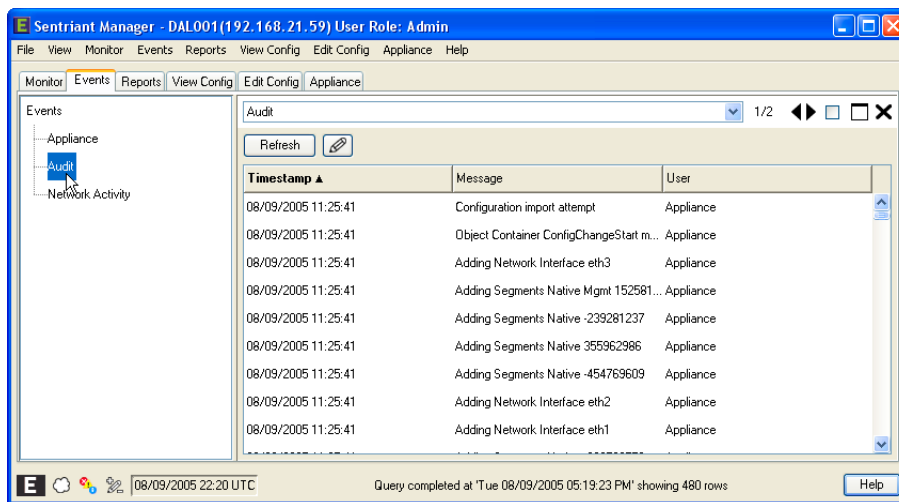
The Audit Events Panel List contains the following information:

Table 3: Audit Event Information

Information	Meaning
Timestamp	The date and time when the event occurred.
Message	A message describing the event.
User	Login ID of the user.

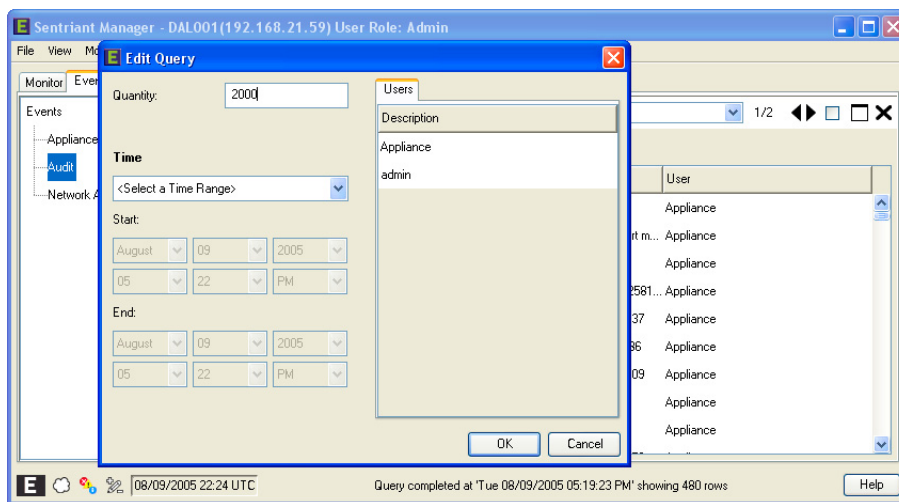
To view Audit Events:

- 1 From **Events Tab**, select **Audit** from the list.



To query the Audit Events list:

- 1 Click the **Query** button.
- 2 The **Edit Query** dialog opens.



You can query appliance event parameters by the following:

- **Quantity** - The default events record quantity returned is 2000. This value may be changed from 1 to 9999.



NOTE

Entering a value that is less than the total amount of records that exist will return the events with the oldest timestamps. For example, if you select a start and end range that contains 250 records and you enter a Quantity of 200, you will not see 50 records with the latest timestamps.

- **Time**

- Select a Time Range - You may enter a custom timestamp or select one of the following:
 - Last Minute
 - Last 5 Minutes
 - Last Hour
 - Last Day
 - Last Week
 - Start - Enter a specific date and time when events occurred
 - End - Enter a specific date and time when events concluded
- Users - You may select a user from the list

Network Activity Events

The Network Activity events panel contains events, within the Fabric, logged by Sentriant NG appliances. For example, an activity started, a threat was detected, an activity has stopped. The Network Activity can be used for troubleshooting threats on the Fabric.

The types of events found in the Network Activity Events Panel are:

- Activity Started - Event denoting the start of an event stream.
- Activity Stopped - Event denoting the stop or end of an event stream.
- Information - Event that is not part of an event stream.
- Threat - Event denoting that a threat was detected and an action has taken place.

View Network Activity Events

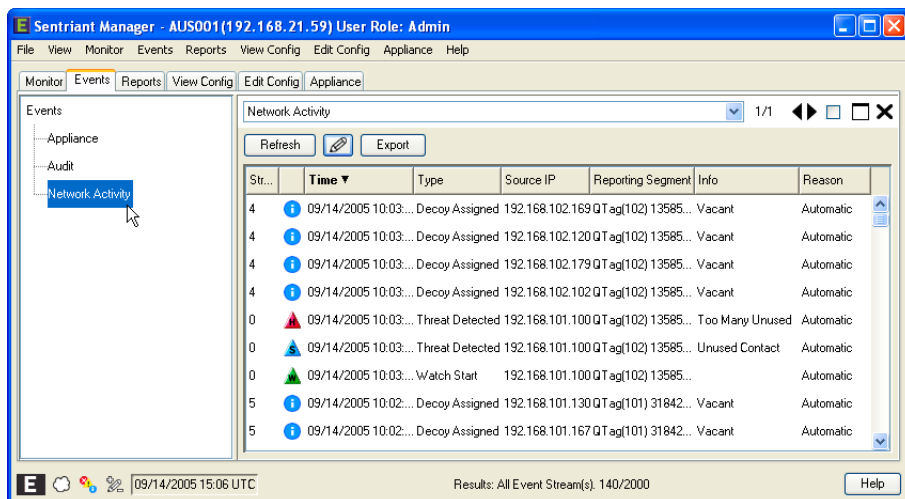
The Network Activity Events Panel List contains the following information:

Table 4: Network Activity Events Information

Information	Meaning
Type	An icon representing the type of event.
Time	The date and time the event occurred.
Event Types	Text message describing the event. For example, Activity Started, Threat Released, Activity Stopped.
Source IP	The IP Address of the source where the event originated.
Source Segment	The Segment name where the source originated.
Info	The name of the rule that was triggered by a threat type event.
Reason	The reason the rule was triggered, either Automatic or Manual.

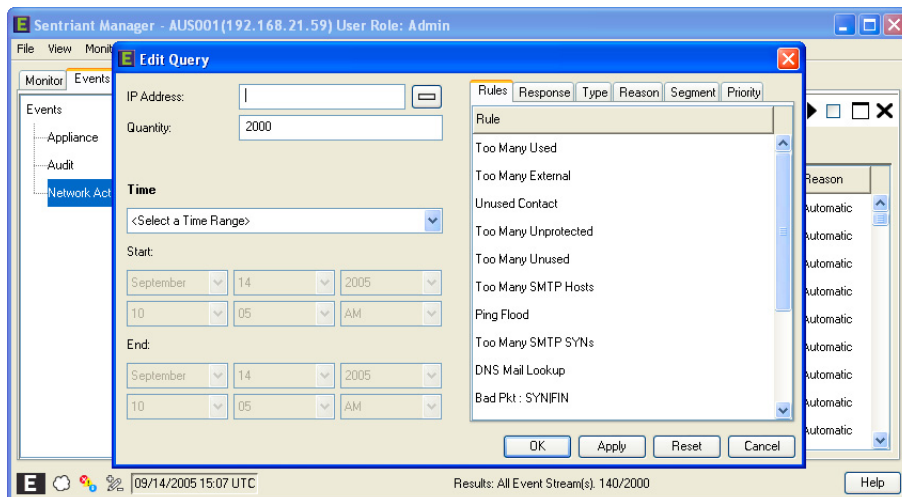
To view Network Activity Events:

- 1 From **Events Tab**, select **Network Activity** from the list.



To query the Network Activity Events list:

- 1 Click the **Query** button.
- 2 The **Edit Query** dialog opens.



You can query appliance event parameters by the following:

- IP Address - Enter an IP Address of a source
- Quantity - The default events record quantity returned is 2000. This value may be changed from 1 to 9999.



NOTE

Entering a value that is less than the total amount of records that exist will return the events with the oldest timestamps. For example, if you select a start and end range that contains 250 records and you enter a Quantity of 200, you will not see 50 records with the latest timestamps.

- Time
 - Select a Time Range - You may enter a custom timestamp or select one of the following:
 - Last Minute
 - Last 5 Minutes
 - Last Hour
 - Last Day
 - Last Week
 - Start - Enter a specific date and time when events occurred
 - End - Enter a specific date and time when events concluded
- Rules - Select a rule or multi-select rules
- Response - Select a response or multi-select responses
- Type - Select the event type message or multi-select event types
- Reason - Select the reason message or multi-select reasons
- Reporting Segment - Select the segment that is reporting the threat

**NOTE**

The reporting segment may not be the segment where the threat occurred. For example, in a Broadcast Only configuration, network traffic between segments does not go through a switch.

- Priority - Select the threat priority or multi-select priorities

Clicking the **OK** button will invoke the query on the Network Activity threats. You may remove the query by clicking the **Reset** button and then the **OK** button from the Query dialog.

Network Activity Details

The Network Activity Details Panel contains detailed event information to assist in processing source/target threat information. The Network Activity Details Panel is grouped by the type of data displayed. The groups are:

- **General** - High level source information including gateways, current and active target counts
- **IP** - Displays Spoofed As information for source IP Addresses
- **Port** - Displays Port information that sources and targets utilized
- **Packet** - Displays detailed packet information
- **Threats** - Displays all triggered rules

Double-clicking on a source in the Sources Panel or right-clicking on a source and selecting **Details** will activate the Details Panel.

General

The General panel contains high-level information for a selected event. This information is:

- IP Address of the event's source
- MAC Address of the event's source

- Start - Time the event occurred
- Last Traffic - the last time the event's source communicated with a Target IP Address within the Sentriant NG appliance's protected range
- Source Segment - The segment where the threat originated
- Reporting Segment - The segment reporting the threat

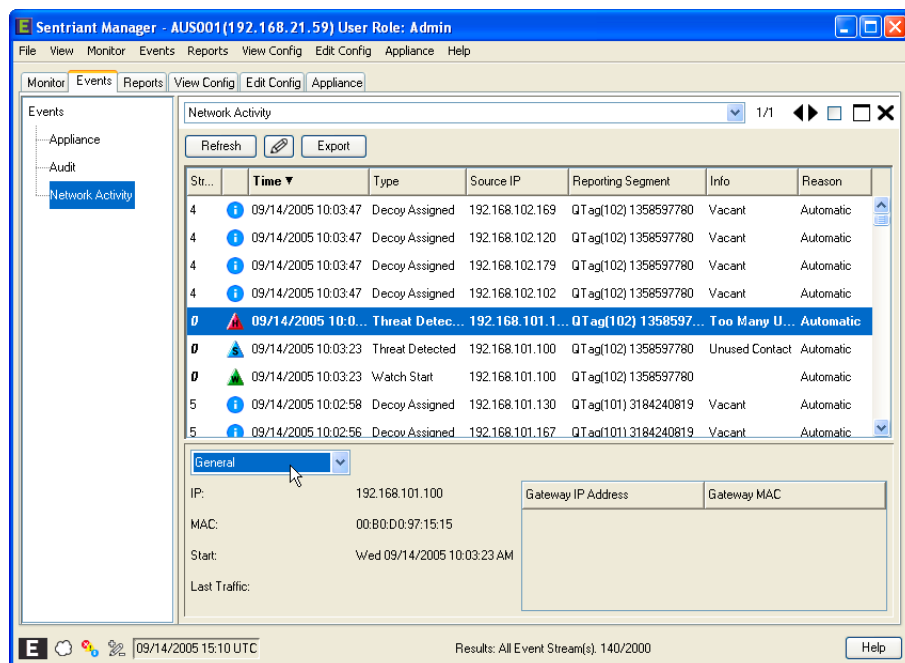
**NOTE**

The reporting segment may not be the segment where the threat occurred. For example, in a Broadcast Only configuration, network traffic between segments does not go through a switch.

- Remote Segment - A segment that passed the sources communication to the reporting segment
- General Table - Displays the Gateway IP Address and MAC where the event's source originated if originating from a gateway outside of the protected range.

To view an event's General information:

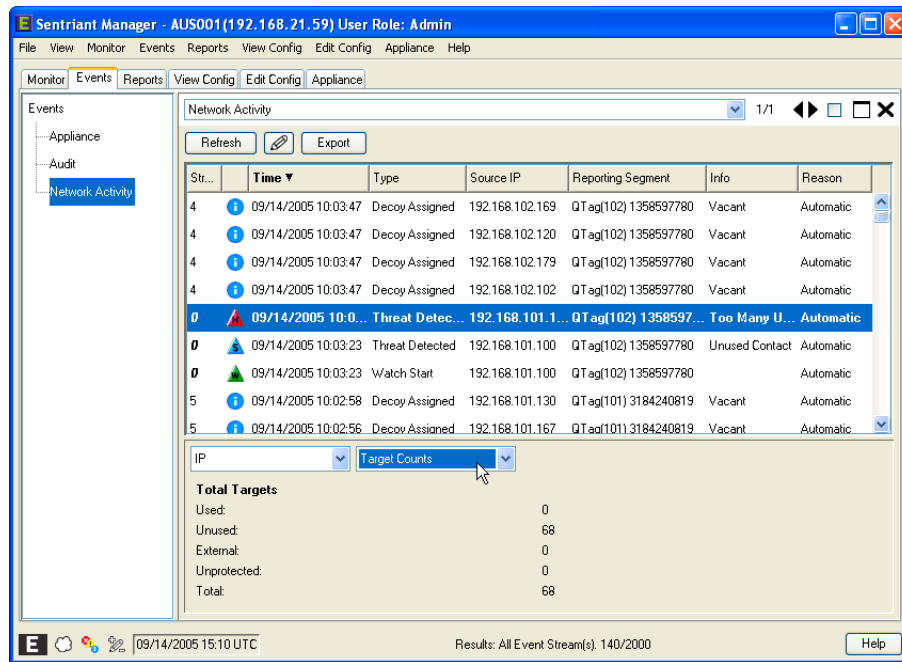
- 1 From **Events > Network Activity** tab, select an event.
- 2 Right-click to display the pop up menu and select **Details**. (The General Tab is default for the Details panel)

**IP**

The IP panel contains information specific to the number of active and total targets that the source has communicated with.

To view a source's Target Counts:

- 1 Select a source from the Network Activity Panel.
- 2 Select **IP** from the Details Panel drop-down list.



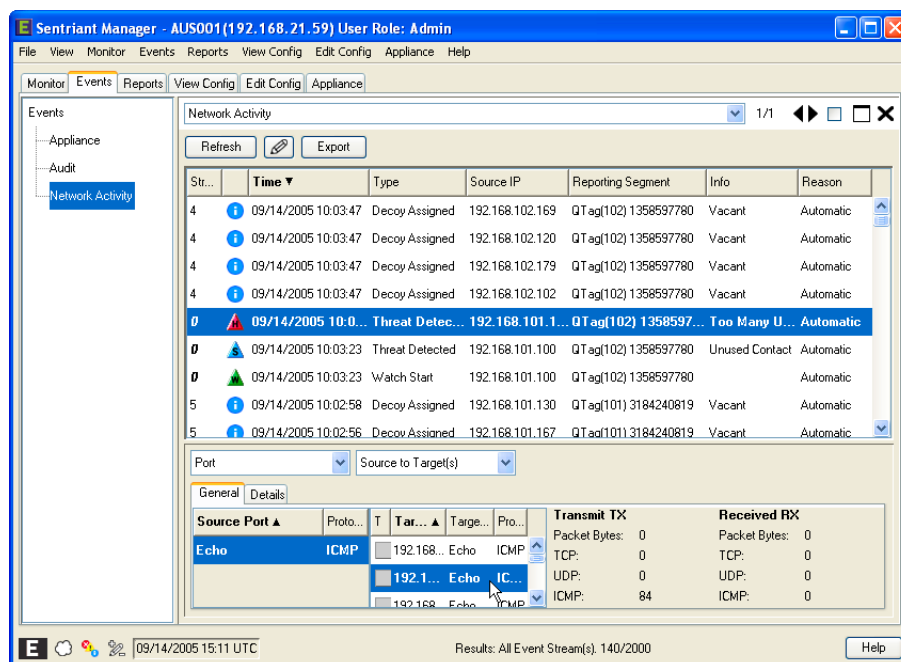
The Target Counts displays a list of **Active Targets**. Active Targets are sources that are currently communicating with targets. Each type of target, used, unused, protected, and unprotected quantity is displayed along with the total number of active targets.

Port

The Port panel contains information specific to the number of ports and type of port that the source has communicated with including total number of packet bytes transmitted and received and the targets that have responded.

To view the Ports that a source communicated with:

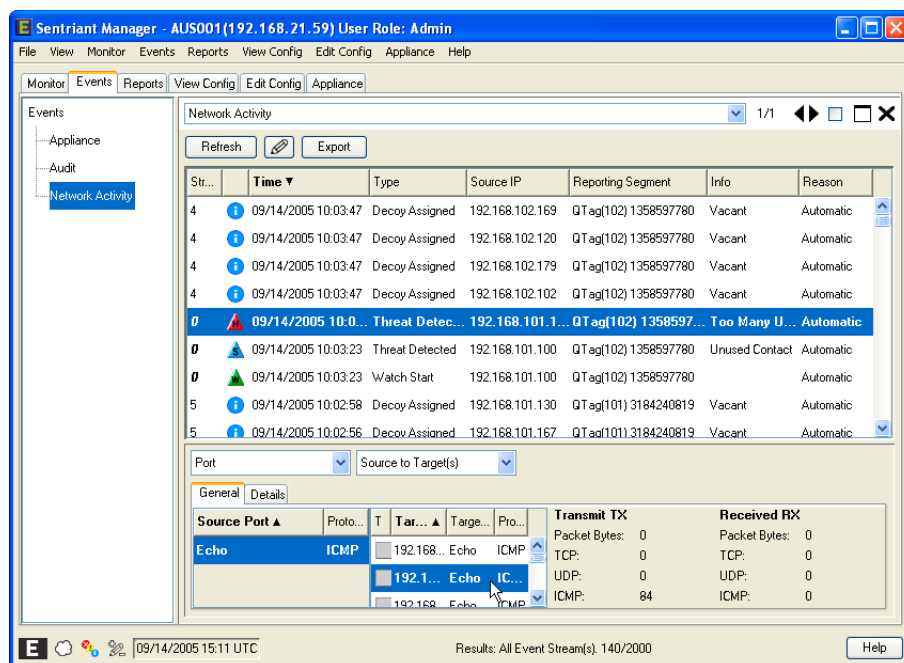
- 1 Select an event from the Events Panel.
- 2 Select **Port** from the Details Panel drop-down list.
- 3 Select a **Source Port** from the table.



The Time Based details panel is displayed.

To view Source to Targets:

- 1 Select an event from the Events Panel.
- 2 Select **Port** from the Details Panel drop-down list.
- 3 Select **Source to Targets** from the drop-down list.
- 4 Select a Source Port from the table.



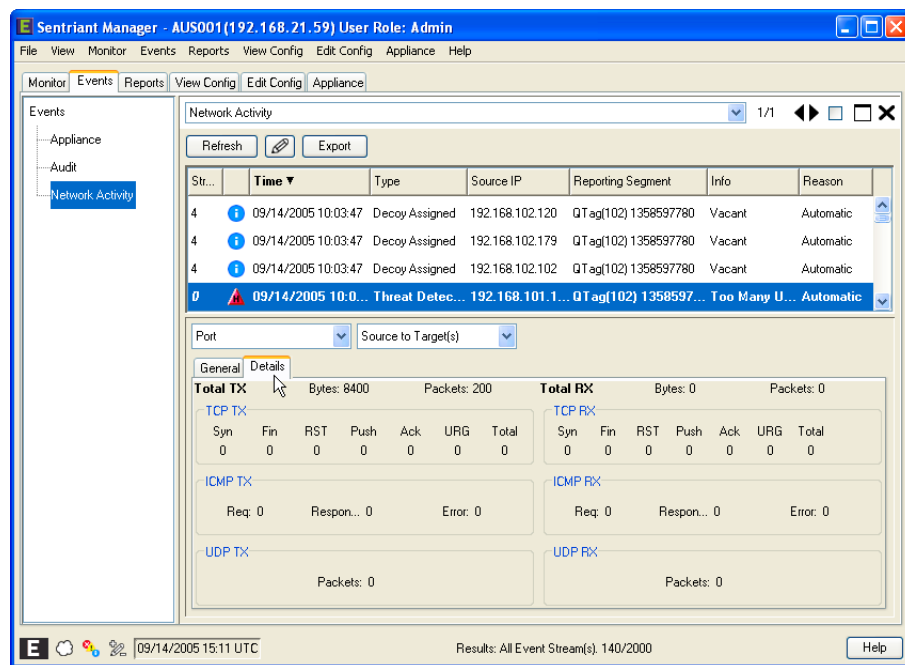
The port and the port's protocol type is displayed in the left-most table for the source IP Address. Selecting a Source Port displays the Packet Bytes transmitted and received. In addition, the bytes are broken down into the TCP, UDP and ICMP communication layers.

Selecting a row from the Source Port's table filters the target table.

Selecting a row from the Source Port's table, then selecting a row from the Target Port's table filters the TX and RX information.

To view Source to Target details:

- 1 From the **Port > Source to Target** details panel, select the Details tab.



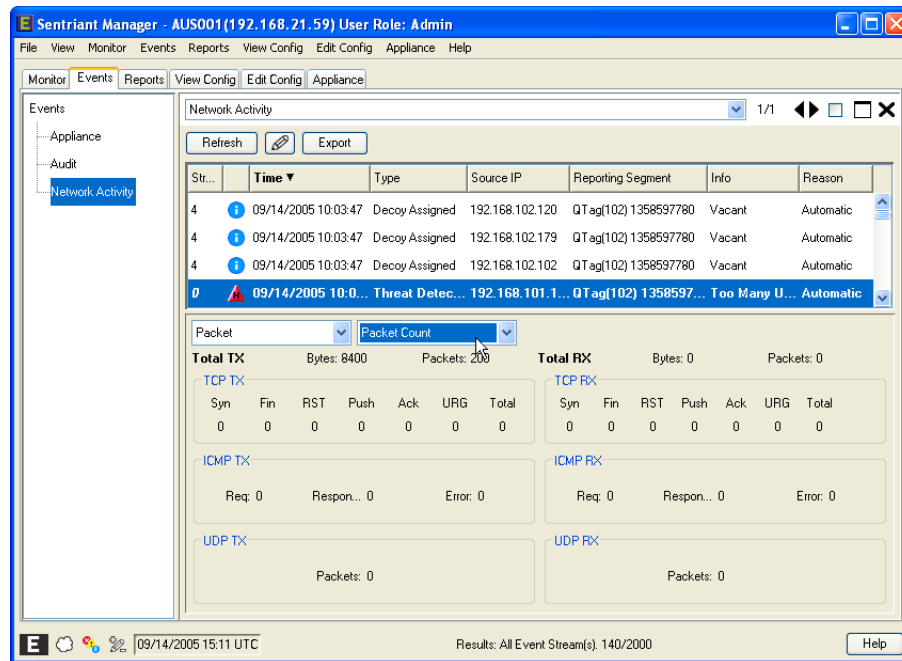
The traffic between the selected source and target are displayed showing the count of packet and bytes transmitted and received. In addition, the bytes are broken down into the TCP, ICMP and UDP communication layers.

Packet

The Packet panel contains specific packet information for the selected event. The total packet count for transmitted and received packet bytes is displayed and the packet count pair for each port type.

To view Packet Count:

- 1 Select an event from the Events Panel.
- 2 Select **Packet** from the Details Panel drop-down list.



The information displayed is the count of how many packets were sent from that selected Source IP to the selected Target IP. The information is displayed showing each packet relative to the communication layer where it was sent and received.

Totals are displayed across the top of the view for the number of bytes and packets transmitted and received and UDP.

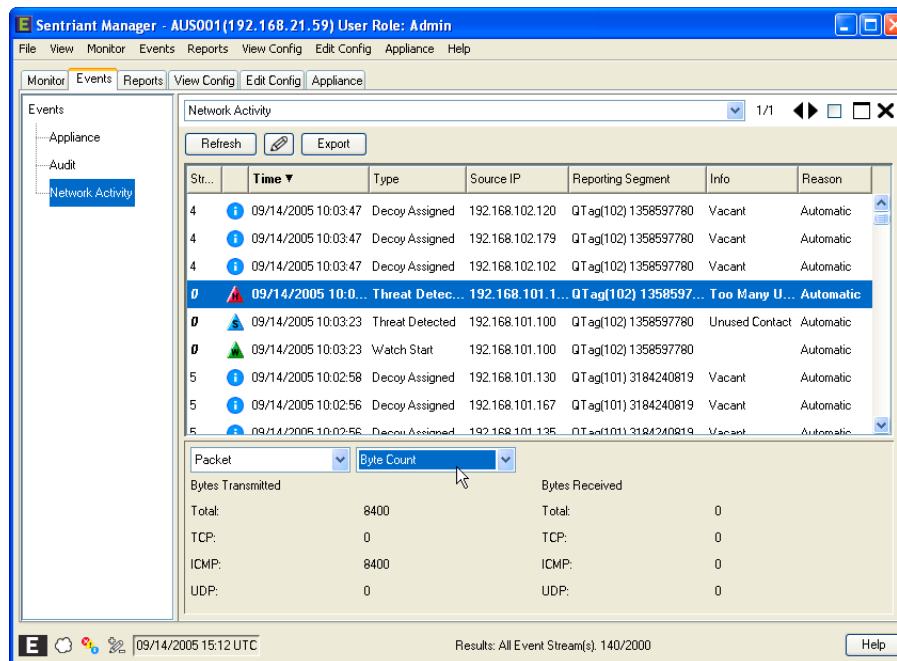
The second row of data shows the number of packets sent and received to the TCP header fields and a roll-up total for each.

The third row of data shows the number of packets sent and received to the ICMP layer for Requested, Response and Unread Destination packets and a roll-up total for each.

The last row of data shows the number of packets sent and received to the UDP header.

To view Byte Count:

- 1 Select an Event from the Newtork Activity Panel.
- 2 Select **Byte Count** from the Details view drop-down list.



The information displayed is the count of how many bytes were sent from that selected Source IP to the selected Target IP. The information is displayed showing each byte relative to the communication layer where it was sent and received.

Totals are displayed across the top of the panel view for the number of bytes transmitted and received.

The second row of data shows the number of bytes sent and received to the TCP header.

The third row of data shows the number of bytes sent and received to the ICMP header.

The bottom row of data shows the number of bytes sent and received to the UDP layer.

Threat

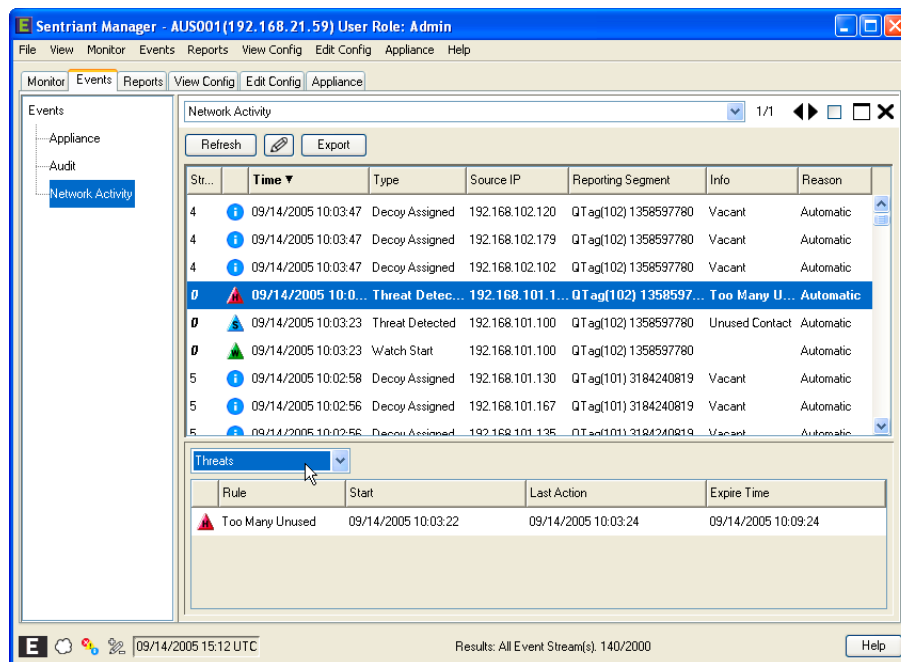
In the Events Panel, a threat is displayed for each instance a source triggered a rule. For example, a source triggers a medium threat and a high threat. The Events Panel will display each triggered rule event in the Detail View.

The administrator can dismiss threats by right-clicking a threat in the Details Panel and selecting Dismiss.

To view an Event's Threats:

- 1 Select an event from the Events Panel.
- 2 Select **Threats** from the Details Panel drop-down list.

All Threat Priorities, High, Medium, Low, and Suspect are displayed for the selected event.



Network Activity Events Actions

The following actions can be performed within the Events Panel. A right-click pop up menu contains the following actions:

- [Show Event Stream](#) - Filters the Network Activity Events Panel to a single communication stream of events
- [Lookup IP Address on the Web](#) - Opens a web browser to the various IP look up providers
- [IP Address Lookup](#) - A tool that returns the host name and IP Address of a source using the client's DNS
- [Select/Deselect All](#) - Selects/Deselects All source IP Addresses in the Events panel
- [View Network Activity Details Panel](#) - Displays the Details Panel
- [View Network Activity Targets Panel](#) - Displays a list of Targets when an event is selected

Show Event Stream

This view displays events for a single IP Address communication stream including all associated events. For example, a communication stream has a start and stop event and in some cases information and/or threat activity events.

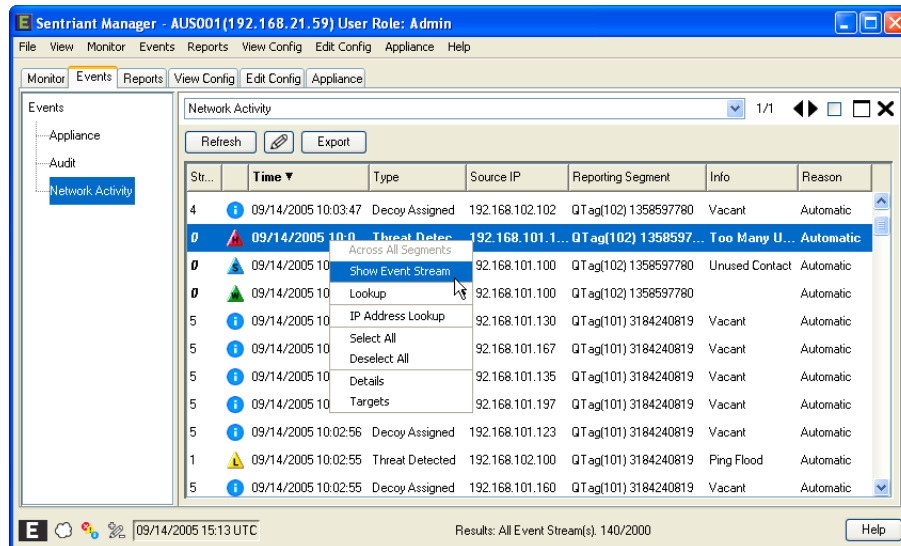


NOTE

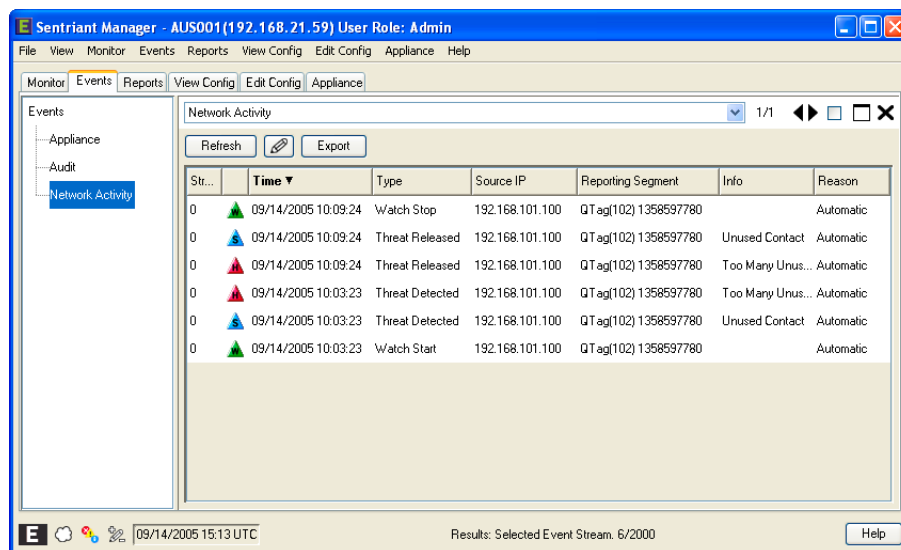
If an event stream only contains a start event, the communication stream is still active.

To show an Event Stream:

- 1 Select an event from the Network Activity Panel.
- 2 Right-click and select **Show Event Stream**.

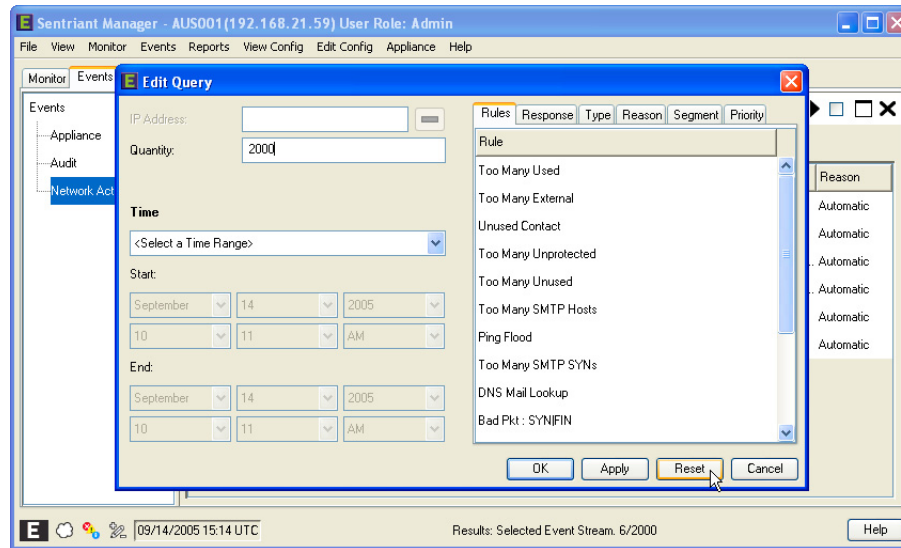


Only the events for the selected communication stream are displayed.



To redisplay all events:

- 1 Click the **Query** button.
- 2 Uncheck the **Limit results to current Event Stream** box.
- 3 Click **OK** to close the dialog and refresh the Network Activity Panel.



Lookup IP on the Web

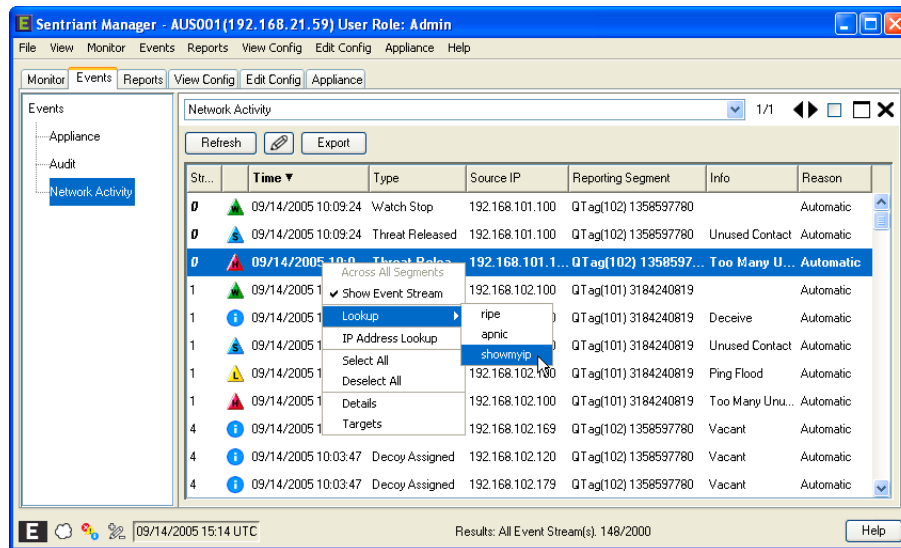
It may become necessary to look up the location of an IP Address to understand where it is coming from. Sentriant NG Manager's Lookup IP Address on the web tool contains all of the regional internet registry services. The Internet Registry services are:

- APNIC represents the Asia Pacific region, comprising 62 economies.
- RIPE represents a membership base of around 3,500 members. The RIPE NCC service region consists of more than 90 countries across Europe, the Middle East, Central Asia and African countries located north of the equator.
- ShowMyIP represents the entire world wide web. The website will look up an IP Address and give it's location along with other information.

The tool will direct you to the correct internet page and start the search of the IP Addresses location.

To look up an IP Address on the web:

- 1 Select an event from the Events Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Lookup** and then one of the registry services from the list.



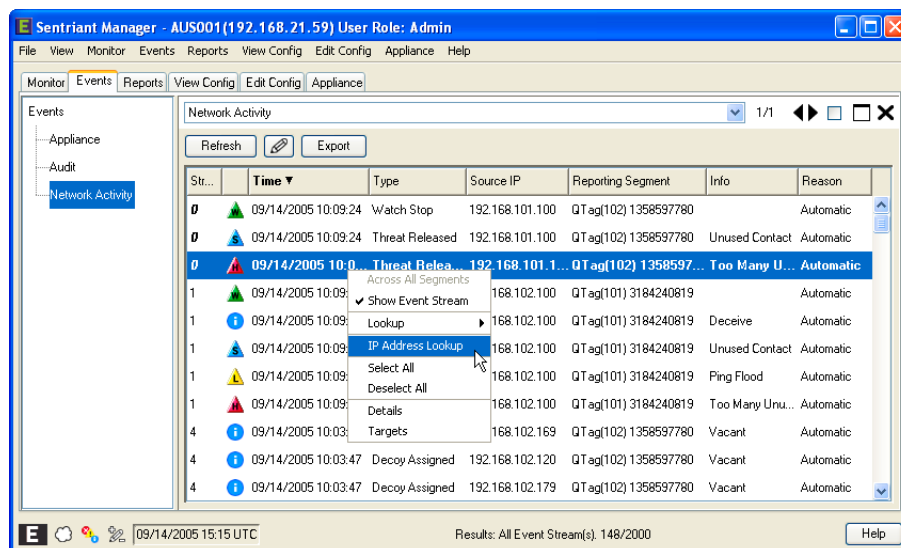
The selected IP Address is populated in the 'who is' section of the registry service. Search results are displayed for the selected IP Address. Each registry service displays results differently so review carefully.

IP Address Lookup

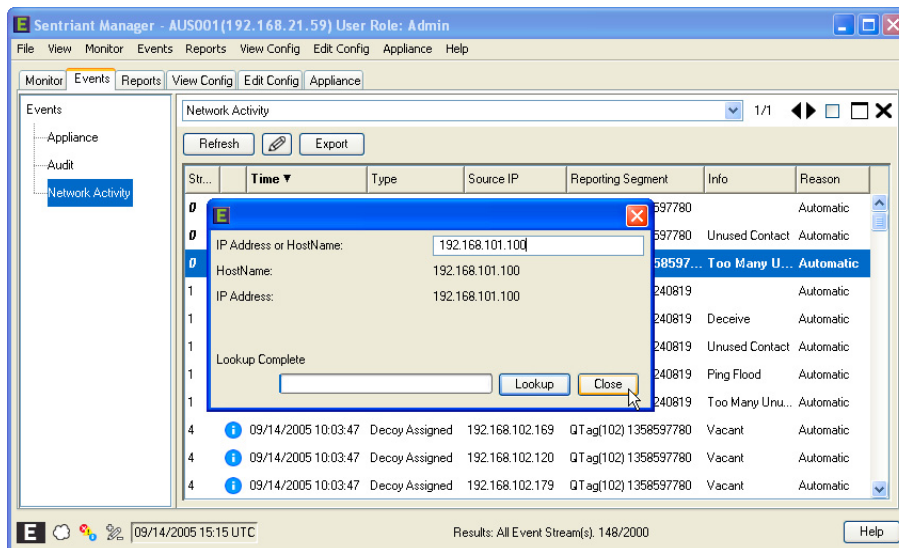
The IP Address Lookup tool will display the IP Address of an event's source and the HostName returned by the client's DNS.

To look up an event's source IP Address and HostName:

- 1 Select an event from the Network Activity Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select IP Address Lookup.



The HostName is displayed along with the IP Address. You may enter another IP Address or HostName in the IP Address or HostName field and click the Lookup button.

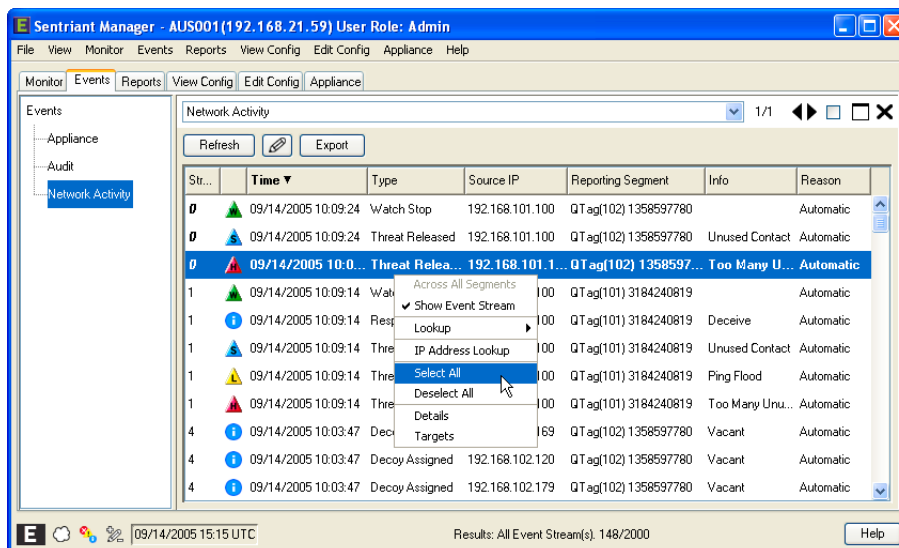


- 4 Click the **Close** button to return to the Network Activity Panel.

Select and Deselect Events

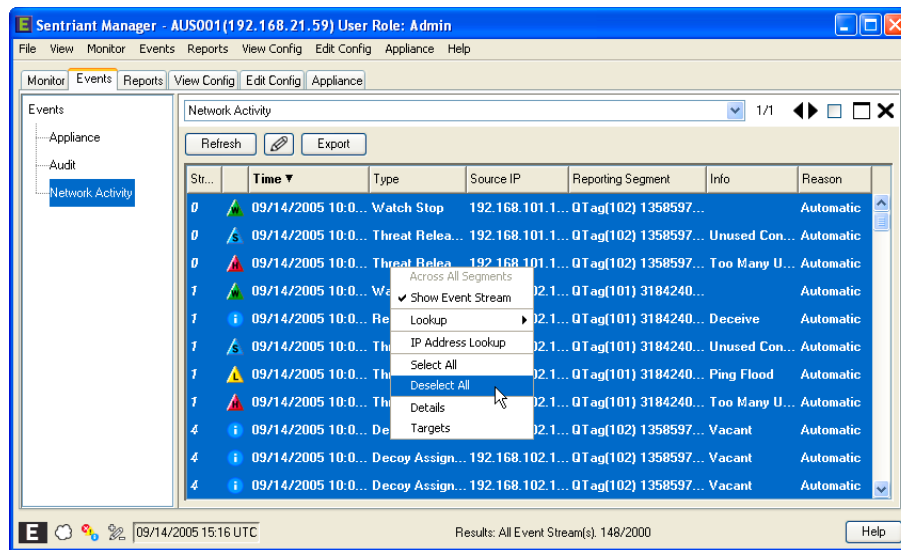
To select all events in the Network Activity Panel:

- 1 Select an event from the Network Activity Panel.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Select All**.

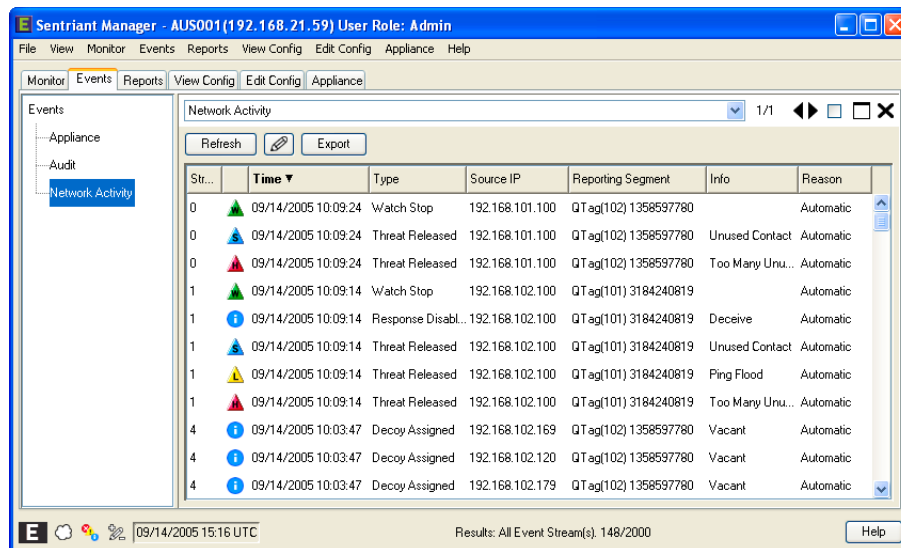


To deselect events in the Network Activity Panel:

- 1 Right-click in the Network Activity Panel to bring up the pop-up menu.
- 2 Select **Deselect All**.



All events are deselected.

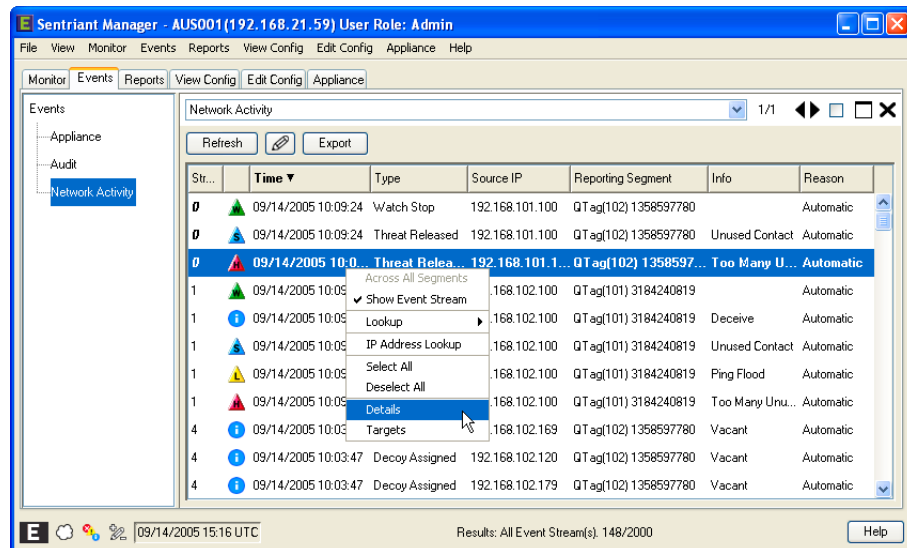


View Network Activity Details Panel

Details about events are displayed in the Events Details Panel.

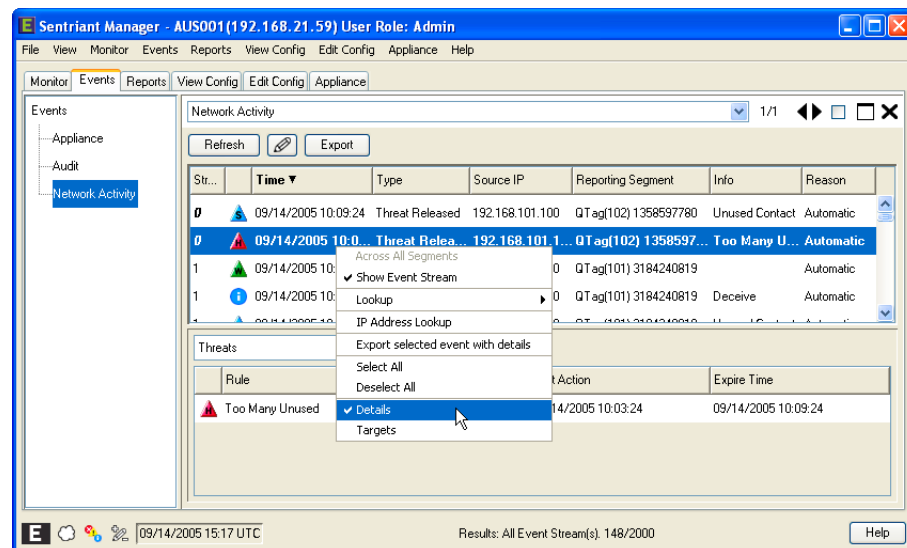
To activate the Network Activity Details Panel:

- 1 Select an event in the Network Activity Panel.
- 2 Right-click and select **Details**.



To close the Network Activity Details Panel:

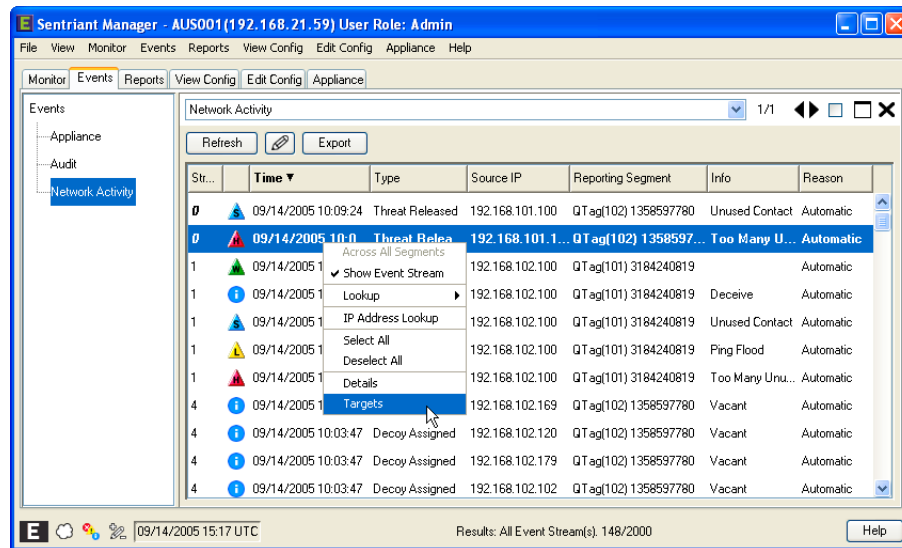
- 1 Right-click in the Network Activity Panel to bring up the pop-up menu.
- 2 Deselect **Details**.



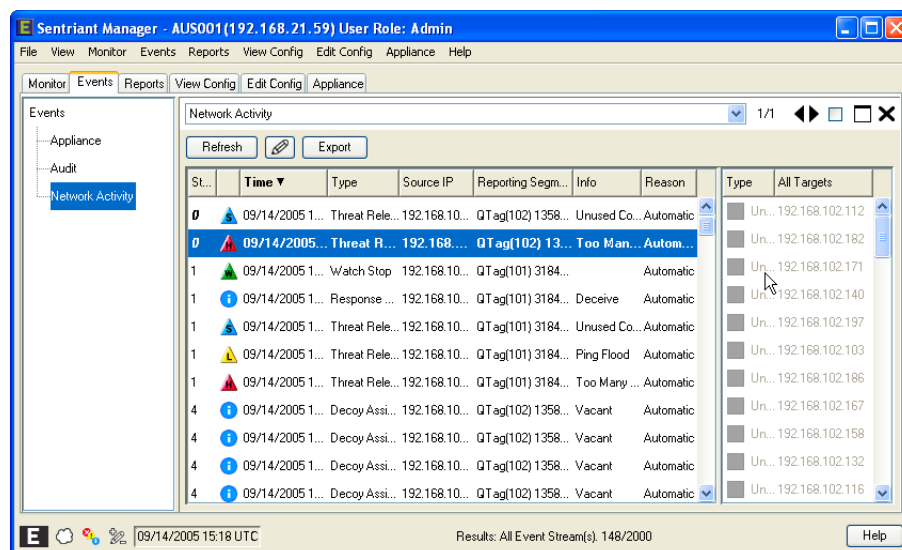
View Network Activity Targets Panel

To view the IP Addresses of targets affected by the source:

- 1 From the Sources Panel, select the row of any **Source IP Address**.
- 2 Double-click on the target or right-click to bring up the pop-up menu.
- 3 Select **Targets**.



The Target IP table on the far right of the screen is populated with all contacted targets.



To close the Network Activity Targets panel:

- 1 Select an event in the **Network Activity** Panel to bring up the pop-up menu.
- 2 Deselect **Targets**.

Sentriant Manager - AUS001(192.168.21.59) User Role: Admin

File View Monitor Events Reports View Config Edit Config Appliance Help

Monitor Events Reports View Config Edit Config Appliance

Events

- Appliance
- Audit
- Network Activity

Network Activity

Refresh Export

St...	Time	Type	Source IP	Reporting Segm...	Info	Reason	Type	All Targets
0	09/14/2005 1...	Threat Rele...	192.168.10...	QTag(102) 1358...	Unused Co...	Automatic		Un... 192.168.102.112
0	09/14/2005 1...	Threat B...	192.168...	QTag(102) 13...	Too Man...	Autom...		Un... 192.168.102.182
1	09/14/2005 1...	Lookup		QTag(101) 3184...		Automatic		Un... 192.168.102.171
1	09/14/2005 1...	IP Address Lookup		QTag(101) 3184...	Deceive	Automatic		Un... 192.168.102.140
1	09/14/2005 1...			QTag(101) 3184...	Unused Co...	Automatic		Un... 192.168.102.197
1	09/14/2005 1...			QTag(101) 3184...	Ping Flood	Automatic		Un... 192.168.102.103
1	09/14/2005 1...			QTag(101) 3184...	Too Many ...	Automatic		Un... 192.168.102.186
4	09/14/2005 1...			QTag(102) 1358...	Vacant	Automatic		Un... 192.168.102.167
4	09/14/2005 1...	Decoy Assi...	192.168.10...	QTag(102) 1358...	Vacant	Automatic		Un... 192.168.102.158
4	09/14/2005 1...	Decoy Assi...	192.168.10...	QTag(102) 1358...	Vacant	Automatic		Un... 192.168.102.132
4	09/14/2005 1...	Decoy Assi...	192.168.10...	QTag(102) 1358...	Vacant	Automatic		Un... 192.168.102.116

09/14/2005 15:18 UTC Results: All Event Stream(s). 148/2000

Help

Reports

The Sentriant NG appliance lets you define the timing and contents of reports for system overview activity and enhanced threat and audit reporting.

From the Reports panel you can select a daily or weekly **System Overview Report** of activity on one or all network segments over a specified time period.















The System Overview Report summarizes the condition of the Extreme Security Fabric over the reporting period for the following categories:

- System Availability
- Overall Session Activity
- Overall Suspect and Threat Trend
- Per-Segment Suspect and Threat Trend

System Overview Report

Using the Toolbar

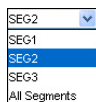
The following functions are available in the Toolbar:

-  Save the System Overview Report
-  Print the System Overview Report
-  Refresh the screen with existing parameters
-  Go to first page
-  Go to previous page
-  Go to next page
-  Go to last page
-  Set to actual size
-  Fit to page
-  Fit to width
-  Zoom in
-  Zoom out
-  Set zoom ratio
-  Refreshes screen after modifying parameters

Specifying Report Parameters

To specify segment(s) and time period:

- 1 From the Segment(s) pull-down menu, select the desired segment or **All Segments** to create reports for all segments in the group.



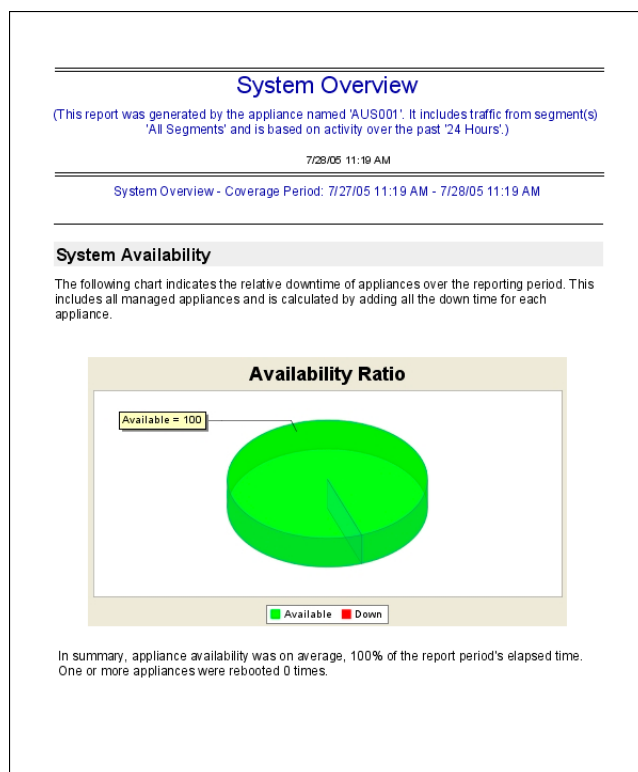
- 2 From the Period pull-down menu, select **24 hours** or **1 week**.



- 3 The reports are displayed. To view each report, click on the **Next Page** button. Below is an example of each report.

System Availability Report

The System Availability Report displays the ratio of up-time and down-time for all Sentriant NG appliances within the fabric over the reporting period. The reporting period is either 24 hours or 1 week.



Overall Session Activity Report

The Overall Session Activity Report displays a ratio of the number of session or watch occurrences to the total number of suspect and threat occurrences detected within the reporting range, either 24 hours or 1 week.

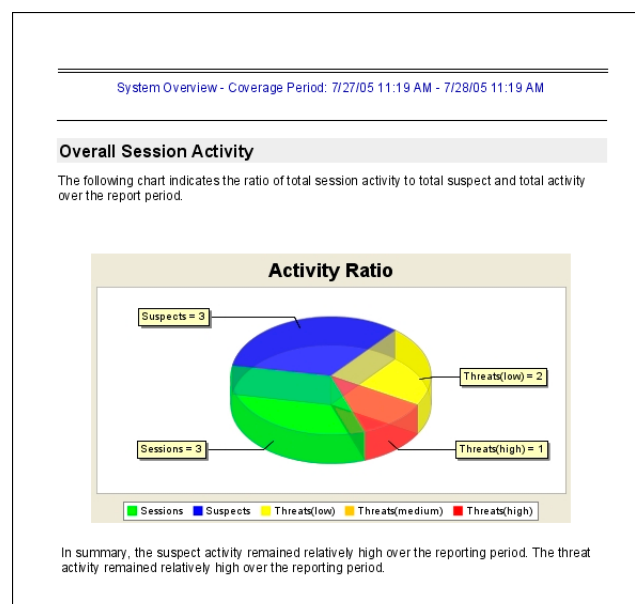
An occurrence is identified as the aggregate number of watches, suspects or threats. For example, a source triggers a threat rule. That is counted as one threat occurrence. If the same source threat times out and is detected again, that threat is again counted. The report will aggregate the total and display it in the graph.

The reporting period maintains the total number of aggregates for all Sentriant NG appliances within the fabric.



NOTE

The Status Bar, which also displays watches, suspects, and threats does not show an aggregate. It displays the number of unique sources that have triggered a watch, suspect or threat rule.



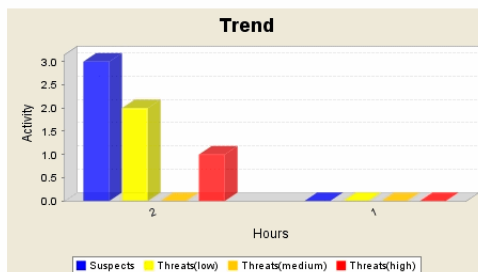
Overall Suspect and Threat Trend Report

The Overall Suspect and Threat Trend Report displays a ratio of the number of suspect and threat occurrences detected within the reporting range, either 24 hours or 1 week. The total is identified as the aggregate number of suspects and threats.

System Overview - Coverage Period: 7/27/05 11:19 AM - 7/28/05 11:19 AM

Overall Suspect and Threat Trend

The following chart indicates the total suspect and threat activity trend over the reporting period. The values are cumulative for each tick on the horizontal scale. In the case of a weekly report, each day tick value represents the total activity arrival count over that day. Similarly, each hour tick in the daily report represents the total activity arrival count over the hour.



In summary, suspect activity has decreased since the beginning of the reporting period. The threat activity has decreased since the beginning of the reporting period.

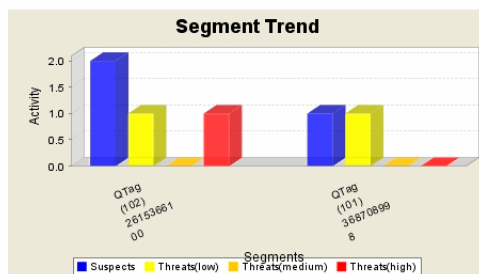
Per-Segment Suspect and Threat Trend Report

The Per-Segment Suspect and Threat Trend Report displays a ratio of the number of suspect and threat occurrences detected within the reporting range, either 24 hours or 1 week broken down for each segment. The totals are identified as the aggregate number of suspects and threats for each segment within the fabric.

System Overview - Coverage Period: 7/27/05 11:19 AM - 7/28/05 11:19 AM

Per-Segment Suspect and Threat Trend

The following chart indicates the suspect and threat activity trend for each segment and over the reporting period. The values are the total activity arrival count values for each segment over the reporting period.

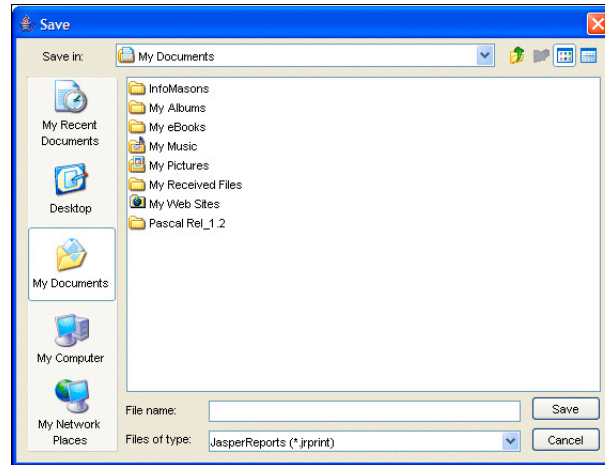


In summary the segment with the most suspect activity is segment 'QTag(102) 2615366100'. The segment with the most threat activity is segment 'QTag(102) 2615366100'.

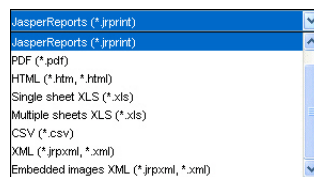
Saving the System Overview Report to a File

To save the Report to a file:

- 1 In the toolbar, click the **Save** button.



- 2 In the Save in pull-down menu, specify a file location.
- 3 In the File name field, enter a file name.
- 4 In the Files of type pull-down menu, select one of the following file types, then click **Save**.



Enhanced Reporting

The Sentriant NG Manager provides enhanced reporting about threats and audit history that are delivered via email. Reports are generated at midnight and delivered in .csv or HTML format to a selected email address once per day or week.

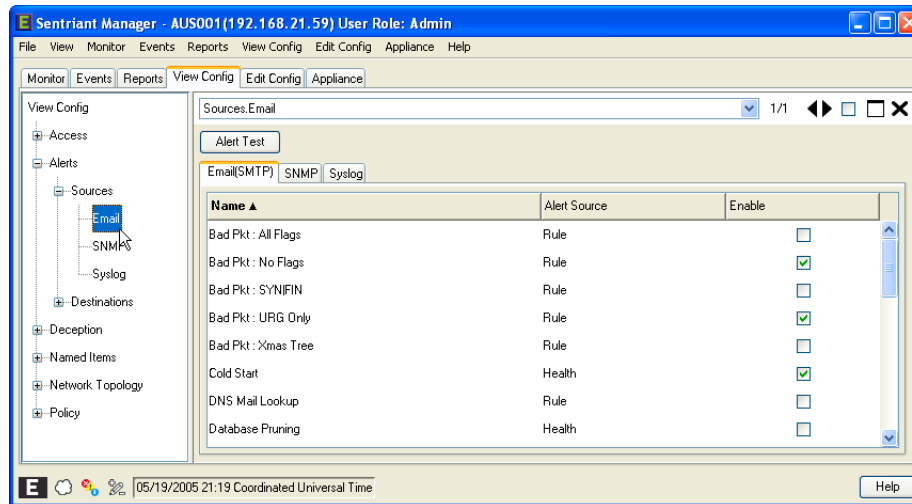
- The *information* used for these reports can be viewed in the Sentriant NG Manager under the Events tab as Audit and Network Activity.
- The *following reports* cannot be viewed in the Sentriant NG Manager. They are only available via email or as archives on the appliance. A user with sufficient privileges (admin/root) can access the archives of the reports on the appliance.

Following is an example of how these reports can be activated as an SMTP Alert Source:

- 1 From **Edit Config > Alerts > Sources > SMTP**, specify the **Alert Name** as Daily Reports.
- 2 Specify the **Alert Source** as Reporting.
- 3 Save the Configuration by clicking the **Configuration Changed** icon at the bottom left of the screen.

When the configuration is exported, the SMTP locations and values are included in the export.

Following is an example of the activation page:



Threat Report

A Threat Protection Status report breaks down the threats and responses that have occurred on the network. This report can be used to examine the most recent 24-hour period of activity on the Sentriant NG appliance. The reports can be scheduled to be delivered in .csv or HTML format to a selected email address once per day or week.



NOTE

This report may be quite large, so be sure to enter an email address that can handle large SMTP content.

The header contains title, date range, name, and the IP Address of the Sentriant NG generating the report. The threat report contains the following groupings:

- Threat Breakdown and Response Breakdown contain overall counts of each unique threat and response by rule name and response type.
- Threats by Segment groups the threats by segment and by threat roll up, indicating all threats within the named segment.
- Threat Sources displays the IP Address, MAC address, rule name, and number of times that the rule was triggered.
- Advisory note cautions that although there might have been no *new* threats in the last 24 hours, consult the Sentriant Manager to determine whether there still are old or existing threats.

Following is an example of a daily HTML threat report that can be received by email:

Extreme Networks Sentriant NG Daily Top Offender Report for 2008-02-22 Sentriant: c245 - 10.25.0.245 - 2.5.0-5458				
Threat Breakdown			Response Breakdown	
Threat	Level	Count	Response	Count
Unused Contact	Suspect	1	Track	1
Threats by Segment				
Segment	Threat	Level	Count	
Kevin-450-20x	Unused Contact	Suspect	1	
Threat Sources				
IP Address	MAC Address	Threat	Level	Count
20.0.172.241	00:04:96:26:60:2B	Unused Contact	Suspect	1
For the latest Threat Data always consult the Sentriant Manager				

Audit Report

An Audit report shows who logs into the Sentriant NG appliance and who alters system configuration. This report can be used for audit trail history and compliance of changes made to the Sentriant NG appliance.

The header contains the title, date range, name, and IP Address of the Sentriant NG appliance generating the report. Columns indicate date, audit message, and the user performing the action. The report includes both interactive and batch logins.

Following is an example of a daily auditing report that can be received by email:

Extreme Networks Sentriant NG Audit Report for 2007-10-25 Sentriant: extremenare 10.35.10.38		
Audit Events		
Date	Message	User
10/29/2007 11:16:03	Configuration exported	admin
10/29/2007 11:16:03	Configuration import successful	admin
10/29/2007 11:16:03	Object Container ConfigChangeEnd modified to false	admin
10/29/2007 11:16:03	Personality Set Default Personalities modified to [1451959169, 63947589, 1256199272, 328222029]	admin
10/29/2007 11:16:03	Personality Set Default Percentages modified to [0, 25, 50, 25]	admin
10/29/2007 11:16:03	Object Container ConfigChangeStart modified to true	admin
10/29/2007 11:16:03	Configuration import attempt	admin
10/29/2007 11:15:28	Configuration exported	admin
10/29/2007 11:15:28	Configuration import successful	admin
10/29/2007 11:15:28	Object Container ConfigChangeEnd modified to false	admin
10/29/2007 11:15:28	Rule RuleA.MNRuleChain 2916354027 - Function Action Count Exceeded 2256879566 Parameters modified to 6	admin
10/29/2007 11:15:28	Object Container ConfigChangeStart modified to true	admin
10/29/2007 11:15:27	Configuration import attempt	admin
10/29/2007 11:14:17	Configuration exported	admin
10/29/2007 11:14:17	admin logged in 10manare/10.25.0.38	Appliance
10/29/2007 11:14:11	LOGIN_SUCCESS: admin by Shell GUI or SCP or SSH command [remote: 10.25.0.5]	Appliance
10/29/2007 11:14:11	LOGIN_SUCCESS: admin by Shell GUI or SCP or SSH command [remote: 10.25.0.5]	Appliance
10/29/2007 11:10:01	LOGOUT: mirage by su.	Appliance
10/29/2007 11:10:00	LOGIN_SUCCESS: mirage by su.	Appliance
10/28/2007 23:10:00	LOGOUT: mirage by su.	Appliance
10/28/2007 23:10:00	LOGIN_SUCCESS: mirage by su.	Appliance

View Configuration

The View Configuration (View Config) panels display the Sentiariant NG appliance current configuration. The purpose of the configuration view is to display a “snapshot” of the Sentiariant NG appliance configuration before changes are made by an administrator. This allows the administrator to review current configuration parameters before new changes are persisted to the Sentiariant NG appliance.

Alert tests are conducted from the Alerts Panel. Alert tests can be performed on E-mail (SMTP), SNMP, and Syslog. The alert test confirmation is sent to the **Events > Appliance** Panel.

The View Config panels of the Sentiariant NG Manager display the following configuration information:

Access - users, privileges, and the workstation IP Addresses of users

Alerts - E-mail, SNMP, and Syslog alerts and recipients of alerts

Deception - decoy personalities and distributions to specific IP Addresses

Named Items - information that can be applied and reused when configuring Segment and Policy settings

Network - configure network topology including Segments, Segment Sets and the Sentiariant NG appliance

Policy - configure rules used to detect and mitigate malicious network behavior and create Rule Sets to apply to Segment Sets

Access

User Configuration

Sentiariant NG Manager is installed with a default configuration for one user with the user name “admin” so that the system administrator can access Sentiariant NG Manager and create the initial set of users. The admin can then grant security settings to selected users for subsequent configuration changes.

The following table summarizes Sentiariant NG Manager’s default groups. The admin can modify or delete the users at any time.

Table 5: Default User Table

User Name	Capabilities
Admin	Can fully administer the system
Operator	Can perform mitigation operations and change E-mail and password Cannot perform configuration activities

Table 5: Default User Table

User Name	Capabilities
Observer	Can only view operations and change their E-mail and password Cannot perform mitigation activities Cannot perform configuration activities

Client Configuration

It is necessary to specify which clients will be connecting to Sentriant NG Manager in an administrative role. A client is defined as the IP Address of the PC running Sentriant NG Manager.



NOTE

In the case of multi-homed PCs, all relevant IP Addresses must be added as a client.

On initial installation, a client is specified for the default administrator. The Clients screen defines additional IP Addresses that are allowed to administer the Sentriant NG Manager.

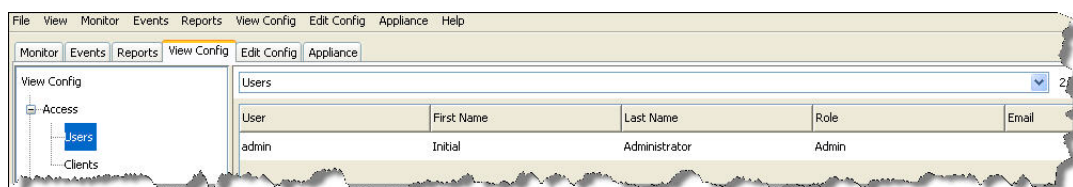


NOTE

After adding IP Addresses to the Access Clients list, you may wish to add those IP Addresses to the Exceptions screen and set the Mitigation Modifiers to Never Cloak. This will prevent the administrator from losing contact with Sentriant NG Manager should the Access Client be declared a threat. While this action reduces the level of network security to a degree, it provides the benefit of ensuring the uninterrupted access to the Sentriant NG Manager.

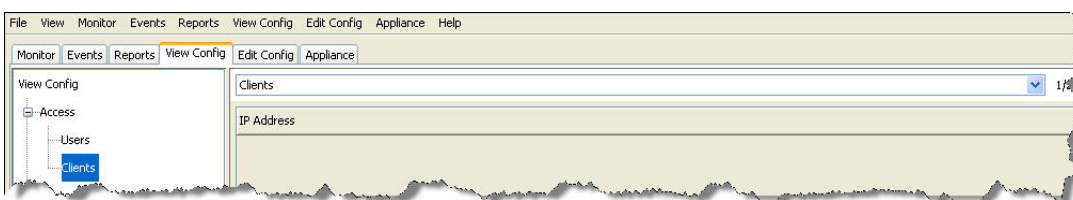
User Accounts

The Users panel is used to create and delete user accounts.



Clients

The Clients panel is used to add and delete users' workstations as clients to the Sentriant NG appliance. IP Addresses are used to identify the workstation.



Alerts

The Sentiart NG appliance can be configured to send alerts notifying the administrator that threat behavior has been detected. To send alerts, destinations must first be configured and sources selected. [Sources](#) or rules are what triggers the alerts to be sent. [Destinations](#) need to be defined for each type of alert. The types of alert vehicles are:

E-mail

The Sentiart NG appliance generates E-mail messages and sends them to a single destination mail server. The server address is configured in the Sentiart NG Manager, as well as each destination's e-mail address. The destination mail server must be configured to receive relay messages from the Sentiart NG appliance's management IP Address. E-mail messages are queued and delivered as resources are available.

SNMP

A single MIB defines the Extreme alert information block. The MIB can be downloaded through the Sentiart NG appliance's UI. The Extreme SNMP message is an enterprise trap that is registered with **IANA**. The Extreme enterprise number is 13693. (See iana.org for more information about enterprise numbers and registration.)

Currently, the Extreme Sentiart NG appliance MIB is importable into any SNMP enterprise-enabled workstation that supports SNMP v.1. SNMP messages are queued and delivered as resources are available. The SNMP trap monitor addresses are configured in the Sentiart NG appliance's UI.

Syslog

The Sentiart NG appliance generates messages that are sent to log files and records them to a specified location on a server or work station. The destination must be configured to receive the data and write to the Syslog recorder. The recording system may record these in any desired manner including writing them to a file, sending them on to other systems, and printing them out.

Destinations

The Destinations panel identifies the destination to which the alert will be sent. The destination is comprised of two parts, the user or recipient and the IP Address of the server or workstation that will receive the message. For example, an alert is created that sends an email message to johndoe10@Extremenetworks.com on server 10.10.1.1.



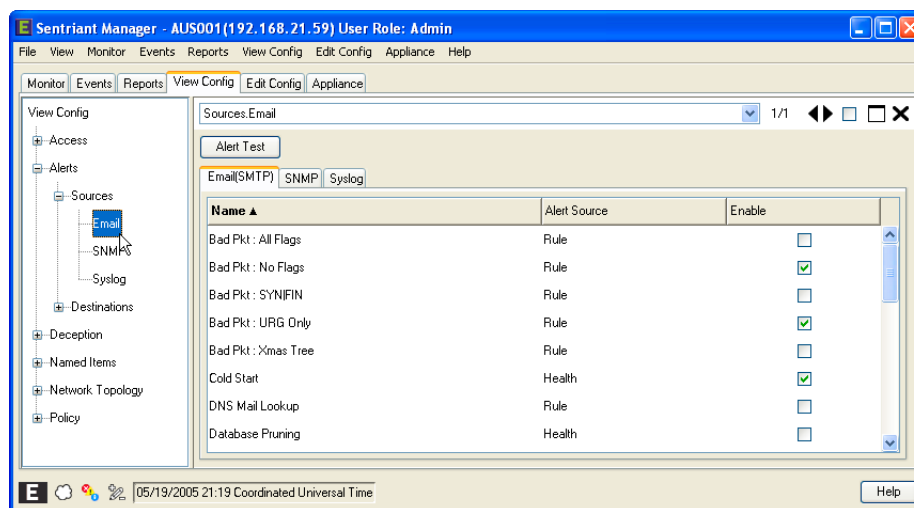
Sources

Alerts are set by selecting from a list of rules. An alert can have each type selected (E-mail, SNMP, Syslog). Pre-configured messages are then sent to various systems.

From the Sources panel, you can perform a test for the alert destinations to determine if each is valid.

To perform an Alert test:

- 1 From **View Config > Alerts**, select **Sources**.
- 2 Select one of the source types, E-mail, SNMP or Syslog. (The default panel that is displayed is E-mail.)



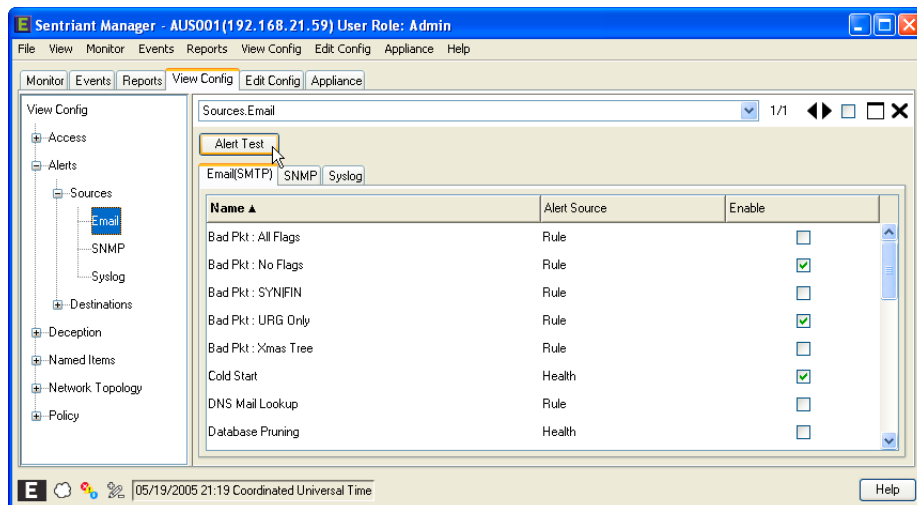
A list of rules is displayed with Name, Alert Source and Enable check box for each rule.



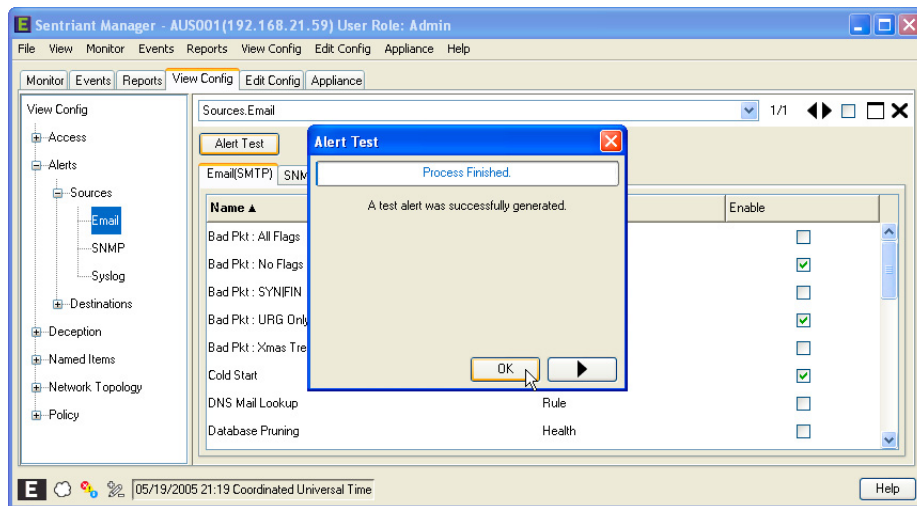
NOTE

This panel is read-only and represents the current configuration residing on the Sentriant NG appliance.

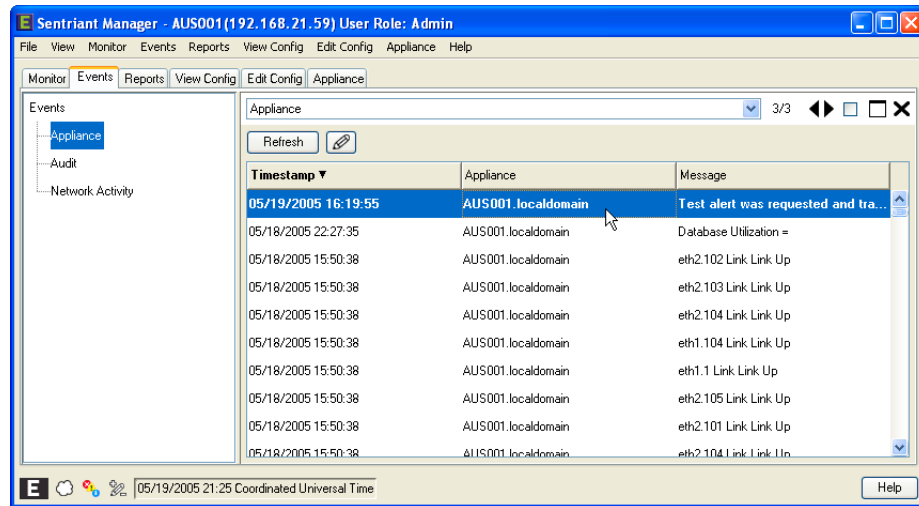
- 3 Click the **Alert Test** button to test that source destinations are valid.



Upon completion, the following dialog is displayed.



- 4 Click **OK** to close the dialog.
- 5 Clicking on the **Arrow** button will bring up the Events Panel showing that the Alert Test has completed and the request was transmitted.



Deception

The Sentriant NG appliance can take advantage of IP Addresses that are not used by any hosts (unused address space) to present a deceptive view of the network to attackers. For a percentage of unused address space, the Sentriant NG responds as though real computers were using the address space effectively creating decoys on the network to draw in would-be attackers. These decoys can behave as though they are specific devices running specified operating systems called Personalities.

Unused address space can be configured as a collection of non-hosts, Linux hosts, Windows XP hosts, or Windows 98 hosts. In addition, the administrator can customize not only the emulated operating system for a virtual host, but also the open TCP and/or UDP ports on the host.

Deceptive responses can be configured to inhibit an attacker. The administrator can utilize provided Example [Personalities](#) or create customized Personalities. The Deception Panel allows the creation and modification of Personalities and to view the way Personalities will be utilized within the Unused address space.

Once a Personality or group of Personalities has been created, a [Personality Set](#) is created containing a Personality or multiple Personalities. A Personality Set is then assigned to individual Segments and deception is started. Distribution for each Personality can be set at various percentages that send out that Personality when a threat is detected on the unused address space.



NOTE

Deception can only be utilized to respond to attempts to contact Unused IP Addresses. Deception is not utilized to hide existing Used IP Addresses.

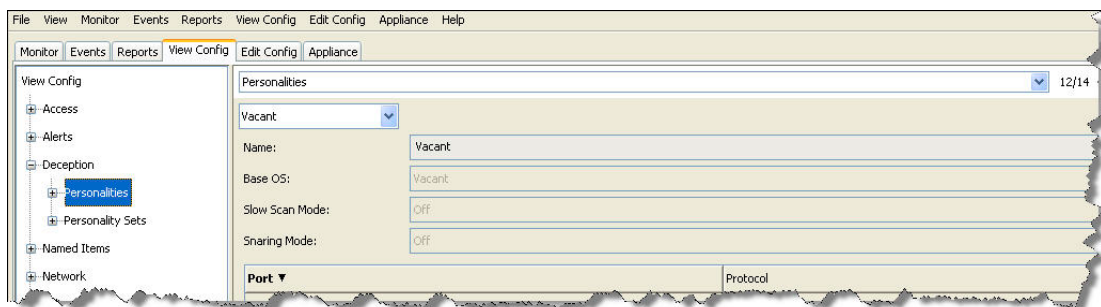


NOTE

Deception must be turned on and a Distribution assigned to the Segment.

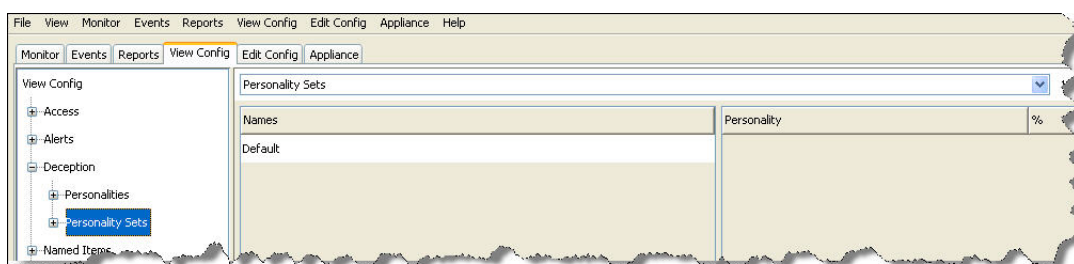
Personalities

The Personalities panel is used to create and delete personalities.



Personality Sets

The Personality Sets panel is used to create and delete personality sets.



Named Items

Named Items are groups or sets of information that can be applied and reused when configuring Segment and Policy objects without the need to re-enter data. For example, in a large environment containing several Sentriant NG appliances monitoring 10, 12, or more Segments, it would be time consuming to enter all the Segment IP Addresses for deception, never cloak, deceive and other related IP Address settings for Segments, Segment Sets, and Policies. Upon completing configuration for one Sentriant NG appliance, the Named Items can be exported to the other appliances and applied. Benefits of creating Named Items include:

- Completing environment settings quickly with fewer errors
- Sets can be applied to added Sentriant NG appliances.
- Updates made to the named sets are automatically applied to respective configuration settings

There are three Named Item sets. Each set is based on the type of information and how it will be utilized by the Sentriant NG appliance during monitoring, detection and mitigation actions. These sets are:

IP Sets - contain an IP Address or collection of IP Addresses

Port Sets - contain a Port number and Port protocol or collection of Port numbers and a Port protocol

Traffic Sets - contain a collection of five (5) pieces of data that defines a traffic item which specifies Source and Target traffic monitored by the Sentiariant NG appliance

IP Sets

Each IP Set is given a unique name and then IP Addresses are added to the set. An IP Address can be added per line or multiple IP Addresses may be added a line at a time. A line can be a single IP Address or wildcards may be used. For example, to select the entire range of IP Addresses use an asterisk (*). You may also specify ranges for an octet of the IP Addresses. You can use commas (,) and dashes (-) for multiple ranges. For example (192.168.21,23.* or 192.168.25.1-254).

Named IP Sets are used to populate the following configuration parameters:

- **Edit Config > Network Activity > Segment Sets > Policy-Deception > Excludes from Rule Responses**
- **Edit Config > Network Activity > Segments > Deception**
- **Edit Config > Named Items > Traffic Sets**

Port Sets

Each Port set is given a unique name and then Port numbers and Port protocol is added a line at a time. A line can be a single Port number or wildcards may be used. For example to select a range of Port numbers use commas(,) or dashes (-) for multiple ranges. For example (1,2,23,112 or 1-119, or 1,2,3,100-200).

When creating a Port Set with multiple Port numbers, you may only select one Port protocol. For example, a Port Set is created containing port numbers 3, 4, 56-200. The Port protocol can either be UDP or TCP.

Named Port Sets are used to populate the following configuration parameters:

- **Edit Config > Deception > Personalities > Ports**
- **Edit Config > Named Items > Traffic Sets**

Traffic Sets

A traffic item may contain only one piece of data to be considered a complete. For example, you may create a traffic item with only one Source IP Address and the Port protocol.

Each Traffic set is given a unique name and then Source and/or Traffic IP Addresses, Port numbers and a Port protocol is added a line at a time.



NOTE

Traffic Sets are created using IP Sets and Port Sets.

Named Traffic Sets are used to populate the following configuration parameters:

- **Edit Config > Network > Segment Sets > Policy-Deception > Omit**

- **Edit Config > Network > Policy > Rules > Include**
- **Edit Config > Network > Policy > Rules > Exclude**

Network

On initial install, the Sentriant NG appliance will monitor traffic on its Ethernet ports (and trunks) to determine the range of Segments it can access. This information is made available to the user via the **Configure > Network > Segments** page. It is necessary for the administrator to edit the supplied information and enable the Segment for monitoring.

A Segment Set is a collection of Segments that exhibit similar policy behaviors. For example, if a Segment Set is reserved for DHCP clients (laptops), then a set can be created containing all laptops within a Segment and then parameters can be set for rules, deception distributions and modifiers. Creating Segments is accomplished using the Segment Assistant.

A default Segment Set is created initially. All discovered or unconfigured Segments will be added to the default set and can later be moved to newly created Segment Sets.

Before a Segment can be monitored by the Sentriant NG appliance, the ports must be enabled. The Segments Panel and Physical Panel contain port information in two formats. The Segment Panel displays logical ports relative to the Segment. The Physical Panel displays information with a hierarchy starting with the Sentriant NG appliance to the physical ports to the logical ports. Segment information is also displayed at the logical port level.

The Network panel contains detailed areas showing specific information under each tab. These tabs are as follows:

- **Segments** - Create and manage Segment Sets and logical ports.
- **Segment Sets** - Create and assign Segments to a set.
- **Physical** - Manage Sentriant NG appliances, physical and logical ports.

Segments

A Segment is a collection of IP Address for each logical network port, the Sentriant NG appliance begins monitoring a contiguous range of addresses on each of the Segments. This range can be further refined by configuring the Protected Ranges for each logical Segment.

Traffic to and from any address in this range is analyzed for behavioral patterns consistent with suspect or threat activity. Unlike host resident security solutions, the Sentriant NG appliance is able to take into account network behavior across entire Segments for a more comprehensive threat analysis.

Segment Sets

A Segment Set is a collection of Segments that exhibit similar policy behaviors. For example, if a Segment Set is reserved for DHCP clients (laptops), then a set can be created containing all laptops within a Segment and then parameters can be set for rules, deception distributions and modifiers. Creating Segments is accomplished using the Segment Assistant.

A default Segment Set is created initially. All discovered or unconfigured Segments will be added to the default set and can later be moved to newly created Segment Sets.

Appliance

The Appliance Tab represents the network topology from a physical point of view starting with the Sentriant NG appliance and then each physical port on the Sentriant NG appliance followed by configured VLANs in the broadcast domain. A broadcast domain contains network Segments where all network devices communicate with each other without going through a router.

From the Appliance screen, you can do the following:

- View Sentriant NG appliance's name, state, IP Address, Gateway, and Subnet Mask
- View Physical Port's name, states, the Sentriant NG appliance where it resides, port delay, MAC Addresses, and read-write state
- View Logical Port's name, state, Segment name, the Sentriant NG appliance where it resides, MAC Addresses, read-write state, and the logical port it is paired with

Policy

The Sentriant NG appliance provides a rules-based engine to detect behavioral patterns that do not reflect normal network traffic. Typically, rules are created and then added to a Rule Set and the Rule Set is assigned to a Segment Set.

A **Rule** is made up of two components: defining the type of rule (i.e., host, port, traffic) and then setting rule detection and response parameters.

A **Rule Set** is a collection of rules configured specifically for the type of network Segments to be monitored. Rule Sets are assigned to Segment Sets that are monitored by the Sentriant NG appliance.

When a Rule Set is added to a Segment Set it affects all IP Addresses within the Segment Set's range. However, the administrator can exclude specific IP Addresses and/or ranges of IP Addresses by adding the addresses to the Policy Panel found under the **Configure > Segment Sets > Policy** tab.

Rules

Rules are what drive the Detection and Response actions of the Sentriant NG appliance. Once a Segment is configured and is being monitored by the Sentriant NG appliance, Rules must be assigned before mitigation actions are in effect. There are two components to a rule:

Detection - used to detect malicious network behavior.

Response - action(s) taken by the Sentriant NG appliance will take to mitigate malicious network behavior.

A variety of rules can be defined based upon a set of predefined Rule Types. Each rule type represents a different behavioral pattern that can be detected by the Sentriant NG appliance. The rule types are:

- **Host** - Host rules trigger a threat when a source is contacting too many unique IP Addresses within a Segment
- **Port** - Port rules trigger a threat when a source attempts to count ports within a Segment
- **Port per Host** - This rule triggers a threat based upon a number of (configured) ports contacted on a Unique Target IP Address
- **Traffic** - Traffic rules trigger a threat based on ANY traffic between a configured set of hosts
- **Packet** - Packet rules trigger a threat upon matching the “out-of-spec” contents of a packet
- **Spoof** - This rule triggers a threat when it detects a Spoofed IP Address in the Segment

Rule Sets

A Rule Set is added to each Segment Set allowing for the best detection possible based on the type of network Segment configuration. When a rule is triggered by a source threat, deception, alerts and cloaking activities are activated.

Edit Sentriant NG Configuration Settings

The Sentriant NG Manager allows administrators of the Sentriant NG appliance to perform the following configuration services:

Access - specify administrative access and privileges for user and clients

Alerts - configure E-mail, SNMP, and SysLog alerts to recipients

Deception - configure decoy personalities and personality sets to specific IP Addresses

Named Items - information that can be applied and reused when configuring Segment and Policy settings

Network - configure network topology including ports, network segments, and switches

Policy - configure rules used to detect and mitigate malicious network behavior

Load/Save Configuration Settings - load/save appliance configuration for backup purposes

Initial Segment Configuration

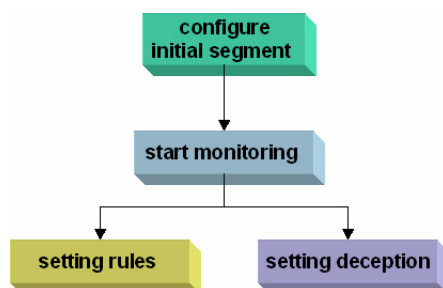
In order for the Sentriant NG appliance to begin monitoring network traffic, a Set must be created for segments accessible via the Sentriant NG appliance's Ethernet ports. Network Segments are then configured and assigned to a Segment Set. A default Segment Set with a list of segments is created after completing the initial set up of the Sentriant NG appliance (refer to the Installation Guide packaged with the Sentriant NG appliance). Additional Segment Sets and Segments can be created as needed. Below is a high-level flowchart sequencing each activity to begin monitoring and mitigating network traffic threats.



NOTE

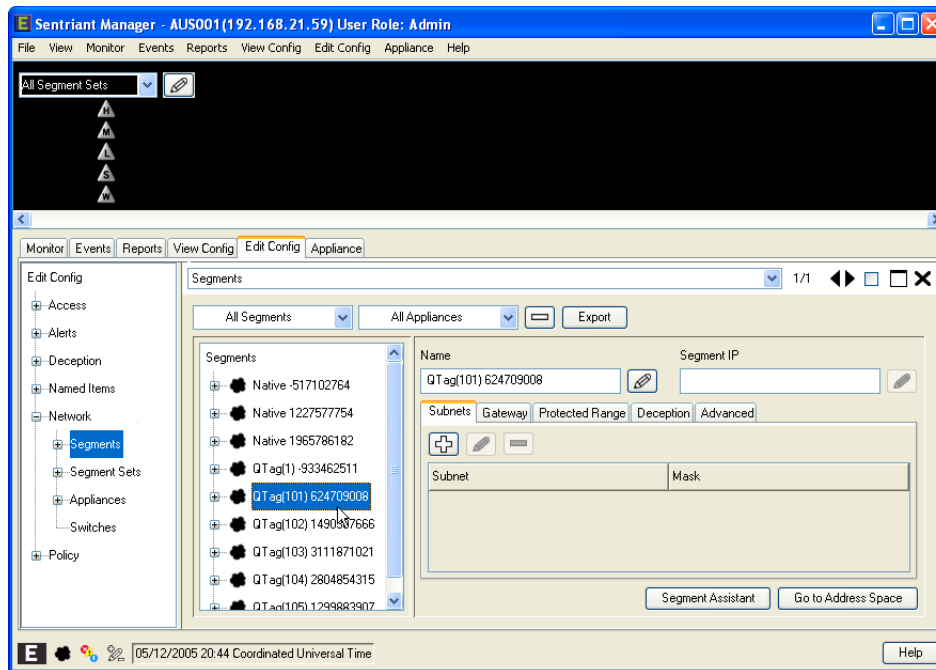
Configuration changes must be saved to the Sentriant NG appliance. See [“Saving Changes to the Sentriant NG Appliance” on page 133](#) for more information.

The base configuration is shown in the flowchart below.

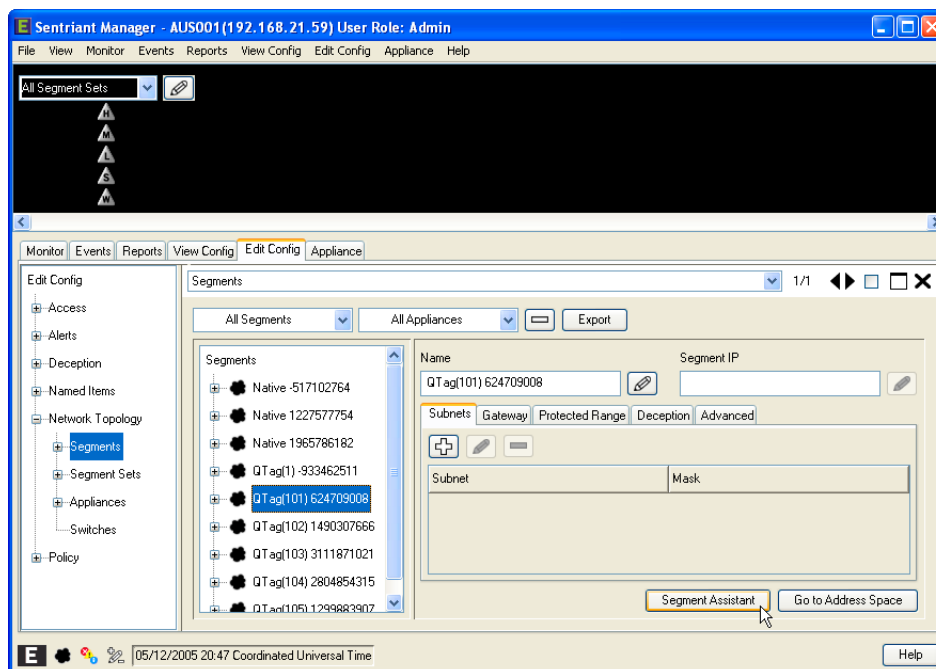


To configure initial Segment:

- 1 From **Edit Config > Network**, select **Segments**.
- 2 Select the Management network Segment from the list.



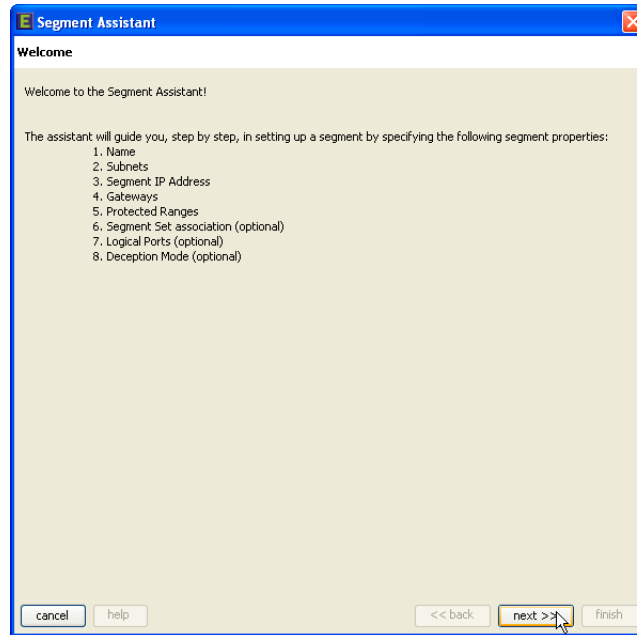
- 3 Click the **Segment Assistant** button located at the bottom right of the screen.



- 4 The Segment Assistant is displayed. Run through the Segment Assistant to configure a Segment.

You will need the following information to complete a Segment:

- Subnet IP Address or Addresses and Mask of the network Segment.
- Segment IP Address that will be monitored.
- Gateway IP Address of the Sentriant NG appliance.
- IP Addresses to identify the protected range or ranges of Segment IP Addresses.
- A Logical Port that is identified by the Sentriant NG appliance.



Saving Changes to the Sentriant NG Appliance

To start monitoring traffic on newly created segments, you must save the configuration changes to the Sentriant NG appliance.

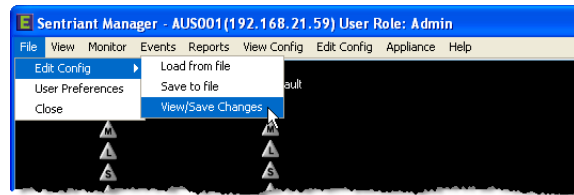


NOTE

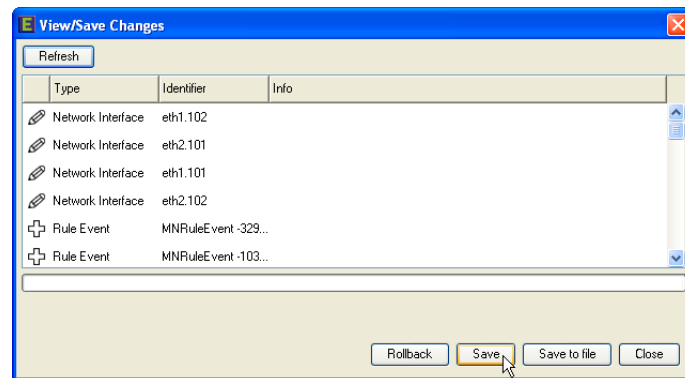
Configuration changes are not committed to the Sentriant NG appliance immediately, but are kept locally until all necessary configuration activities have been completed such as Segment, rule and deception information.

To save configuration changes to the Sentriant NG appliance:

- 1 Save the changes to the Sentriant NG appliance by selecting **File > Edit Config > View/Save Changes** or by clicking on the Edit Configuration button in the General Status Bar located at the bottom left of the panel.



- 2 The View/Save Changes dialog is displayed. Click **Apply** to save the changes to the Sentriant NG appliance.
- 3 The changes are persisted to the Sentriant NG appliance. Click **Close** to return to the Edit Config Panel.

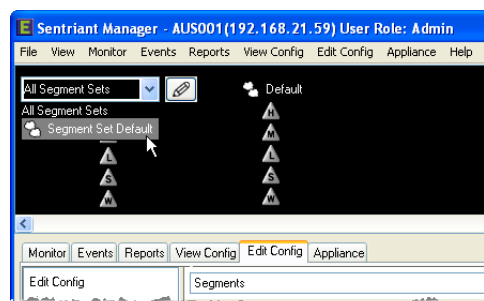


Start Monitoring a Segment

Once the configuration changes have been saved to the Sentriant NG appliance, you may begin monitoring network traffic on that Segment.

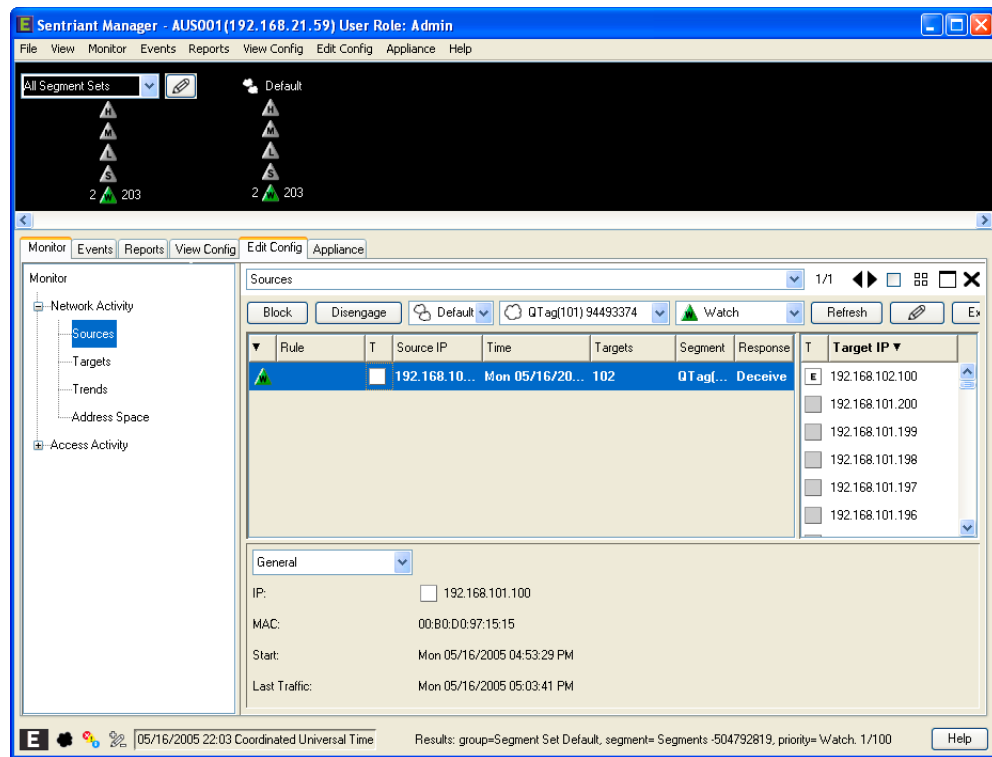
To begin monitoring network traffic on a Segment:

- 1 From the **Status Bar**, select the **Segment Sets** drop-down list.
- 2 Select the **Default** Segment Set to bring up the Default Segment Set in the Threats List.



You should see traffic in the Watch section under the Default Segment Set.

- Click the Watch icon. The Sentriant NG Manager will navigate to the **Monitor > Network Activity > Sources** panel and display a list of sources being watched on the Segment.



Setting Rules

Now that the Segment is being monitored, it is necessary to determine if any traffic is considered a threat. The way the Sentriant NG appliance identifies threats is through Rules. Threat rules can be configured by the administrator, and should be customized for each network to allow for the best detection possible. A default set of rules is shipped with the product and can be used out of the box.

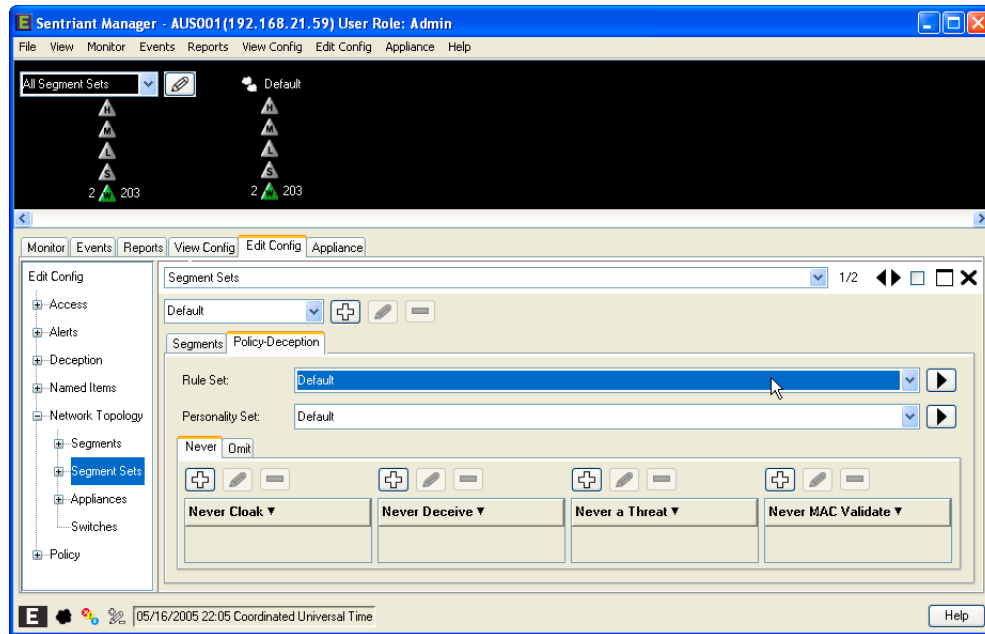
To turn rules on:

- From **Edit Config > Segment Sets**, select a **Segment Set**.



Initially created segments are placed in the Default Segment Set unless otherwise specified.

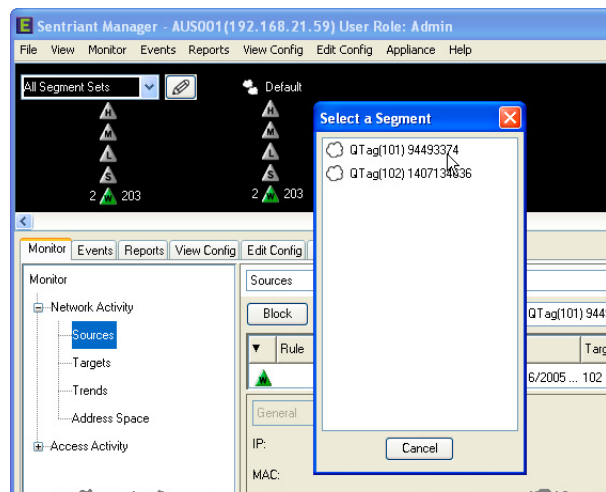
- Select the **Policy-Deception Tab** and select a Rule Set from the Rule Sets List.



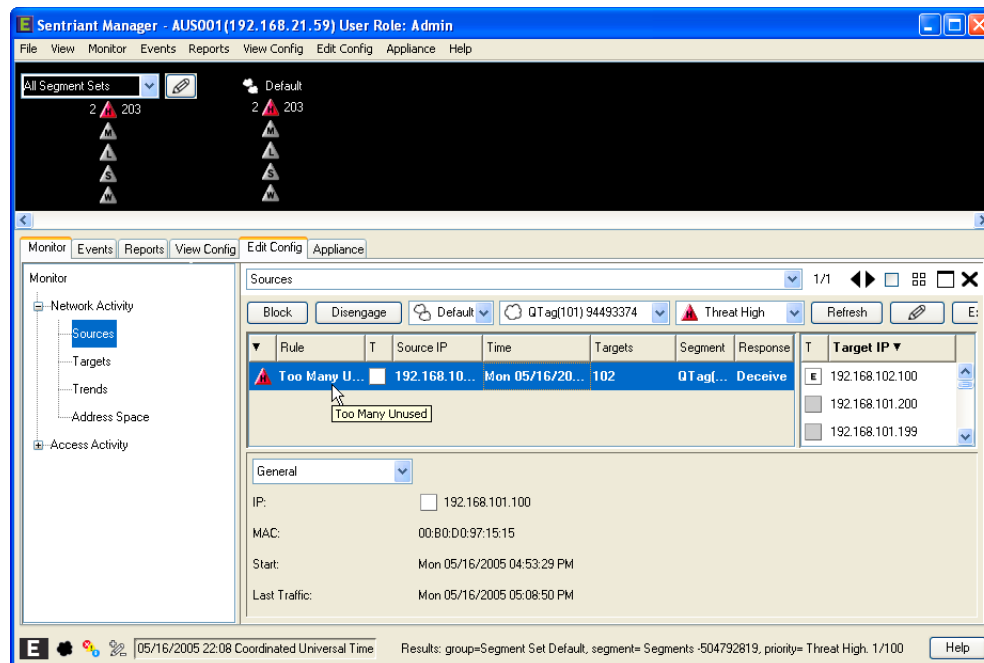
NOTE

It may be necessary to change the parameters of the selected rules to simulate a threat. See [“Rules” on page 255](#) for more information. For example, set # of Packets to 1 and Priority to 999 on a traffic rule.

- 3 Save the [changes](#) to the Sentriant NG appliance. The Rules are now active and you should see threats in the Status Bar.
- 4 From the Status Bar select a source by clicking on the number to the right of the threat icon and then selecting a Segment.



The selected threat is displayed in the Sources Panel.

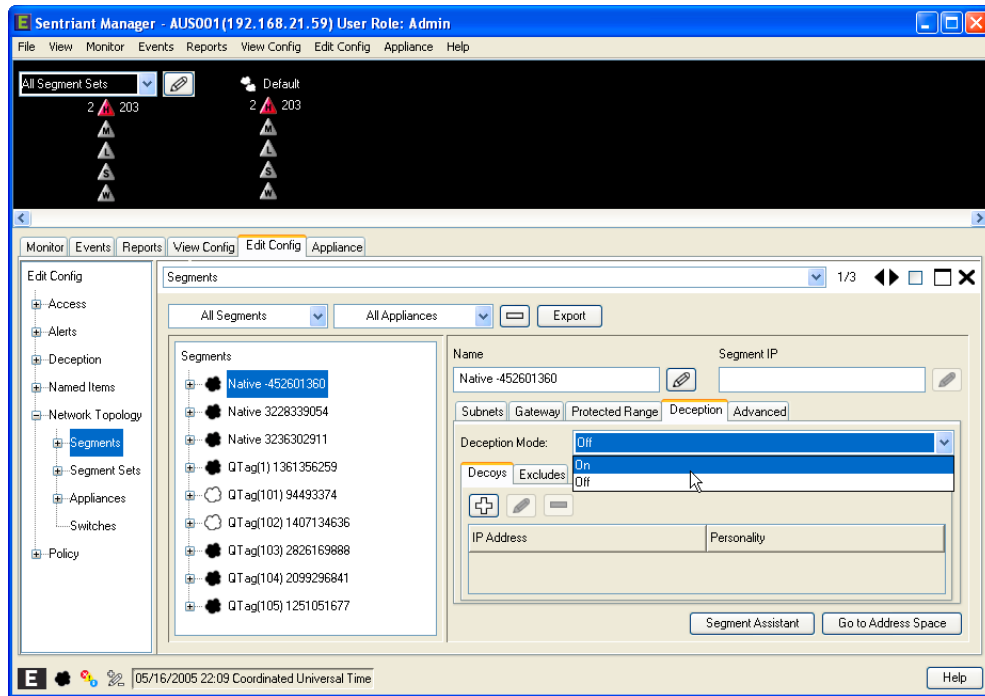


Setting Deception

Deception allows a threat to continue with its network activity, however the activity of the source is still monitored. For example, a threat is encountered that scans **Unused IP Addresses**, steps can be taken to deceive the threat by configuring deceptions.

To set Deception:

- 1 From **Edit Config > Network > Segment**, select the Segment.
- 2 Click the **Deception Tab**.
- 3 Turn **Deception** on by selecting **On** from the **Deception Mode** drop-down list.



4 Save the [changes](#) to the Sentriant NG appliance. Deception is now active.

Access

User Configuration

Sentriant NG Manager is installed with a default configuration for one user with the user name "admin" so that the system administrator can access Sentriant NG Manager and create the initial set of users. The admin can then grant security settings to selected users for subsequent configuration changes.

The following table summarizes Sentriant NG Manager's default groups. The admin can modify or delete the users at any time.

Table 6: User Capabilities

User Name	Capabilities
Admin	Can fully administer the system
Operator	Can perform mitigation operations and change E-mail and password Cannot perform configuration activities
Observer	Can only view operations and change their E-mail and password Cannot perform mitigation activities Cannot perform configuration activities

Client Configuration

It is necessary to specify which clients will be connecting to Sentriant NG Manager in an administrative role. A client is defined as the IP Address of the PC running Sentriant NG Manager.



NOTE

In the case of multi-homed PCs, all relevant IP Addresses must be added as clients.

On initial installation, a client is specified for the default administrator. The Clients screen defines additional IP Addresses that are allowed to administer the Sentriant NG Manager.



NOTE

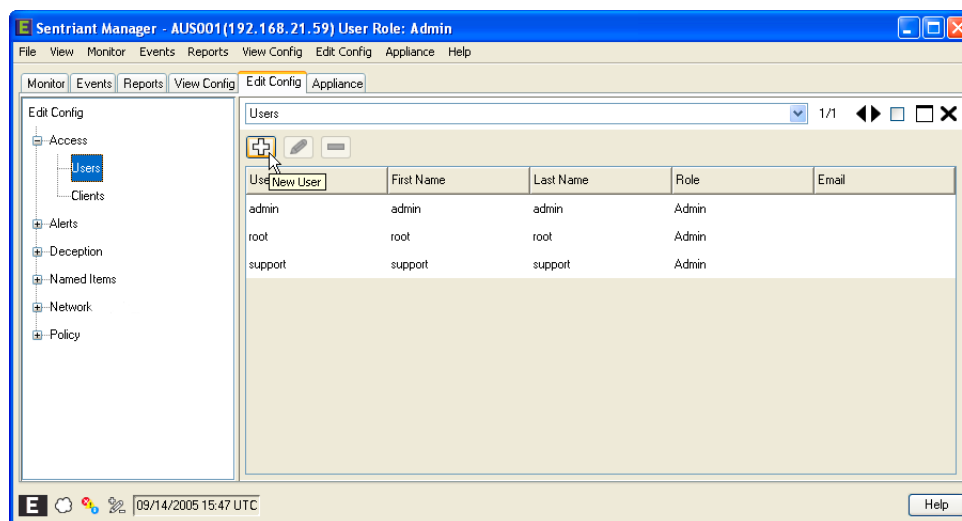
After adding IP Addresses to the Access Clients list, you may wish to add those IP Addresses to the Exceptions screen and set the Mitigation Modifiers to Never Cloak. This will prevent the administrator from losing contact with Sentriant NG Manager should the Access Client be declared a threat. While this action reduces the level of network security to a degree, it provides the benefit of ensuring uninterrupted access to the Sentriant NG Manager.

Creating User Accounts

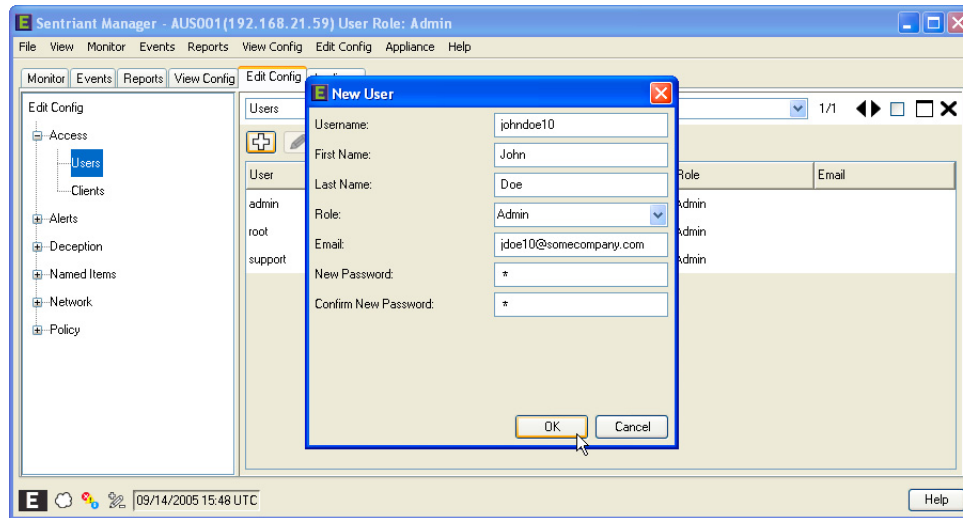
To start Sentriant NG Manager, a user must have a user account. A user account includes the Username, role and other information, such as the user's full name, E-mail address, and password.

To create a user account:

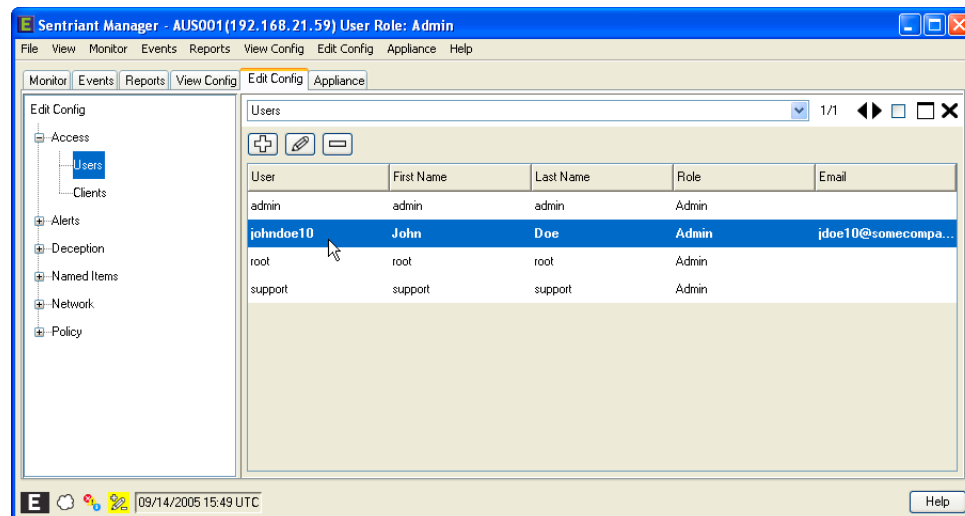
- 1 From **Configure > Access**, select **Users** to display the User panel.



- 2 In the Users panel, click the **New** button to open the New User dialog box.



- 3 Type the Username and other user information. Select the type of role for the user from the drop-down list. Enter E-mail and password.
- 4 Type in the Admin password.
- 5 Click OK to add the new user.

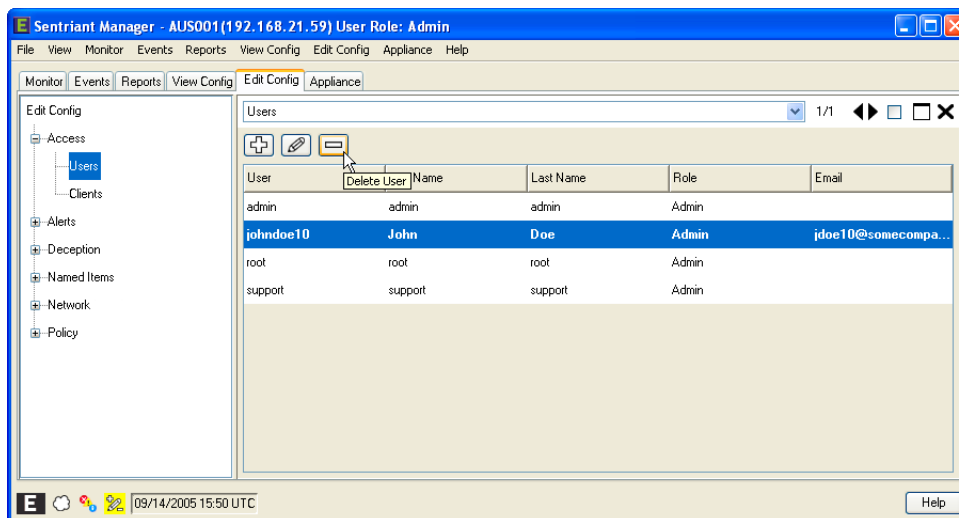
**NOTE**

Clicking OK adds the user to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#).

Deleting User Accounts

To delete a User Account:

- 1 From **Configure > Access**, select to display the **Client Panel**.
- 2 Select the User and then click the **Delete User** button. To select multiple Users, either Shift-click or Ctrl-click.

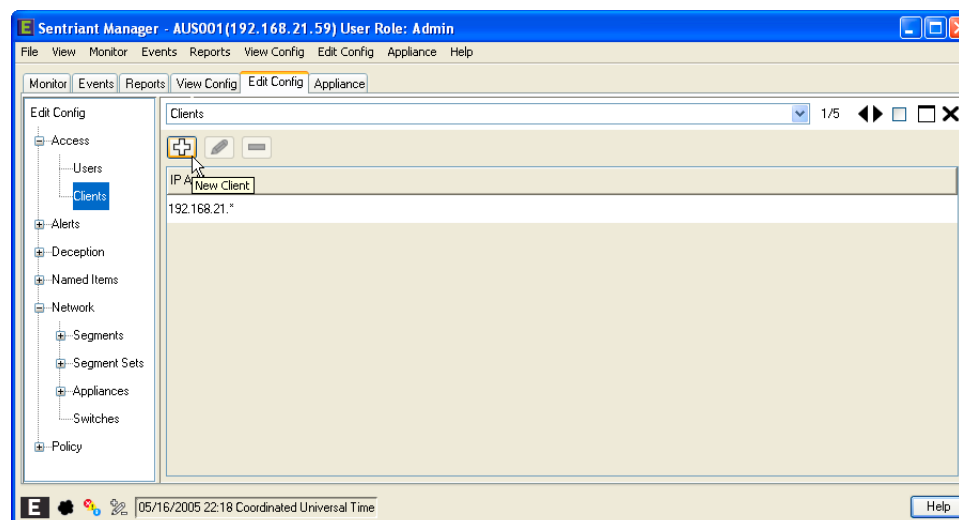


Creating Clients

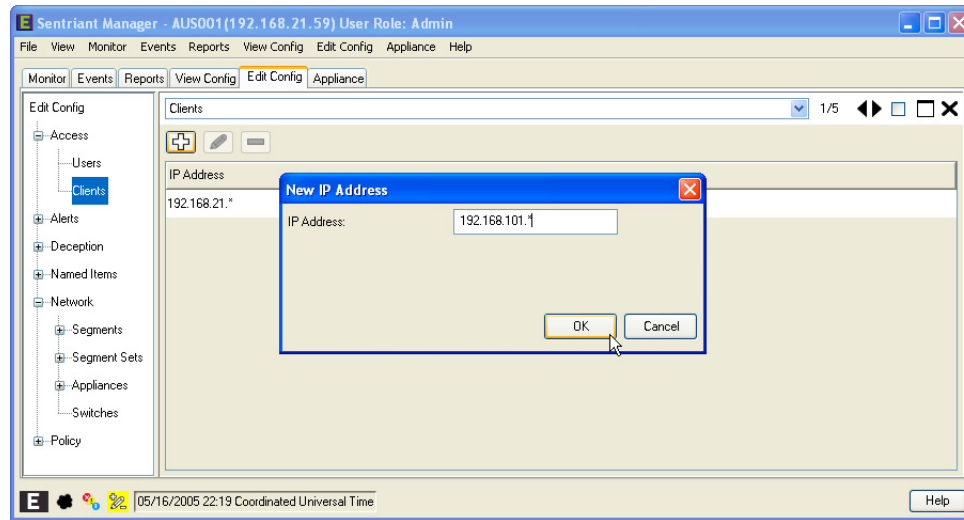
In order to have access to the Sentriant NG Manager, the IP Address of the user's workstation must be added as a client.

To add a client:

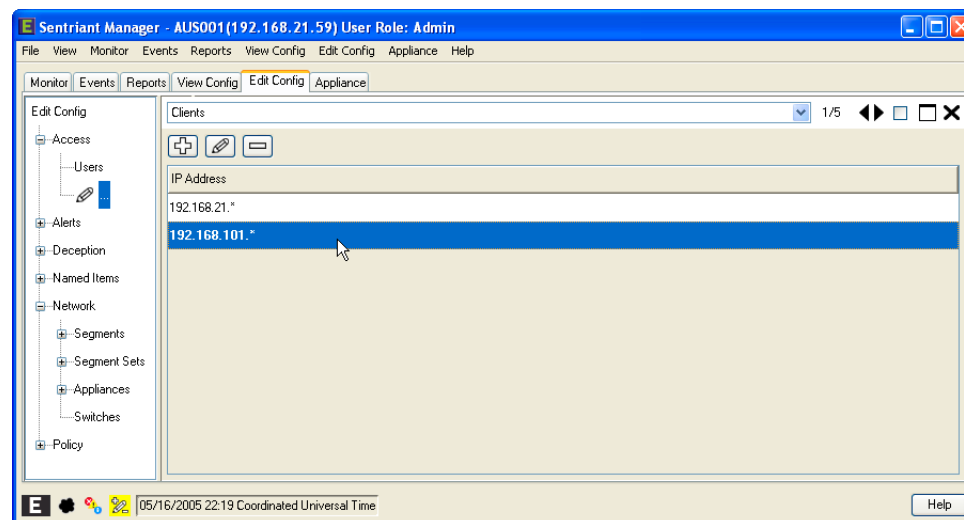
- 1 From **Configure > Access**, select **Clients** to display the **Client Panel**.



- 2 In the Client Panel, click the **New** button to open the **New IP Address** dialog box.



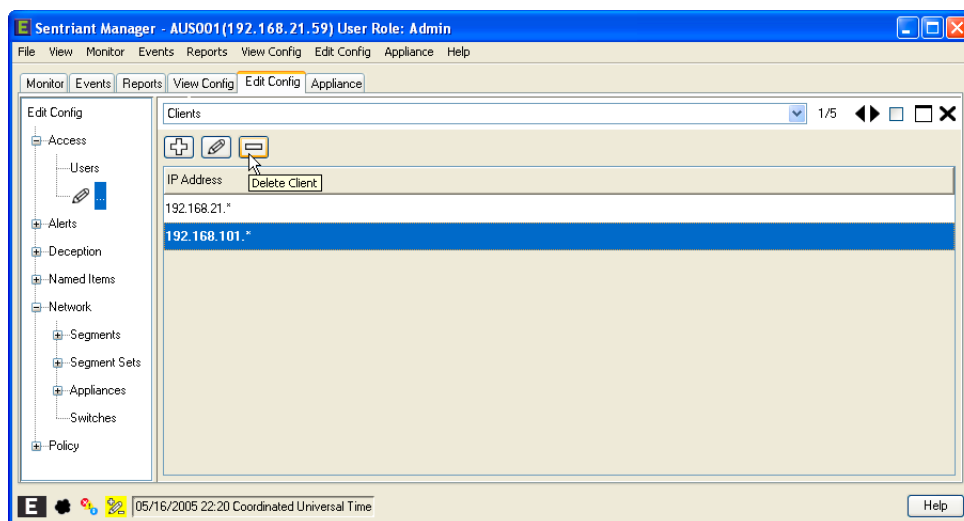
- 3 Type the IP Address in the IP Address field.
- 4 Click **OK** to add the new IP Address.



Deleting Clients

To delete a Client:

- 1 From **Configure > Access**, select **Clients** to display the **Client Panel**.
- 2 Select the IP Address and then click the **Remove** button. To select multiple IP Addresses either Shift-click or Ctrl-click a range of IP Addresses.



Alerts

The Sentriant NG appliance can be configured to send alerts to destinations on specific events that occur. To send alerts, destinations must first be configured and then a source selected. Sources or [Rules](#) are what trigger the alerts to be sent. Destinations need to be defined for each type of Alert. The types of Alert vehicles are:

SMTP

The Sentriant NG appliance generates E-mail messages and sends them to a single destination mail server. The server address is configured in the Sentriant NG Manager, as well as each recipient's E-mail address. The destination mail server must be configured to receive relay messages from the Sentriant NG appliance's management IP Address. E-mail messages are queued and delivered as resources are available.

SNMP

A single MIB defines the Extreme Alert information block. The Extreme SNMP message is an enterprise trap that is registered with [IANA](#). The Extreme enterprise number is 1960. (See iana.org for more information about enterprise numbers and registration.) The MIB file is located under the \Program Files\SentriantManager\snmp directory. The file name is snmp.mib.

Currently, the Sentriant NG MIB is importable into any SNMP enterprise-enabled workstation that supports SNMP v.1. SNMP messages are queued and delivered as resources are available. The SNMP trap monitor addresses are configured in the Sentriant NG appliance's UI.

Syslog

The Sentriant NG appliance generates messages that are sent to log files and records them to a specified location on a server or work station. The destination must be configured to receive the data and write to the Syslog recorder. The recording system may record these in any desired manner including writing them to a file, sending them on to other systems, and printing them out.

Alert Message Types

Alerts are grouped into three types based on how they were generated and which component they cover. The types are as follows:

- System - Cold and Warm boot alerts from the Sentriant NG appliance
- Network Activity - Threat escalate, de-escalate and Response enable/disable alerts. The Threat escalate/de-escalate alerts are generated when the status of a threat that has triggered a rule or a watch has been changed. For example, a watch is escalated to suspect, an Alert will be generated displaying the status change. Response enable/disable alerts are generated when the response is automatically or manually triggered.
- Rules - Default and custom rules, when triggered, may be configured to generate an Alert.

Receiving Alert Messages

When receiving an Alert message, the contents of an Alert are based on the type of mechanism that generated the Alert and the Alert message type. For SMTP generated Alerts, the contents is formatted using a new line for each field or part of the Alert message. An example of an Alert generated by SMTP is below:

```
Appliance=AustinSite
Reporting Segment=QTag(3) 459378252
Action=Threat escalated
Rule=Unused Contact
Priority=Suspect(2500)
Response=Initiating Cloak
Source Segment=Unprotected
Source IP=107.21.10.100
Source MAC=00:C0:9F:36:5B:4F
Current Target Count=1
```

Alerts generated by SNMP and Syslog are formatted using comma-delimited strings with a field header and the body of the field separated by a comma(.). An example of an Alert generated by SNMP or Syslog is below:

```
Appliance=AustinSite,Reporting Segment=QTag(3) 459378252,Action=Response
enabled,Response=Cloak,Source Segment=Unprotected,Source
IP=107.21.10.100,Source MAC=00:C0:9F:36:5B:4F,Current Target Count=1
```

Creating SMTP Destinations

Sentriant NG Manager provides alerts to be sent to users that have access to the Sentriant NG Manager and additional personnel who may need to be notified of events (i.e.: network administrators, managers, etc.).

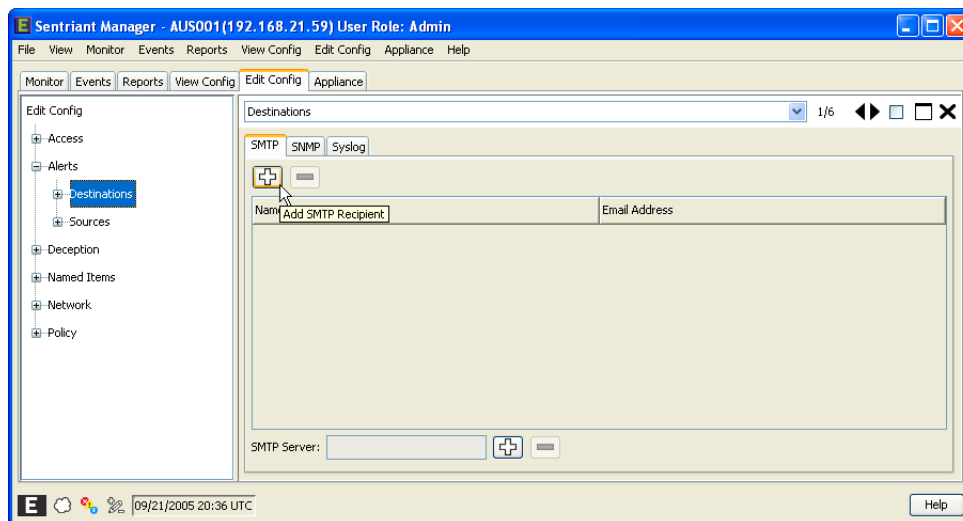


NOTE

You may create an E-mail group and add it as an alerts destination to broadcast alerts to a number of personnel therefore lessening the number of entries needed within the Destinations table.

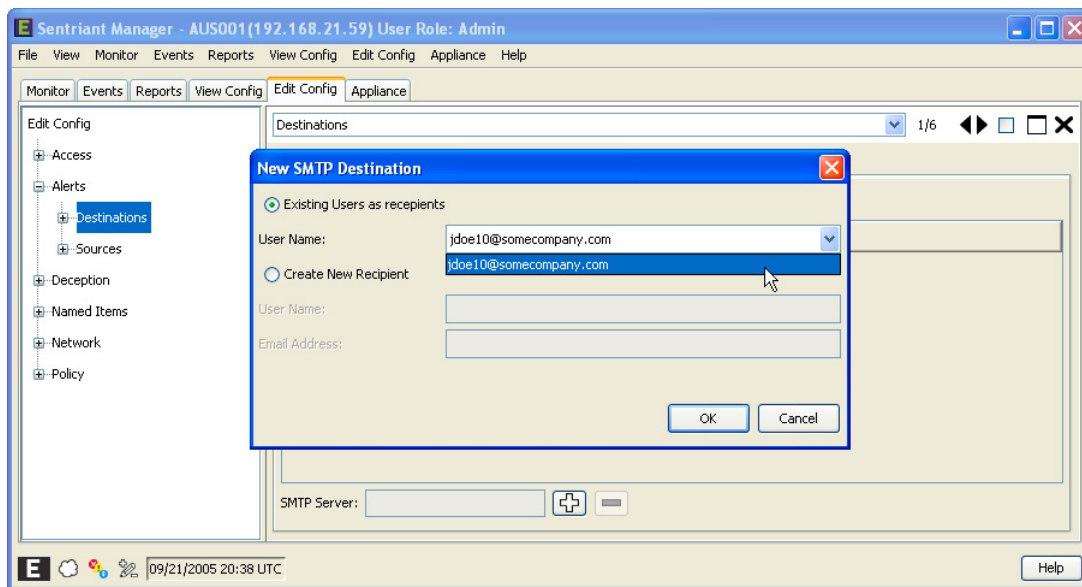
To create an SMTP Destination:

- 1 From **Edit Config > Alerts**, select **Destinations**.
- 2 Select the **SMTP** tab in the **Information Panel**.
- 3 Click the **Add SMTP Recipient** button.



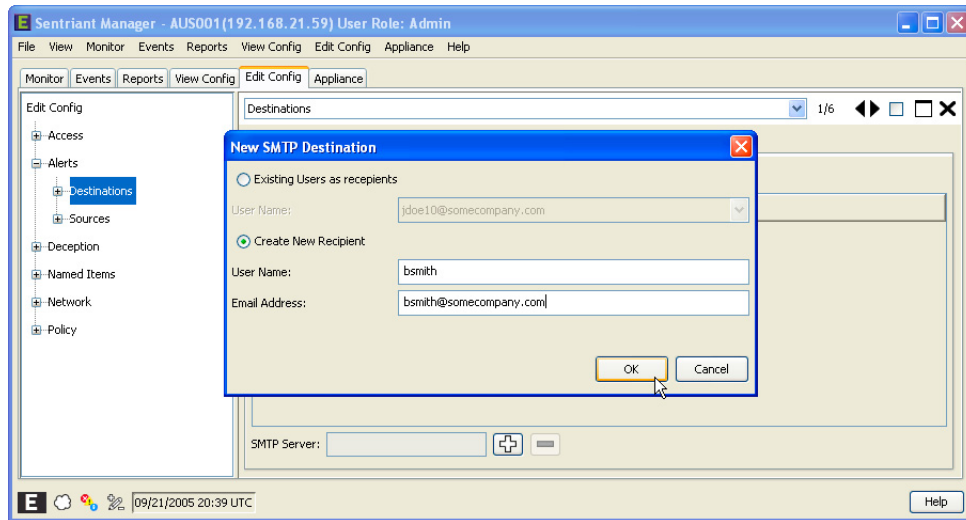
There are two methods for adding an E-mail destination:

- a Select an E-mail address from the drop-down list



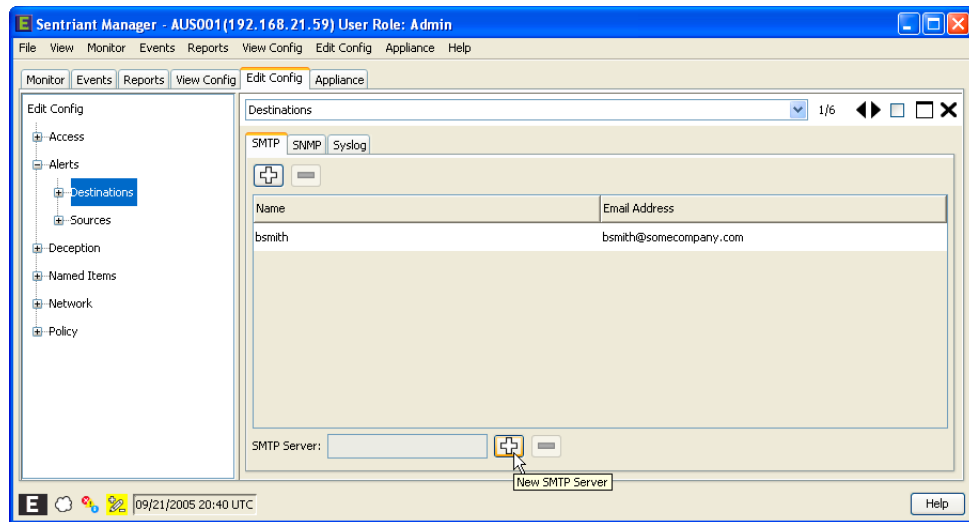
or...

- b Click the **Create New Recipient** radio button.
- c Enter a user name and E-mail address.
- 4 Click **OK**.

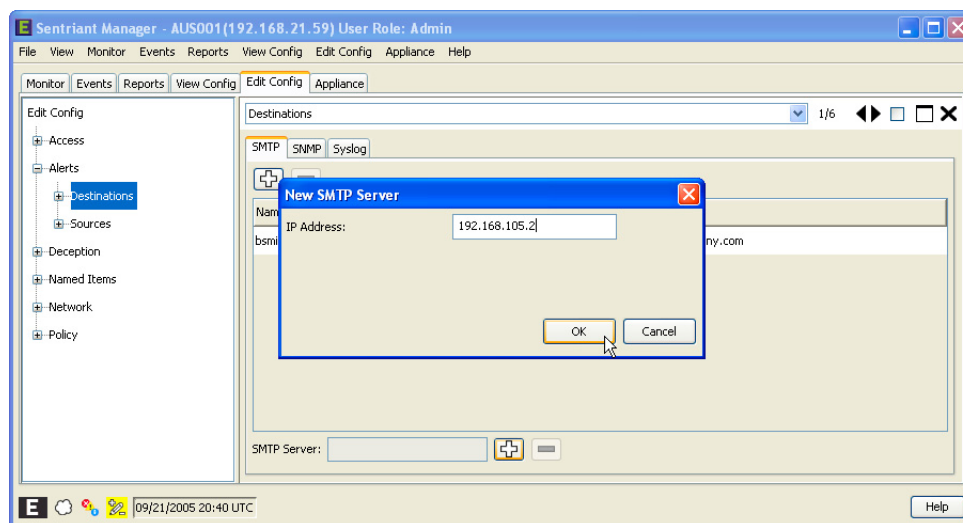


Once the users are added, you must enter the IP Address of the SMTP Server that will receive E-mail.

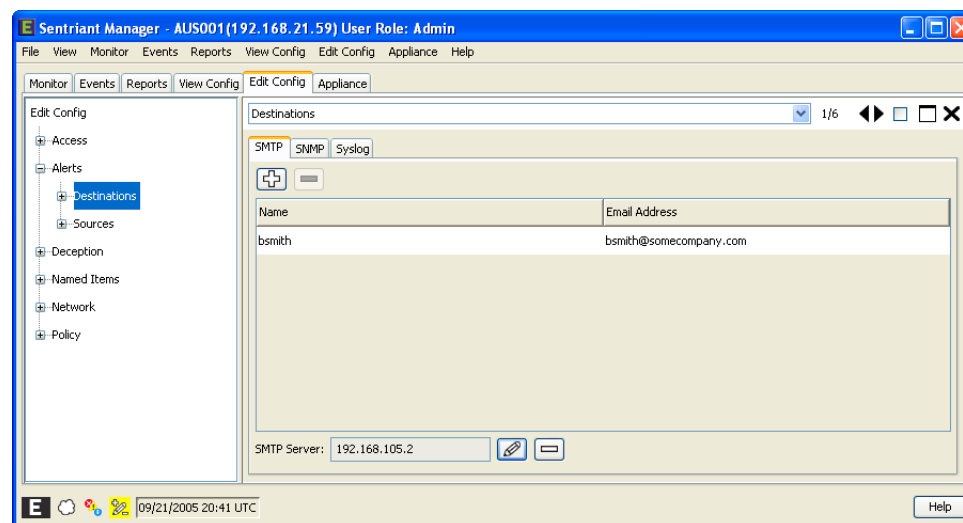
- 5 Click the **New SMTP Server** button.



- 6 Enter the IP Address of the SMTP Server and click **OK**.



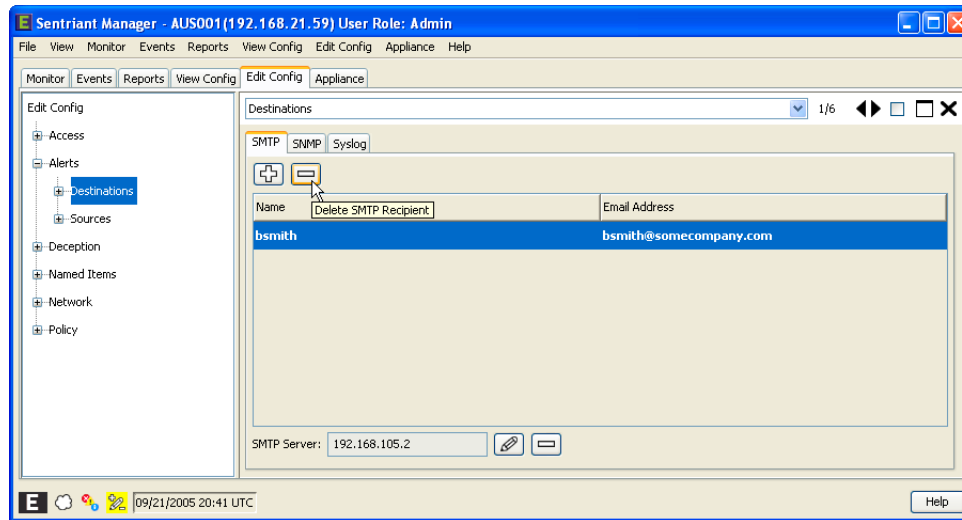
The users are now ready to receive E-mail from the Sentriant NG appliance.



Deleting E-mail Destinations

To delete E-mail Recipients:

- 1 From **Edit Config > Alerts**, select **Destinations**.
- 2 Select the **E-mail** tab in the **Information Panel**.
- 3 Select the **Username** to be deleted.
- 4 Click **Delete E-mail Recipient** button.

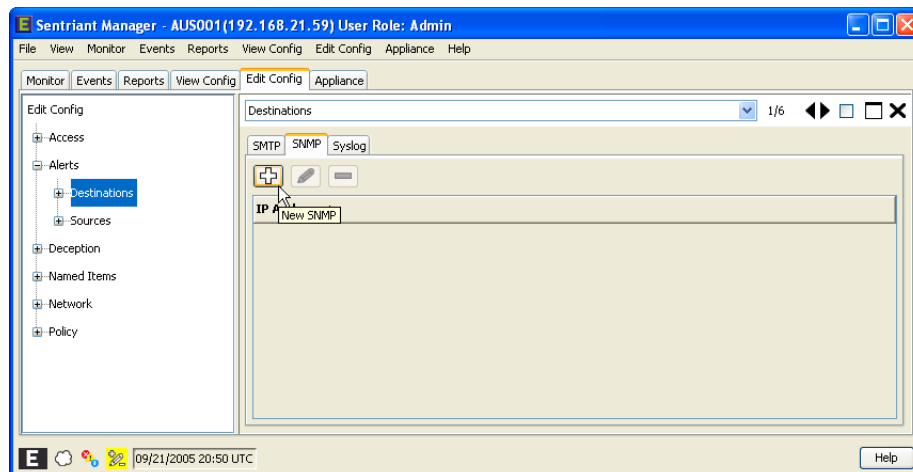


Creating SNMP Destinations

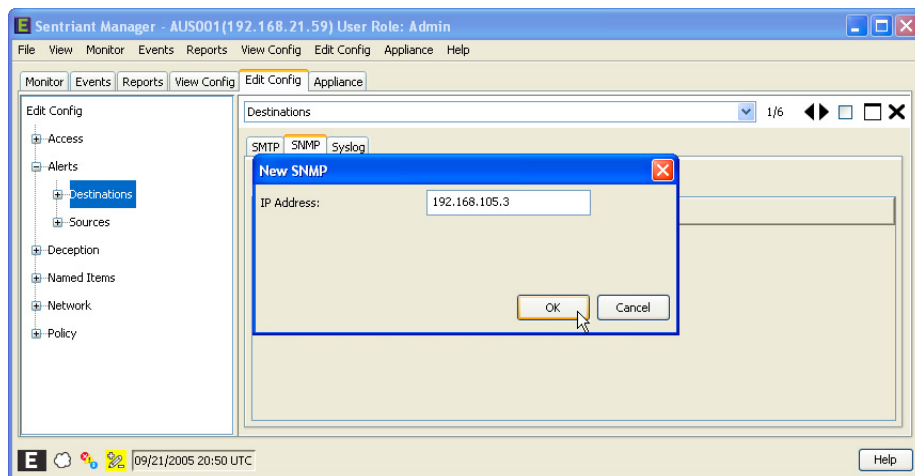
In order for SNMP Alerts to be functional, your network administrator must configure the SNMP trap using the provided MIB file. The MIB file is located under \Program Files\Sentriant\snmp directory. The file name is **snmp.mib**.

To create SNMP Destinations:

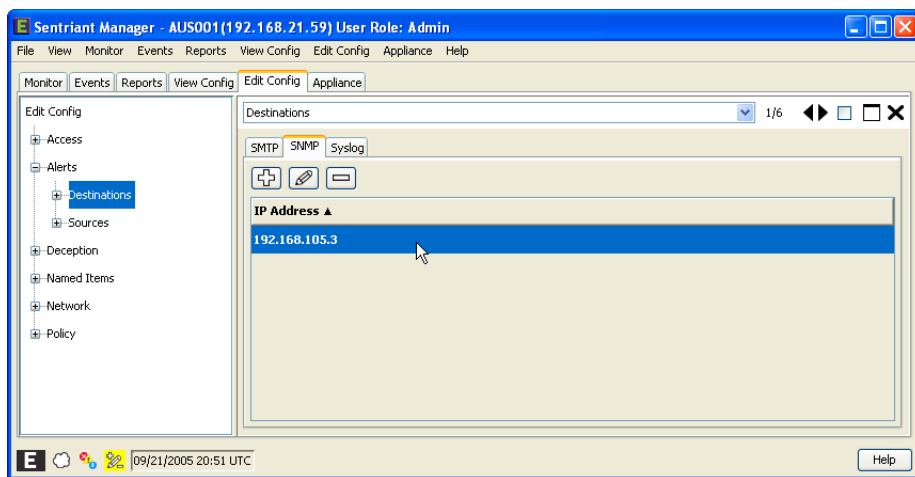
- 1 From **Edit Config > Alerts**, select **Destinations**.
- 2 Select the **SNMP** tab in the **Information Panel**.
- 3 Click **New SNMP** button.



- 4 Enter the IP Address of the SNMP Server IP Address and click **OK**.



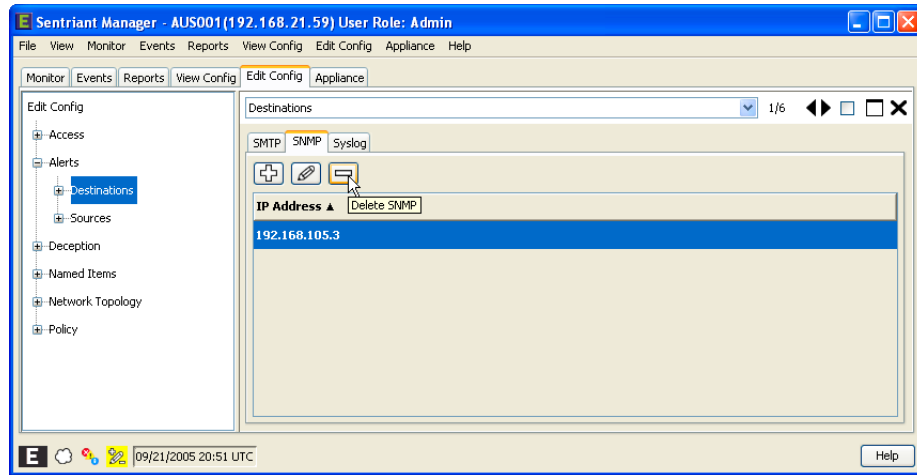
- 5 Continue adding the SNMP Server IP Address for each server that will receive Alerts.



Deleting SNMP Destinations

To delete SNMP Destinations:

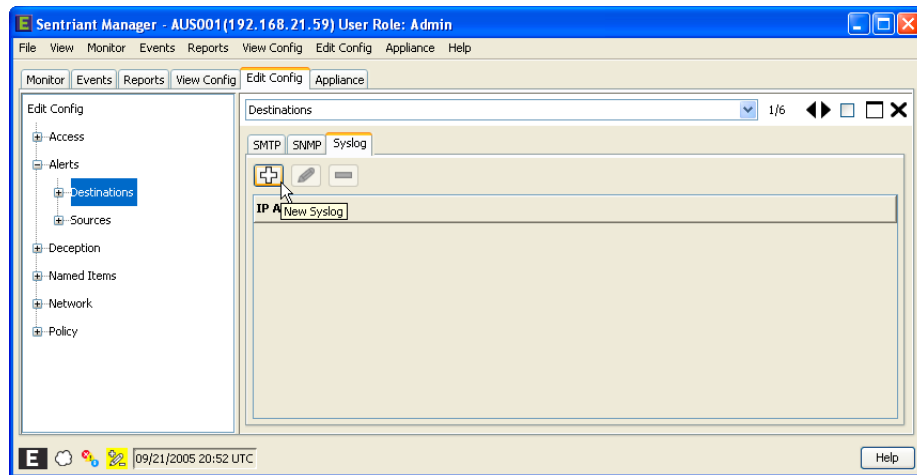
- 1 From **Edit Config > Alerts**, select **Destinations**.
- 2 Select the **SNMP** tab in the **Information Panel**.
- 3 Select the SNMP Server's IP Address to be deleted.
- 4 Click **Delete SNMP** button.



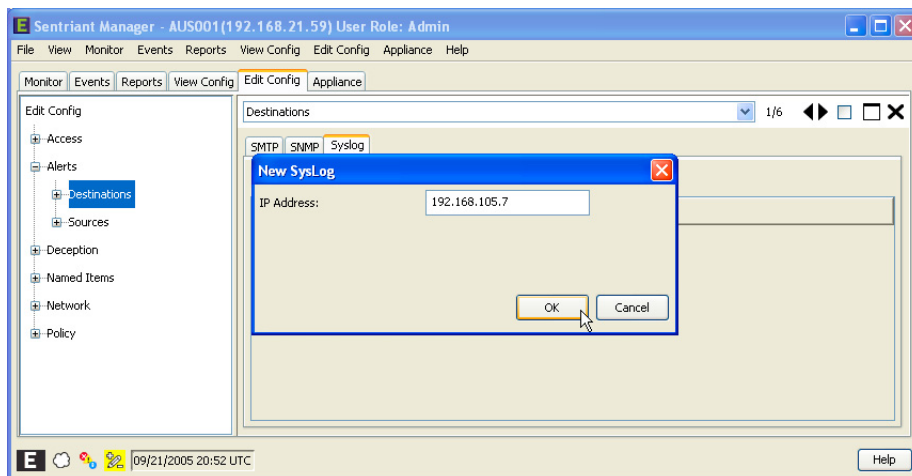
Creating Syslog Destinations

To create Syslog Destinations:

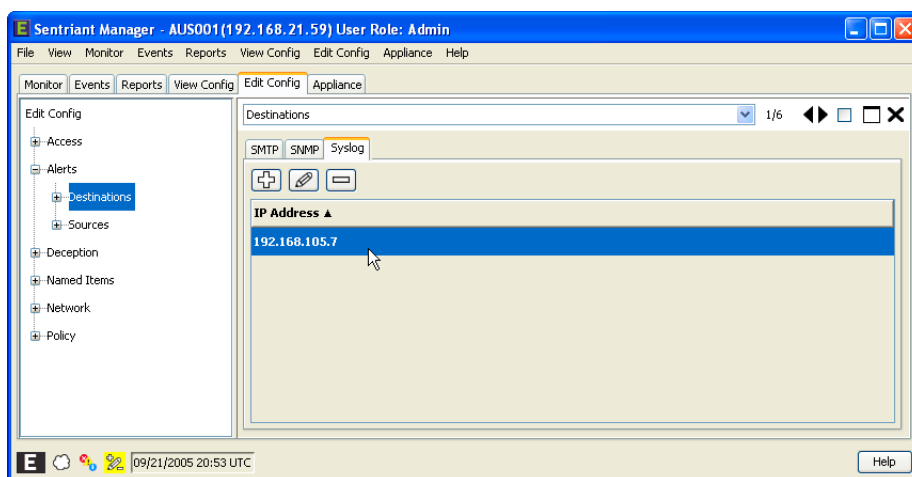
- 1 From **Edit Config > Alerts**, select **Destinations**.
- 2 Select the **Syslog** tab in the **Information Panel**.
- 3 Click **New Syslog** button.



- 4 Enter the IP Address of the Syslog Server IP Address and click **OK**.



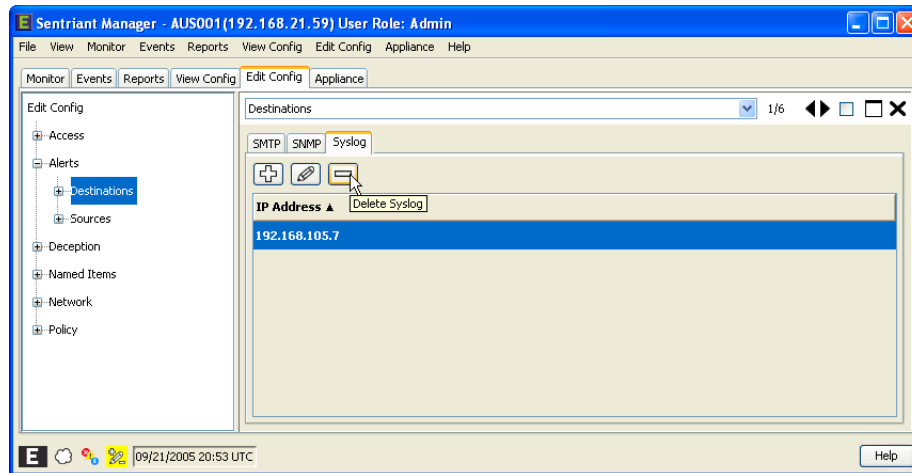
- 5 Continue adding the Syslog Server IP Address for each server that will receive Alerts.



Deleting Syslog Destinations

To delete Syslog Destinations:

- 1 From **Edit Config > Alerts**, select **Destinations**.
- 2 Select the **Syslog** tab in the **Information Panel**.
- 3 Select the Syslog Server's IP Address to be deleted.
- 4 Click **Delete Syslog** button.



Setting Up Sources

To set up Sources:

- 1 From **Edit Config > Alerts**, select **Sources**.

Name ▲	Alert Source	Enable
Archive Rotated In	Health	<input checked="" type="checkbox"/>
Archive Rotated Out	Health	<input type="checkbox"/>
Bad Pkt : All Flags	Rule	<input checked="" type="checkbox"/>
Bad Pkt : No Flags	Rule	<input type="checkbox"/>
Bad Pkt : SYN/FIN	Rule	<input checked="" type="checkbox"/>
Bad Pkt : URG Only	Rule	<input type="checkbox"/>
Bad Pkt : Xmas Tree	Rule	<input type="checkbox"/>
Cloak	Response	<input type="checkbox"/>
Cloak Notify	Response	<input type="checkbox"/>
Cold Start	Health	<input type="checkbox"/>
Configuration Imported	Configuration	<input type="checkbox"/>
DNS Mail Lookup	Rule	<input type="checkbox"/>
Daily Audit Report	Rule	<input checked="" type="checkbox"/>
Daily Top Offender Report	Rule	<input checked="" type="checkbox"/>
Disk Utilization	Health	<input type="checkbox"/>

A list of rules is displayed with Name, Alert Source and Enable check box for each rule.

- 2 Select an Alert Type tab. Types are SMTP, SNMP, Syslog.
- 3 Select a rule from the list and turn on the Enable check box.

You may click the **Select All** button to set an Alert for all rules or **Deselect All** button, however, if you do not select a recipient type, you will not receive an Alert for the triggered rules.

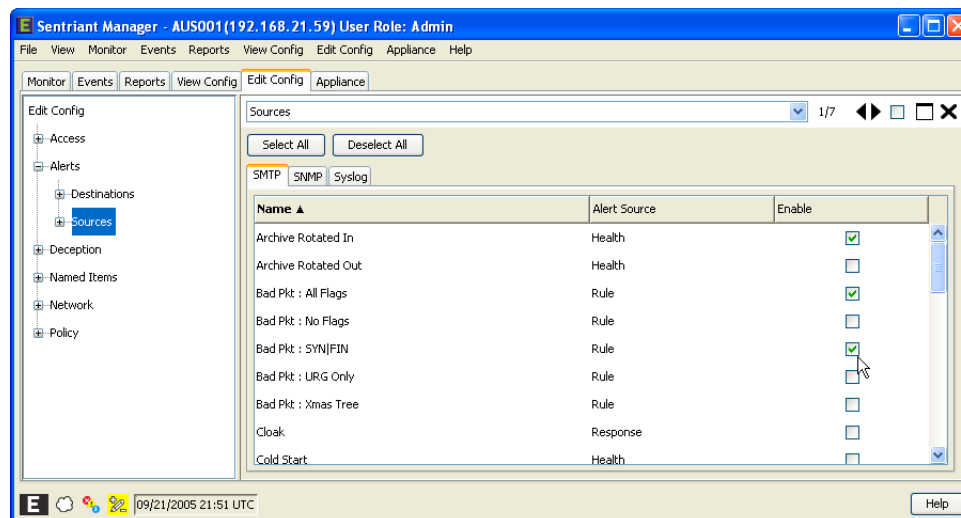


NOTE

The Daily Audit Report and the Daily Top Offender Report are only available if you select the SMTP type.

**NOTE**

The Daily Audit Report and the Daily Top Offender Report are run and delivered at midnight.

**NOTE**

Clicking OK adds the Alerts to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, See ["Saving Changes to the Sentriant NG Appliance"](#) on page 133.

Deception

The Sentriant NG appliance can take advantage of IP Addresses that are not used by any hosts (unused address space) to present a deceptive view of the network to attackers. For a percentage of unused address space, the Sentriant NG appliance responds as though real computers were using the address space, effectively creating decoys on the network to draw in would-be attackers. These decoys can behave as though they are specific devices running specified operating systems and services personalities.

Unused address space can be configured as a collection of non-hosts, Linux hosts, Windows XP hosts, or Windows 98 hosts. In addition, the administrator can customize not only the emulated operating system for a virtual host, but also the open TCP and/or UDP ports on the host.

Deceptive responses can be configured to inhibit an attacker. The administrator can utilize provided Example Personalities or create customized Personalities. The Deception Panel allows the creation and modification of Personalities and to view the way personalities will be utilized within the unused address space.

Once a personality or group of personalities have been created, a Personality Set is created containing a personality or multiple personalities. A Personality Set is then assigned to a Segment Set. Distribution is turned on for each Segment.

**NOTE**

Deception responds only to sources attempting to contact Unused IP Addresses. Deception is not utilized to hide existing Used IP Addresses.

**NOTE**

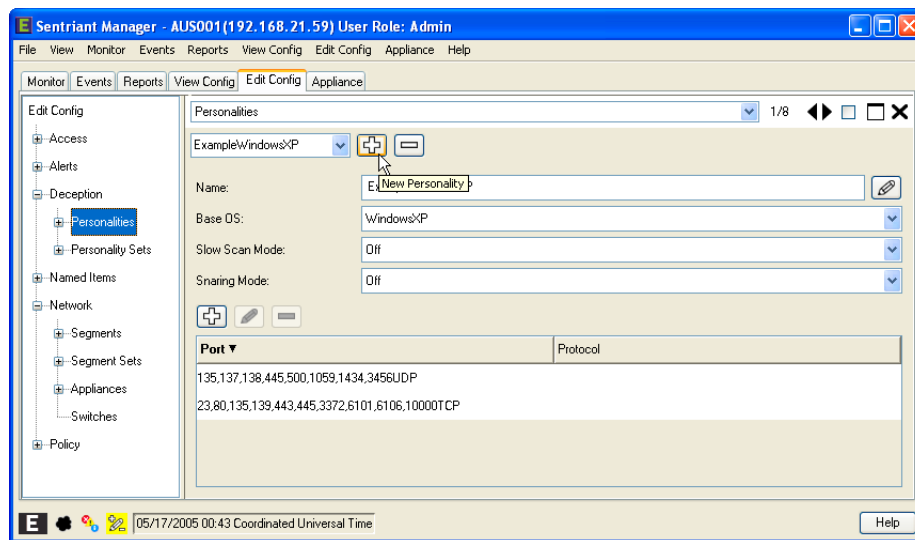
Deception must be turned on at the Segment level and a Personality Set assigned to a Segment Set.

Creating Personalities

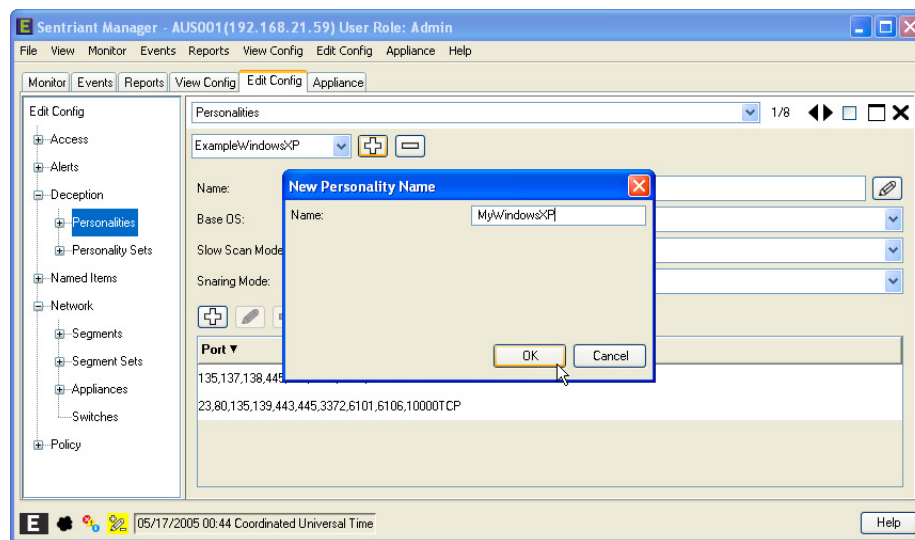
The Sentriant NG appliance comes with pre-configured personalities that you may use out of the box. However, you may either modify or add new personalities as you need.

To create a Personality:

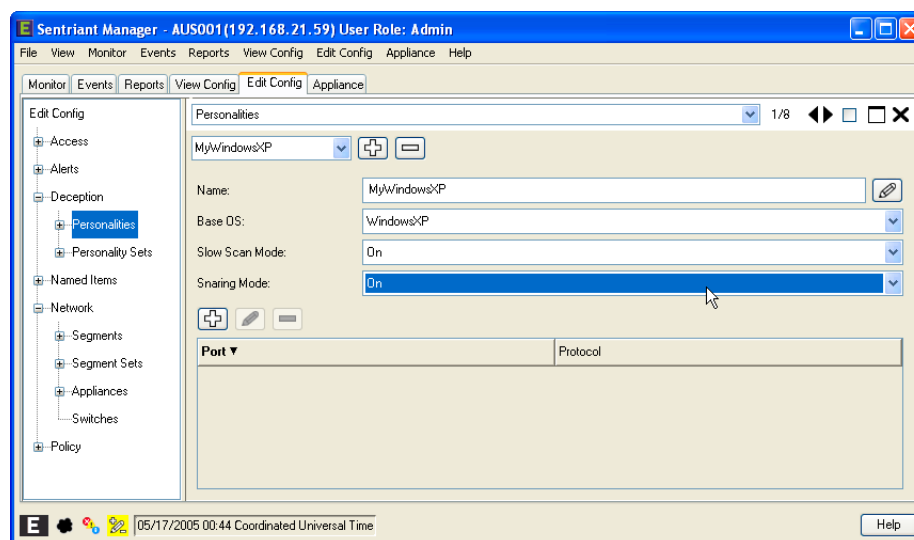
- 1 From **Edit Config > Deception**, select **Personalities**.
- 2 Click the **New Personality** button.



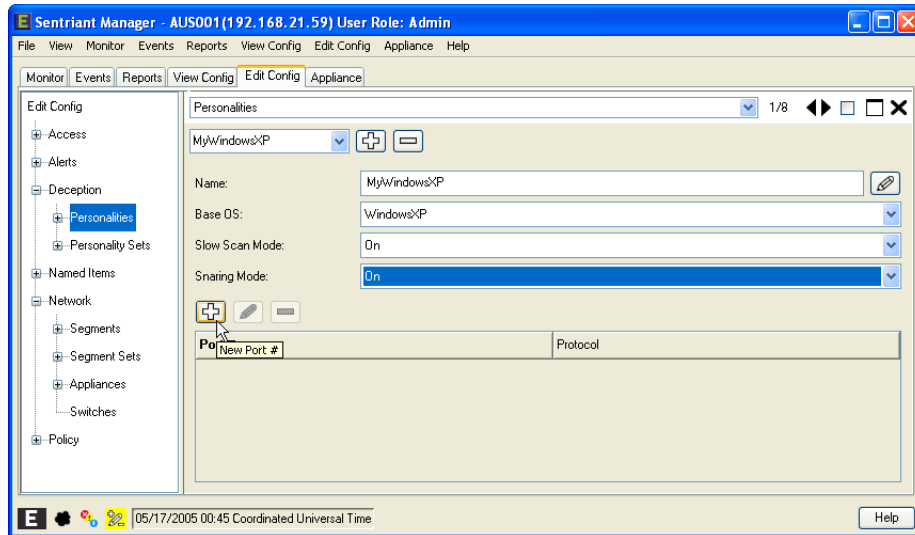
- 3 Type a name for the new personality.
- 4 Click **OK**.



- 5 From the **Base OS** field, select the OS type.
- 6 Set the **Slow Scan Mode** to on or off.
- 7 Set the **Snaring Mode** to on or off.



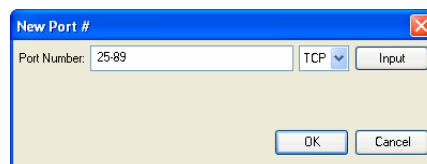
- 8 Click the **New Port #** button.



- 9 Enter a Port Number by one of the two methods:
 - a Type a Port number in the Port Number field.
 - b Select the Port type, either TCP or UDP.
 - c Click OK.

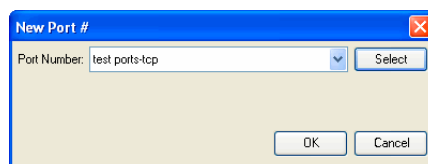
**NOTE**

When typing in a Port, you may enter a range of ports using syntax (121-123) or a series of ports (233,236,239).

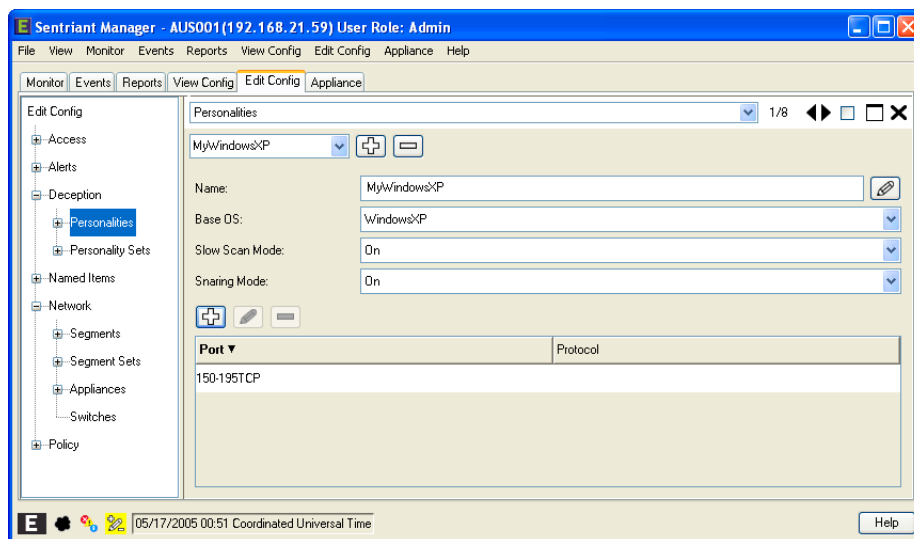


or...

- d Use a Port Set by clicking the Input button and then selecting a Port Set from the drop-down list.
- e Click OK.



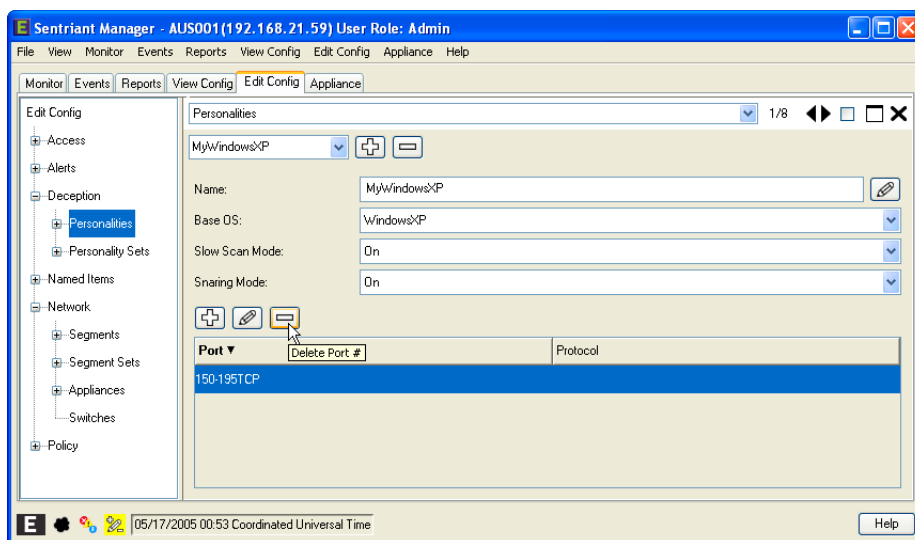
Continue to add ports for each unused address space.



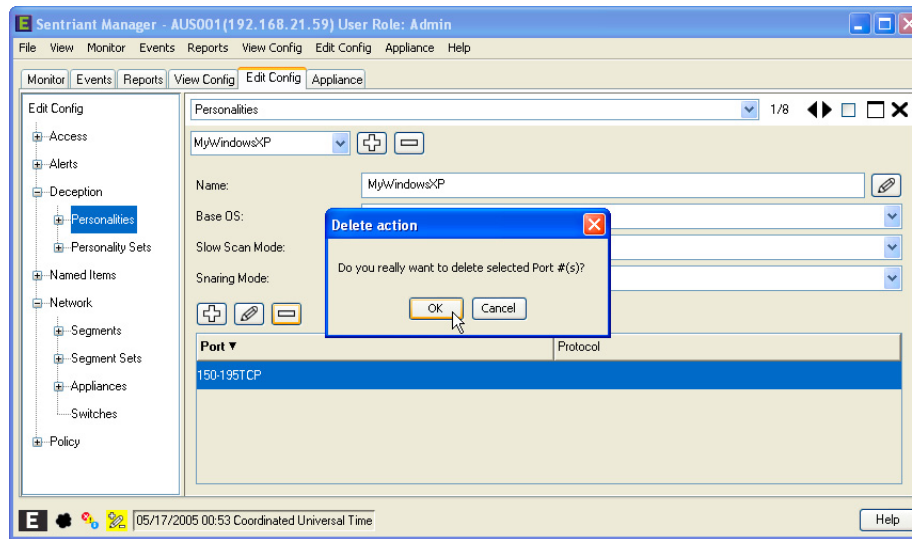
Deleting Personalities

To delete a Personality:

- 1 From **Edit Config > Deception**, select **Personalities**.
- 2 Select a personality from either the Folder List or by selecting from the drop-down list in the Information Panel.



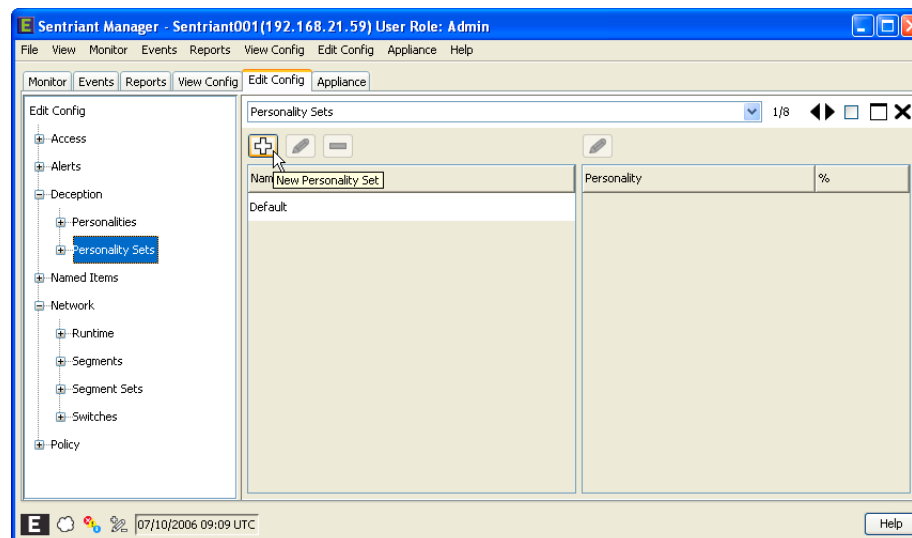
- 3 Click the **Delete Personality** button.
- 4 A dialog is displayed. Click **OK** to delete the personality.



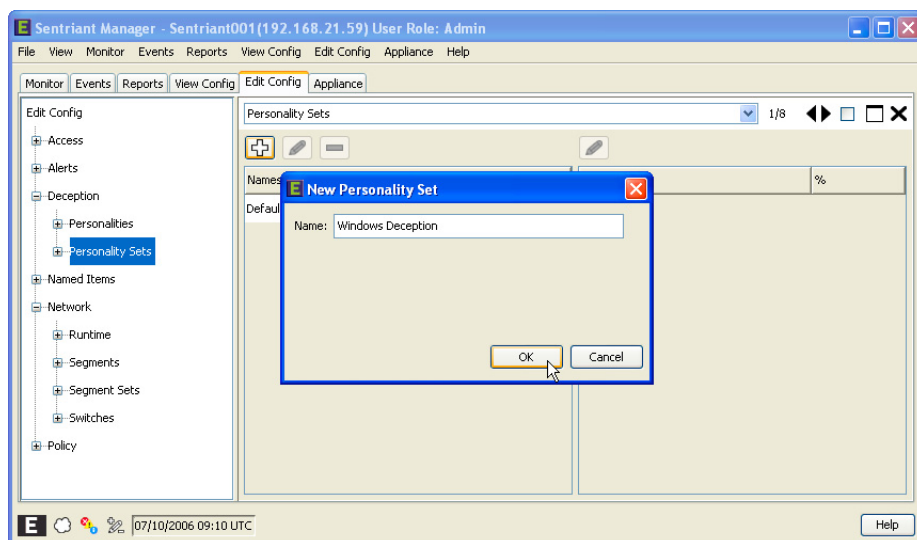
Creating Personality Sets

To create a Personality Set:

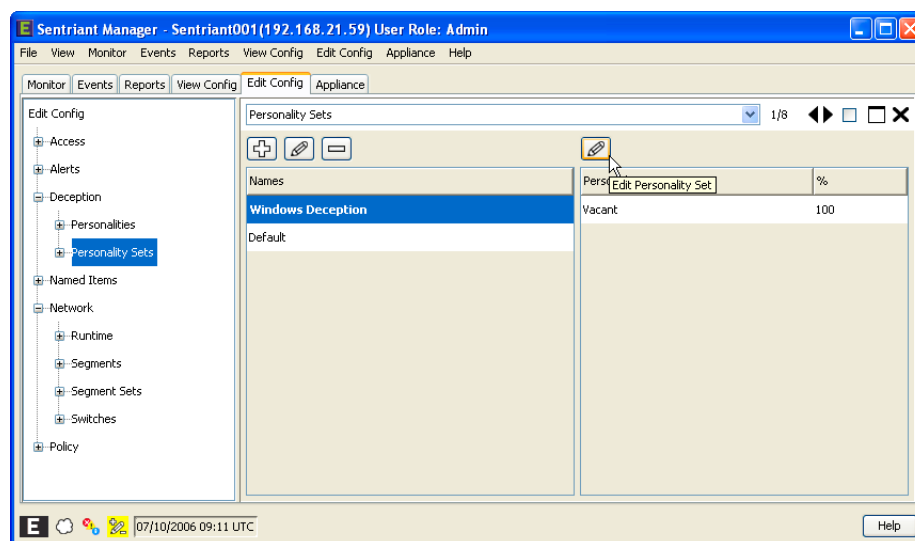
- 1 From **Edit Config > Deception**, select **Personality Sets**.
- 2 Click the **New Personality Set** button.



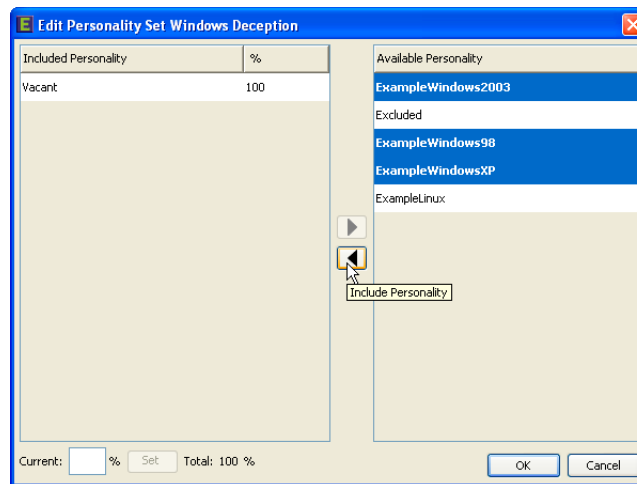
- 3 Type a name for the new personality.
- 4 Click **OK**.



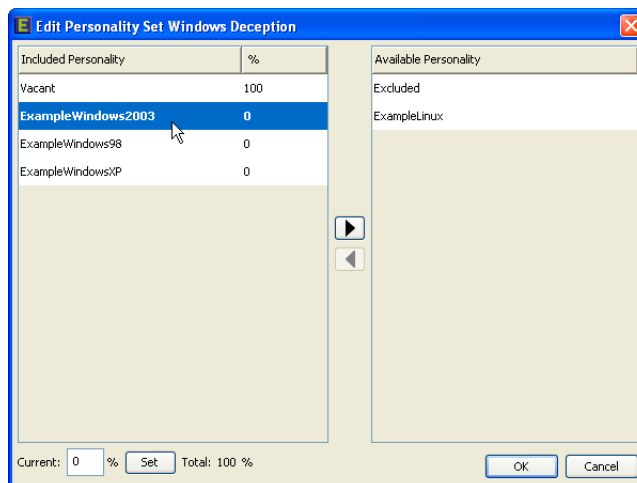
- 5 Select the new Personality Set from the list.
- 6 Click the **Edit Personality** button.



- 7 Select an **Available Personality** from the **Available Personality List**. You may Shift-Click or Ctrl-Click to select a range.
- 8 Click the **Include Personality** button.



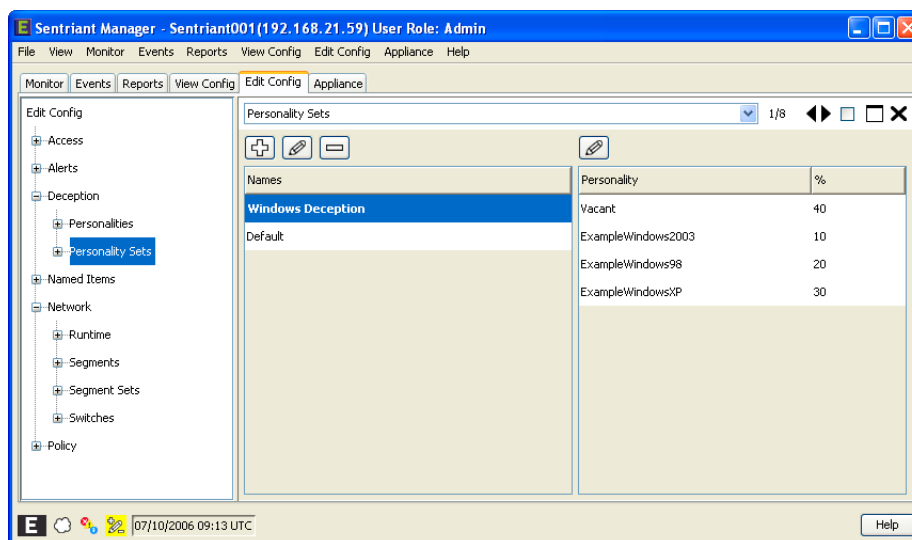
- 9 Select a personality from the Included Personality list and change the percentage.



NOTE

The Vacant personality is default and cannot be changed manually. As you add personalities and assign a deception percentage, the vacant total is decreased. If you attempt to add more than 100 percent, a dialog is displayed indicating over allocation.

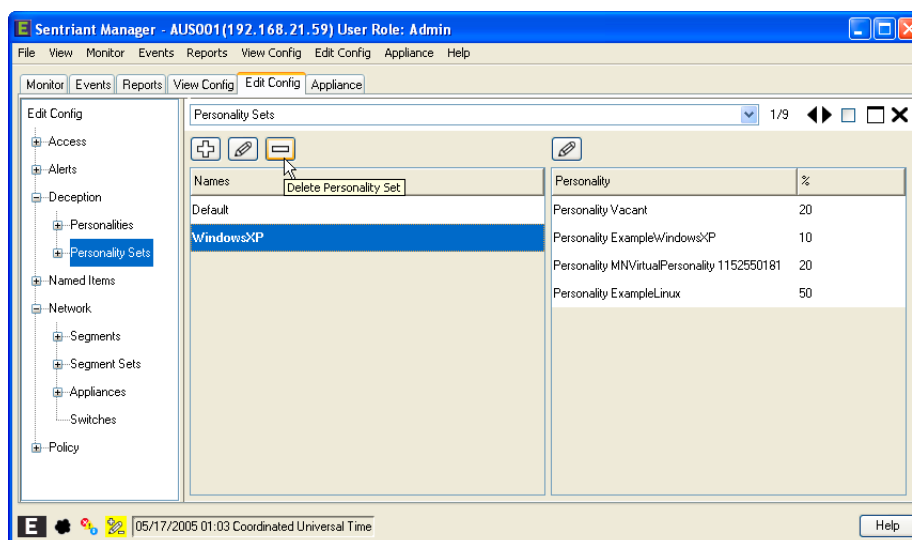
- 10 Enter a deception percent value in the **Current** field.
- 11 Click the **Set** button.
- 12 Continue changing the deception percent values for each personality.
- 13 Click **OK**.



Deleting Personality Sets

To delete a Personality Set:

- 1 From **Edit Config > Deception**, select **Personality Sets**.
- 2 Select a personality from either the Folder List or by selecting from the drop-down list in the Information Panel.



- 3 Click the **Delete Personality Set Name** button.
- 4 A dialog is displayed. Click **OK** to delete the personality.

Named Items

Named Items are groups or sets of information that can be applied and reused when configuring Segment and Policy objects without the need to re-enter data. For example, in a large environment containing several Sentriant NG appliances monitoring 10, 12, or more segments, it would be time consuming to enter all the Segment IP Addresses for deception, never cloak, deceive and other related IP Address setting for Segments, Segment Sets, and Policies. Upon completing configuration for one Sentriant NG appliance, the Named Items can be exported to the other appliances and applied. Benefits of creating Named Items include:

- Completing environment settings quickly with fewer errors
- Sets can be applied to added Sentriant NG appliances within the Fabric
- Updates made to the named sets are trickled down respective configuration settings

There are three Named Item sets. Each set is based on the type of information and how it will be utilized by the Sentriant NG appliance during monitoring, detection and mitigation actions. These sets are:

IP Sets - contain an IP Address or collection of IP Addresses

Port Sets - contain a Port number and Port protocol or collection of Port numbers and a Port protocol

Traffic Sets - contain a collection of five (5) pieces of data that defines a traffic item which specify Source and Target traffic monitored by the Sentriant NG appliance



NOTE

When deleting Named Sets, care must be taken. Named Sets, if used in the above configuration items will be removed once you save the configuration changes to the Sentriant NG appliance. A list of each object using the Named Sets will be displayed in the Configuration Dialog.

Creating IP Sets

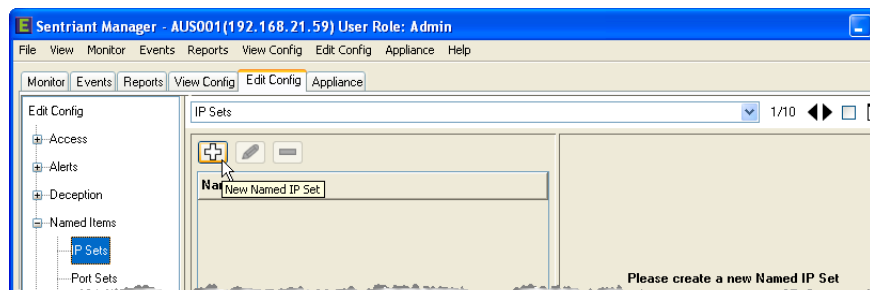
Each set is given a unique name and then IP Addresses are added to the set. An IP Address can be added per line or multiple IP Addresses may be added a line at a time. A line can be a single IP Address or wildcards may be used. For example to select the entire range of IP Addresses use an asterisk (*). You may also specify ranges for an octet of the IP Addresses. You can use commas (,) and dashes (-) for multiple ranges. For example (192.168.21,23.* or 192.168.25.1-254).

Named IP Sets can be used to populate the following configuration parameters (click an item to learn how to use a Named Set):

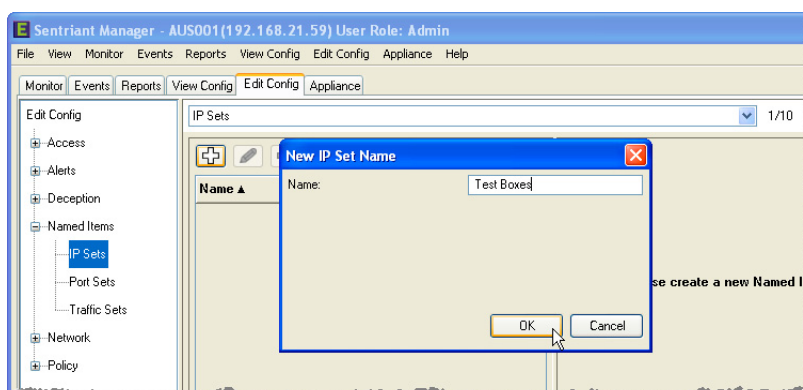
- **Edit Config > Network Activity > Segment Sets > Policy-Deception > Excludes from Rule Responses**
- **Edit Config > Network Activity > Segments > Deception**
- **Edit Config > Named Items > Traffic Sets**

To create an IP Set:

- 1 From **Edit Config > Network > Named Items**, select **IP Sets**.
- 2 Click the **New Named IP Set** button.

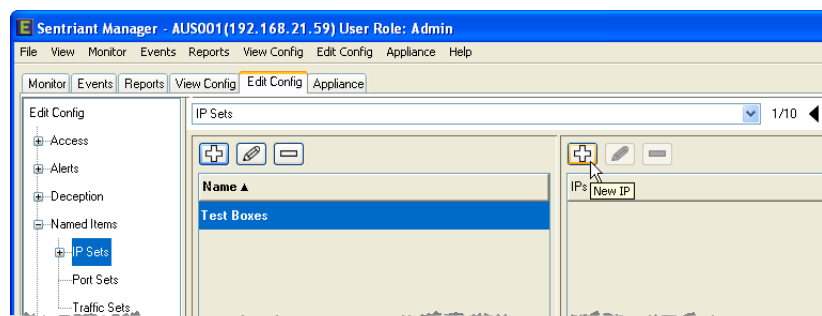


- 3 Type in a name for the new Named IP Set and click **OK**.

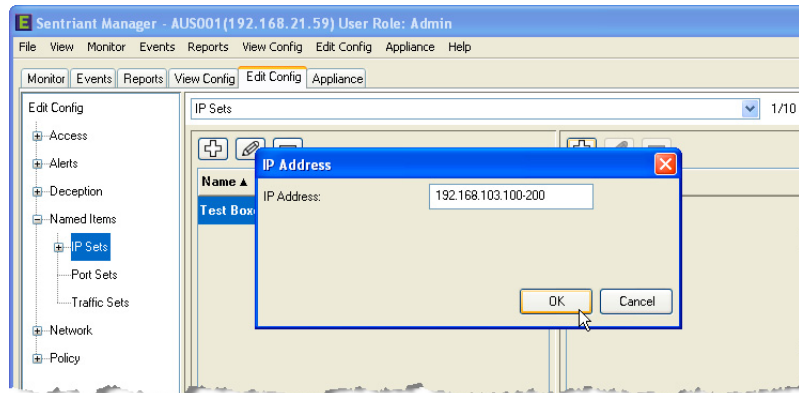


Once an IP Set has been created you may begin adding IP Addresses.

- 4 Select the Named Set and then click the **New IP Set** button.



- 5 Type an IP Address and click **OK**. The example shows an IP Address using the asterisk(*) wildcard for one of the octets which selects the entire octet range.



The new IP Set is added to the list. You may continue adding IP Sets to the Named list as necessary.



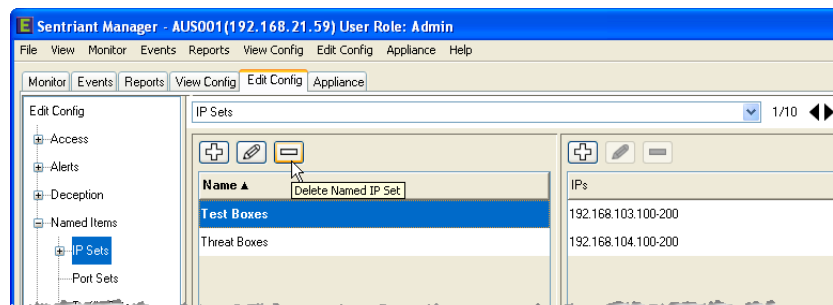
NOTE

Clicking OK adds the new Named Set to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see [“Saving Changes to the Sentriant NG Appliance” on page 133.](#)

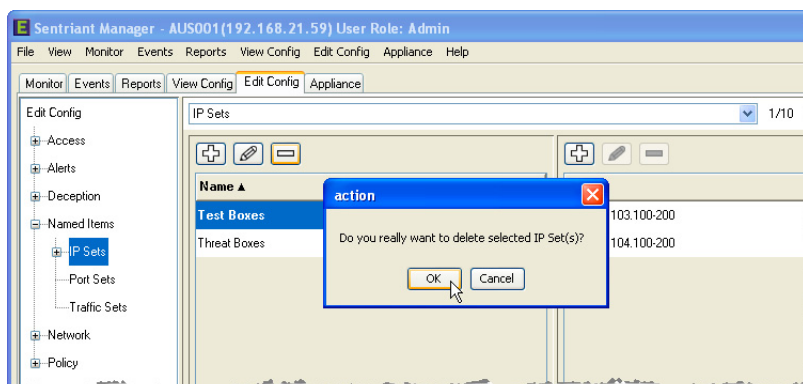
Deleting IP Sets

To delete an IP Set:

- 1 From **Edit Config > Network**, select **IP Sets**.
- 2 Select an **IP Set** and then click the **Delete Named IP Set** button. To select multiple Named IP Sets, either Shift-click or Ctrl-click.



- 3 Click **OK**.



The IP Set is marked for deletion with a minus sign in the Folder and Tab tree but not deleted from the IP Sets list. Also, the Configure Changes icon is highlighted stating that there are changes to be persisted to the Sentriant NG appliance.

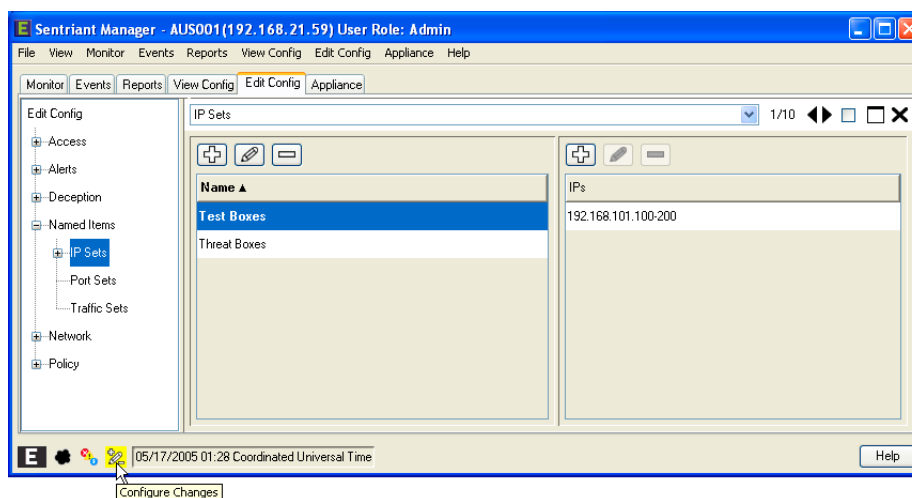
NOTE

When deleting Named Sets, care must be taken. Named Sets, if used in configuration items, will be removed once you save the configuration changes to the Sentriant NG appliance.

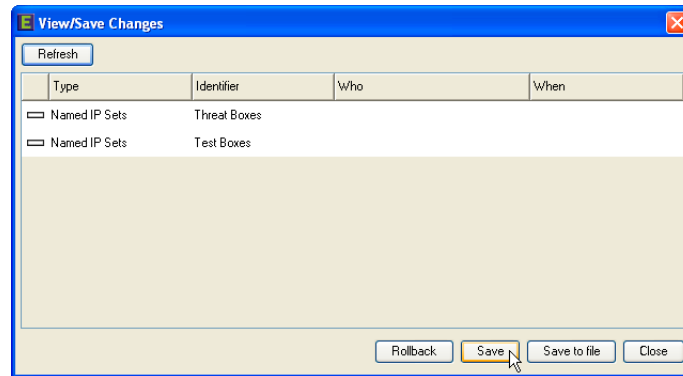
NOTE

Clicking OK changes the state of the IP Set to delete in the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration.

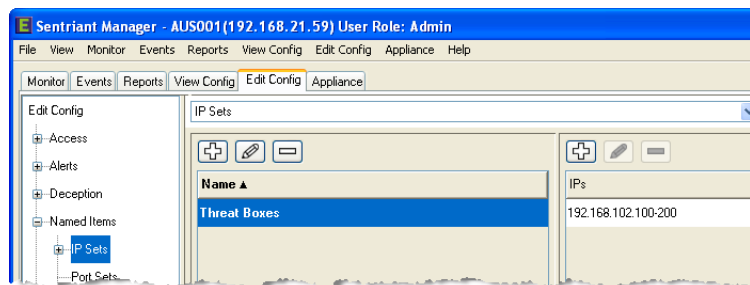
- 4 Click the **Configure Changes** button in the General Status Bar to persist the changes.



- 5 In the Configure Changes dialog, you will see a list of objects and the types of pending changes. Click the **Save** button to save the new configuration changes to the Sentriant NG appliance.



Once the configuration changes have persisted, the IP Sets are deleted and the panel is refreshed.



Creating Port Sets

When creating a Port Set with multiple Port numbers, you may only select one Port protocol. For example, a Port Set is created containing Port numbers 3, 4, 56-200. The Port protocol can either be UDP or TCP.

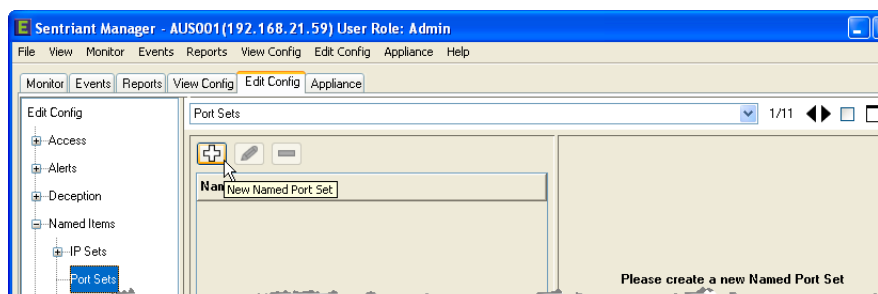
Each set is given a unique name and then Port numbers and Port protocol is added a line at a time. A line can be a single Port number or wildcards may be used. For example to select a range of Port numbers use commas(,) or dashes (-) for multiple ranges. For example (1,2,23,112 or 1-119, or 1,2,3,100-200).

Named Port Sets can be used to populate the following configuration parameters:

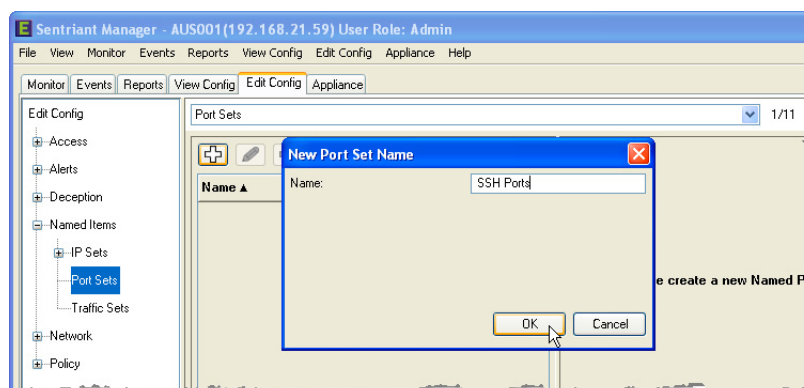
- Edit Config > Deception > Personalities > **Ports**
- Edit Config > Named Items > **Traffic Sets**

To Create a Port Set:

- 1 From **Edit Config > Network > Named Items**, select **Port Sets**.
- 2 Click the **New Named Port Set** button.

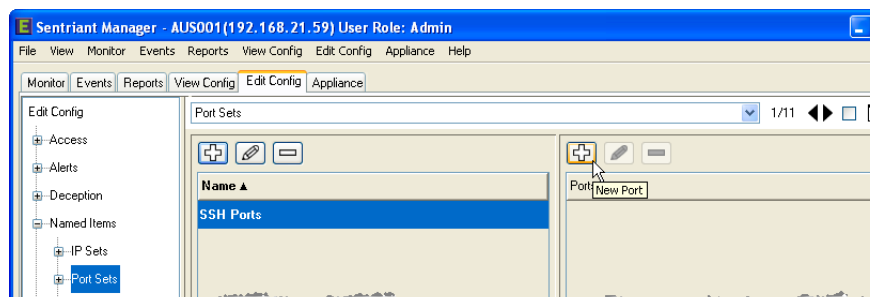


- 3 Type in a name for the new Named Port Set and click **OK**.

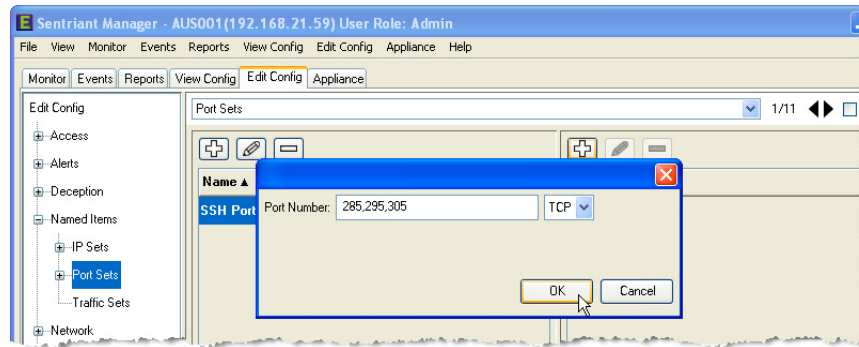


Once a Port Set has been created you may begin adding Port numbers.

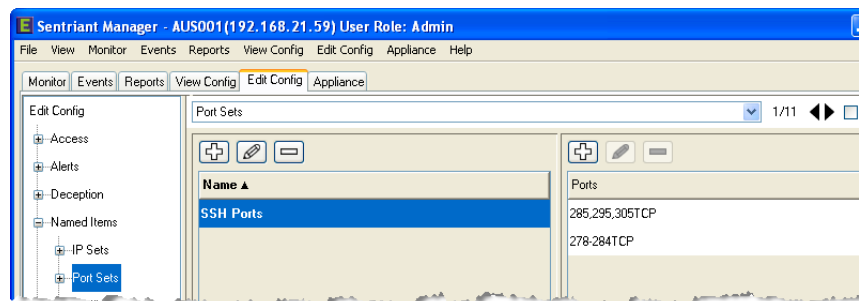
- 4 Select the Port Named Set and then click the **New Port Set** button.



- 5 Type a Port number and click **OK**. The example shows a set of Port numbers using a comma(,) wildcard.



The new Port Set is added to the list. You may continue adding Port numbers to the Named list as necessary.



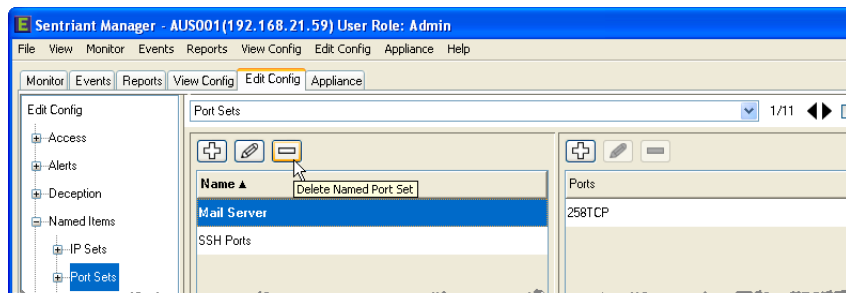
NOTE

Clicking OK adds the new Named Set to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#).

Deleting Port Sets

To delete a Port Set:

- 1 From **Edit Config > Network > Named Items**, select **Port Sets**.
- 2 Select an IP Set and then click the **Delete Named Port Set** button. To select multiple Named Port Sets, either Shift-click or Ctrl-click.



- 3 Click OK.

The IP Set is marked for deletion with a minus sign in the Folder and Tab tree but not deleted from the IP Sets list. Also, the Configure Changes icon is highlighted stating that there are changes to be persisted to the Sentriant NG appliance.

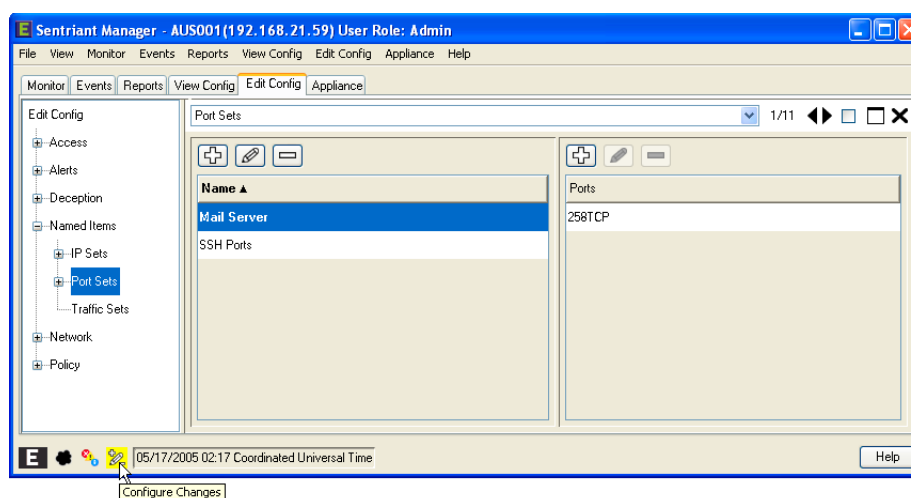
**NOTE**

When deleting Named Sets, care must be taken. Named Sets, if used in configuration items, will be removed once you save the configuration changes to the Sentriant NG appliance.

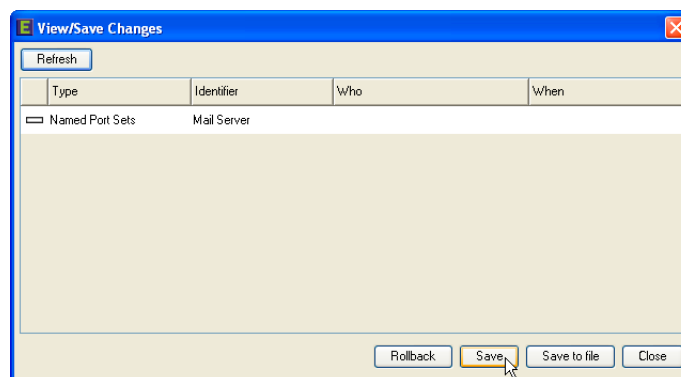
**NOTE**

Clicking OK changes the state of the IP Set to delete in the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration.

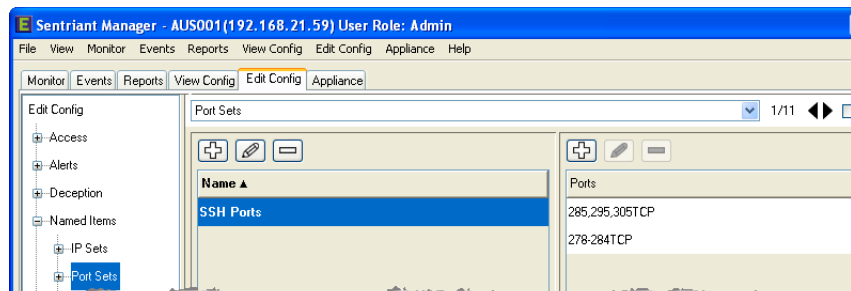
- 4 Click the **Configure Changes** button in the General Status Bar to persist the changes.



- 5 In the Configure Changes dialog, you will see a list of objects and the types of pending changes. Click the **Save** button to save the new configuration changes to the Sentriant NG appliance.



Once the configuration changes have persisted, the IP Sets are deleted and the panel is refreshed.



Creating Traffic Sets

A traffic item may contain only one piece of data to be considered a complete set. For example, you may create a traffic item with only one Source IP Address and the Port protocol.

Each Traffic set is given a unique name and then Source and/or Traffic IP Addresses, Port numbers and a Port protocol is added a line at a time.



NOTE

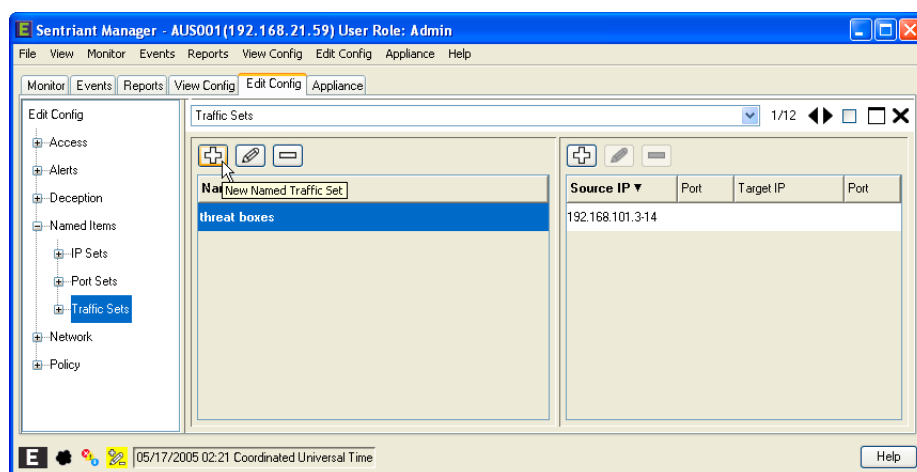
Traffic Sets can be created using IP Sets and Port Sets.

Named Traffic Sets can be used to populate the following configuration parameters:

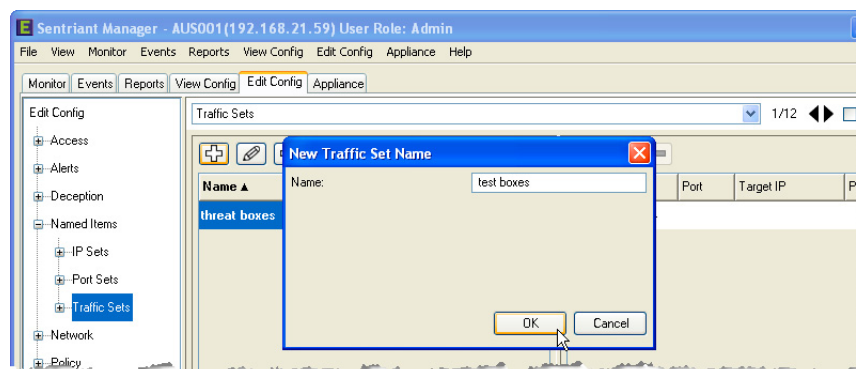
- Edit Config > Network > Segment Sets > Policy-Deception > **Omit**
- Edit Config > Network > Policy > Rules > **Include**
- Edit Config > Network > Policy > Rules > **Exclude**

To Create a Traffic Set:

- 1 From Edit Config > Network > Named Items, select **Traffic Sets**.
- 2 Click the **New Named Traffic Set** button.

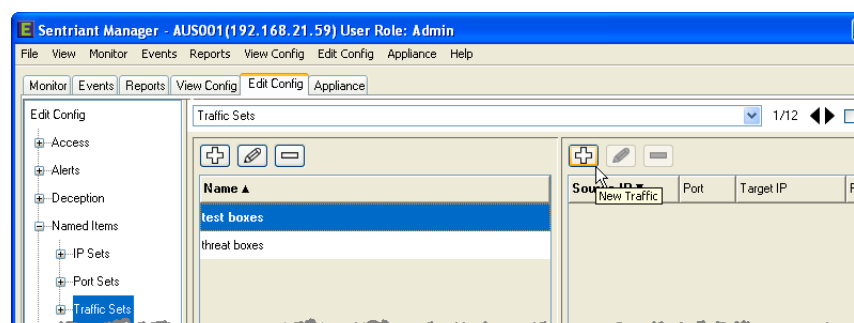


- 3 Type in a name for the new Named Traffic Set and click **OK**.



Once a Traffic Set has been created you may begin adding traffic data.

- 4 Select the Traffic Named Set and then click the **New Traffic** button.



Adding Traffic Data

The procedures described below demonstrate how to enter each piece of data for a Traffic item, however new traffic items may contain only one piece of data to be considered complete, for example, you may create a traffic item with only one Source IP Address.

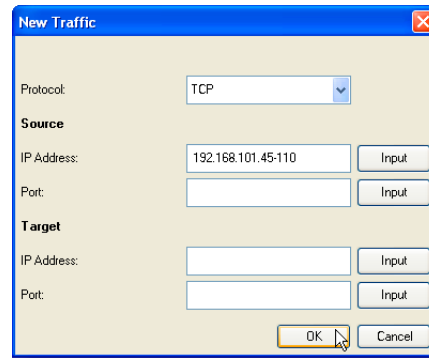
Traffic items can be created using IP Sets and Port Sets. However, when using Port Sets, the Port protocol of the New Traffic takes precedence over the Port Set and may disable the Source or Target Port Set entry. For example, You've created a Port Set with UDP as the Port protocol and now want to create a Traffic Set. If you set the Port protocol in the New Traffic Set dialog as TCP, Port Sets with a protocol of UDP will not be visible in the selector.

- 5 Select a Port Protocol from the drop-down list. Choices are TCP, UDP, and ICMP.
- 6 Enter a Source IP Address by one of the two methods:
 - Type an IP Address in the Source IP Address field. The example shows an IP Address using the hyphen (-) wildcard for one of the octets which selects a range of the octet.
 - Use an IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.



NOTE

To revert back to entering an IP Address, click the **Select** button.



New Traffic

Protocol: TCP

Source

IP Address: 192.168.101.45-110 Input

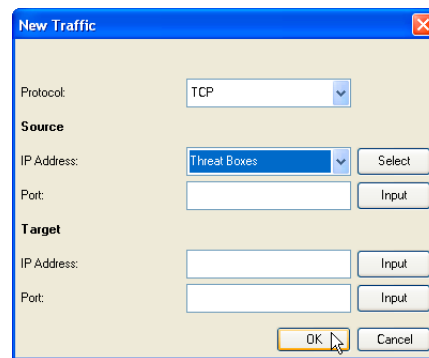
Port: Input

Target

IP Address: Input

Port: Input

OK Cancel



New Traffic

Protocol: TCP

Source

IP Address: Threat Boxes Select

Port: Input

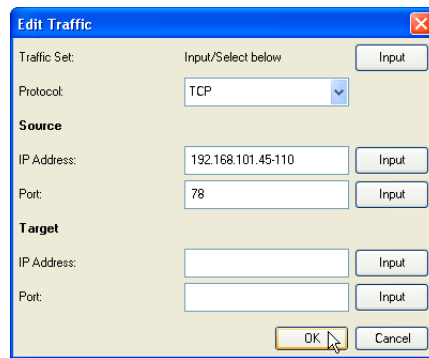
Target

IP Address: Input

Port: Input

OK Cancel

- 7 Enter a Source Port Number by one of the two methods:
- 8 Type a Port number in the Source Port field.
- 9 Use a Port Set by clicking the **Input** button and then selecting a Port Set from the drop-down list.



Edit Traffic

Traffic Set: Input/Select below Input

Protocol: TCP

Source

IP Address: 192.168.101.45-110 Input

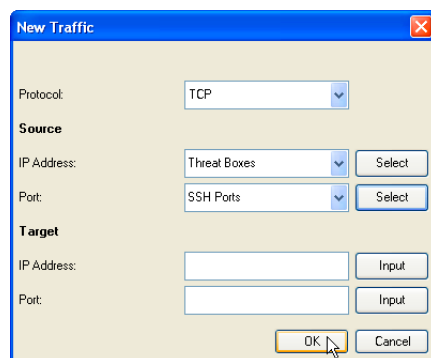
Port: 78 Input

Target

IP Address: Input

Port: Input

OK Cancel



New Traffic

Protocol: TCP

Source

IP Address: Threat Boxes Select

Port: SSH Ports Select

Target

IP Address: Input

Port: Input

OK Cancel

10 Enter a Target IP Address by one of two methods:

- Type an IP Address in the Targets IP Address field.
- Use a IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.

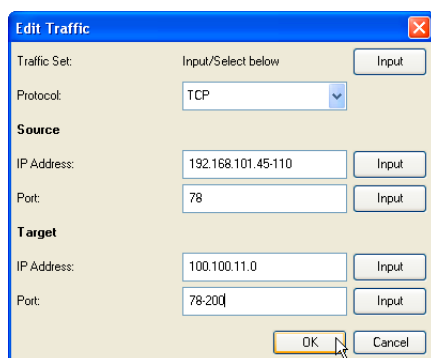


NOTE

To revert back to entering an IP Address, click the **Select** button.

11 Enter a Source Port Number by one of two methods:

- Type a Port number in the Source Port field.
- Use a Port Set by clicking the **Input** button and then selecting a Port Set from the drop-down list.



Edit Traffic

Traffic Set: Input/Select below Input

Protocol: TCP

Source

IP Address: 192.168.101.45-110 Input

Port: 78 Input

Target

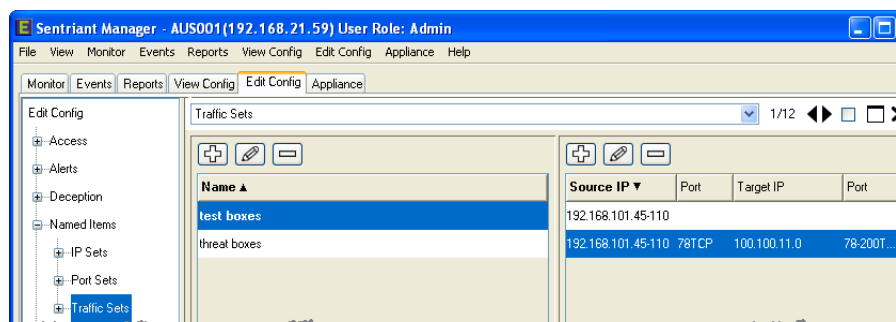
IP Address: 100.100.11.0 Input

Port: 78-200 Input

OK Cancel

12 Click **OK** to save the new Traffic item.

The new Traffic item is added to the list. You may continue adding new Traffic items to the Named list as necessary.



Sentriant Manager - AUS001(192.168.21.59) User Role: Admin

File View Monitor Events Reports View Config Edit Config Appliance Help

Monitor Events Reports View Config Edit Config Appliance

Traffic Sets 1/12

Name ▲	Source IP ▼	Port	Target IP	Port
test boxes	192.168.101.45-110			
threat boxes	192.168.101.45-110	78TCP	100.100.11.0	78-200T...

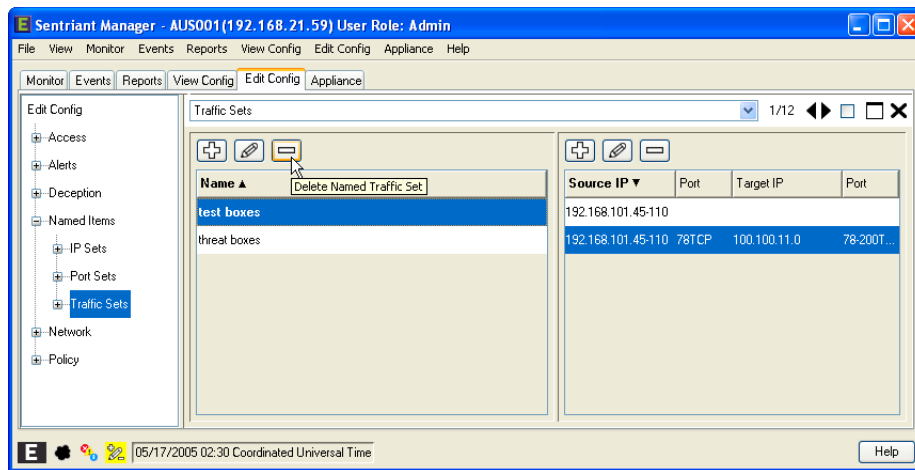
**NOTE**

Clicking OK adds the new Named Set to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see [“Saving Changes to the Sentriant NG Appliance” on page 133.](#)

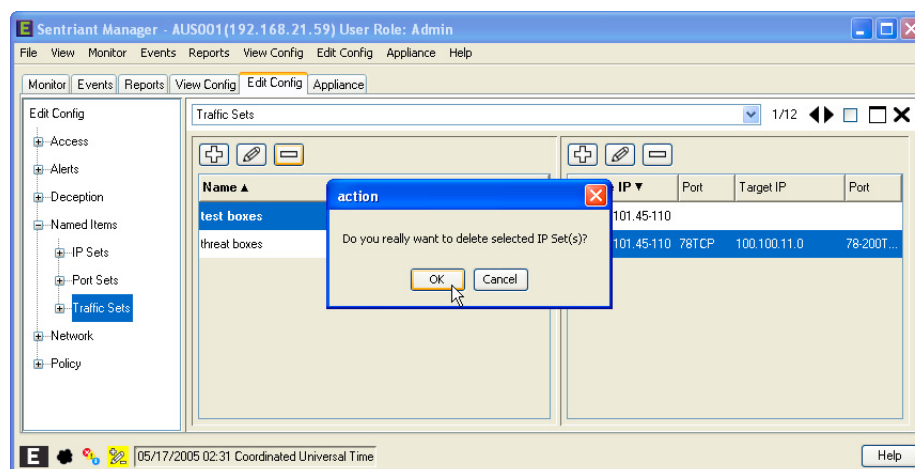
Deleting Traffic Sets

To delete a Traffic Set:

- 1 From **Edit Config > Network > Named Items**, select **Traffic Sets**.
- 2 Select a Traffic Set and then click the **Delete Named Traffic Set** button. To select multiple Named Traffic items, either Shift-click or Ctrl-click.



- 3 Click **OK**.



The IP Set is marked for deletion with a minus sign in the Folder and Tab tree but not deleted from the IP Sets list. Also, the Configure Changes icon is highlighted stating that there are changes to be persisted to the Sentriant NG appliance.

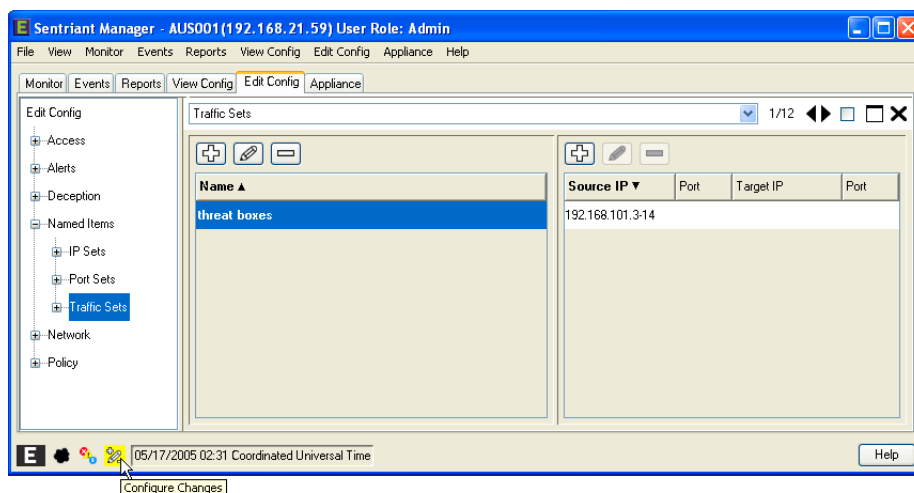
**NOTE**

When deleting Named Sets, care must be taken. Named Sets, if used in configuration items, will be removed once you save the configuration changes to the Sentiangt NG appliance.

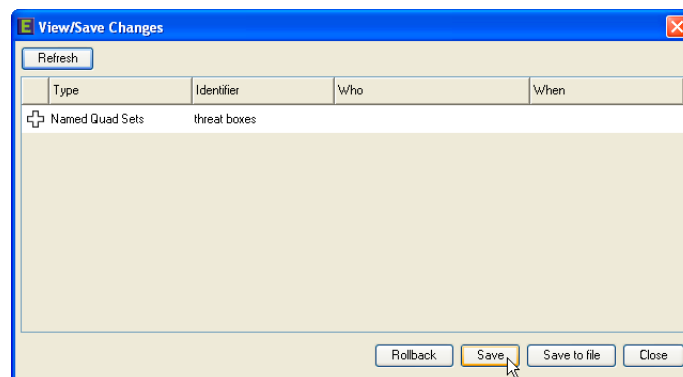
**NOTE**

Clicking OK changes the state of the IP Set to delete in the stack of local configuration changes however, it does not update the Sentiangt NG appliance's configuration.

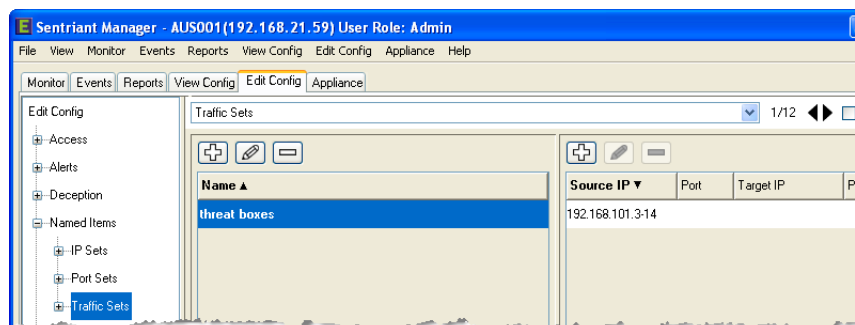
- 4 Click the **Configure Changes** button in the General Status Bar to persist the changes.



- 5 In the Configure Changes dialog, you will see a list of objects and the types of pending changes. Click the **Save** button to save the new configuration changes to the Sentiangt NG appliance.



Once the configuration changes have persisted, the IP Sets are deleted and the panel is refreshed.



Network

On initial install, the Sentriant NG will monitor traffic on its Ethernet ports (and trunks) to determine the range of Segments it can access. This information is made available to the user via the **Configure > Network > Segments** page. It is necessary for the administrator to edit the supplied information and enable the Segment for monitoring.

A Segment Set is a collection of segments that exhibit similar policy behaviors. For example, if a Segment Set is reserved for DHCP clients (laptops), then a set can be created containing all laptops within a Segment and then parameters can be set for rules, deception distributions and modifiers. Creating segments is accomplished using the Segment Assistant.

A default Segment Set is created initially. All discovered or unconfigured segments will be added to the default set and can later be moved to newly created Segment Sets.

Before a Segment can be monitored by the Sentriant NG appliance the ports must be enabled. The Segments Panel and Physical Panel contain Port information in two formats. The Segment Panel displays logical ports relative to the Segment. The Physical Panel displays information with a hierarchy from the Sentriant NG appliance to the physical ports to the logical ports. Segment information is also displayed at the logical Port level. Actions can be taken at all levels in the hierarchy.

The Network panel contains detailed areas showing specific information under each tab. These tabs are as follows:

- **Runtime** - Configure discovered segments and view Sentriant NG appliance's physical and logical interfaces
- **Segments** - Create and manage Segment Sets and logical ports
- **Segment Sets** - Create and assign segments to a set
- **Switches** - Identify and manage the switch that an appliance is connected to and monitoring

Saving Changes to the Sentriant NG

As you set up segments to be monitored, configuration settings are not saved to the Sentriant NG appliance immediately, but rather are saved locally until the configuration changes have been completed. This lets you configure a Segment completely before saving to the Sentriant NG appliance preventing erroneous threats in the Monitoring Panel with incomplete Segment configurations. (See [“Saving Changes to the Sentriant NG Appliance”](#) on page 133.)

Runtime

The Runtime tab represents the network topology from a Segment and interface view. The Segment tab displays all discovered segments. The Interface tab displays the Sentriant NG appliance's physical Port followed by the logical ports (VLANs) in the broadcast domain. A broadcast domain contains network segments where all network devices communicate with each other without going through a router.

From the Runtime panel you can:

- View the Sentriant NG appliance name, state, IP Address, Gateway, and Subnet Mask
- View and configure segments discovered by the Sentriant NG appliance using the Segment Assistant
- View and Edit Interface names, states, the Sentriant NG appliance where it resides, Port delay, MAC Address, speed and read-write state

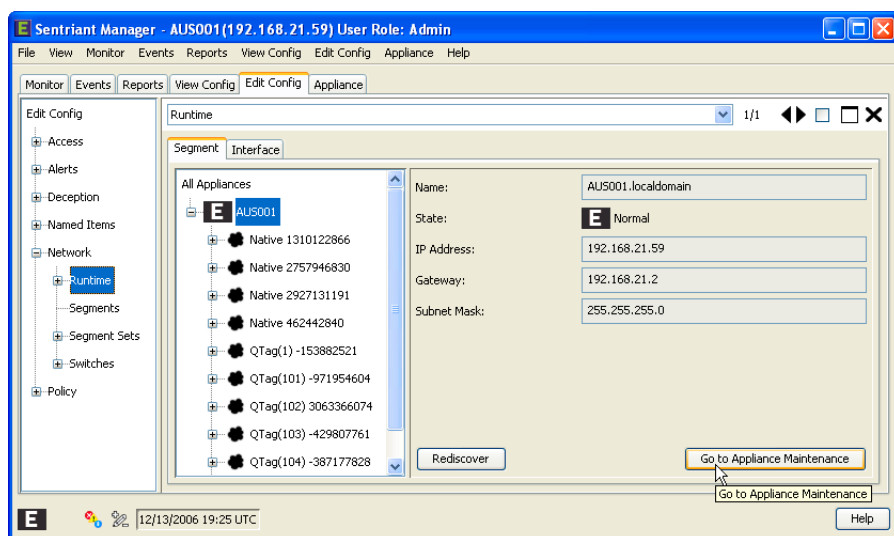
View Sentriant NG Information

Clicking on a Sentriant NG appliance in the Runtime panel will display:

- Name of the Sentriant NG appliance
- Current state or status - for example, if there is a problem with one of the physical ports the state will be set to warning
- IP Address assigned to the Sentriant NG appliance
- Gateway IP Address
- Subnet Mask IP Address

To change the name of the Sentriant NG appliance:

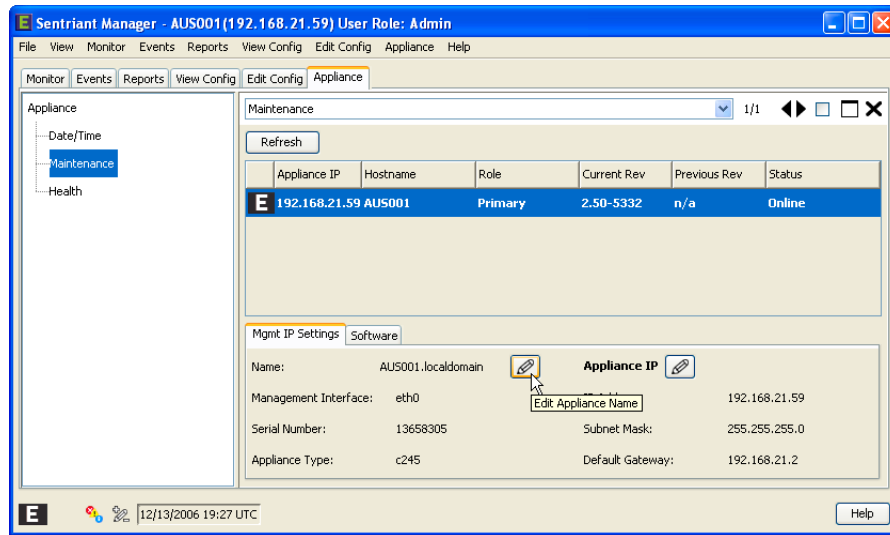
- 1 From **Edit Config > Network**, select Runtime.
- 2 Click the **Go to Appliance Maintenance** button.



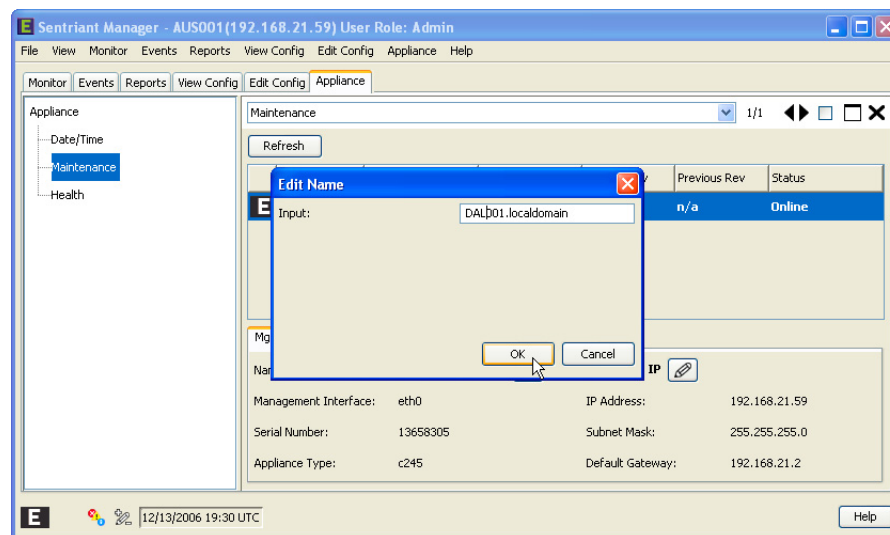
The Appliance > Maintenance page opens.

To change the name of a Sentriant NG appliance:

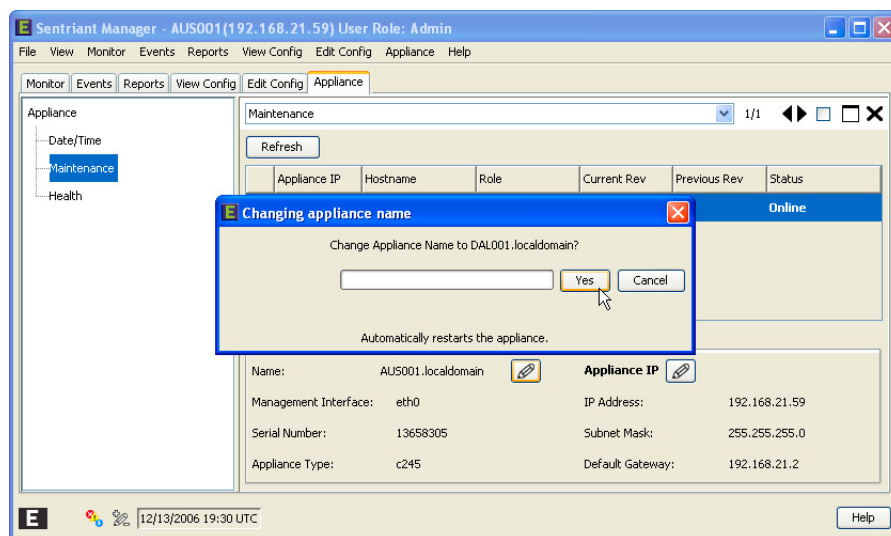
- 1 From the **Appliance > Maintenance** tab, double-click the Sentriant NG appliance.
- 2 Click the **Edit Appliance Name** button.



- 3 Enter a name. The name should be no longer than 200 characters.
- 4 Click the **OK** button.



- 5 Click Yes to save changes.

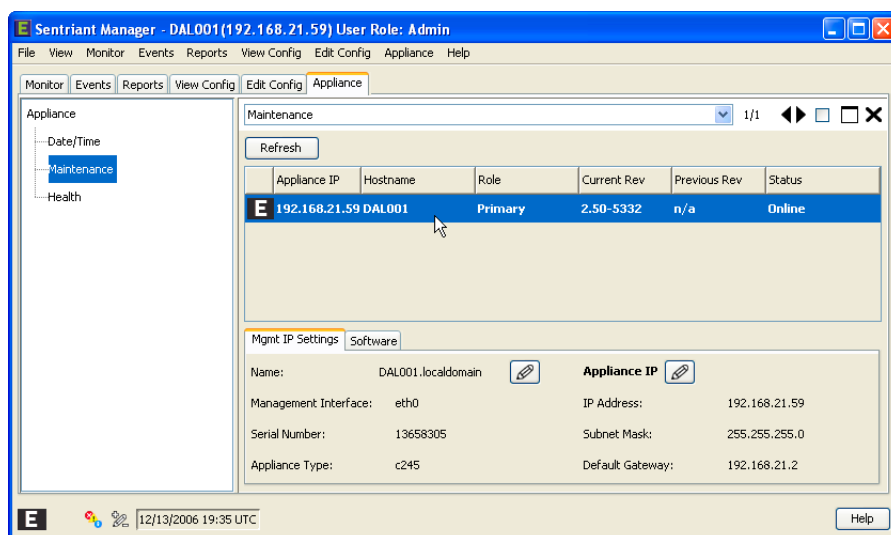


The Appliance Host Name Changed dialog is displayed. Click **Exit** to close the application and restart the appliance.

NOTE

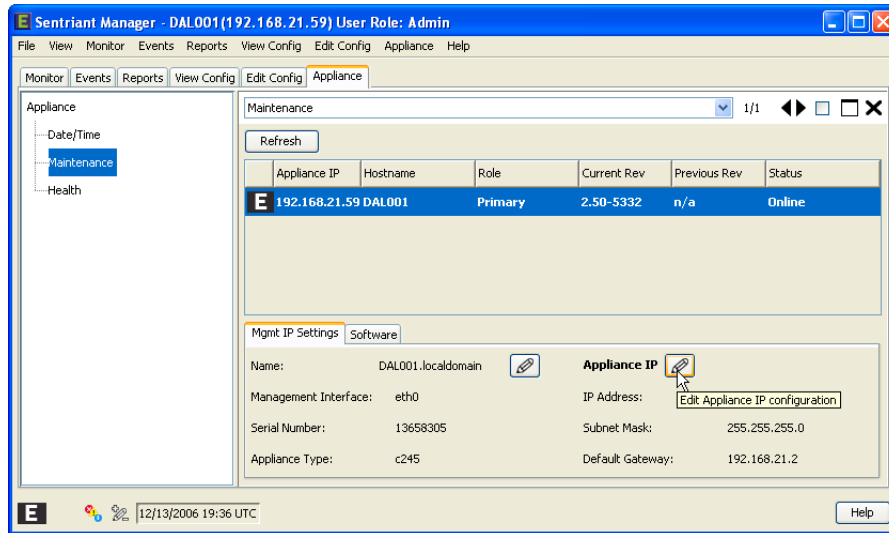
Depending on the Sentriant NG appliance and the network connection, it may take several minutes for the Sentriant NG appliance to complete the restart. Once the restart has completed, you may log back into Sentriant NG Manager. If the Sentriant NG appliance has not restarted, an error will be displayed at the Sentriant NG Manager login screen.

The appliance name has now been updated.



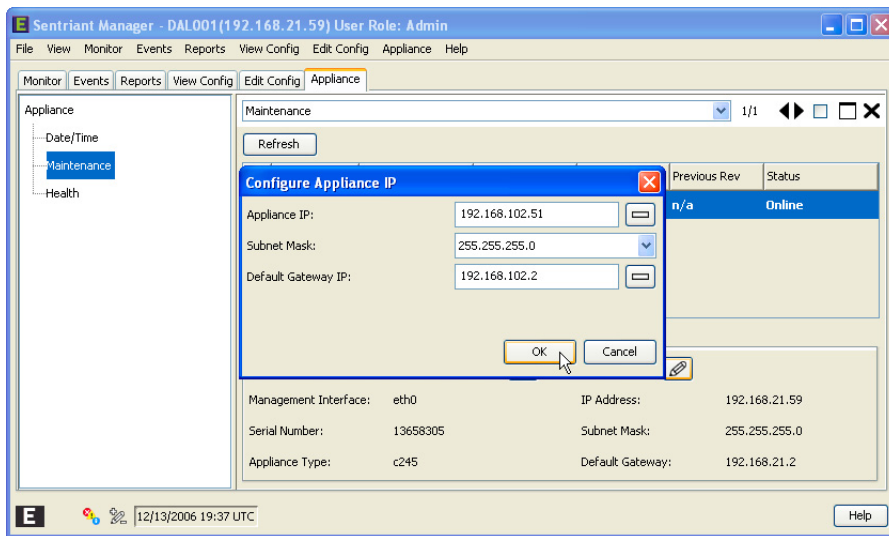
To change the IP Address of a Sentriant NG appliance:

- 1 From the **Appliance > Maintenance** tab, select a Sentriant NG appliance.
- 2 Click the **Edit Appliance IP Configuration** button.

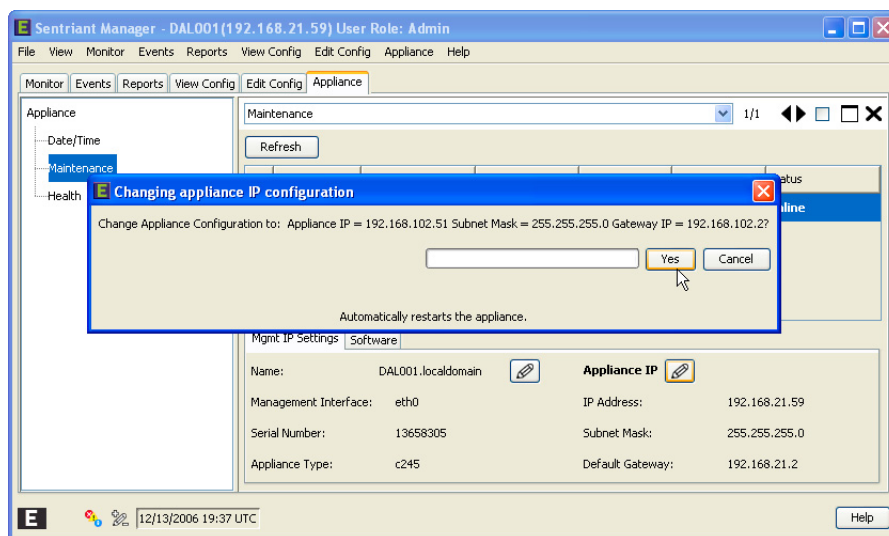


From the Configure Appliance IP dialog, you can edit or change the IP Addresses for the Appliance IP, Subnet Mask, and the Default Gateway. You may change one, all or a combination.

- 3 Enter an IP Address for each of the items that you want to change.
- 4 Click **OK**.



- 5 Click **Yes** to restart the appliance.

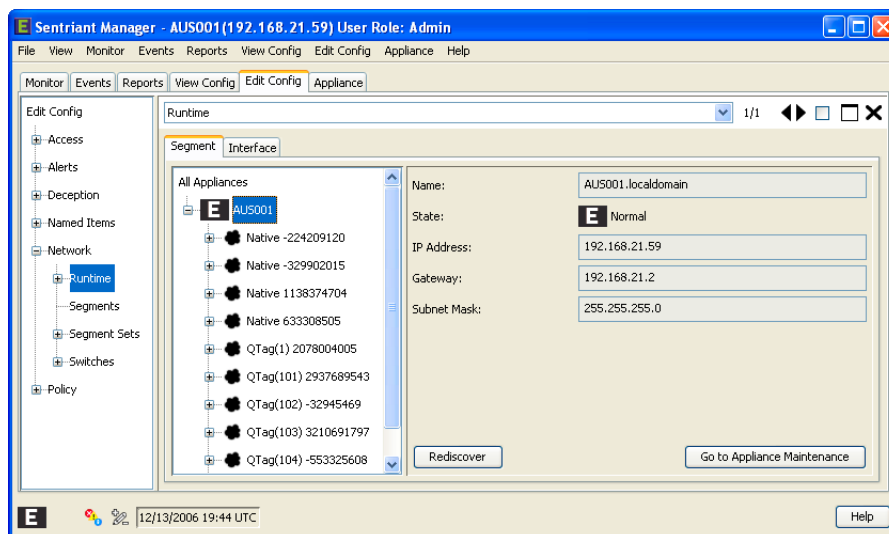


NOTE

Depending on the Sentriant NG appliance and the network connection, it may take several minutes for the Sentriant NG appliance to complete the restart. Once the restart has completed, you may log back into Sentriant NG Manager. If the Sentriant NG appliance has not restarted, an error will be displayed at the Sentriant NG Manager login screen.

View and Configure Segments

When the Sentriant NG appliance is turned on, it automatically searches for segments (VLANs) and are listed under the **Network > Runtime > Segment** tab. Clicking the **Rediscover** button will start a scan to search for segments and refresh the Segment list.



Once the segments have been discovered, they can be configured to detect and mitigate potential threats. Configuring segments is accomplished using the Segment Assistant.

The Segment Assistant guides you through the steps to specify Segment parameters. The Segment Assistant Welcome page opens when you press the **Plus** button under **Configure > Network > Runtime**.

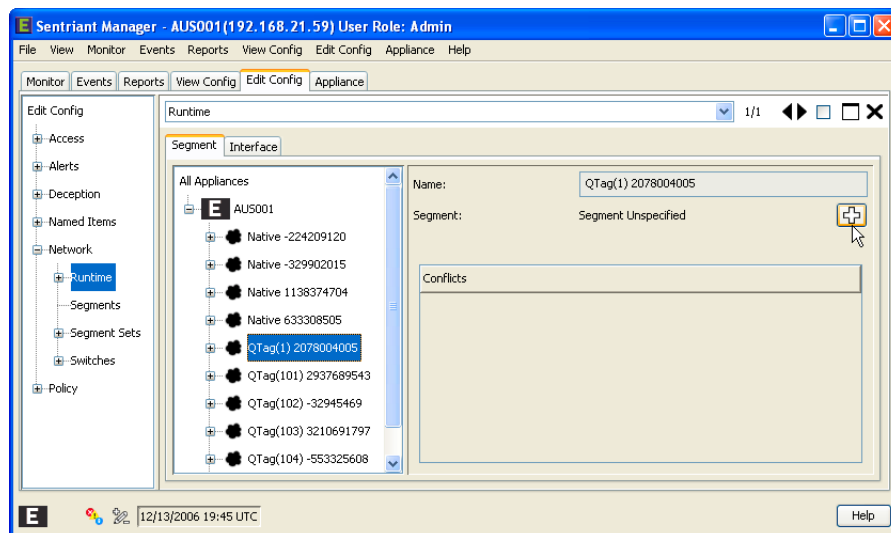
**NOTE**

Configuration changes are not committed to the Sentriant NG appliance immediately, but are kept locally until all necessary configuration activities have been completed such as Segment, rule and deception information.

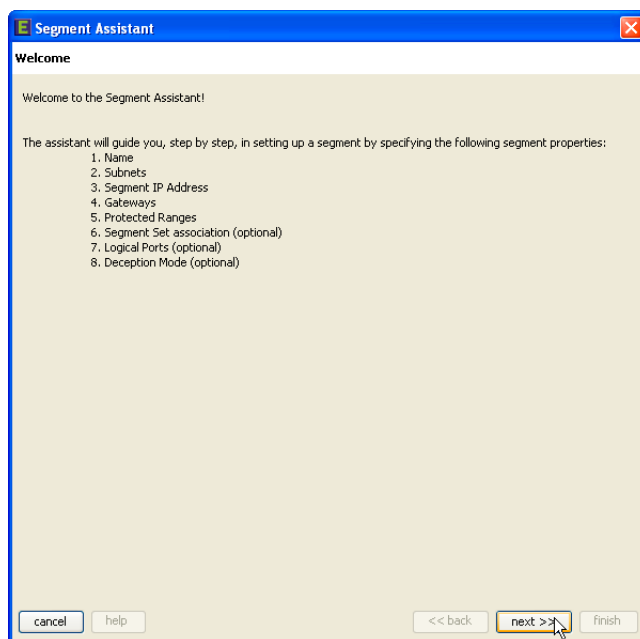
Configuring a Segment. This screen is used to configure a discovered Segment using the Segment Assistant. The first step in configuring a Segment is selecting one of the discovered segments.

To configure a Segment:

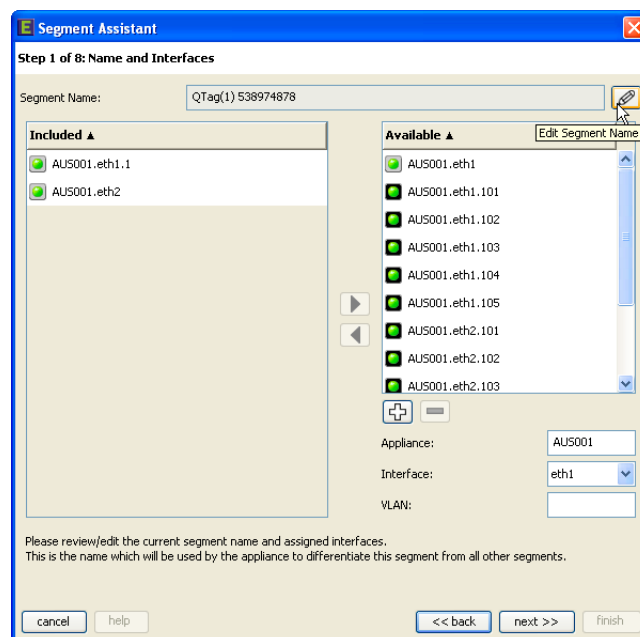
- 1 From **Configure > Network > Runtime**, select a Segment from the list.
- 2 Click the **Add** button.



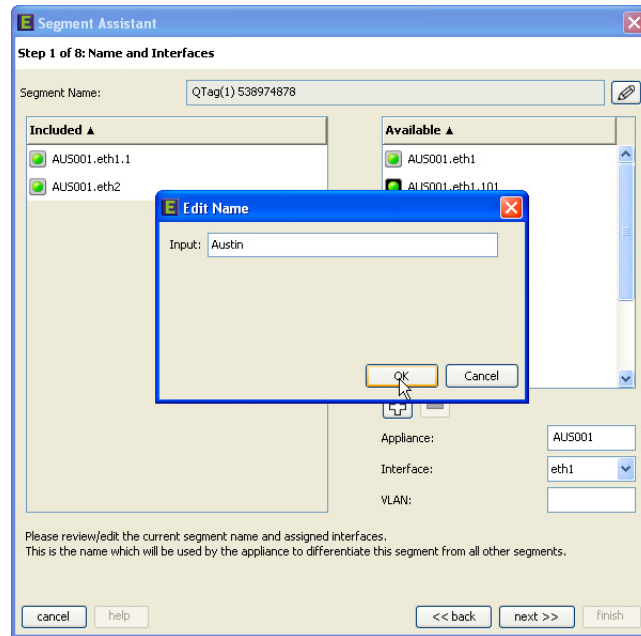
The Welcome screen displays with instructions.



- 3 Click the **next >>** button to display Step 1 of 8: Name and Interfaces screen. The name of the selected Segment is displayed in the Segment Name field.
- 4 Click the **Edit Segment Name** button.



- 5 Enter a name for the new Segment and then click **OK**.



6 Click the **next >>** button to display **Step 2 of 8 Subnets**.

Specifying Subnets. This screen is used to identify a list of subnets that will be protected within this Segment. Known subnets are populated in the Subnet Hints table.

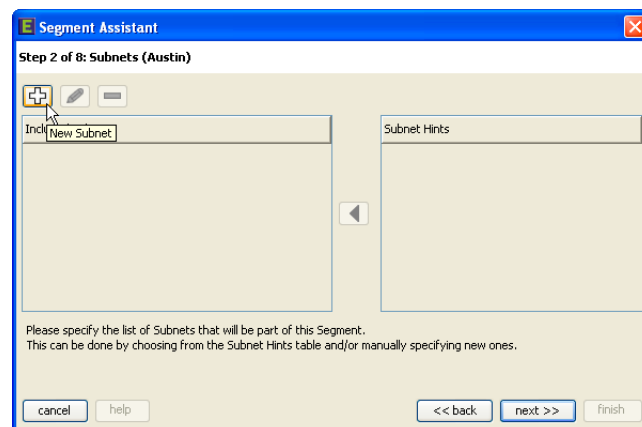


NOTE

At least one Subnet Address is needed per Segment. The purpose of the Subnet Address and Mask is to identify the broadcast domain, or ARP horizon, that the Sentriant NG appliance is operating within and identify local traffic being monitored. The Subnet is important for devices communicating on that network because it defines where to send traffic.

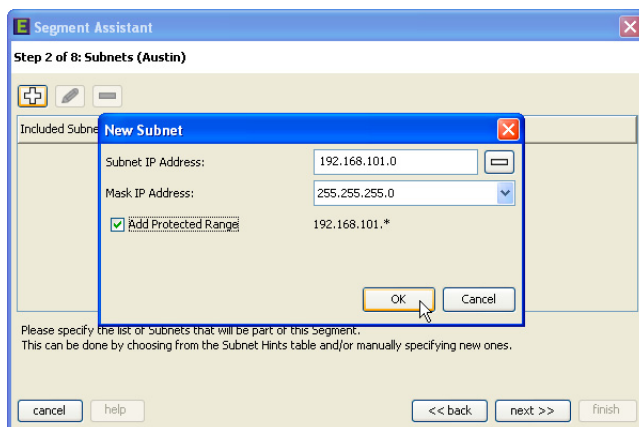
To enter a Subnet:

1 Click the **New Subnet** button located in the upper left of the screen.

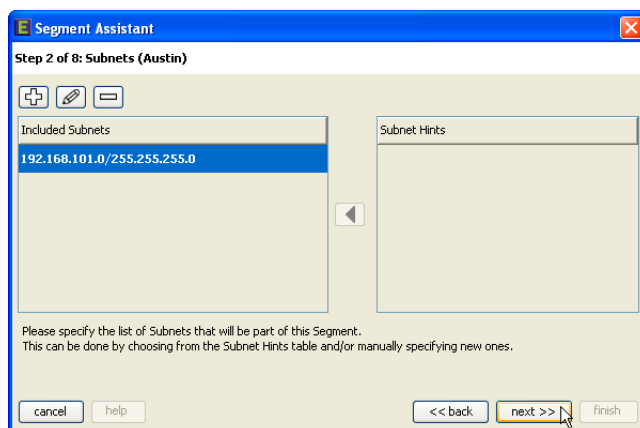


2 Enter a new subnet address.

- 3 Select a Mask IP Address from the drop-down list. Default Mask is 255.255.255.0.
- 4 To add a Protected Range of IP Addresses automatically, check the Add Protected Range box. This will set the protected range for all IP Addresses in the subnet.
- 5 Click **OK**.



The new subnet is added into the Included Subnets table.



NOTE

You may select subnet(s) from the Subnet Hints table and clicking the Add button.

- 6 Click the **next>>** button to display [Step 3 of 8: View Mgmt IP Address](#) screen.

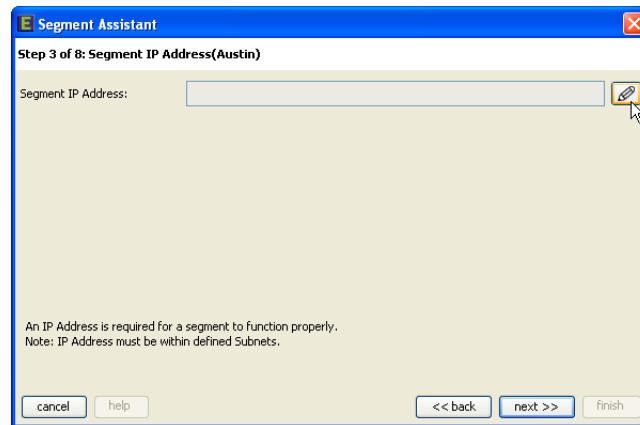
To remove a subnet:

- 1 Select the subnet from the Included Subnets table and click the **Remove** button.

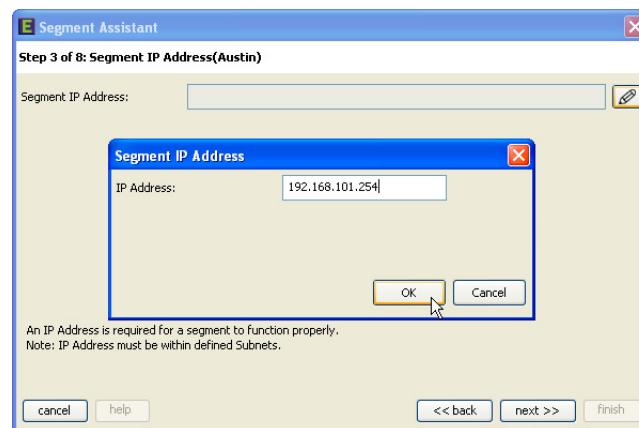
Edit Segment IP Address. This screen displays the IP Address which is used to communicate with the Sentiang NG appliance and Sentiang NG Manager for the Segment that is being configured. The Segment IP Address is set to an unused IP Address within the Segment's IP Address range.

To set the Segment's IP Address:

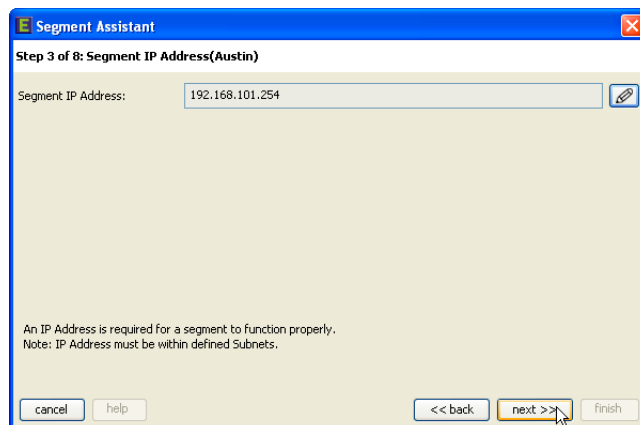
- 1 Click the **Edit Segment IP Address** button.



- 2 Enter a Segment IP Address and click **OK**.



- 3 Click the **next >>** button to display **Step 4 of 8: Gateways** screen.

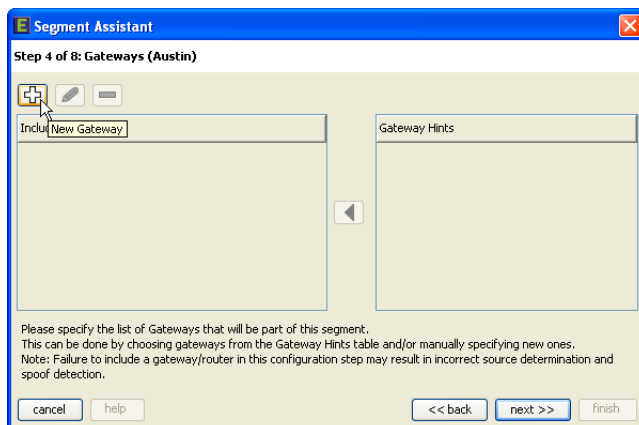


Setting Gateways. This screen is to specify the Gateway or Gateways for the Segment. The purpose of setting the Gateway is to inform the Sentriant NG appliance of which devices are forwarding traffic from other segments. The Sentriant NG appliance uses its spoofing detection technology to determine

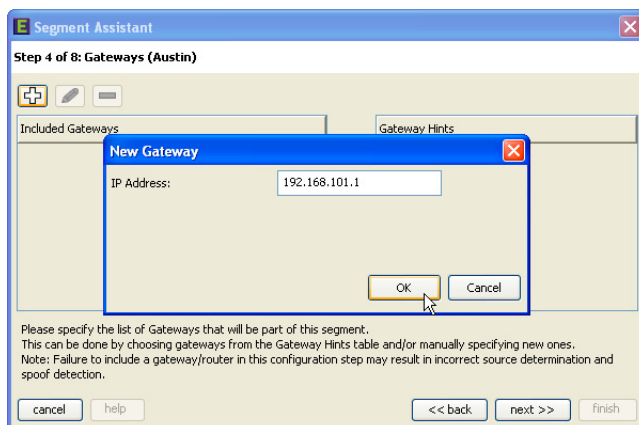
that all received packets were transmitted from the source listed as the source address in the packet thereby validating traffic received, that it came from the correct host, and that traffic from remote segments entered the network via a gateway.

To add a Gateway:

- 1 Click the **New Gateway** button located in the upper left of the screen.



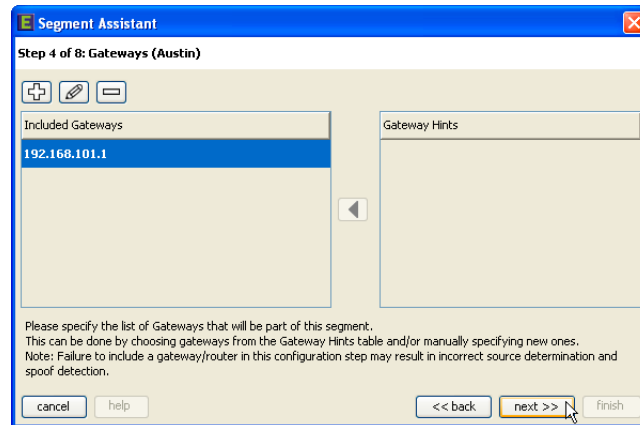
- 2 Enter the Gateway address and then click **OK**.



NOTE

Adding invalid gateway IP Addresses that do not represent a real host will cause spoof detection to be disabled. All gateways must respond to ARP communication.

The gateway is added to the Included Gateways table. Adding gateways to a Segment is optional and will reduce the amount of traffic if the spoof rule is invoked. (See [“Rules” on page 255.](#))



NOTE

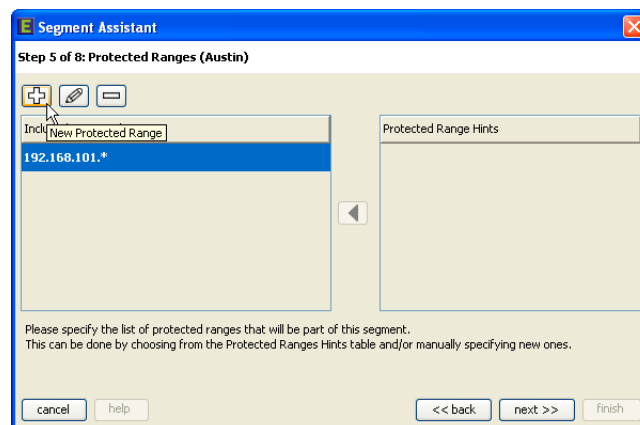
You may select gateway(s) from the Gateway Hints table by clicking the Add button.

- 3 Click the **next >>** button to display **Step 5 of 8 Protected Ranges** screen.

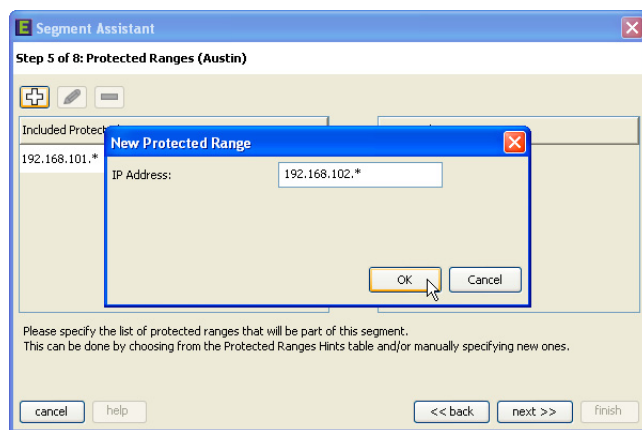
Setting Protected Ranges. This screen is used to specify the IP Addresses that will be protected in this Segment. Groups or ranges can be added to the Included Protected Ranges table by either selecting from the Protected Range Hints table or by specifying a new IP Address.

To add a Protected Range:

- 1 Click the **New Protected Range** button.



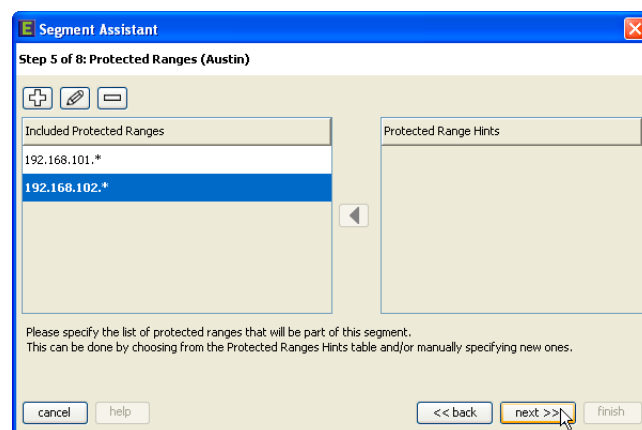
- 2 Enter the IP Address and click **OK**. Wildcards may be used, for example to select the entire range of IP Addresses use an asterisk (*). You may also specify ranges for an octet of the IP Addresses. You can use commas (,) and dashes (-) for multiple ranges. For example (192.168.21,23.* or 192.168.25.1-254).



NOTE

You may select protected range(s) from the Protected Range Hints table and click the Add button.

The new IP Address is added to the Included Protected Ranges table.



Once a protected range of IPs are specified, the Segment may be completed. Additional configuration may be completed if desired.

- 3 Click the **next >>** button to display [Step 6 of 8: Associate with a Segment Set](#) screen.

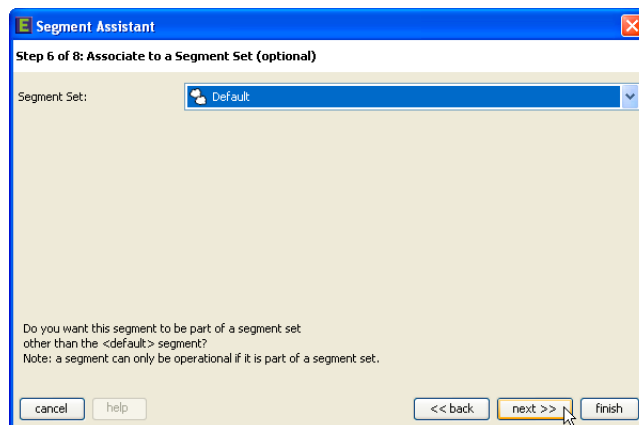
To remove an IP Address from the Included Protected Ranges list:

- 1 Select the IP Address.
- 2 Click the **Delete Protected Range** button.

Associating with a Segment Set. This screen is used to add or associate the new Segment with a Segment Set. All segments are placed in the Default Segment Set and can be moved as needed.

To associate a Segment with a Segment Set:

- 1 Select a Segment Set from the drop-down list.



Once the Segment Set is specified, the Segment may be completed. Additional configuration may be completed if desired.

- 2 To complete Segment configuration, click the **Finish** button.
To specify additional configuration:
- 3 Click the **next >>** button to display [Step 7 of 8: Setting Logical Ports](#) screen.

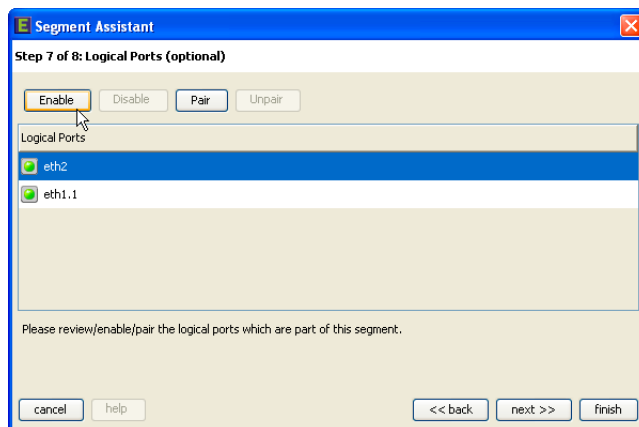
Setting Logical Ports. Logical Ports is used to enable, disable or pair logical Ports of the Segment. In order for the Segment to start monitoring traffic on the Segment, the Port(s) must be enabled.

The Sentriant NG appliance requires full read-write access to the ARP (Address Resolution Protocol) Horizon of each protected address range. In the event that the switch's SPAN Port connected to the Sentriant NG appliance is read-only it can be configured to internally be paired with a read-write Ethernet Port. To learn how to verify read and/or write Ethernet Port, see ["Port Verification" on page 235](#).

To enable the logical Port or Ports:

- 1 Select a Port(s) from the **Logical Ports Table**.
- 2 Click the **Enable** button.

The icon will turn from disabled to enabled indicating that the Port is active.



Continue enabling all Logical Ports for the Segment.

To pair a read-only Port with a write Port:

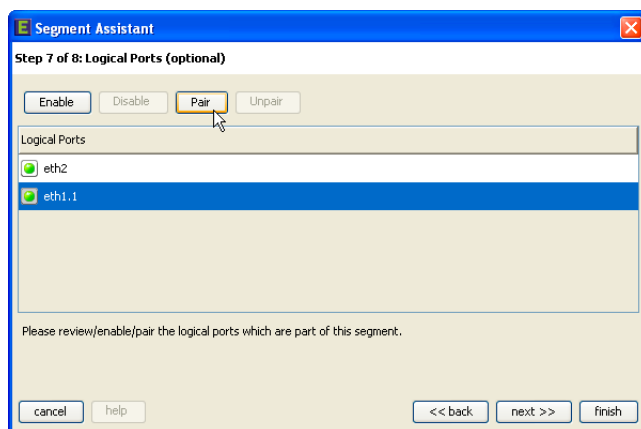
- 3 Select the SPAN Port from the list and click **Pair** to bring up the Pair Dialog.



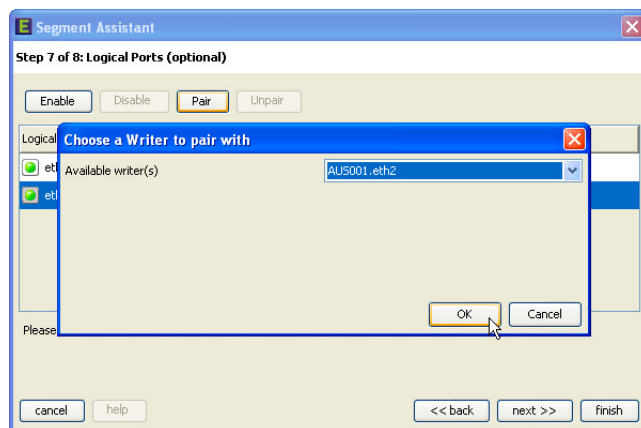
NOTE

Check with your network administrator to determine which Port is tagged as the SPAN Port. Traffic will not be monitored if other than the SPAN Port is paired with a write Port.

- 4 Select a write Port from the list and click **OK**.



The mirror Port is now paired with a write Port. The icon changes to show which Ports are paired.



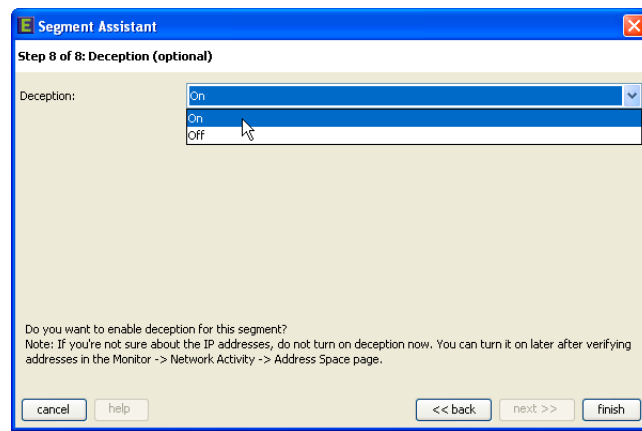
Once the Port or Ports are enabled, the Segment may be completed. Additional configuration may be completed if desired.

- 5 To complete the Segment, click the **Finish** button.
- 6 To specify additional configuration proceed to the next screen, click the **next >>** button to display [Step 8 of 8: Setting Deception Mode](#) screen.

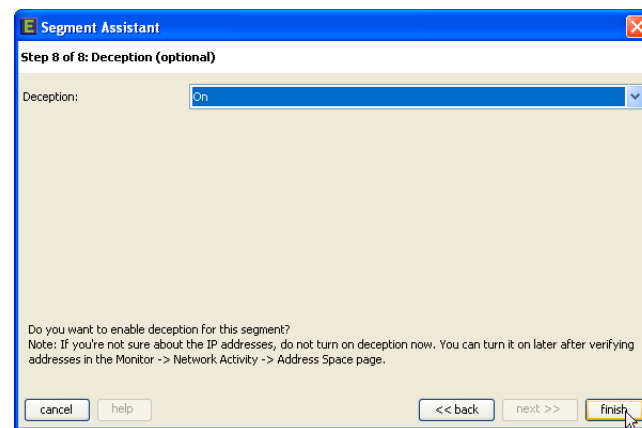
Setting Deception Mode. This screen is used to turn Deception Mode on or off. Deception should only be turned on if all friendly IP Addresses have been identified and configured.

To activate Deception:

- 1 Select **on** from the **Deception** drop-down list.



- 2 Click the **Finish** button to save the Segment and close the **Segment Assistant**.



The new Segment will be displayed in the Default Segment Set. If a new Segment Set was specified, the Segment will be displayed under that new set identified in [Step 6 of 8: Associating with a Segment Set](#).



NOTE

Clicking the *finish* button adds the Segment configuration to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#)

View and Edit Interface Information

Clicking on a physical Port from the **Runtime > Interfaces** panel will display information for that Port and allow you to edit the Port Name and configure Port Delay.

The Port Delay configuration option allows the Admin to configure the initial activation behavior of a Port on the Sentriant NG appliance. When Fast is enabled on a Sentriant NG appliance interface, the

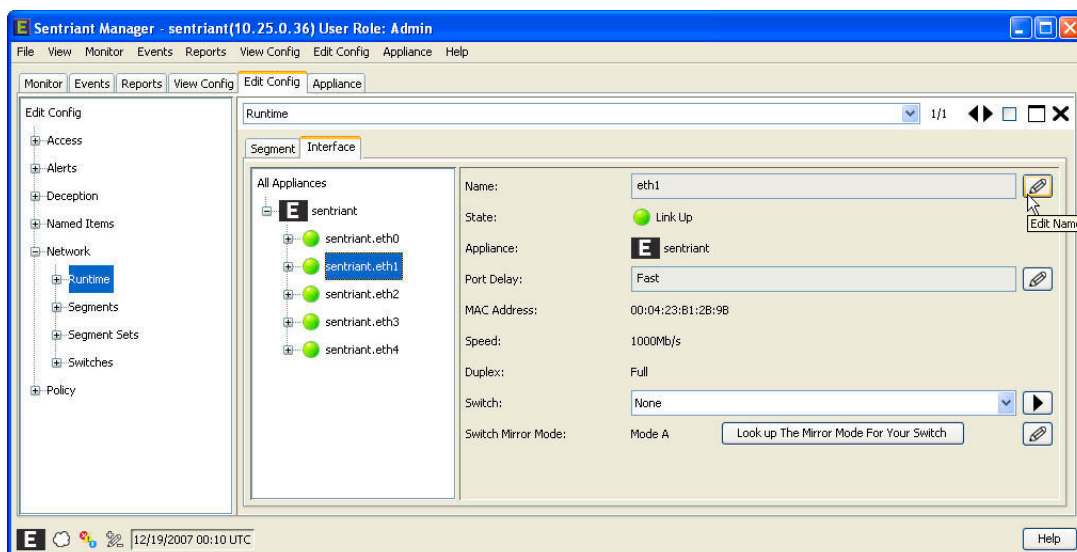
appliance will process traffic from that interface immediately. If the Admin is seeing inconsistent data, or a high number of IP Addresses on the Segment being detected as spoofs, it may be due to a mismatch between the Sentriant NG appliance's Port activation behavior and corresponding switch Port spanning tree configuration. A good practice is to synchronize the Sentriant NG appliance and the switch's Port delay values or set the delay longer for the Sentriant NG appliance. A longer Sentriant NG appliance Port delay will result in fewer false positives and inconsistent spoofed IP Addresses.

The Admin can disable Fast mode for the Sentriant NG appliance and configure a time out value, in milliseconds. When this time out value is configured, the Sentriant NG appliance will delay packet processing for the selected number of milliseconds. The available delay range is 0 - 320,000 milliseconds (0-32 seconds).

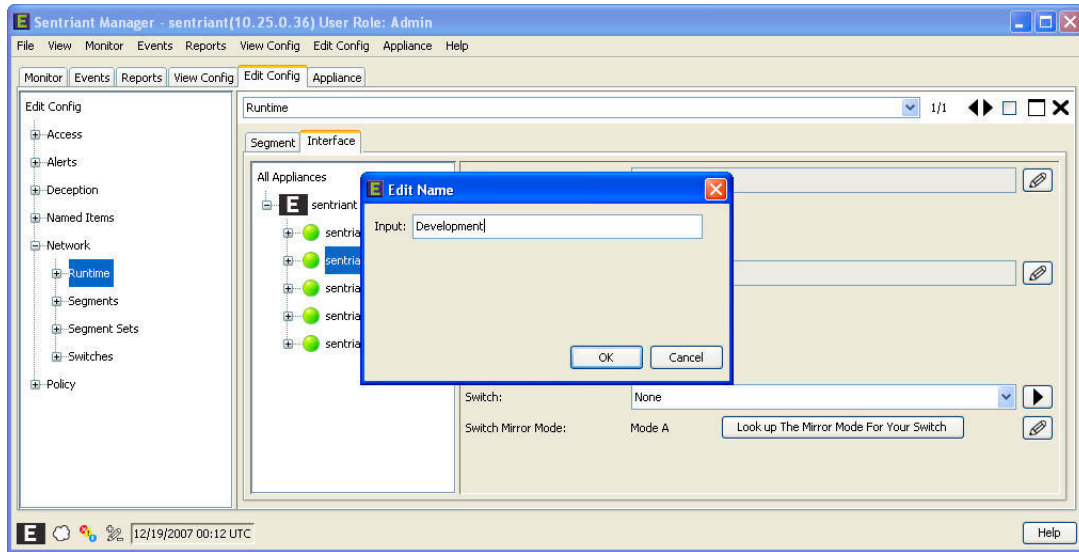
The Default mode sets the Sentriant NG appliance's initial activation at 30,000 milliseconds.

To change the name of a Physical Port:

- 1 From **Edit Config > Network > Runtime > Interface**, select an appliance.
- 2 Select a Physical Port from the list.
- 3 Click the **Edit Name** button.

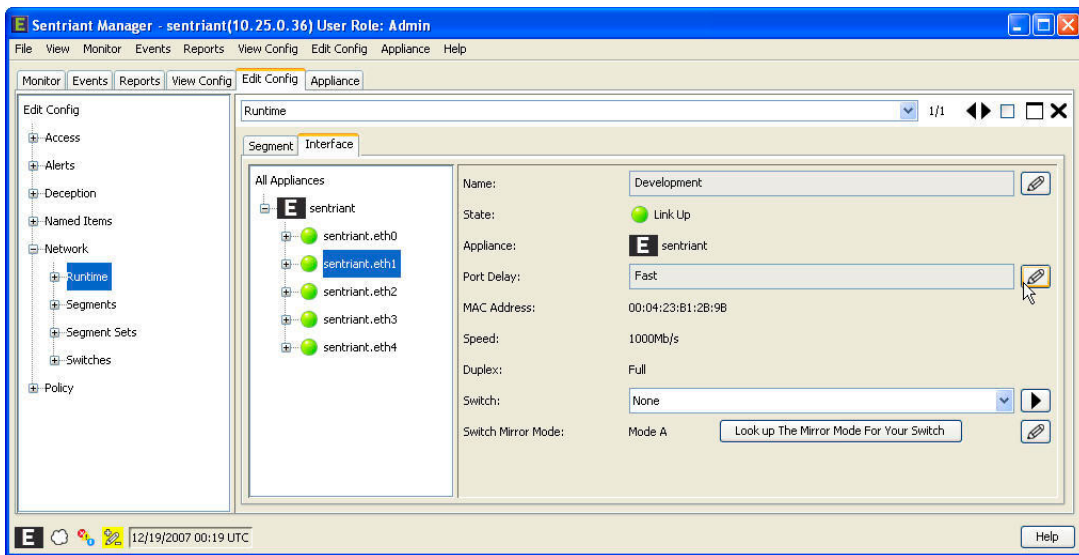


- 4 Enter an new name for the Physical Port.
- 5 Click **OK**.

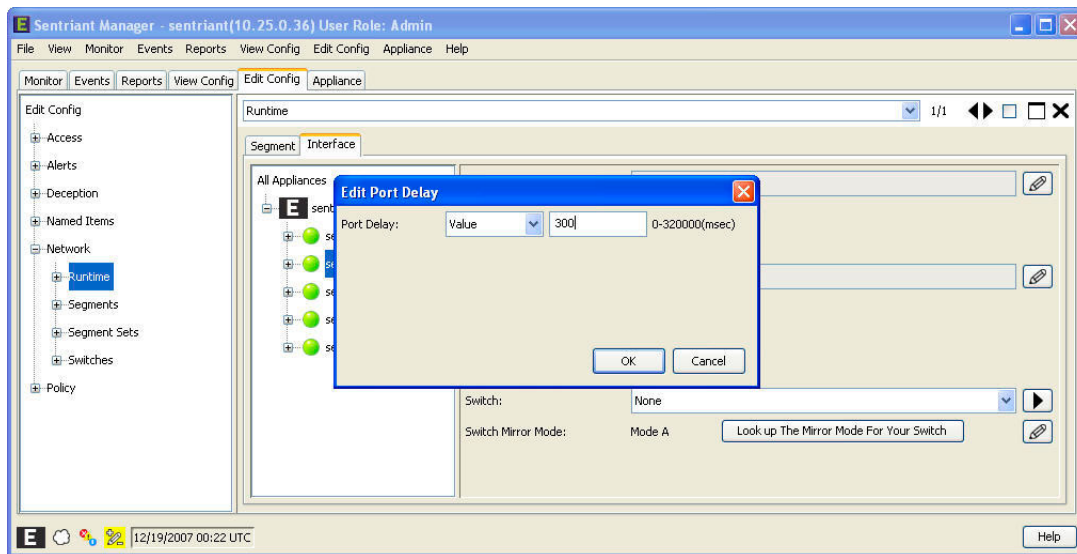


To configure Port Delay:

- 1 From **Edit Config > Network > Runtime > Interface**, select a Physical Port from the list.
- 2 Click the **Edit Port Delay** button.

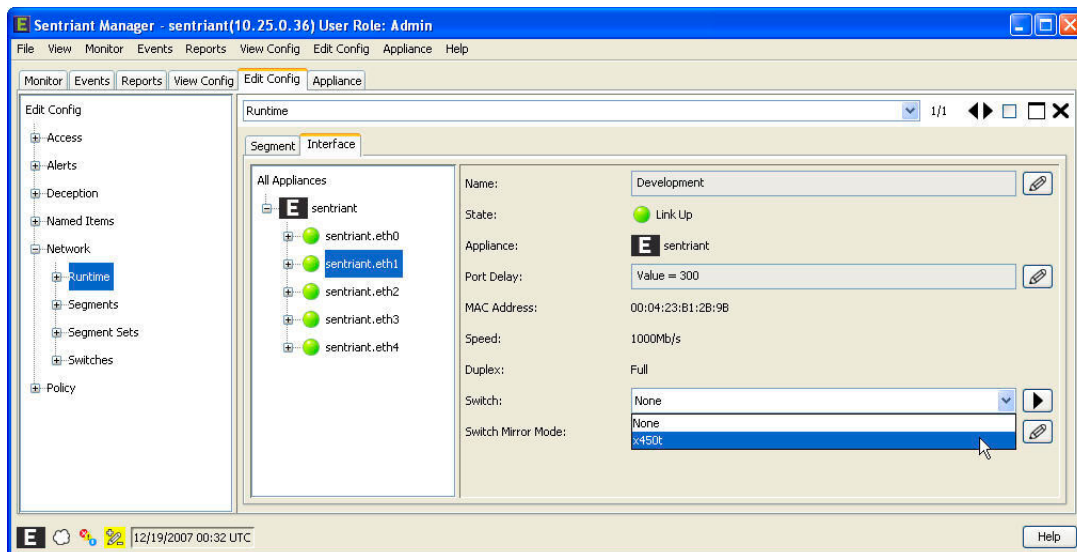


- 3 From the Port Delay drop-down list, select either Fast, Value or Default. Selecting Value requires a millisecond value.
- 4 Enter a value from 0 to 320,000 milliseconds.
- 5 Click **OK**.



To assign a switch to a Physical Port:

- 1 From **Edit Config > Network**, select the Appliance tab.
- 2 Select a Physical Port from the list.
- 3 Select a switch from the drop-down list.

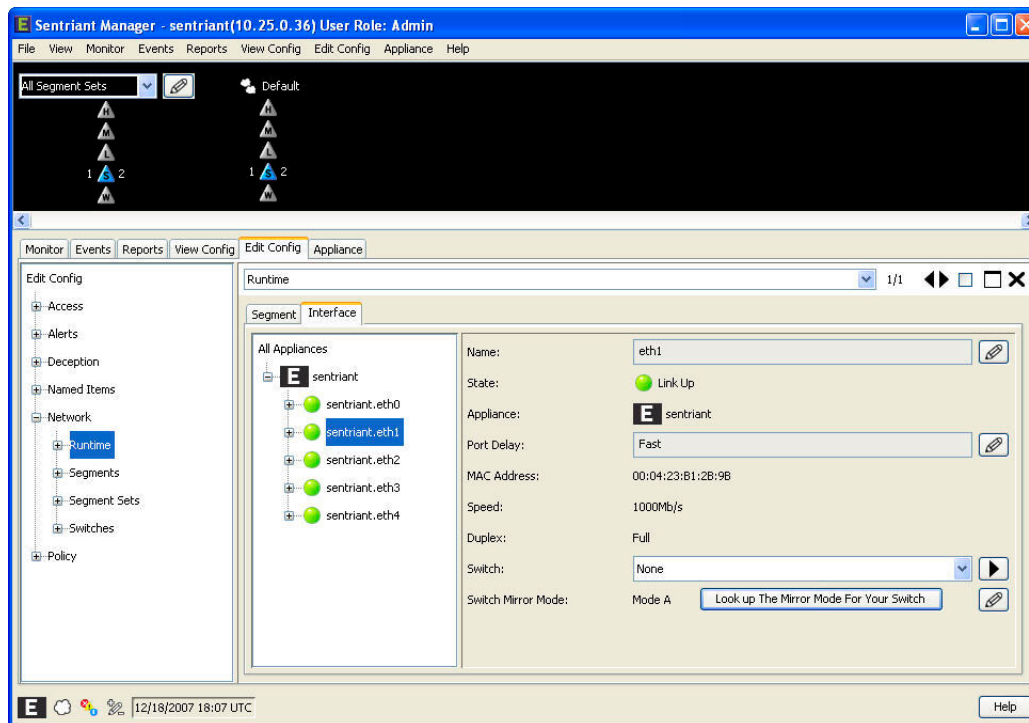


Switch Mirror Mode

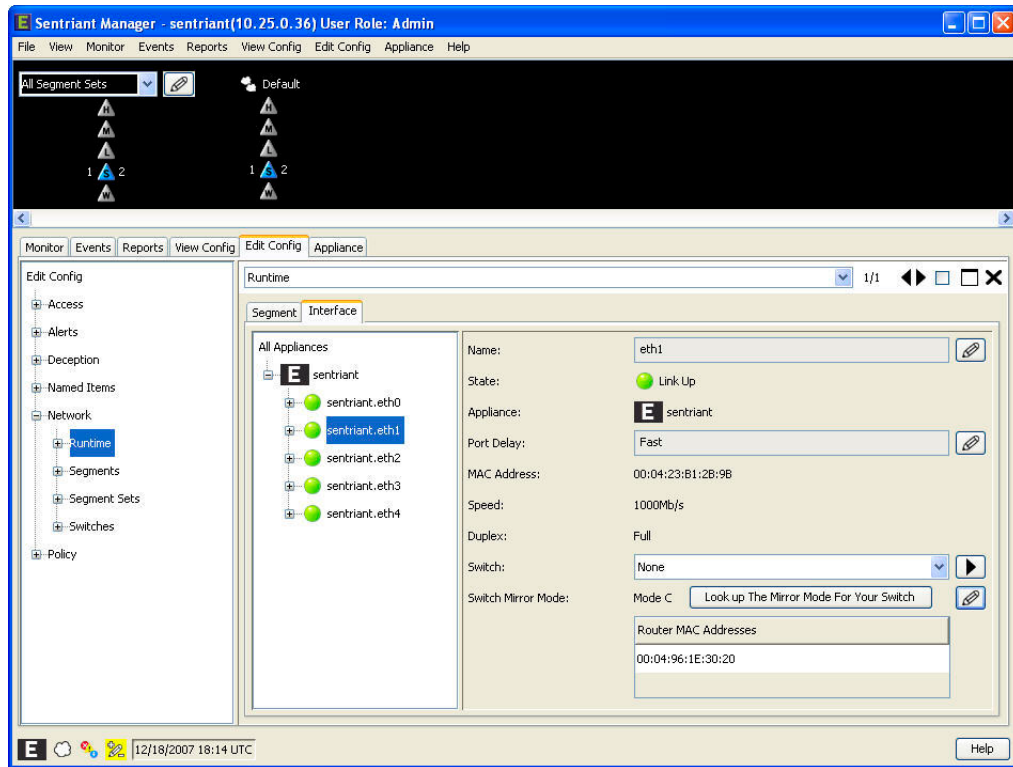
Some adjustment of the Switch Mirror Mode may be required depending on the type of Extreme Networks switches to which your Sentriant NG is connected.

To set the **Switch Mirror Mode**:

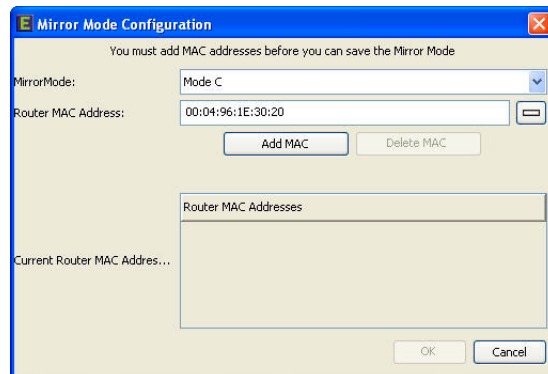
- 1 From **Edit Config > Network > Runtime**, select the Interface tab.



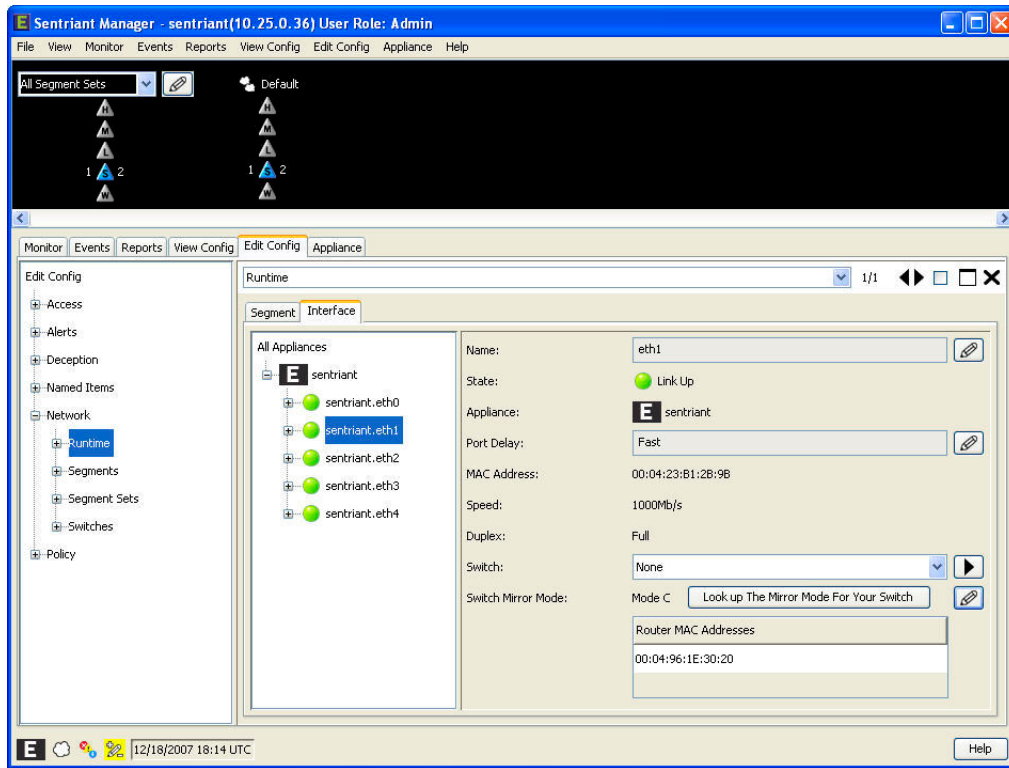
- 2 Select a read-only physical interface from the list.
- 3 Click the **Look up The Mirror Mode For Your Switch** button to display a list of Extreme Networks switch types and a correct mode to select.
- 4 Select the correct Switch Mirror Mode, then click the edit icon.
- 5 If you select Mode B or Mode C, you need to add the MAC address of the switch.



- a To find the MAC address, log in to the Extreme Networks switch.
- b Run **show switch**.
- c Use the MAC address that is displayed.



- 6 Click **Add MAC**.
- 7 Click **OK**



Segments

A Segment is a collection of IP Addresses for each logical network Port. The Sentriant NG appliance begins monitoring a contiguous range of addresses on each of the segments. This range can be further refined by configuring the Protected Ranges for each logical Segment.

Traffic to and from any address in this range is analyzed for behavioral patterns consistent with suspect or threat activity. Unlike host resident security solutions, the Sentriant NG appliance is able to take into account network behavior across entire segments for a more comprehensive threat analysis.

From the Segments Panel, you can:

- [Add a Segment](#)
- [Change the Segment name](#)
- [Edit the Segment IP Address](#)
- [Edit appliance and interface Port configuration](#)
- [Edit Segment Subnet and Mask IP Addresses](#)
- [Edit Segment Gateway IP Addresses](#)
- [Edit the Protected Range of IP Addresses monitored by a Segment](#)
- [Turn Deception on or off, configure Decoy IP Addresses, and exclude IP Addresses used as Decoys](#)
- [Set cloaking parameters for a Segment](#)
- [Set advanced Segment parameters](#)
- [Delete Segments](#)

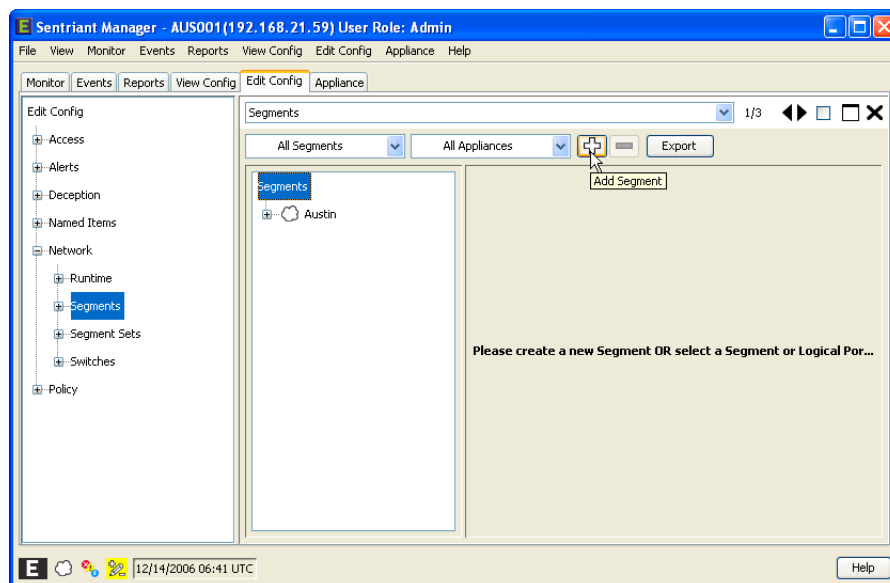
- Port Verification

Adding Segments

Sentriant NG Manager provides the option of adding segments to the appliance with discovered switch interfaces or manually created interfaces. This gives the user the ability to pre-configure segments before a switch has been completely configured. For example, a Sentriant NG appliance has been deployed in an environment where the switch has not been fully configured with VLAN interfaces. The switch administrator may pass along information on how the switch will be configured to the Sentriant NG appliance Admin. Using this information, The Admin can pre-configure the segments by manually creating the interfaces and then completing the Segment parameters using the Segment Assistant. Once the switch comes on-line, the Sentriant NG appliance will discover the switch interfaces and synchronize them with the pre-configured data.

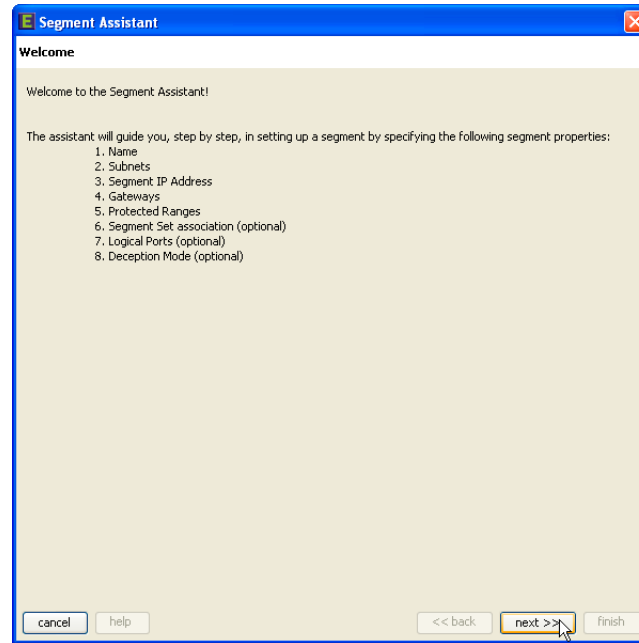
To add a new Segment:

- 1 From **Edit Config > Network > Segments**, select the **Segments** heading.
- 2 Click the **Add** button.



The Segment Assistant Welcome screen opens.

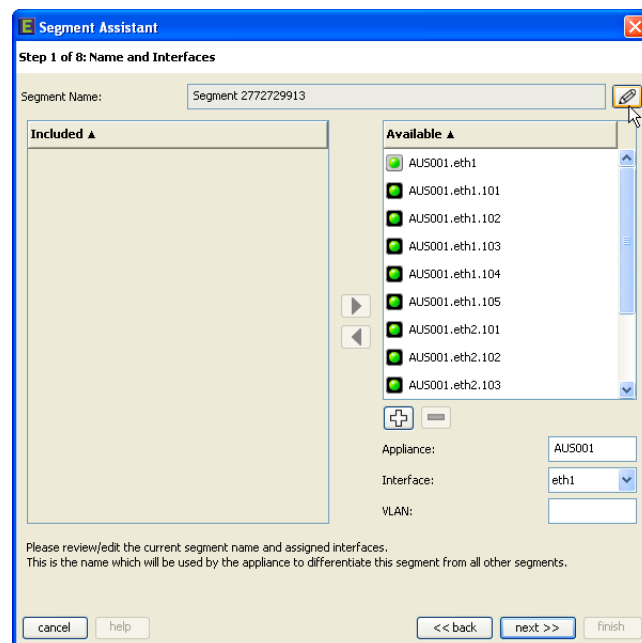
- 3 Click the **next >>** button.



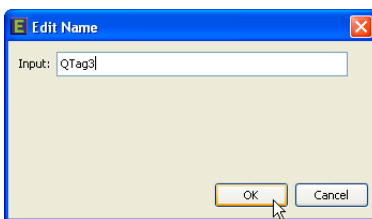
The Name and Interfaces screen opens and displays a randomly generated Segment name and a list of available interfaces discovered on the Sentriant NG appliance.

To change the name of the Segment:

- 4 Click the **Edit Segment Name** button.



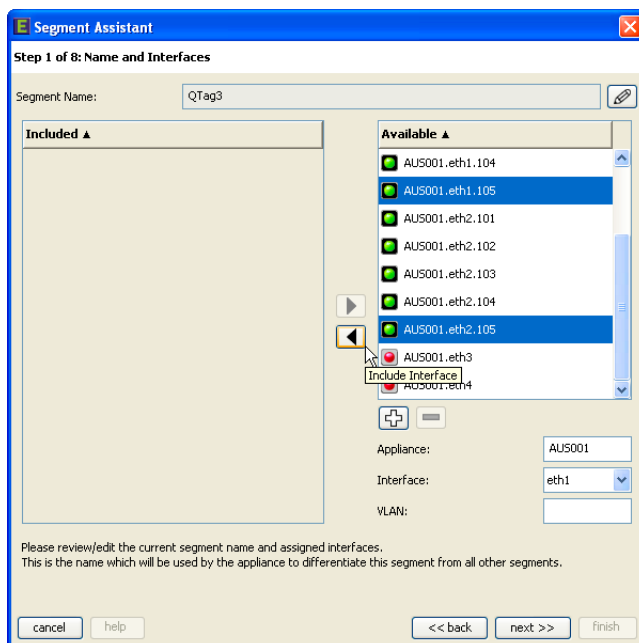
- 5 Enter a name for the Segment and then click OK.



The next step is to add interfaces and identify the VLAN to the Segment. There are two methods of adding interfaces. One is to select discovered interfaces and add them to the Included list. The other method is to create interfaces for pre-configured segments.

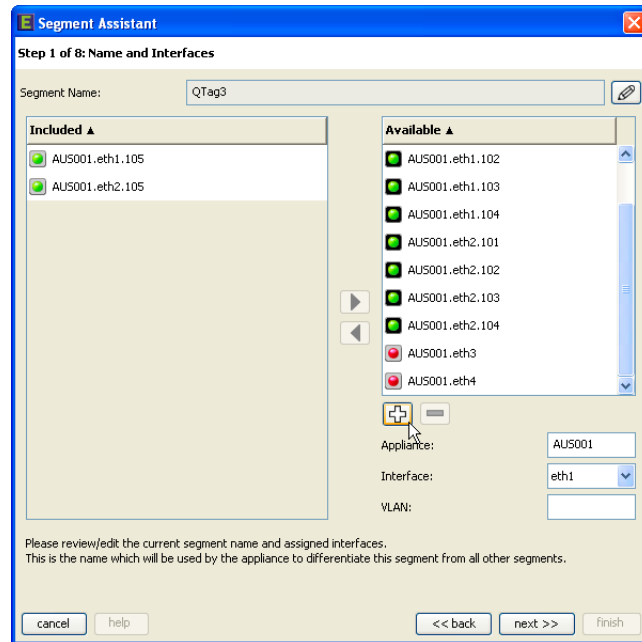
To include discovered interfaces to a Segment:

- 6 Select an interface from the Available list of interfaces on the right of screen. You may multi-select interfaces by Shift-clicking or Ctrl-clicking the interfaces.
- 7 Click the **Include Interface** button.



To manually create interfaces and include them on a Segment:

- 8 In the lower right of the Name and Interfaces screen, enter the name of an appliance, select an Interface from the drop-down list, and enter a name for the VLAN.
- 9 Click the **Add** button.
- 10 Continue adding interfaces for the Segment.



Click the **next >>** button to display [Step 2 of 8 Subnets](#).



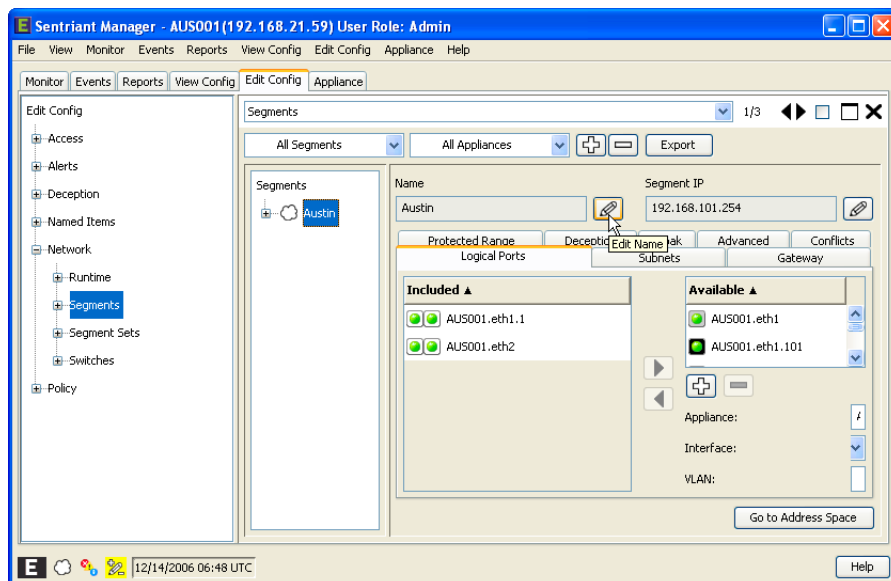
NOTE

Changing the Segment name does not change it on the Sentriant NG appliance. The changes are made to the stack of configuration changes made and is displayed in the Tab/Folder List with an edit icon. However, the Sentriant NG appliance's configuration has not been updated with the new changes. (See [“Saving Changes to the Sentriant NG Appliance”](#) on page 133.)

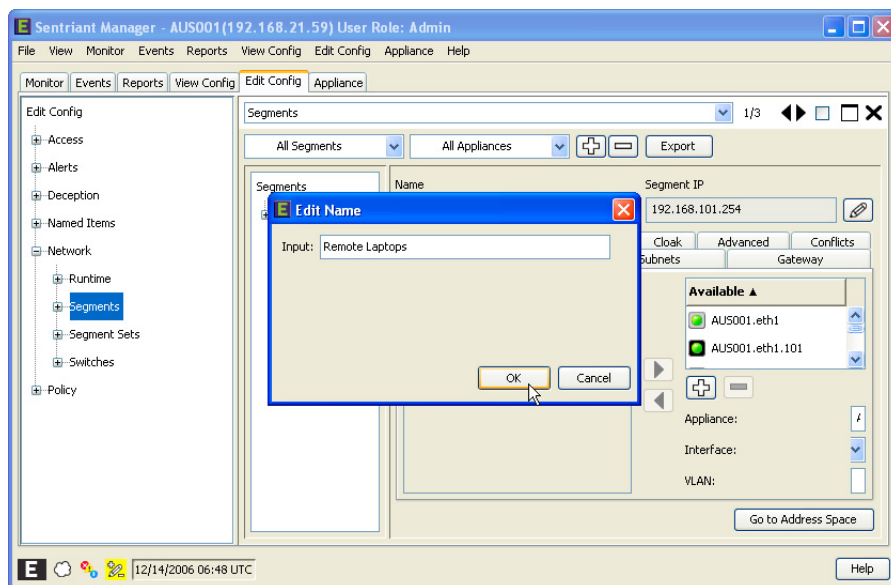
Segment Name

To change the Segment name:

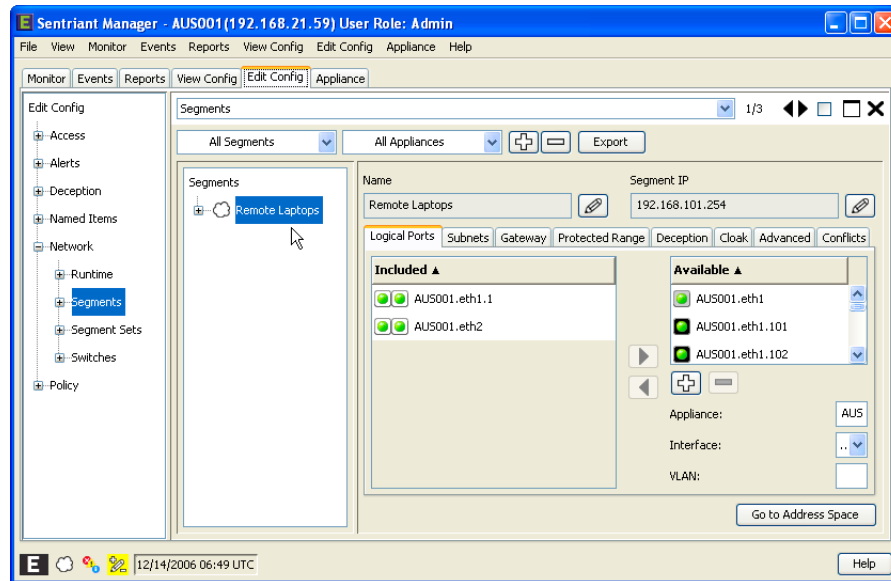
- 1 From **Edit Config > Network > Segments**, select a Segment from the drop-down list.
- 2 Click **Edit Name** button.



- 3 The **Edit Name** dialog opens. Enter a name for the Segment.
- 4 Click **OK**.



The new Segment name is displayed in the Name Field and in the Navigation Tree.

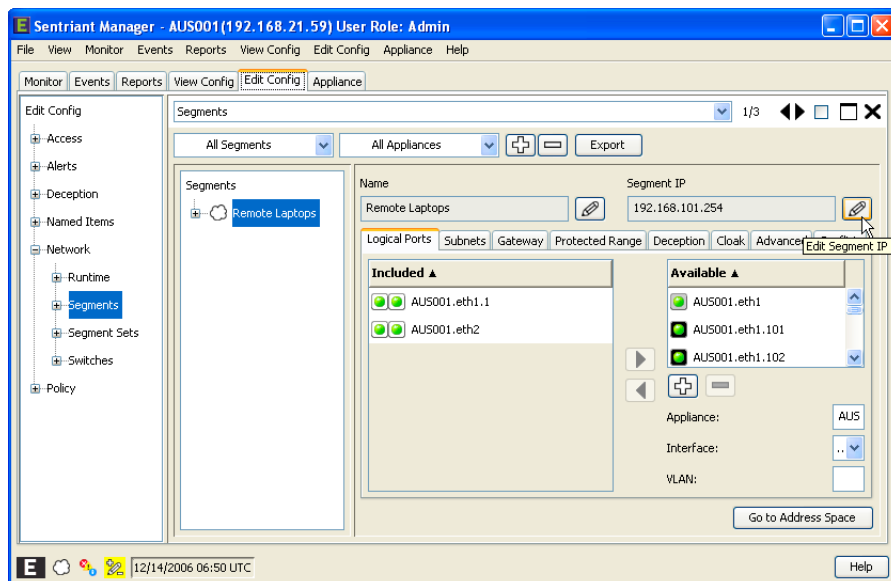
**NOTE**

Changing the Segment name does not change it on the Sentriant NG appliance. The changes are made to the stack of configuration changes made and is displayed in the Tab/Folder List with an edit icon. However, the Sentriant NG appliance's configuration has not been updated with the new changes. (See [“Saving Changes to the Sentriant NG Appliance”](#) on page 133.)

Segment IP Address

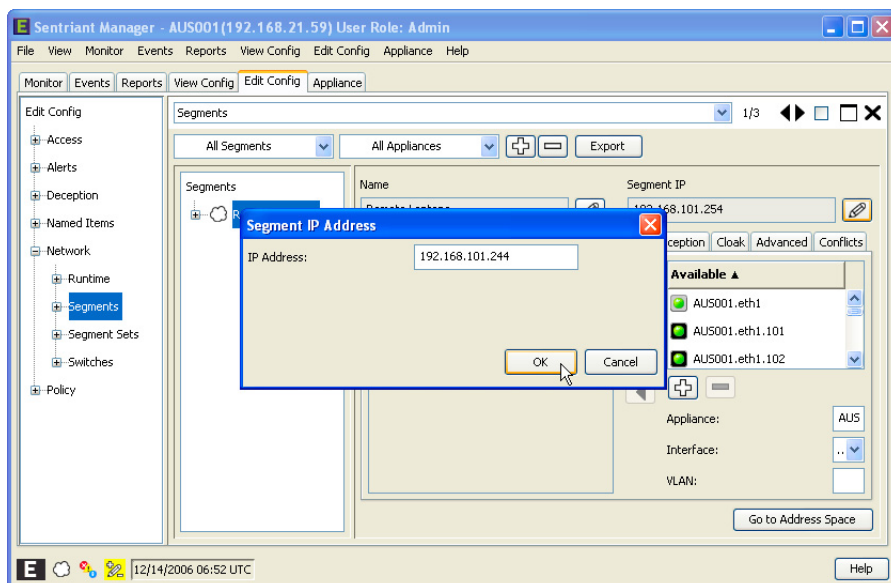
To change the Segment IP Address:

- 1 From **Edit Config > Network > Segments**, select a Segment from the drop-down list.
- 2 Click the **Edit Segment IP** button.

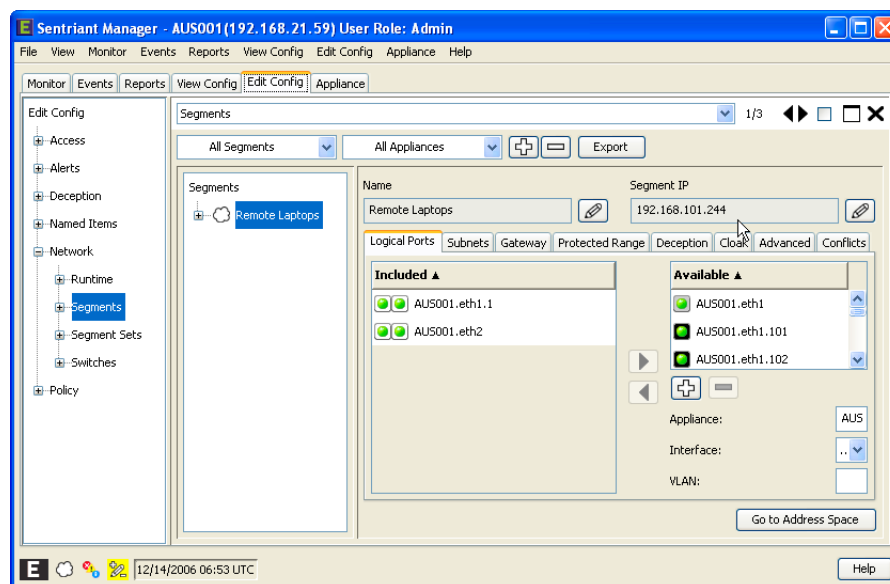


3 The Edit Segment IP dialog opens. Enter an IP Address for the Segment.

4 Click OK.



The new Segment IP Address is displayed in the Segment IP field.



Segment Logical Ports

Each Segment's logical Port(s) must be **enabled** and, in cases with read-only Ports, paired with a writable Port for the Sentriant NG appliance to begin monitoring network traffic on the Segment. Information displayed is the state of the Port, MAC Address, Read/Write State, Paired With state, and the Segment Name.

The Sentriant NG appliance is designed to be deployed **out-of-band** meaning that it can analyze traffic that traverses the network without having to be placed within a critical data path. Therefore, it is strongly recommended that the switch Ports connected to the Sentriant NG appliance be configured as Switched Port Analyzer (SPAN) Ports or mirror Ports.

The Sentriant NG appliance requires full read-write access to the ARP (Address Resolution Protocol) Horizon of each protected address range. In the event that the switch's SPAN Port connected to the Sentriant NG appliance is **read-only** it can be configured to internally be **paired** with a read-write Ethernet Port.

Add/Remove Logical Ports. The Add/Remove Logical Ports panel allows the admin to add and remove logical Ports from configured segments. When a switch's configuration has changed, the Sentriant NG appliance must be reconfigured with the new Segment interface parameters.

The Add/Remove Logical Ports panel also provides the ability to create interfaces and include them when pre-configuring segments.



NOTE

Adding or removing interfaces from configured segments may result in configuration conflicts with other segments or if the interfaces are pre-configured and included in a Segment, a conflict will result stating that no real Segment exists.

To add logical Ports to a Segment:

- 1 From **Edit Config > Network > Segments**, select a Segment from the drop-down list.

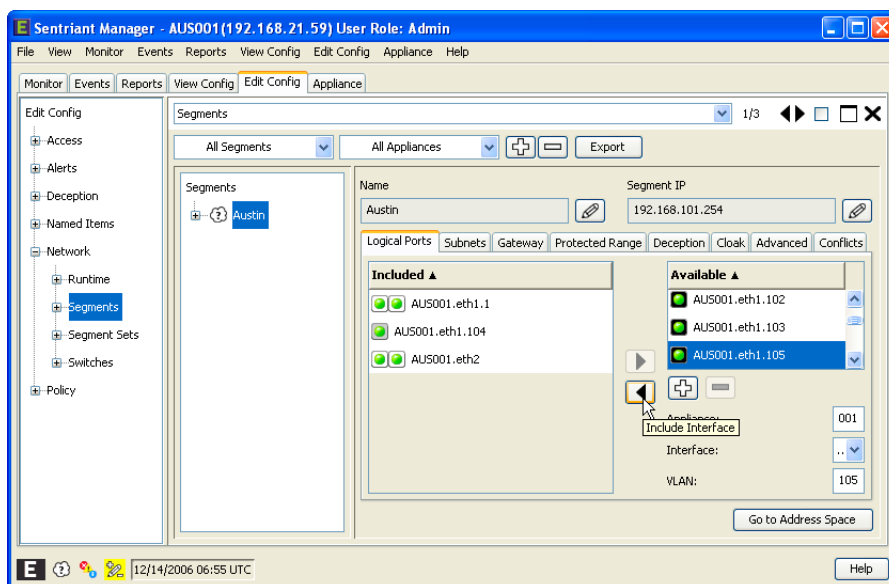
The Logical Ports panel opens with a list of logical Ports in the Included list.

There are two methods to add logical Ports to a Segment. One method is to select discovered logical Ports from the Available list. The second method is to create new logical Ports and include them with a Segment.

To add logical Ports from discovered interfaces:

- 1 From the Available list of logical Ports, select a logical Port.
- 2 Click the **Include Interface** button.

The logical Port is added to the Segment.

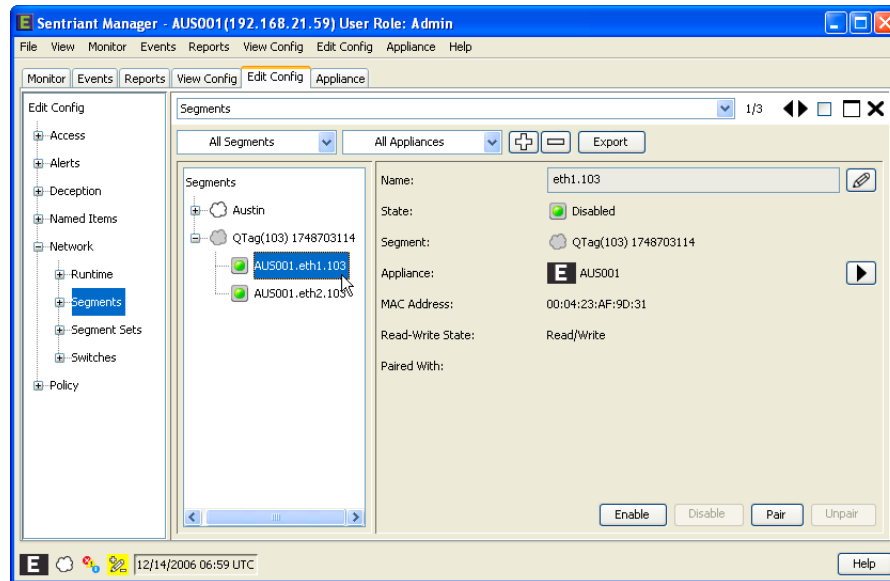


To manually create interfaces and include them on a Segment:

- 1 In the lower right of the Name and Interfaces screen, enter the name of an appliance, select an Interface from the drop-down list, and enter a name for the VLAN.
- 2 Click the **Add** button.
- 3 Continue adding interfaces for the Segment.

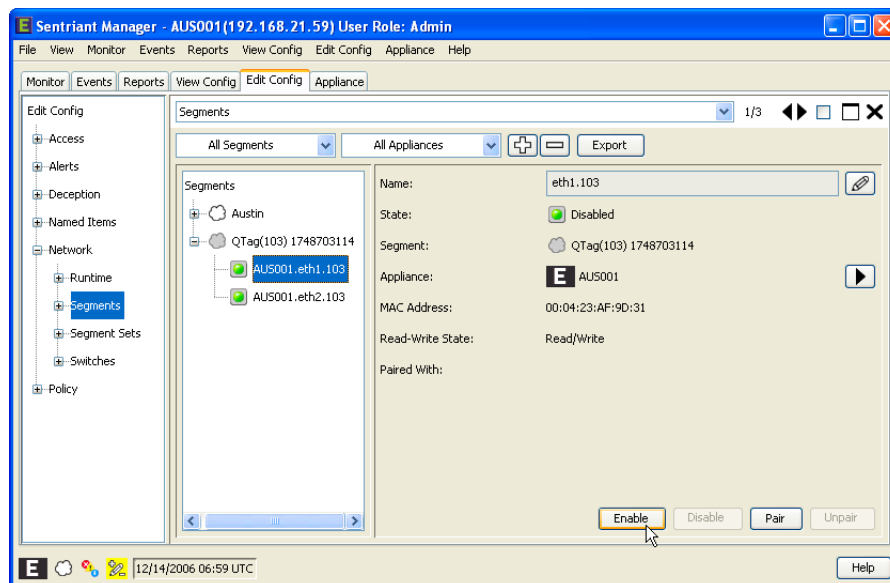
Enable a Segment's Port. To Enable Ports:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Either double-click or for Windows users, click on the plus (+) sign. This displays the logical Ports for the Segment.
- 3 Click on a Port to display the state information.

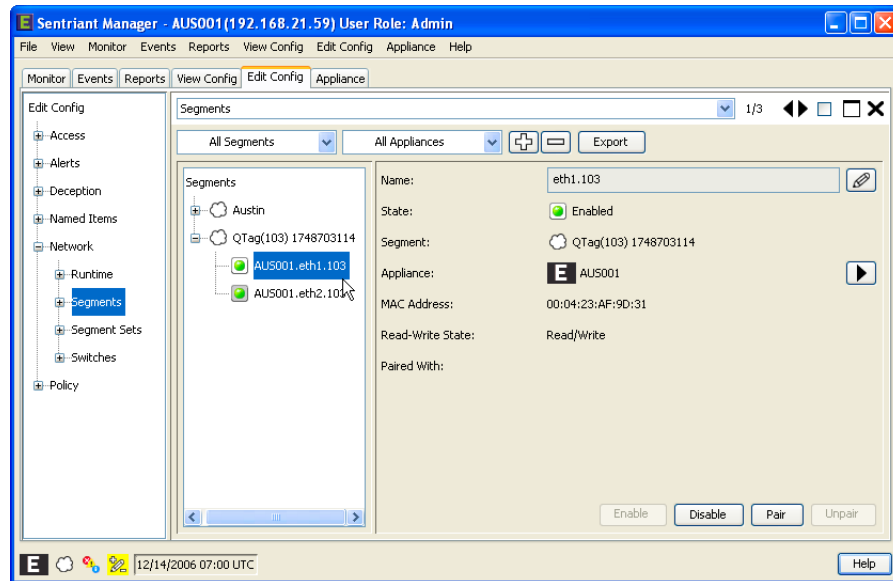


The State shows the Port disabled and the Segment not monitoring network traffic. Notice the Segment cloud is black meaning it's in a state of Discovery and Port icons are grey meaning they are disabled.

- 4 Click the **Enable** button.

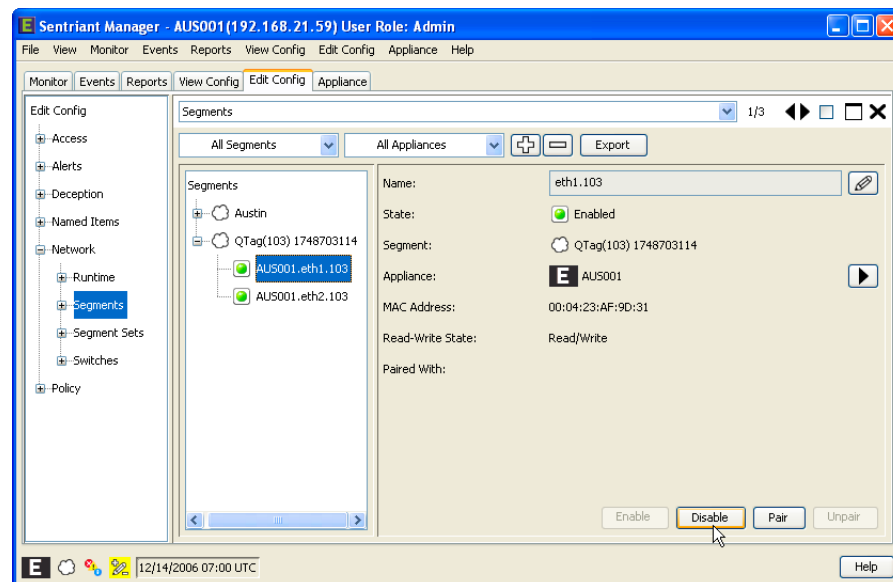


The Port icon changes to enabled.

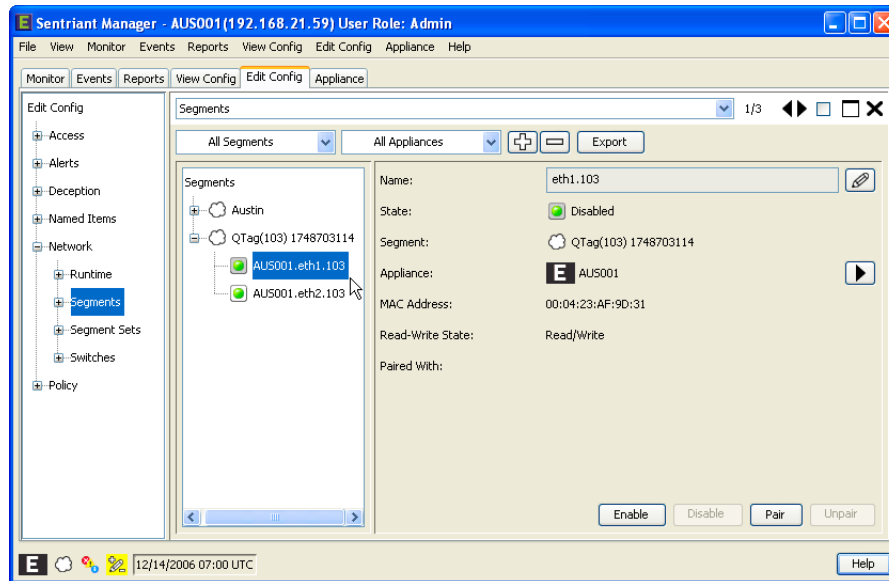


Disable Ports. To Disable Ports:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select an enabled Port and click the **Disable** button.



The State shows the Port disable. The Segment will no longer monitor network traffic.



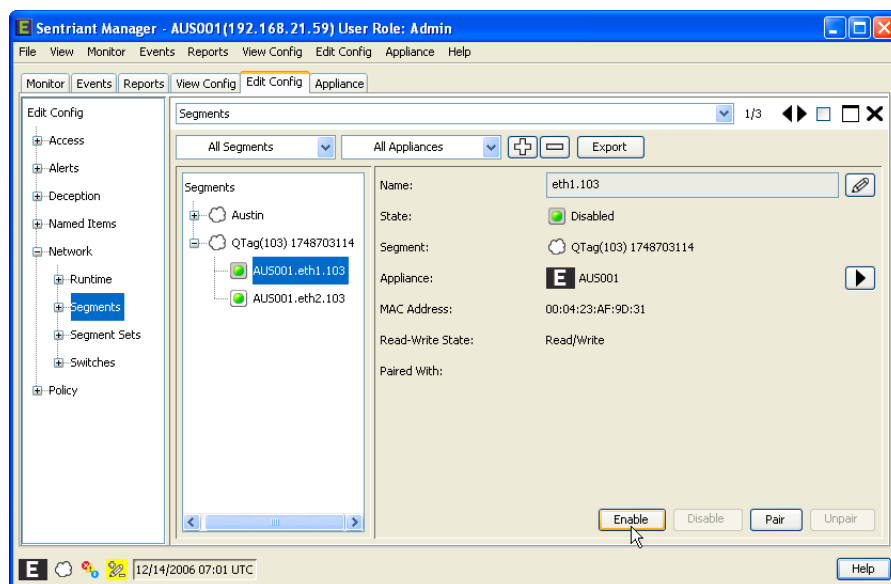
Pair Ports. The Sentriant NG appliance requires full read-write access to the ARP (Address Resolution Protocol) Horizon of each protected address range. In the event that the switch's SPAN Port connected to the Sentriant NG appliance is **read-only** it can be configured to internally be **paired** with a read-write Ethernet Port.

To pair a Port:

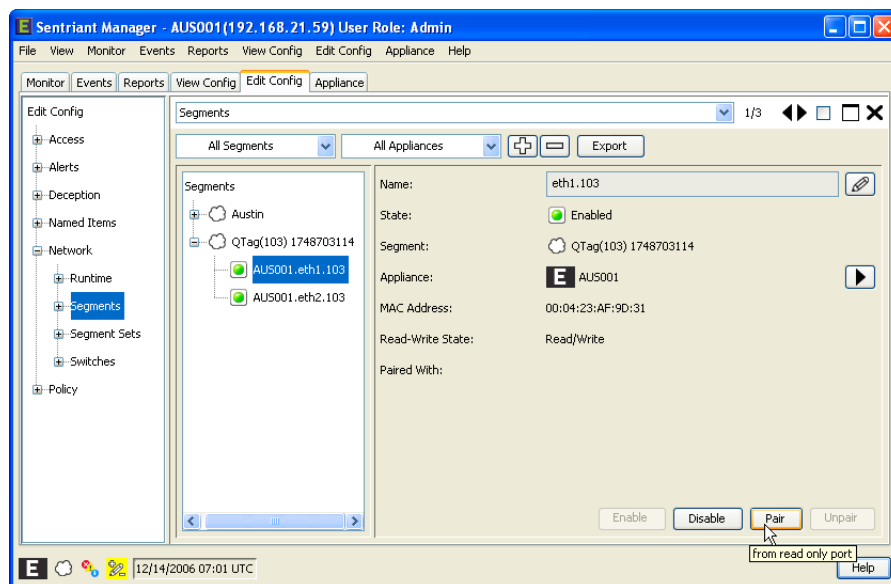
- 1 From **Edit Config > Network > Segments**, select a Port in the Segment tree list.
- 2 Click the **Enable** button.

NOTE

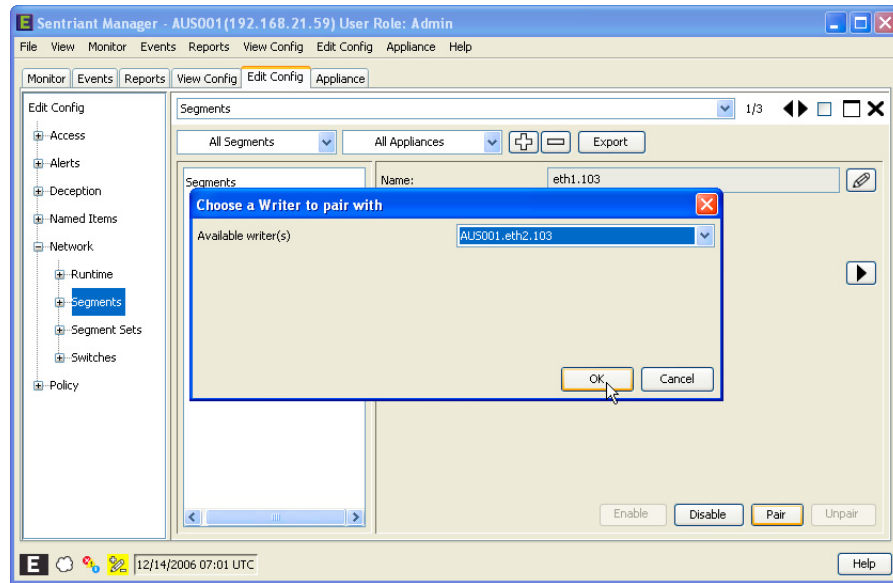
The Sentriant NG appliance does not recognize if a Port is read-only or read/write. It is up to the network administrator to determine if the Ports on the switch are configured as read-only.



- 3 Select an available Port from the list and click **Pair** to bring up the Pair Dialog.

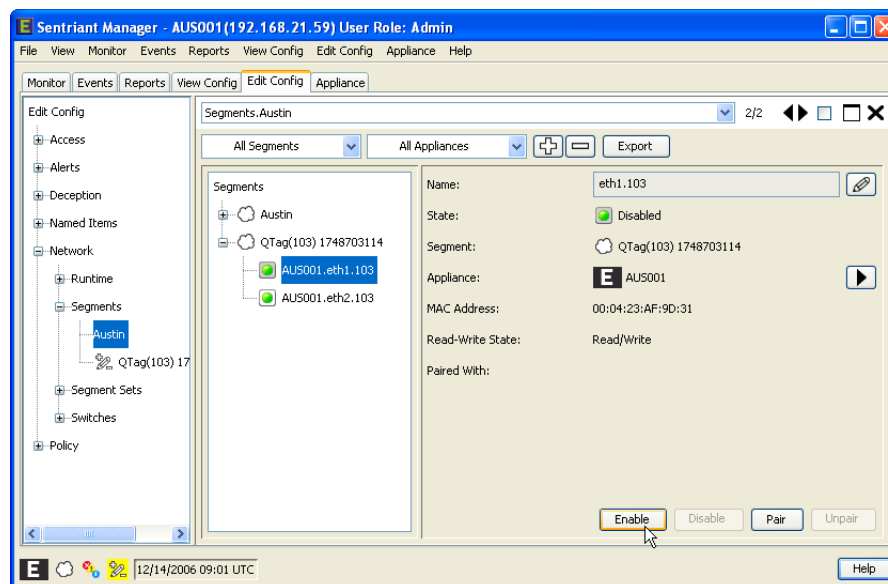


- 4 Select a Port from the list and click **OK**.

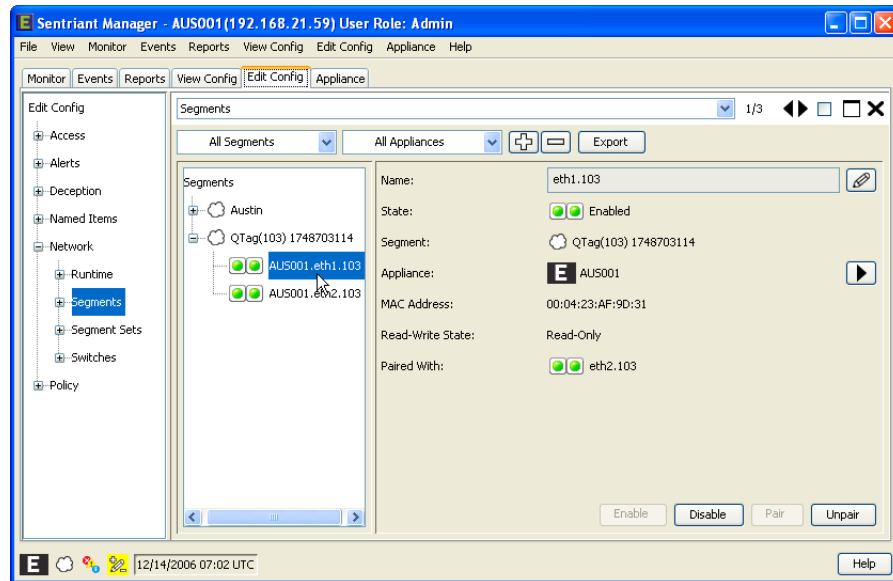


The Port type icon changes reflecting that the Port is paired.

- 5 Click the **Enable** button.

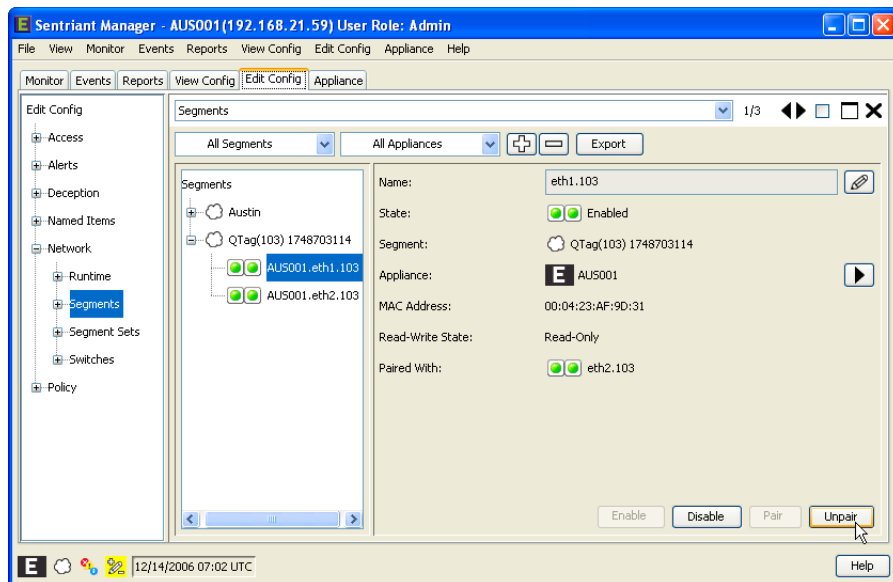


The Ports are now enabled for the Segment. The Segment is now ready to be monitored by the Sentriant NG appliance once the changes have been persisted. See [“Saving Changes to the Sentriant NG Appliance”](#) on page 133 to save changes to the Sentriant NG appliance.



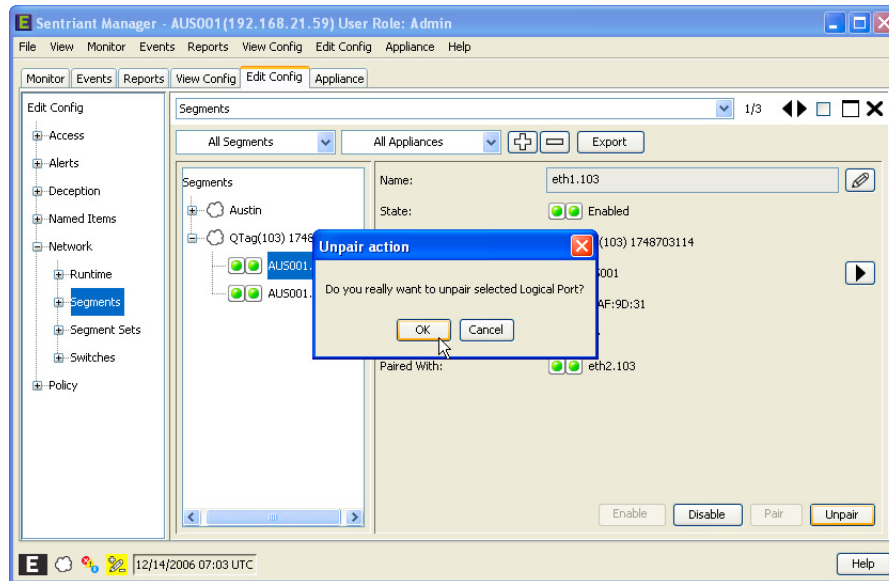
Unpair Ports. To unpair Ports:

- 1 From **Edit Config > Network > Segments**, select the Port in the Segment tree list.
- 2 Click the **Unpair** button.

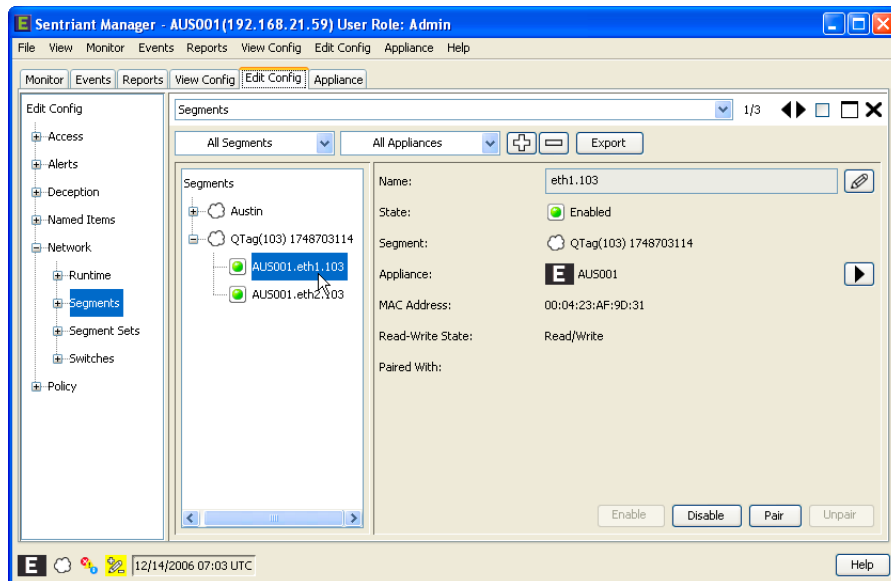


The Unpair Dialog is displayed.

- 3 Click **OK**.



The Paired With field is empty and the icon changed to single.



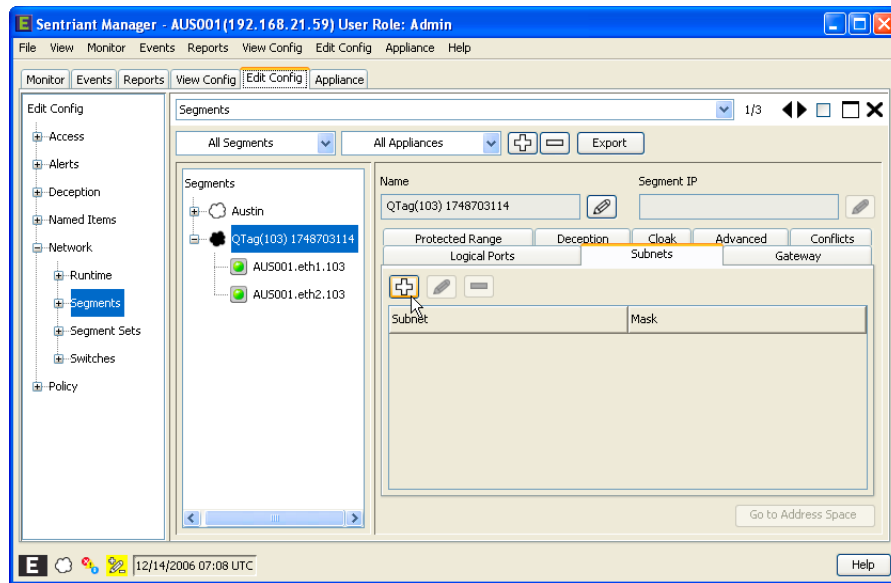
Subnet and Mask

By default, when a subnet is added to a Segment, the entire subnet is added as a protected range. The administrator can modify the range to include only a portion of the subnet. Ranges of IP Addresses and wildcards can be used to specify which addresses will be in the protected range.

To modify Subnet and Mask:

- 1 From **Edit Config > Network > Segments**, select a Segment from the list.
- 2 Click the **Subnet Tab**.

- Click the **Add** button.



- Enter a **Subnet** and **Mask IP Addresses**.
- Select a Mask IP Address from the drop-down list. The default Mask is 255.255.255.0.
- Click the **Add Protected Range** checkbox. This will add the segments range of IP Addresses to the Protected Range Tab.

**NOTE**

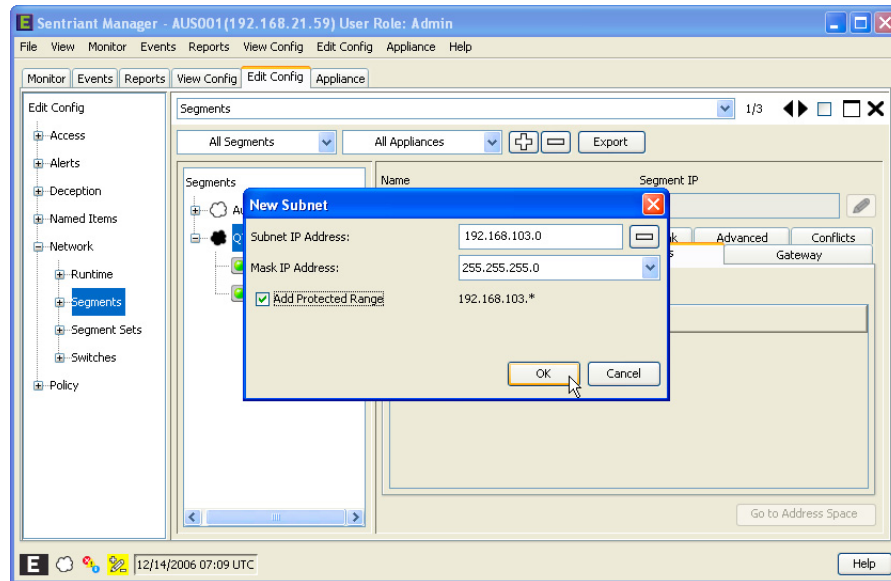
Clicking the Delete Subnet button clears the fields.

**NOTE**

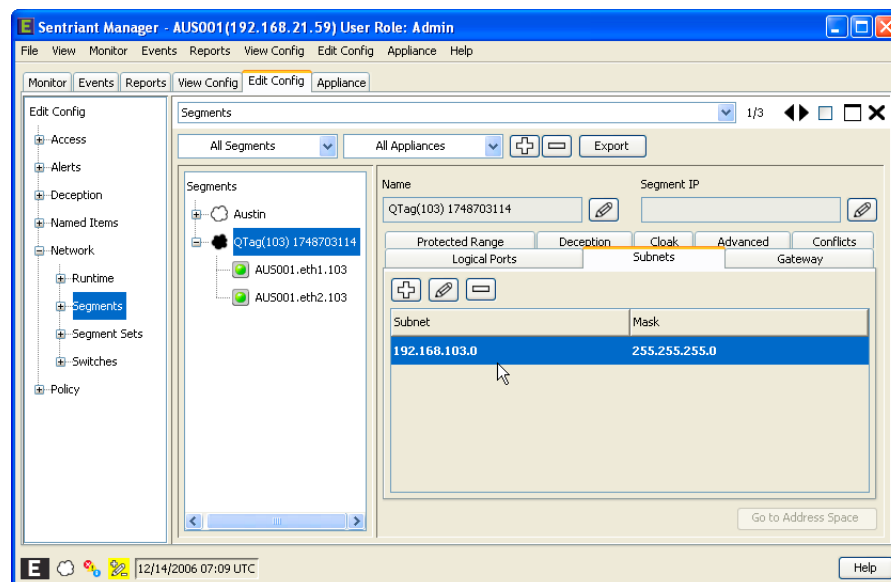
The subnet IP Address must be within the range of the Segment.

**NOTE**

When editing an existing Subnet, the Add Protected Range is disabled. If the Subnet is changed, the Segment IP Address, Protected Range, and Gateway are removed and must be updated.



7 Click OK to add the new Subnet and Mask IP Addresses to the Segment.



Gateway

It is imperative that all gateway IP Addresses are identified and added to the Sentriant NG Manager's configuration for the Segment. This is to ensure that all devices on each monitored network Segment are 'known' for proper traffic monitoring and detection.

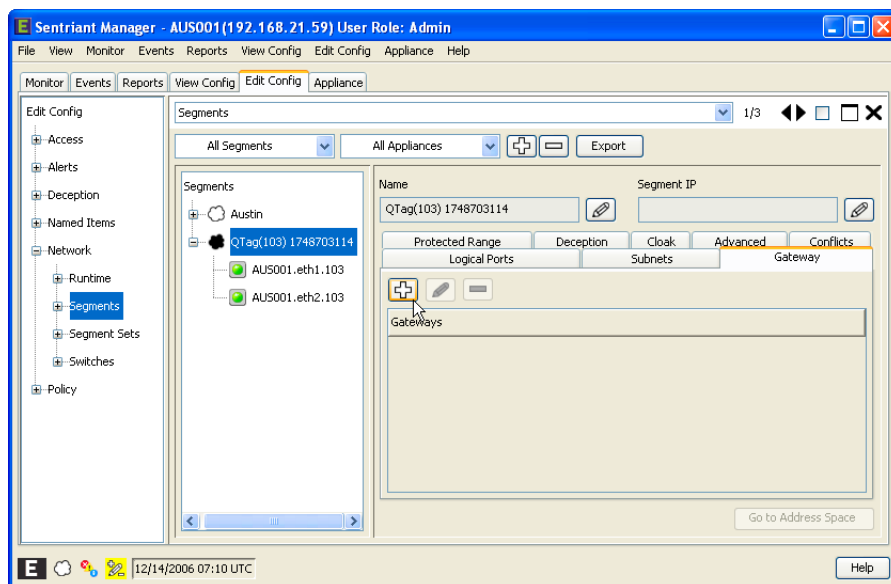


NOTE

Adding invalid gateway IP Addresses that do not represent a real host will cause spoof detection to be disabled. All gateways must respond to ARP communication.

To add gateway(s) to the Segment:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Gateway** tab.
- 3 Click the **Add** button.

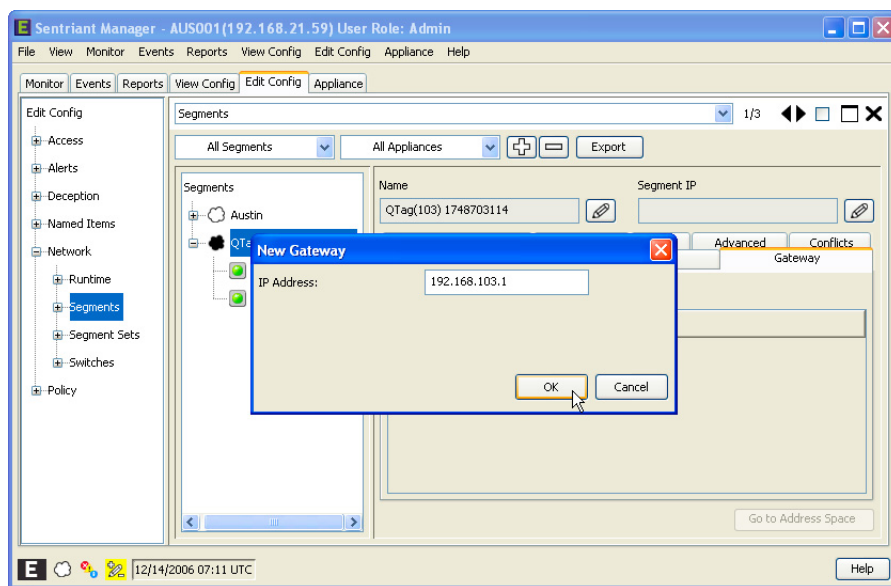


- 4 Enter a Gateway IP Address.
- 5 Click **OK**.

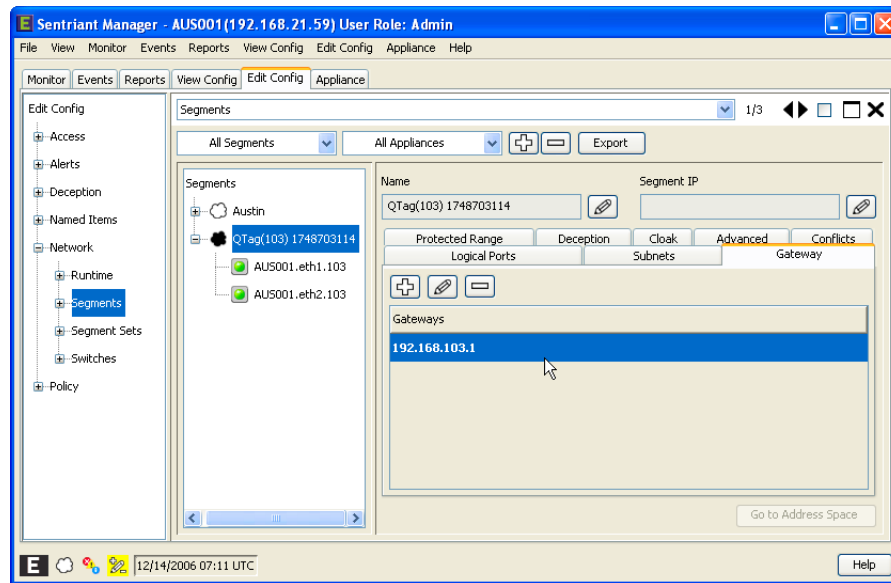


NOTE

The Gateway Addresses must be inside the range of the of subnet.



The new Gateway is added to the list.

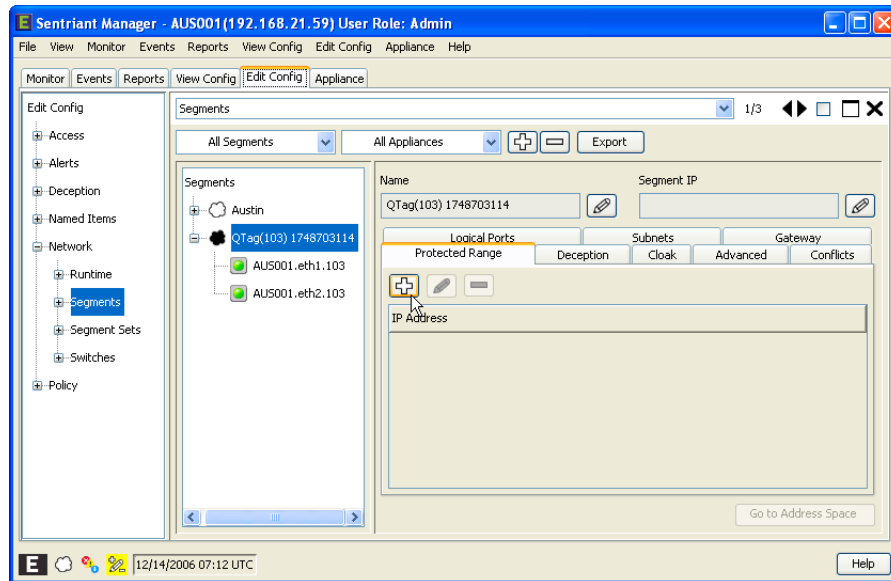


Protected Range

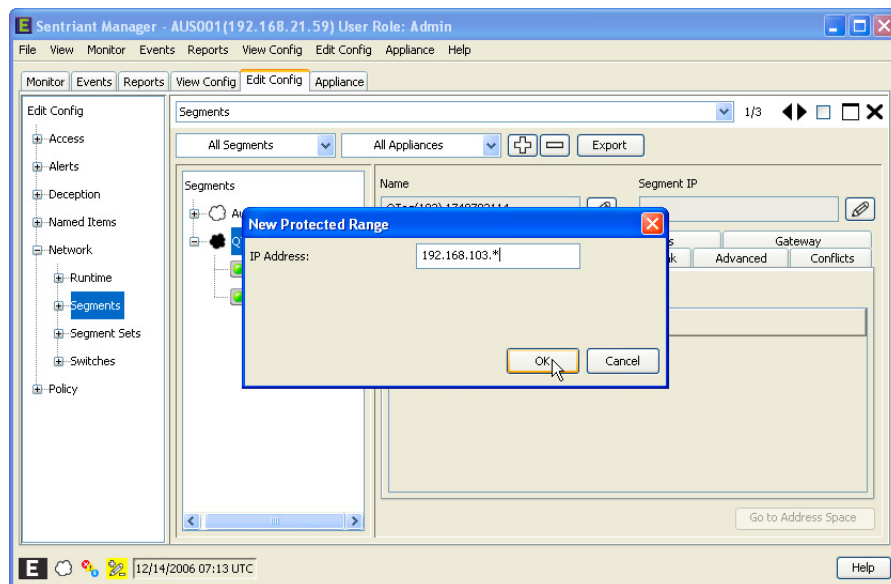
By default, when a subnet is added to a Segment, the entire subnet IP Address range is added as a Protected Range. The administrator can modify this range to include only a subset of the subnet, if that is desired.

To add a protected range of IP Addresses to the Segment:

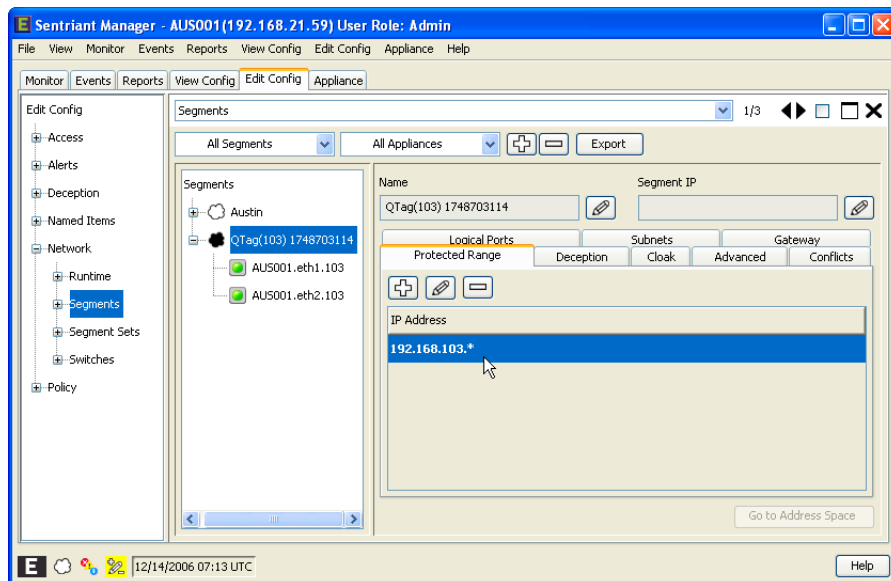
- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Protected Range** tab.
- 3 Click the **Add** button.



- 4 Enter the protected range for the Segment. Wildcards may be used, for example to select the entire range of IP Addresses use an asterisk (*). You may also specify ranges for an octet of the IP Addresses. You can use commas (,) and dashes (-) for multiple ranges. For example (192.168.21,23.* or 192.168.25.1-254).
- 5 Click OK.



The Protected Range is added to the Segment.



Edit Segment Deception

The Sentriant NG appliance provides an advanced technology that greatly enhances the security of a protected network by providing ActiveDeception, which maps operating system 'personalities' on to the unused IP Address space of the monitored address ranges. This allows the Sentriant NG appliance to employ anti-fingerprinting mechanisms and to slow or snare the reconnaissance phase of a malicious attack, worm, or virus.



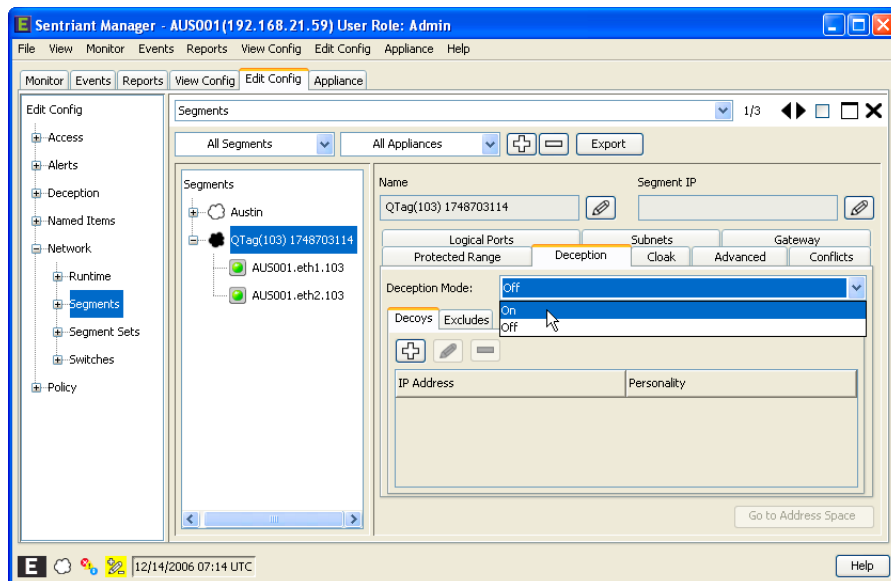
NOTE

Deception is not used to hide used IP Addresses.

Turning Deception on allows the Sentriant NG appliance to respond to threats attacking unused IP Addresses on the network Segment. This response can be tailored to the specific network topology that suits the network that is being protected. Deception can further be configured to include or exclude unused IP Address(es) and set individual personalities. Decoys can be configured for a Segment that, when communicated with an outside source, will send a personality as a decoy to the true nature of the IP Address. In addition, you may exclude IP Addresses when deception is turned on.

To start Deception:

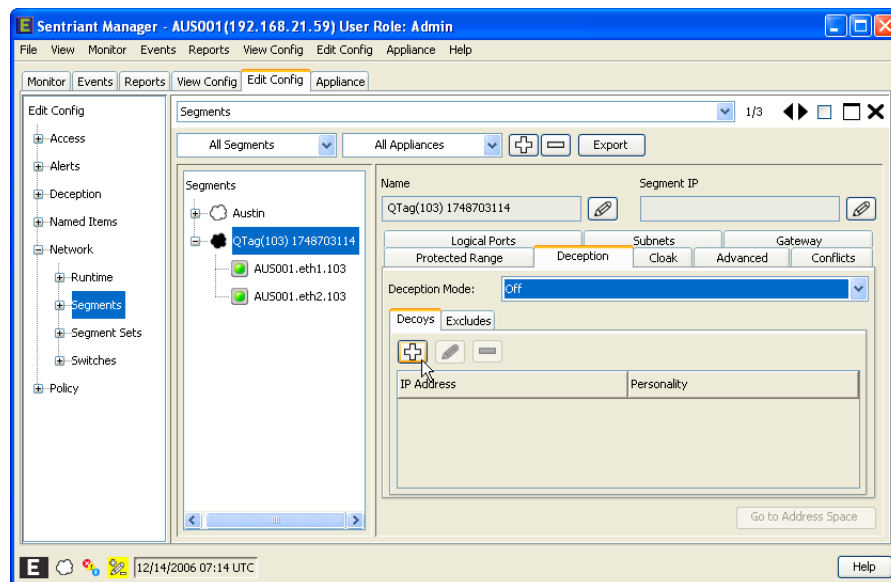
- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Deception** tab.
- 3 Select **On** from the **Deception Mode** drop-down list.



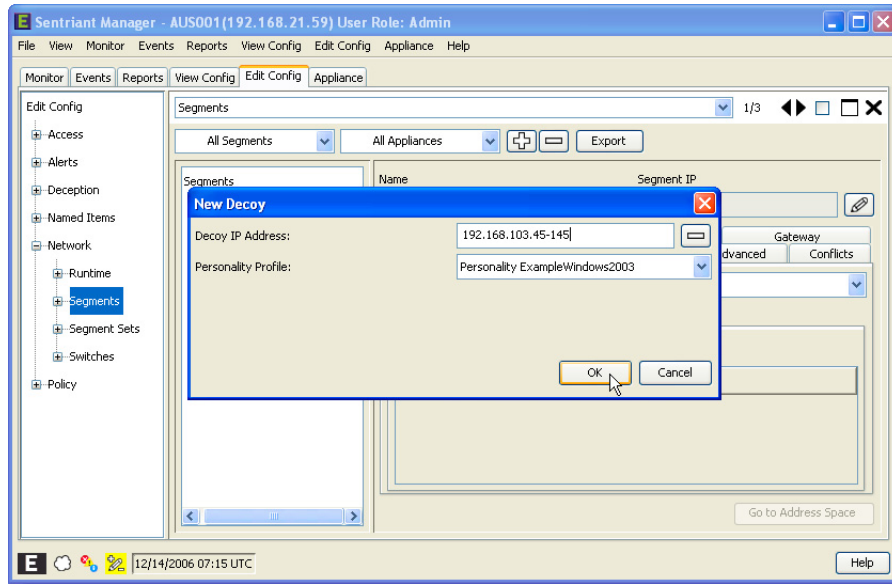
Deception has now been turned on for the Segment. The default Personality Set is used across the entire unused IP Address range of the Segment.

To add Decoys:

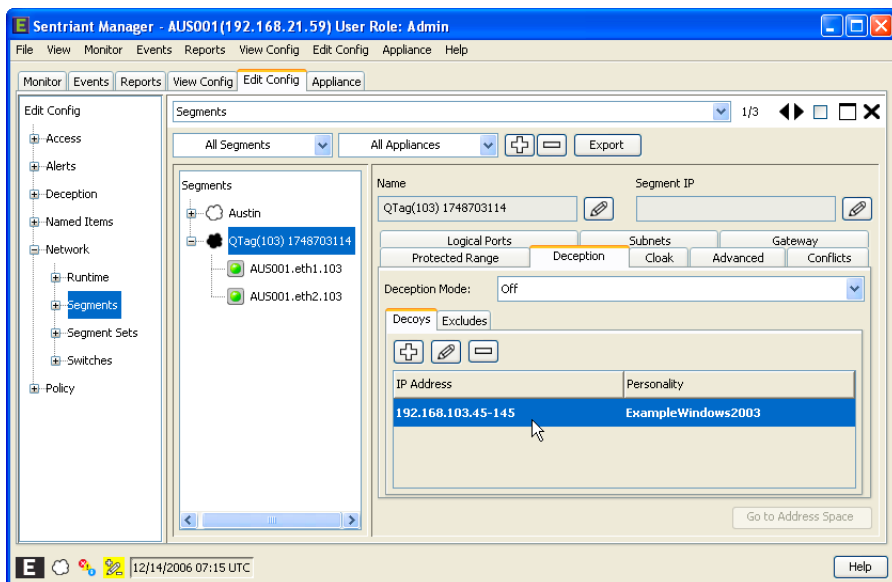
- 1 Click the **Decoy** tab.
- 2 Click the **Add** button.



- 3 Enter an IP Address(es).
- 4 Select a Personality from the drop-down list.
- 5 Click **OK**.

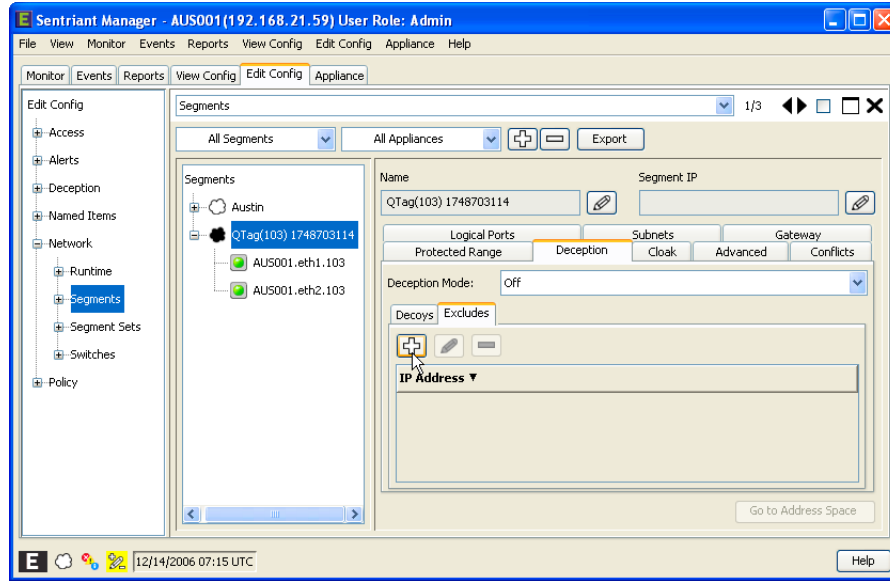


The IP Address(es) is now set as a Decoy and is displayed in the list.



To exclude Segment IP Address(es):

- 1 Click **Exclude** tab.
- 2 Click the **Add** button to bring up the New Exclude IP Address dialog.



3 Enter a Source IP Address by one of the two methods:

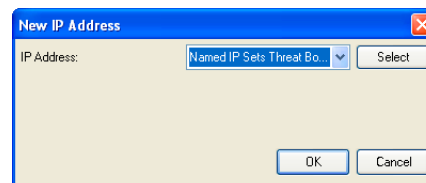
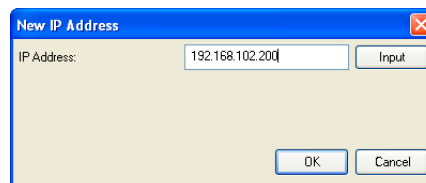
- Type an IP Address in the Source IP Address field. The example shows an IP Address using the hyphen(-) wildcard for one of the octets which selects a range of the octet.
- Use a IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.



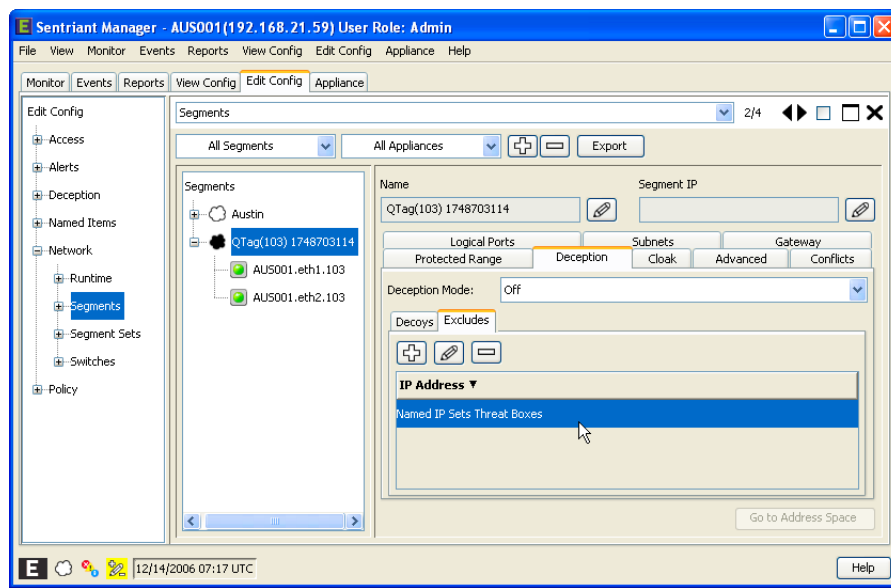
NOTE

To revert back to entering an IP Address, click the **Select** button.

4 Click **OK**.



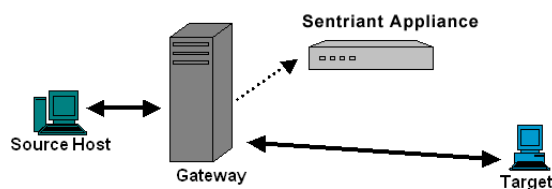
The IP Address(es) are added to the table.



Cloak

The Sentriant NG appliance has a patent-pending technique by which it unilaterally controls and terminates a communications flow between two or more computers. Cloaking can be manually or dynamically invoked by the Sentriant NG appliance when threats are identified or policy conditions violated.

In a network environment with an Sentriant NG appliance installed, the normal communication path may look something like the figure below. A source host goes through a gateway and contacts a target. The target starts a communication stream with the source.



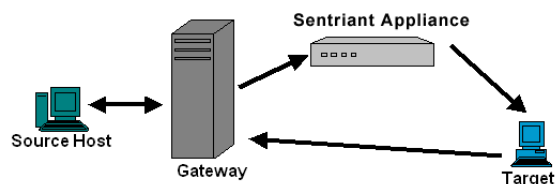
When Cloak All is selected as the response to a source, the Sentriant NG appliance inserts itself into **all** communication paths that exist between all known used IP Addresses of the monitored network and the threat source address. In this mode, the Sentriant NG appliance has taken over the critical communication path for much of the traffic between the monitored address range and the source. Due to the nature of Cloak All, the network traffic that is intended to communicate with the threat source is removed from the communication stream, while other traffic is allowed.

The source will remain cloaked until the configured threat time-out has been exceeded. At this time, the Sentriant NG appliance removes itself from the data path between all monitored addresses and threat sources, barring the existence of another threat that would not allow uncloaking.

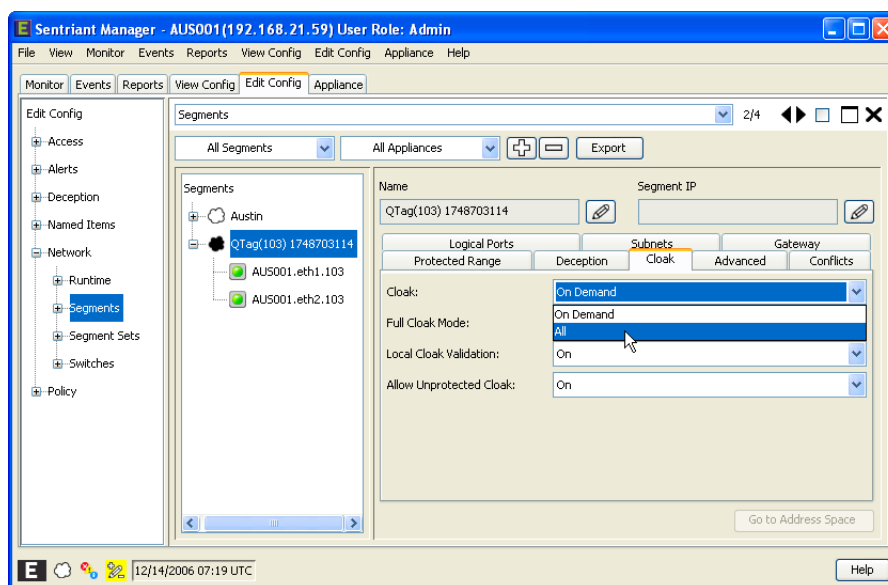
When Cloak On Demand is selected as the response, only sources that have triggered a threat response are removed from the communication stream.

**NOTE**

Only the source host is removed from the communication stream.

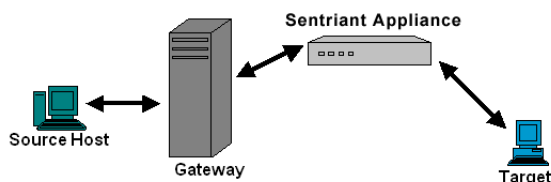
**To set Cloak for a Segment:**

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Cloak** tab.
- 3 Select **On Demand** or **All** from the **Cloak** drop-down list. Default value is On Demand.



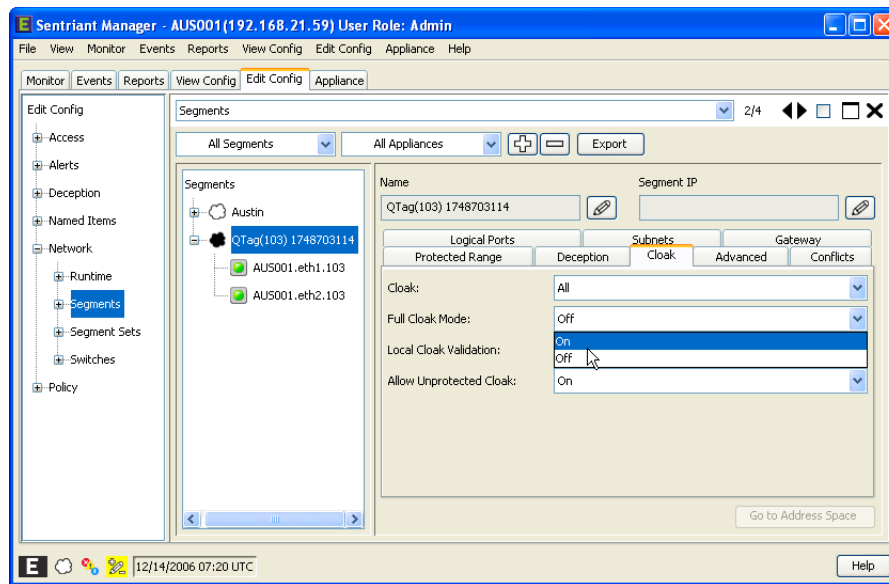
Full Cloak. Cloaking however does not monitor the traffic from the responding target. Full Cloak requires that both directions of the traffic to be routed to the Sentriant NG appliance.

By turning Full Cloak mode on, the responding target traffic is also routed through the Sentriant NG appliance to be monitored.



To turn Full Cloak on for a Segment:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Cloak** tab.
- 3 Select **On** from the **Full Cloak** drop-down list.



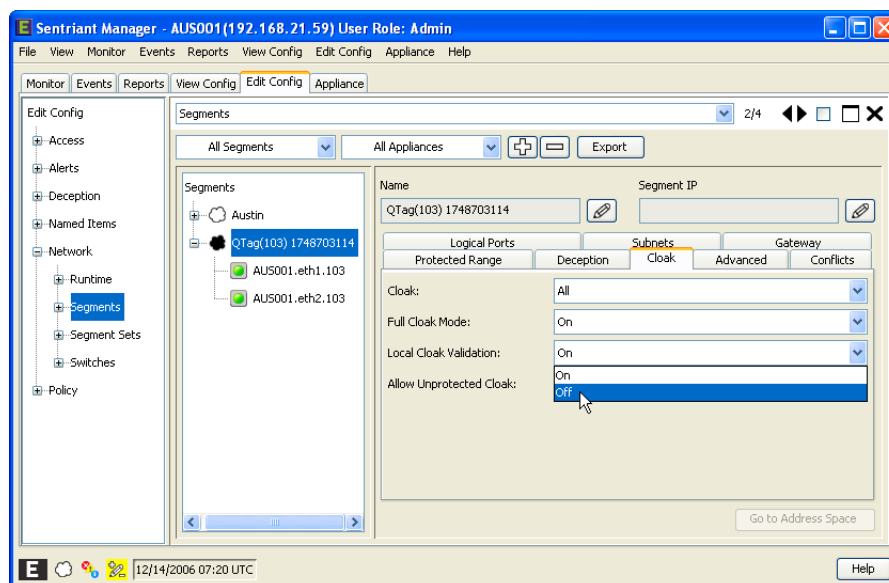
Local Cloak Validation. When a Segment detects a threat that originates in another Segment, the detecting Segment will request the originating Segment to cloak the threat source. When Local Cloak Validation is turned ON, the appliance will validate that the traffic did occur before allowing the source to be Cloaked. When Local Cloak Validation is turned Off, the originating Segment will trust the detecting Segment, and cloak the source regardless if the source is sending traffic.

**NOTE**

In a Broadcast Only deployment, Local Cloak Validation must be set to Off.

To set Local Cloak Validation:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Cloak** tab.
- 3 Select **On** or **Off** from the **Local Cloak Validation** drop-down list.



Allow Unprotected Cloak. Allow Unprotected Cloak prohibits SentiManager NG from cloaking sources that originate from an unprotected source. When SentiManager NG cloaks a source from an unprotected Segment, it must redirect all traffic from gateways in the traffic path to the SentiManager NG insuring that the cloaked source's traffic is filtered. Traffic from other sources is redirected from the SentiManager NG to their targeted hosts.

Disabling Allow Unprotected Cloak prohibits the appliance from cloaking unprotected sources, therefore prohibiting SentiManager NG from processing the gateway's traffic. It is important to note that External devices will still be cloaked by their local Segment no matter which Segment detects the threatening traffic. If a Segment is configured as a Transit Segment, Allow Unprotected Cloak is disabled as it would allow SentiManager NG to process, or take control of, all traffic between the configurable gateways.

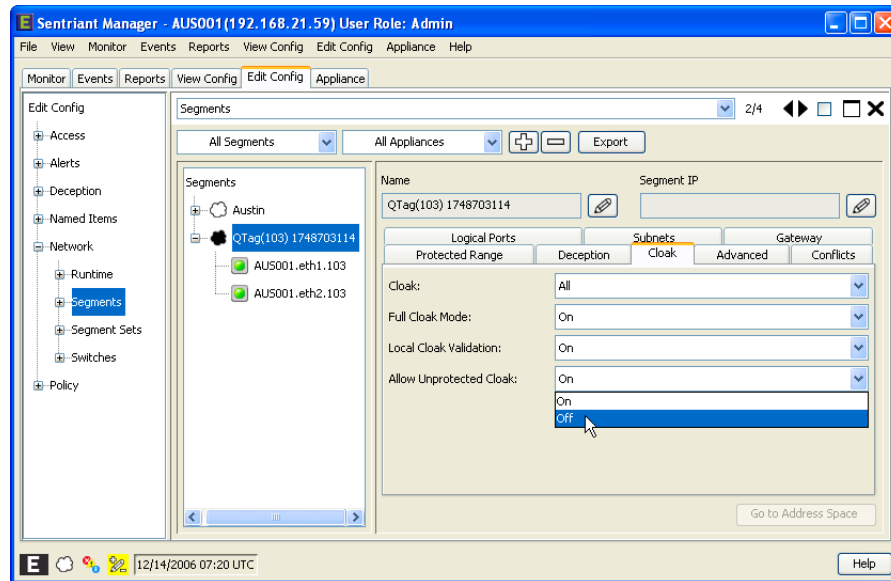


NOTE

If Transit Segment is turned on, Allow Unprotected Cloak will be disabled.

To set Allow Unprotected Cloak:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Cloak** tab.
- 3 Select **On** or **Off** from the **Allow Unprotected Cloak** drop-down list.



Advanced Segment Parameters

Transit Segment. Traffic from one Segment to another may be routed through an intermediate Segment or a Transit Segment. Sentriant NG Manager can be configured to analyze and validate this traffic coming from the targeted source through the Transit Segment and ending at a protected source. The default value is set to off.

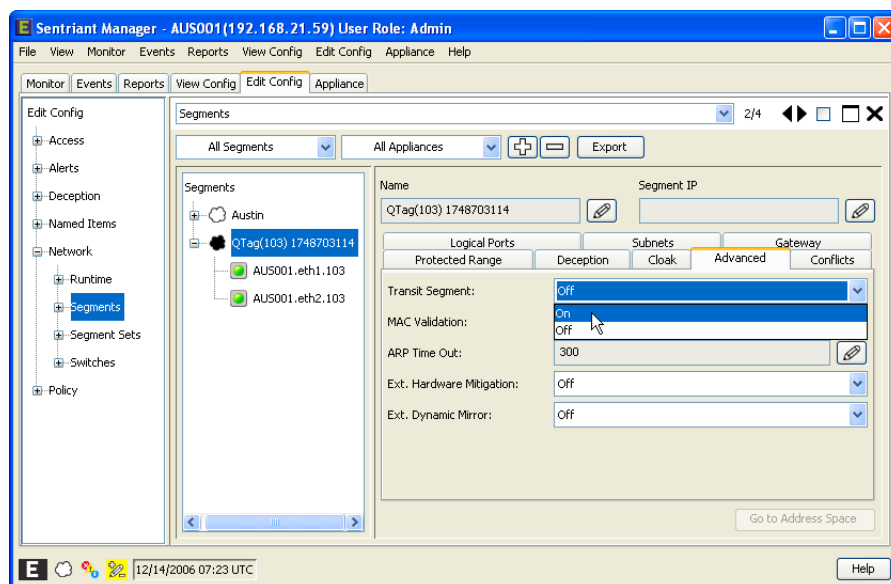


NOTE

Turning Transit Segment on will disable Allow Unprotected Cloak. See [“Allow Unprotected Cloak” on page 227](#) for more information.

To set Transit Segment:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Advance** tab.
- 3 Select **On** from the **Transit Segment** drop-down list.



MAC Validation. The Sentriant NG appliance uses its detection technology to determine that all received packets were transmitted from the source listed as the source address in the packet. These types of packets are referred to as spoof packets. Spoof packets are packets that are sent out from the local network but have false source addresses. This could signal the presence of a virus or worm.

When a spoofed packet is detected, the Sentriant NG Manager displays the true source of the packet as a threat. The address that was given as the false source of the spoofed packet is listed in the Spoofed As table located in the **Monitoring > Network > Sources > Details** table. The Spoofed As list appears for all sources that spoof network traffic, regardless of whether Spoofed Packets is the highest ranked threat for that source.

This spoofing technology validates that traffic received on the logical network Segment came from the correct host and that traffic from remote Segments entered the network via a gateway.

By turning on MAC Validation, Sentriant NG Manager will verify the MAC address of the source against the packet sent from the source. If the MAC address differs from the MAC address in the packet, the source is treated as a threat.

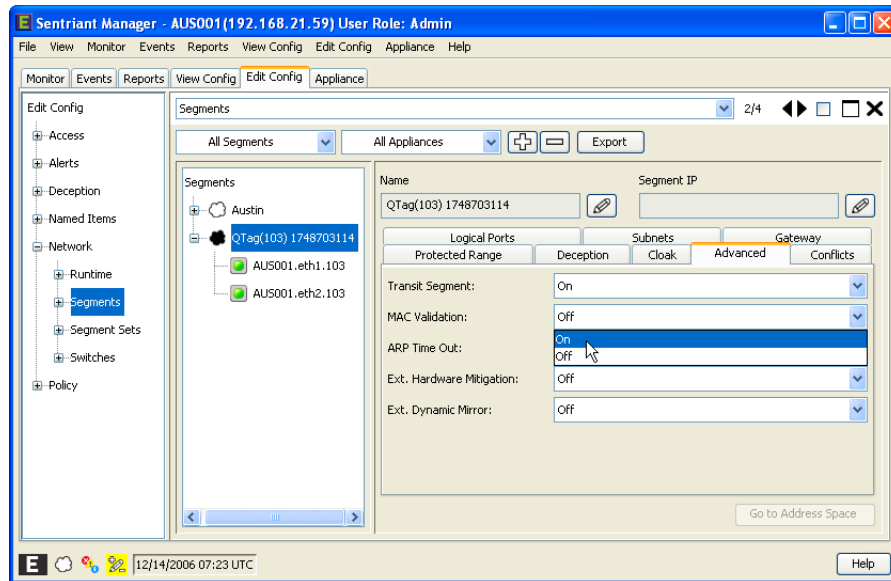


NOTE

To view source IP Addresses in the Sources Panel, MAC Validation must be turned on for the Segment. Turning MAC Validation on validates the sources MAC address and retrieves the IP Address. If MAC Validation is turned off for the Segment, the source IP Address and MAC address will not be displayed in the Sources Panel. The Sources Panel will show the source as masked.

To set MAC Validation:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Advance** tab.
- 3 Select **On** or **Off** from the **MAC Validation** drop-down list.

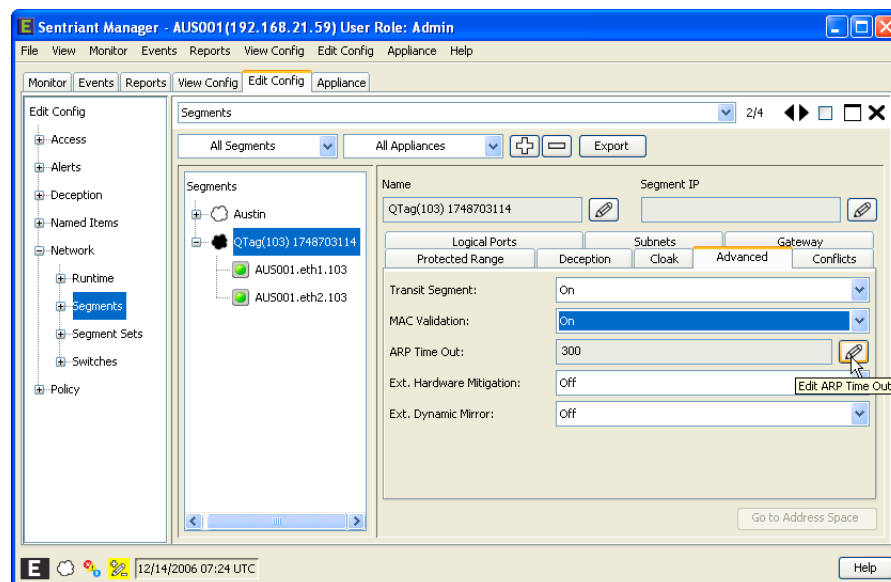


ARP Time Out. The ARP Time Out is used to set the response delay from the source's host. The response may be delayed in larger network environments and/or due to large amounts of traffic causing a rule to trigger erroneously.

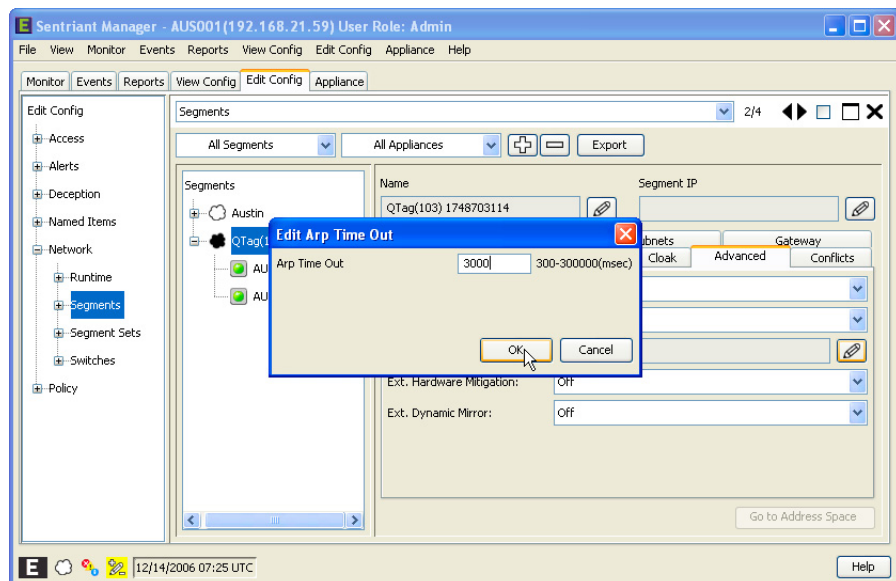
The default ARP Time Out is set to 300 milliseconds.

To edit the ARP Time Out:

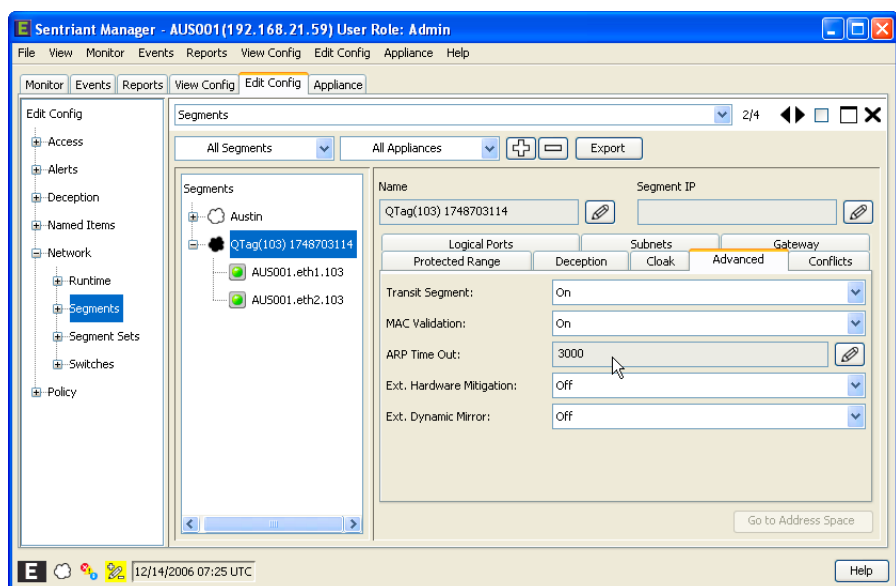
- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Advance** tab.
- 3 Click the **Edit ARP Time Out** button.



- 4 Enter a value. Legal values are from 300 to 300,000 milliseconds.



The ARP time out delay is set.



External Hardware Mitigation. Instructs the system on whether to utilize external hardware to mitigate threats, in addition to cloaking.



NOTE

External Hardware Mitigation is specific to configurations with BlackDiamond™ 10808 switches.

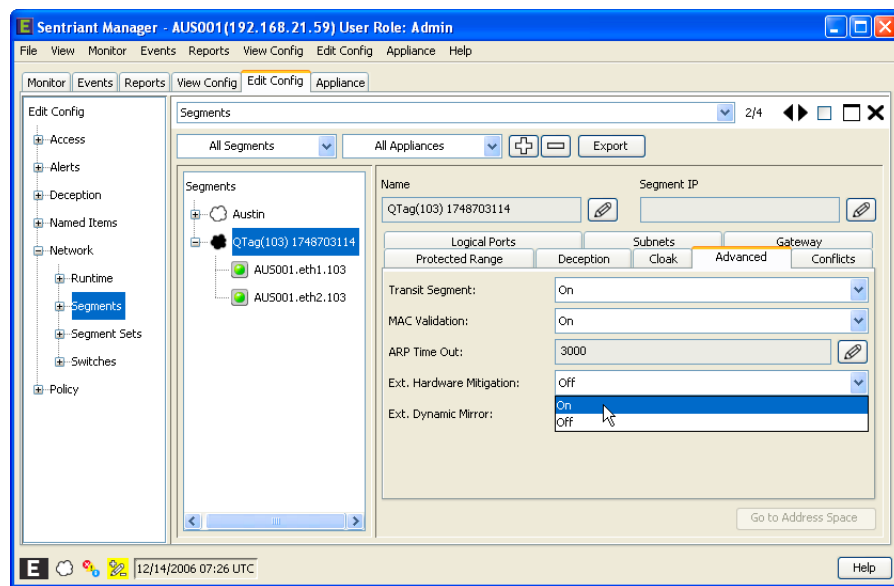


NOTE

A switch must be added to activate the External Hardware Mitigation field. See to add a switch.

To set Transit Segment:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Advance** tab.
- 3 Select **On** from the **MAC Validation** drop-down list.



External Dynamic Mirror. Informs the system on whether External Dynamic Mirroring is to occur on this Segment.

**NOTE**

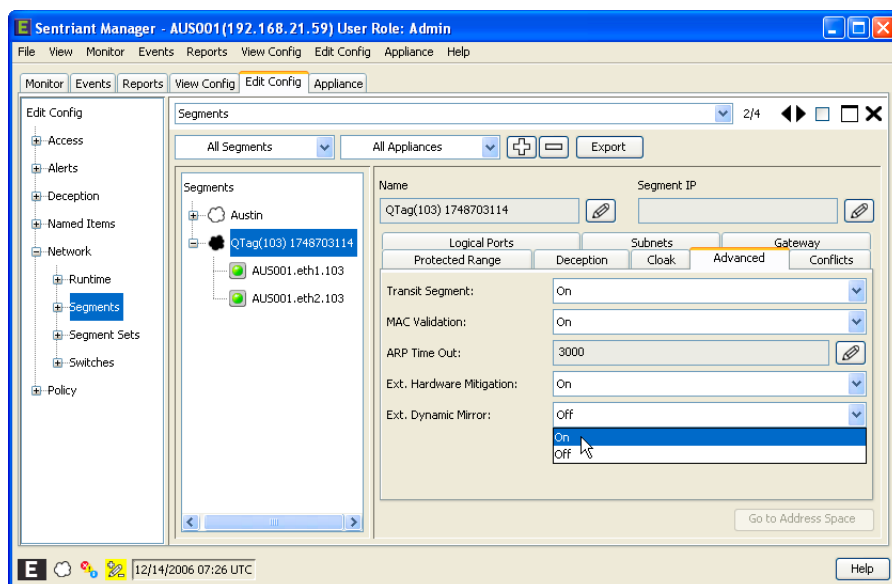
External Dynamic Mirror is specific to configurations with BlackDiamond 10808 switches.

**NOTE**

A switch must be added to activate the External Dynamic Mirror field. See [“Adding Switches”](#) on page 252 to add a switch.

To set External Dynamic Mirror:

- 1 From **Edit Config > Network > Segments**, select a Segment from the Network Segment list.
- 2 Select the **Advance** tab.
- 3 Select **On** from the **External Dynamic Mirror** drop-down list.

**NOTE**

Changing Advanced settings does not change the Sentriant NG appliance's configuration. The changes are made locally to a stack of configuration changes and is displayed in the Tab/Folder List with an edit icon. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#).

Deleting Segments

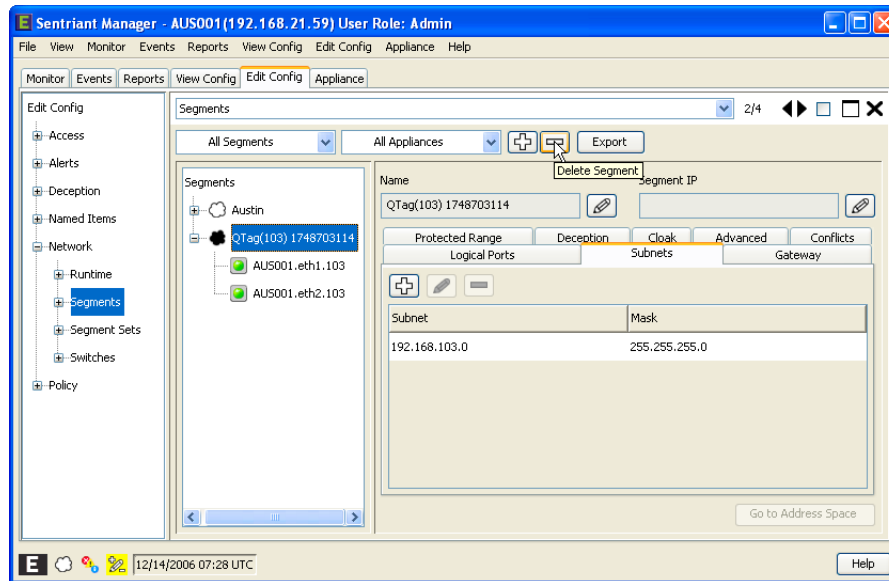
When segments or VLANs on the switch are deleted, it will be necessary to remove them from the Sentriant NG Manager. The Segment data, though no longer used will remain in the database therefore will be displayed as valid Segment.

**NOTE**

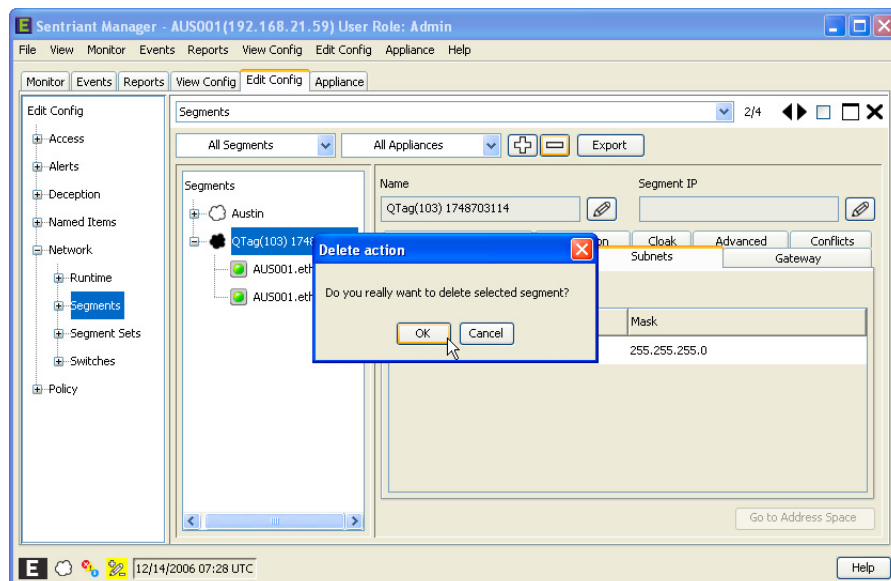
The segments should be removed from the switch prior to deleting from Sentriant NG Manager. If the segments are not deleted, they will reappear once the Sentriant NG Manager refreshes.

To delete a Segment:

- 1 From **Edit Config > Network > Segments**, select a Segment from the drop-down list.
- 2 Click the **Delete Segment** button.

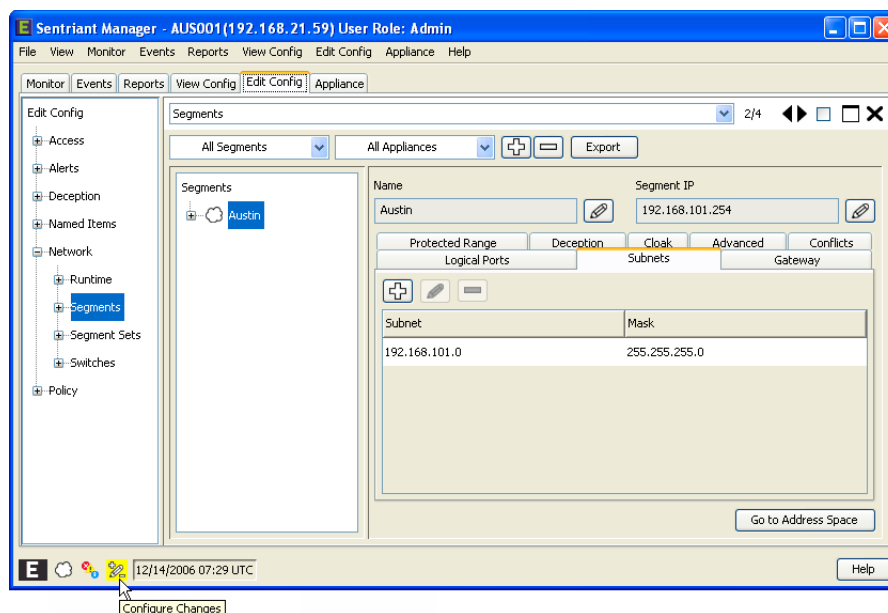


3 Click OK to delete the Segment and close the dialog.



NOTE

Clicking OK adds the deleted Segment to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#).



Port Verification

The command line interface provides access to the topology.pl script that check and report on the low-level topology discovery processes. This script provides insight into both the Segment creation and interface discovery portions of the topology probe packets. The script is run without any arguments, and consists of two basic sections. The first section lists which interfaces are active under which Segment. The second section lists which interfaces recognize each other. An example of running topology.pl on a Sentriant NG yields the following output:

```
[support@]$ topology.pl
Segments to interfaces
1: [eth3, eth2, eth1]
4: [eth0]
5: [eth1.100, eth2.100]
6: [eth1.200, eth2.200]
7: [eth1.300, eth2.300]
8: [eth1.400, eth2.400]
9: [eth3.100, eth4.100]
10: [eth3.200, eth4.200]
11: [eth3.300, eth4.300]
12: [eth3.400, eth4.400]
Interface sees:
eth0: []
eth1: [eth2, eth3, eth4]
eth2: []
eth3: [eth1, eth2, eth4]
eth1.100 [eth2.100]
eth2.100: []
eth1.200: [eth2.200]
eth2.200: []
eth1.300: [eth2.300]
eth2.300: []
eth1.400: [eth2.400]
```

```
eth2.400: []
eth3.100: [eth4.100]
eth4.100: []
eth3.200: [eth4.200]
eth4.200: []
eth3.300: [eth4.300]
eth4.300: []
eth3.400: [eth4.400]
eth4.400: []
[support@]$
```

Note that for the purposes of interface grouping, the logical OR condition is met, since the ETH1.xxx interfaces "sees" the ETH2.xxx interfaces and the ETH3.xxx interfaces see the ETH4.xxx interfaces. All ETH1.xxx interfaces should be flagged as "Read Only" and paired with the corresponding ETH2.xxx interface. Likewise, all ETH3.xxx interfaces should be flagged as "Read Only" and paired with the corresponding ETH4.xxx interface.

Segment Sets

A Segment Set is a collection of segments that exhibit similar policy behaviors. For example, if a Segment Set is reserved for DHCP clients (laptops), then a set can be created containing all laptops within a Segment and then parameters can be set for rules, deception distributions and modifiers. Creating segments is accomplished using the Segment Assistant.

A default Segment Set is created initially. All discovered or unconfigured segments will be added to the default set and can later be moved to newly created Segment Sets.

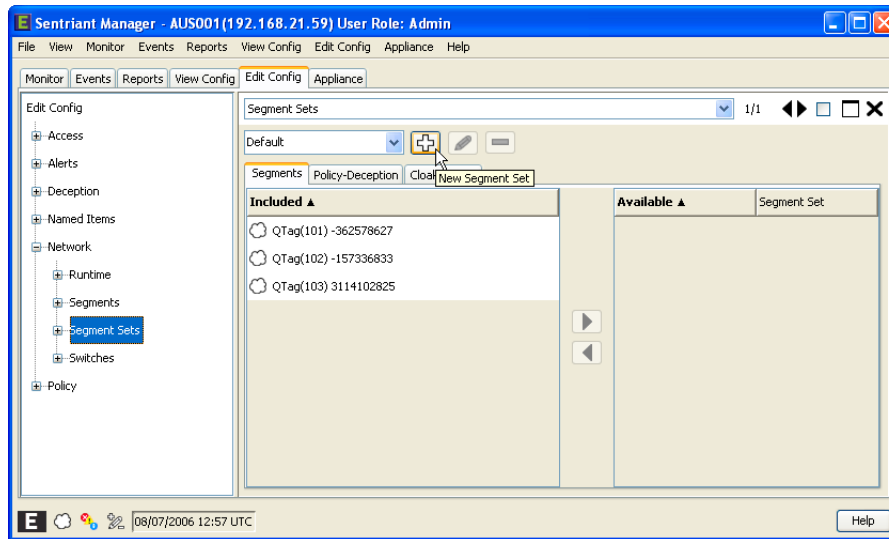
From the Segment Set Panel, you can:

- [Create a Segment Set](#)
- [Associate segments](#)
- [Associate Rule and Personality Sets](#)
- [Exclude IP Addresses from Rule Responses](#)
- [Omit communication streams from being monitored](#)

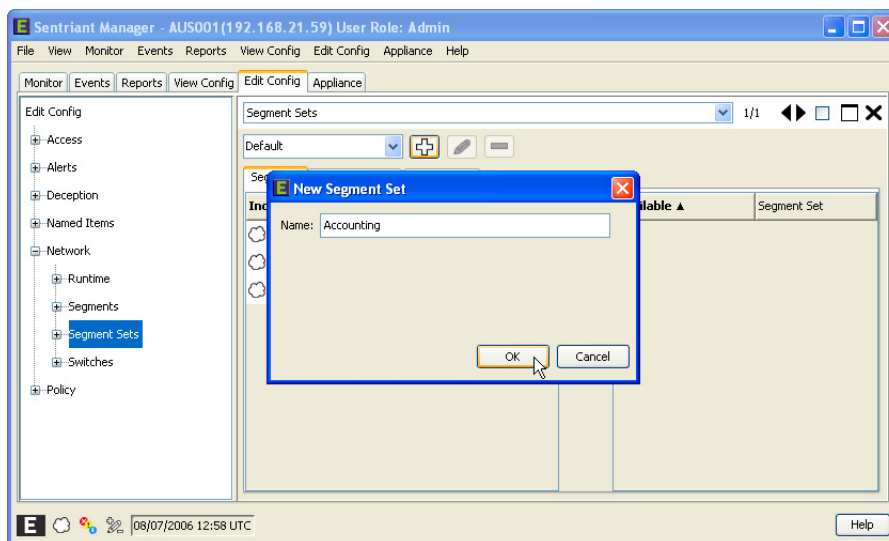
Creating Segment Sets

To create a Segment Set:

- 1 From **Edit Config > Network**, select **Segment Sets**.
- 2 Click the **New Segment Set** button.



3 Enter a Segment Set name.



The new Segment Set is displayed in the Name field and in the navigation tree located on the left side of the screen.



NOTE

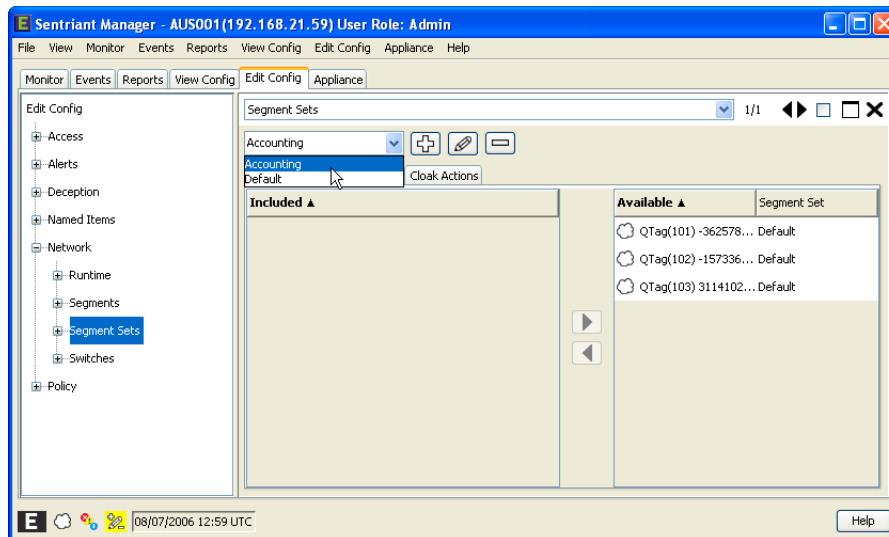
The new Segment Set is not added to the Sentriant NG appliance. The changes are made to the stack of local configuration changes and is displayed in the Tab/Folder List with an edit icon. However, the Sentriant NG appliance's configuration has not been updated with the new changes. To learn about saving configuration changes to the Sentriant NG appliance, see [“Saving Changes to the Sentriant NG Appliance” on page 133](#).

Associating Segments

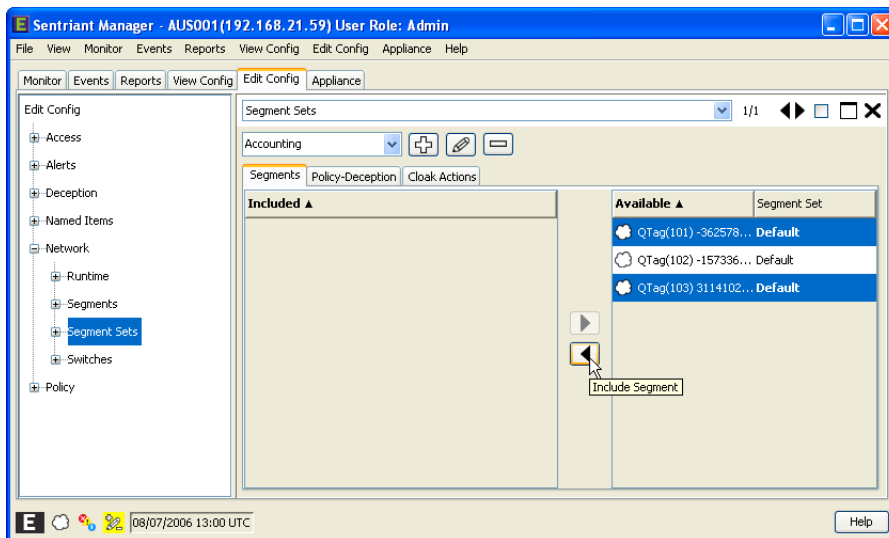
When you select the **Segment Sets** tab, the panel displays a list of all of the Segment Sets and associated segments. The **Default** Segment Set is displayed initially. Segments can be associated with new Segment Sets so that each set contains similarly configured segments.

To associate a Segment with a Segment Set:

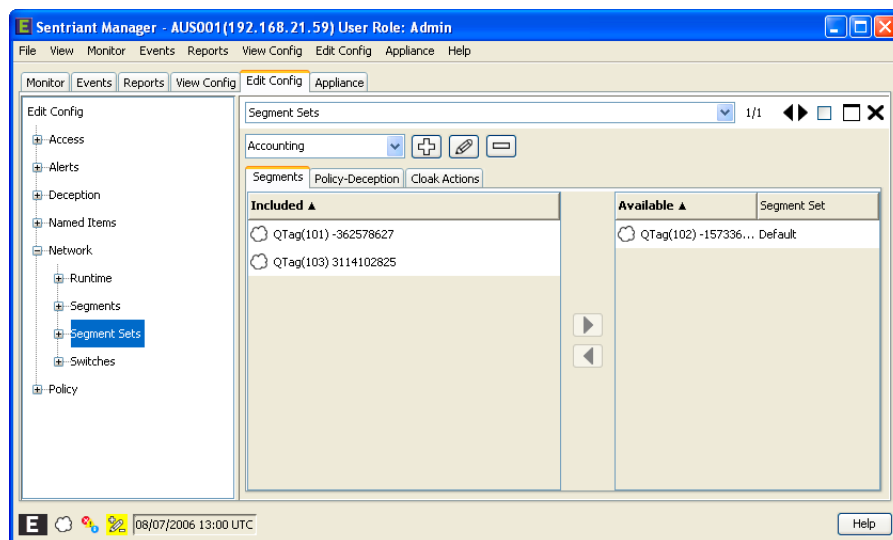
- 1 From **Edit Config > Network > Segment Sets**, select a Segment Set from the list.



- 2 From the **Available** List on the right of the screen, select the Segment(s) which will be moved to the Laptop Segment Set.



- 3 Click the **Include** Segment button to move the segments to the Laptop Segment Set. The new Segment is associated with the selected Segment Set.



Associating Rule and Personality Sets

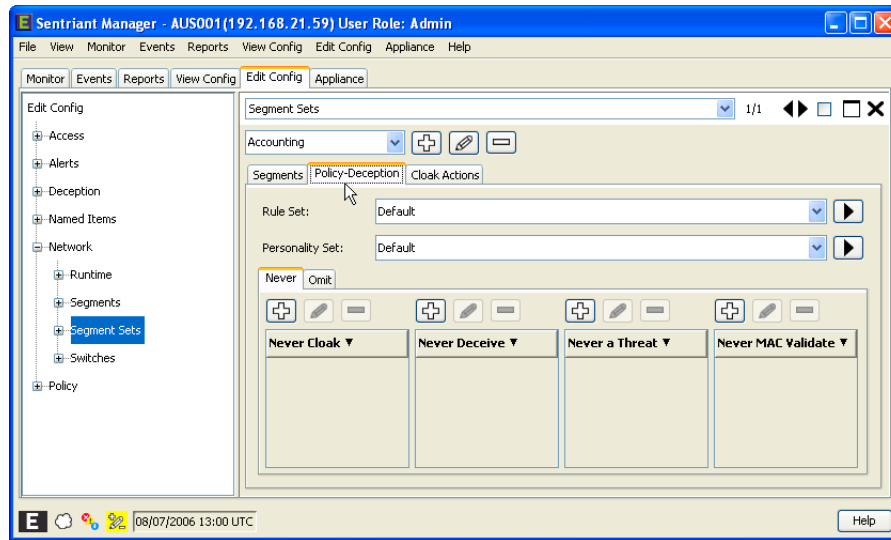
A Rule Set is global in functionality meaning once a Rule Set is assigned to a Segment Set, any network traffic to the IP Addresses within the Segment contained in the Segment Set that violates a rule will activate deception or rule mitigation responses.

A Personality Set contains a personality or multiple personalities making up a collection of non-hosts, Linux hosts, Windows XP hosts, or Windows 98 hosts that emulated operating systems when communicated by a source.

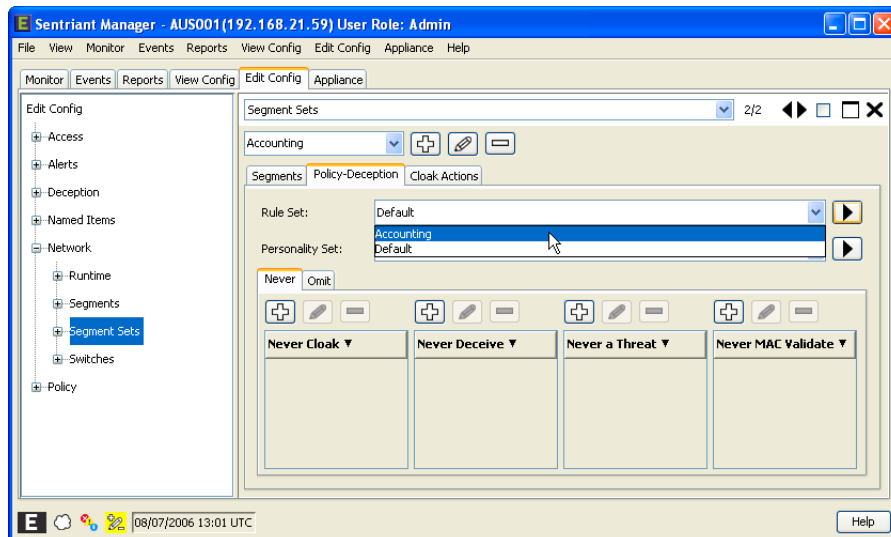
A Personality Set is assigned to a Segment Set. The purpose of the Personality Set is when a threat is detected on the unused address space a percentage of the personalities with the set is sent to the source disguising the Port and IP Address.

To associate a rule set:

- 1 From **Edit Config > Network > Segment Sets**, select the **Policy-Deception** tab.

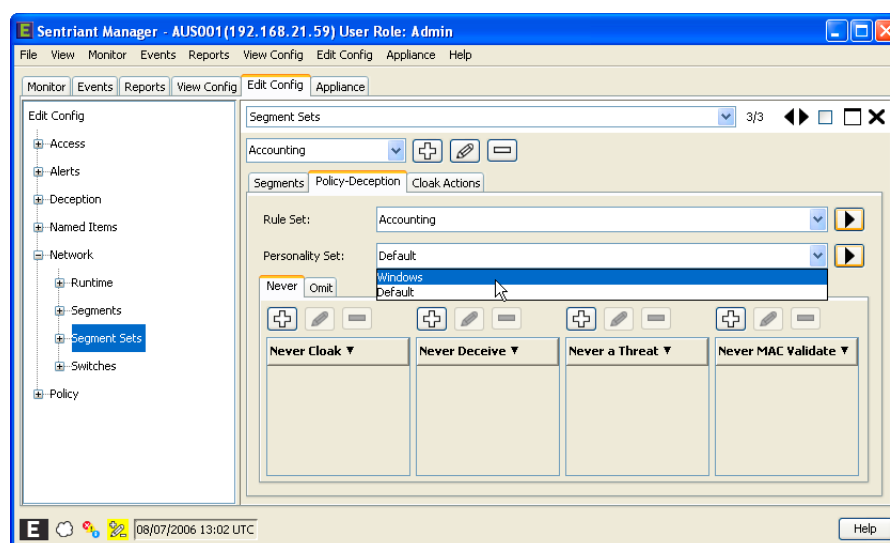


- 2 From the Rule Set drop-down list, select a Rule Set with associate to the Segment Set.



To associate a personality set:

- 1 From the Personality Set drop-down list, select a Personality Set to associate with the Segment Set.



NOTE

Setting the Rule and Personality Sets to a Segment Set does save the setting to the Sentriant NG appliance. The changes are made to the stack of local configuration changes and is displayed in the Tab/Folder List with an edit icon. However, the Sentriant NG appliance's configuration has not been updated with the new changes. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance"](#) on page 133.

Exclude from Rule Responses

When Rules are added to a Segment Set it affects all the IP Addresses within the set's range.

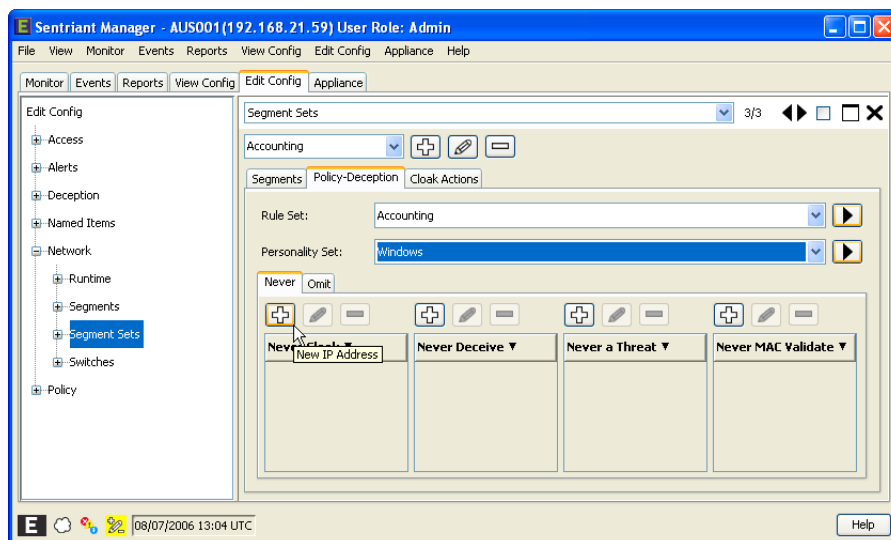
The four rule types that prevent source threats from attacking Segment IP Addresses are:

- Cloak - Sources are taken out of the communication paths only for devices the source attempted to communicate with.
- Deceive - Sources are allowed to continue with its current network activity without cloaking, however it is configured to deceive the source address if the source attempts to contact an unused IP Address and will activate a deception distribution or personality profile.
- Threats - A packet that does not comply with relevant protocol specifications. Many worms, viruses, and automated network probes exhibit reconnaissance-like patterns. The Sentriant NG appliance evaluates every packet sent by a source to determine whether its out of specification.
- MAC Validate - A packet that is sent out from the local network but has a false source IP Address. This could signal the presence of a virus or worm. The Sentriant NG appliance uses its detection technology to determine that all received packets were transmitted from the source listed as the source address in the packet.

The administrator can exclude specific IP Addresses and/or ranges of IP Addresses by adding the IP Addresses to the Never tables. For example, if a source threat is a spoof and communicates with an IP Address contained within the Never MAC Validate table, the MAC Validate will not be activated preventing spoofing activities.

To add IP Addresses to Never Tables:

- 1 From **Edit Config > Network > Segment Sets** , select the **Policy-Deception** tab.
- 2 From one of the Never tables, click the **Add** button where you would like to add IP Addresses.



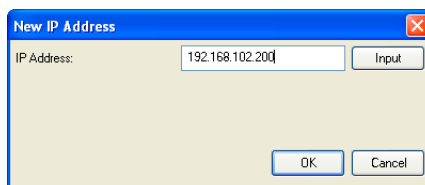
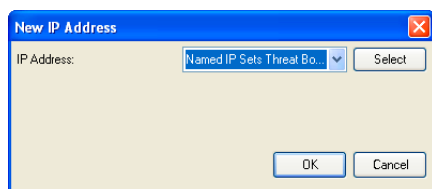
- 3 Enter an IP Address by one of the two methods:
 - Type an IP Address in the Source IP Address field. The example shows an IP Address using the hyphen (-) wildcard for one of the octets which selects a range of the octet.
 - Use a IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.

NOTE

To revert back to entering an IP Address, click the **Select** button.

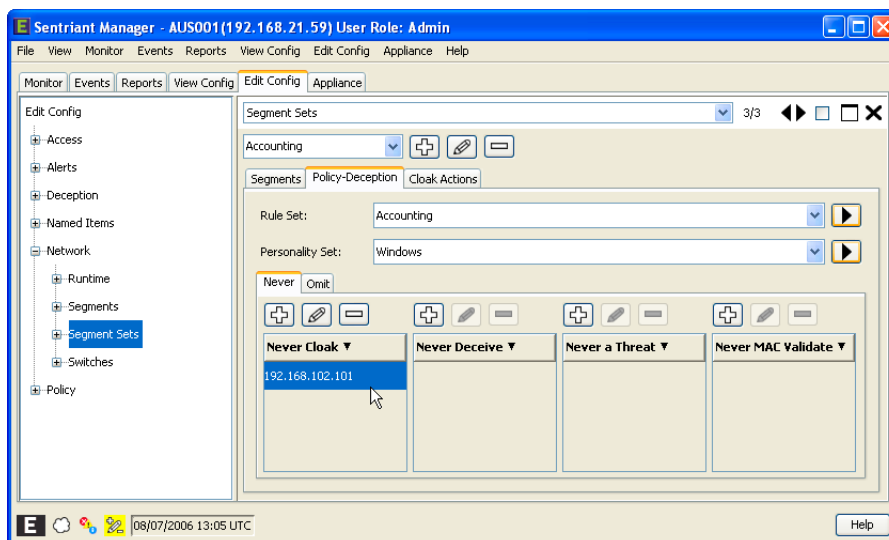
NOTE

Wildcards may be used, for example to select the entire range of IP Addresses use an asterisk (*). You may also specify ranges for an octet of the IP Addresses. You can use commas (,) and dashes (-) for multiple ranges. For example (192.168.21,23.* or 192.168.25.1-254).



4 Click OK.

The IP Address is added to the table.



Omitting Communication Streams

Traffic to and from a monitored host may be a watch, suspect or threat activity. The Sentriant NG appliance considers all network traffic it monitors to be a bidirectional communication stream. A single TCP session between two hosts, or source and target, is considered as one distinct communication stream within the Sentriant NG appliance. Since all communication streams are monitored by the Sentriant NG appliance, it may be necessary to omit certain communication streams from being detected and monitored. To prevent erroneous threat activity, each host's IP Addresses must be added to the Omit table. Omitting a communication stream is unidirectional, therefore requires both IP Addresses of the communication stream to be included in the Omit table to ignore the communication stream traffic monitored by the Sentriant NG appliance.

The Omit table also includes the capability to omit ranges of IP Addresses by the use of wildcards. Wildcards may be used, for example to select the entire range of IP Addresses, use an asterisk (*). You may also specify ranges for an octet of the IP Addresses. You can use commas (,) and dashes (-) for multiple ranges. For example (192.168.21,23.* or 192.168.25.1-254).

Ports and Port types may also be omitted from being monitored by the Sentriant NG appliance. Ports can be omitted for a source and/or target of the communication stream. If a source Port number is entered, traffic **from** that Port will be ignored. If a target Port number is entered, the traffic **to** the target Port will be ignored.

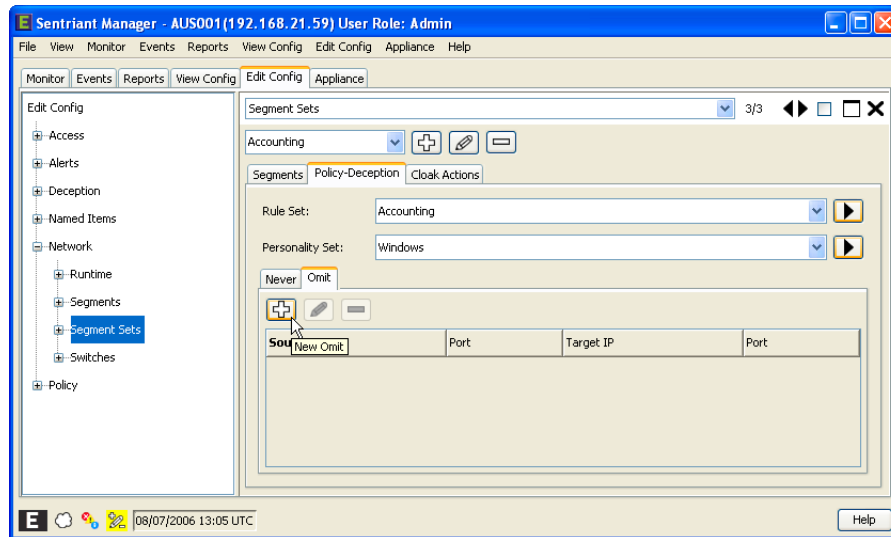


NOTE

When a communication stream is omitted, the traffic will not be visible in the Status Bar or in the Sources Panel.

To omit a communication stream:

- 1 From **Edit Config > Network > Segment Sets** , select the **Policy-Deception** tab.
- 2 Click the **Omit** button.

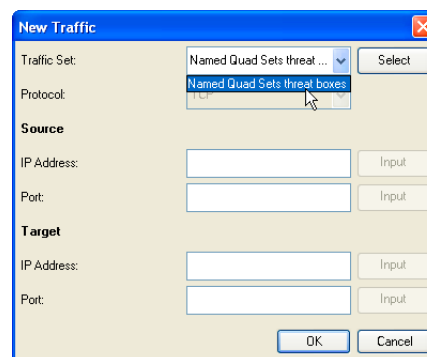


- 3 The **New Traffic** dialog opens.

There are various methods of adding traffic items to the dialog. You may select a Traffic Set from the Named Items, enter each traffic item or use a combination of entered traffic item data and select IP and Port Sets from Named Items.

To use a Traffic Set:

- Click the **Input** button on the Traffic Set line to add a Traffic Set. The remaining traffic data items are disabled because each data item is using the Traffic Set data.



Entering data items and/or using IP and Port Sets:

- Select a Port Protocol from the drop-down list. Choices are TCP, UDP, and ICMP.
- Enter a Source IP Address by one of the two methods:
 - Type an IP Address in the Source IP Address field. The example shows an IP Address using the hyphen (-) wildcard for one of the octets which selects a range of the octet.
 - Use a IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.

**NOTE**

To revert back to entering an IP Address, click the *Select* button.

- Enter a Source Port Number by one of the two methods:
 - Type a Port number in the Source Port field.
 - Use a Port Set by clicking the **Input** button and then selecting an Port Set from the drop-down list.
- Enter a Target IP Address by one of the two methods:
 - Type an IP Address in the Targets IP Address field.
 - Use an IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.

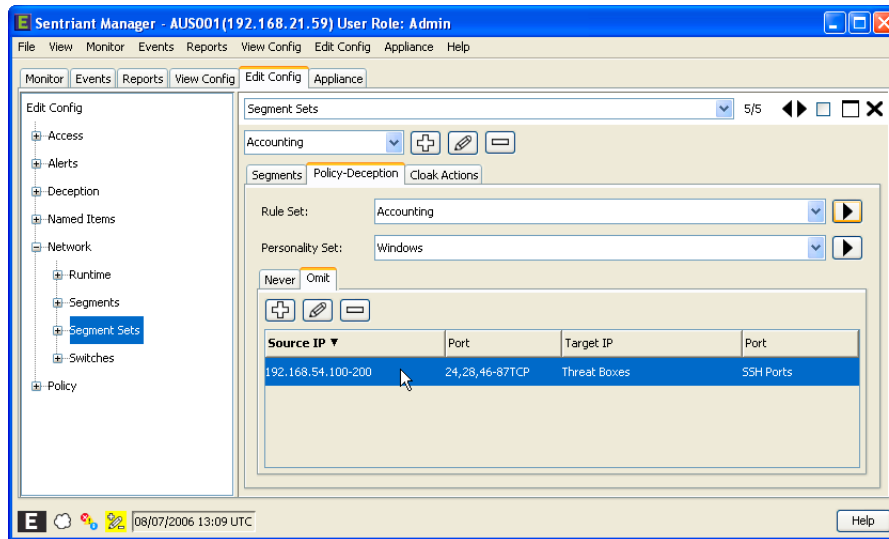
**NOTE**

To revert back to entering an IP Address, click the *Select* button.

- Enter a Target Port Number by one of the two methods:
 - Type a Port number in the Target Port field.
 - Use a Port Set by clicking the **Input** button and then selecting an Port Set from the drop-down list.

- 4 Click **OK**.

The traffic set is added to the Omit table.



NOTE

Clicking OK adds the new Omit item to the stack of local configuration changes however, it does not update the Sentriant NG's configuration. To learn about saving configuration changes to the Sentriant NG, see ["Saving Changes to the Sentriant NG Appliance"](#) on page 133.

Cloak Actions

When the Sentriant NG detects a policy violation, the appliance may be configured to Cloak or prohibit the host from communicating on the network until the threatening behavior subsides or the admin intervenes. Cloak Actions provides a mechanism to alert the host upon being cloaked from the network using an HTML message. For example, a Sentriant NG detects a policy violation and cloaks a user's work station. The user will no longer be able to send or receive network traffic under normal conditions. When the cloaked user attempts to send an HTTP request using an internet browser, the browser is redirected from the home page address to a configured HTML message located on the Sentriant NG. The message notifies the user that network access has been temporarily disabled and directs them to contact the support desk.

Cloak Actions default settings use Port 80 as the access point for sending and receiving traffic from the infected network device to the Sentriant NG or specified web server. It may become necessary to modify the existing access point(s) or add additional access points. For example, you may want to connect to the affected network device using SSH.

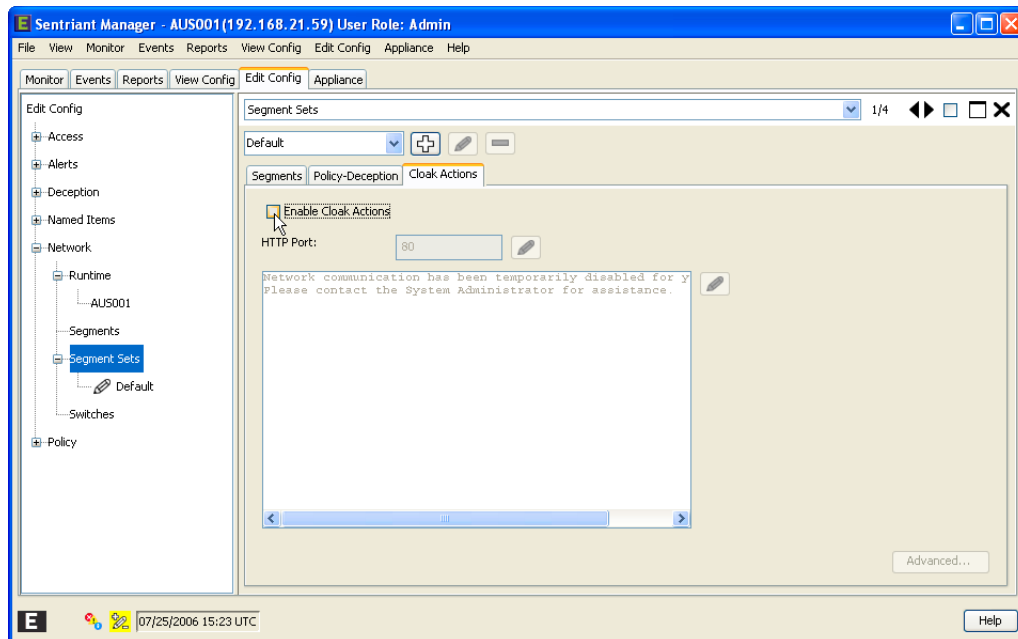
NOTE

If a host is cloaked, and the cloak response message is not served as expected if the browser is currently opened, the web browser has cached the currently viewed page. The user must refresh the web browser to see the page.

[Advanced Cloak Actions](#) settings for packet limiting may be set by clicking the Advance button on the lower right of the panel.

To turn Cloak Actions on:

- 1 From **Edit Config > Network > Segment Sets**, select the **Cloak Actions** tab.
- 2 Click **Enable Cloak Actions** check box to turn **Cloak Actions** on.



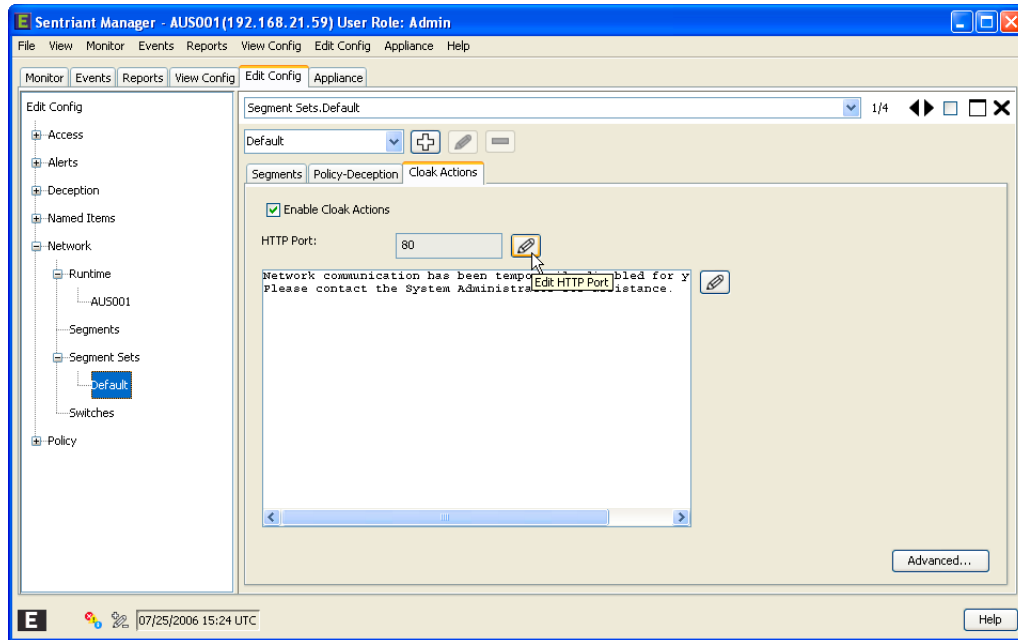
The Sentriant NG, utilizing a web server, sends an HTML message to cloaked users when they attempt to open an Internet browser over Port 80. You may change the Port if the web server resides on a different Port.

NOTE

The default Port type is TCP.

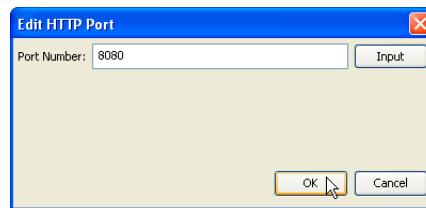
To edit the HTTP Port:

- 3 Click the **Edit HTTP Port** button.

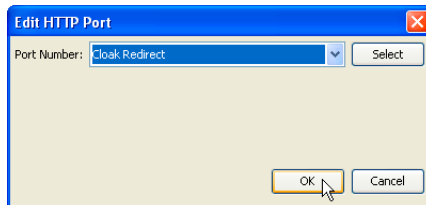


There are two methods of entering a Port number:

- 4 Enter a Port number, or...

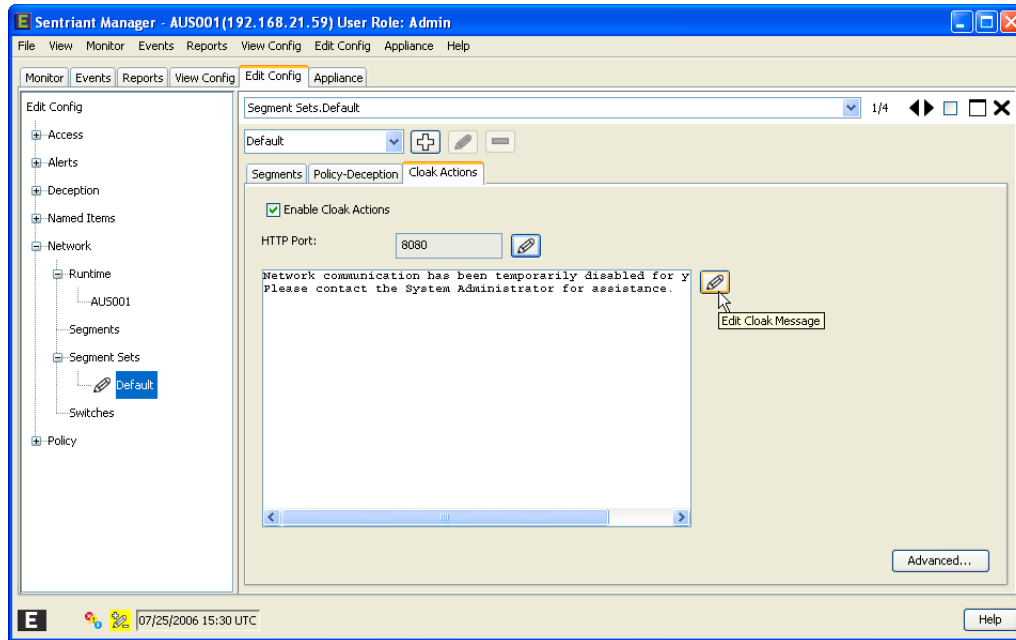


- 5 Click the **Input** button and select a Port set from the drop-down list.
- 6 Click **OK** to close the dialog.

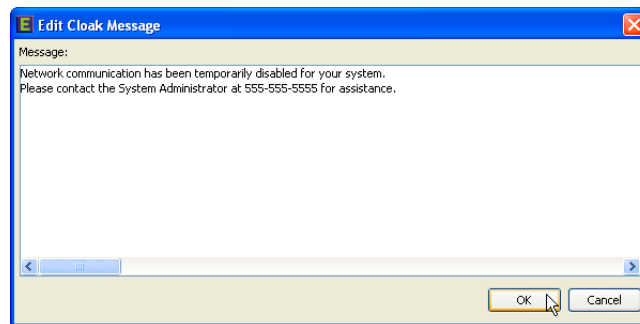


To edit the cloak message:

- 7 Click the **Edit Cloak Message** button.



8 Edit the cloak message.



NOTE

HTML tags or characters are not allowed in the cloak message.

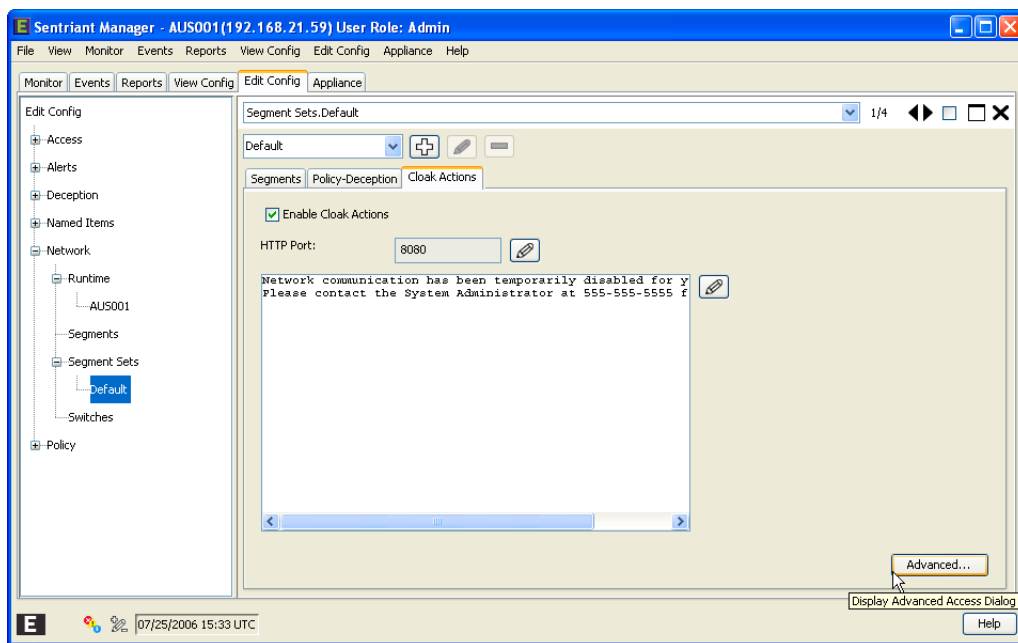
9 Click **OK** to save the message and close the dialog.

10 Save the configuration changes to the SentiManager NG.

Advanced Cloak Actions Settings. Each access point may be set to limit the network traffic passing to and from the infected network devices. It is recommended that best practices of limiting bandwidth be applied in the event of a large number of devices being affected by a worm or other rapidly propagating threat generating large amounts of network traffic. Cloak Actions provides a mechanism to limit the number of network packets per minute sent from a device to the web server and vice versa. The traffic to and from the SentiManager NG may also be limited.

To edit Advanced Cloak Actions settings:

- 1 Click the **Advanced...** button at the lower right of the panel.

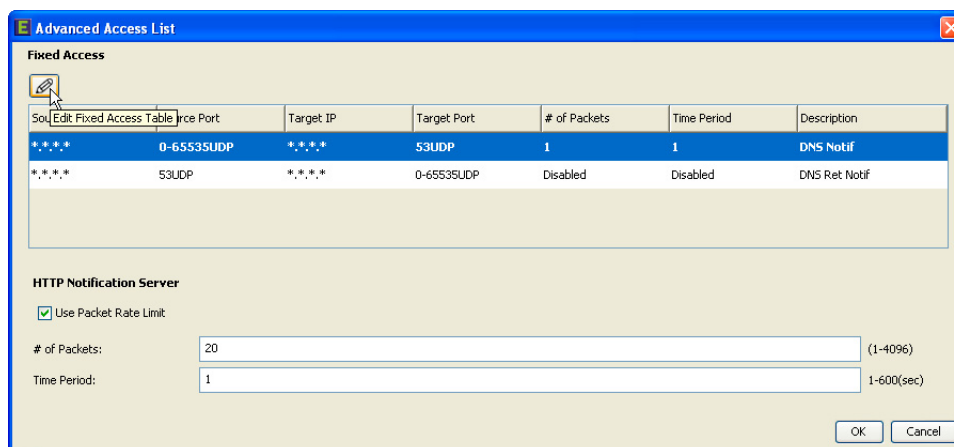


The Advanced Access List dialog opens. The top portion of the dialog displays the fixed access points that allow network traffic to flow between the Sentriant NG and the network device and vice versa. The bottom portion displays the HTTP Notification Server, a component of the Sentriant NG, and packet rate settings.

The default settings use packet rate limiting set to 1 packet per second for DNS Notification and disabled for DNS Return Notification fixed access points. The HTTP Notification Server is set to 5 packets per second.

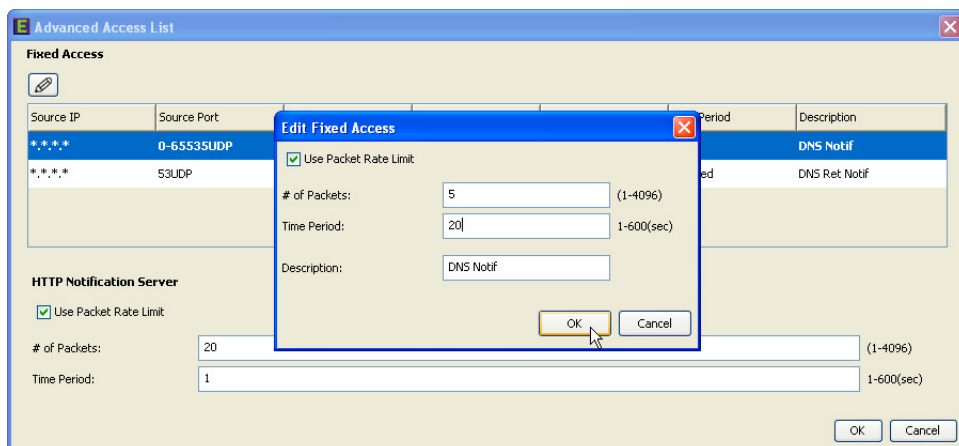
To edit the Fixed Access points packet rating:

- 2 Click the **Edit Fixed Access Table** button.



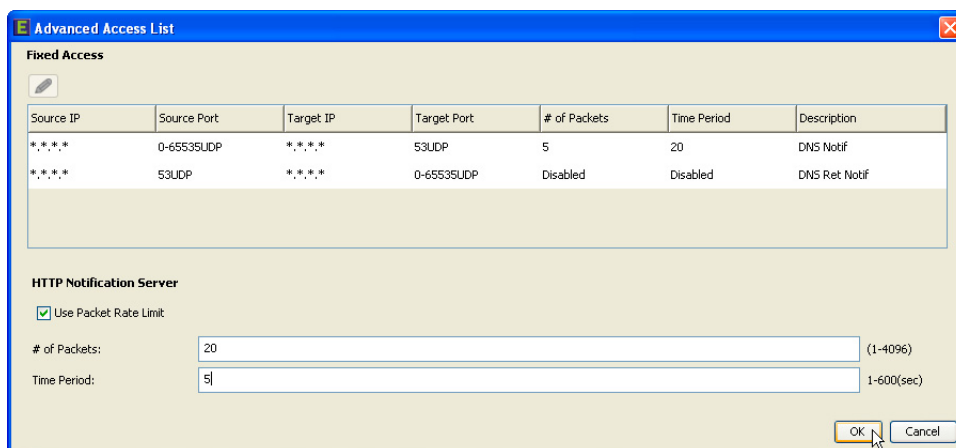
- 3 The **Edit Fixed Access** dialog opens. Make the following changes:

- Turn rate limiting off by unchecking the **Use Packet Rate Limit** checkbox.
 - Enter a new value in the **# of Packets:** field.
 - Enter a new value in the **Time Period:** field.
 - Edit a description of the fixed access point in the **Description:** field.
- 4 Click **OK** to save the changes and close the dialog.



To edit the HTTP Notification Server settings:

- 5 Turn rate limiting off by unchecking the **Use Packet Rate Limit** checkbox.
- 6 Enter a new value in the **# of Packets:** field.
- 7 Enter a new value in the **Time Period:** field.



- 8 Click **OK** to save the changes and close the Advanced Access List dialog.
- 9 Save the changes to the Sentriant NG by clicking the **Configure Changes** icon.

Switch Information

When a Sentriant NG appliance is added into a network environment, the switch managing the VLANs that are to be protected must be added to the Sentriant NG configuration to allow communication between the Sentriant and the switch.

From the Switch Panel, you can perform the following:

- [Add Switches](#)
- [Test the Switch Connection](#)

Adding Switches

Before a Sentriant NG appliance connected to Extreme switch gear can begin to monitor, detect and mitigate threats on network segments, the switch must be added to the Sentriant NG Manager and then the appliance's physical Port(s) must be assigned to the switch.

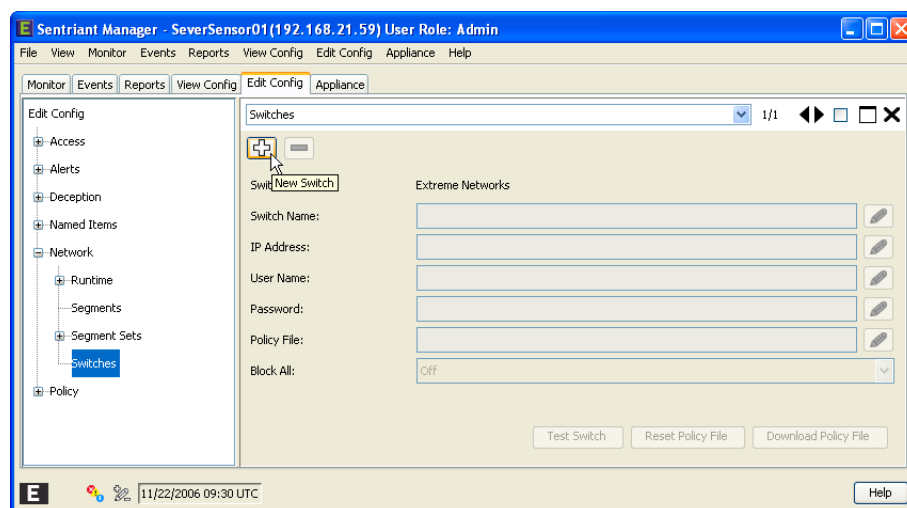


NOTE

A maximum of two (2) switches can be added per Sentriant NG appliance.

To Add Switch Information:

- 1 From **Edit Config > Network**, select **Switch**.
- 2 Click the **New Switch** button.



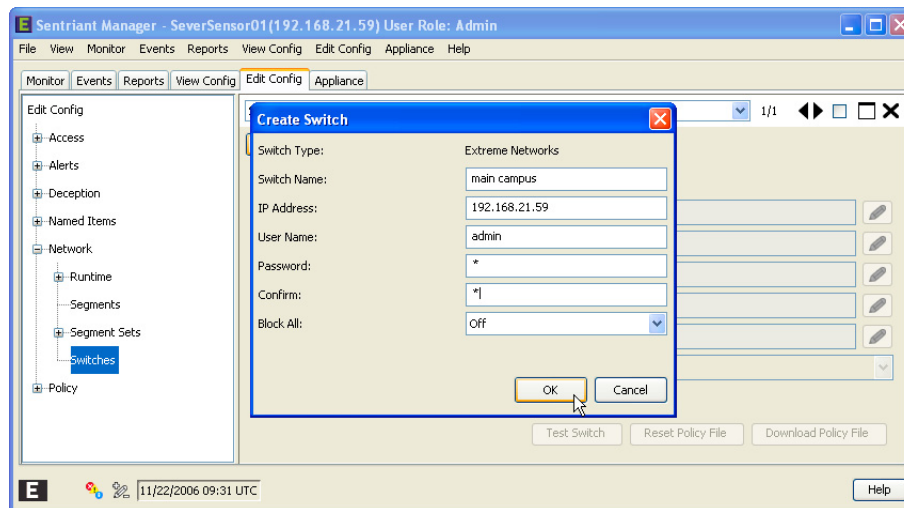
- 3 Enter the switch information.



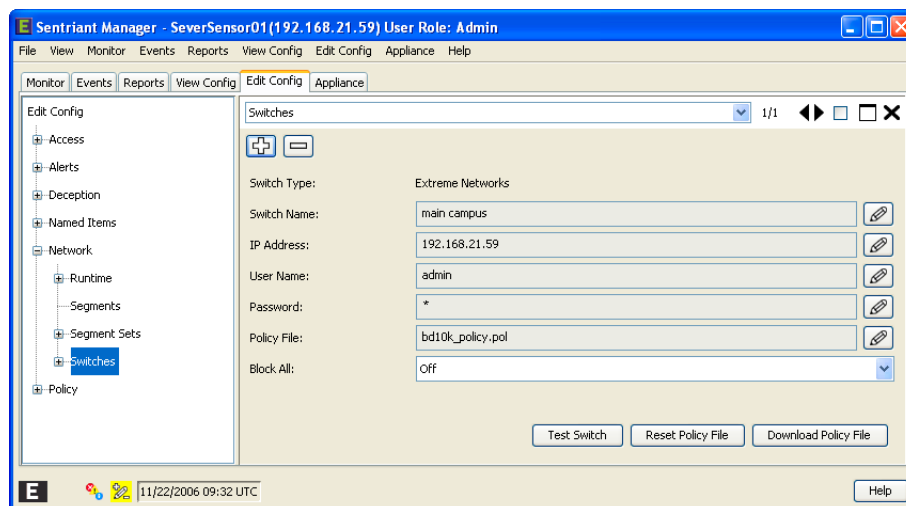
NOTE

Setting the Block All option to On will block threat producing IP Addresses on all VLANs.

- 4 Click **OK**.



The switch is added.



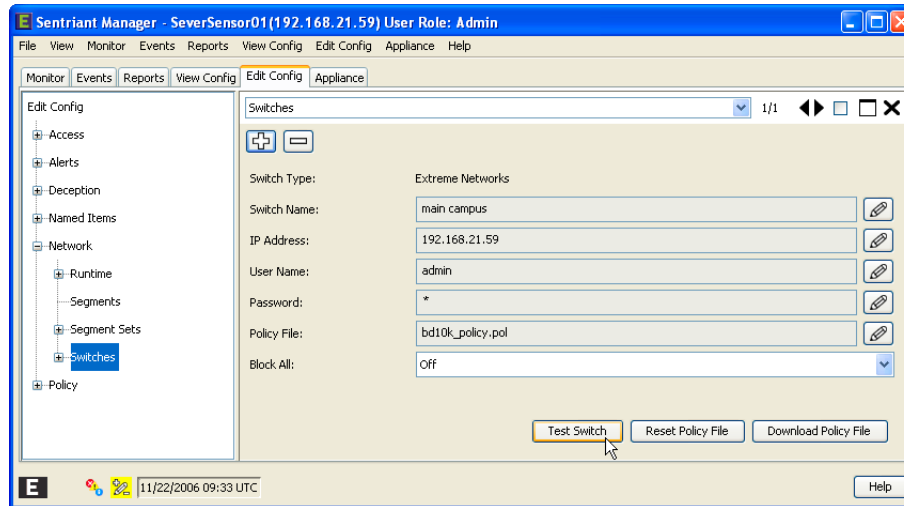
NOTE

Clicking OK adds the new switch to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#).

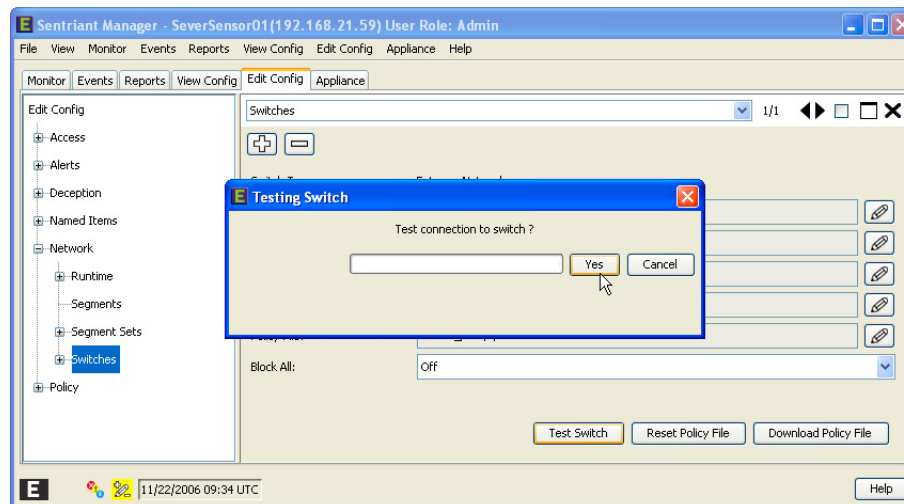
Testing the Switch

Once the switch has been added, connectivity from the Sentriant NG appliance to the switch can be tested.

- 1 Select a switch from the left navigation tree.
- 2 Click the **Test Switch** button.

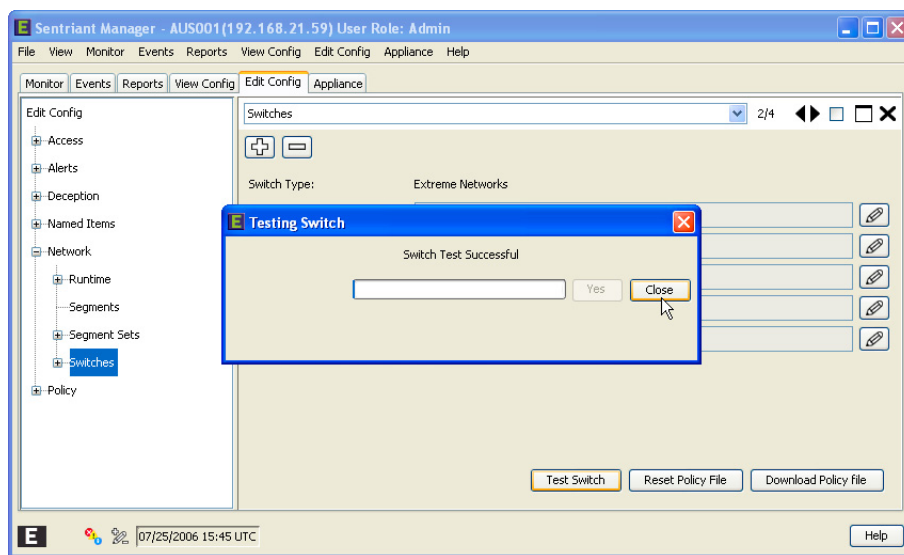


3 Click **Yes** to start the test.



If the switch has been configured correctly, a message stating the switch test was successful. If the test failed, an error message will be displayed.

4 Click **Close** to close the dialog and return to Sentriant NG Manager.



Policy

The Sentriant NG appliance provides a rules-based engine to detect behavioral patterns that do not reflect normal network traffic. Typically, rules are created and then added to a Rule Set and the Rule Set is assigned to a Segment Set.

Creating a rule is a twofold process: defining the type of rule (i.e., host, Port, traffic) and then setting rule detection and response parameters.

A Rule Set is a collection of rules configured specifically for the type of network segments to be monitored. Rule Sets are assigned to Segment Sets that are monitored by the Sentriant NG appliance.

When a Rule Set is added to a Segment Set it affects all IP Addresses within the Segment Set's range. However, the administrator can exclude a specific IP Addresses and/or ranges of IP Addresses by adding the addresses to the Policy Panel found under **Configure > Segment Sets > Policy** tab.

The Policy Panel contains specific information under each tab. These tabs are as follows:

- **Rules** - Create, Edit and Manage individual rules
- **Rule Sets** - Create, Edit and Manage rule sets

Rules

Rules are what drive the Detection and Response actions of the Sentriant NG appliance. Once a Segment is configured and is being monitored by the Sentriant NG appliance, Rules must be assigned before mitigation actions are in effect. There are two components to a rule:

Detection - Used to detect malicious network behavior.

Response - Action(s) taken by the Sentriant NG appliance to mitigate malicious network behavior.

A variety of rules can be defined based upon a set of predefined Rule Types. Each rule type represents a different behavioral pattern that can be detected by the Sentriant NG appliance. The rule types are:

- **Host** - Host rules trigger a threat when a source is contacting too many unique IP Addresses within a Segment.
- **Target Ports per Host** - This rule triggers a threat based upon a number of ports contacted on a Unique Target IP Address.
- **Traffic** - Traffic rules trigger a threat based on ANY traffic between a configured set of hosts.
- **Packet** - Packet rules trigger a threat upon matching the 'out-of-spec' contents of a packet.
- **Spoof** - This rule triggers a threat when it detects a Spoofed IP Address in the Segment.

Sentriant NG Manager includes 16 default rules that have been configured to detect and mitigate a broad range of threats. However, you may need to create your own rules depending on your environment. The default rules are as follows:

Bad Packet Rules - There are five (5) Bad Packet default rules which are All Flags, No Flags, SYN/FYN, URG Only, and XMAS Tree. These are Packet Match type rules that apply to IP packets that violate specifications for TCP flag combinations. Such packet types are often indicative of possible network reconnaissance attempts.

Mail Lookup Rule - This Packet Match type rule helps to identify hosts that are performing excessive DNS lookup requests.

Ping Flood Rule - This Traffic type rule helps to identify hosts that are performing 'ping sweeps' through a network subnet to include unused IP Addresses, indicative of possible network reconnaissance attempts.

Port Scan Rule - This Target Ports Per Host type rule helps to identify hosts that are performing Port scans for hosts within a network subnet and is indicative of possible network reconnaissance attempts.

Spoof Rule - This Spoof type rule identifies threats when it detects a Spoofed IP Address in the Segment (Note: MAC validation must be enabled for the Sentriant NG appliance for this rule to work properly.) A 'spoofed' IP Address is quite possibly one host that is masquerading as another host.

Too Many External Rule - This Hosts type rule triggers when too many external hosts (hosts inside the 'protected' space but outside the 'local' Segment) are contacted.

Too Many SMTP Comm Streams - This Target Ports Per Host type rule triggers when too many SMTP comm streams are initiated.

Too Many SMTP Hosts - This Hosts type rule triggers when too many SMTP hosts have been contacted.

Too Many Unprotected - This Hosts type rule triggers when too many unprotected hosts have been contacted.

Too Many Unused - This Hosts type rule triggers when too many 'unused' hosts (decoys) have been contacted.

Too Many Used - This Hosts type rule triggers when too many 'used' hosts (actual real hosts) are contacted.

Unused Contact - This Hosts type rule triggers upon the first contact of an unused (decoy) host.

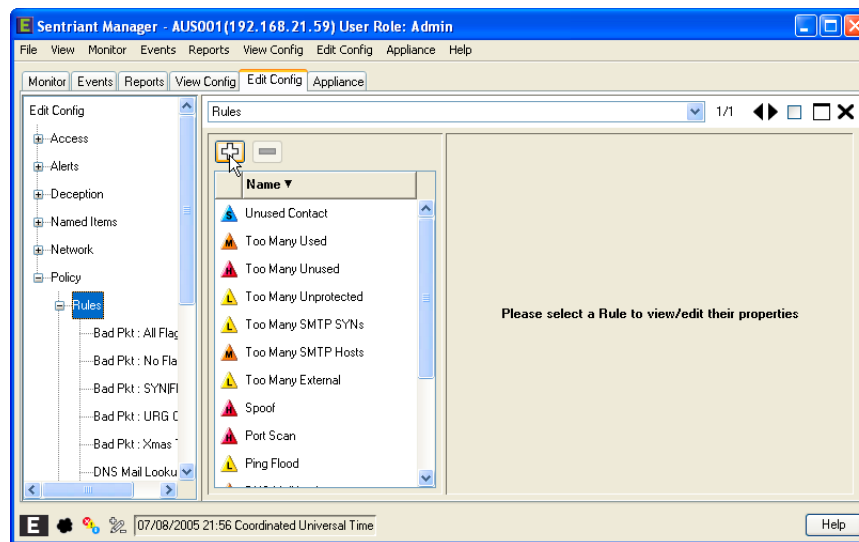
From the Rules Panel, you can:

- Create New Rules
- Delete Rules
- Edit Detection Properties
- Edit Response Properties
- Include IP Addresses
- Exclude IP Addresses

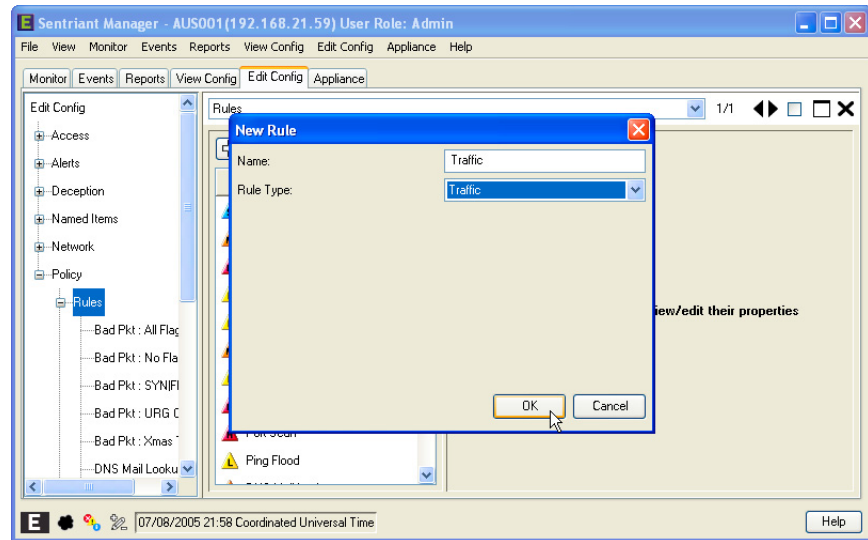
Creating a New Rule

To create a Rule:

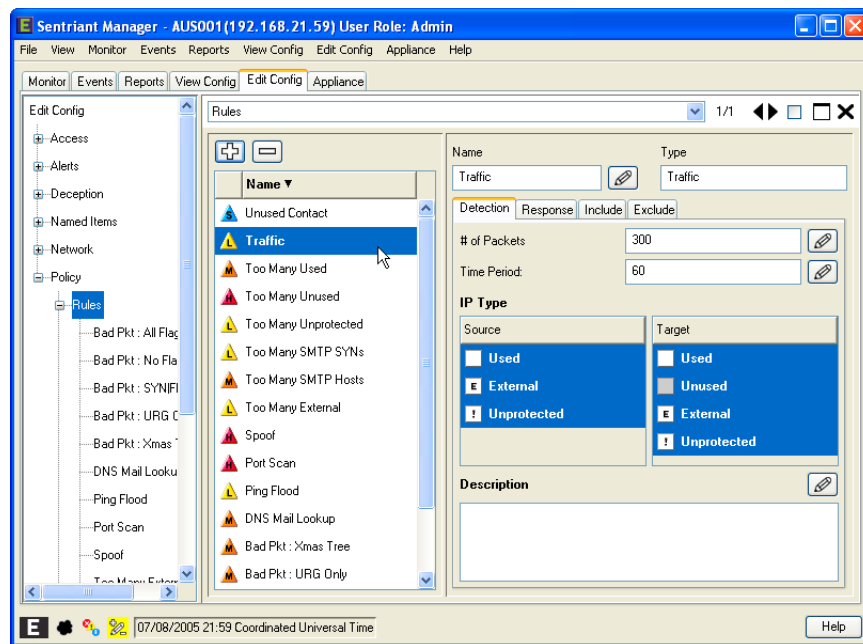
- 1 From **Edit Config > Network > Policy**, click on **Rules** in the Navigation Panel.
- 2 Click the **New Rule** button.



- 3 Type the name of the new rule in the **Name Field**.
- 4 From the **Rule Type** drop-down list, select the rule type.
- 5 Click **OK**.



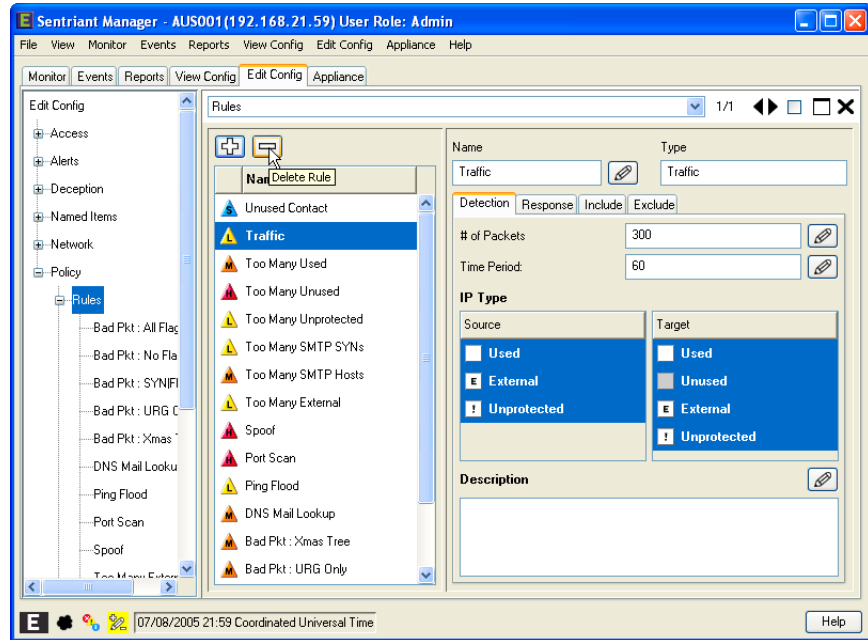
The new rule is created and displayed in the Description table.



Deleting Rules

To delete a Rule:

- 1 From **Edit Config > Network > Policy**, click on **Rules** in the Navigation Panel.
- 2 Select a rule from the list and click the **Delete** button.



The rule is deleted.

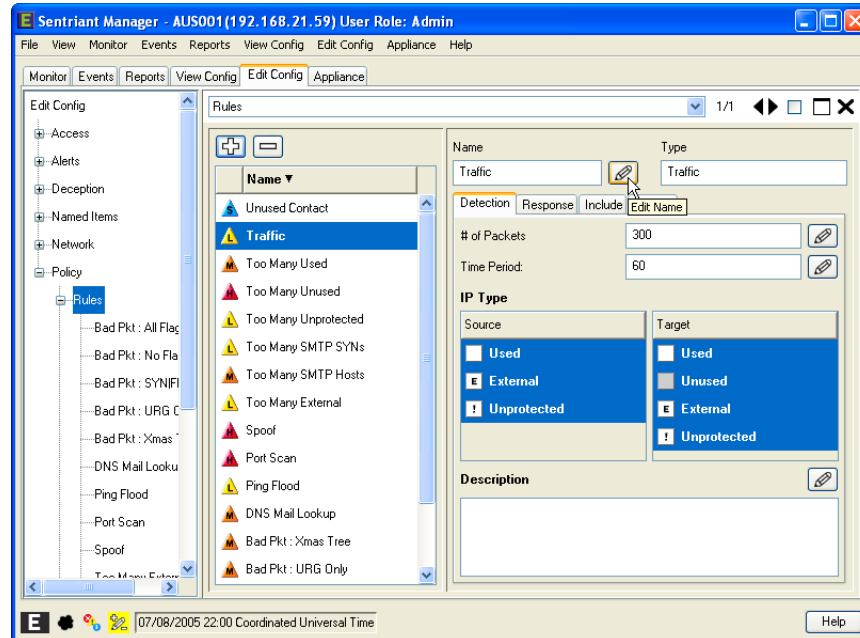
Edit Detection Properties

The detection part of rule configuration consists of the following:

- [Edit Rule Name](#)
- [Edit Number of property](#)
- [Edit Time Period](#)
- [Edit Source and Target IP Types](#)
- [Edit Rule Description](#)
- [Edit Packet Match Properties](#)
- [Edit Spoof Properties](#)

Edit Rule Name. To change the name of a rule:

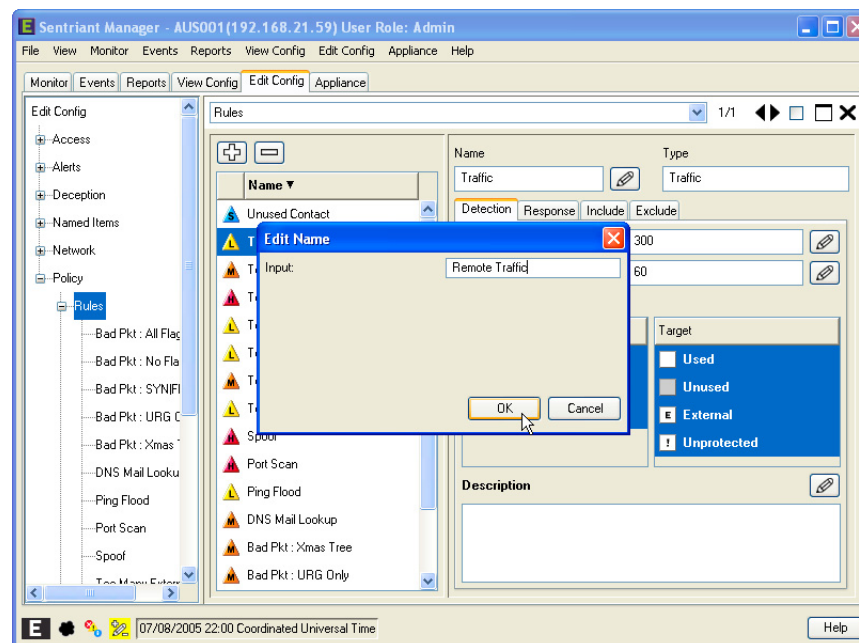
- 1 Select the rule from the Description Field.
- 2 Select the **Detection** tab.
- 3 Click the **Edit Name** button.



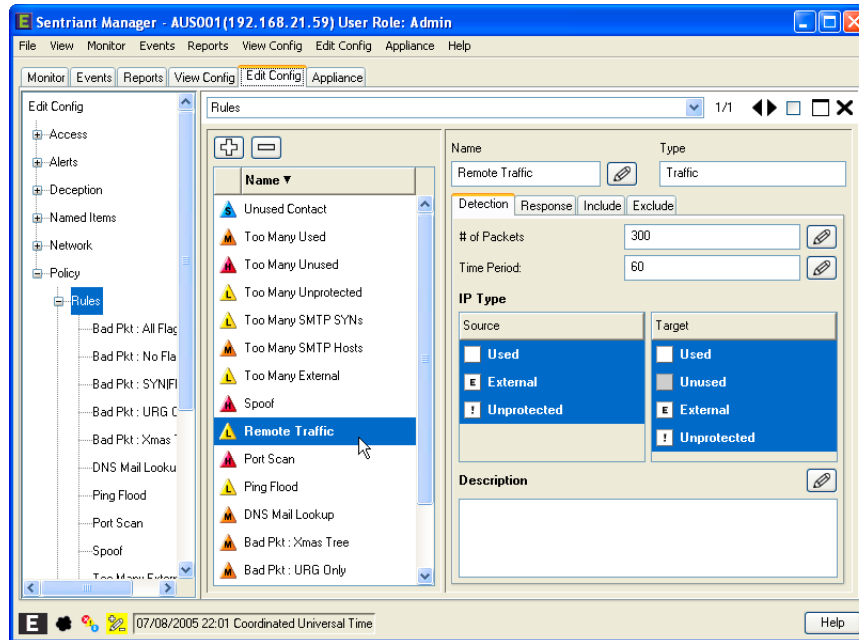
- 4 Type the name in the **Input** field of the **Edit Name** dialog and click **OK**.

NOTE

The name of the rule may only be 20 characters long.



The rule name is updated and displayed in the **Description Table** and **Name Field**.



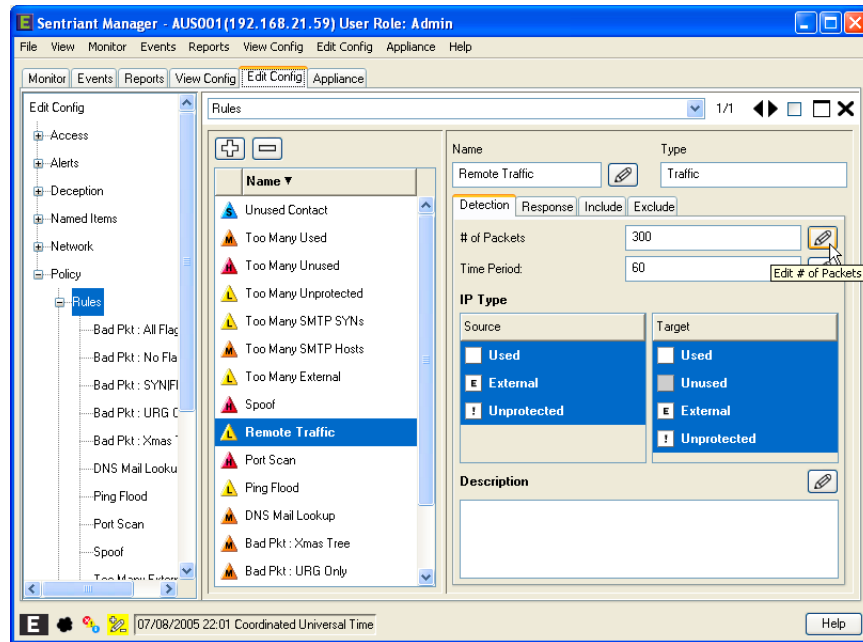
Edit “number of” Property. The “number of” property is a count of events, from a single source on the network, that when reached, triggers the rule as a threat. This property changes name based on the type of rule, but remains a count of events. The various forms of the “number of” property are:

- Number of Hosts - For host type rules - for example, a rule for too many external hits from a source outside the protected range.
- Number of Packets - For traffic, spoof and packet type rules - for example, a rule for packet match.
- Number of Ports - For Port and Port per host type rules - for example, a source hits 20 ports in the protected range.

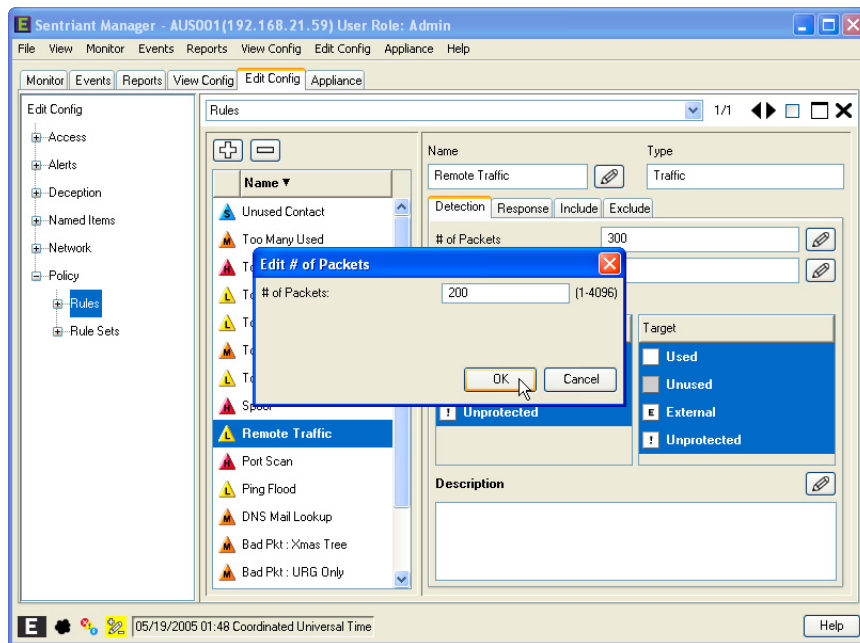
To edit “number of” property:

For this example, host type is used.

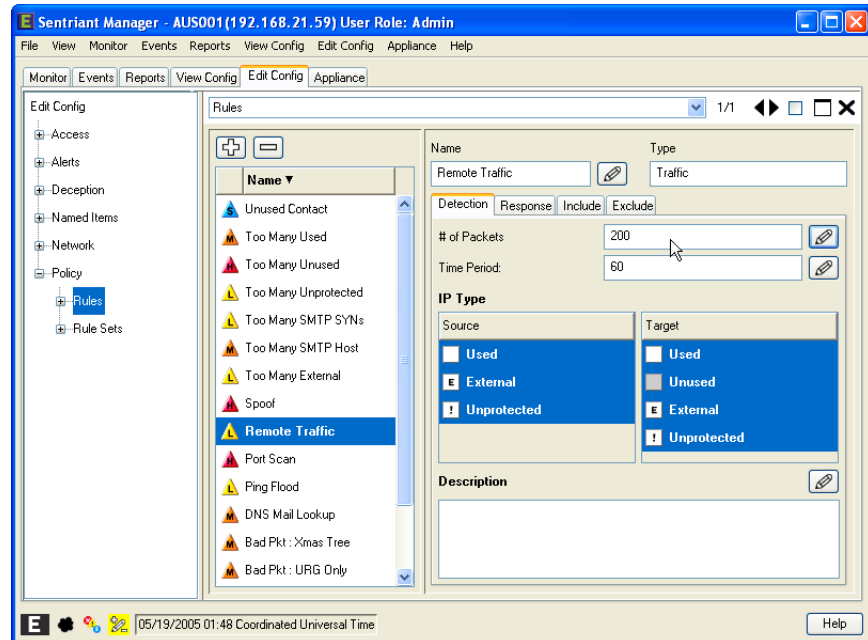
- 1 Select the rule from the Description Table.
- 2 Select the **Detection** tab.
- 3 Click the **Edit # of Host** button.



- 4 Type in a value and then click **OK**. Legal values are between 1 and 4096.



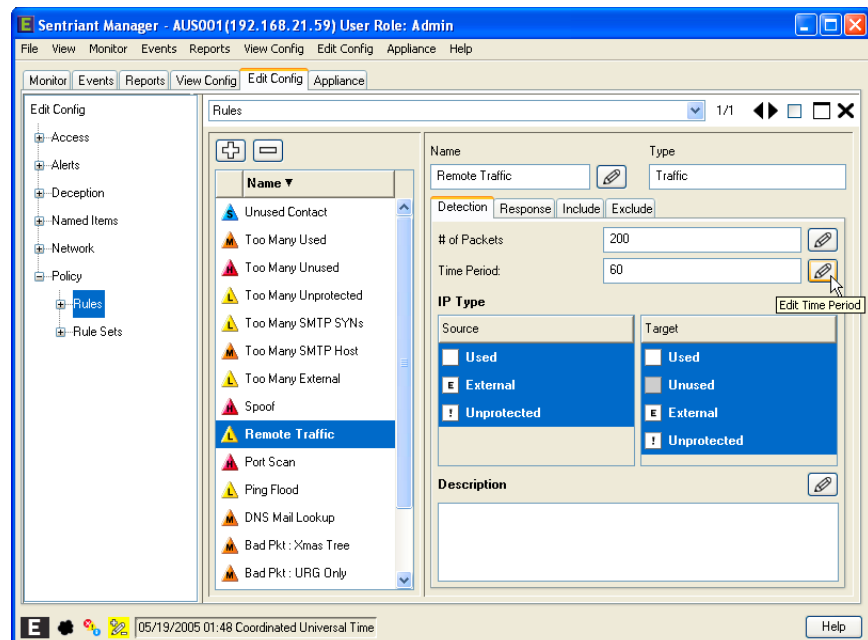
The new value is displayed.



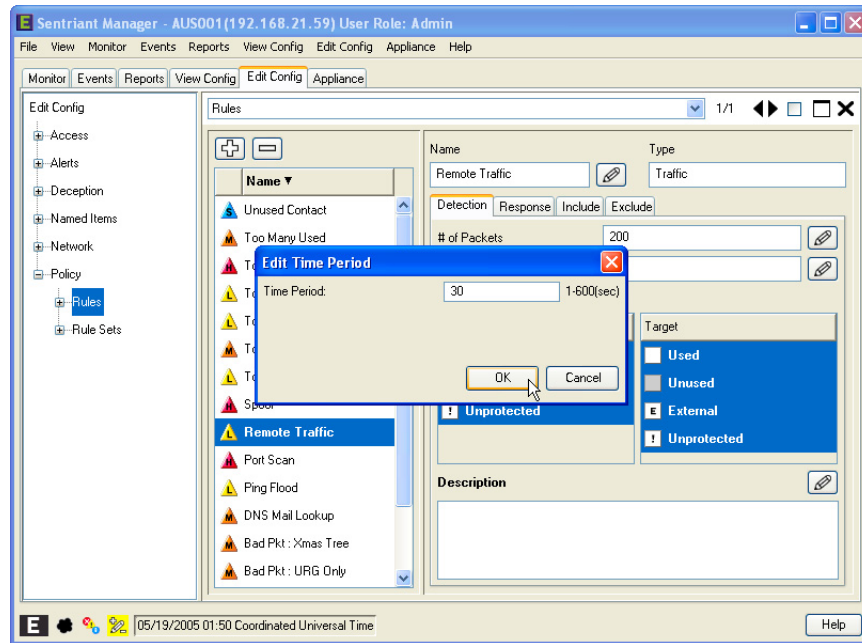
Edit Time Period. This field specifies the time that a packet count must be passed within to trigger the rule. For example, the number of hosts is set to 300 and the time period set to 30 seconds. A host count greater than 300 within 30 seconds is detected on the SentiManager NG appliance which triggers a threat.

To edit Time Period:

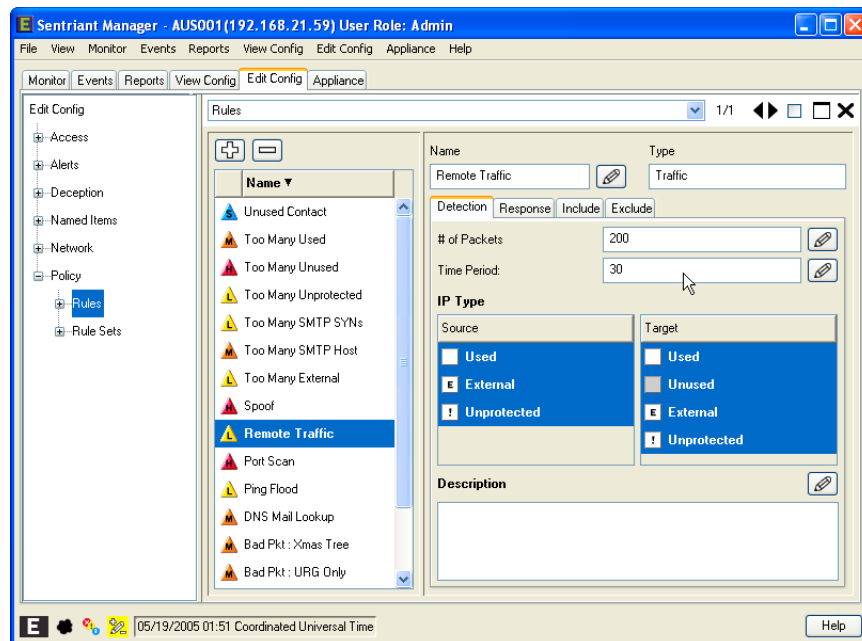
- 1 Select the rule from the **Description Table**.
- 2 Select the **Detection** tab.
- 3 Click on the **Edit Time Period** button.



- 4 Type in a value and then click **OK**. Legal values are from 1 to 600 seconds.



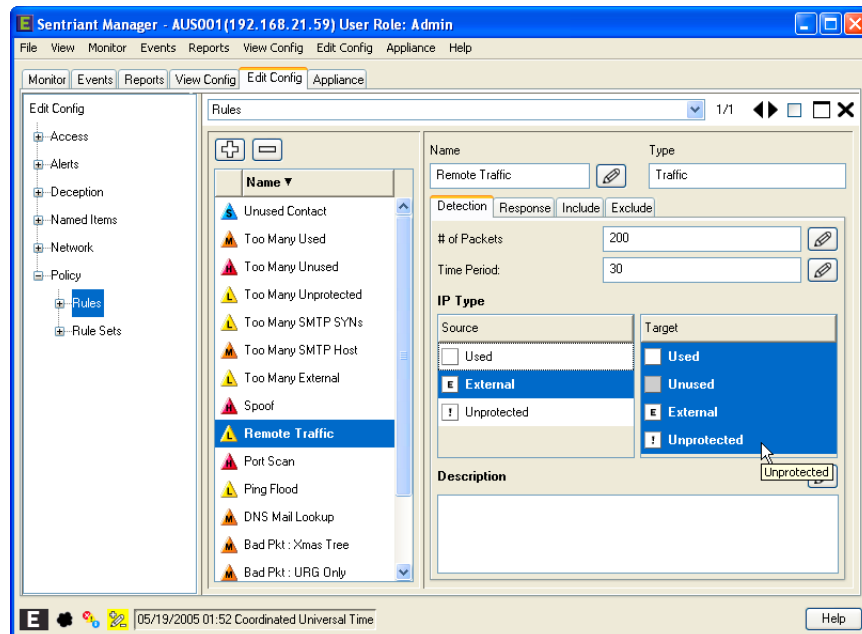
The new value is displayed.



Edit Source and Target IP Types. This field sets the IP type or identity of the source and target when a threat triggers the rule. For example, a source IP type is set to External and the target IP type is set to All. A threat is generated from an external source that triggers the rule.

To set the Source and Target Types:

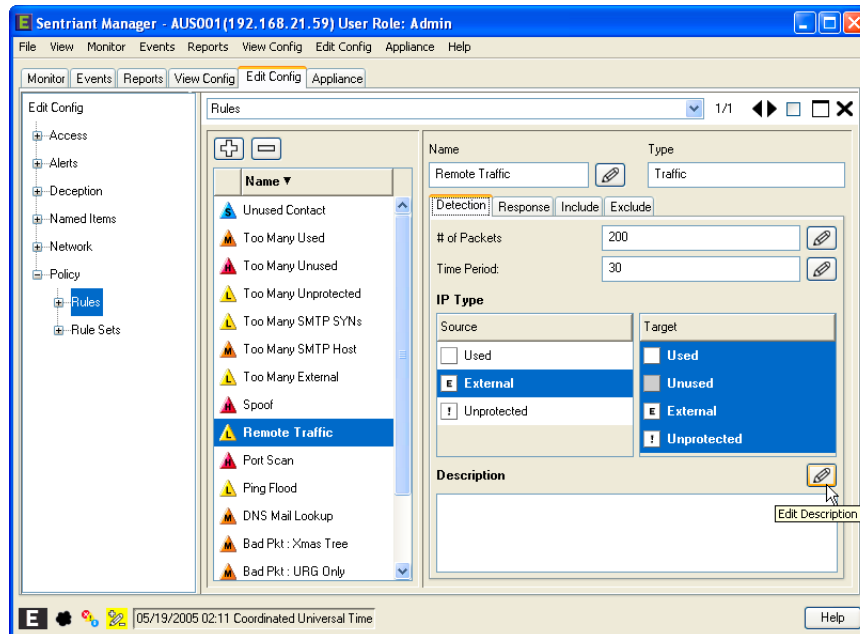
- 1 Select the rule from the Description Table.
- 2 Select the **Detection** tab.
- 3 On the left of the view, select a **Source Type(s)** from the list.
- 4 On the right of the view, select **Target Type(s)** from the list.



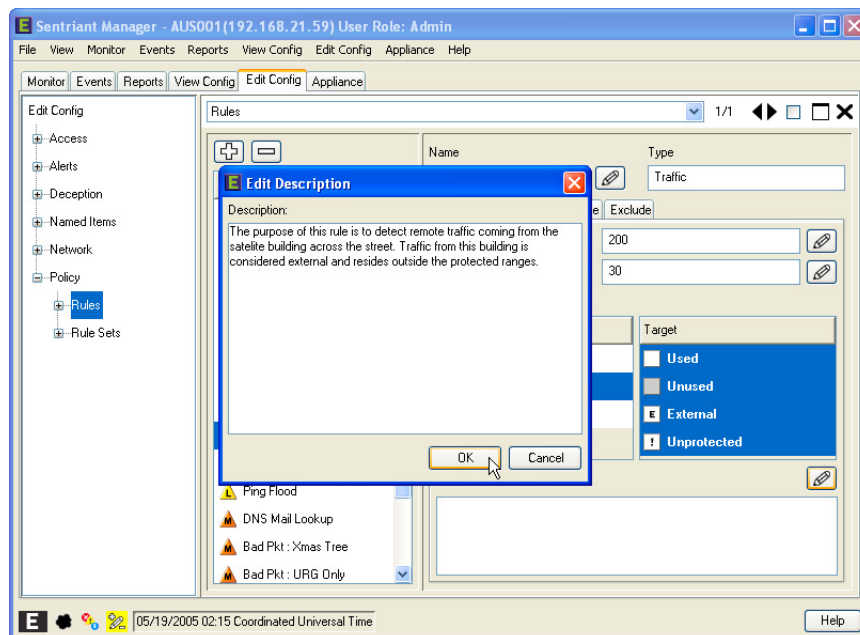
Edit Rule Description. The Rule Description field is used to record and describe the making of a rule. When describing a rule, you should be specific about what makes up the rule (detection) and the results if the rule has been triggered (response).

To add a description to a rule:

- 1 Select the rule from the Description Table.
- 2 Select the **Detection** tab.
- 3 Click the **Edit Description** button located at the bottom right of the panel.



- 4 Type a description for the rule.
- 5 Click OK.

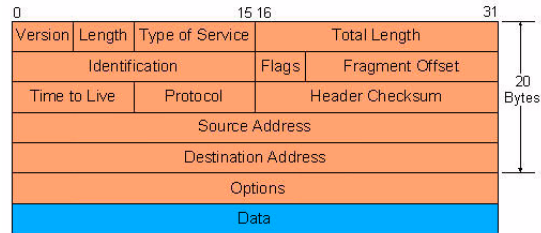


The description is added to the rule.

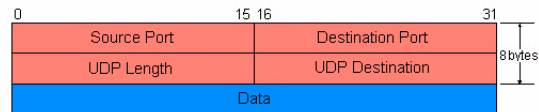
Edit Packet Match Property. When you create a Packet Rule Type, the Packet Match Tab is enabled. The Packet Match Tab is where Packet Content is configured. Using this feature, you can add the Packet Contents that mark packets as threats. A Packet Content row describes a match for a contiguous section of the packet. To match several contiguous sections, the user must enter multiple Packet Content rows. For example, the TCP SYN|FIN rule specifies three Packet Content rows. One to call out IP packet (in

the Frame header), one to call out TCP Packet (in the IP header) and the other to specify the SYN|FIN flags in the TCP Flags field. An example of each header is displayed below:

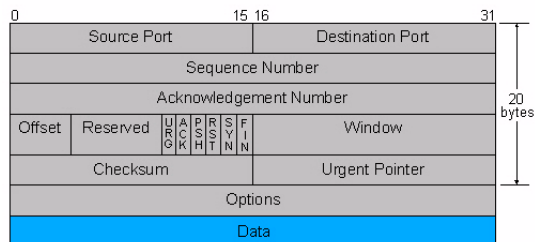
IP Header



UDP Header



TCP Header



NOTE

Understanding the details of a packet is critical when adding Packet Content threat values. These values are in hexadecimal input and erroneous results will occur if not configured properly.

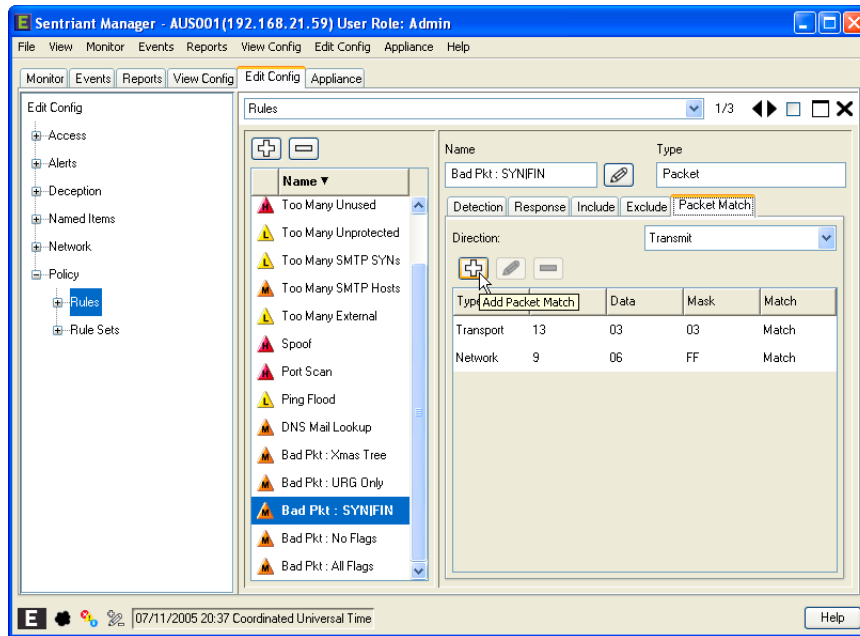
To set Packet Contents:



NOTE

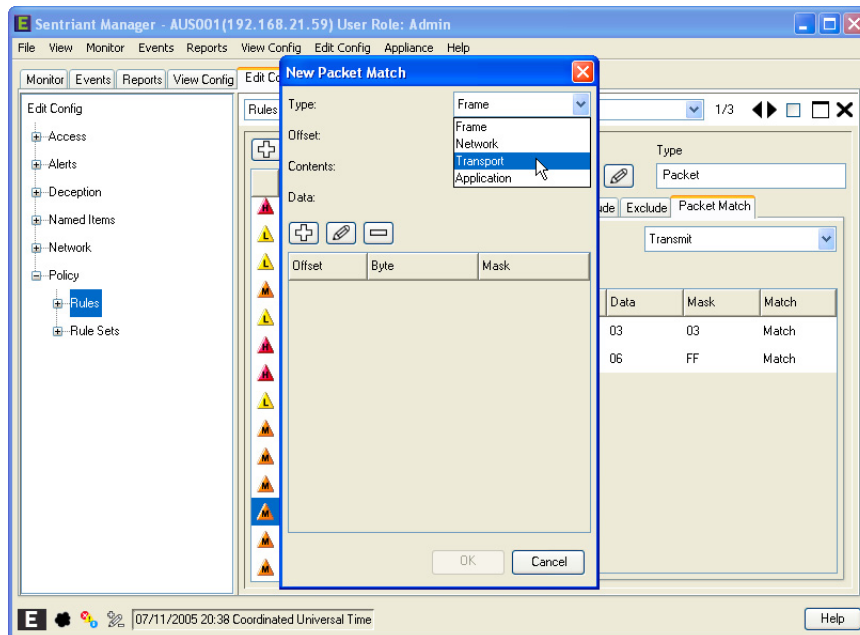
The TCP Header will be used as reference on how to set Packet Content.

- 1 Select a Packet type rule for the Description list.
- 2 Click the **Packet Match** Tab.
- 3 Click the **Add Packet Match** button to open the Packet Match dialog.

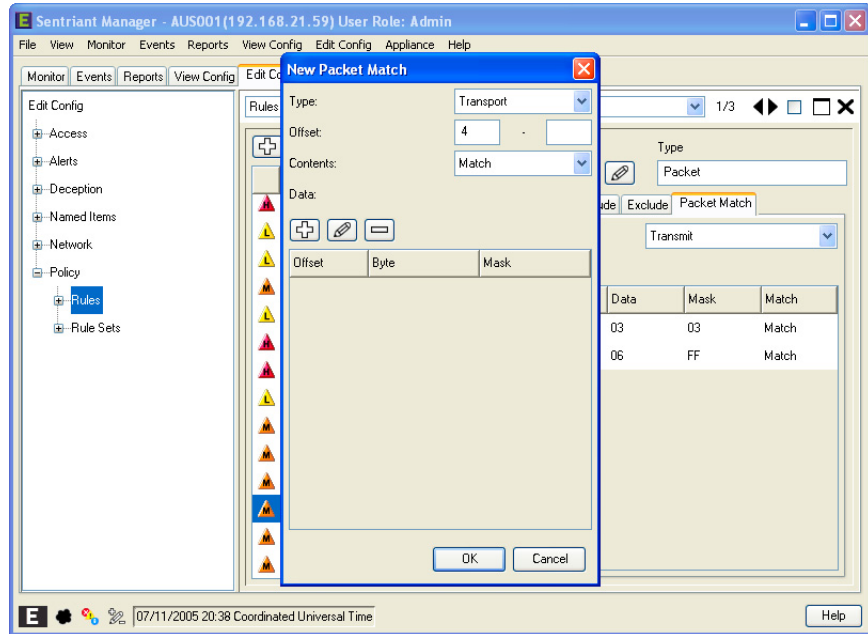


Select the communication layer that the packet match will be in.

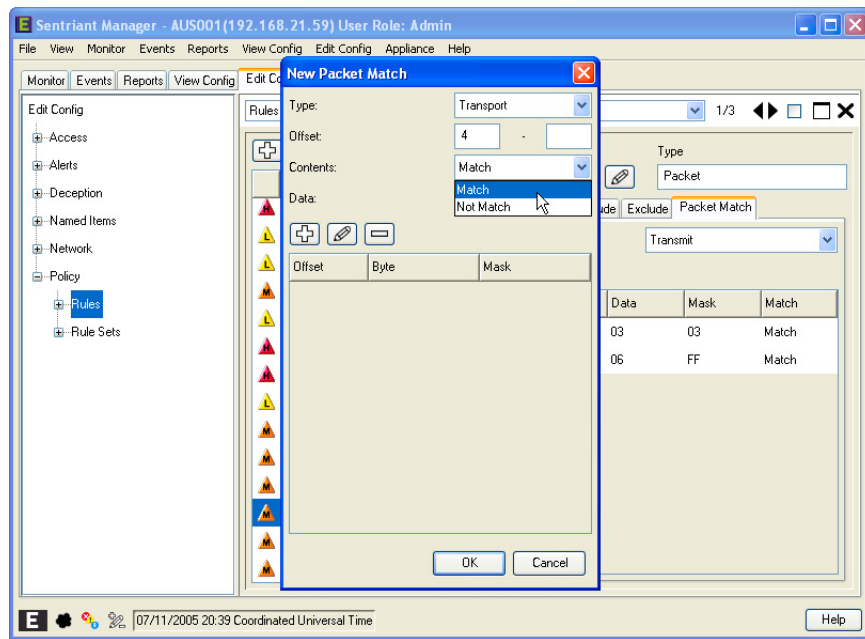
- 4 From the Type drop-down list, select **Transport**.



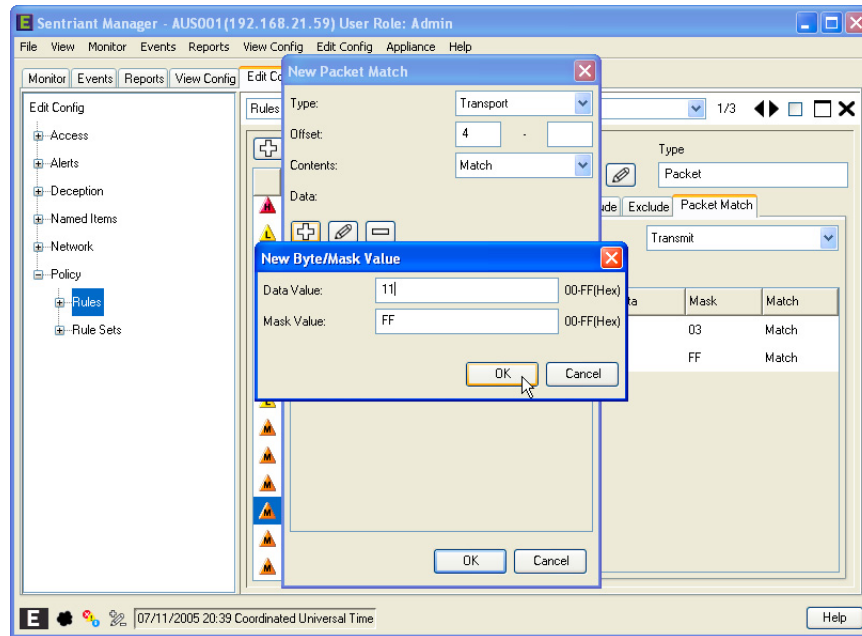
- 5 Enter a value for the offset. This value is based on the byte within the header in hexadecimal.



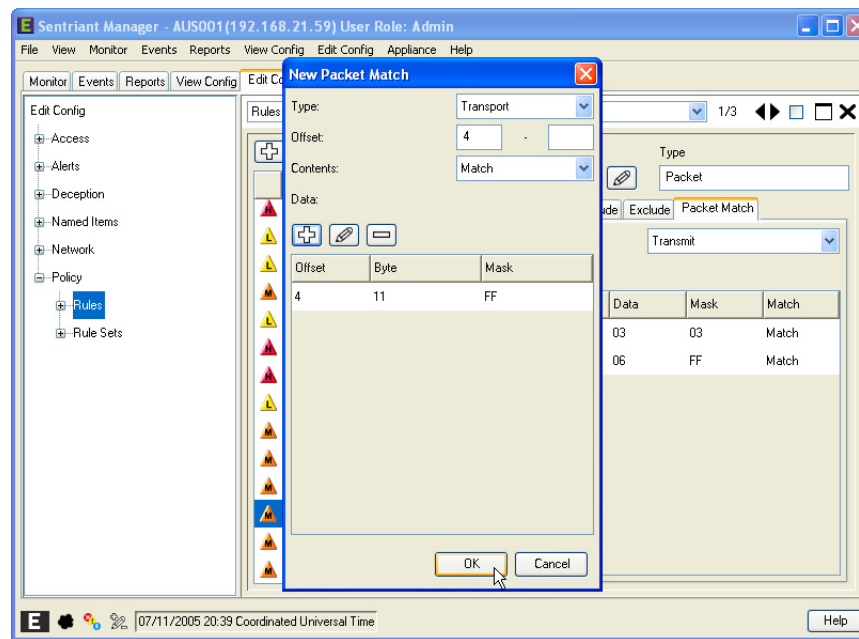
- 6 From the Contents drop-down list. Select either to Match or Not Match the parameters of the header file.



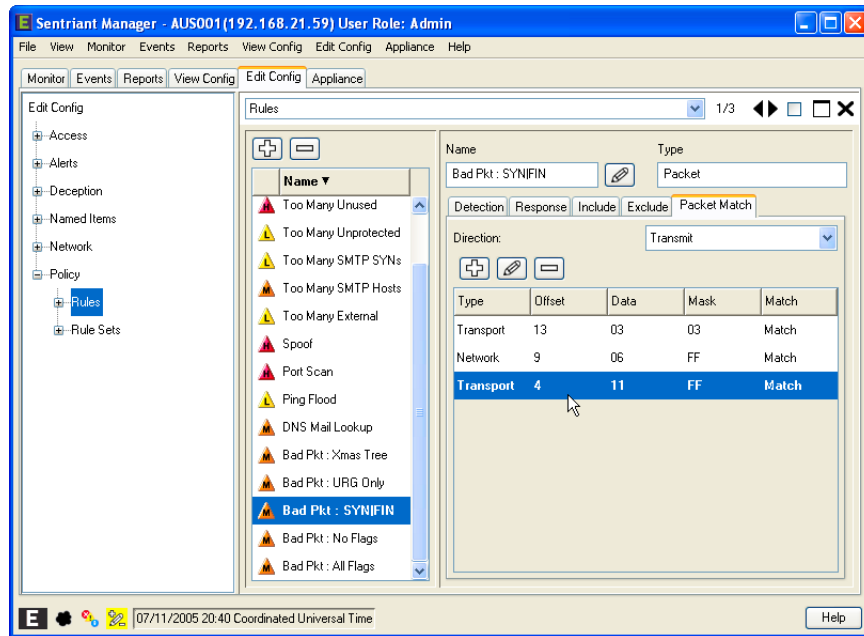
- 7 Click the **New Byte** button to bring up the **New Byte Dialog**. This allows the user to enter a byte stream that defines the data that needs to be matched and Masked. It will be of variable length, but it will have to be contiguous.
- 8 Enter hexadecimal values for each.
- 9 Click **OK**.



10 Click **OK** to save the new Packet Match.

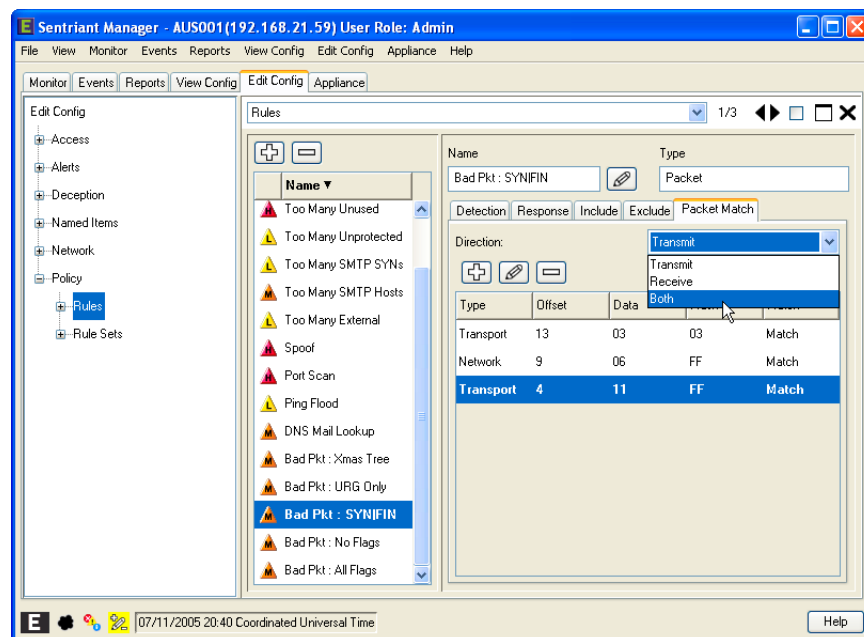


The new Packet Match is displayed.



Select the direction for the packet match. For example if you want to test for packets coming from a source, select Receive.

11 From the **Direction** drop-down list, select the direction.



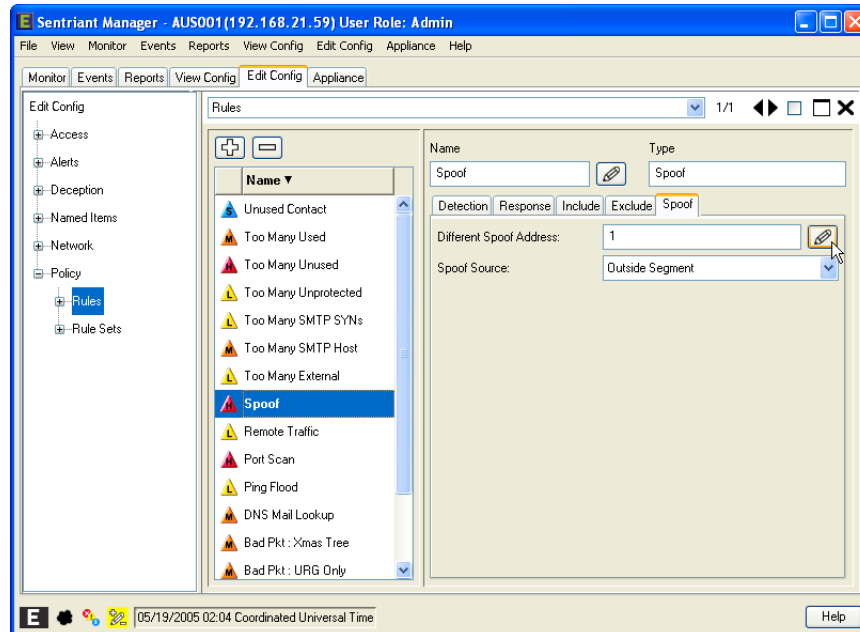
Edit Spoof Properties. This Field determines when a Spoof type rule is triggered depending on the Spoofed As Count value. For example, in the case of multi-homed sources where two IP Addresses are assigned to one work station, the Spoof As Count would be set to 2 therefore not causing the rule to trigger until a third Spoof IP Address is encountered. If users are concerned about both, they should create a Rule that detects with Spoofed As Count set to 1 and set the Rule Priority to Suspect. Then

create another Rule with at least 2 Spoofed As Counts, and make that a Threat priority type (low, medium, high).

Spoof As Count

To set the Spoof As Count:

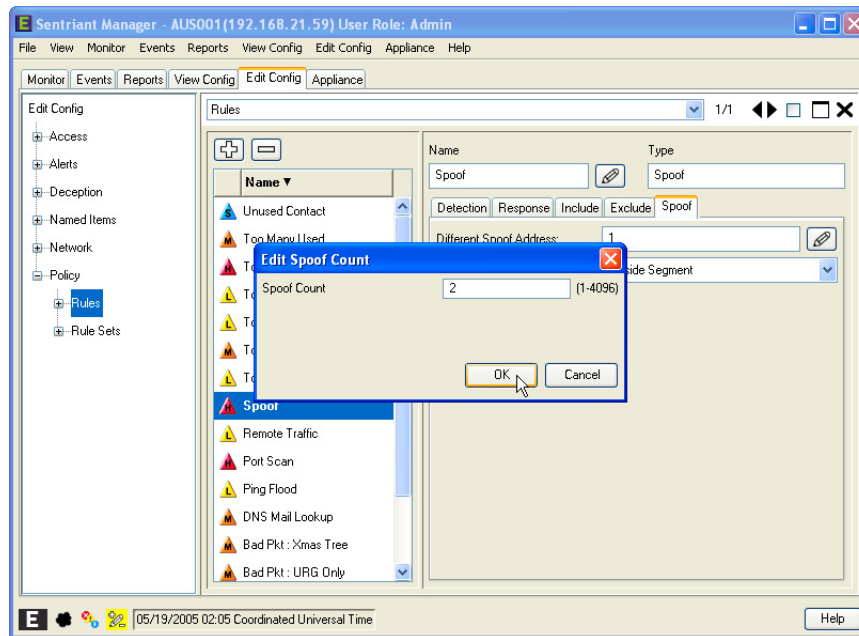
- 1 Select a Spoof type rule from the Description list.
- 2 Click on the **Spoof** tab.
- 3 Click the **Edit** button.



NOTE

The default Spoof As Count value is set to one.

- 4 Enter a value for the Spoof As Count. Legal values are from 1 to 4096.
- 5 Click **OK**.



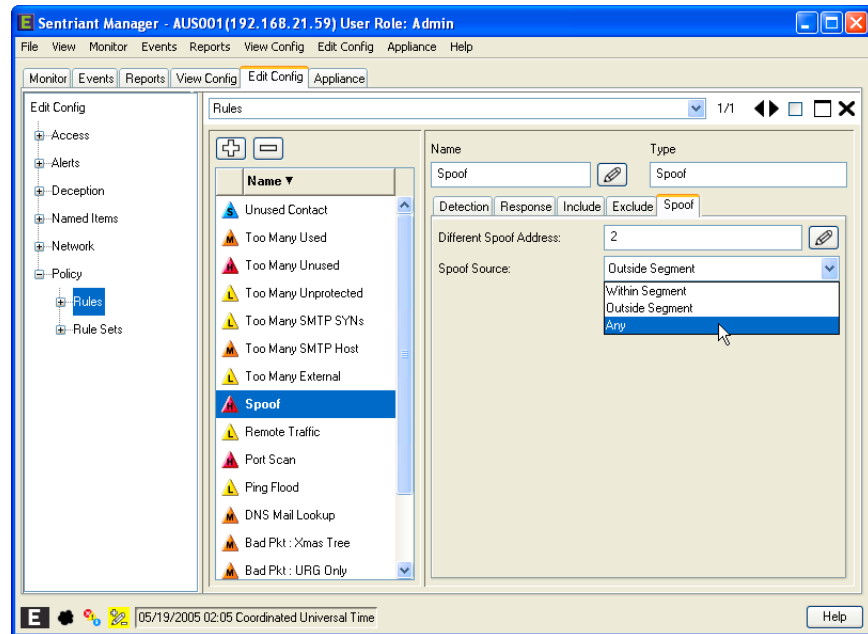
The new Spoofer As Count value is updated.

Edit Spoofer Rules Source Type

This field sets the type or identity of a source's location when a threat triggers the rule. For example, a source type is set to External. A threat is generated from an external source that triggers the rule.

To set the Source Type:

- 1 Select a Spoofer type rule from the Description list.
- 2 Select the **Spoofer** tab.
- 3 Select a **Source Type** from the drop-down list.

**NOTE**

Invalid gateway IP Addresses that do not represent a real host will cause spool detection to be disabled. All gateways must respond to ARP communication.

Edit Response Properties

The response part of rule configuration consists of the following:

- [Edit Priority](#)
- [Edit Time Out Period](#)
- [Edit Response](#)
- [Edit Response Time Out](#)
- [Edit Alerts](#)

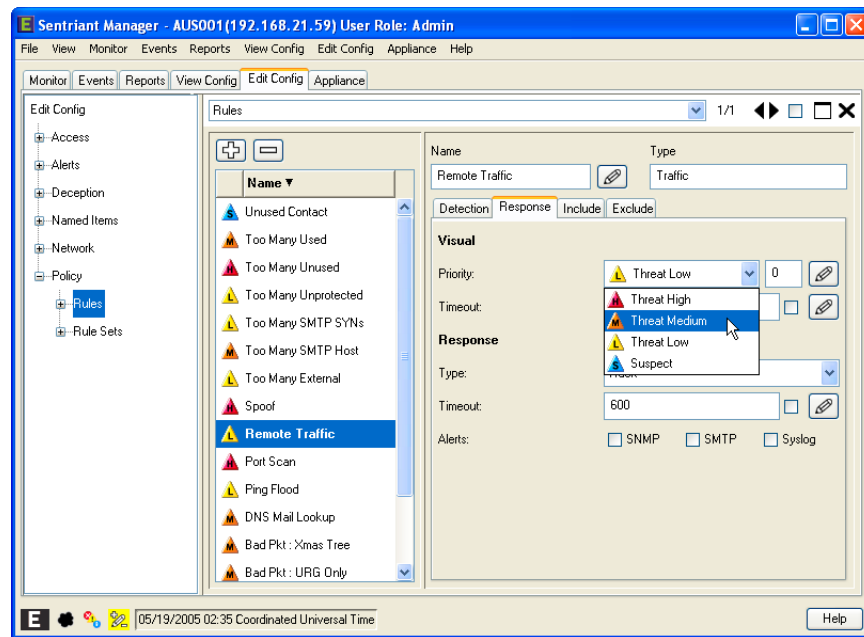
Edit Priority. This field defines the severity of a priority. Priority values are High, Medium, Low and Suspect. Suspect priority is used to determine source threats under any condition or configuration. For example, by default Too Many Unused threats will be set as Suspect.

When a source is displayed as a threat, a rank is also assigned that corresponds to the observed threat activity. The rankings for each threat type are configurable. The ranking is from 0 to 999 with 999 being the higher ranking.

When viewing a threat in the Sources page of the UI, the threat type listed for any IP Address is determined by the Rank assigned to the threats that have occurred. If two threats have occurred for a specific IP Address, only the threat with the highest rank will be displayed.

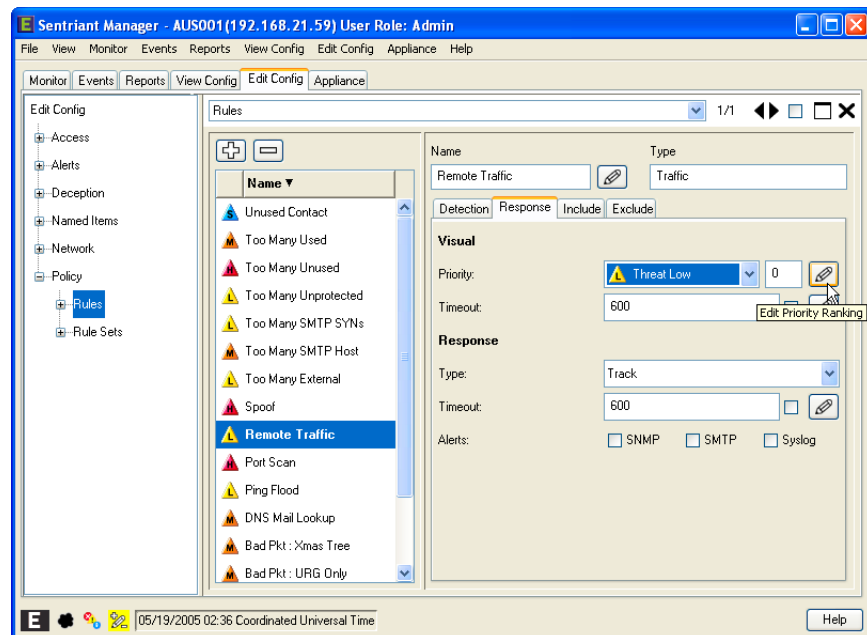
To set the Priority:

- 1 Select the rule from the **Description Table**.
- 2 Select the **Response** tab.
- 3 From the **Priority** drop-down list, select a priority.



To set the Ranking:

- 4 Click the **Edit Priority Ranking** button.

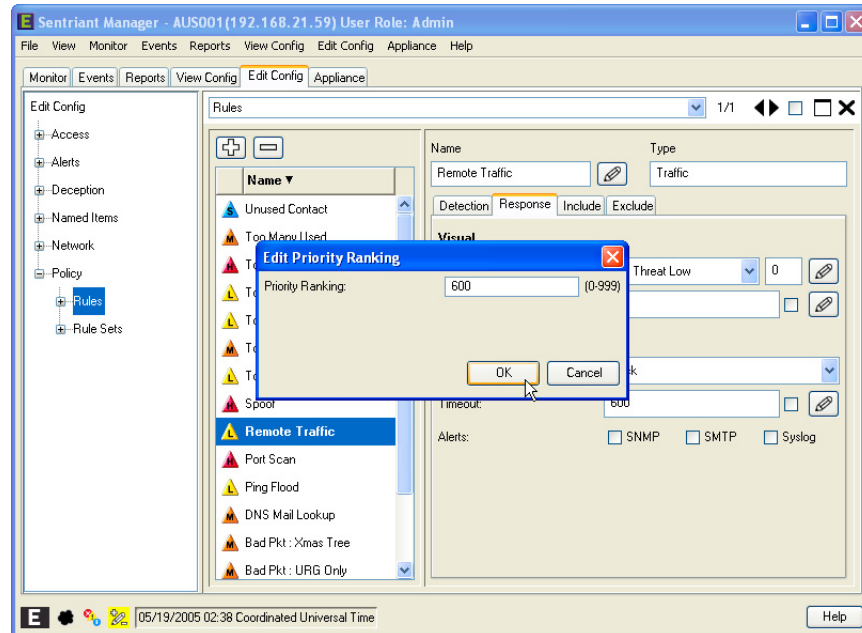


- 5 Enter a value for the ranking. Legal values are 999 to 0 with 999 being the higher priority.

**NOTE**

When viewing a threat in the Sources page of the UI, the threat type listed for any IP Address is determined by the Rank assigned to the threats that have occurred. If two threats have occurred for a specific IP Address, only the threat with the highest rank will be displayed.

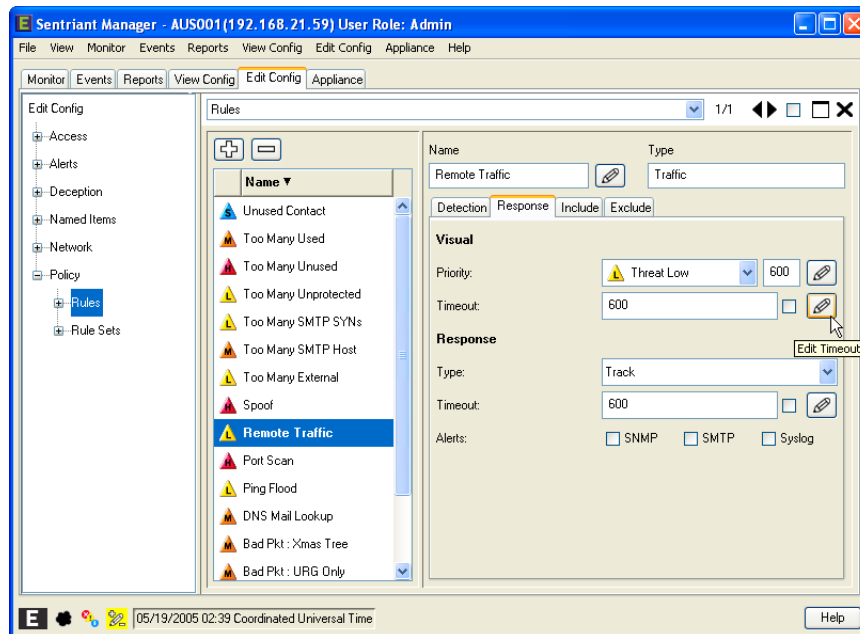
6 Click OK.



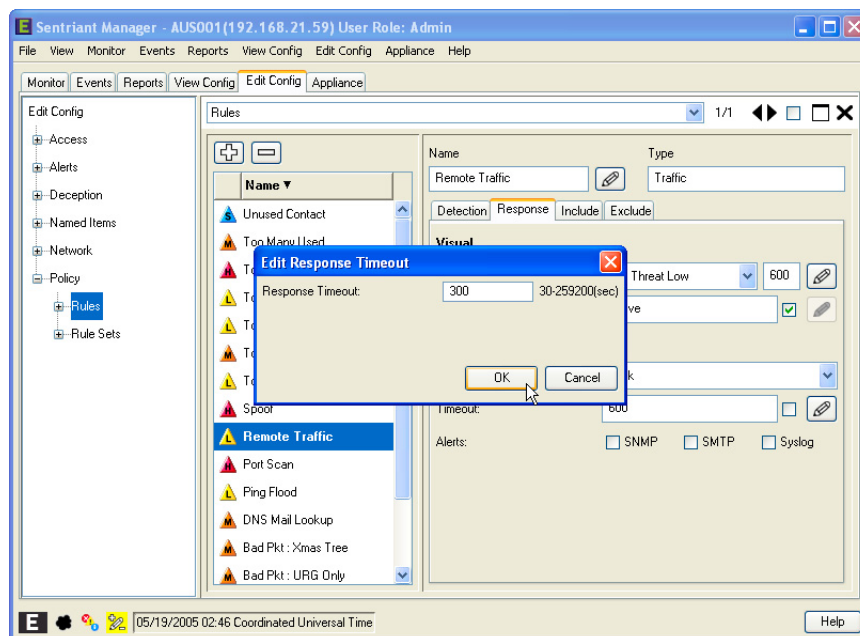
Edit Time Out Period. This field specifies how long a source should remain a threat once the rule has been triggered. If the threat recurs after the time out, the threat will be re-triggered and the time out period reset. You can set the time out period to active. When set to active the source will remain a threat and will not time out.

To edit the Time Out Period:

- 1 Select the rule from the **Description Table**.
- 2 Select the **Response** tab.
- 3 Click on the **Edit Time Out Period** button.



- 4 Type in a value and then click **OK**. Legal values are from 0 to 259200 seconds.

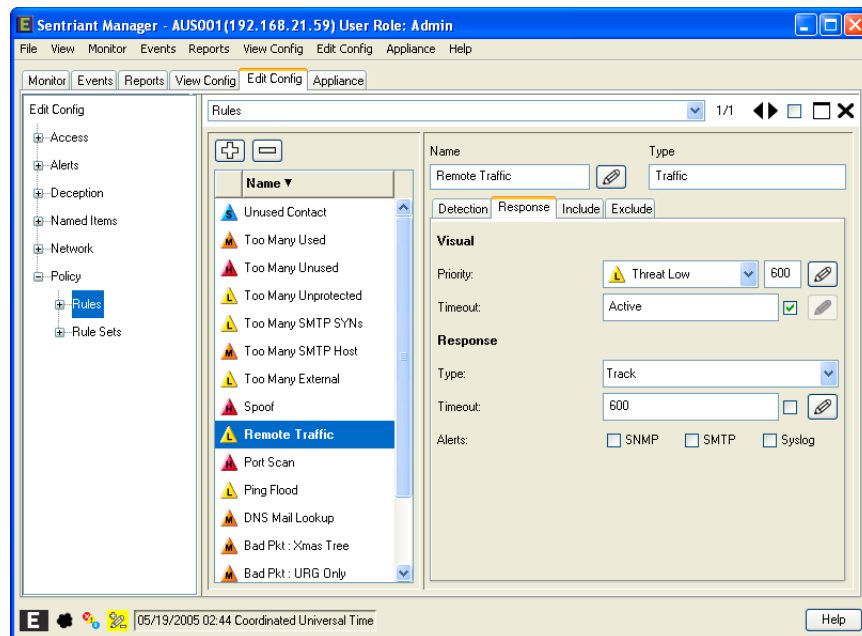


- 5 To set the time out to active, click the checkmark.



The value in the time out field updates to active. If you deselect active, the time out period will return to default value.

The new value is displayed.

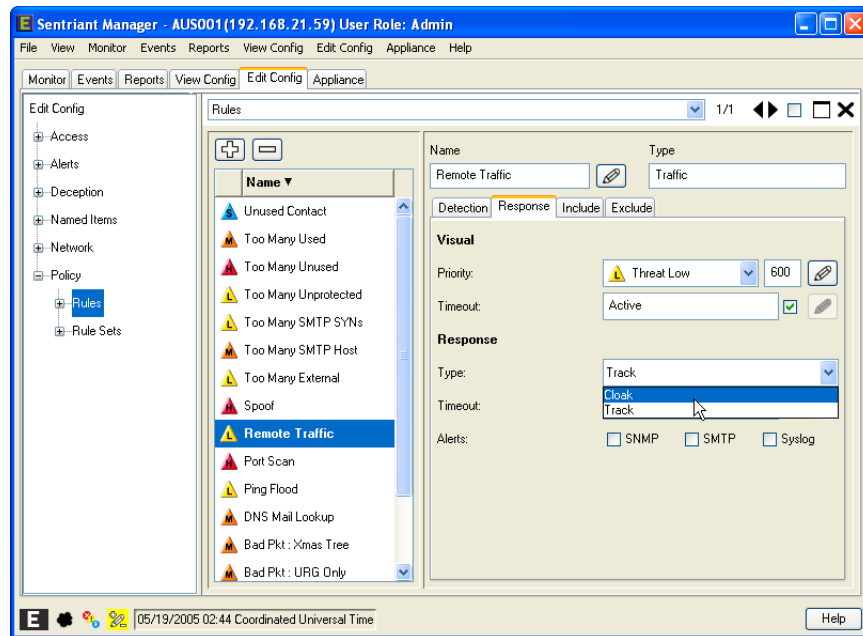


Edit Response Type. This field sets the type of response when a threat triggers the rule. For example, a source threat triggers the rule and the response is set to track. The host will track down the origin of the source and the traffic it creates on the target Segment. Response types are:

- Track - A technique that tracks the source threat throughout the monitored network.
- Cloak - A technique that unilaterally controls and terminates communications flow between two or more computers.

To set the Response Type:

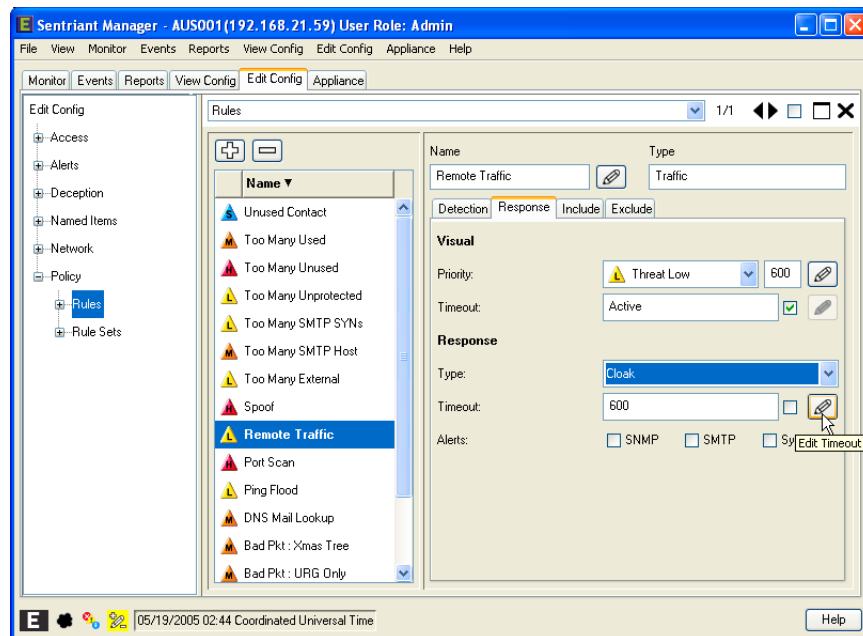
- 1 Select the rule from the **Description Table**.
- 2 Select the **Response** tab.
- 3 Select a **Response Type** from the drop-down list.



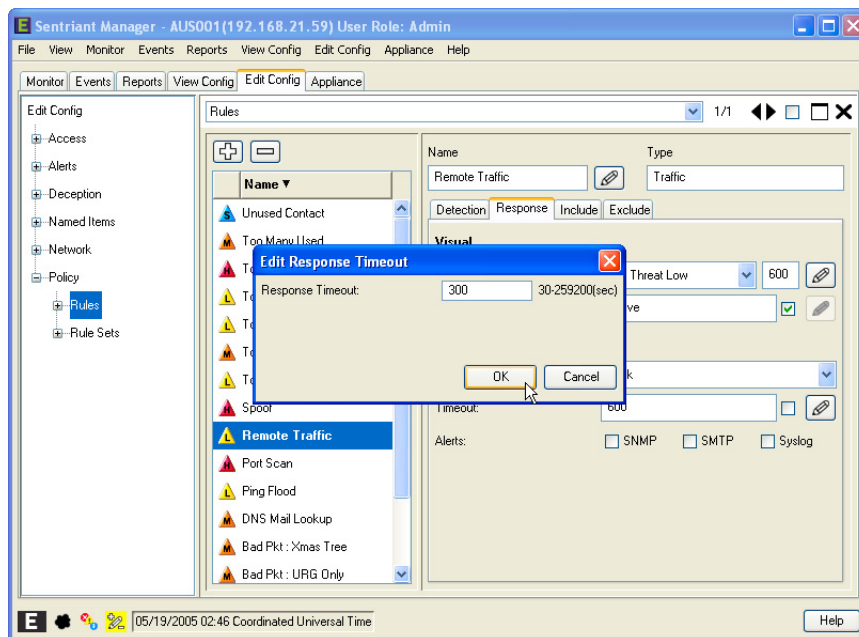
Edit Response Time Out. This field specifies how long a response type is active once the rule has been triggered. If the threat recurs after the time out, the threat will be re-triggered and the response time out reset. Note that the Response Time Out is independent of how long a source remains a threat. You can set the time out period to active. When set to active the source will remain a threat and will not time out.

To edit the Response Time Out:

- 1 Select the rule from the **Description Table**.
- 2 Select the **Response** tab.
- 3 Click on the **Edit Time Out** button.



4 Type in a value and then click **OK**.

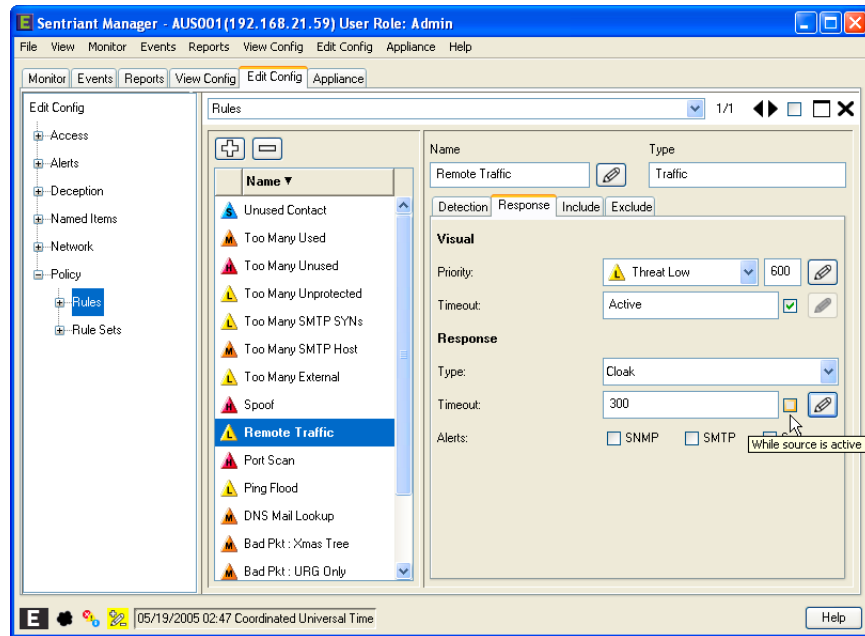


5 To set the time out to active, click the checkmark.



NOTE

The value in the time out field updates to active. If you deselect active, the time out period will return to default value.

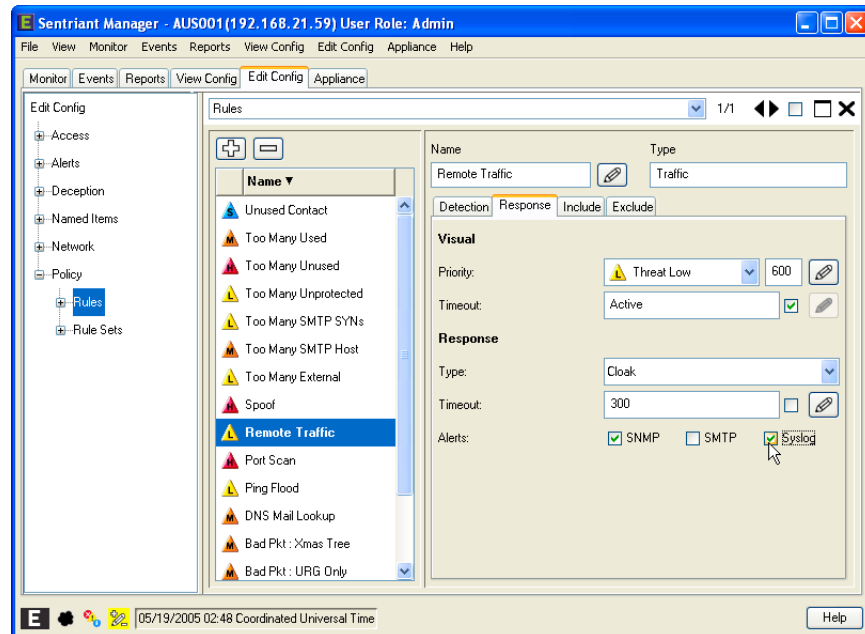


Edit Alerts. This selects the type of Alert source that will receive notification of a detected threat. The types of Alerts are:

- Email(SMTP)
- SNMP
- SysLog

To select an Alert:

- 1 Select the rule from the **Description Table**.
- 2 Select the **Response** tab.
- 3 Click on a checkbox for each type of Alert used for the rule.



Included IP Addresses

Included allows the configuration of specific IP Addresses and ports to be monitored by the Sentriant NG appliance. IP Addresses and ports are added to a rule using a session profile that sets a single or range of source and/or IP Addresses and ports. When session profiles are added to a rule, only values that are in the session profile are monitored on the source Segment. For example, if you wish to create a Too Many Protected Web Server rule where protected web server IP Addresses are 10.10.10.1 through 10.10.10.5 with one more at 10.10.10.19, then a session profile would have the following values:

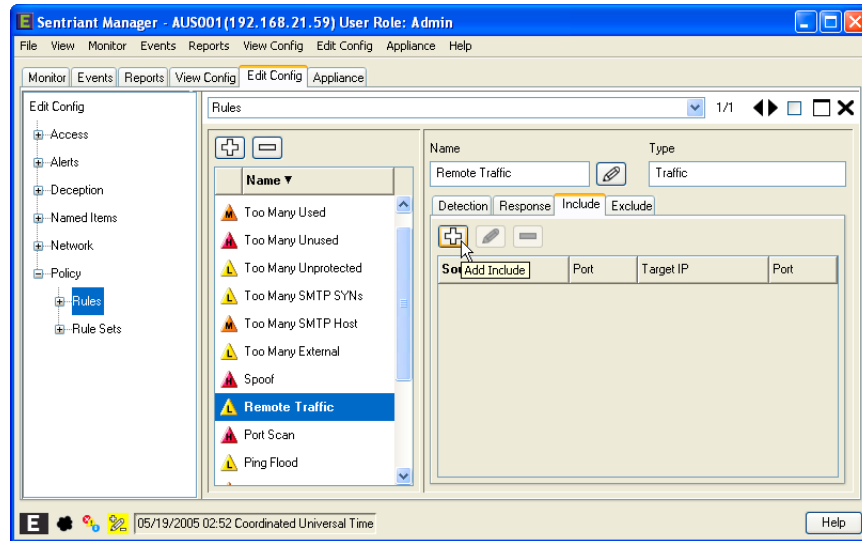
- Source IP - empty
- Source Port - empty
- Target IP - 10.10.10.1-5,19
- Target Port - empty

If you only wanted to count the threats on Port 80, then you would change the Target Port to 80.

If no session profiles are entered, then by default all traffic will be included.

To configure Included IP Addresses:

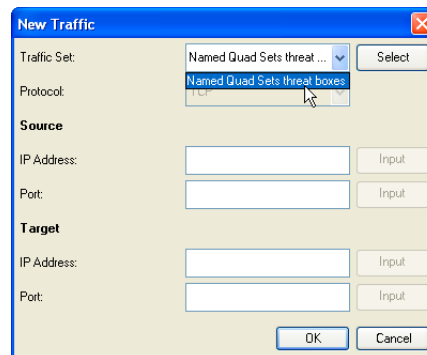
- 1 Select the rule from the **Description table**.
- 2 Select the **Include Tab**.
- 3 Click the **Add** button.



There are various methods of adding include profiles to the dialog. You may select a Traffic Set from the Named Items, enter each traffic item or use a combination of entered traffic item data and select IP and Port Sets from Named Items.

To use a Traffic Set:

- Click the **Input** button on the Traffic Set line to add a Traffic Set. The remaining traffic data items are disabled because each data item is using the Traffic Set data.



Entering data items and/or using IP and Port Sets:

- Select a Port Protocol from the drop-down list. Choices are TCP, UDP, and ICMP.
- Enter a Source IP Address by one of the two methods:
 - Type an IP Address in the Source IP Address field. The example shows an IP Address using the hyphen (-) wildcard for one of the octets which selects a range of the octet.
 - Use a IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.



NOTE

To revert back to entering an IP Address, click the **Select** button.

- Enter a Source Port Number by one of the two methods:
 - Type a Port number in the Source Port field.
 - Use a Port Set by clicking the **Input** button and then selecting an Port Set from the drop-down list.
- Enter a Target IP Address by one of the two methods:
 - Type an IP Address in the Targets IP Address field.
 - Use a IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.

**NOTE**

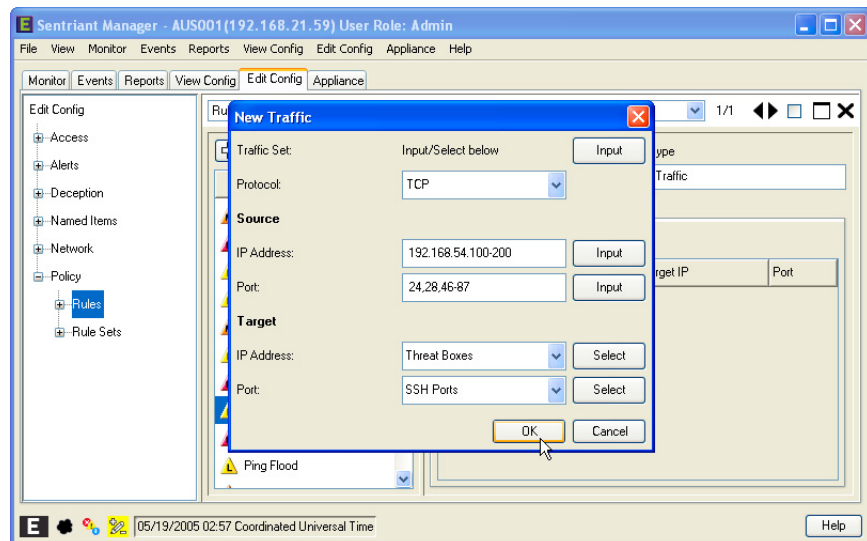
To revert back to entering an IP Address, click the Select button.

- Enter a Target Port Number by one of the two methods:
 - Type a Port number in the Target Port field.
 - Use a Port Set by clicking the **Input** button and then selecting an Port Set from the drop-down list.

- 4 Click **OK** to save the include session profile.

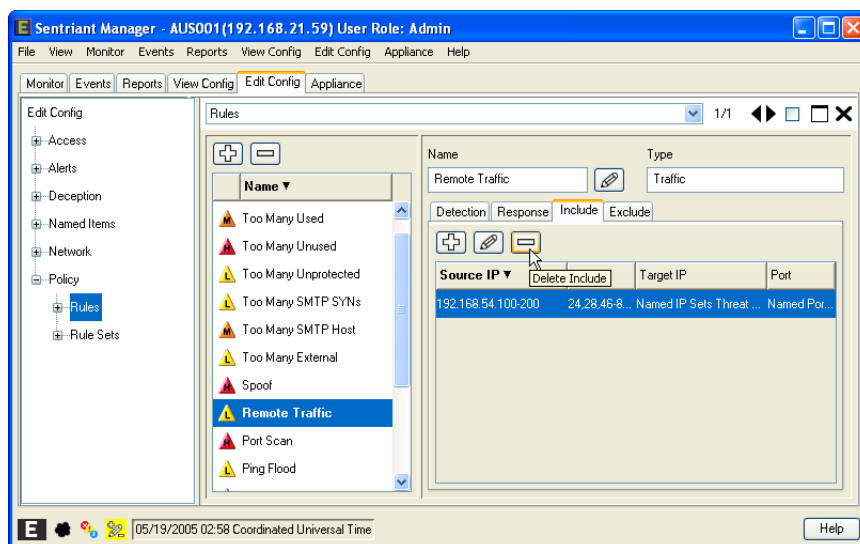
**NOTE**

Source IP Address and Port may be left blank therefore setting to the rule to monitor all traffic on the Segment.

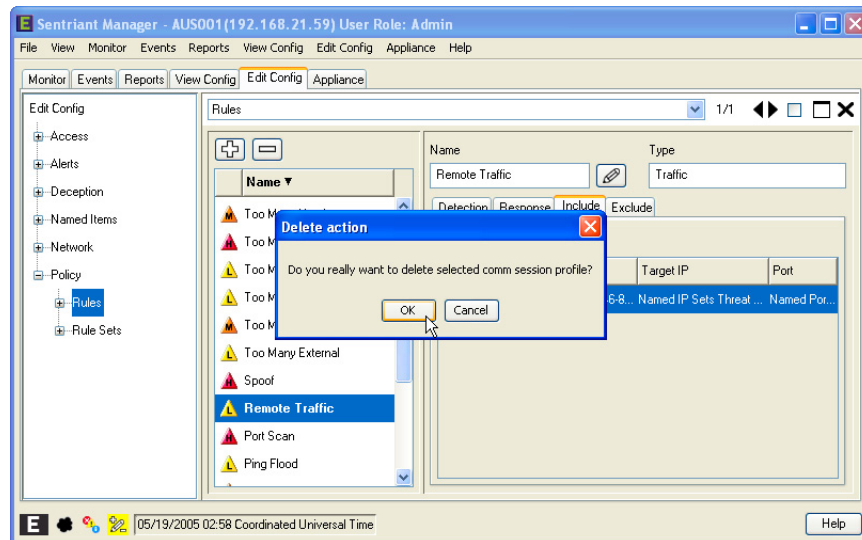


To delete a profile:

- 1 Select the profile from the list and click the **Delete** button.



- 2 Click the **OK** button on the Delete Action dialog.

**NOTE**

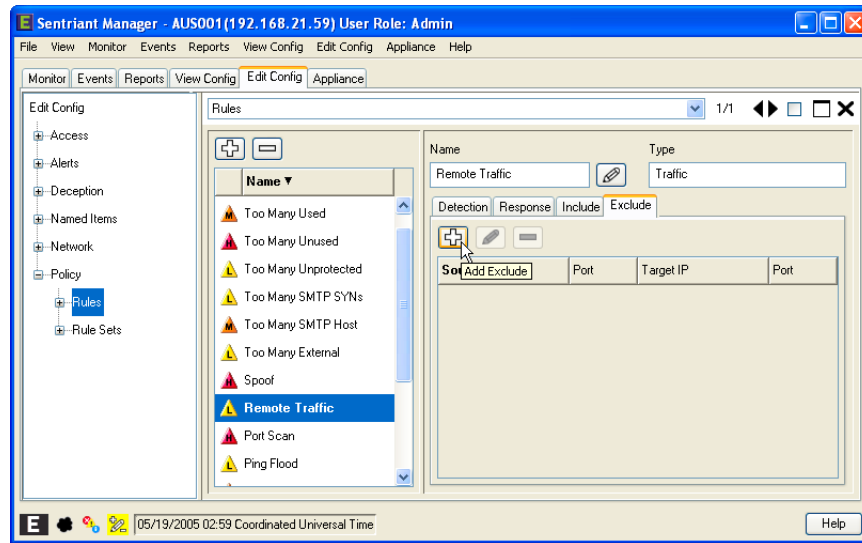
Clicking OK adds the new Include profile to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#).

Excluded IP Addresses

Exclude IP Address tab works similarly to Include IP Address tab except that the range of IP Addresses are excluded from the Include IP Addresses value. For example, you may set a global for IP Addresses to check 10.10.10.0-254 but to exclude 10.10.10.50-75. By entering this value in Source IP, the IP Addresses will be excluded from the monitored traffic for that rule.

To configure Exclude IP Addresses:

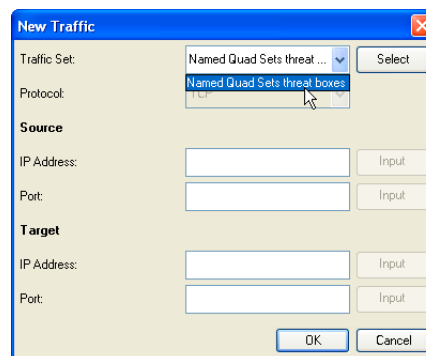
- 1 Select the rule from the Description table.
- 2 Select the **Exclude** tab.
- 3 Click the **Add** button.



There are various methods of adding an exclude profile to the dialog. You may select a Traffic Set from the Named Items, enter each traffic item or use a combination of entered traffic item data and select IP and Port Sets from Named Items.

To use a Traffic Set:

- Click the **Input** button on the Traffic Set line to add a Traffic Set. The remaining traffic data items are disabled because each data item is using the Traffic Set data.



Entering data items and/or using IP and Port Sets:

- Select a Port Protocol from the drop-down list. Choices are TCP, UDP, and ICMP.
- Enter a Source IP Address by one of the two methods:
 - Type an IP Address in the Source IP Address field. The example shows an IP Address using the hyphen (-) wildcard for one of the octets which selects a range of the octet.
 - Use an IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.



NOTE

To revert back to entering an IP Address, click the **Select** button.

- Enter a Source Port Number by one of the two methods:
 - Type a Port number in the Source Port field.
 - Use a Port Set by clicking the **Input** button and then selecting an Port Set from the drop-down list.
- Enter a Target IP Address by one of the two methods:
 - Type an IP Address in the Targets IP Address field.
 - Use an IP Set by clicking the **Input** button and then selecting an IP Set from the drop-down list.

**NOTE**

To revert back to entering an IP Address, click the Select button.

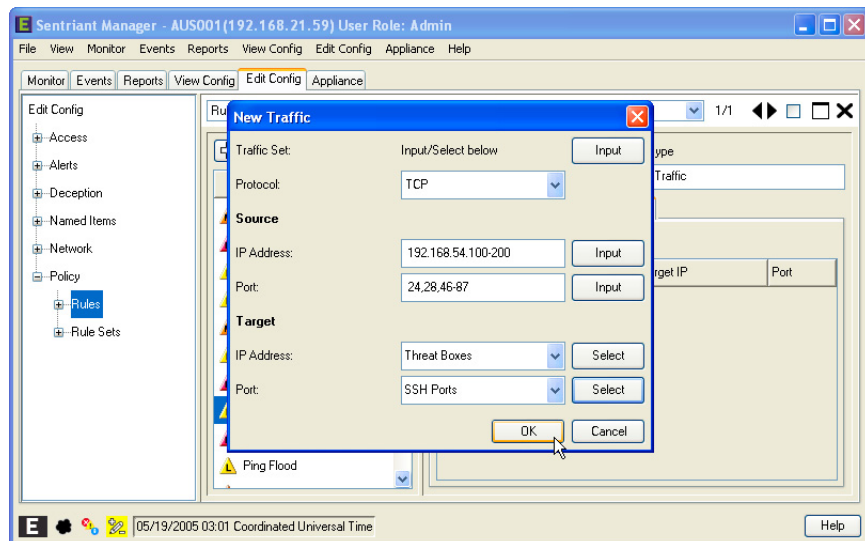
- Enter a Target Port Number by one of the two methods:
 - Type a Port number in the Target Port field.
 - Use a Port Set by clicking the **Input** button and then selecting an Port Set from the drop-down list.

4 Click **OK**.

The new traffic set is added to the Exclude table.

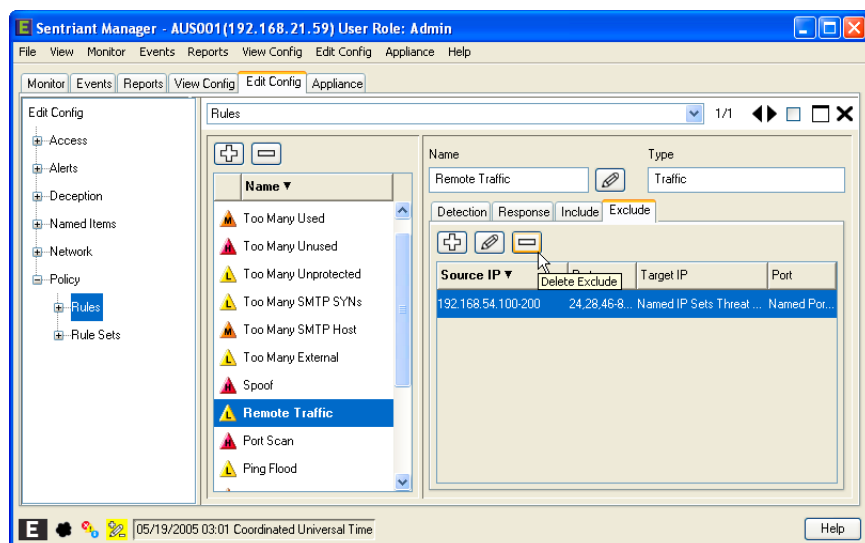
**NOTE**

If Both is selected for the Port Type, both UDP and TCP traffic to the same Port counts as two distinct Port hits for purposes of the Port scan rule threshold. Detection settings for Port # should reflect this setting.

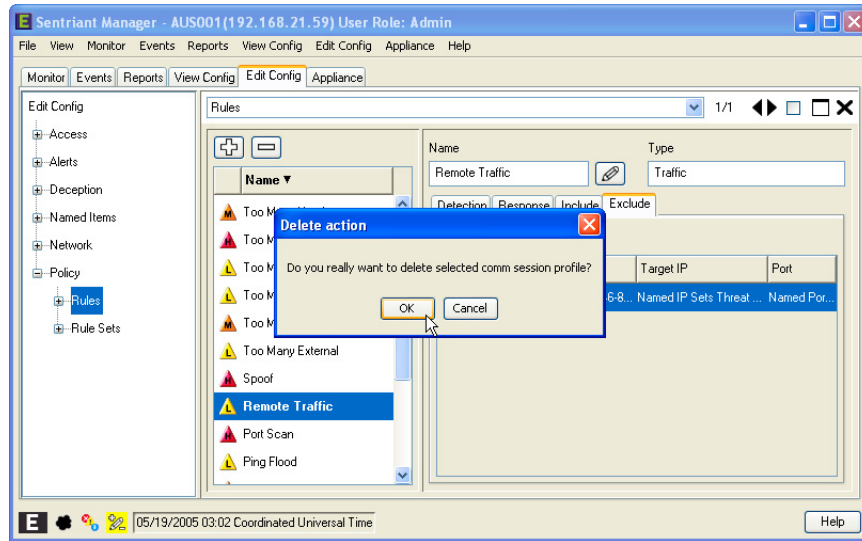


To delete an exclude profile:

- 1 Select a profile from the list and click the **Delete** button.



- 2 Click the **OK** button on the **Delete Action** dialog.

**NOTE**

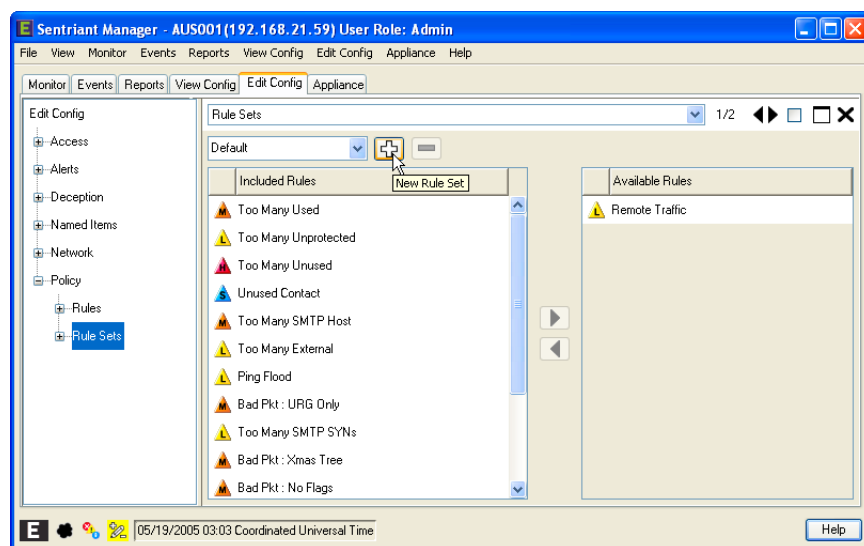
Clicking OK adds the new Exclude profile to the stack of local configuration changes however, it does not update the Sentriant NG appliance's configuration. To learn about saving configuration changes to the Sentriant NG appliance, see ["Saving Changes to the Sentriant NG Appliance" on page 133](#).

Rule Sets

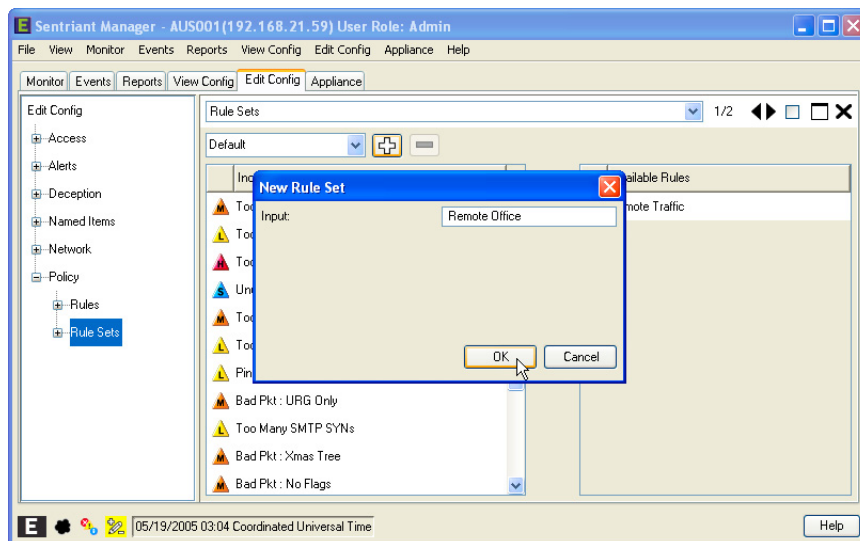
A Rule Set is added to each Segment Set allowing for the best detection possible based on the type of network Segment configuration. When a rule is triggered by a source threat, deception, alerts and cloaking activities are activated.

To create a new Rule Set

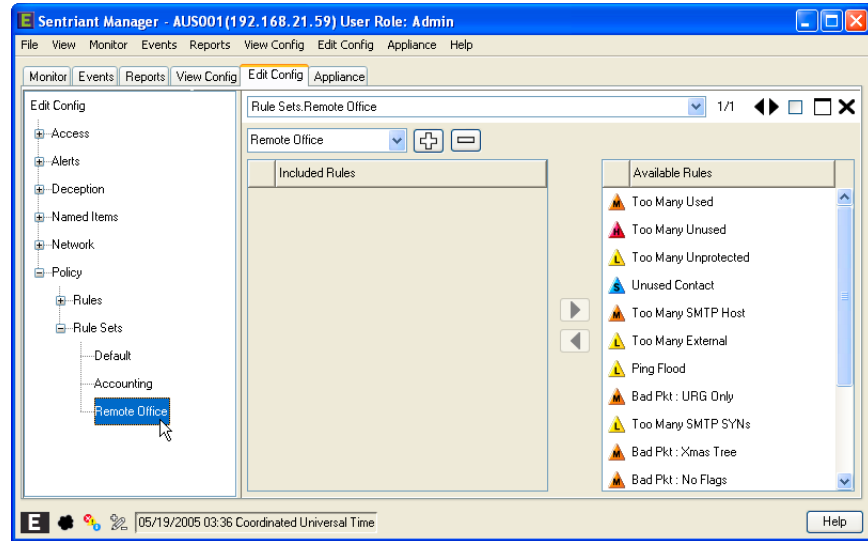
- 1 From **Edit Config > Network > Policy**, click on **Rule Sets** in the Navigation Panel.
- 2 Click the **New Rule Set** button.



- 3 Type in a new Rule Set name.
- 4 Click OK.

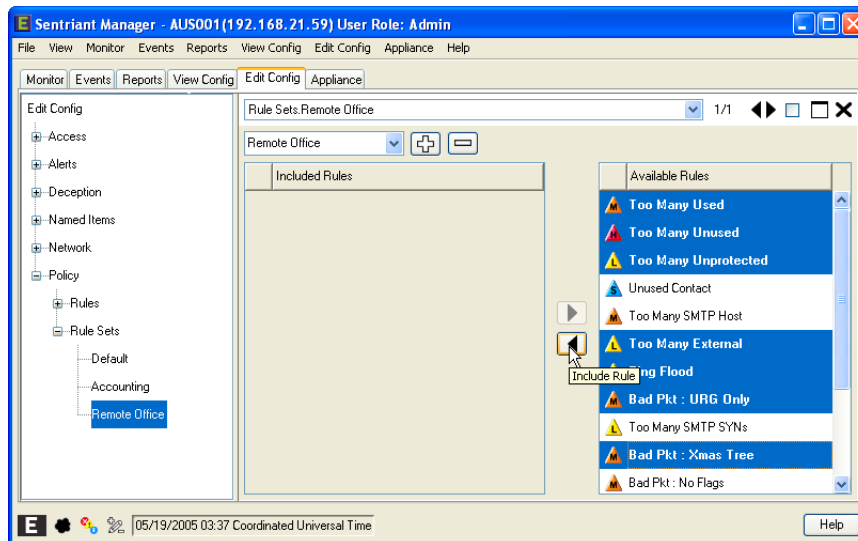


The new Rule Set is created.

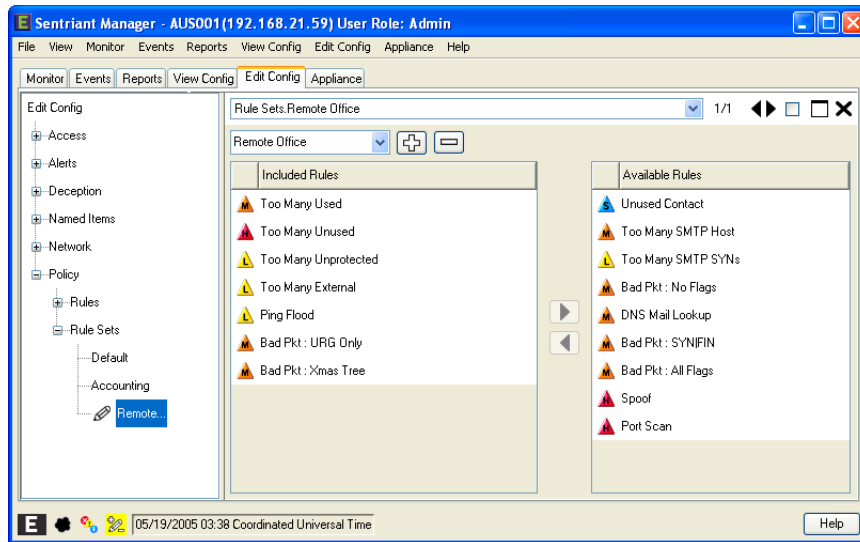


To add a Rule Set to a Segment Set:

- 1 From **Configure > Network > Policy**, select the **Rule Sets**.
- 2 Select a **Rule Set** from the Rule Sets drop-down list.



The Rules are added to the Rule Set.



Save/Load Configuration Settings

The Sentriant NG Manager incorporates three methods of saving configuration settings:

- **From the File Menu** - Saves all of the current configuration for system back up and disaster recovery.
- **From the Configuration Changes Dialog** - Saves pending configuration changes.
- **From the Navigation Bar** - Saves configuration subsets such as access, alerts, segments.

Loading is done from the File menu by selecting the appropriate .xml file. Once the file has been loaded, the user can review changes displayed in the Navigation Bar represented by the new/delete/modify icons. If the loaded changes are satisfactory, the changes can then be persisted to the Sentriant NG appliance through the Configuration Changes Dialog.



NOTE

If there are problems with the loading, configuration changes may be rolled back by clicking the Rollback button located in the Configuration Changes Dialog.



NOTE

Loading Access, or 'user-base' configuration, from one Sentriant NG appliance that differs from the other will trigger a notification stating that all passwords will be reset to 'password'. This is due to the password encryption utilized to secure user passwords. Access configuration can be moved within a monitored environment containing multiple Sentriant NG appliances without resetting passwords, however moving the Access configuration to a Sentriant NG appliance to a dissimilar environment will cause the user's passwords to be reset.

Save Configuration From File Menu

The purpose of the Save Configuration from File menu is more for system back and to load configuration data to new Sentriant NG appliances. All configuration data is saved into a file that represents a configuration snapshot of the Sentriant NG appliance. The save file is defined by the Sentriant NG appliance's hostname. The Sentriant NG appliance can be reconfigured by resetting the Sentriant NG appliance to factory settings through the TUI using the same hostname as before and then loading a saved configuration file. The saved configuration file may also be used when replacing hardware if the current hardware is damaged or fails.

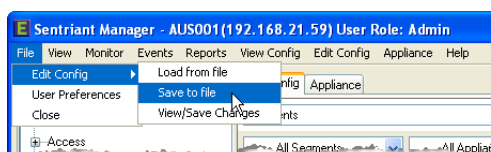


NOTE

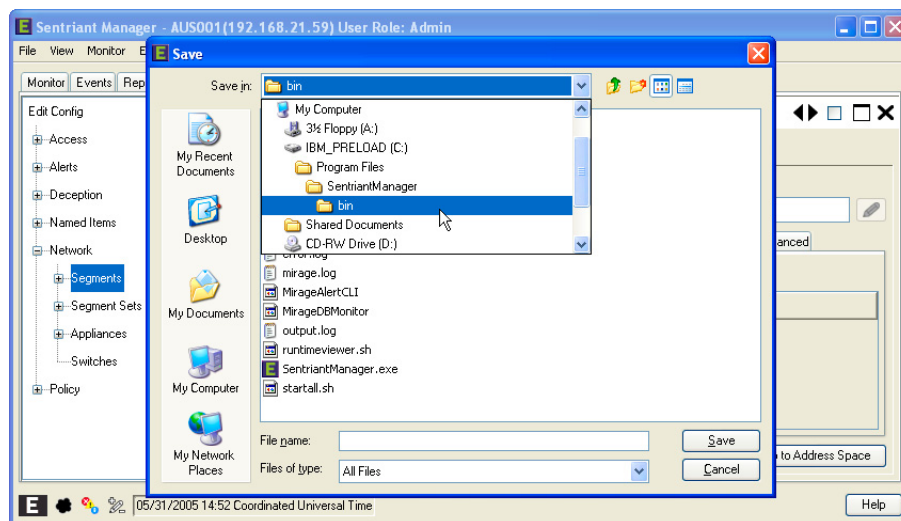
Loading the file from one Sentriant NG appliance to another with a different hostname may result in errors.

To Save Configuration from the File Menu:

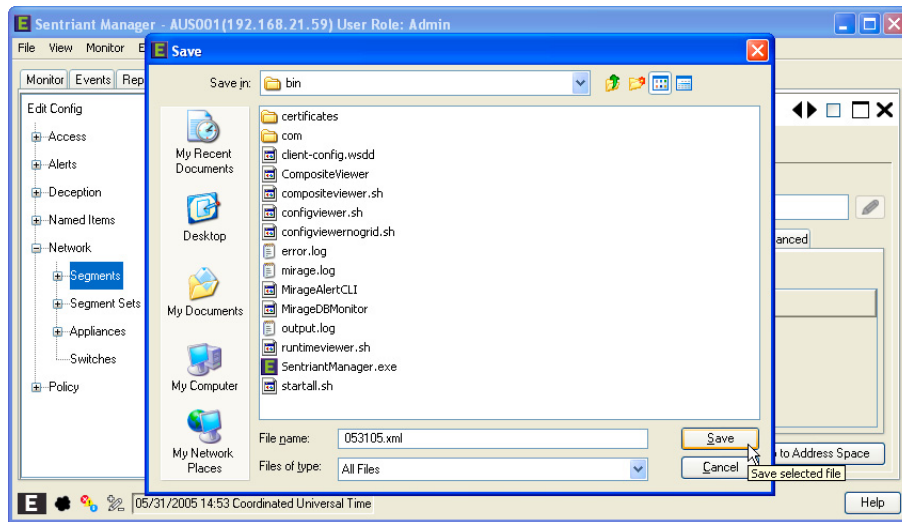
- 1 From the **File** menu, Select **Edit Config > Save to file**.



- 2 Select a folder to save the configuration file. The default folder is under SentriantManager/bin.



- 3 Enter a name for the file.
- 4 Click **Save** selected file.

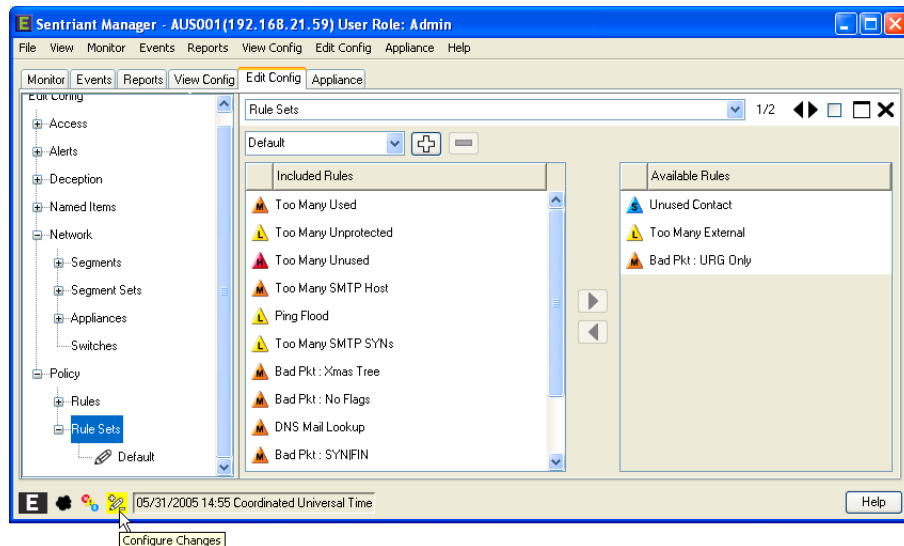


Save Configuration From the Configuration Changes Dialog

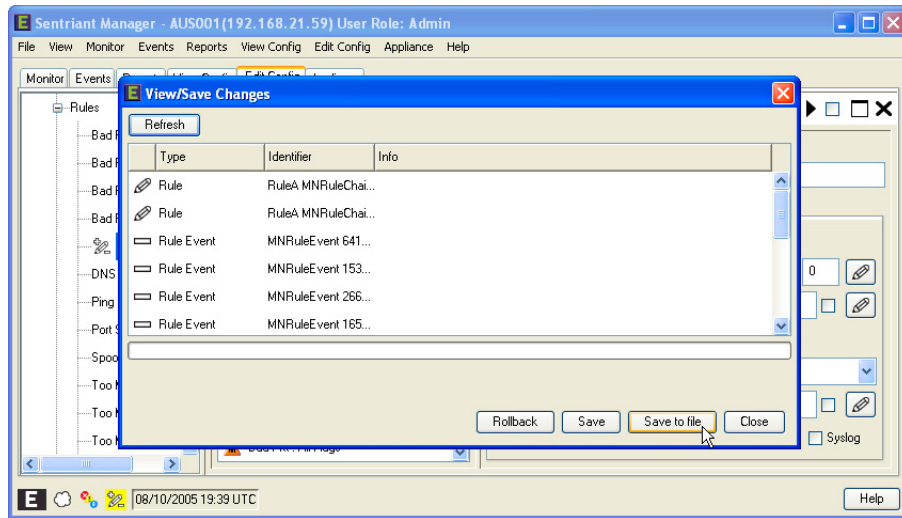
The purpose of save configuration from the Configuration Changes Dialog is to give administrators the option of saving complex configuration changes to a file without persisting them to a Sentriant NG appliance.

To Save Configuration from the Configuration Changes Dialog:

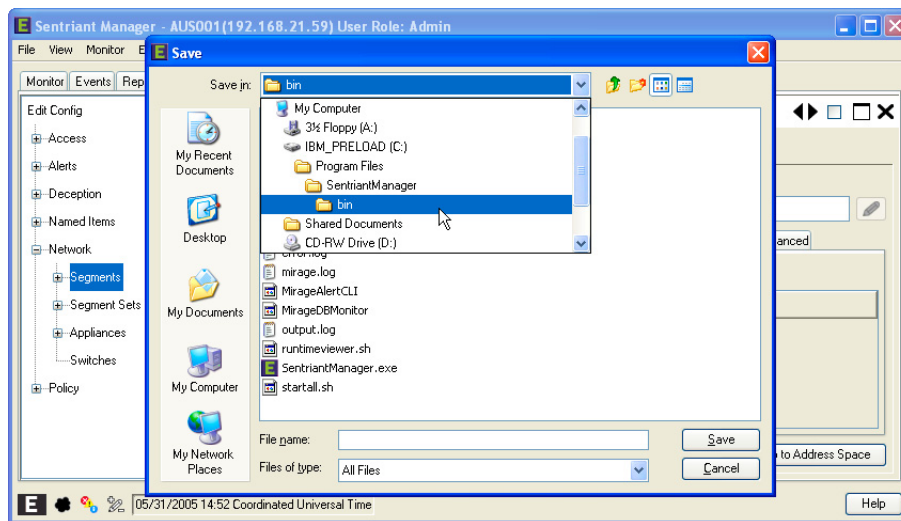
- 1 From the **General Status Bar**, click the **Configure Changes** button.



- 2 Click the **Save to File** button.

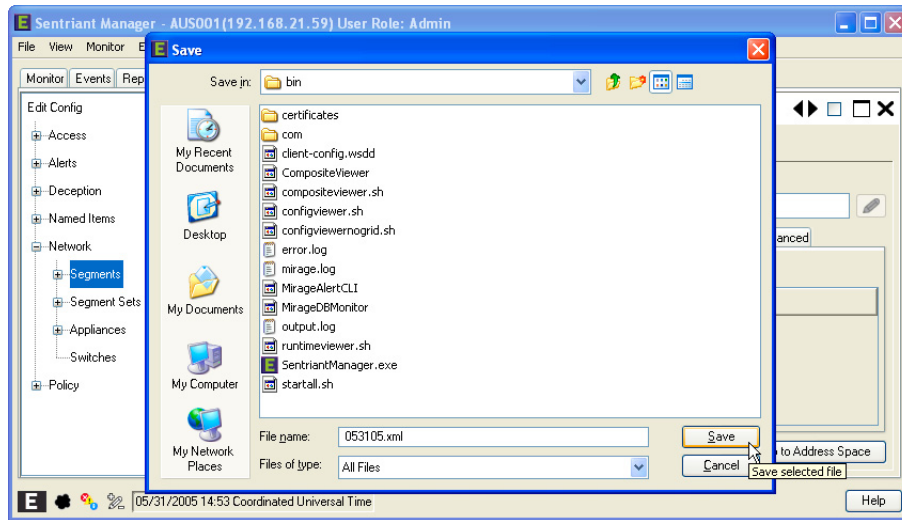


3 Select a folder to save the configuration file. The default folder is under SentriantManager/bin.



4 Enter a name for the file.

5 Click **Save** selected file.



Save Configuration From Navigation Bar

The purpose of save configuration from the Navigation Bar is to give the administrator the option of saving specific subset configuration settings. For example, from the Navigation Bar, right-clicking on a rule will save that rule and its configuration components. Right-clicking a rule set will save all the subrules assigned and the rule set information. Right-clicking a Segment Set will save the rule set, personality set, and Segment Set information.



NOTE

Saving segments is a Sentriant NG 'appliance-specific' task since the interfaces define the segments and the configuration is saved with the segments. Therefore, segments should only be loaded to originating appliance.

Loaded configuration components that may be shared between Sentriant NG appliances are decoys, rules, rule sets, personalities, personality sets, and alerts.

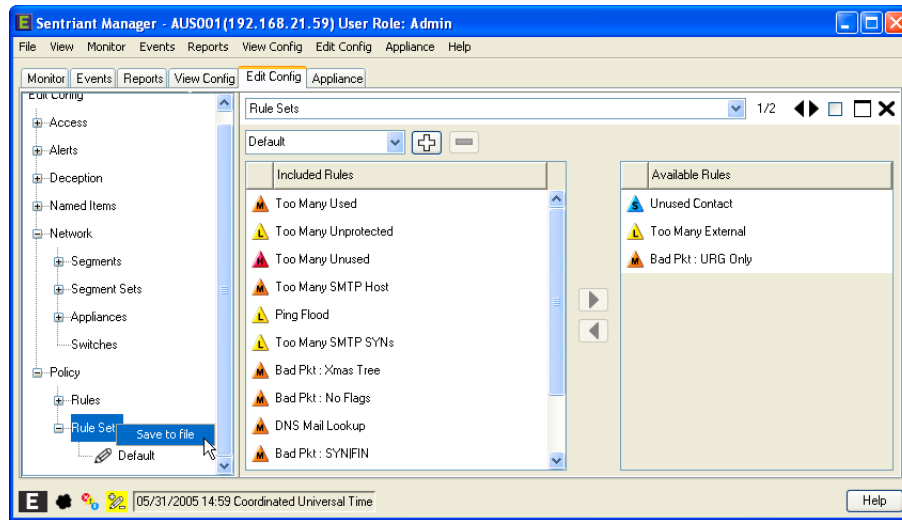


NOTE

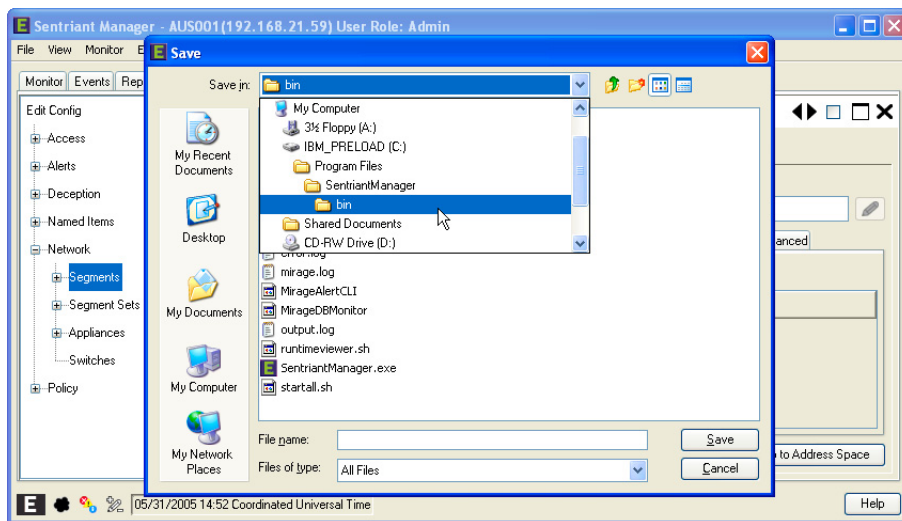
Loading access, or 'user-base' configuration, from a Sentriant NG appliance that is outside of the protected fabric, will trigger a notification stating that all passwords will be reset to 'password'. This is due to the password encryption utilized to secure user passwords. Access configuration can be moved within a monitored fabric containing multiple Sentriant NG appliances without resetting passwords, however moving the Access configuration to a Sentriant NG appliance outside the fabric will cause the user's passwords to be reset.

To Save Configuration from the Navigation Bar:

- 1 From the **Navigation Bar**, select a component to save.
- 2 Right-click and select **Save to file**.

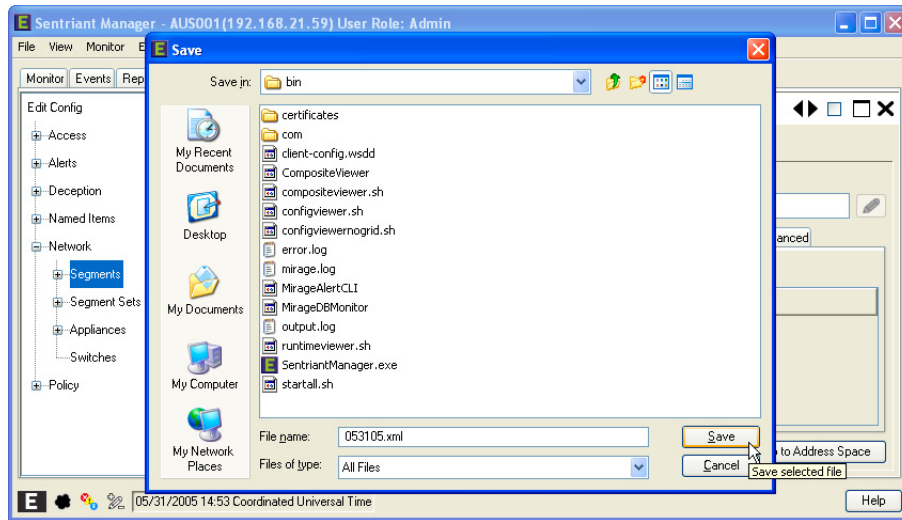


3 Select a folder to save the configuration file. The default folder is under SentriantManager/bin.



4 Enter a name for the file.

5 Click **Save** selected file.



Load Configuration Settings

Loading is done from the File menu by selecting the appropriate file. Once the file has been loaded, the user can review changes displayed in the Navigation Bar represented by the new/delete/modify icons. If the loaded changes are satisfactory, the changes can then be saved to the Sentriant NG appliance through the Configuration Changes Dialog.



NOTE

If there is a problem loading configuration changes, they may be rolled back by clicking the Rollback button located in the Configuration Changes Dialog and start from the current configuration.

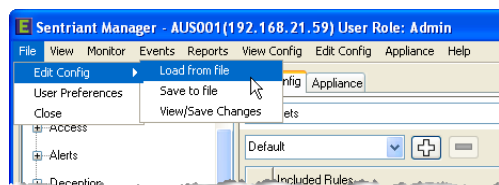


NOTE

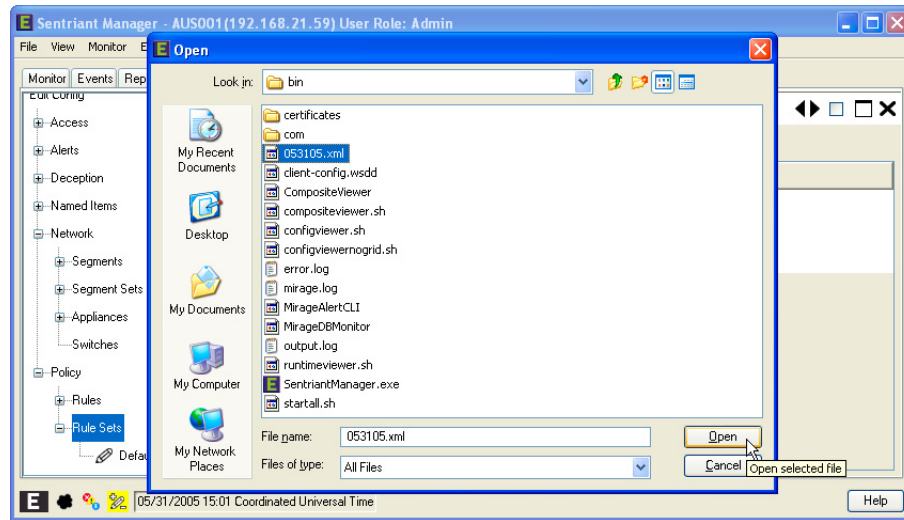
Loading access, or 'user-base' configuration, from a Sentriant NG appliance that is outside of the protected fabric, will trigger a notification stating that all passwords will be reset to 'password'. This is due to the password encryption utilized to secure user passwords. Access configuration can be moved within a monitored fabric containing multiple Sentriant NG appliances without resetting passwords, however moving the Access configuration to a Sentriant NG appliance outside the fabric will cause the user's passwords to be reset.

To load Configuration Changes:

- 1 From the **File** menu, select **Edit Config > Load from file**.



- 2 Navigate to a saved export file and click the **Open** button.



Once the Open Dialog closes the load is complete. You can check the success of the load by clicking the Configuration Changes button in the General Status Bar to bring up the Configuration Changes Dialog. The dialog will display a list of pending configuration changes from the loaded file.

NOTE

When loading the configuration file, only configuration items that are not alike will be displayed in the dialog. In other words, if no configuration changes have been made from the loaded file versus the current configuration, the dialog will be empty.

Appliance

The Appliance Panel within the Sentriant NG Manager is used as a system management and monitoring tool.

At the bottom left of the screen in the General Status Bar is the Appliance Health icon that shows the health or state of the Sentriant NG appliance. The following states are shown:

- E** normal The Sentriant NG appliance is working normally
- E** warning There is a problem that could escalate into an issue. For example, disk space is close to maximum usage.
- E** error An error indicates a threshold has been exceeded. For example, disk space is above maximum usage.
- E** off Indicates that the Sentriant NG appliance is off-line.

The icon in the General Status Bar represents a status but does not specify the area that is in question. Clicking on the Appliance Health Icon brings up the **Appliance Health Panel**. This panel contains an overview of categories being monitored.

The features included within the Appliance Panel are:

- **Date and Time** - The purpose of the Date/Time Panel is to synchronize the time between the Sentriant NG appliance and workstations running Sentriant NG Manager.
- **Maintenance** - The purpose of the Maintenance Panel is for the administrator to perform maintenance tasks such as restarting, changing the name, IP Address and other Sentriant NG appliance functions.
- **Health** - The Health Panel displays Sentriant NG appliance services for disk, database and network activities. Each service is linked with notification features that alert the administrator of problems with the health of the Sentriant NG appliance. Sentriant NG Manager appliance notifications cover the following:
 - Disk Management - monitors individual disk partitions
 - Database Management - monitors database, table, and archive statistics
 - Network Interface Management - monitors each network interface link

Date and Time

The purpose of the Date/Time Panel is to synchronize the time between the Sentriant NG appliance and workstations running with Sentriant NG Manager. There are two methods to synchronize time, one is to manually enter the time using the time and date controls, the other method is to specify a remote server using the Network Time Protocol.

To set the date and time manually:

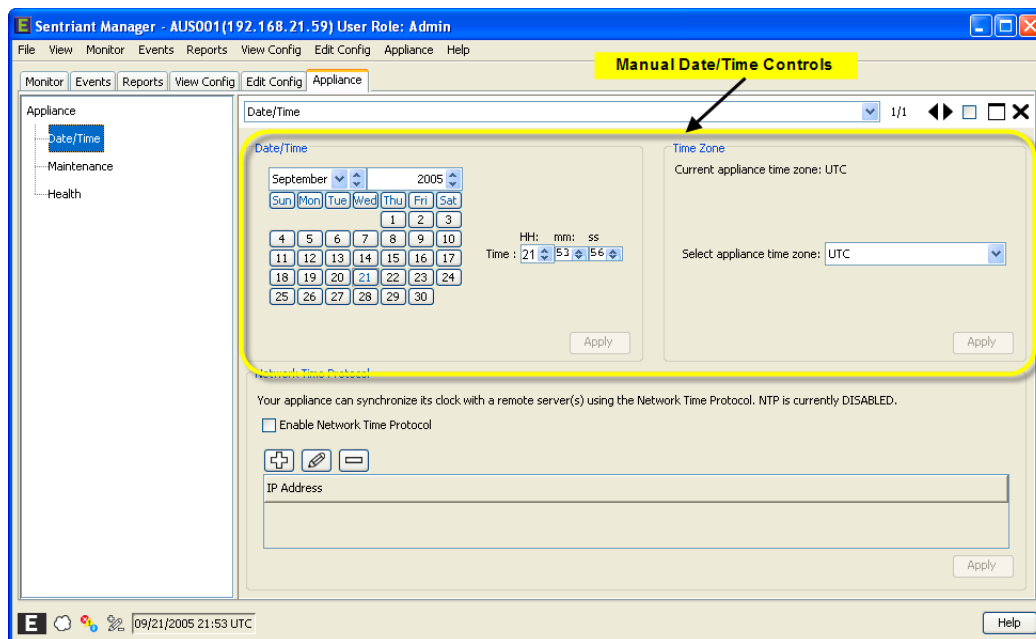
- 1 From **Appliance** tab > **Date/Time**, set the date/time using the controls.
- 2 Select a time zone from the list.

NOTE

Changing the time zone will require a reboot of the Sentriant NG appliance to take affect.

NOTE

The date/time must be within +/- five (5) minutes of the Sentriant NG appliance and the workstations running Sentriant NG Manager. If the times are not synchronized, the traffic on the segments will not be displayed correctly in the Monitor Panel.



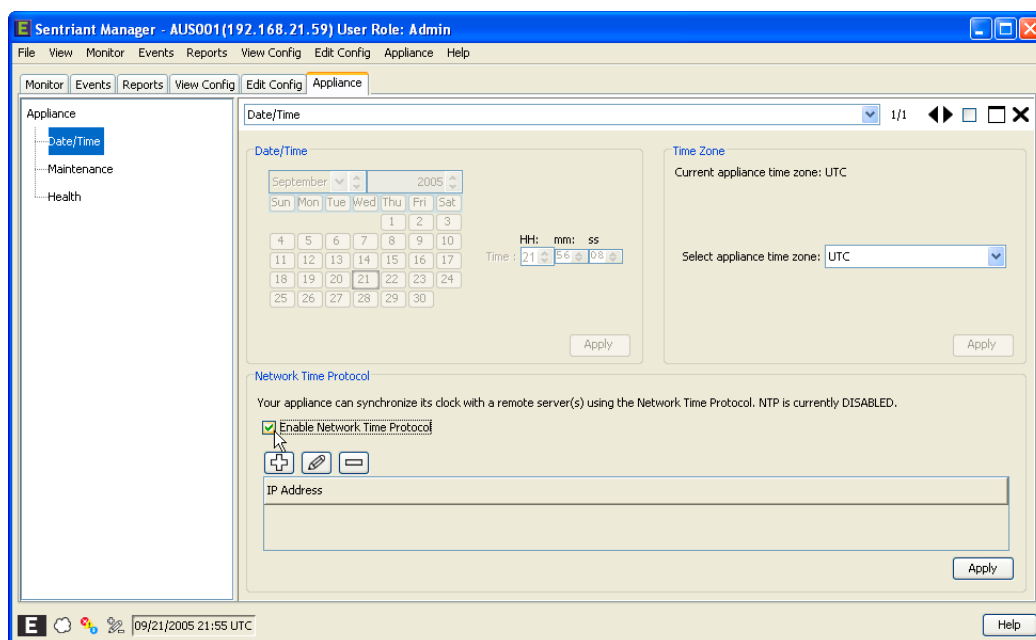
- 3 Click the **Apply** button to save the date/time change or Time Zone change and restart the appliance.

NOTE

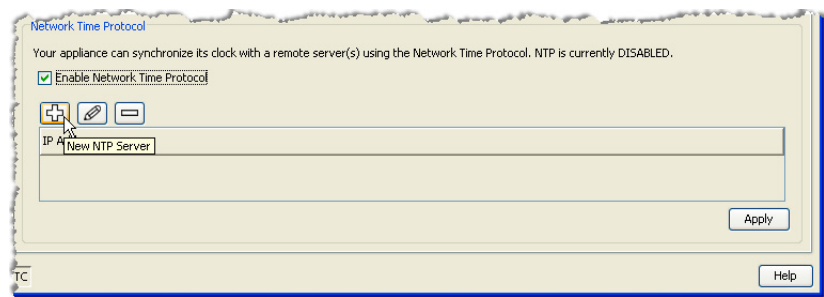
Depending on the Sentriant NG appliance and the network connection, it may take several minutes for the Sentriant NG appliance to complete the restart. Once the restart has completed, you may log back into Sentriant NG Manager. If the Sentriant NG appliance has not restarted, an error will be displayed at the Sentriant NG Manager login screen.

To set a remote server using Network Time Protocol:

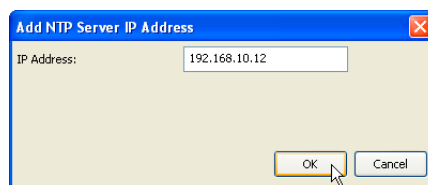
- 1 Click the **Enable Network Time Protocol** checkbox.



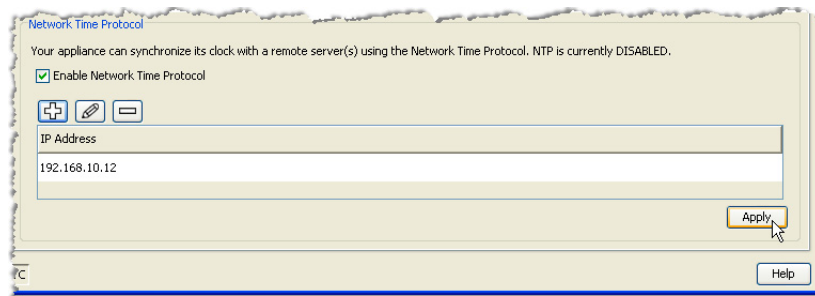
- 2 Click the **New NTP Server** button.



- 3 Enter the **IP Address** of the **NTP Server** and click **OK**.



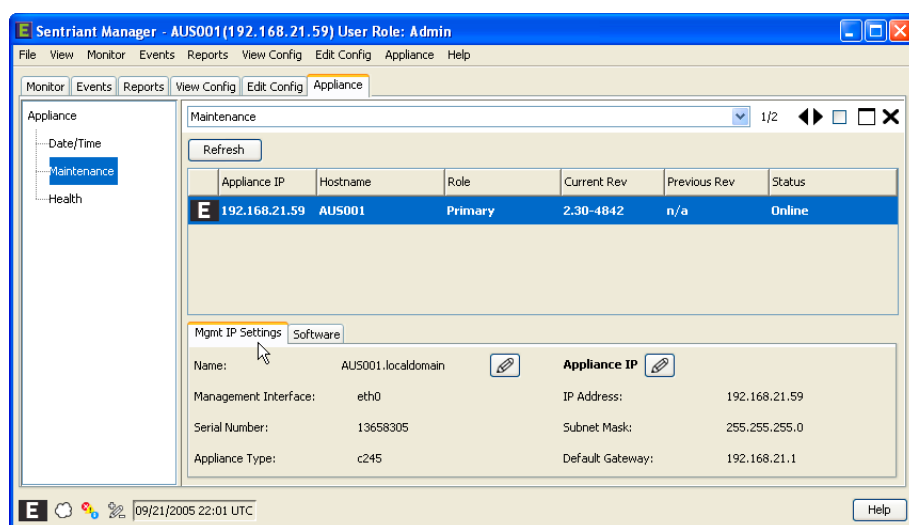
- 4 Click the **Apply** button to save the NTP Server settings.



The NTP Server is added to the Date and Time panel.

Maintenance

Maintenance activities can be performed on Sentriant NG appliances from the Sentriant NG Manager remotely to ensure that the Sentriant NG appliance and its services are operating normally.



The Maintenance Panel contains the following appliance information:

- Appliance IP - IP Address of the Sentriant NG appliance
- Hostname - Name given to the Sentriant NG appliance during initial configuration
- Current Rev - Current Sentriant NG Manager software version loaded on the Sentriant NG appliance
- Previous Rev - If the software has been update, the previous version will be displayed.
- Status - Displays information regarding the status which can be Online, Offline, Restarting or Error

Double-clicking on a Sentriant NG appliance or right-clicking and selecting Details brings up the Details Panel containing two tabs, Mgmt IP Settings and Software.

Right-clicking on a Sentriant NG appliance will display the pop-up menu containing available actions that can be performed on a Sentriant NG appliance. See [“Maintenance Actions” on page 308](#) to learn more about the individual actions.

The **Mgmt IP Setting Tab** is where changes can be made on the following parameters:

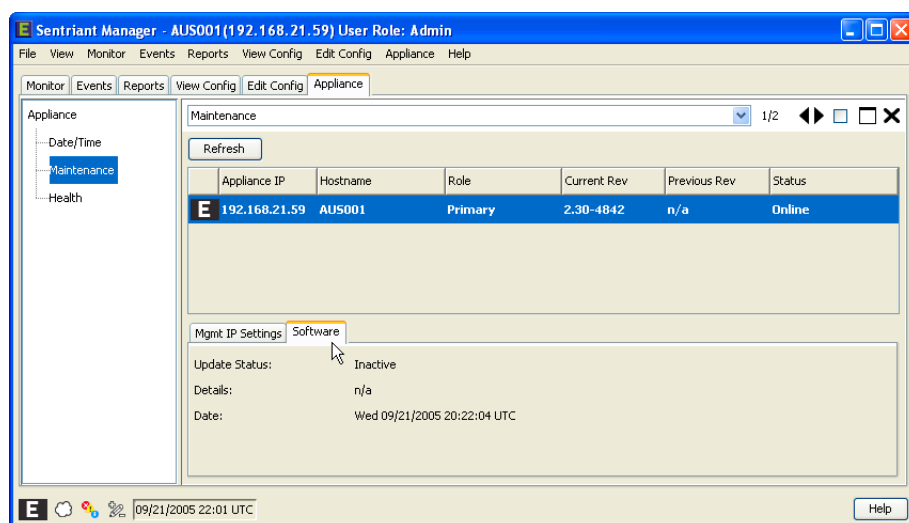
- Name - Edit the name of the Sentries NG appliance
- IP Address - Edit the IP Address of the Sentries NG appliance
- Subnet Mask - Edit the IP Address of the Subnet Mask
- Default Gateway - Change the default gateway to another by entering the new IP Address

Additional information about the appliance is also displayed:

- Serial Number - Serial number of the appliance
- Management Interface - Physical Port designated as the management port of the appliance
- Appliance Type - Model of the Sentries NG appliance

The **Software Tab** displays the following:

- Update Status - Status of software updates which can be Inactive or Active
- Details - Results of the last software update/rollback
- Date - Date and time in UTC of the last software installation or update

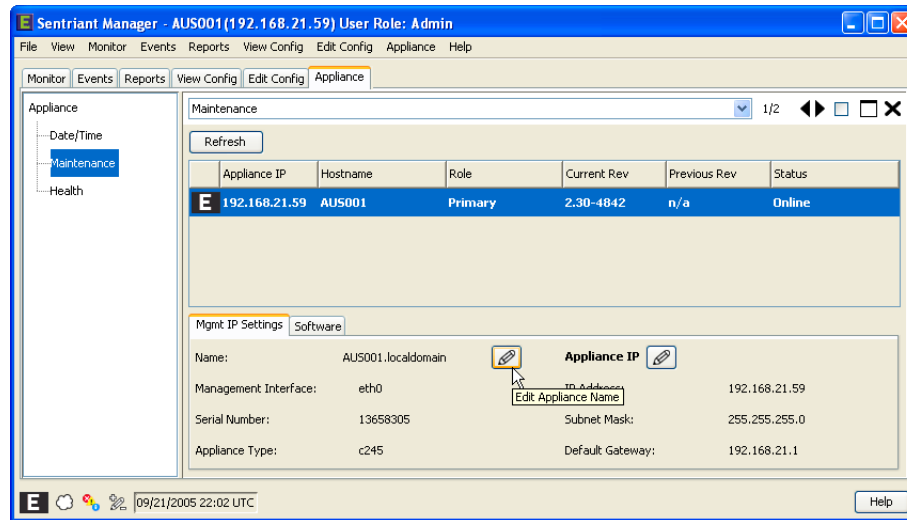


Edit Appliance Name

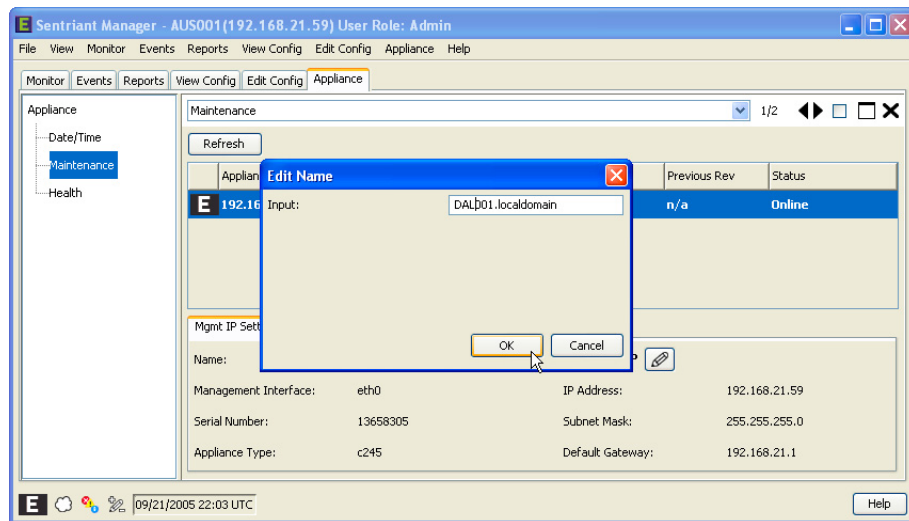
You may change the name of the Sentries NG appliance at any time once the appliance has been initially configured.

To change the name of an appliance:

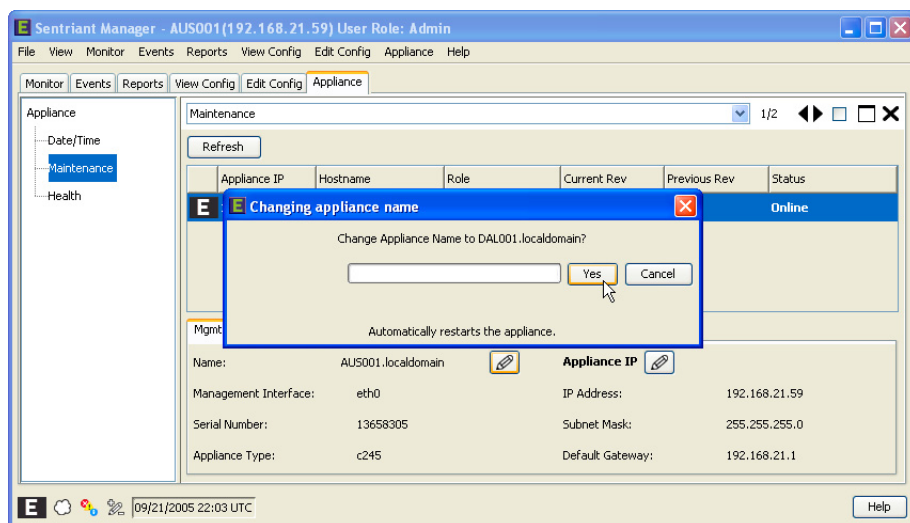
- 1 From the **Appliance > Maintenance** tab, select a Sentries NG appliance.
- 2 Click the **Edit Name** button.



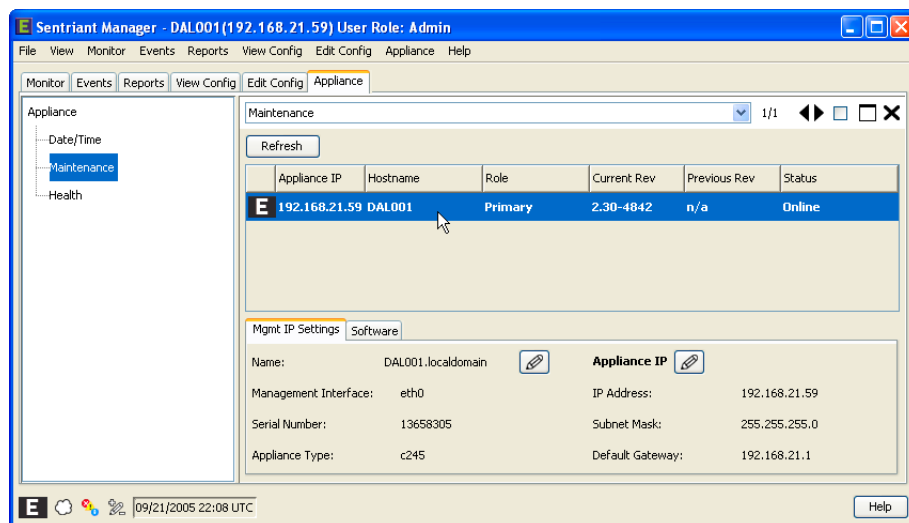
- 3 Enter a name. The name should be no longer than 200 characters.
- 4 Click the **OK** button.



- 5 Click **Yes** to save changes.



The Maintenance panel is updated with the new appliance name.



Edit Appliance IP Configuration

It may become necessary to change the IP Addresses of a Sentriant NG appliance due to moving the appliance or standardizing Sentriant NG appliance IP Addresses.

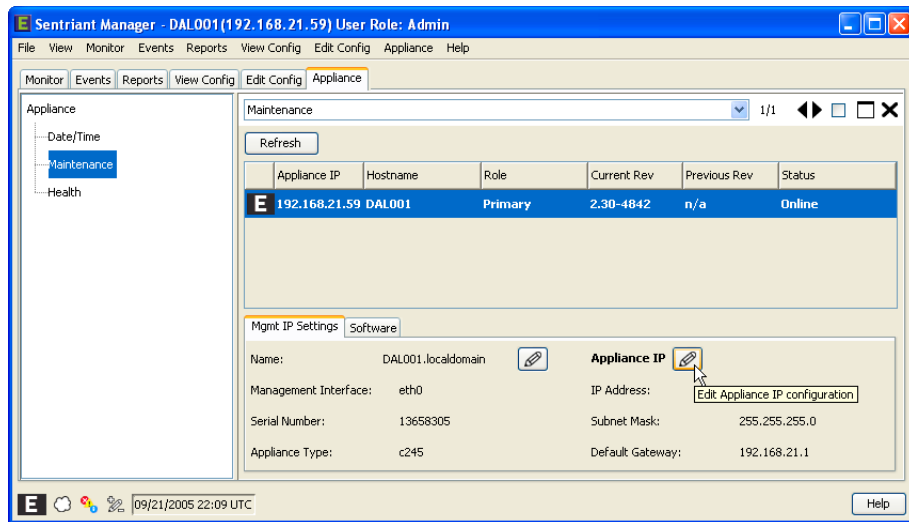


NOTE

If the IP Address is changed, it will no longer monitor segment traffic. The Sentriant NG appliance will need to be reinitialized.

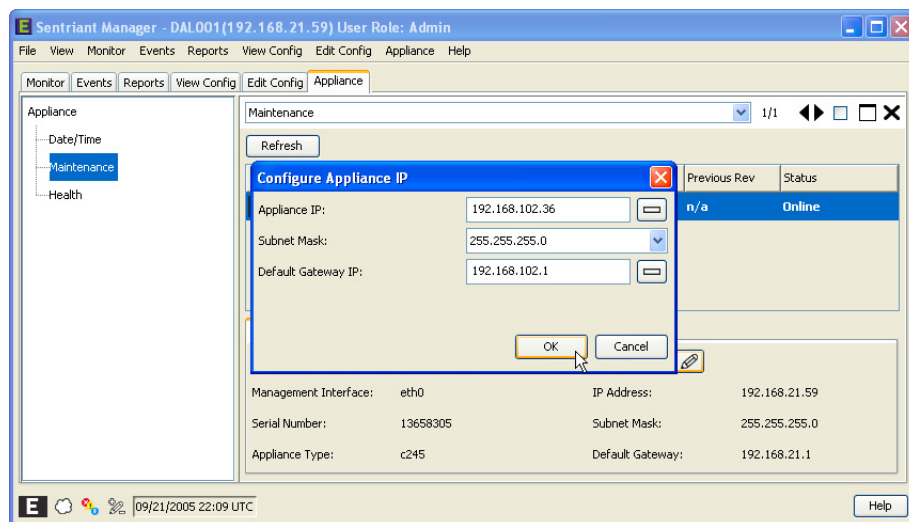
To change the IP Address of a Sentriant NG appliance:

- 1 From the **Appliance > Maintenance** tab, select a Sentriant NG appliance.
- 2 Click the **Edit Appliance IP Configuration** button.



From the Configure Appliance IP dialog, you can edit or change the IP Addresses for the Appliance IP, Subnet Mask, and the Default Gateway. You may change one, all or a combination.

- 3 Enter an **IP Address** for each of the items that you want to change.
- 4 Click **OK**.



Maintenance Actions

Maintenance actions can be performed to Sentriant NG appliances from the Sentriant NG Manager. The purpose of the actions is to ensure that the Sentriant NG appliance and its services are operating normally. The following actions can be taken:

- **Export Logs** - Exports log files from the Sentriant NG appliance to a specified location

- **Reboot** - Reboots the selected Sentriant NG appliance
- **Shutdown** - Shuts down the Sentriant NG appliance
- **Update Software** - Uploads a patch from a specified location with the latest Extreme Network software updates for the Sentriant NG appliance and Sentriant NG Manager
- **Rollback** - Rollback the installed patches to the previous software version
- **Details** - Brings up the Details Panel which contains additional information about the selected Sentriant NG appliance
- **Editing SNMP Agent** - Allows retrieval of SOC information through an SNMP agent

Maintenance Actions can be accessed by right-clicking on a Sentriant NG appliance displayed in the list within the Maintenance Panel.

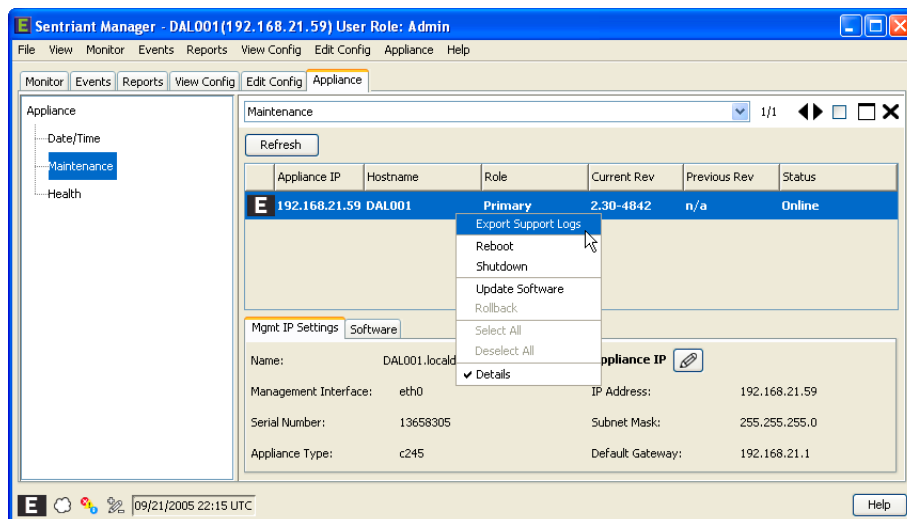
Export Support Logs

The Export Support Logs is used to pull support log files off the Sentriant NG appliance and store them on the client. These logs are pulled off the Sentriant NG appliance from "/var/log/Extreme".

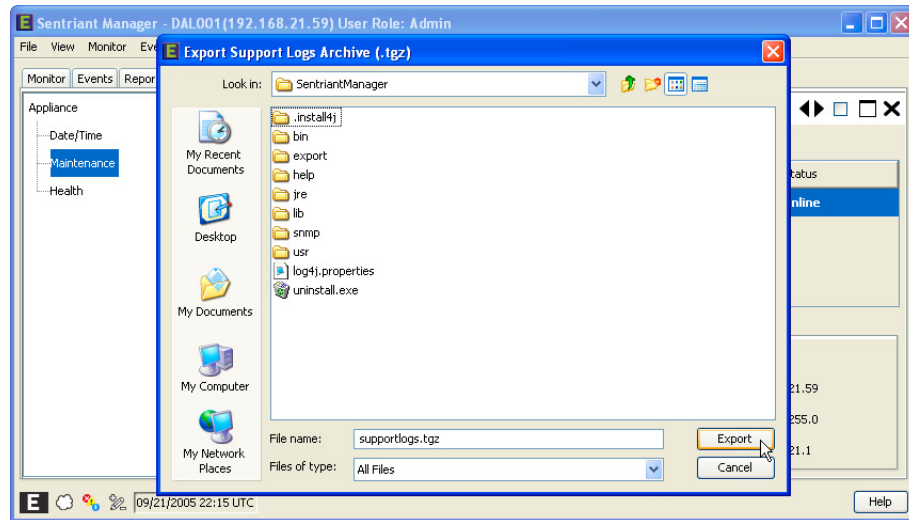
The logs are stored in a tar (.tgz) file that can be viewed using Winzip or other similar compression software package.

To export log files from a Sentriant NG appliance:

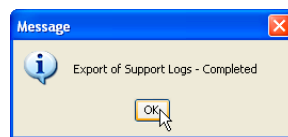
- 1 From **Appliance > Maintenance** tab, select a Sentriant NG appliance.
- 2 Right-click and select **Export Support Logs**.



- 3 Select a folder to save the export file.
- 4 Click **Export** to begin exporting the support files.



- 5 Once the export has been completed a dialog is displayed. Click **OK** to close the dialog.

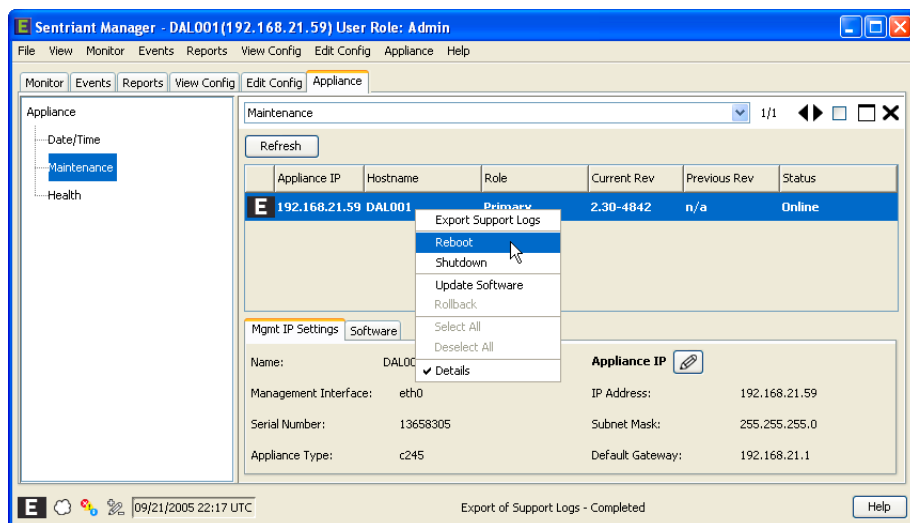


Reboot

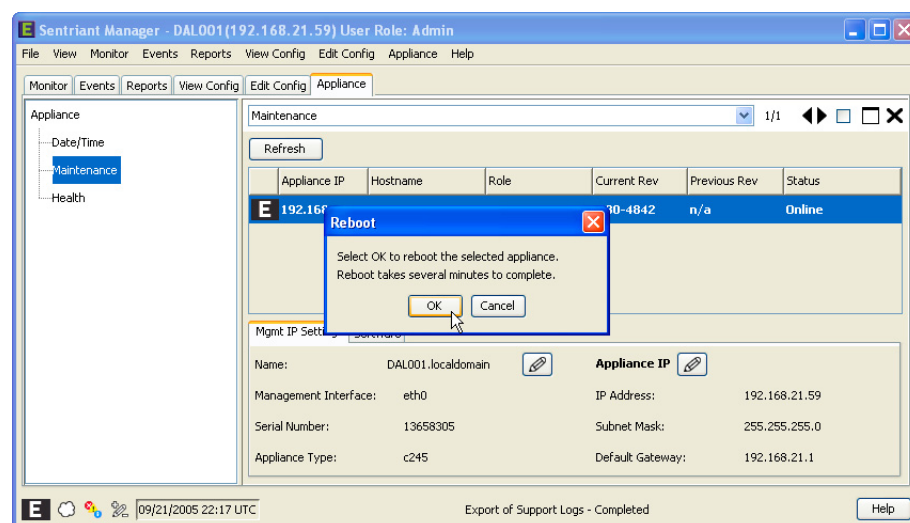
Rebooting of the Sentriant NG appliance may be necessary to clear any unusual behaviors such as network interruptions or disk errors. Reboots can be done at the Sentriant NG appliance or remotely through the Sentriant NG Manager.

To reboot a Sentriant NG appliance:

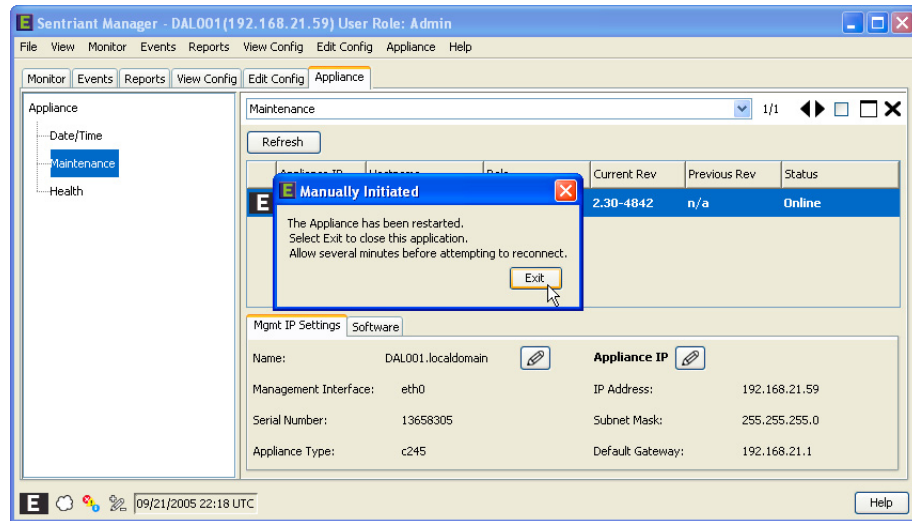
- 1 From **Appliance > Maintenance** tab, select a Sentriant NG appliance.
- 2 Right-click and select **Reboot**.



- 3 The Reboot dialog opens. Click **OK** to start the reboot process.



- 4 The Manually Initiated dialog opens. Click **Exit** to close Sentriant NG Manager and give the Sentriant NG appliance time to reboot. You will need to restart Sentriant NG Manager after the reboot has completed.



NOTE

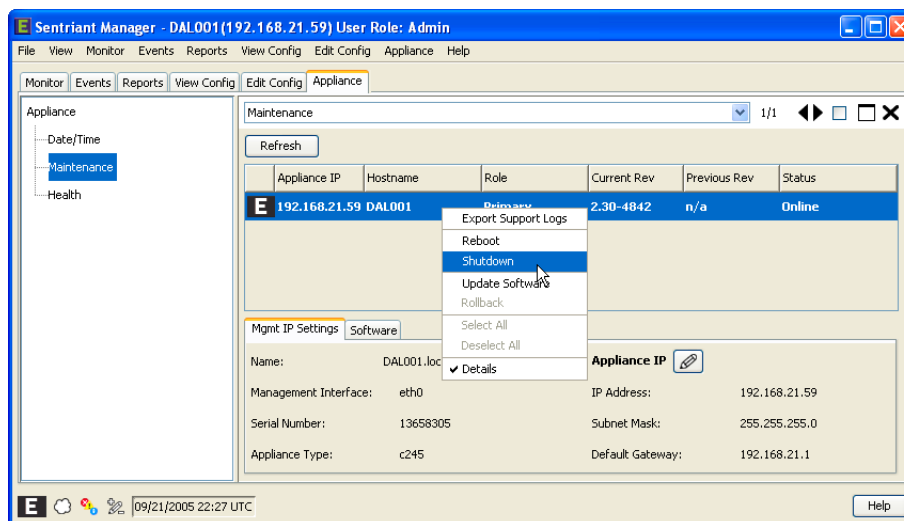
Depending on the Sentriant NG appliance and the network connection, it may take several minutes for the Sentriant NG appliance to complete the reboot. Once the reboot has completed, you may restart the Sentriant NG Manager. If the Sentriant NG appliance has not rebooted, an error will be displayed at the Sentriant NG Manager login screen.

Shutdown

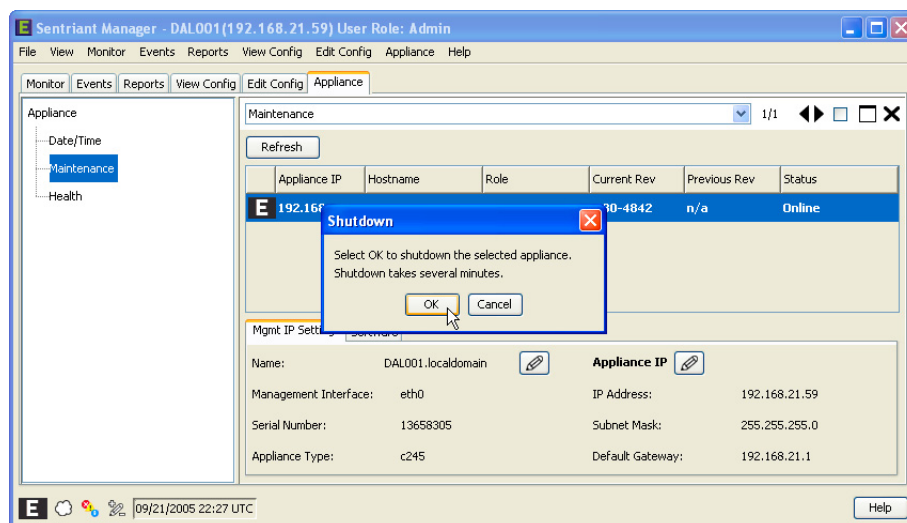
Shutting down the Sentriant NG appliance may be necessary to perform software updates and other workstation related activities where the Sentriant NG appliance may detect an erroneous threat. Shutting down the Sentriant NG appliance can be done at the Sentriant NG appliance or remotely through the Sentriant NG Manager.

To shutdown a Sentriant NG appliance:

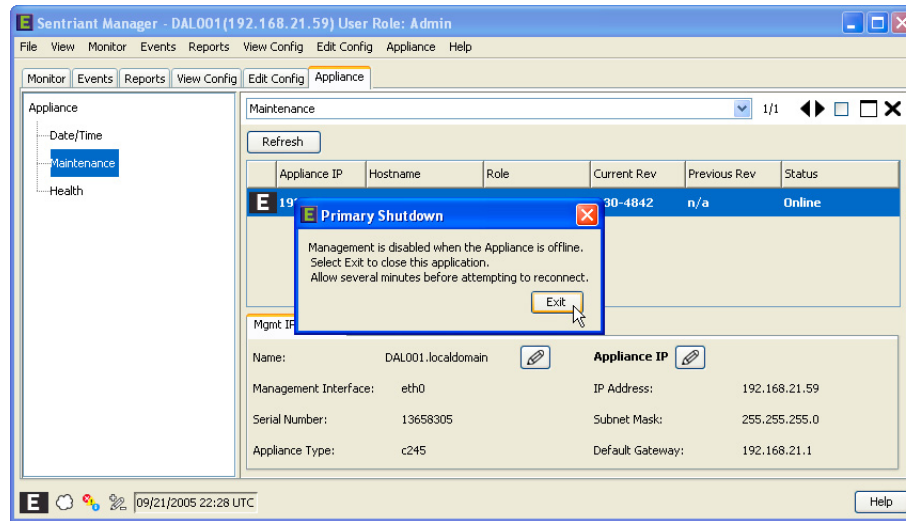
- 1 From **Appliance > Maintenance** tab, select the Sentriant NG appliance.
- 2 Right-click and select **Shutdown**.



- 3 Click the **OK** button to start the shutdown process.



- 4 The Primary Shutdown dialog opens. Click **Exit** to close Sentriant NG Manager and give the Sentriant NG appliance time to reboot. You will need to restart Sentriant NG Manager after the reboot has completed.



NOTE

Depending on the Sentriant NG appliance and the network connection, it may take several minutes for the Sentriant NG appliance to complete the shutdown.

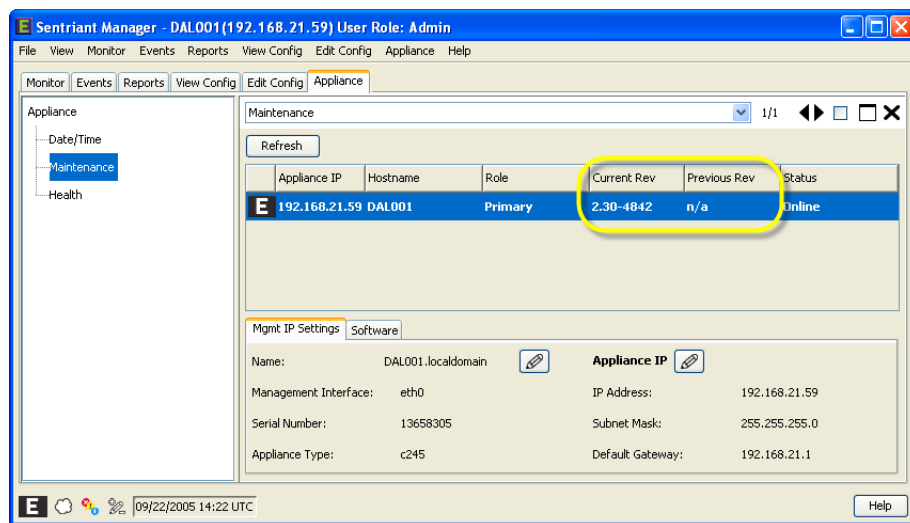
Update Software

When new features are available for the Sentriant NG appliance and Sentriant NG Manager, patches will become available. These patches can be used to update the current configuration using the Update Software action.

Before a patch is applied to a Sentriant NG appliance, the administrator should verify the current software version loaded on the Sentriant NG appliance.

To verify software version:

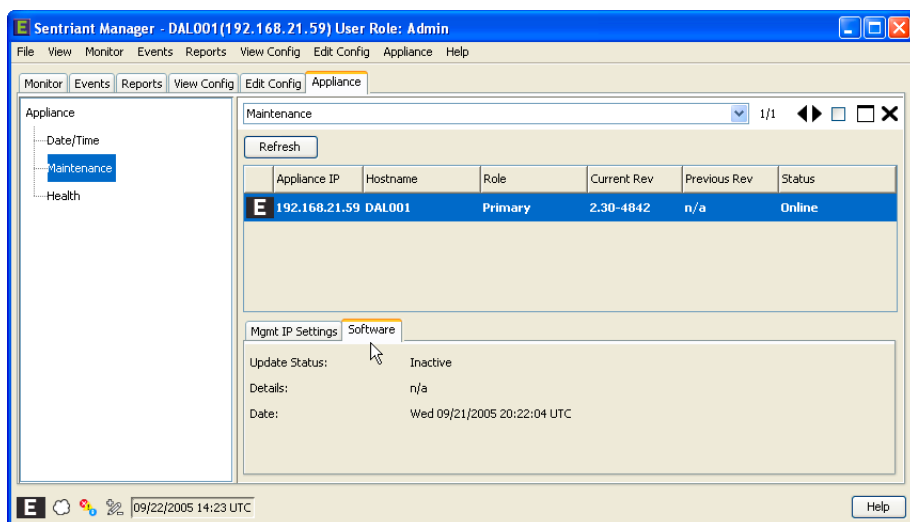
- 1 From the **Appliance > Maintenance Panel**, select the Sentriant NG appliance.
- 2 Determine the current revision and previous revision of the Sentriant NG appliance.



3 Select **Software** Tab to view details about the last update.

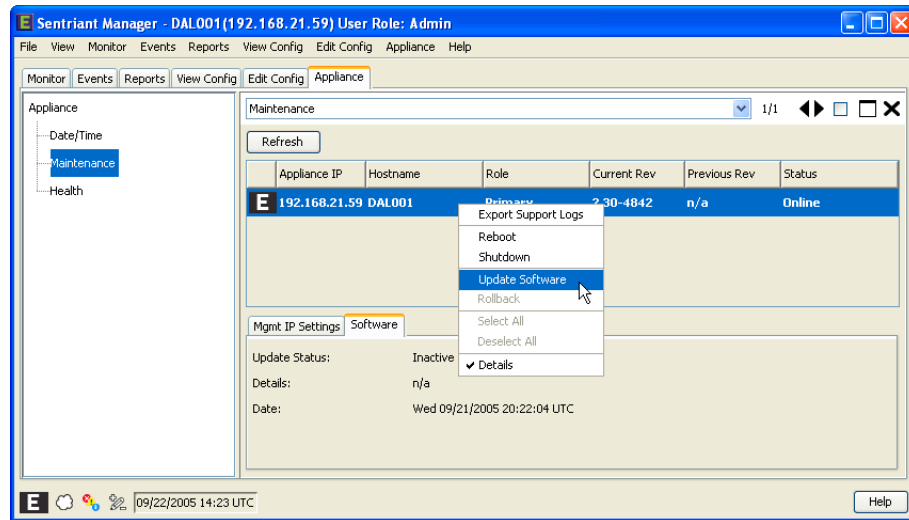
The Software Panel displays the following:

- Update Status - Active or Inactive
- Details - The results of the last software update/rollback
- Date - The date of the last update



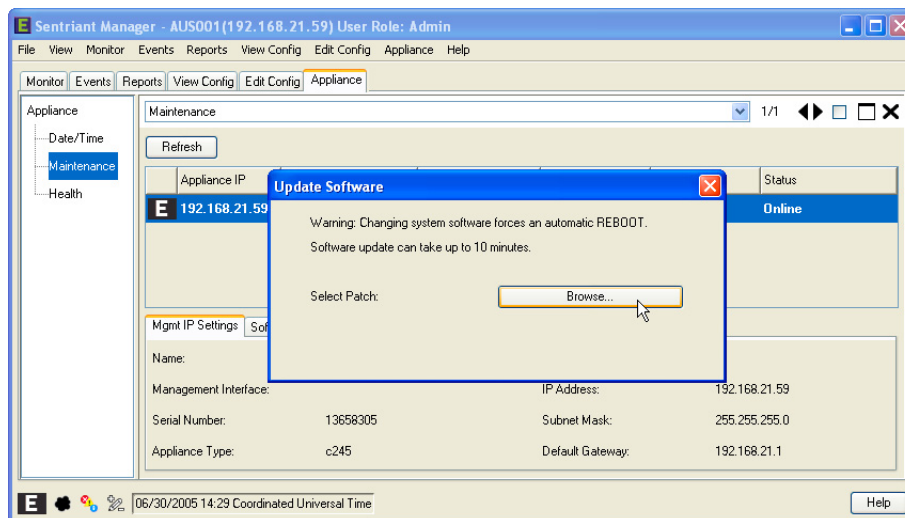
To update software:

- 1 From the **Appliance > Maintenance** panel, select the Sentriant NG appliance.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Update Software**.

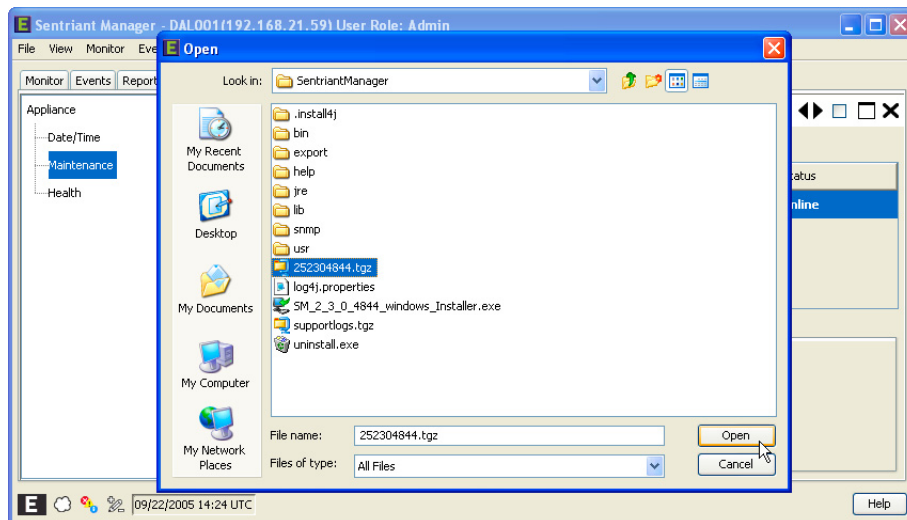


4 The **Update Software** dialog is displayed.

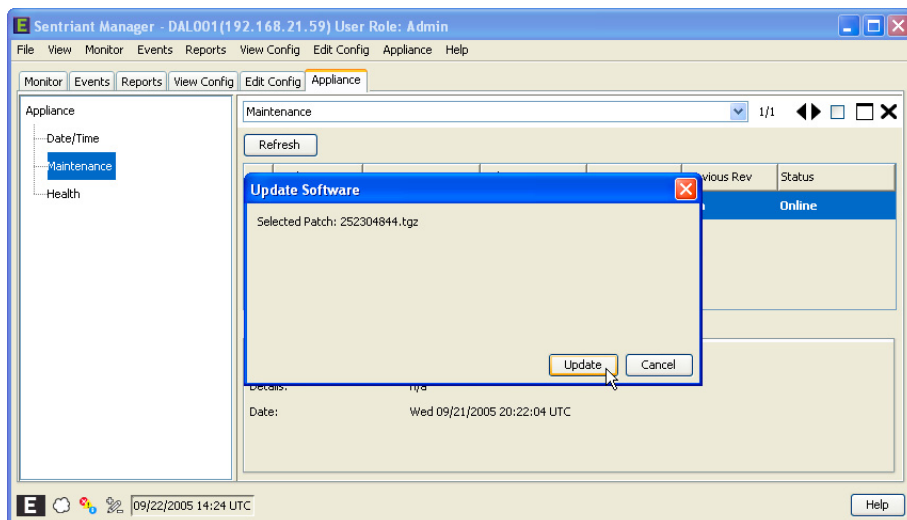
5 Click the **Browse** button.



6 From the File Chooser, select the patch to install.



7 Click the **Update** button to begin the update process.

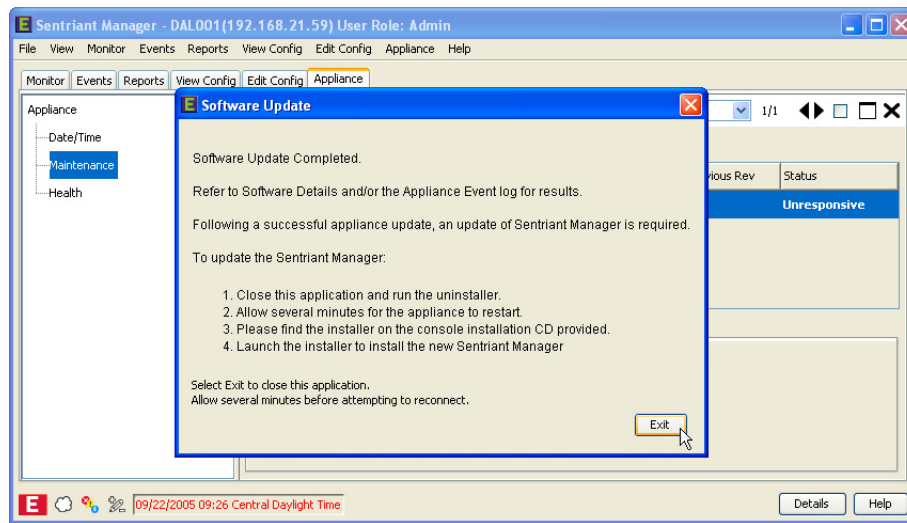


When the update begins the following process occurs:

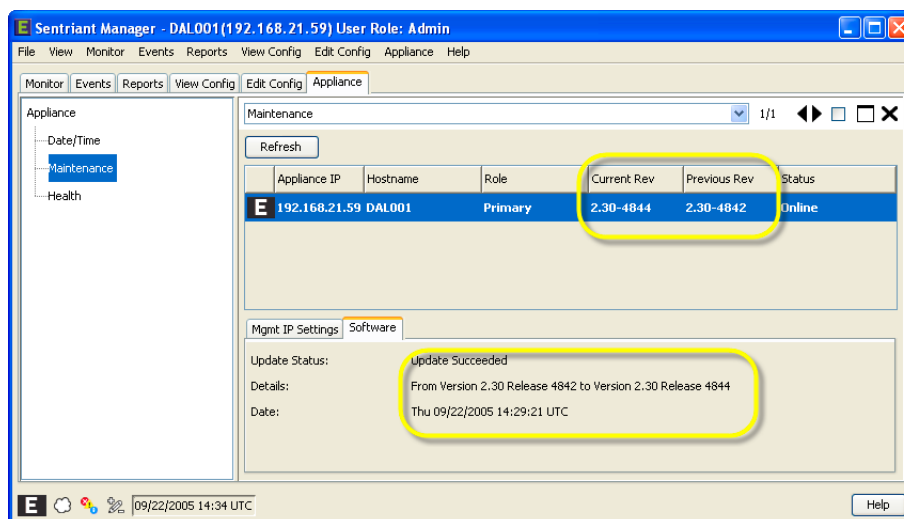
- the client pushes the patch to the Sentriant NG appliance
- the patch is applied to the Sentriant NG appliance in a test mode that verifies the file changes have been loaded correctly and that the changes are successful
- reboots the Sentriant NG appliance and applies all of the Extreme software components

Once the Sentriant NG appliance completes the software update, the admin can then upgrade the Sentriant NG Manager software following the on-screen instructions.

8 Click the **Exit** button to close Sentriant NG Manager.



The Sentriant NG appliance is update with the Current Revision number and Previous Revision number.



Rollback

The Rollback action is used to rollback the software version currently on a Sentriant NG appliance.

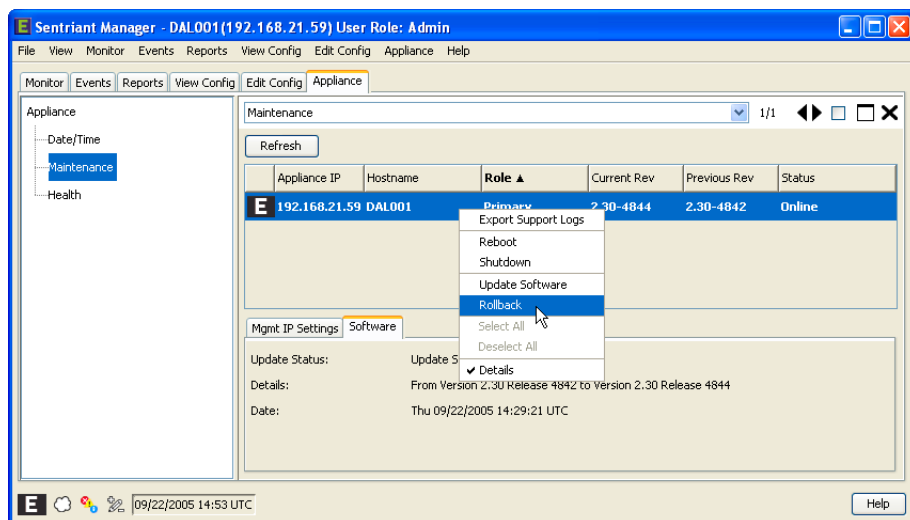


NOTE

When a rollback is performed, the Sentriant NG appliance will restart and no longer be monitoring network traffic.

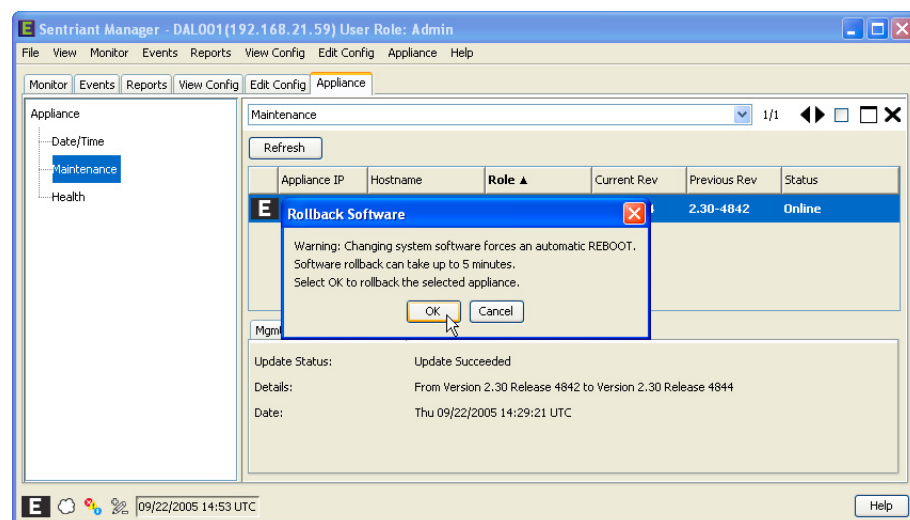
To rollback the software version on a Sentriant NG appliance:

- 1 From **Appliance > Maintenance** panel, select the Sentriant NG appliance.
- 2 Right-click to bring up the pop-up menu.
- 3 Select **Rollback**.

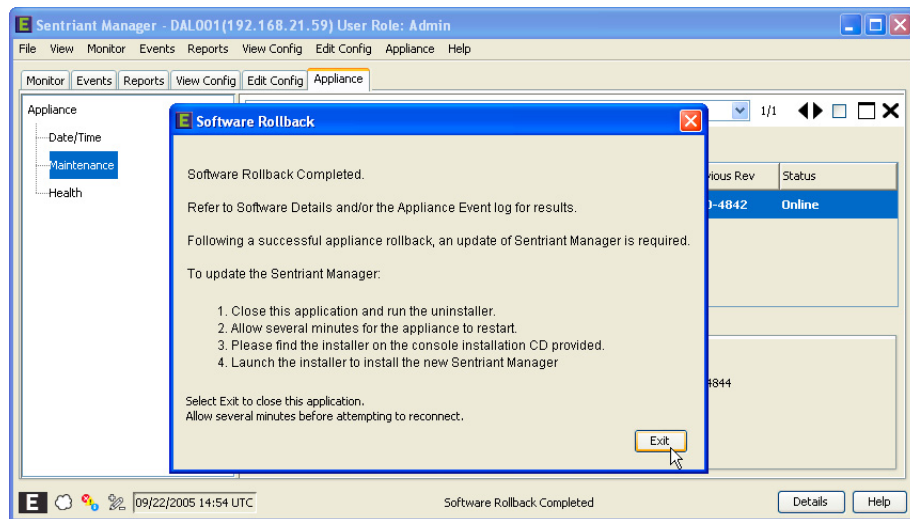


A dialog is displayed that gives the user a warning of the pending rollback changes.

- 4 Click **OK** to continue with the software rollback.



The Sentriant NG appliance will initiate a restart and perform the rollback. The Status column will be updated whether the rollback was successful or not. Sentriant NG Manager must be closed when you run the uninstaller. The previous version of Sentriant NG Manager then is reloaded using a web browser and connecting to the Sentriant appliance by entering the IP Address.

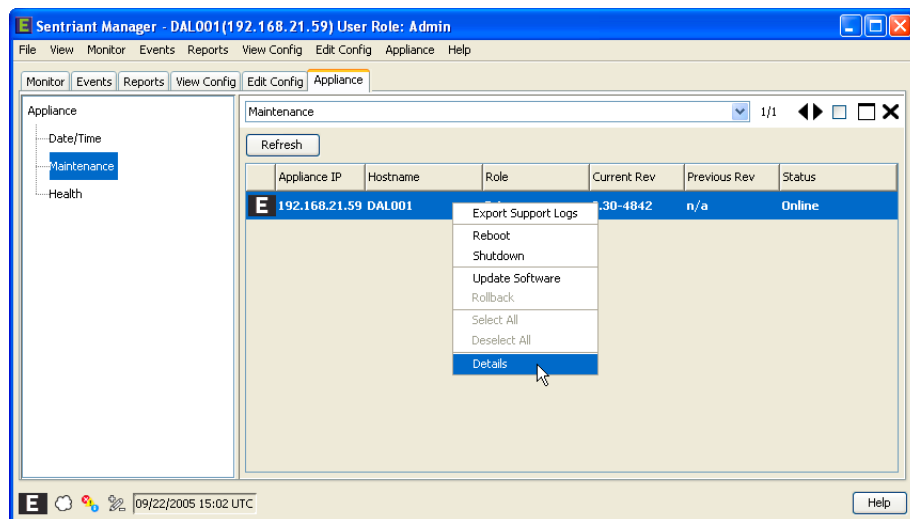


Details

Brings up the Details Panel which contains additional information about the selected Sentriant NG appliance.

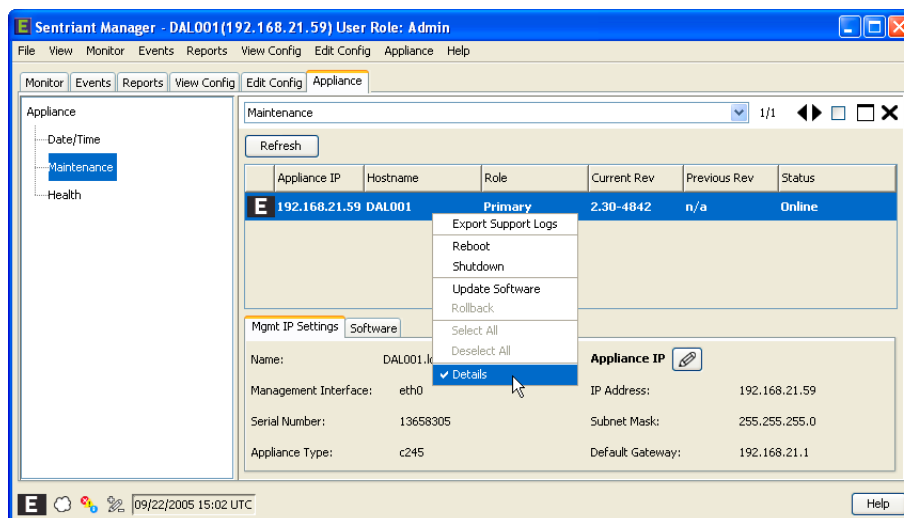
To display the Details Panel:

- 1 From **Appliance > Maintenance** panel, right-click the Sentriant NG appliance.
- 2 Select **Details**.



To hide the Details Panel:

- 1 From **Appliance > Maintenance** panel, right-click the Sentriant NG appliance.
- 2 Select **Details**.



SNMP Agent

By enabling the appliance SNMP Agent settings, clients can retrieve SOC information through an SNMP agent instead of using the SOC user interface.

To configure SNMP Agent settings:

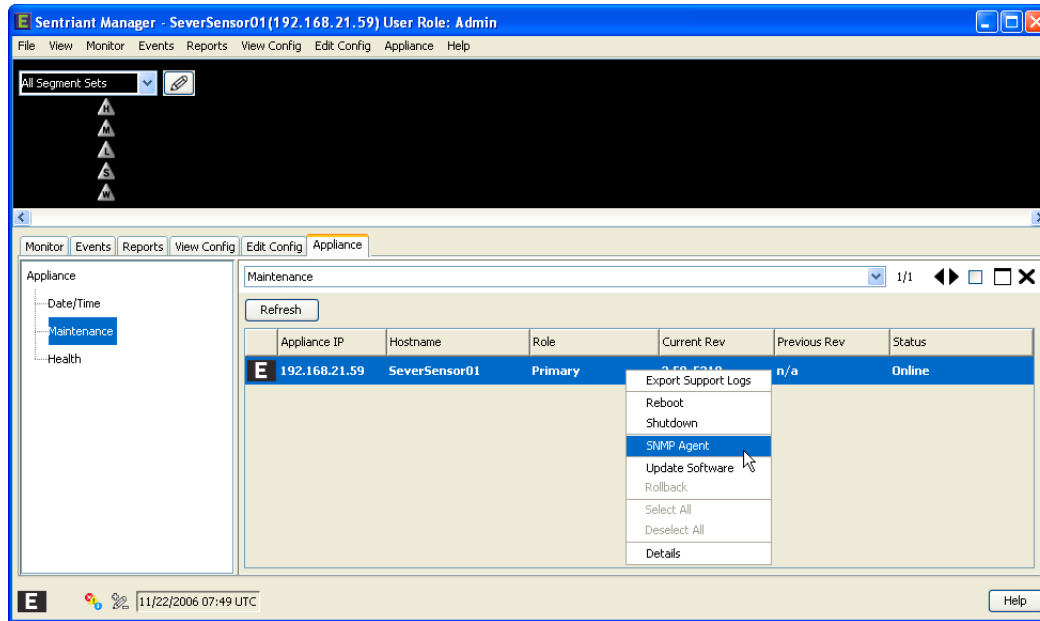
- 1 From the **Appliance > Maintenance** panel, right-click the Sentriant NG appliance.



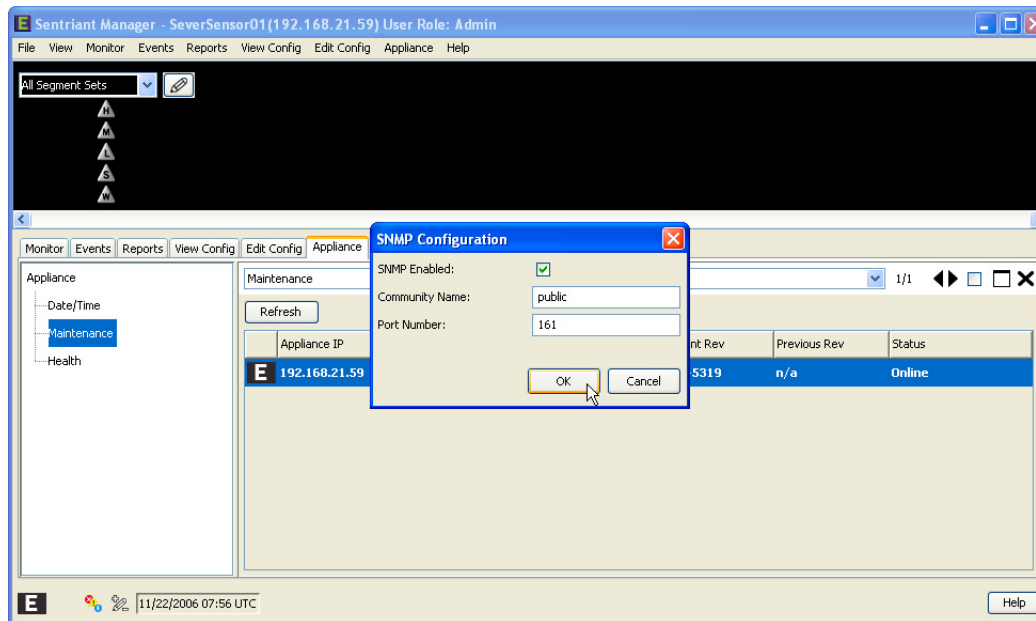
NOTE

The SNMP server must first be added to the access list using **Edit Config > Access > Clients** for the SNMP server to connect to the SNMP agent on the appliance.

- 2 Select **SNMP Agent**.



- 3 Click on the **SNMP Enable** check box.
- 4 Enter the **Community Name**. Default is **public**.
- 5 Enter the **Port** number of the SNMP agent. Default is 161.
- 6 Click the **OK** button.



Health

The purpose of the Health Panel is to display services and Sentriant NG appliance operations in real time giving the administrator a visual representation of problems with the Sentriant NG appliance. Services and appliance components monitored are:

Disk Management - Monitors individual disk partitions

Database Management - Monitors database, table, and archive statistics

Network Interface Management - Monitors each network interface link



NOTE

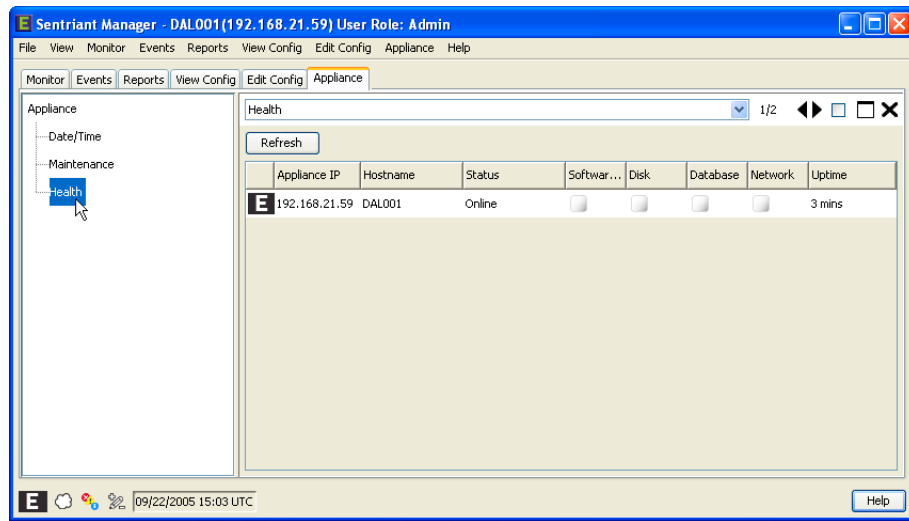
The Health Panel shows the current state of the appliance once the Health Panel opens. Click the Refresh button to refresh the appliance information if necessary.

To view the health of the Sentriant NG appliance:

From the **Appliance** tab, select **Health** from the navigation list. The following information is provided for the Sentriant NG appliance:

- The IP Address of the Sentriant NG appliance
- The Hostname given to the Sentriant NG appliance during initial configuration
- The status of the Sentriant NG appliance, which is either Online or Offline
- The status of Software Synchronization between the Sentriant NG appliance and workstations running the Management Console
- The status of the hard drives within the Sentriant NG appliance
- The status of the Sentriant NG appliance database
- The status of the network connections to the Sentriant NG appliance
- The cumulative time that the Sentriant NG appliance has been running since the last shutdown or reboot

Icons within the panel represent the status of each component, disk, database, network. If an issue is encountered, the icon will change from a normal status to either warning or error.



Details

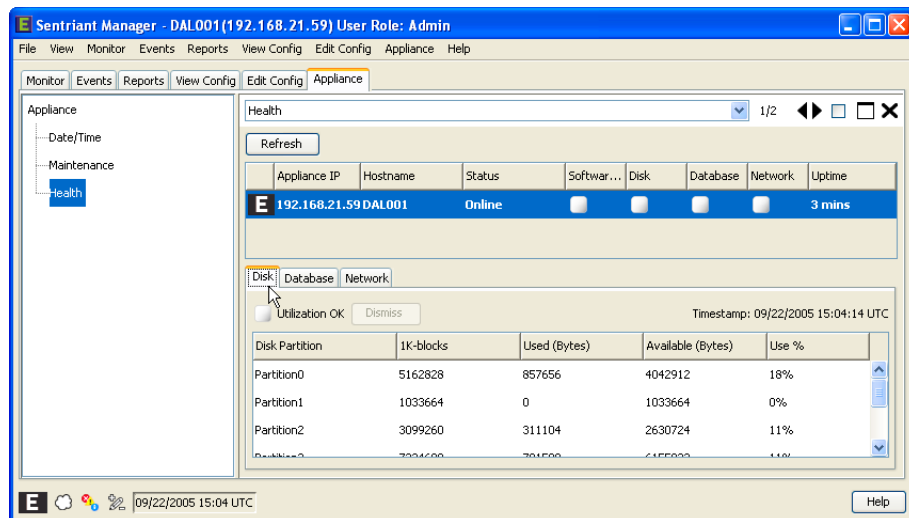
Details about the health, or working status, of the Sentriant NG appliance's hardware components and services can be viewed by either double-clicking on an appliance or right-clicking and selecting Details.

To view Disk details:

- 1 Double-click on the **Sentriant NG appliance** or right-click and select **Details**.
- 2 Click the **Disk** tab.

The Disk Details panel organizes information by Disk Partition. The information for each disk partition is:

- 1K-blocks - Total number of 1K-blocks for the partition
- Used (bytes) - Total number of used Bytes for the partition
- Available (bytes) - Total number of remaining Bytes available for the partition
- Use % - Percent of used space consumed on the partition

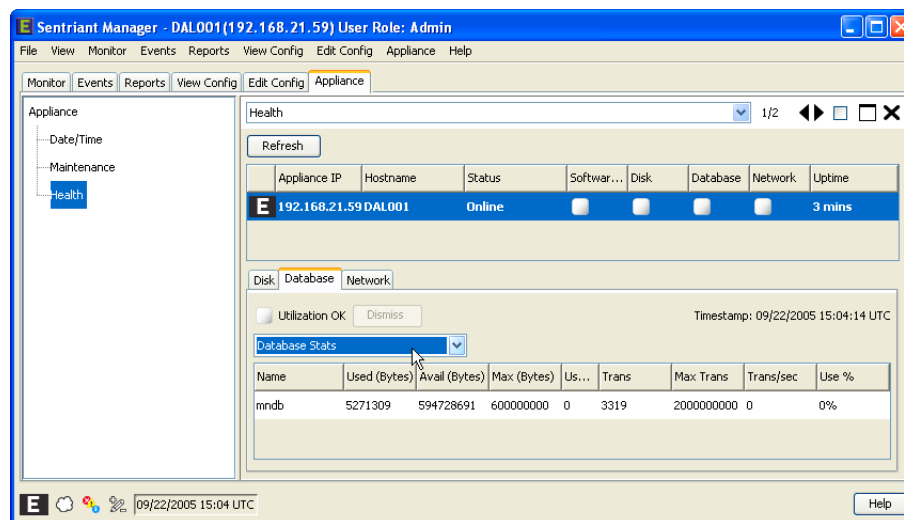


To view Database Statistics details:

- 1 Double-click on the **Sentriant NG appliance** or right-click and select **Details**.
- 2 Click the **Database** tab.
- 3 Select **Database Stats** from the drop-down list. (NOTE: this is the default view)

The Database Details panel organizes information by database name. The information for each database is:

- Name - Database name
- Used (Bytes) - Total number of used Bytes for the database
- Available (Bytes) - Total number of remaining Bytes available for the database
- Max (Bytes) - Size in Bytes of the database partition space
- Used Rate (kb/sec) - Number of kilobytes used per second for data transfer
- Transactions - Number of transactions completed since either last reboot or startup
- Max Transactions - Maximum number of transactions
- Transaction/second - Number of transactions completed per second
- Use % - Percent of used space consumed by the database

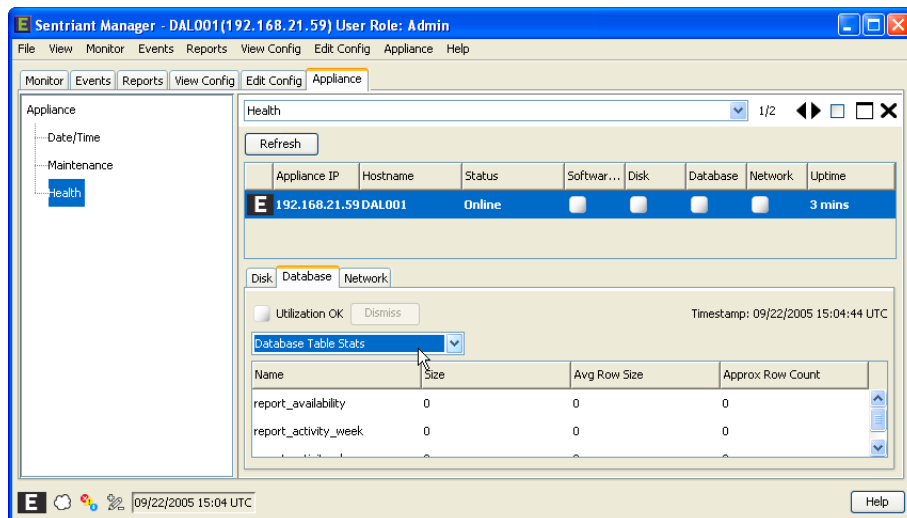


To view Database Table Statistics details:

- 1 Double-click on the **Sentriant NG appliance** or right-click and select **Details**.
- 2 Click the **Database** tab.
- 3 Select **Database Table Statistics** from the drop-down list.

The Database Details panel organizes information by database table name. The information for each database table is:

- Name - Table name
- Size - Current table size in Bytes
- Average Row Size - Average row size in Bytes
- Approximate Row Count - Current approximate rows per table

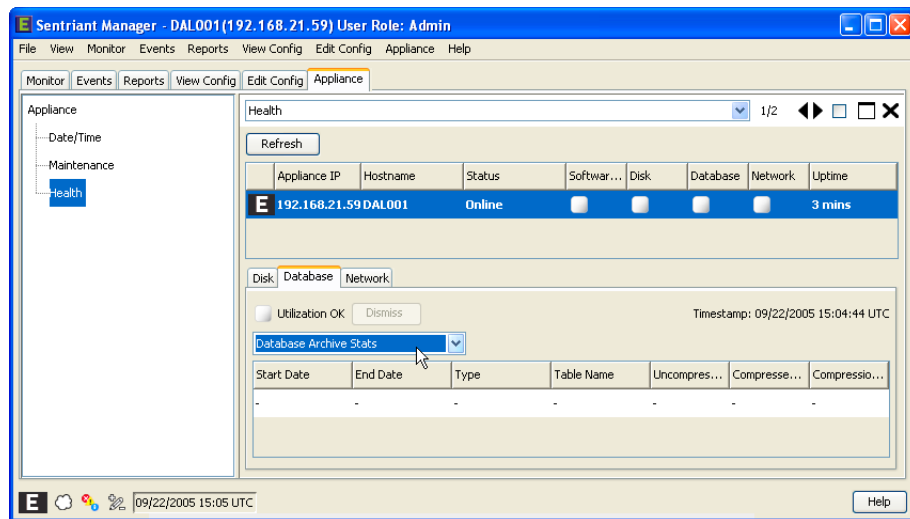


To view Database Archive Statistics details:

- 1 Double-click on the **Sentriant** or right-click and select **Details**.
- 2 Click the **Database** tab.
- 3 Select **Database Archive Statistics** from the drop-down list.

The Database Details panel organizes information by the date and time in UTC when the archive was performed. The information for each database is:

- Date - Date and time in UTC when the archive was performed
- Type - Type of archive performed
- Table Name - Name of the database table
- Uncompressed Bytes - Size of the database table before compression in Bytes
- Compressed Bytes - Size of the compressed database table
- Compression Type - Type of compression used for the data. Compression types are normal, fast, none

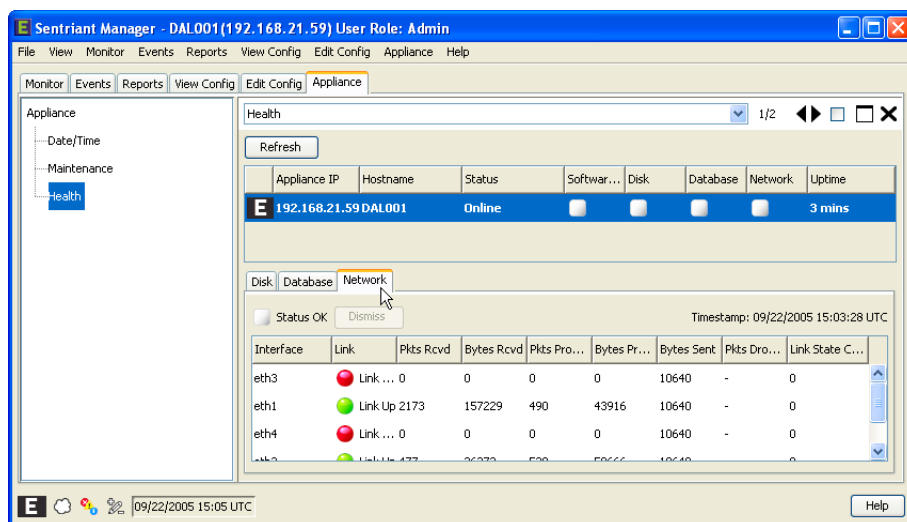


To view Network details:

- 1 Double-click on the **Sentriant NG appliance** or right-click and select **Details**.
- 2 Click the **Network** tab.

The Network Details panel organizes information by the Sentriant NG appliance's physical interface. The information for each interface is:

- Interface - Name of physical network interface
- Link - Link status, either “up” or “down”
- Packets Received - Number of packets received by the Sentriant NG appliance since either last reboot or startup
- Bytes Received - Total Bytes received by the Sentriant NG appliance since either last reboot or startup
- Bytes Sent - Total Bytes sent by the Sentriant NG appliance since either last reboot or startup
- Packets Dropped - Number of packets dropped by the Sentriant NG appliance since either last reboot or startup
- Bytes Processed - Total Bytes received and processed by the Sentriant NG since either last reboot or startup
- Link State Changes - Number of times the link status has changed, for example the link status went from link “up” to link “down” 3 times



Glossary

A

access client	Workstations that have Sentiariant Manager installed and that are accessing a Sentiariant NG appliance. Access clients, based on the type of user logged in, can perform Sentiariant NG appliance configuration actions, can monitor the fabric and perform manual and automatic mitigation activities.
admin	<i>System Administrator</i> - Extreme Networks Sentiariant NG appliance system user with full read/write access to system and application monitoring, display, and control commands.
alerts	The Sentiariant NG appliance can be configured to send alerts notifying the administrator that threat behavior has been detected. Sources or rules trigger alerts to be sent. Alerts can be sent via E-mails, SNMP Syslog, or a combination of all.
ARP Horizon	An Address Resolution Protocol (ARP) Horizon is the area of a network in which MAC addresses can be resolved. ARP is also commonly referred to as Broadcast Domain or segment when referring to the Sentiariant NG appliance. Network devices within an ARP Horizon communicate directly without passing traffic through a router.

B

bad packet	A packet that does not conform to the protocol standard has been detected indicating a possible attack.
broadcast domain	Also known as ARP horizon, a broadcast domain is the area of a network in which all network devices can communicate with each other without going through a router.

C

cloak	A patent-pending technique by which the Sentiariant NG appliance unilaterally controls and terminates a communications flow between two or more computers. Cloaking can be manually or dynamically invoked by the Sentiariant NG appliance when threats are identified or policy conditions violated.
--------------	---

C (Continued)

cloak all	Cloak All inserts itself into all communication paths that exist between all known used IP Addresses of the monitored network and removes threats from the communication stream, while other traffic is allowed. The source will remain cloaked until the configured threat time-out has been exceeded. At this time, the Sentriant NG appliance removes itself from the data path between all monitored addresses and threat sources, barring the existence of another threat that would not allow uncloaking.
cloak on demand	When Cloak is selected as the response to a threat, the Sentriant NG appliance initially inserts itself into communication paths for only the devices that have communicated with the threat and removes the communication stream. Traffic to/from other (non-threat) hosts will be permitted. Once the threat source is determined to no longer be a threat it can be Uncloaked so that communication is permitted within the Sentriant NG appliance's protected segments.
communication stream	The transmission and receiving of packets between two hosts.

D

deception	A special technique that is employed by the Sentriant NG appliance to mislead hackers by providing misleading data about the network. Deception uses configurable OS and IP personas to slow attackers.
detection	The screening and identification of network traffic for potential worms or viruses that may attack or infect hosts by the use of configurable rules. Rules are configured that look inside individual packets for suspicious behavior. If a rule is triggered, a mitigation action, or response, may be taken either automatically or manually.
dismiss	Command to dismiss a threat to a priority of watch. Threats with priority status of high, medium, low or suspect can be dismissed to a watch priority. The threat will remain a watch unless the threat triggers a rule with a higher priority level.
DNS	<i>Domain Name System</i> - An Internet service that translates domain names into IP Addresses.

E

escalate	To manually increase the priority status of a threat to a higher priority level. The priority level can be escalated from any priority to a higher priority by applying a configured rule to the threat. For example a low priority can be escalated to a high priority. The threat will remain at the higher priority until the rule times out. The threat, if still present, will return as the lower priority if it triggers a rule.
event viewer	The event viewer panel used to view and manage network activity events. The Events Viewer maintains logs about Sentriant NG appliance configuration, network activity events.

E (Continued)

exclude Exclude is used to fine tune IP Addresses and ports to be monitored when Include is used to monitor range(s) of IP Addresses. For example, if an IP Address falls within the Include IP Addresses that are used for network management purposes only, it may become necessary to exclude that IP Address to prevent erroneous threats. By adding the IP Address to the Exclude tables, it will not be monitored by the Sentriant NG appliance.

F

fabric Term used that covers the IP Addresses and traffic between the IP Addresses monitored by Sentriant NG appliance(s). A fabric may be made up of multiple switches, gateways, and Sentriant NG appliances of a WAN.

I

include Include allows the configuration of specific IP Addresses and ports to be monitored by the Sentriant NG appliance. IP Addresses and ports are added to a rule using a session profile that sets a single or range of source and/or IP Addresses and ports. When session profiles are added to a rule, only values that are in the session profile are monitored on the source segment. For example, if you wish to create a Too Many Protected Web Server rule where protected web server IP Addresses are 10.10.10.1 through 10.10.10.5 with one more at 10.10.10.19, then a session profile would have the following values:

Source IP - empty

Source Port - empty

Target IP - 10.10.10.1-5,19

Target Port - empty

If you only wanted to count the threats on port 80, then you would change the Target port to 80.

If no session profiles are entered, then by default all traffic will be included.

IP Address Also referred to as Internet Protocol Address. It consists of four 8-bit numbers (represented as integers) called octets. Most often, each part of the IP Address is a number between 0 and 225; however, the first number must be less than 224 and the last number cannot be 0. Networks using the TCP/IP protocol to route messages based on the IP Address of the destination. Connecting a private network to the Internet requires using registered IP Addresses (called Internet Addresses) to avoid duplicates.

M

MAC Address The low-level address consisting of a 48-bit hexadecimal number (12 characters) assigned to a device on an ethernet network. MAC addresses are resolved to IP Addresses via ARP. Each NIC is assigned a unique address at the factory.

M

MAC Validation	A process performed by the Sentriant NG appliance that validates the low-level address sent by a host consisting of a 48-bit hexadecimal number (12 characters) assigned to a device on an ethernet. Each NIC is assigned a unique address at the factory. In cases where IP Addresses are found to be spoofed as, the Sentriant NG appliance will trigger a rule that may either cloak, snare, or send decoy information based on the rule that is triggered.
management segment	The segment identified during Sentriant NG appliance configuration that will be used to manage and monitor the appliance.
manual escalation	The Sentriant NG appliance admin has chosen to manually respond to a specific source IP Address as a potential threat and change the threat priority to high, medium or low which will trigger a rule and configured mitigation actions.
masked source	When a threat is detected by the Sentriant NG appliance but the source of the attack cannot be immediately determined, the source is referred to as masked. This usually occurs during initial network segment startup when the Sentriant NG appliance has not yet <i>learned</i> all of the address mappings, or when a spoofed packet is sent through a gateway utilizing a protected IP Address.
monitor	Monitoring screens and tracks suspicious and potentially threatening network behavior across one or more network segments that are under the protection of the Sentriant NG appliance. Threat behavior can be monitored whether it originates from a source inside or outside of the Sentriant NG appliance's protected range.

N

native segment	The portion of an ARP Horizon or Broadcast Domain that is native to a switch and does not need Qtag identifiers since the IP Addresses are not broadcast as a VLAN.
network segment	The portion of an ARP Horizon or Broadcast Domain that is protected by the Sentriant NG appliance. Segments have multiple attributes necessary for proper operation that are configured using "Edit Configuration" for segments.
NMAP	A network scanning/mapping tool used to determine the network topology and type of network.
NTP	Network Time Protocol. A standard for synchronizing a user's system clock with the "true time" defined as the average of many high-accuracy clocks around the world.

O

observer	Extreme Networks Sentriant NG appliance system user with read-only access to the system and application controls.
-----------------	---

O

operator Extreme Networks Sentriant NG appliance system user with read/write access to all of the application monitoring and display commands but does not have access to network segment configuration and Sentriant NG appliance maintenance.

P

packet A piece of a message transmitted over a network. One of the key features of a packet is that it contains the destination address in addition to the data.

packet match A Sentriant NG appliance can be configured with packet match rules. The administrator can define a specific portion of the packet which must match a supplied data value. In defining the packet location, the admin must specify the packet base. The base is a well known, defined location in the packet (by protocol specification).

application A packet match rule specifying an application-based location indicates that the offset and data parameters should be applied starting at the end of the the Transport Header. This is typically considered the data portion of the TCP or UDP packet. In ICMP it marks the end of the ICMP control header and the beginning of the ICMP data. The application header extends to the end of the data packet.

data/mask A packet match rule that compares the contents or data of a packet (at the specified base/offset) with the user supplied data value. If a mask is specified, then the contents of the packet (at the specified base/offset) will first be logically AND'ed with the Mask value and the result will be compared to the data value.

frame A packet match rule specifying a frame-based location indicates that the offset and data parameters should be applied starting from the Frame header of the packet. Most commonly, the Ethernet header is stored within the Network portion of the packet.

match An administrator can configure whether packet match rules should trigger for packets that Match the defined parameters, or for packets that do not match the supplied parameters.

network A Packet Match rule specifying a network-based location indicates that the offset and data parameters should be applied starting from the Network header of the packet. Most commonly, the IP protocol header is stored within the Network portion of the packet.

offset For packet match rules, the administrator must first define a base from which an offset can be defined. This will describe the network header that should be inspected. The offset defines the number of bytes, into a specified header, that should be advanced before inspection begins. The offset value also provides a second field for input (after a '-'). If this field is populated, the Sentriant NG appliance will search the data packet, starting at the specified offset and end at the value provided in the second input field.

P (Continued)

receive	The admin can specify the direction in which packet match traffic should be inspected. If Receive is selected, then packets which are received by the source (as responses to a communication stream initiated by the source) are inspected to determine if the packet contents match the supplied parameters.
transmit	The admin can specify the direction in which packet match traffic should be inspected. When Transmit is selected, the packets which are transmitted by the source are inspected to determine if the packet contents match the supplied parameters.
transport	A packet match rule specifying a transport-based location indicates that the offset and data parameters should be applied starting from the Transport header of the packet. Most commonly, the TCP, UDP or ICMP protocol header is stored within the Transport portion of the packet.
personality	A personality is a set of open ports designed to emulate a particular OS. It is used to mislead source hosts when a query or probe is conducted. A personality can be configured as a Linux, Windows 98, Windows XP-based system, or a user-customized personality. Ports may be added to the personality that are watched for source host activity.
personality set	A personality set is made up of multiple personalities. The percentage of personalities sent to a host may be configured within a set. For example, a personality set may consist of Linux, Windows 98, and Windows XP. Each is set to 30 percent as a response with the remaining 10 percent set to vacant.
ping flood	A ping flood is an attempt to use Internet Control Message Protocol (ICMP)-based packets, (for example, to attempt a denial of service ping attack) to determine the layout of a network.
policy	A collection of configuration settings that are applied to a Segment Set that defines Sentriant NG appliance detection and response actions.
port scan	When a host on the network scans a specified number of ports on a single target that has been detected. This could indicate an attempt to determine what services are running on the scanned host.
protected range	The range of IP Addresses under the protection of a Sentriant NG appliance.

Q

Qtag	The Institute of Electrical and Electronics Engineers (IEEE) standard 802.1Q enables VLAN traffic to span many broadcast domains or switches. It does this by inserting a special <i>Qtag</i> that carries a VLAN identifier (VID) into each Ethernet frame. This tagged traffic carries VLAN membership information between switches, thus enabling a VLAN to span multiple switches.
-------------	--

R

response	The action taken by the Sentriant NG appliance to counter potential worms or viruses that may attack or infect hosts. Responses are triggered by rules or personalities.
rule	Rules are what drive the detection and response actions of the Sentriant NG appliance. Once a segment is configured and is being monitored by the Sentriant NG appliance, configurable rules are created to detect and respond to malicious network activity.
rule set	A collection of rules assigned to a Segment Set.

S

Segment Set	A Segment Set is a collection of segments that exhibit similar policy behaviors. For example, if a Segment Set is reserved for DHCP clients (laptops), then a set can be created containing all laptops within a segment and then parameters can be set for rules, deception distributions and modifiers. Creating segments is accomplished using the Segment Assistant.
slow scanning	A tactic employed by the Sentriant NG appliance specifically designed to significantly increase the time it takes for an external host to scan the monitored network, causing the attacker to consume time and resources. This feature is only enabled when deception is turned on and slow scan is part of a configured personality.
SMTP	<i>Simple Mail Transport Protocol</i> - A TCP-based application layer, Internet standard protocol for sending E-mail messages between servers. The Sentriant NG appliance uses it to send alerts and allow remote monitoring.
snaring	A Sentriant NG appliance uses a special technique to engage and hold TCP-based attacks, thus preventing them from spreading. Snaring ties up an attack thread so it cannot move to another computer, slowing or even stopping the attack. This feature is enabled when deception is turned on and if snaring is part of a configured personality.
SNMP	<i>Simple Network Management Protocol</i> - Industry standard network management protocol that is used to send alerts.
source	An IP Address that has originated traffic in a monitored network segment and attempts to communicate with a target.
SPAN port	<i>Switched Port Analyzer</i> - Mirrors network traffic from a switched segment onto a specified port for traffic monitoring purposes.
spoof count	The number of spoof IP Addresses sent from a computer or device. For example, a source IP Address of 1.1.1.2 has spoofed IP Addresses of 2.2.2.1, 2.2.2.2, 2.2.2.3 and 2.2.2.4 totalling four(4).

S (Continued)

spoof origin	The computer or location where a spoofed as IP Address or spoof packet originated. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a known computer by “spoofing” the IP Address of that machine.
spoof packet	A packet whose source IP has been changed but its MAC address remains constant.
spoof packets	Packets that are sent out from the local network but have a false source address. This could signal the presence of a virus, worm or a rogue gateway.
spoofed as	The address that was given as the false source of a spoof packet.
suspect	A suspect is a source which has communicated with a configurable number of Unused Hosts (the default is usually one). A suspect can be escalated to a Threat.
Syslog	A method of collecting message logs from many systems. Each system sends short text messages to a syslog recorder. The recording system may record these in any desired manner including writing them to a file, sending them on to other systems, and printing them out. The Sentriant Manager uses Syslog for alerting users of activities on Sentriant NG appliances.

T

target	The host or workstation that a source host attempts to communicate with.
too many externals	A local system on the network is contacting a large number of external hosts. This could signal the presence of a virus or worm.
too many unprotected	A local system on the network is contacting a large number of remote hosts. This could signal the presence of a virus or worm.
too many used	Too many used (i.e., <i>real</i>) IP Addresses have been contacted by a single host. A used address is an address that has a real machine associated with it.
too many unused	The Sentriant NG appliance has detected a source attempting to contact too many unused IP Addresses.

U

Universal Time	A time scale that is the basis for the worldwide system of civil time. Referred to as <i>Coordinated Universal Time</i> (abbreviated UTC), this time scale is maintained by highly precise atomic clocks located around the world. UTC is accurate to a nanosecond per day.
-----------------------	---

U**used**

A host or workstation using an IP Address within the protected range of a Sentiariant NG appliance. It responds to Address Resolution Protocol (ARP) requests and sends traffic on the network.

V**VLAN**

Virtual Local Area Network - A logical, or administratively configured, LAN or broadcast domain that is defined by software rather than by fixed, physical port connections.

W**watch**

A watch is a source that has communicated within (or itself resides within) the protected range(s) of the Sentiariant NG appliance.

A

- access, 119, 131
- access activity, 86
- access client, 120
- across all segments, 43
- across all segments action, 47
- add a protected range of IP addresses to the segment, 218
- add as gateway, 80
- add gateway(s) to the segment, 217
- add IP addresses to never tables, 242
- Adding Switches, 252
- address space actions, 79
- admin, 119, 138
- alerts, 119, 121, 131, 143
- Appliance, 252
- application, 333
- ARP horizon, 329
- associate a personality set, 240
- associate a rule set, 239
- associate a segment to a segment set, 238
- associating rule and personality sets, 239
- associating with a segment set, 189

B

- bad packet, 329
- broadcast domain, 128, 329

C

- change segment name, 202
- Client Configuration, 120
- cloak, 241, 278, 329
- cloak all, 330
- cloak on demand, 224, 330
- communication stream, 102, 330
- create a segment set, 236
- creating clients, 141
- creating personalities, 154
- creating personality sets, 158
- creating user accounts, 139

D

- data/mask, 333
- date/time panel, 301

- deceive, 241
- deception, 119, 124, 131, 152, 330
- deception decoy, 77
- deception exclude, 77
- decoys, 124, 220
- Destinations, 121
- detection, 128, 255, 330
- disable segment ports, 209
- disengage and engage, 44
- display the fabric details panel, 320
- DNS, 330

E

- edit alerts, 281
- edit detection properties, 259
- edit number of property, 261
- edit packet match property, 266
- edit priority, 274
- edit response properties, 274
- edit response time out, 279
- edit response type, 278
- edit segment deception, 220
- edit source and target IP types, 264
- edit spoof properties, 271
- edit time out period, 276
- edit time period, 263
- event viewer, 330
- exclude, 77, 255, 331
- exclude from Rule responses, 241
- exclude IP address, 79
- exclude IP address tab, 286
- export log files from a Sentriant NG appliance, 309

F

- fabric, 301, 331
- frame, 333

G

- gateway/router, 78

H

- host, 256

I

- include, 77, 331
- included IP addresses, 282
- Initial Segment Configuration, 131
- IP address, 331
- IP address lookup, 82, 102
- IP Address Select/Deselect All, 83
- IP Sets, 126

L

- last traffic, 62
- look up a target's IP address, 73
- look up IP address on the web, 48, 102
- look up source IP address, 50

M

- MAC address, 62
- MAC validate, 241
- match, 333
- modify subnet and mask, 214
- monitor, 332

N

- named items, 119, 125, 131
- network, 333
- Network Activity, 27
- Network Activity Details, 95
- Network Activity Events Actions, 102
- network segment, 111, 131, 220, 255
- network time protocol, 301
- network topology, 119, 127, 131
- never cloak, 120
- NMAP, 332
- NTP, 332
- number of hosts, 261
- number of packets, 261
- number of ports, 261

O

- observer, 332
- offset, 333
- omitting communication streams, 243
- operator, 333
- overall session activity report, 113

P

- packet, 99, 256, 333
- packet match, 261
- pairing ports, 210

- per-segment suspect and threat trend report, 114
- personalities, 124
- personality, 62, 334
- personality set, 124, 239, 334
- policy, 119, 128, 131, 334
- port per host, 256
- Port Sets, 126
- primary, 206
- protected range, 218

Q

- Qtag, 334
- querying address space, 78
- querying IP Types, 25
- querying sources, 46
- querying targets, 71

R

- reboot a Sentiariant NG appliance, 310
- receive, 334
- refresh sources panel, 27
- reset candidate flags, 81
- response, 255, 335
- response - cloak and uncloak, 55
- responses, 42
- rollback the software version on a Sentiariant NG appliance, 318
- rule set, 290, 335
- rules, 255, 335

S

- secondary, 206
- segment set, 131, 176, 236, 335
- select and deselect Sentiariant NG appliances, 320
- Selecting and Deselecting Sources, 58
- set packet contents, 267
- set the source type, 273
- set the spoof as count, 272
- set the threat priority, 274
- set the threat ranking, 275
- setting deception, 137
- setting deception mode, 191
- setting gateways, 186
- setting protected ranges, 188
- setting rules, 135
- setting up rule sources, 144
- show event stream, 102
- Show/Hide Details Panel, 85
- shutdown a Sentiariant NG appliance, 312
- slow scan mode, 155
- SMTP, 143, 146, 281, 335

- snaring, 155, 335
- SNMP, 143, 335
- source, 335
- source actions, 44
- source IP list - IP look up, 64
- source IP list - response, 69
- source IP list - threat, 66
- Sources, 122
- SPAN port, 206, 210
- Specifying Report Parameters, 112
- spoof, 256
- start monitoring a segment, 134
- suspect, 127, 336
- SysLog, 143
- system availability report, 112
- System Overview Report, 111

T

- target, 336
- targets details, 61
- threat - escalate and dismiss, 51
- threats, 40, 241
- to add decoys, 221
- to create SNMP destinations, 148
- to create SysLog destinations, 150
- to escalate a threat, 66
- to uncloak a cloaked source, 70
- to view a source's all target counts, 34
- to view a source's spoof as data, 35
- to view a source's spoof origin data, 34
- to view a source's target counts, 96
- to view a source's threats, 40
- to view packet count, 39, 99
- to view the IP addresses of sources communicating with targets, 63
- to view the IP addresses of targets affected by the source, 108
- to view the ports that a source communicated with, 36, 97
- to view the responses to source threats, 42
- too many externals, 336
- track, 278
- traffic, 256
- Traffic Sets, 126
- transmit, 334
- transport, 334
- trend chart, 73

U

- unpairing ports, 213
- update Sentriant NG appliance software, 314
- used, 337

- User Configuration, 119
- using the sources panel, 28
- using the targets panel, 59

V

- verify software version, 314
- view affected targets, 31
- view database archive statistics details, 326
- view database statistics details, 324
- view database table statistics details, 325
- view disk details, 323
- view Network Activity events, 93
- view network details, 327
- view segments, 25
- view source details, 33
- view Source IP Addresses, 28
- view source IP list, 62
- view the health of the Sentriant NG appliance, 322
- viewing address space details, 76
- viewing target IP addresses, 59
- VLAN, 128, 337

W

- watch, 337

