OmniVista SafeGuard Manager

Release 3.0

Administration Guide

PART NUMBER: 005-0034 REV A1
PUBLISHED: MARCH 2007

ALCATEL-LUCENT
26801 WEST AGOURA ROAD
CALABASAS, CA 91301 USA
(818) 880-3500

WWW.ALCATEL-LUCENT.COM

Alcatel-Lucent Proprietary

Contents

Preface

Chapter 1: Getting Started

Chapter 2: Installation and Setup

Chapter 3: General Navigation

Chapter 4: Visualization

Chapter 5: Device Configuration

Chapter 6: Query and Reports

Chapter 7: Managing the Server

Chapter 8: Audit Logs and Statistics

Index

Preface

In this preface:

About This Guide

This guide describes the OmniVista SafeGuard Manager command center features, including how to use and navigate through different views. This guide also provides detailed installation procedures for the server and client.

Intended Audience

The OmniVista SafeGuard Manager Administration Guide is for experienced network administrators who are responsible for installing, configuring, and maintaining the Alcatel-Lucent devices and OmniVista SafeGuard Manager command center.

Guide Overview

The information in this guide is separated into several chapters to make it easy for you to find exactly what you are looking for.

Chapter	Description
Chapter 1, Getting Started	Provides installation procedures and a brief overview of the key features of the OmniVista SafeGuard Manager command center.
Chapter 2, Installation and Setup	Provides detailed installation and setup instructions.
Chapter 3, General Navigation	Describes different navigation techniques such as, search and sorting.
Chapter 4, Visualization	Describes the configuration of dashboards and the checking of user activity, health of the host system, violation histories, and other network activity.
Chapter 5, Device Configuration	Provides instructions for configuring device objects and templates.
Chapter 6, Query and Reports	Describes the creation, printing, and viewing of reports on network traffic and incidents.
Chapter 7, Managing the Server	Describes client settings, user accounts, and user authentication. Additionally, it describes server settings: how to restore, purge, or back up the database and set up the OmniVista SafeGuard Manager mailer so email notifications can be sent on Malware events and reports.
Chapter 8, Audit Logs and Statistics	Provides audit log information and device and server health and statistics.

Conventions Used in This Guide

This document uses the following conventions:

Italic	Italics are used the first time a glossary term is introduced, for the titles of books, and for menu items.
■ Bulleted lists	Bulleted lists designate items of equal importance.
1 Numbered lists	Numbered lists designate a specific sequence of steps required to complete a procedure.
Boldface type	Boldface type is used for button names.
`Code`	Code excerpts and command line sequences are shown in this type face.
`Ellipsis....`	Is used in code and argument syntax to indicate that inconsequential information is not shown.

NOTE: Means readers pay special attention to the information. Notes contain helpful suggestions or references to materials covered in the guide.

CAUTION: Informs users to be careful of situation described in Cautions. In this situation, you could do something that could result in deletion of information or damage of equipment.

WARNING: Informs users of safety conditions. In this situation, you could do something that could result in bodily injury or electric shock.

Related Documentation

- *OmniAccess SafeGuard Controller Installation Guide*

  Describes the OmniAccess SafeGuard Controller. The guide provides detailed installation instructions and technical specifications for the OmniAccess SafeGuard Controller.

- *OmniAccess SafeGuard OS Administration Guide*

  Provides concepts and configuration instructions for the major features of OmniAccess SafeGuard OS and its supported products, which includes End Point Validation (EPV) the integral component for using ICS.

- *ICS Dissolvable Agent for SafeGuard Administration Guide*

  Describes how to configure the Integrity Clientless Security (ICS) module of the Alcatel-Lucent Network Admission Control (NAC).

Additional Resources

Alcatel-Lucent publishes documents for Alcatel-Lucent customers at:
www.Alcatel-Lucent.com

chapter

1 Getting Started

This section includes the following:

Overview

The OmniVista SafeGuard Manager command center provides centralized and easy-to-use management of one or more Alcatel-Lucent devices, enabling network administrators to perform basic configuration, management, and monitoring of several devices in a single interface. OmniVista SafeGuard Manager provides the foundation for gaining usage awareness and flagging network security incidents by users; it also enables global policy configuration with the ability to take real-time action from the control panel. Powerful predefined reports provide clear views on enterprise network health and user actions.

Unlike traditional network management systems that report at the MAC or IP level, OmniVista SafeGuard Manager maps events to the network users. A user is identified by the SafeGuard Controller enforcement devices during the authentication phase. This user ID is then bound to the MAC and IP addresses of the computer, such that, that any future communication from that machine is bound to the user ID. This allows an administrator to identify any user incidents or identify the location of the violating machine.

User-based features combined with drillable data navigation enable OmniVista SafeGuard Manager to communicate business information simply at a top level, yet the details are only a click away. This real-time correlation of network incident or awareness events to the user saves hours of manual association and custom scripting.

OmniVista SafeGuard Manager 3.0 supports the following:

- Devices: OAG 1000, OAG 2400, OAG 4048x
- SafeGuard platform: SafeGuard software release 3.0

Key Features

The OmniVista SafeGuard Manager command center Release 3.0 supports the following features:

- Device Configuration—Allows you to manage devices with detailed views of devices and physical ports. Also keeps your network under a single management system allowing you to select actions on the canned policies and push down to devices.
- User Authentication—In addition to local database authentication, OmniVista SafeGuard Manager users can be authenticated using an external RADIUS server.
- Visualization Filters—Allows you to set up visualization filters such that you can selectively view events based on VLAN ID, application type, or user role.
- VLAN Filters—Allows you set up visualization filters based on VLAN IDs.
- Drillable Database Query—Allows you to execute pre-defined and custom queries.

- Policy Creation Using Flows—Allows you to create policy filters from data available in an application flow.
- CSV/HTML Report Generator—Allows you to create customized reports with server-side Scheduler; these reports can be e-mailed and printed easily.
- Real-time Incident Dashboard—Displays total number of users, authenticated and unauthenticated, device health, and policy, posture, and malware incidents. Also displays incidents for unauthenticated users and top user roles with incidents/incident counts. Administrators can remove offending machines off the network and revoke user privileges by de-authenticating users.
- Real-time User Incident Dashboard—Displays authentication failures by users, users with policy, posture, and malware incidents, and top user roles with incidents.
- Real-time Awareness Dashboard—Displays top 10 user sessions by bandwidth, top 10 destinations, top 10 Web Sites, top 10 applications by flow count, bottom 10 applications by flow count, or top 10 applications by bandwidth.
- Audit Logs—Provides logs that indicate who did what and when and on which device. These logs are for user and device operations and can be helpful for auditing purposes.
- Device and Server Health—Allows you to collect, view, and store statistics relating to device or server health. These statistics are helpful in analyzing each device’s performance and its current connections.
- Software Upgrade—Allows you to upgrade the software version on the device.
- File Distribution—Allows you to manage files in a repository and distribute as necessary.
- Reboot—This feature allows you to reboot the selected device(s).
- Online Help—The online help feature is available using the F1 function key.

Getting Started

The OmniVista SafeGuard Manager command center has client and server components. The server runs on a Windows server system, and the client runs on a Windows client system using Internet Explorer. The client can be deployed directly from the server using the Java Web Start technology.

To quickly get started with OmniVista SafeGuard Manager, you need the following:

- *System Requirements*
- *OmniVista SafeGuard Manager Client Requirements*
- *Starting the Server*
- *Starting the Server*
- *Installing the Client*
- *Logging In to the Client*
- *Dashboards*
- *Menus*
- *Adding a Device*

System Requirements

The following requirements are for OmniVista SafeGuard Manager server installation. The software installation enforces these requirements, and exits you out of the installation if the minimum requirements are not met. For more installation information, see *Installing the OmniVista SafeGuard Manager Server*.

- 2-GB RAM
- 60-GB free disk space

NOTE: The disk space is allocated as 5GB for installation and 55GB for data. Installation needs to be performed using the C drive and this drive should have a minimum of 5GB free space; however, data can be saved to the D drive that should have a minimum of 55GB space.

- Microsoft Windows Server 2003 (Enterprise, Standard, or Web Edition)

NOTE: Microsoft Windows Server 2003 should have SP1 installed. Alcatel-Lucent supports 32 bit versions only.

- 2.8-GHz processor speed
- 2 processors

NOTE: The appliance that ships from Alcatel-Lucent meets all these requirements.

OmniVista SafeGuard Manager Client Requirements

The OmniVista SafeGuard Manager client can be run on most Windows systems. Minimum requirements are:

- One of the following Windows platforms:
  - Microsoft Windows Server 2000
  - Microsoft Windows Server 2003 (Enterprise or Standard)
  - Microsoft Windows XP Professional
- 2.8-GHz single CPU
- 512-MB RAM
- 2-GB hard disk
- Internet Explorer 6.0 or higher
- Screen resolution of 1024 x 768 pixels
- Internet connectivity to install Java Web Start

Starting the Server

When you boot up the OmniVista SafeGuard Manager appliance, the OmniVista SafeGuard Manager server is started automatically. However, if you upgraded the software version or re-installed the software, you must manually start the server. For more information on installing, upgrading, or uninstalling, see *Installation and Setup*.

To manually start the server:

1 Use the Windows shortcut from the Start menu, *Programs > OmniVista SafeGuard Manager > Start Server*.

A GUI window displays. This window performs checks to verify that all ports needed for the server are available, starts all the server components as Windows services, and informs you when the server is ready.

2 Click **OK** to close the window.

The OmniVista SafeGuard Manager server runs in the background. If you now reboot the system, the server should come up automatically.

Installing the Client

The OmniVista SafeGuard Manager client is based on Java Web Start technology, allowing you to install the client automatically with a single click over the network. For more information on client installation, see *Installation and Setup*.

To install the client:

1 Launch Internet Explorer.

2 Access the OmniVista SafeGuard Manager system by typing the following URL:

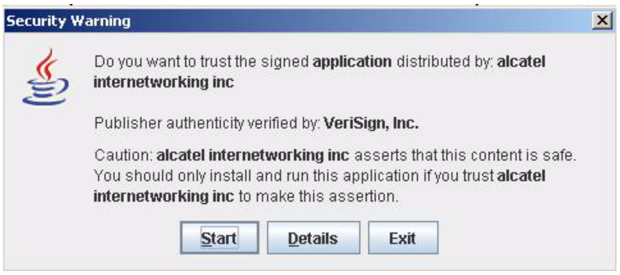
```
http://<server-ip-address>
```

If the client does not have Java Web Start already installed, you are prompted to install Java Runtime Environment (JRE). Follow the on-screen prompts using the default options to install JRE. Java Web Start is included with JRE.

NOTE: The automatic installation of JRE requires ActiveX controls to be enabled on your Internet Explorer. If ActiveX controls are not enabled, a "*download Java Web Start*" link displays. Internet Explorer also alerts you if ActiveX controls are not enabled and gives you an option to enable ActiveX controls. You can choose to enable ActiveX controls for automatic installation of Java Web Start, or you can download JRE version 1.5.0 by going to the download link. If you manually install Java Web Start, repeat Step 2.

After Java Web Start is installed, the OmniVista SafeGuard Manager client code is downloaded and installed. Java Web Start displays a dialog box informing you that the application is authored by Alcatel-Lucent and needs some privileges on your client system (*Figure 1*).

Figure 1 Security Warning



Security Warning

Do you want to trust the signed **application** distributed by: **alcatel internetworking inc**

Publisher authenticity verified by: **VeriSign, Inc.**

Caution: **alcatel internetworking inc** asserts that this content is safe. You should only install and run this application if you trust **alcatel internetworking inc** to make this assertion.

3 Click **Start**. A prompt appears asking if you want to create a shortcut on the desktop.

4 Select **Yes** to create a shortcut. If you select No, you can still launch the client using the URL from Step 2.

The client launches. See *Logging In to the Client* for information on logging procedures.

NOTE: Every time the OmniVista SafeGuard Manager client is launched, it compares its version with the OmniVista SafeGuard Manager server. If the client version is different than that of the server, the client automatically updates itself from the new version of the server.

Logging In to the Client

To log in to the client:

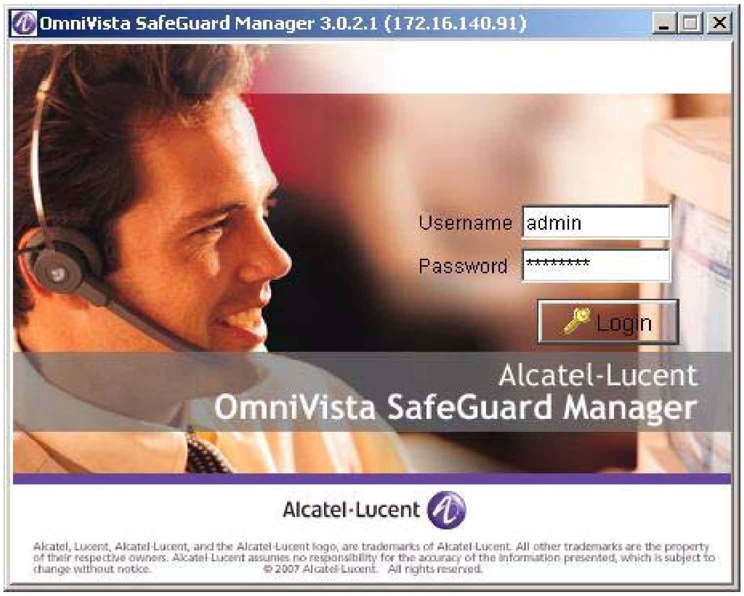
1 Launch the client using either of the following methods:

- — Double-click on the shortcut that was created on your desktop when you first installed the client.
- — Invoke from Internet Explorer by typing the URL (http://ip-address-of-OmniVistaSafeGuardManager-server).
- — Launch from the start menu using start menu > OmniVista SafeGuard Manager > Client

NOTE: If you are launching the client from the server for the first time, you might be prompted to install certain applications. See *Installing the Client* for more information.

The Login screen appears (*Figure 2*).

Figure 2 OmniVista SafeGuard Manager Client Login Screen



OmniVista SafeGuard Manager 3.0.2.1 (172.16.140.91)

Username admin

Password *********

Alcatel, Lucent, Alcatel-Lucent, and the Alcatel-Lucent logo, are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice. © 2007 Alcatel-Lucent. All rights reserved.

2 In the Username field, type **admin** as the default user.

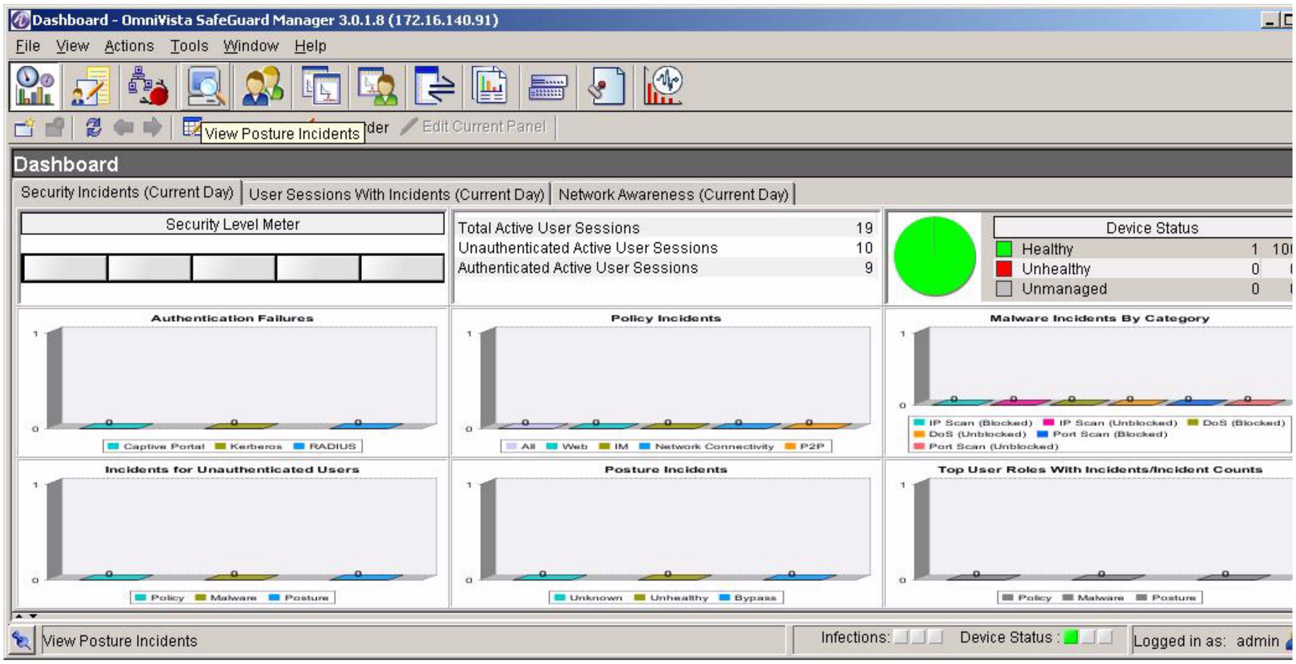
3 In the Password field, type **password**.

4 Click **Login**. If you are logging in for the first time to the OmniVista SafeGuard Manager server, the Alcatel-Lucent License Agreement will be displayed. You must accept it to use OmniVista SafeGuard Manager.

NOTE: The license agreement is a one-time acknowledgement for each server and is not displayed for this client or any other client or this server.

The client is successfully launched, and the OmniVista SafeGuard Manager command center panel displays (*Figure 3*).

Figure 3 OmniVista SafeGuard Manager Dashboard



Dashboard - OmniVista SafeGuard Manager 3.0.1.8 (172.16.140.91)

Dashboard

Security Incidents (Current Day) | User Sessions With Incidents (Current Day) | Network Awareness (Current Day)

Total Active User Sessions	19
Unauthenticated Active User Sessions	10
Authenticated Active User Sessions	9

Device Status		
🟩 Healthy	1	10
🟥 Unhealthy	0	
□ Unmanaged	0	

View Posture Incidents

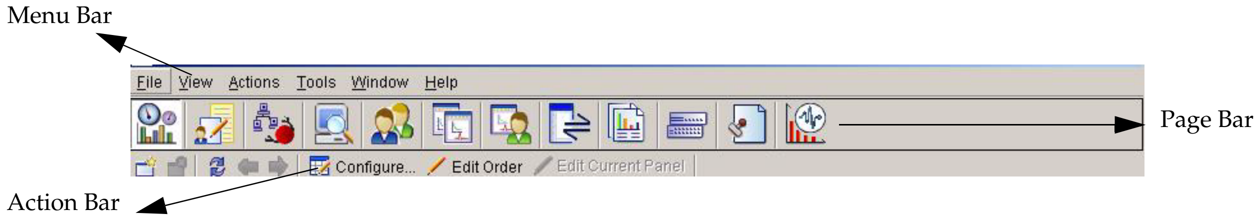
Infections: Device Status : Logged in as: admin

Navigation

When you log into the OmniVista SafeGuard Manager command center, a navigation panel displays that allows you to access the various features by simply clicking a button or using a menu item. You can navigate the OmniVista SafeGuard Manager command center using the following:

- Dashboards
- Menu Bar
- Page Bar
- Action Bar

Figure 4 OmniVista SafeGuard Manager Navigation Elements



Dashboards

The OmniVista SafeGuard Manager command center has three dashboards that provide a high-level network summary. These dashboards can be used to further investigate either actionable user incidents or informational and user traffic patterns. For more information on how to use the visualization features of the dashboard, see *Visualization*. The three dashboards are:

- Incidents—Displays total number of users, authenticated and unauthenticated, device health, and policy, posture, and malware incidents. Administrators can remove offending machines off the network and revoke user privileges by de-authenticating users.
- User Incidents—Displays authentication failures by users, users with policy, posture, and malware incidents, and top user roles with incidents.
- Network Awareness—Displays various application usage patterns and statistics for active users, such as top 10 user sessions by bandwidth, top 10 user sessions with most blocked incidents, top 10 destinations, top 10 Web Sites, and so forth. The modules are automatically refreshed every 5 minutes.

Menus

You can access the OmniVista SafeGuard Manager features by selecting menu commands that are located in the menu bar, which is the toolbar located at the top of the screen (*Figure 4*).

Page Bar

The OmniVista SafeGuard Manager Page Bar icons allow you to access the various features of OmniVista SafeGuard Manager while retaining the context as much as possible. The Page Bar icons provide a quick single-click action that is synonymous with the menu items:

Table 1 Navigating within OmniVista SafeGuard Manager

Page Bar Icon	Menu Sequence	Key Sequence	Displays View	Description
	View > Go To > Dashboard	Ctrl + 0	Dashboards	Displays Incidents, User Incidents, and Global Awareness dashboards.
	View > Go To > Policy Incidents	Ctrl + 1	Policy Incidents	Displays all policy incidents.
	View > Go To > Malware Incidents	Ctrl + 2	Malware Incidents	Displays all malware incidents.
	View > Go To > Posture Incidents	Ctrl + 3	Posture Incidents	Displays all posture Incidents.
	View > Go To > Users	Ctrl + 4	Users	Displays network activity per user.
	View > Go To > Applications	Ctrl + 5	Applications	Displays network activity per application.
	View > Go To > Application Instances	Ctrl + 6	Application Instances	Displays the user bandwidth usage for each user, application type, destination port, and destination IP address.
	View > Go To > Application Flows	Ctrl + 7	Application Flows	Displays application flows for all application.
	View > Go To > Reports	Ctrl + 9	Reports	Allows you to create and view reports on network traffic patterns and anomalies.

Table 1 Navigating within OmniVista SafeGuard Manager *(continued)*

Page Bar Icon	Menu Sequence	Key Sequence	Displays View	Description
	View > Go To > Config Management	Shift + 1	Config Management	Enables you to manage Alcatel-Lucent devices, view inventory, and perform minimal configuration of the device system and ports.
	View > Go To > Audit Logs	Shift + 2	Audit Logs	Displays log entries that are relevant for auditing purposes.
	View > Go To > Statistics	Shift + 3	Statistics	Displays device and server health statistics.

When you click on any of the Page Bar icons, a table view is displayed that shows the Navigation Tree on the left-side, the contents in the upper-half of the screen and details for the selected object in the lower-half of the screen. The Navigation Tree and the Action Bar change based on the action task selected in the Page Bar.

Action Bar

The Action Bar allows you to access commands, as you need them, by a simple click of a button.

To use the Action Bar, do any of the following:

- To choose a command from the bar, click the command button or *Actions* > command
- To view what a command does, position the mouse over the command button to see its tooltip.
- To close the Action Bar, choose *View* > *Toolbars* > *Actions*.

Viewing Tips

The following tips expedite your navigation through the OmniVista SafeGuard Manager Manager panels and windows:

- Buttons in the Action Bar are used to execute actions. Select a row and then click the action button. If an action is not applicable for the selected row, the corresponding button is disabled.
- In the table views, some information about the table size is displayed above the table (the number of rows) and the alarm and infection status is displayed in the status bar below the table.
- You can search the data from the visualization database using filters. To view filters, click **Find** in the Action Bar. A free-form search field is displayed where you can type keywords to search data displayed in table views. To search the data from the database, click **Database Search**. A new search and sort header opens at the top of the table header. Click on the search bar of the column to specify the filtering criteria for that column. Click on the sort bar for the column to specify the sort criteria for that column. You can select multi-column sort order. After you have finished setting filters for one or more columns, click **Refresh** to see the new results. To clear all filters, click **Clear**. For more information on how to use the search and sort features, see *General Navigation*.
- Select a row to view detailed information on the selected row.
- Right-click on a row to display applicable actions.

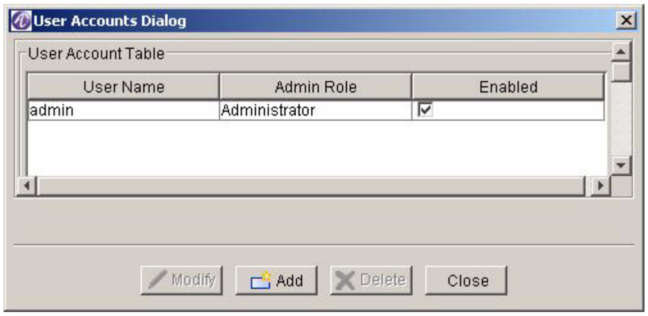
Modifying Your Password

The Account Management feature of OmniVista SafeGuard Manager allows an administrator to perform basic modifications to user accounts, such as adding users, changing passwords, and configuring dual-admin.

To modify your password:

1 Select *Tools* > *OmniVista SafeGuard Manager Users* > *User Accounts...* The Account Management window (*Figure 5*) displays.

Figure 5 Account Management Window



User Name	Admin Role	Enabled
admin	Administrator	☑

2 Select one of the following Admin Login Setting:

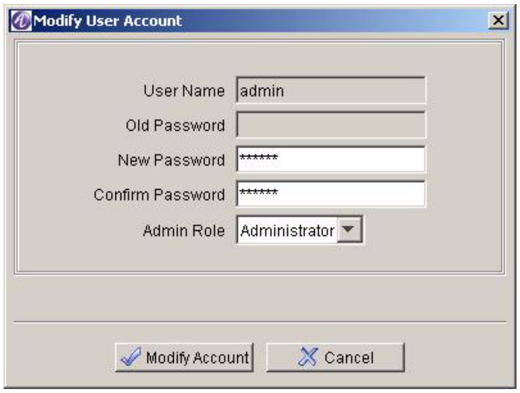
- Standard—requires a single login and password
- Dual-admin—requires two logins and passwords

3 Click **Apply** to apply the login setting.

NOTE: The Enabled checkbox shows the status of the user account. This is used to indicate whether the user can log in or not. For all user accounts, except admin, when an authentication method is changed from Radius to local, the account is set to "*disabled*". The account remains in a disabled state until the administrator resets the password for the account.

4 Select the "admin" user and click **Modify** to change the password for the "admin" user. The Modify User Account dialog box (*Figure 6*) displays.

Figure 6 Modify User Account Dialog Box



User Name: admin

Old Password:

New Password: ******

Confirm Password: ******

Admin Role: Administrator

5 Modify the password, as needed, and click **Modify Password**.

6 Click **Modify Account** if you are changing the admin role or user information.

NOTE: For more information on adding a new user or the different types of user roles, see *User Accounts*.

Adding a Device

Before you can visualize any data, you need to add a device. For more information on device management, see *Device Configuration*.

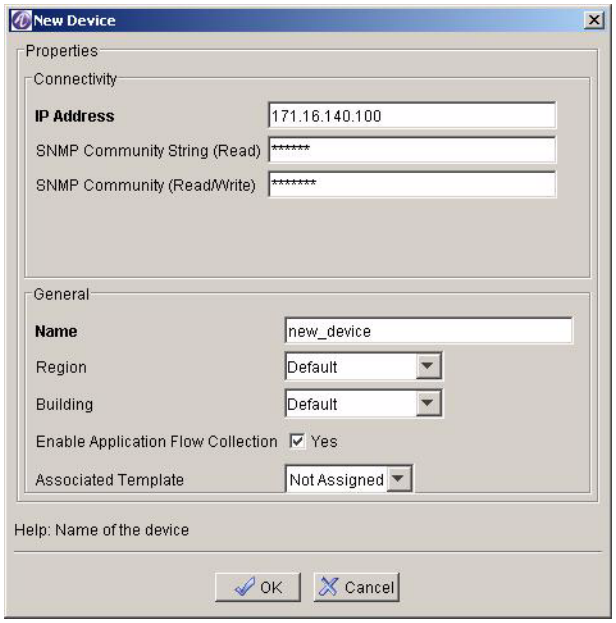
To add a single device:

1 Select the Device Configuration icon from the Page Bar or select the *View* > *Go To* > *Config Management* menu item.

2 Click the New icon from the Action Bar.

3 Select Single Device. The New Device (*Figure 7*) dialog box displays.

Figure 7 New Device Dialog Box



New Device

Properties

Connectivity

IP Address 171.16.140.100

SNMP Community String (Read) ******

SNMP Community (Read/Write) *******

General

Name new_device

Region Default

Building Default

Enable Application Flow Collection ☑ Yes

Associated Template Not Assigned

Help: Name of the device

4 Enter the following device attributes:

Table 2 Add Device Attributes

Attribute	Description
IP Address	The Management IP address of the device.
SNMP Community String (Read)	Simple Network Management Protocol (SNMP) read community name that was configured when the device was initially set up.
SNMP Community (Read/Write)	SNMP read/write community name that was configured when the device was initially set up.
Name	Device name.
Region	Name of the region in which the device is located.
Building	Name of the building in which the device is located.
Enable Application Flow Collection	Click this box if you want to collect application flow data.
Associated Template	Select a template from the pull-down list that you want to associate with the device. For more information on templates, see *Templates*.

NOTE: Make sure that the attributes are specified correctly; otherwise, adding a device fails producing one of the following error messages, *"Device unreachable,"* or *"Device is not a Alcatel-Lucent device,"* or *"Unable to communicate with IP Address."*

5 Click **OK** to add the device. The add process reads the system configuration and the list of outstanding visualization events from the device using a combination of SNMP and Alcatel-Lucent proprietary OmniVista SafeGuard Manager Visualization Channel.

NOTE: The device periodically ages out the visualization data; therefore, some of the events may be lost by the time you add the device.

The device displays in the All Devices panel and the device objects display in the Device Hierarchy navigation tree.

NOTE: The device must be reachable with appropriate community strings for the device to be added.

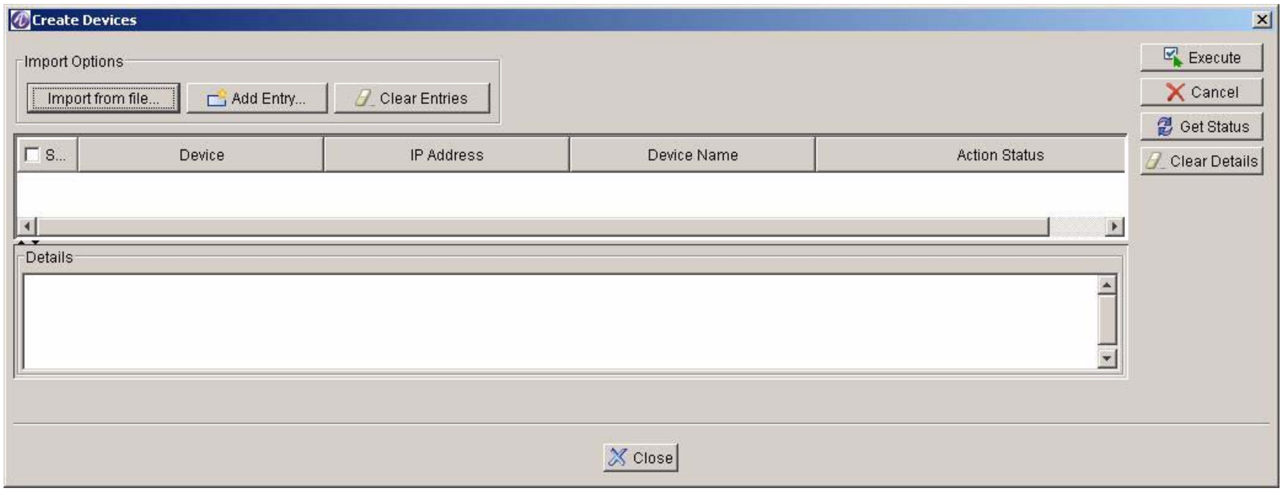
To add multiple devices:

1 Select the Device Configuration icon from the Page Bar or select the *View > Go To > Config Management* menu item.

2 Click the New icon from the Action Bar.

3 Select Multi Device. The Create Devices (*Figure 8*) dialog box displays. You can populate this table using either the **Import From File** or the **Add Entry** option.

Figure 8 Add Multiple Devices



4. Click **Import From File** to import a list of devices written in a specific format. For example:

```
#########################################################################
Name: Device List File #Purpose: For bulk device addition into OmniVista
SafeGuard Manager Syntax of each line: #
ip,read,readwrite,name,region,building,enable-flow-collection-in-true-
false # # Example: 172.16.3.125,public,private,controller,R1,B1,true
#########################################################################
172.16.3.125,public,private,controller,R1,B1,true
172.16.1.53,public,private,switch,R1,B2,true
```

5. Click **Add Entry** to add another entry in the table. This can be used to create a list.

6. The following device attributes are displayed:

Table 3 Add Device Attributes

Attribute	Description
Select Device	Select the Select Device checkbox to select all devices in the list.
Device	Show the device name with its IP address.
IP Address	The Management IP address of the device.
SNMP Community String (Read)	Simple Network Management Protocol (SNMP) read community name that was configured when the device was initially set up.
SNMP Community (Read/Write)	SNMP read/write community name that was configured when the device was initially set up.
Device Name	Device name.
Action Status	Status of the action you selected.

7. Click **Clear Entries** to clear all entries from the table.

8. Click **Execute**. The server schedules and processes each entry and provides feedback and action detail in the Action Status column.

chapter

2 Installation and Setup

This section includes the following:

- *Installing the OmniVista SafeGuard Manager Server*
- *Upgrading the OmniVista SafeGuard Manager Server*
- *Uninstalling the Server*
- *Starting the Server*
- *Shutting Down the Server*
- *Installing the OmniVista SafeGuard Manager Client*
- *Installing the OmniVista SafeGuard Manager Client*
- Logging into the OmniVista SafeGuard Manager Client
- *Connecting Over Firewall*

Installing the OmniVista SafeGuard Manager Server

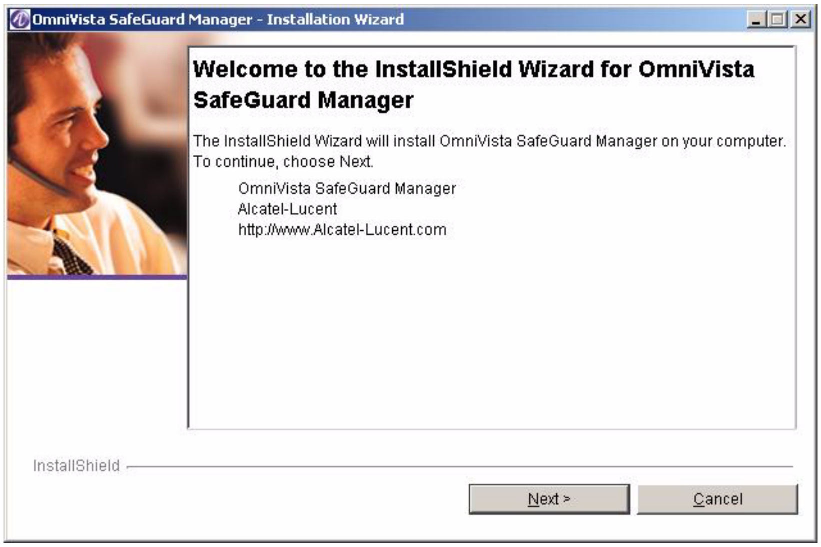
To install the OmniVista SafeGuard Manager server:

1 Double-click the executable file (omnivista-safeguard-<version>.exe).

The Installation Wizard prepares Java Virtual Machine (JVM) and initializes the installation wizard. This could take a few seconds.

After the initialization process is completed, the Welcome screen displays (*Figure 9*).

Figure 9 Installation Welcome Screen



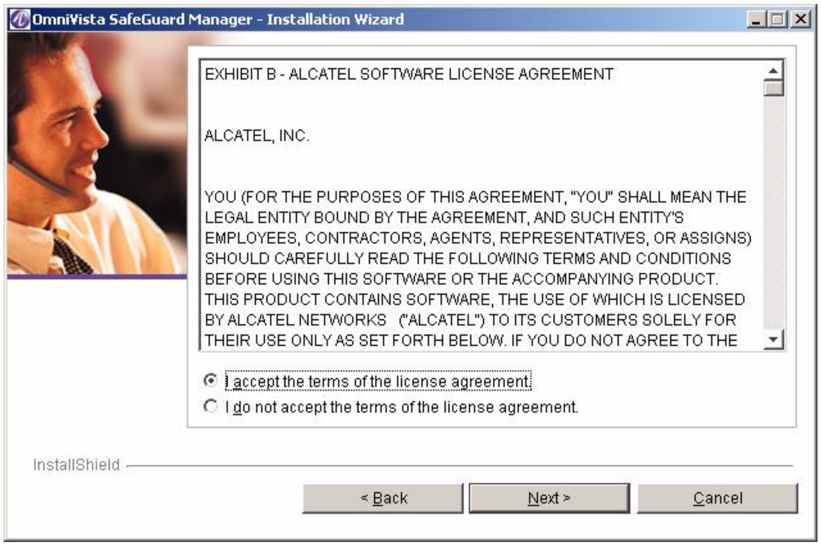
Welcome to the InstallShield Wizard for OmniVista SafeGuard Manager

The InstallShield Wizard will install OmniVista SafeGuard Manager on your computer. To continue, choose Next.

OmniVista SafeGuard Manager
Alcatel-Lucent
http://www.Alcatel-Lucent.com

2 Click **Next**. The Alcatel-Lucent license agreement displays (*Figure 10*).

Figure 10 Alcatel-Lucent License Agreement



OmniVista SafeGuard Manager - Installation Wizard

EXHIBIT B - ALCATEL SOFTWARE LICENSE AGREEMENT

ALCATEL, INC.

YOU (FOR THE PURPOSES OF THIS AGREEMENT, "YOU" SHALL MEAN THE LEGAL ENTITY BOUND BY THE AGREEMENT, AND SUCH ENTITY'S EMPLOYEES, CONTRACTORS, AGENTS, REPRESENTATIVES, OR ASSIGNS) SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THIS SOFTWARE OR THE ACCOMPANYING PRODUCT. THIS PRODUCT CONTAINS SOFTWARE, THE USE OF WHICH IS LICENSED BY ALCATEL NETWORKS ("ALCATEL") TO ITS CUSTOMERS SOLELY FOR THEIR USE ONLY AS SET FORTH BELOW. IF YOU DO NOT AGREE TO THE

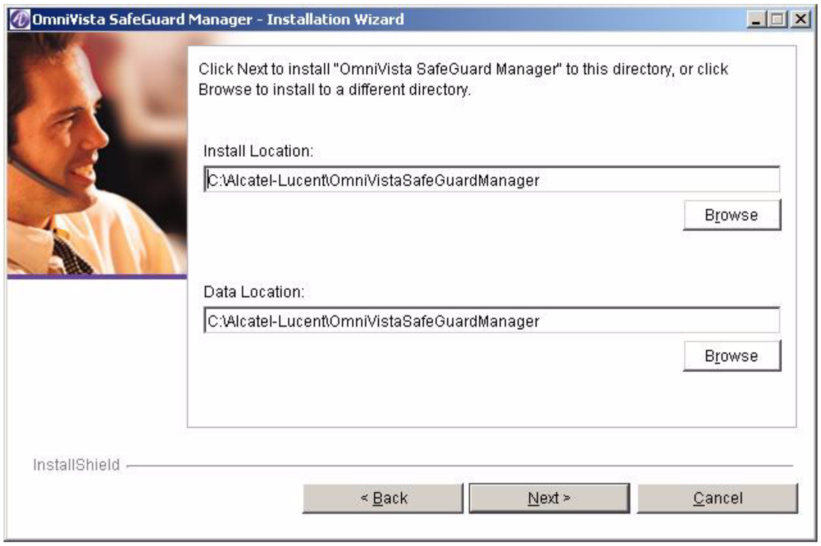
● I accept the terms of the license agreement.

○ I do not accept the terms of the license agreement.

3 Accept the licensing terms and click **Next**.

4 The Directory Location screen displays (*Figure 11*).

Figure 11 OmniVista SafeGuard Manager Alcatel-Lucent Installation Directory Location



OmniVista SafeGuard Manager - Installation Wizard

Click Next to install "OmniVista SafeGuard Manager" to this directory, or click Browse to install to a different directory.

Install Location: C:\Alcatel-Lucent\OmniVistaSafeGuardManager

Data Location: C:\Alcatel-Lucent\OmniVistaSafeGuardManager

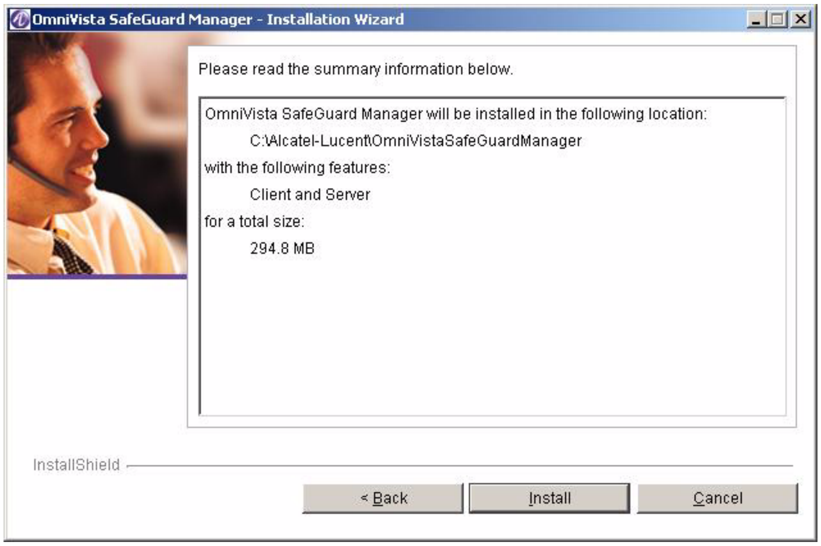
5 Accept the default location to which the installation files will be downloaded for the Install Location, or click **Browse** to choose a different directory. The default location is `C:\Alcatel-Lucent\OmniVistaSafeGuardManager`. Specify a data directory where all application, application flow, and visualization data is saved. The data directory allows you to save data when you uninstall or upgrade to a newer version of OmniVista SafeGuard Manager.

6 If a previous version of OmniVista SafeGuard Manager already exists on your system, a warning is displayed and you are given an option to exit the installation.

7 Click **Exit Installation** to quit the installation process. Uninstall OmniVista SafeGuard Manager and then re-install.

8 If a previous version is not installed, click **Next**. The Summary screen displays giving you a summary of where the installation files will be downloaded and the size of the files for the server and client installation.

Figure 12 Installation Summary



Please read the summary information below.

OmniVista SafeGuard Manager will be installed in the following location:

C:\Alcatel-Lucent\OmniVistaSafeGuardManager

with the following features:

Client and Server

for a total size:

294.8 MB

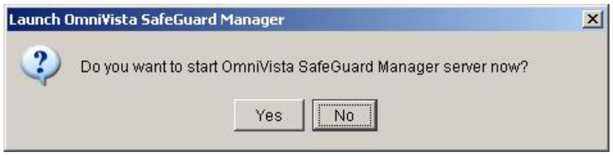
9 Click **Next**. The installation process begins. You can see the progress bar as the files are downloaded. A console window displays informing you of services and database being started.

10 After installation is completed, the OmniVista SafeGuard Manager Successfully Installed screen displays. Click **Finish**.

OmniVista SafeGuard Manager server and client are now installed on your system. The server is installed as a Windows service. An icon for the OmniVista SafeGuard Manager client is created on your desktop.

11 Server start screen displays asking if you want to start the server. Click **Yes** to restart the server.

Figure 13 Server Start



Do you want to start OmniVista SafeGuard Manager server now?

Upgrading the OmniVista SafeGuard Manager Server

When the appliance is shipped from Alcatel-Lucent it comes pre-installed with OmniVista SafeGuard Manager. You need to uninstall OmniVista SafeGuard Manager and then re-install to upgrade. For more information on installing, upgrading, and uninstalling the server, see *Installation and Setup*.

WARNING: When you upgrade the OmniVista SafeGuard Manager server, the existing database and reports are overwritten. Make sure that you make a backup copy of the database and the reports.

Pre-Upgrade Tasks

When upgrading the OmniVista SafeGuard Manager server from version 2.x to 3.0, 2.x data is not upgraded. Before performing an uninstall, administrators must export the device data using the following procedure, this will help them import back all the previously added devices:

1. Execute cimExportData.bat. This creates a file called "devices.txt" under the `C:\Alcatel-Lucent\OmniVistaSafeGuardManager|ExportData` directory.
2. Uninstall the older version of the OmniVista SafeGuard Manager server.
3. Install the newer version of the OmniVista SafeGuard Manager server.
4. Import all devices through using the Add Multiple Devices > Import from File option. For more information, see *Adding Multiple Devices*.

To upgrade the OmniVista SafeGuard Manager command center to the latest release:

1. Log in to the system using the administrator account.

   NOTE: To uninstall or upgrade software, you must have administrator-level privileges. Make sure you log in using the user account that is set up with these privileges.

2. Uninstall the existing version using the Windows shortcut from the Start menu, *Programs > OmniVista SafeGuard Manager > Uninstall > Uninstall OmniVista SafeGuard Manager*.
3. Follow the on-screen prompts using default options.
4. Reboot the system when the uninstallation is completed.
5. After the system is rebooted, double-click on the installation package (omnivista-safeguard-<version>.exe) available on the installation CD.

6 Follow the on-screen prompts using default options.

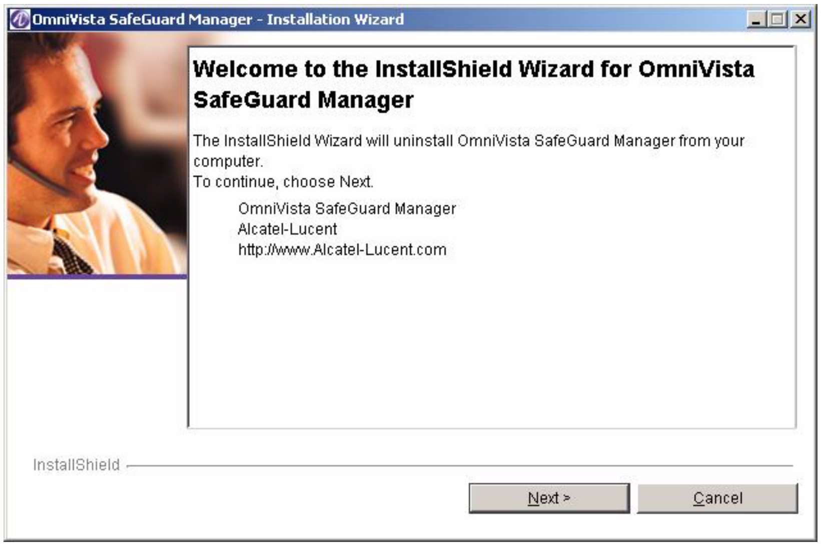
7 After the installation is completed, you have to start the OmniVista SafeGuard Manager server. For more information on starting the server, see *Starting the Server*.

Uninstalling the Server

To uninstall the server:

1 From the Start menu, click *Programs > OmniVista SafeGuard Manager > Uninstall > Uninstall OmniVista SafeGuard Manager*. The Welcome screen displays (*Figure 14*).

Figure 14 Uninstallation Welcome Screen



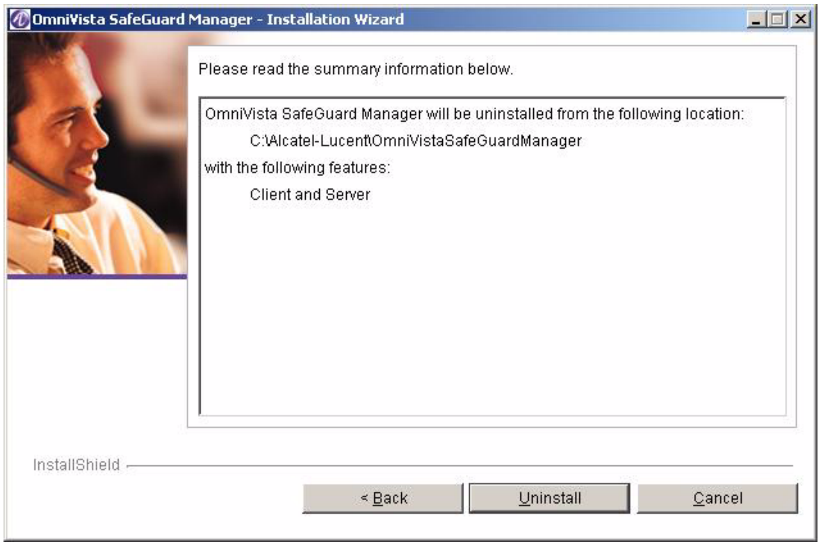
Welcome to the InstallShield Wizard for OmniVista SafeGuard Manager

The InstallShield Wizard will uninstall OmniVista SafeGuard Manager from your computer.
To continue, choose Next.

OmniVista SafeGuard Manager
Alcatel-Lucent
http://www.Alcatel-Lucent.com

2 Click **Next**. A summary information window displays with directory location information.

Figure 15 Uninstallation Summary



Please read the summary information below.

OmniVista SafeGuard Manager will be uninstalled from the following location:

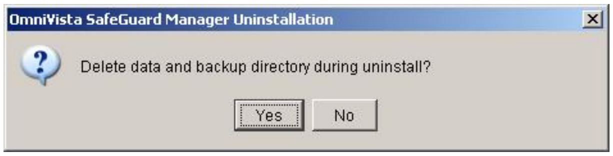
C:\Alcatel-Lucent\OmniVistaSafeGuardManager

with the following features:

Client and Server

3 Install asks you if you want to delete backup and data directories. Select **No** if you want to save the data.

Figure 16 Delete Data Directory



Delete data and backup directory during uninstall?

4 Follow the on-screen prompts to uninstall the server. The uninstall wizard stops the server and database, cleans the log files and begins the uninstallation process. The status is displayed in a console window.

The uninstall process completes and a “OmniVista SafeGuard Manager successfully uninstalled” window is displayed.

5 Click **Next**. Uninstall will ask you to restart the system.

6 Select the restart option and click **Finish** to complete the uninstall. All associated files and shortcuts are removed from your system.

Starting the Server

When you boot up the OmniVista SafeGuard Manager appliance, the OmniVista SafeGuard Manager server is started automatically. However, if you upgraded the software version or re-installed the software, you must manually start the server.

To manually start the server:

1. Use the Windows shortcut from the Start menu, *Programs > OmniVista SafeGuard Manager > Start Server.* A GUI window displays. This window performs checks to verify that all ports needed for the server are available, starts all the server components as Windows services, and informs you when the server is ready.
2. Click **OK** to close the window.

The OmniVista SafeGuard Manager server runs in the background. If you now reboot the system, the server should come up automatically.

Shutting Down the Server

To shut down the server:

1. From the Start menu, click *Programs > OmniVista SafeGuard Manager > Stop Server.* The OmniVista SafeGuard Manager server is stopped along with the Windows services.

NOTE: When you shut down the OmniVista SafeGuard Manager appliance, the OmniVista SafeGuard Manager server is stopped automatically.

Installing the OmniVista SafeGuard Manager Client

The OmniVista SafeGuard Manager client is based on Java Web Start technology, allowing you to install the client automatically over the network with a single click.

NOTE: If the client machine has a JRE version that is earlier than 1.5, then the client is automatically upgraded to JRE 1.5.

To install the client:

1 Launch Internet Explorer.

NOTE: Currently, only Internet Explorer version 6.0 or higher is supported.

2 Access the OmniVista SafeGuard Manager system by typing the following URL:

```
http://<server-ip-address>
```

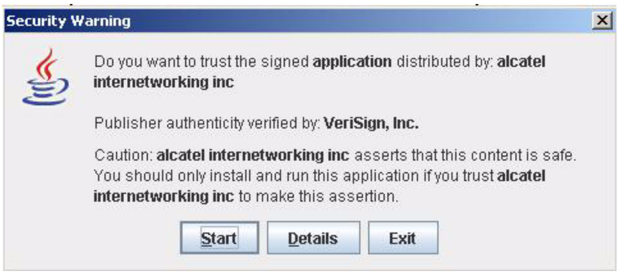
If the client does not have Java Web Start already installed, you are prompted to install Java Runtime Environment (JRE). Follow the on-screen prompts using the default options to install JRE. Java Web Start is included with JRE.

NOTE: The automatic installation of JRE requires ActiveX controls to be enabled on your Internet Explorer. If ActiveX controls are not enabled, a "*download Java Web Start*" link displays. Internet Explorer also alerts you if ActiveX controls are not enabled and gives you an option to enable ActiveX controls. You can choose to enable ActiveX controls for automatic installation of Java Web Start, or you can download JRE version 1.5.0 by going to the download link. If you manually install Java Web Start, repeat Step 2.

After Java Web Start is installed, the OmniVista SafeGuard Manager client code is downloaded and installed when you access the OmniVista SafeGuard Manager server (Step 2).

Java Web Start displays a dialog box informing you that the application is authored by Alcatel-Lucent and needs some privileges on your client system.

Figure 17 Security Warning



Do you want to trust the signed **application** distributed by: **alcatel internetworking inc**

Publisher authenticity verified by: **VeriSign, Inc.**

Caution: **alcatel internetworking inc** asserts that this content is safe. You should only install and run this application if you trust **alcatel internetworking inc** to make this assertion.

3 Click **Start**. A prompt appears asking if you want to create a shortcut on the desktop.

4 Select **Yes** to create a shortcut. If you select No, you can still launch the client using the URL from Step 2.

The client launches. See Logging into the OmniVista SafeGuard Manager Client for information on logging in procedures.

NOTE: Every time the OmniVista SafeGuard Manager client is launched, it compares its version with the OmniVista SafeGuard Manager server. If the client version is different than that of the server, the client automatically updates itself with the new version of the server.

Logging into the OmniVista SafeGuard Manager Client

To log into the client:

1 Launch the client using either of the following methods:

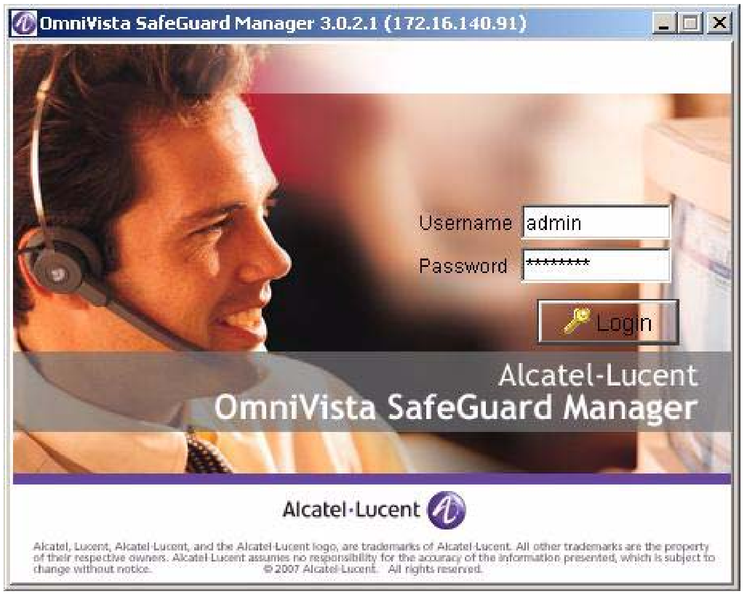
— Double-clicking on the shortcut that was created on your desktop when you first installed the client.

— Invoking from the Internet Explorer by typing the URL (http://ip-address-of-OmniVistaSafeGuardManager-server).

NOTE: If you are launching the client from the server for the first time, you might be prompted to install certain applications. See *Installing the OmniVista SafeGuard Manager Client* for more information.

The Login screen displays (*Figure 18*).

Figure 18 OmniVista SafeGuard Manager Client Login Screen



OmniVista SafeGuard Manager 3.0.2.1 (172.16.140.91)

Username admin

Password *********

Alcatel, Lucent, Alcatel-Lucent, and the Alcatel-Lucent logo, are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice. © 2007 Alcatel-Lucent. All rights reserved.

2 In the Username field, type **admin** as the default user.

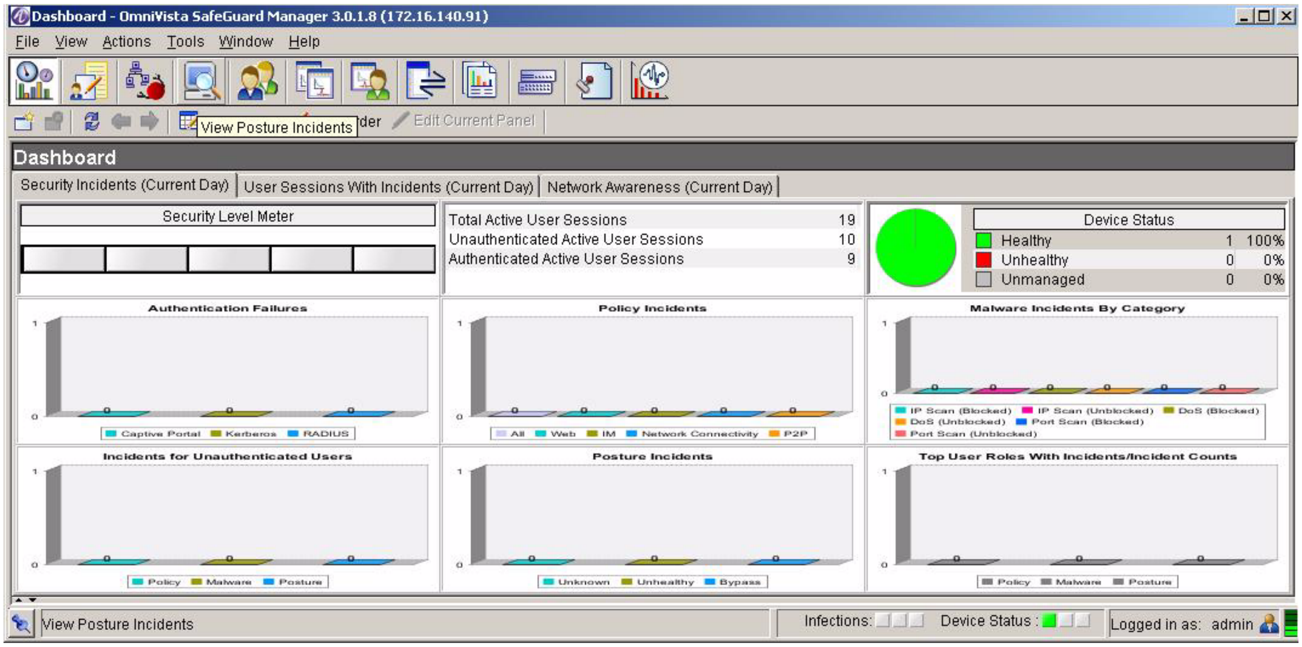
3 In the Password field, type **password**.

4 Click **Login**. If you are logging in for the first time to the OmniVista SafeGuard Manager server, the Alcatel-Lucent License Agreement displays. You must accept it to use OmniVista SafeGuard Manager.

> **NOTE:** The Alcatel-Lucent license agreement is a one-time acknowledgement for each server and is not displayed for this client or any other client or this server.

The client is launched and the dashboard is displayed (*Figure 19*).

Figure 19 OmniVista SafeGuard Manager Client - Dashboard



Total Active User Sessions	19
Unauthenticated Active User Sessions	10
Authenticated Active User Sessions	9

Device Status		
🟩 Healthy	1	100%
🟥 Unhealthy	0	0%
□ Unmanaged	0	0%

Connecting Over Firewall

If a firewall exists between the OmniVista SafeGuard Manager client and the OmniVista SafeGuard Manager server, or between the OmniVista SafeGuard Manager server and the SafeGuard OS device, certain ports must be opened for successful deployment. *Table 4* gives the number of ports that must be open:

Table 4 Ports that must be open for successful deployment

When connecting...	Ports that need to be open...
Between the OmniVista SafeGuard Manager server and client	■ TCP 80 ■ TCP 1099 ■ TCP 8003 ■ TCP 8004 ■ TCP 8011
Between the OmniVista SafeGuard Manager server and the SafeGuard OS device	■ UDP 161 ■ TCP 16001 ■ TCP 16002 ■ TCP 16005 ■ UDP 69

chapter

3 General Navigation

This section includes the following:

Viewing Visualization Tables

Visualization allows administrators to track what a user is doing, what applications are being used, and what is being done to a network. Such tracking is useful for forensic and postmortem purposes, that is, for debugging and ensuring that the network is performing at its optimum and there are no threats to the network. SafeGuard collects this data and periodically pushes it in tabular format to OmniVista SafeGuard Manager as visualization data.

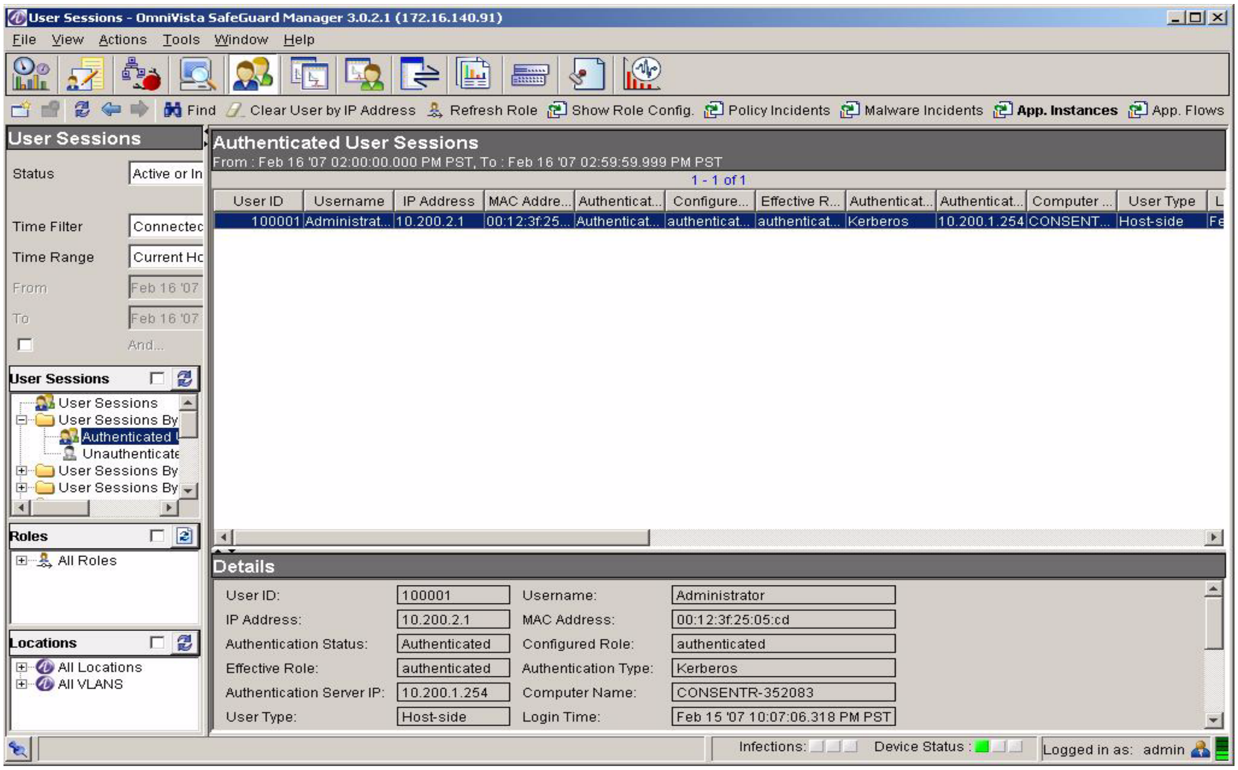
Visualization data can be viewed in tabular format for the following objects:

Table 5 Table Views

Table Type	Description
Policy Incidents	Displays a list of all policy incidents against a user. For more information, see *Viewing Policy Incidents*.
Malware Incidents	Displays a list of malware incidents. This table also displays the counts of various severities of the infection events. For more information, see *Viewing Malware Incidents*.
Posture Incidents	Displays all posture incidents, including EPV incident ID, host IP and MAC addresses. For more information, see *Viewing Posture Incidents*.
User	Displays user authentication and bandwidth usage that is aggregated for each user. Typically this has a navigation tree on the left panel that helps finds users belonging to a specific group/role or connected to a specific port of a specific device. For more information, see, Viewing User Sessions.
Application Type	Displays the user bandwidth usage that is aggregated for each type of application. For more information, see *Viewing Application Types*.
Application Instance	Displays the user bandwidth usage for each user, application type, destination port, and destination IP address. For more information, see *Viewing Application Instances*.
Application Flows	Allows an administrator to view application flows for a selected user or application. For more information, see *Viewing Application Flows*.

When you click on a table view, you are presented with a table that shows all visible data and a column to the left that lets you customize or view data by time, incident, location, and so forth (*Figure 20*).

Figure 20 Table View (Users)



Authenticated User Sessions

From : Feb 16 '07 02:00:00.000 PM PST, To : Feb 16 '07 02:59:59.999 PM PST

1 - 1 of 1

User ID	Username	IP Address	MAC Addre...	Authenticat...	Configure...	Effective R...	Authenticat...	Authenticat...	Computer ...	User Type	L
100001	Administrat...	10.200.2.1	00:12:3f:25...	Authenticat...	authenticat...	authenticat...	Kerberos	10.200.1.254	CONSENT...	Host-side	Fe

Details

User ID:	100001	Username:	Administrator
IP Address:	10.200.2.1	MAC Address:	00:12:3f:25:05:cd
Authentication Status:	Authenticated	Configured Role:	authenticated
Effective Role:	authenticated	Authentication Type:	Kerberos
Authentication Server IP:	10.200.1.254	Computer Name:	CONSENTR-352083
User Type:	Host-side	Login Time:	Feb 15 '07 10:07:06.318 PM PST

Viewing Table Data

To view table data:

1. Use the Action Bar buttons to navigate from one type of table view to another. See *Viewing Visualization Tables* for more information on different table views.

2. Use the scroll buttons at the top of the table to scroll through the data, one page at a time, previous page, next page, first page, or last page.

3. Use the fields in the left column to customize viewable data as follows:

Attribute	Description
Status	From the dropdown list, select to view incidents by status: ■ Active—displays all active incidents ■ Inactive—displays all inactive incidents

Attribute	Description
Time Range	From the dropdown list choose a time for which you want to view table data. Following values are available: ■ Current Hour—displays incidents for the current hour ■ Last Hour—displays incidents for the last hour ■ Current Day—displays incidents for the current day ■ Last Day—displays incidents for the day before ■ Previous Day—displays incidents for the previous 24 hours. ■ Previous Hour—displays incidents for the hour before the current time. ■ Custom—allows you to enter a specific time in the From and To time fields
Time Filter	Display incidents by: ■ Detection Time—time when incident was detected (first occurrence, last occurrence, login time, and logout time depending on the view) ■ Cleared Time—time when incident was cleared
From/To	These fields are only applicable if you select Custom in the time range. A dropdown arrow provides you with a calendar to specify the date and time in the From and To fields.
And...	Click **And** to specify additional time filters. For more information on using the this field, see *Additional Time-based Filtering*.
Users	Select to view users by authentication state, type, application group, and so forth.
All roles	Select to view incidents for a specific role.
VLAN Filtering	Allows you set up visualization filters based on VLAN IDs.
All locations	Select to view incidents for a specific building or location.

In general, all table views allow you to search and sort the data. You can search and sort data:

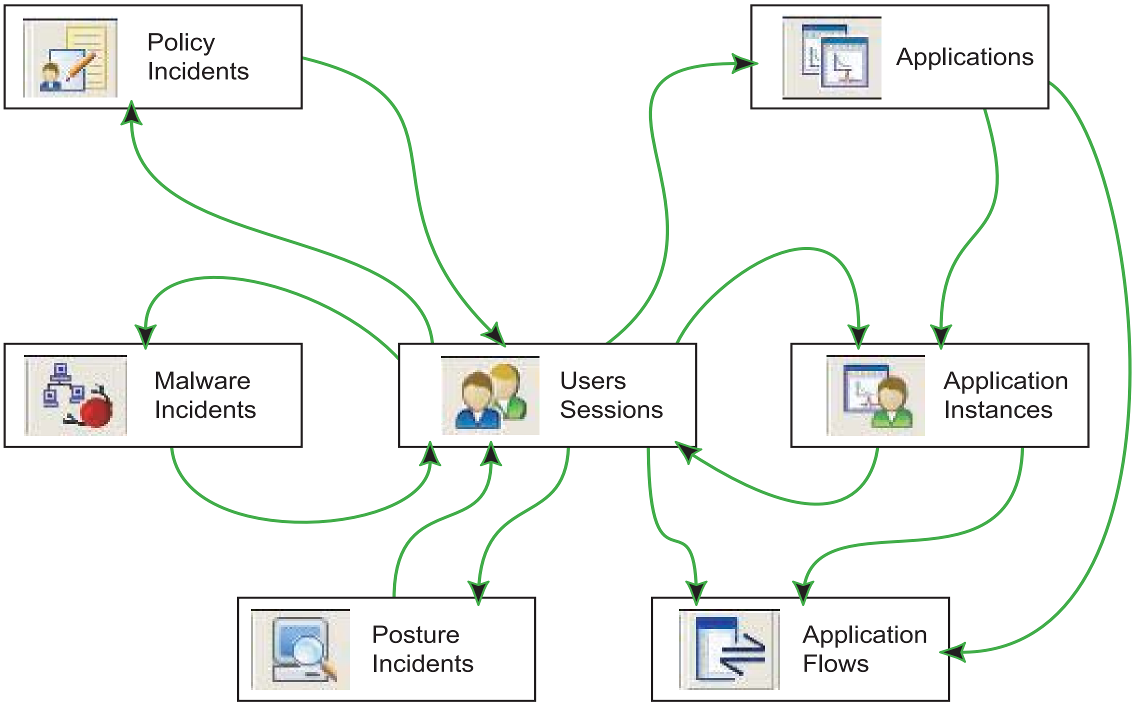
- at the currently displayed page level
- at the database level

For more information on how you can search and sort data, see *Searching and Sorting*.

Navigating between Different Table Views

The single-window design in OmniVista SafeGuard Manager lets you navigate from one view to another with a single click of a button. *Figure 21* below shows the different views to which you can navigate from a given table view. For example, from the User view you can use the Action Bar buttons to access Posture Incidents, Malware Incidents, Policy Incidents, Applications, and Application Instances.

Figure 21 Navigating between Different Table Views



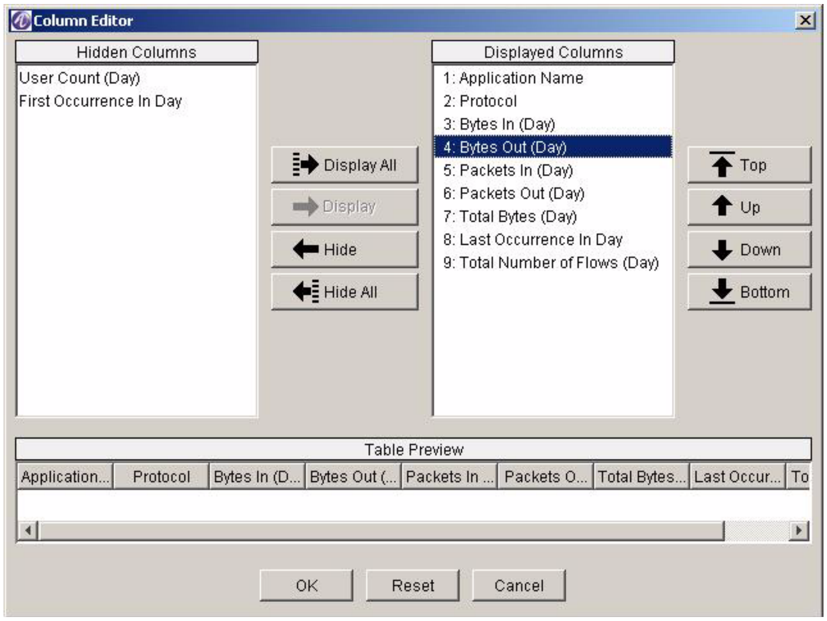
Choosing Columns in a Table

OmniVista SafeGuard Manager allows you to choose and set the order in which you view the columns in a given table view. These settings are remembered in Windows for each user and are applied when you visit the same table again. However, you can reset the column order to its default value at any given time. From the menu bar, select *Tools > Client Settings> Reset Views>*.

To hide or select the columns in a table view:

1 From a table view (All Users, All Application Types, and so on), click the Edit icon from the Action Bar. The Column Editor displays with a list of hidden and displayed columns (*Figure 22*).

Figure 22 Column Editor



Column Editor

Hidden Columns

User Count (Day)
First Occurrence In Day

Displayed Columns

1: Application Name
2: Protocol
3: Bytes In (Day)
4: Bytes Out (Day)
5: Packets In (Day)
6: Packets Out (Day)
7: Total Bytes (Day)
8: Last Occurrence In Day
9: Total Number of Flows (Day)

Table Preview

Application...	Protocol	Bytes In (D...	Bytes Out (...	Packets In ...	Packets O...	Total Bytes...	Last Occur...	To

2 Use the Column Editor buttons as described to hide or display a column in the table view:

Table 6 Column Editor Buttons

Button Name	Function
Display All	Select **Display All** to display all the columns available in the table.
Display	Highlight a column in the Hidden Columns panel and click **Display** to add to the Displayed Columns panel.

Table 6 Column Editor Buttons *(continued)*

Button Name	Function
Hide	Select a column in the Displayed Columns panel and click **Hide** to remove it from the display list. This will hide the column from the table view.
Hide All	Select **Hide All** to hide all the columns from the table view.
Top	Select a column in the Display Columns panel and click **Top** to move the selected column to the top of the list. This will be the first column displayed in your table view.
Up	Select a column in the Display Columns panel and click **Up** to move the selected column one level up in the list.
Down	Select a column in the Display Columns panel and click **Down** to move the selected column one level down in the list.
Bottom	Select a column in the Display Columns panel and click **Bottom** to move the selected column to the bottom of the list. This will be the last column in the table view.

The Table Preview panel (bottom of the Editor window) gives you a preview of your table as you make these selections.

3 Click **OK** to apply the changes. When you go into the table view, the columns are displayed in the order you selected here.

4 Click **Reset** to reset the columns to the previous settings.

5 Click **Cancel** to exit out of the Column editor without making any changes.

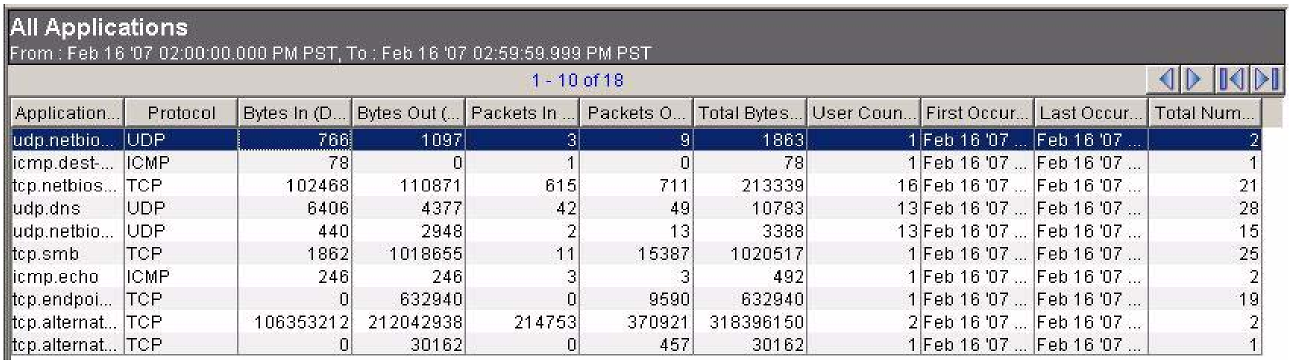
NOTE: When in table view, you can also change the display order of the columns in a table by selecting and dragging a column. You can also change the column width by dragging the column header separator. These settings are remembered by the Windows client machine for each user.

Searching and Sorting

Most of the visualization tables display a maximum of 1,000 rows. When the number of rows that exist in the database is more than can be displayed in a window, page navigation buttons are shown in the top-right corner of the screen (*Figure 23*).

NOTE: If you increase the page size from 1,000 rows, data retrieval may take longer.

Figure 23 Tables - Partial View



All Applications
From : Feb 16 '07 02:00:00.000 PM PST, To : Feb 16 '07 02:59:59.999 PM PST

1 - 10 of 18

Application...	Protocol	Bytes In (D...	Bytes Out (...	Packets In ...	Packets O...	Total Bytes...	User Coun...	First Occur...	Last Occur...	Total Num...
udp.netbio...	UDP	766	1097	3	9	1863	1	Feb 16 '07 ...	Feb 16 '07 ...	2
icmp.dest-...	ICMP	78	0	1	0	78	1	Feb 16 '07 ...	Feb 16 '07 ...	1
tcp.netbios...	TCP	102468	110871	615	711	213339	16	Feb 16 '07 ...	Feb 16 '07 ...	21
udp.dns	UDP	6406	4377	42	49	10783	13	Feb 16 '07 ...	Feb 16 '07 ...	28
udp.netbio...	UDP	440	2948	2	13	3388	13	Feb 16 '07 ...	Feb 16 '07 ...	15
tcp.smb	TCP	1862	1018655	11	15387	1020517	1	Feb 16 '07 ...	Feb 16 '07 ...	25
icmp.echo	ICMP	246	246	3	3	492	1	Feb 16 '07 ...	Feb 16 '07 ...	2
tcp.endpoi...	TCP	0	632940	0	9590	632940	1	Feb 16 '07 ...	Feb 16 '07 ...	19
tcp.alternat...	TCP	106353212	212042938	214753	370921	318396150	2	Feb 16 '07 ...	Feb 16 '07 ...	2
tcp.alternat...	TCP	0	30162	0	457	30162	1	Feb 16 '07 ...	Feb 16 '07 ...	1

You can search and sort the data displayed in tabular views using either of the following methods:

- Search and sort the data displayed in table views by entering text in the free-form search panel. This method applies a search and sort order that is local to the data currently displayed.
- Search the whole database by applying database queries and search criteria. This method applies the search to the server database and refreshes the client data.

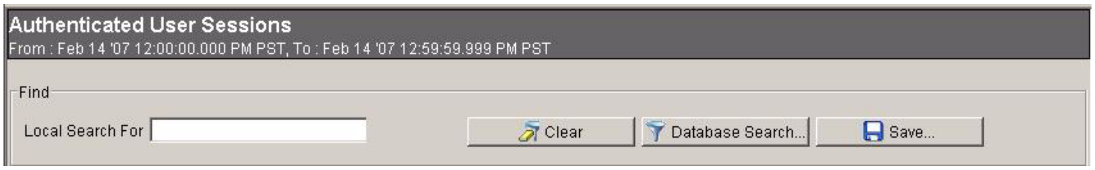
NOTE: The page forward, page back, first page, and last page buttons allow you to navigate between multiple pages of the search/sort results. You can also change the limit on the number of records that are displayed. Simply, click on the page number at the top of the table and enter the page size in the text box that is displayed.

Searching Table Data Locally

To search table data locally:

1. Select *View* > *Go To* > *Users* (or any other menu item, or click an icon from the Page Bar to get to a table view). In a table view, click the Find Find icon. A free-form text search field displays (*Figure 24*).

Figure 24 Free-Form Search Fields



Authenticated User Sessions

From : Feb 14 '07 12:00:00.000 PM PST, To : Feb 14 '07 12:59:59.999 PM PST

2. Enter a keyword on which to base the search.

Sorting Table Data Locally

To sort the table data locally:

1. In table view, click on a column header. The first column header that you click on becomes the primary sort field (indicated by a slightly larger arrow). You can click on several column headers to add them to the sort as a secondary sort and perform a multi-level sort.
2. Double-click on a column header to reset the sort to a single column and clear the sort on all other fields.
3. Single-click on an already sort-enabled header to toggle the sort order between ascending or descending.

Searching and Sorting Data in the Entire Database

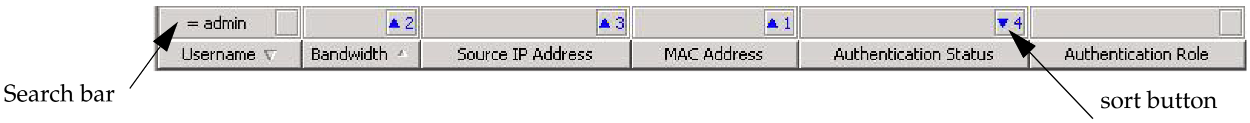
Most table columns allow search and sort on the database; however, certain columns do not have this functionality.

To search and sort the database on the server:

1 In a table view, click the Find Find icon. A search panel displays (*Figure 24*).

2 Click **Database Search**. The column headers now have search fields and sort buttons (*Figure 25*).

Figure 25 New Search Fields for Table Headers

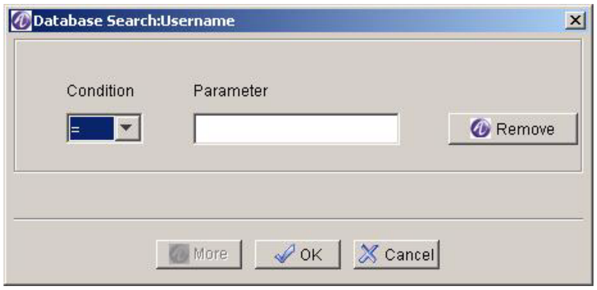


Search bar

sort button

3 Click on the search bar of the column. A search criteria dialog box opens, allowing you to specify the search criteria.

Figure 26 Search Criteria Dialog



4 Select a condition from the dropdown list, and specify a search condition (username, IP address, and so on). If you want to specify more than one search condition, select a condition from the condition dropdown list; then click **More** to add more than one parameter. Up to 5 search conditions can be applied using the following operators combined together:

=	equal to
!=	more than one
<	less than
<=	less than or equal to
>	greater than
>=	greater than or equal to

5 Click **OK**. Your search criteria are applied.

6 Click on the sort button (*Figure 25*) to apply the sort criteria for that column. You can apply multi-level sorts. The numbers on the sort buttons signify the sorting order. A sort can be applied in either an ascending or a descending order. If you want to reset the sort order, double-click a column to make it the primary sort and reset all other columns.

7 After you have set the filters for one or more columns, click the Refresh icon in the Action Bar to see new results.

NOTE: Toggle the **Advance** button to clear the advance filters.

Exporting and Printing Data

OmniVista SafeGuard Manager allows you to export data into a comma-separated value (CSV) file format. CSV format is often used to exchange data between disparate applications. CSV files can easily be exported, for example, into Excel worksheets. You can also print any visualization tables or columns or reports.

To export data in CSV format:

1 From a table view, click the Export icon. A Windows file browser dialog box displays.

2 Specify the name and location for the file. The file is saved with a csv extension.

To print data:

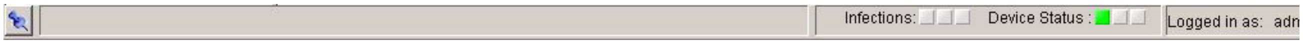
1 From a table view, click the Print icon. A Windows Print browser dialog box displays.

2 Select a printer and click **OK**. The file is printed to the printer you specified.

Using the Status Bar

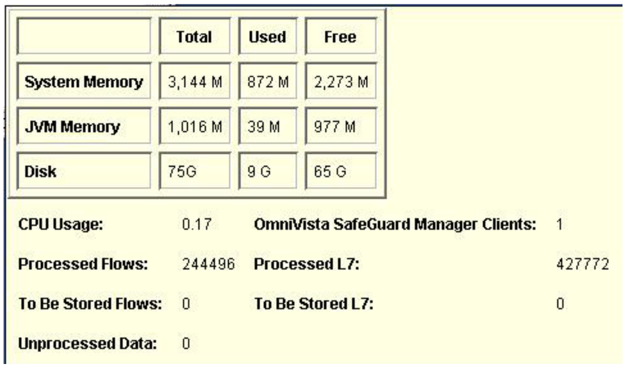
The status bar displays the progress of an action, for example, when you synchronize a device or retrieve data, and when there are any alarms or infections on a device (*Figure 27*).

Figure 27 Status Bar



Infections: □□□ Device Status : 🟩□□ Logged in as: adn

The little green icon 🟩 on the right corner of the status bar has a tool tip which displays the current OmniVista SafeGuard Manager Server Health parameters. A sample display of current values using tooltip is shown below.



	Total	Used	Free
System Memory	3,144 M	872 M	2,273 M
JVM Memory	1,016 M	39 M	977 M
Disk	75G	9 G	65 G

CPU Usage:	0.17	OmniVista SafeGuard Manager Clients:	1
Processed Flows:	244496	Processed L7:	427772
To Be Stored Flows:	0	To Be Stored L7:	0
Unprocessed Data:	0		

chapter

4 Visualization

This section includes the following:

- *Overview*
- *Dashboards*
- *Configuring Dashboards*
- *Viewing Visualization Data*
- Viewing Time-based Data

Overview

Network visualization is the ability to determine detailed information about what users are doing in the network. Data collected during visualization is aggregated and maintained in a relational database using a set of tables (see *Table 10* for more information on the kind of data collected).

By having the events be user-based, network visualization allows an administrator to monitor data in a manner that presents the data in a drillable and easily digestible format. You can take remediation steps faster when you have a better understanding of a problem and can act upon a network event.

For example, you have a vendor working on site on a regular basis. You might want to give this vendor more privileges than a visitor, but might also want to restrict vendor use to certain applications or file types. Network visualization allows you to configure policies to block access and log information about that access to OmniVista SafeGuard Manager. You can also set up visualization filters that enable you to selectively view events based on VLAN ID, application type, or user role.

Network visualization provides all the user, application, and performance information you need to have visibility into the network usage through the real-time dashboards (for more information, see *Dashboards*). This usage is constant and covers all points in the network. Visualization events are collected and stored for each user or application. The OmniVista SafeGuard Manager command center provides dynamic, high-level views of security information, including:

- Providing real-time and historical data
- Identifying who is using the network and viewing aggregated data for each user
- Identifying applications and resources as they interact with each other and viewing aggregated data for each application
- Identifying traffic patterns that represent normal and legitimate use of the network
- Identifying which traffic patterns represent abnormal (and possibly abusive) behavior
- Identifying when important events occur
- Identifying classified documents that passed over the network
- Maintaining the malware state of all hosts and allowing administrators to reset the malware state of hosts

Dashboards

The OmniVista SafeGuard Manager command center comes with three pre-defined real-time dashboards:

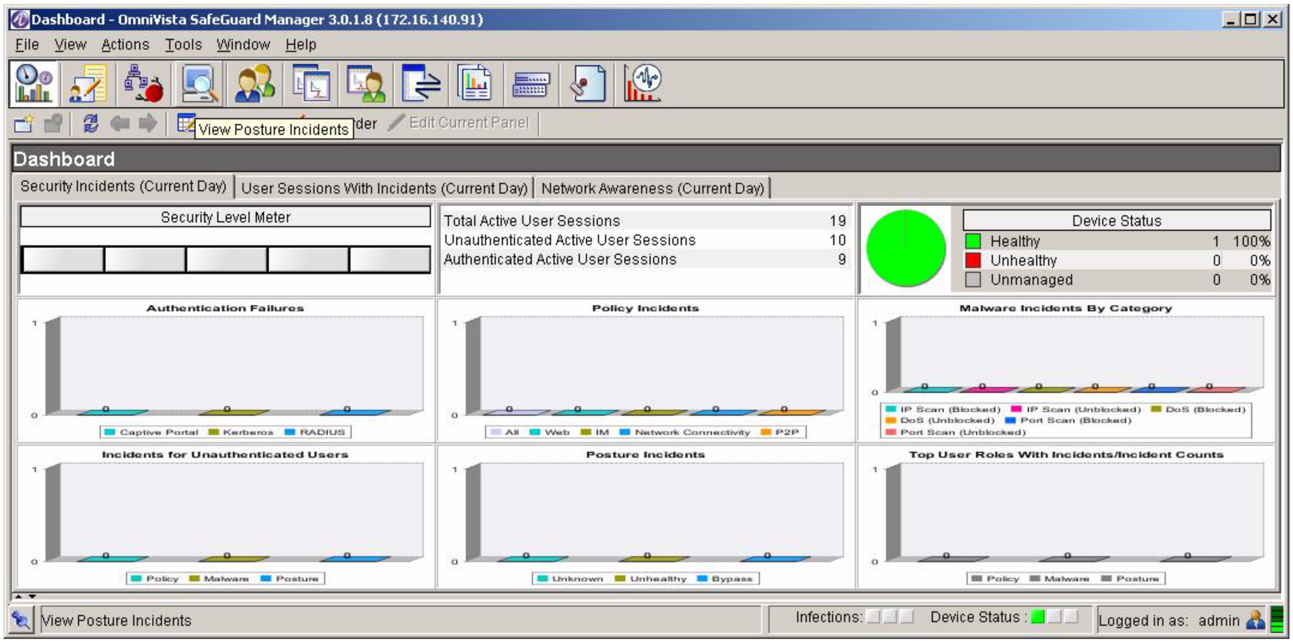
- Security Incidents
- User Sessions with Incidents
- Network Awareness

These dashboards display current day counters.

Security Incidents

The Security Incidents dashboard refreshes every 60 seconds but can also be refreshed using the F5 key. You can access this dashboard (*Figure 28*) by clicking the Incidents tab on the dashboard. The Incidents tab displays statistics based on incident instances irrespective of users. For example, if user U1 has 100 incidents and user U2 has one incident, this tab is going to show 101 incidents. Any new incident will raise the bar height.

Figure 28 Dashboards - Security Incidents Tab



Total Active User Sessions	19
Unauthenticated Active User Sessions	10
Authenticated Active User Sessions	9

Device Status		
🟩 Healthy	1	100%
🟥 Unhealthy	0	0%
□ Unmanaged	0	0%

View Posture Incidents

Infections: □□□ Device Status : 🟩□□

Logged in as: admin

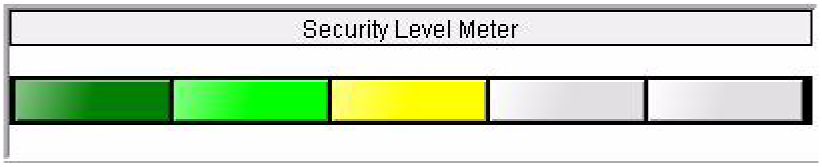
The Incidents dashboard displays the following information:

- *Security Level Meter*
- User Sessions Summary
- Device Status
- *Authentication Failures*
- *Policy Incidents*
- Malware Incidents by Category
- *Incidents for Unauthenticated Users*
- Top User Roles with Incidents/Incident Counts

Security Level Meter

The Security Level Meter (top-left panel) shows weighted incidents per user. The gauge moves to the right as the incidents grow. The severity level is indicated on a scale of 1-5, where 1 is the lowest and 5 is the highest severity level.

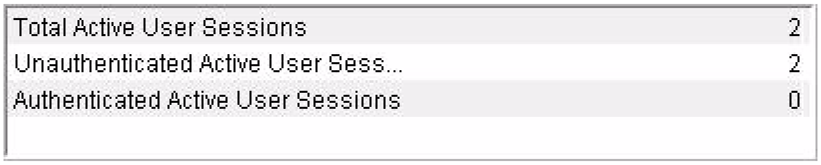
Figure 29 Security Level Meter



User Sessions Summary

The User Summary table (top-center panel) displays important statistics about the host-side user counts: total active users, authenticated active users, unauthenticated active users.

Figure 30 User Sessions Summary

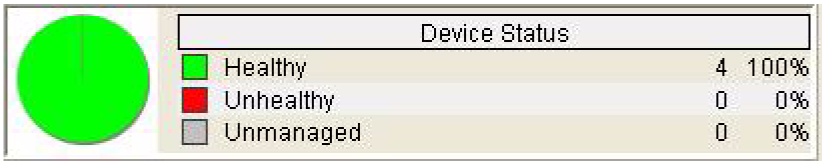


Total Active User Sessions	2
Unauthenticated Active User Sess...	2
Authenticated Active User Sessions	0

Device Status

The Device Health pie chart shows the connectivity health of a device. Devices that are healthy show up in green and devices that cannot be reached, show up in red.

Figure 31 Device Health



Device Status		
🟩 Healthy	4	100%
🟥 Unhealthy	0	0%
▨ Unmanaged	0	0%

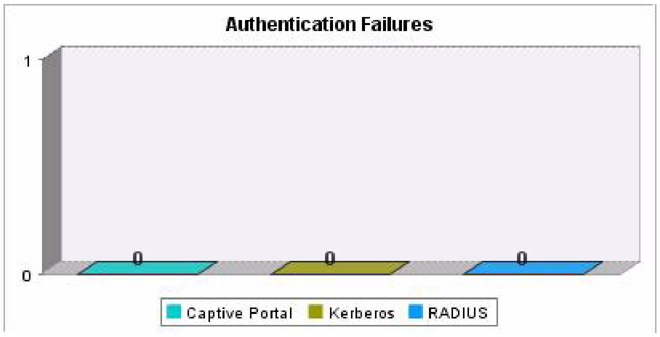
You can access Device Management by clicking on the Device Health panel. For more information on Device Management, see Chapter 5, Device Configuration.

Authentication Failures

The Authentication Failures bar chart displays the various kinds of access control incidents:

- Captive Portal—displays the number of users that have failed authentication using the Captive Portal.
- Kerberos—displays login failures occurred authenticating users through Kerberos.
- RADIUS—displays the number login failures occurred authentication users through RADIUS.

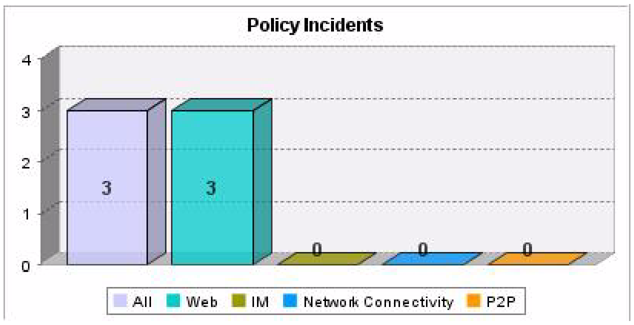
Figure 32 Authentication Failures



Policy Incidents

The Policy Incidents bar chart shows various types of policy incidents, all policy incidents, Web, IM, or network connectivity incidents only. For more information on policy incidents, see *Viewing Policy Incidents*.

Figure 33 Policy Incidents



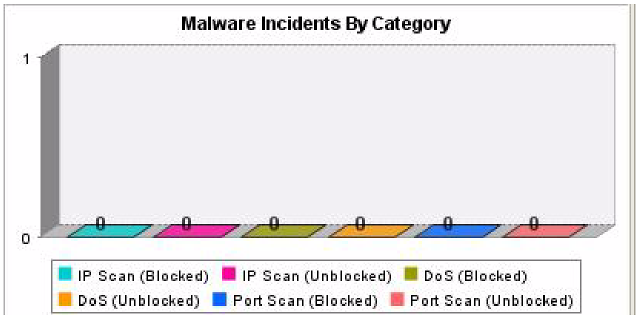
Malware Incidents by Category

The Malware Incidents bar chart shows various types of malware incidents: by category:

- number of IP scans that were blocked
- number of IP scans that were unblocked
- number of port scans that were blocked
- number of port scans that were unblocked
- number of DoS incidents that were blocked
- number of DoS incidents that were unblocked

Click on each bar to display a corresponding list of malware events. For more information on viewing malware incident details, see *Viewing Malware Incidents*.

Figure 34 Malware Incidents by Category



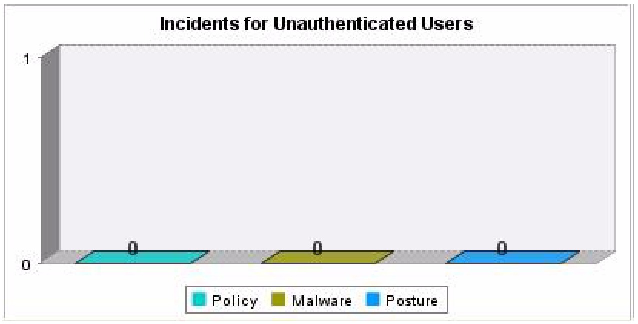
For more information on viewing malware incident details, see *Viewing Malware Incidents*.

Incidents for Unauthenticated Users

The Incidents for Unauthenticated Users chart summarizes the various incidents in the network that are caused by unauthenticated users:

- Users with Policy Incidents—number of unauthenticated users that are violating resource access policies.
- Users with Malware Incidents—number of unauthenticated users that are violating malware policies.
- Posture—number of unauthenticated users that are causing posture incidents.

Figure 35 Incidents for Unauthenticated Users

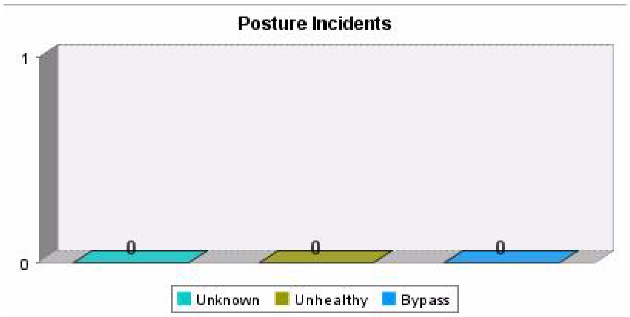


Click on each bar to view user details including corresponding incidents. For more information on viewing user details, see Viewing User Sessions.

Posture Incidents

The Posture Incidents bar chart shows various types of posture incidents, unknown, unhealthy, or bypass. For more information on posture incidents, see *Viewing Posture Incidents*.

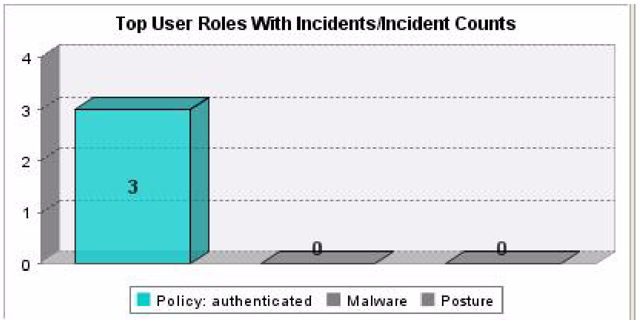
Figure 36 Posture Incidents



Top User Roles with Incidents/Incident Counts

The Top User Roles with Incidents bar chart displays the top user roles that are generating the maximum number of policy, malware, or posture incidents.

Figure 37 Top User Roles with Incidents



Click on any bar to display the associated top roles with most incidents window.

User Sessions with Incidents

The User Sessions with Incidents tab displays similar information as the Security Incidents tab but the statistics displayed is more user-centric. For example, if user U1 has 100 incidents and user U2 has one incident, the statistics are displayed as 2 users generating incidents, even though there are a total of 101 incidents. The bar height goes up only when there is a new user generating an incident.

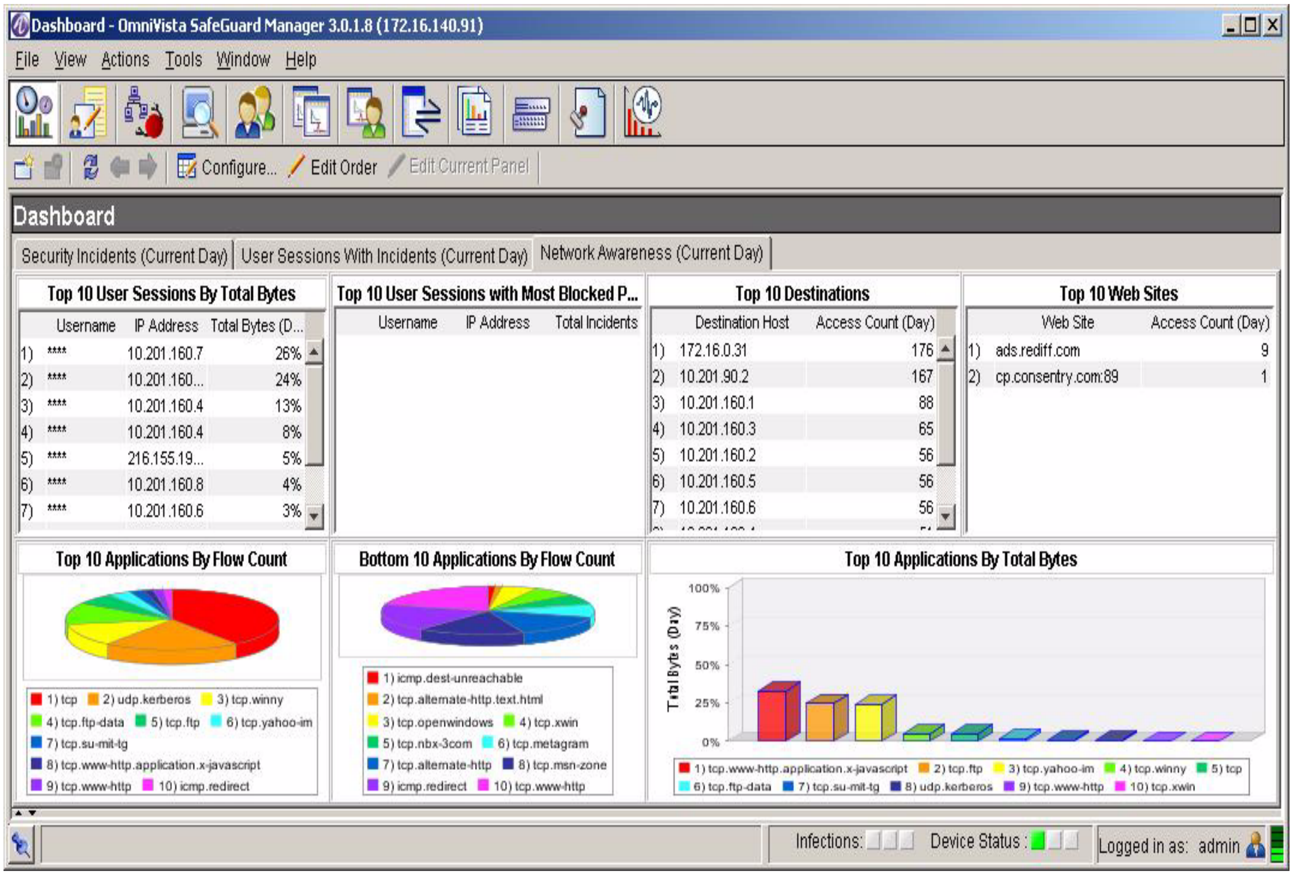
Network Awareness

The Network Awareness dashboard displays various application usage patterns and statistics for active users. The modules are automatically refreshed every 5 minutes. You can also use the F5 key to refresh the modules.

In the Network Awareness dashboard, double-click on the module header to display the associated detail information. For example, if you double-click the Top 10 User Sessions by Bandwidths module header, the Top 10 User Sessions window is displayed with user details and the bandwidth usage. However, some modules allow row details. For such modules, select a row and double-click to see associated detail information.

NOTE: You can right click on any module to display the details in either a bar graph or a pie chart format. You can also select to hide or display the legend that accompanies the graph. You can also position the mouse cursor on any of the bar graph or pie chart element to get tooltips.

Figure 38 Dashboard - Network Awareness Tab


Dashboard - OmniVista SafeGuard Manager 3.0.1.8 (172.16.140.91)
File View Actions Tools Window Help
Configure... Edit Order Edit Current Panel
Dashboard
Security Incidents (Current Day)
User Sessions With Incidents (Current Day)
Network Awareness (Current Day)
Top 10 Applications By Flow Count
🟥 1) tcp 🟧 2) udp.kerberos 🟨 3) tcp.winny
🟩 4) tcp.ftp-data 🟩 5) tcp.ftp 🟦 6) tcp.yahoo-im
🟦 7) tcp.su-mit-tg
🟦 8) tcp.www-http.application.x-javascript
🟪 9) tcp.www-http 🟪 10) icmp.redirect
Bottom 10 Applications By Flow Count
🟥 1) icmp.dest-unreachable
🟧 2) tcp.alternate-http.text.html
🟨 3) tcp.openwindows 🟩 4) tcp.xwin
🟩 5) tcp.nbx-3com 🟦 6) tcp.metagram
🟦 7) tcp.alternate-http 🟦 8) tcp.msn-zone
🟪 9) icmp.redirect 🟪 10) tcp.www-http
Top 10 Applications By Total Bytes
100%
75%
50%
25%
0%
Total Bytes (Day)
🟥 1) tcp.www-http.application.x-javascript 🟧 2) tcp.ftp 🟨 3) tcp.yahoo-im 🟩 4) tcp.winny 🟩 5) tcp
🟦 6) tcp.ftp-data 🟦 7) tcp.su-mit-tg 🟦 8) udp.kerberos 🟪 9) tcp.www-http 🟪 10) tcp.xwin
Infections:
Device Status :
Logged in as: admin

Top 10 User Sessions By Total Bytes

	Username	IP Address	Total Bytes (D...
1)	****	10.201.160.7	26%
2)	****	10.201.160...	24%
3)	****	10.201.160.4	13%
4)	****	10.201.160.4	8%
5)	****	216.155.19...	5%
6)	****	10.201.160.8	4%
7)	****	10.201.160.6	3%

Top 10 User Sessions with Most Blocked P...

Username	IP Address	Total Incidents

Top 10 Destinations

	Destination Host	Access Count (Day)
1)	172.16.0.31	176
2)	10.201.90.2	167
3)	10.201.160.1	88
4)	10.201.160.3	65
5)	10.201.160.2	56
6)	10.201.160.5	56
7)	10.201.160.6	56

Top 10 Web Sites

	Web Site	Access Count (Day)
1)	ads.rediff.com	9
2)	cp.consentry.com:89	1

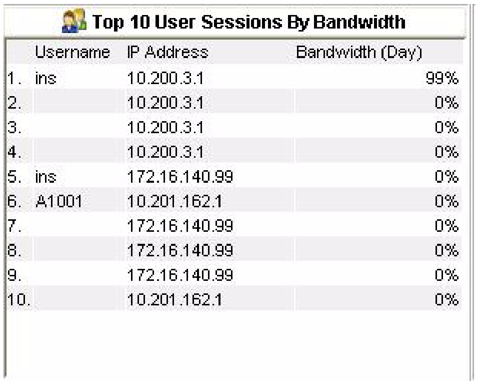
The Network Awareness dashboard displays the following information:

- *Top 10 User Sessions by Bandwidth*
- *Top 10 User Sessions with Most Blocked Incidents*
- *Top 10 Destinations*
- Top 10 Web Sites
- *Top 10 Applications by Flow Count*
- *Bottom 10 Applications by Flow Count*
- Top 10 Applications by Bandwidth (Bar Chart)

Top 10 User Sessions by Bandwidth

The Top 10 User Sessions by Bandwidth table displays the name and usage of the top 10 user sessions by bandwidth. The bandwidth is shown in terms of percentage (%) usage.

Figure 39 Top 10 User Sessions by Bandwidth



Top 10 User Sessions By Bandwidth

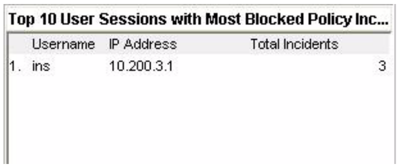
	Username	IP Address	Bandwidth (Day)
1.	ins	10.200.3.1	99%
2.		10.200.3.1	0%
3.		10.200.3.1	0%
4.		10.200.3.1	0%
5.	ins	172.16.140.99	0%
6.	A1001	10.201.162.1	0%
7.		172.16.140.99	0%
8.		172.16.140.99	0%
9.		172.16.140.99	0%
10.		10.201.162.1	0%

Click on the column header to display a list of users, including all user details. For more information on viewing user details, see Viewing User Sessions.

Top 10 User Sessions with Most Blocked Incidents

The Top 10 User Sessions with the Most Blocked Incidents shows the IP addresses of the top 10 user sessions that had the most blocked policy incidents. Username is displayed only if available.

Figure 40 Top 10 User Sessions with Most Blocked Incidents



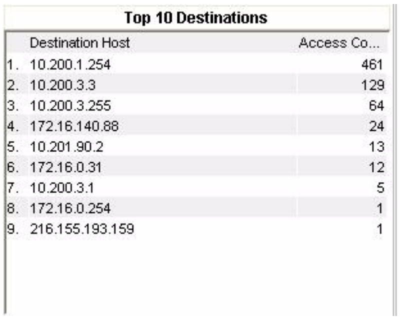
Top 10 User Sessions with Most Blocked Policy Inc...

	Username	IP Address	Total Incidents
1.	ins	10.200.3.1	3

Top 10 Destinations

The Top 10 Destinations table displays IP addresses of the top 10 destinations that users frequently visited, with the destination IP address that has the most hits being displayed at the top.

Figure 41 Top 10 Destinations



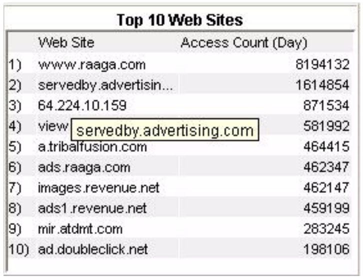
Top 10 Destinations

	Destination Host	Access Co...
1.	10.200.1.254	461
2.	10.200.3.3	129
3.	10.200.3.255	64
4.	172.16.140.88	24
5.	10.201.90.2	13
6.	172.16.0.31	12
7.	10.200.3.1	5
8.	172.16.0.254	1
9.	216.155.193.159	1

Top 10 Web Sites

The Top 10 Web Sites table displays the names of the top 10 sites visited by users, including the number of times each site was visited.

Figure 42 Top 10 Web Sites



Top 10 Web Sites

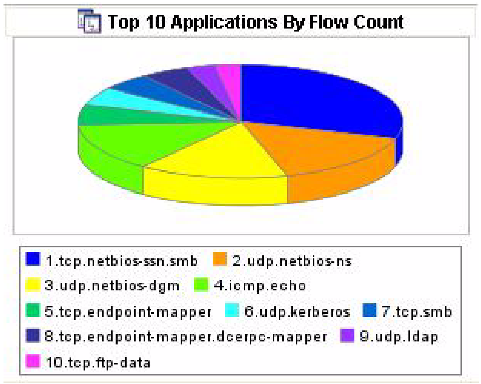
	Web Site	Access Count (Day)
1)	www.raaga.com	8194132
2)	servedby.advertisin...	1614854
3)	64.224.10.159	871534
4)	view	581992
5)	a.tribalfusion.com	464415
6)	ads.raaga.com	462347
7)	images.revenue.net	462147
8)	ads1.revenue.net	459199
9)	mir.atdmt.com	283245
10)	ad.doubleclick.net	198106

servedby.advertising.com

Top 10 Applications by Flow Count

The Top 10 Application by Flow Count table displays the names and the number of instances (destination IP and port pairs) of the top 10 applications by instances.

Figure 43 Top 10 Application by Flow Count

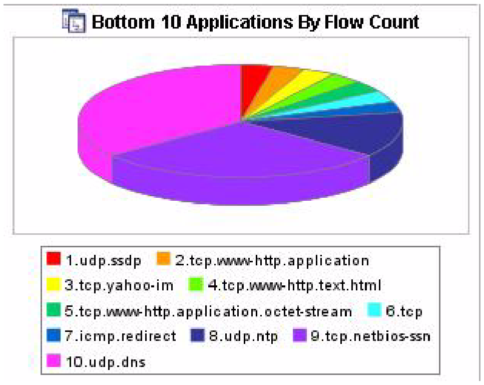


Click on the column header to display a list of applications, including all application instance details. You can also place the mouse cursor on the pie chart to display tooltips. For more information on viewing application instances, see *Viewing Application Instances*.

Bottom 10 Applications by Flow Count

The Bottom 10 Application by Flow Count table displays the names and the number of instances (destination IP and port pairs) of the last 10 applications by instances.

Figure 44 Last 10 Applications by Flow Count

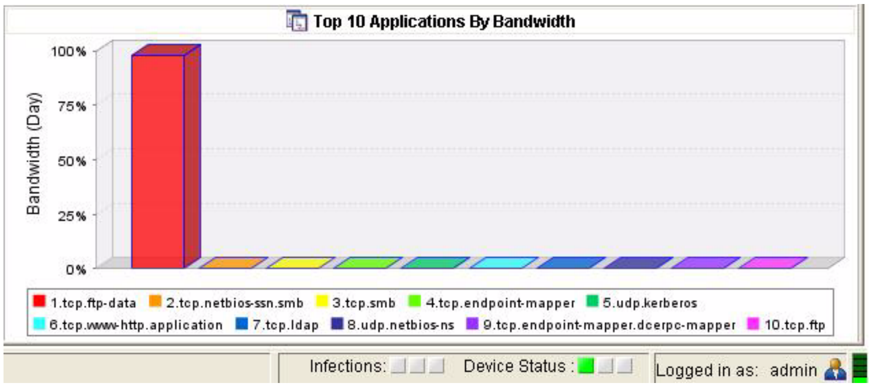


Click on the column header to display a list of applications, including all application instance details. You can also place the mouse cursor on the pie chart to display tooltips.

Top 10 Applications by Bandwidth (Bar Chart)

The Top 10 Applications by Bandwidth bar chart displays the names and usage of the top 10 applications by bandwidth. The bandwidth is shown in terms of percentage (%) usage.

Figure 45 Top 10 Applications by Bandwidth (Bar Chart)



Click on this panel to display a list of applications, including application details. Click on an individual bar to display the details for the selected application, including application statistics, number of users using the selected application, list of destination IP and port pairs (application instances). For more information on application types and instances, see *Viewing Application Types* and *Viewing Application Instances*.

Configuring Dashboards

If you find that the default pre-defined dashboards do not conform to your needs, OmniVista SafeGuard Manager allows you to copy the existing dashboards and then customize them accordingly or create new ones from scratch. Each dashboard comprises of the following three tabs:

- **Layout**—The Layout tab is where you define how the modules are positioned and displayed in a panel. This is where you also define the order in which the dashboards are to be displayed.

- **Modules**—Within any given module, you can configure bars. Each module should have a minimum of one bar. You can select the number of modules you want displayed and how they are displayed. The modules can be configured by the user and OmniVista SafeGuard Manager also comes with pre-defined system modules. The system modules within a dashboard can be of the following sizes:

  — Regular height and width

  — Pre-defined half-height

  — Pre-defined double-width (displays in two columns)

  The configurable modules will always be of regular height and width.

  Any user-configured modules can be cloned or edited; however, only the system modules that are of regular height and width (User Login Failures, Policy Incidents, Users with Policy Incidents, Malware, Unauthenticated User incidents, Posture incidents (Unhealthy, Bypass, Quarantine) can be cloned or modified on a global level, not on a per-user or per-role basis. Any newly cloned (copied) or created dashboard layout can then be modified to rearrange the layout. Any module can only be replaced with a module of the same size. For information on how to configure modules, see *Defining Modules within a Dashboard*

  NOTE: OmniVista SafeGuard Manager does not allow you to configure all modules. Only the User Login Failures, Policy Incidents, Users with Policy Incidents, Malware, Unauthenticated User incidents, Posture incidents (Unhealthy, Bypass, Quarantine) modules can be cloned or modified on a global level, not on a per-user or per-role basis.

- **Bars**—A bar is the smallest component of the dashboard that describes which query template is to be used. Each bar in a module corresponds to a query that retrieves data from the server. The Bar tab is where you define the bar display attributes and their titles. For more information on bars, see *Defining Bars within a Module*.

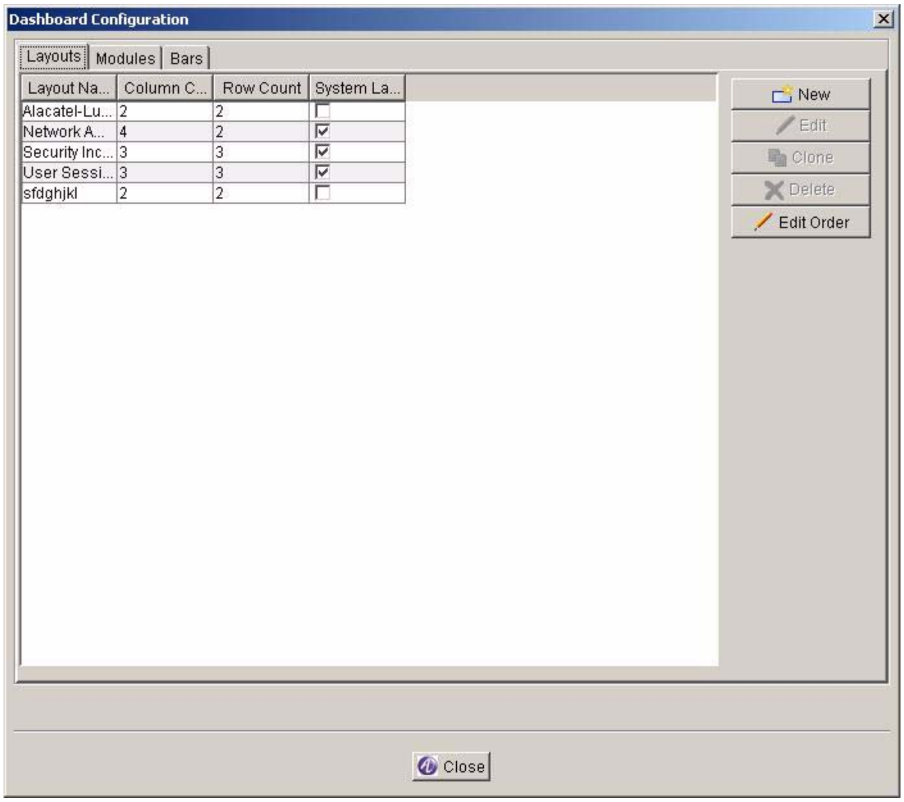
Defining Modules within a Dashboard

To create a new dashboard:

1 Click the Dashboard icon from the Page Bar or from the menu, select *View > Go To > Dashboard* (Ctrl + 0). The Dashboard displays.

2 Click the Configure icon from the Action Bar. The Dashboard Configuration screen displays (*Figure 46*).

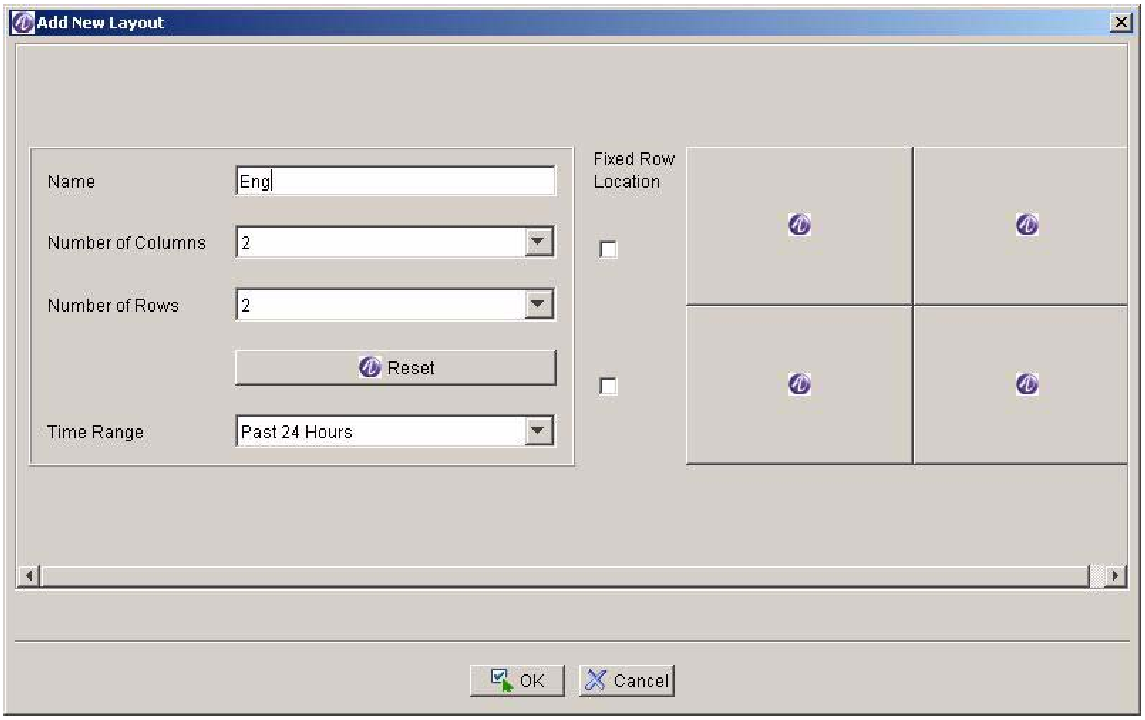
Figure 46 Dashboard Configuration



Layout Na...	Column C...	Row Count	System La...
Alacatel-Lu...	2	2	☐
Network A...	4	2	☑
Security Inc...	3	3	☑
User Sessi...	3	3	☑
sfdghjkl	2	2	☐

3 Click **New**. The Add New Layout window displays (*Figure 47*).

Figure 47 Add New Layout



Add New Layout

Name: Eng

Number of Columns: 2

Number of Rows: 2

Time Range: Past 24 Hours

4 Enter the configuration as follows:

Table 7 New Layout Attributes

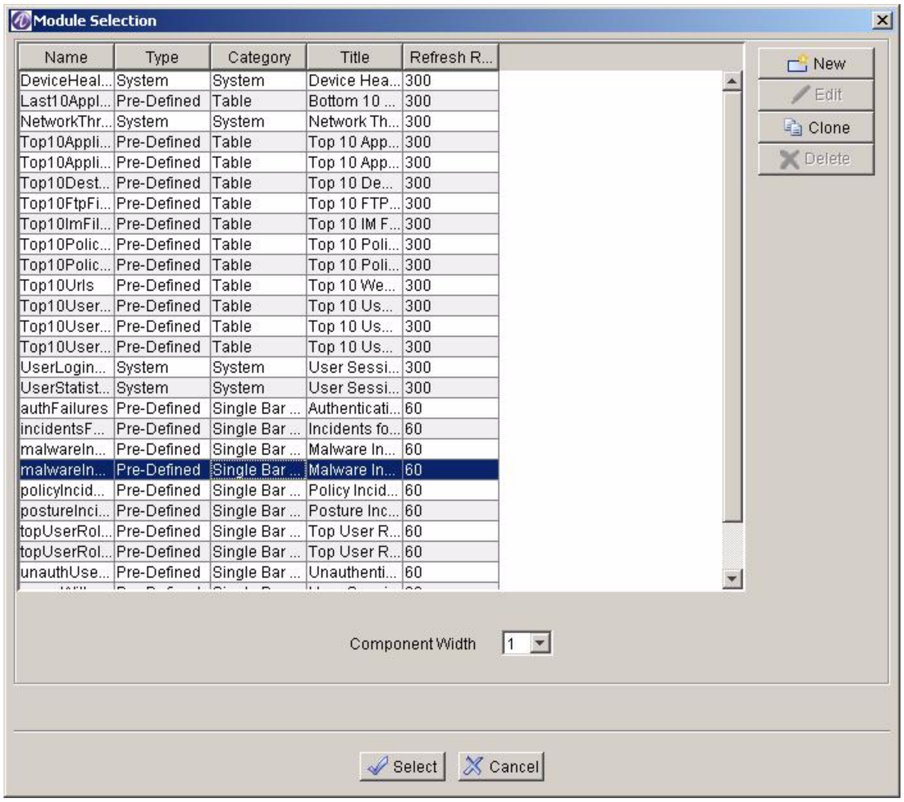
Attribute Name	Description
Name	Enter a name for the new dashboard.
Number of Columns	From the dropdown list, select the number of columns you want in the new dashboard.
Number of Rows	From the dropdown list, select the number of rows you want in the new dashboard.
Reset	Resets the dashboard values to the new values.
Time Range	Specify the time range for which you want to display data. This field uses the time filter applied in the bar chart and then applies the time range applied for the module. Valid values are: ■ Current day: current calendar day ■ Past 24 hours ■ Last hour

Table 7 New Layout Attributes *(continued)*

Attribute Name	Description
Fixed Row Location	Check the top checkbox if you want the fixed row to display at the top of the dashboard. Check the bottom checkbox if you want the fixed row to display at the bottom. Only specific modules are allowed in the fixed row area. For example, Device Health, User Statistics, Top 3 Role with policy incidents.

5 Click a module to configure it. The Module Selection screen displays (*Figure 48*).

Figure 48 Module Selection



Module Selection

Name	Type	Category	Title	Refresh R...
DeviceHeal...	System	System	Device Hea...	300
Last10Appl...	Pre-Defined	Table	Bottom 10 ...	300
NetworkThr...	System	System	Network Th...	300
Top10Appli...	Pre-Defined	Table	Top 10 App...	300
Top10Appli...	Pre-Defined	Table	Top 10 App...	300
Top10Dest...	Pre-Defined	Table	Top 10 De...	300
Top10FtpFi...	Pre-Defined	Table	Top 10 FTP...	300
Top10ImFil...	Pre-Defined	Table	Top 10 IM F...	300
Top10Polic...	Pre-Defined	Table	Top 10 Poli...	300
Top10Polic...	Pre-Defined	Table	Top 10 Poli...	300
Top10Urls	Pre-Defined	Table	Top 10 We...	300
Top10User...	Pre-Defined	Table	Top 10 Us...	300
Top10User...	Pre-Defined	Table	Top 10 Us...	300
Top10User...	Pre-Defined	Table	Top 10 Us...	300
UserLogin...	System	System	User Sessi...	300
UserStatist...	System	System	User Sessi...	300
authFailures	Pre-Defined	Single Bar ...	Authenticati...	60
incidentsF...	Pre-Defined	Single Bar ...	Incidents fo...	60
malwareIn...	Pre-Defined	Single Bar ...	Malware In...	60
malwareIn...	Pre-Defined	Single Bar ...	Malware In...	60
policyIncid...	Pre-Defined	Single Bar ...	Policy Incid...	60
postureInci...	Pre-Defined	Single Bar ...	Posture Inc...	60
topUserRol...	Pre-Defined	Single Bar ...	Top User R...	60
topUserRol...	Pre-Defined	Single Bar ...	Top User R...	60
unauthUse...	Pre-Defined	Single Bar ...	Unauthenti...	60

Component Width 1

6 Highlight a module name.

7 Select a Component Width. This allows you to specify whether your module will span a single column or more than one.

NOTE: How many columns you can have a module spanning depends on the column you are defining. For example, if you are defining a middle column in a three-column dashboard, you will only be able to span that module across two columns, because the first module may already have a column defined.

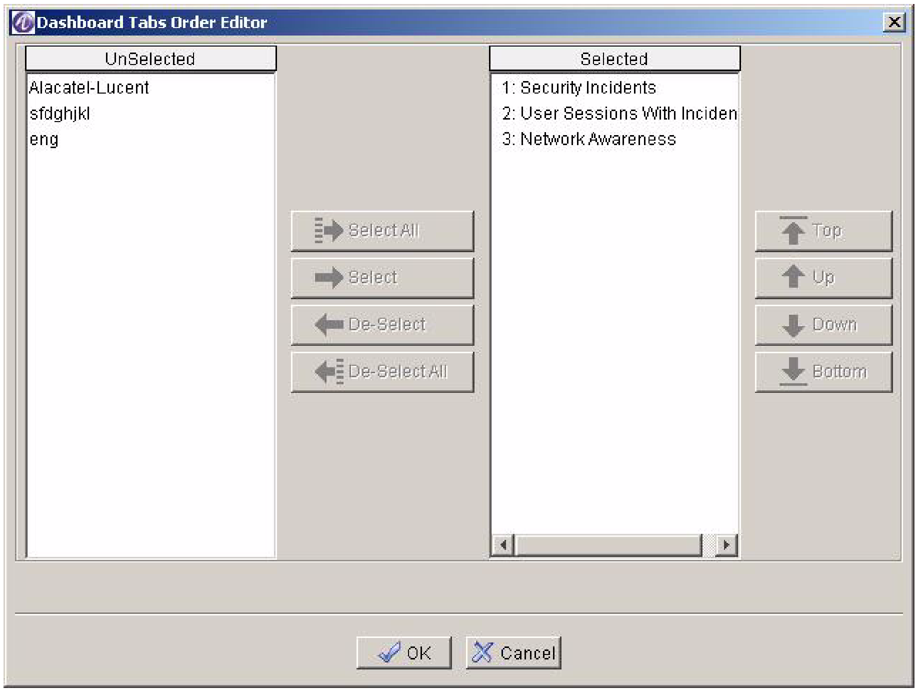
8 Click **Select**. The properties of the selected module are applied to the module in the new dashboard.

9 Repeat the process till all modules have been specified.

NOTE: Not all modules are configurable. If a module can be cloned or edited, the **Clone** and **Edit** buttons are available.

10 Click **Edit Order** on the Dashboard Configuration dialog box (*Figure 46*). The Dashboard Tabs Order Editor displays (*Figure 49*).

Figure 49 Dashboard Tabs Order Editor



Alacatel-Lucent
sfdghjkl
eng

1: Security Incidents
2: User Sessions With Inciden
3: Network Awareness

11 The Dashboard Tabs Order Editor allows you to select the order in which you want the dashboards to be displayed. Use the Tab Editor buttons as described to hide, display, or change the order tab in the dashboard view:

Table 8 Dashboard Tab Order Editor Buttons

Button Name	Function
Select All	Click **Select All** to move all the dashboards in the Selected column. All dashboards will display when you go to the dashboard view.
Select	Highlight a dashboard in the Unselected column and click **Select** to move the dashboard to the Selected column.

Table 8 Dashboard Tab Order Editor Buttons

Button Name	Function
De-select	Highlight a dashboard in the Selected column and click **De-select** to remove it from the selected list. This dashboard will not display as a tab when you go into dashboard view.
De-select All	Click **De-select All** to remove all dashboards from the selected list.
Top	Select a dashboard in the Selected column and click **Top** to move the dashboard to the top of the list. This dashboard will display as the first tab in the dashboard view.
Up	Select a dashboard in the Selected column and click **Up** to move the dashboard one level up in the list.
Down	Select a dashboard in the Selected column and click **Down** to move the dashboard one level down in the list.
Bottom	Select a dashboard in the Selected column and click **Bottom** to move the dashboard to the bottom of the list. This dashboard will display as the last tab in the dashboard view.

12 Click **OK** to apply the changes.

13 Click Refresh in the Action Bar to bring up the configured dashboards to the current dashboard. The dashboard tabs will appear in the order you specified.

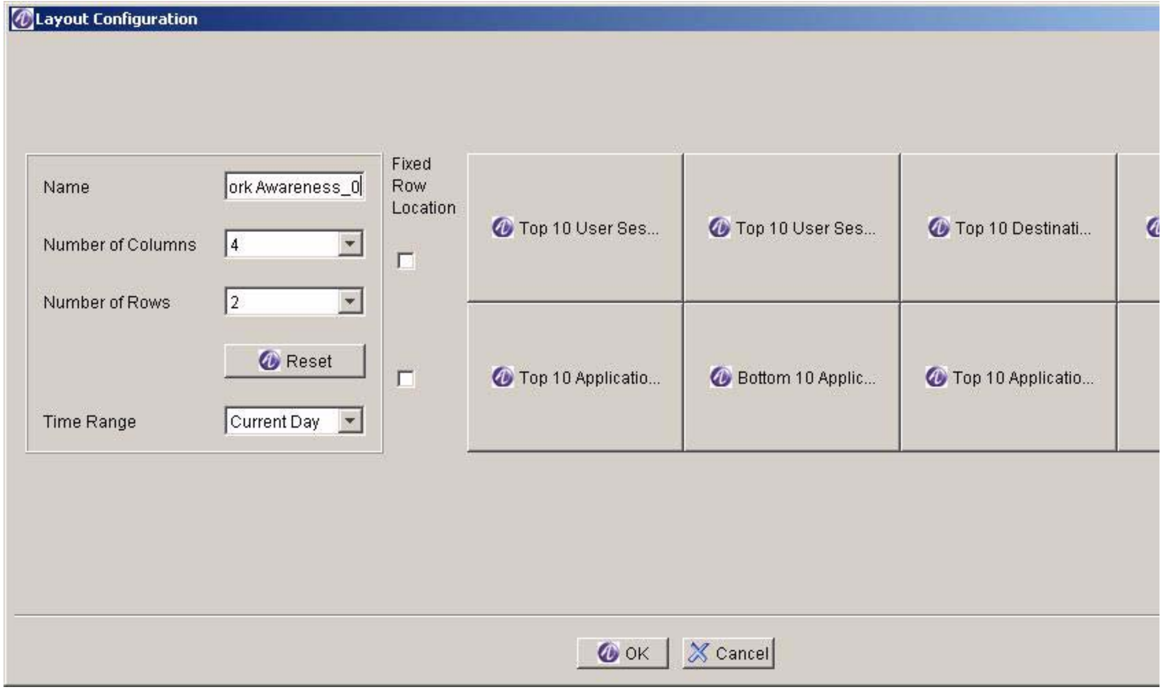
To clone or edit an existing dashboard:

1 In the Dashboards view, click the Configure icon from the Action Bar. The Dashboard Configuration screen displays (*Figure 46*).

2 Select a dashboard configuration that you want to clone or edit.

3 Click **Edit** to change the configuration or **Clone** to copy the configuration of the selected dashboard. The Layout Configuration screen displays (*Figure 50*).

Figure 50 Layout Configuration



Name: ork Awareness_0

Number of Columns: 4

Number of Rows: 2

Time Range: Current Day

4 Select the number of Rows and Columns using the dropdown lists.

5 Select the checkbox for whether you want the fixed row location to be on top or at the bottom.

6 Select the module that you want to change. The Module Selection screen displays (*Figure 48*).

7 If it's a user-configured module, the **Edit**, **Clone**, and **Delete** buttons will be active. Make the modifications as necessary and click **OK**.

NOTE: You can only delete a user-configured module. However, if the module properties are being used in another module or dashboard, an error message is displayed and deletion will not occur.

8 Use the **Order** button to change the order of the dashboard tabs. See *Table 8* for more information on using the **Order** button.

Using Pre-defined Modules

OmniVista SafeGuard Manager allows you to configure custom dashboards. Custom dashboards can be configured using modules that have been pre-defined. Some of these pre-defined modules are:

- Top 10 Applications by Bandwidth—top 10 applications defined by the percentage of usage.
- Top 10 Applications by Instances—top 10 applications by the frequency of application instances.
- Top 10 Destinations—top 10 destination IP addresses.
- Top 10 FTP Files—top 10 File Transfer Protocol (FTP) files either downloaded or uploaded.
- Top 10 IM Files—top 10 Instant Messenger (IM) instances sent or received.
- Top 10 Policy Incidents—top 10 policy incidents that occurred in the specified time range.
- Top 10 Policy Incidents Blocked—top 10 policy incidents that were blocked.
- Top 10 Users by Bandwidth—top 10 users by usage.

Defining Bars within a Module

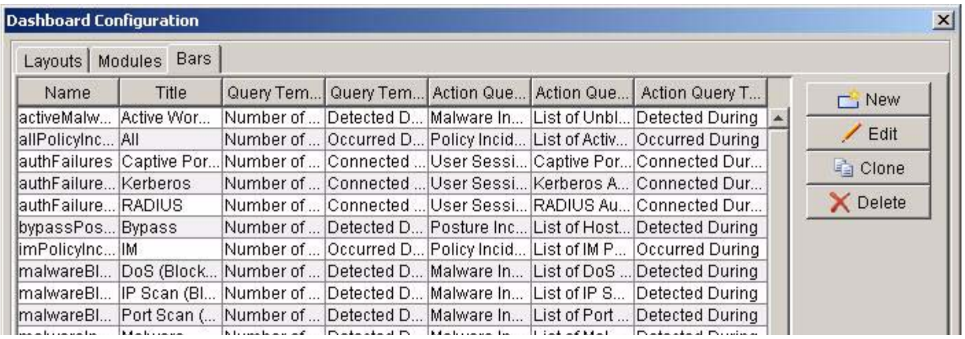
You can configure multiple bars within a module; however, each module should have at least one bar. Each bar within a module has an action query associated with it (this identifies the query that needs to be executed when you click on a bar). The associated query then retrieves data from the server. The following bar characteristics should be noted when defining bars:

- System bars cannot be deleted or cloned.
- Pre-defined bars can be cloned but cannot be deleted.
- User-defined bars can be edited and cloned but can only be deleted if the bar properties are not being used in any other module.

To define bars within a module:

1 On the Dashboard Configuration screen (*Figure 46*), select the Bars tab. The following view displays.

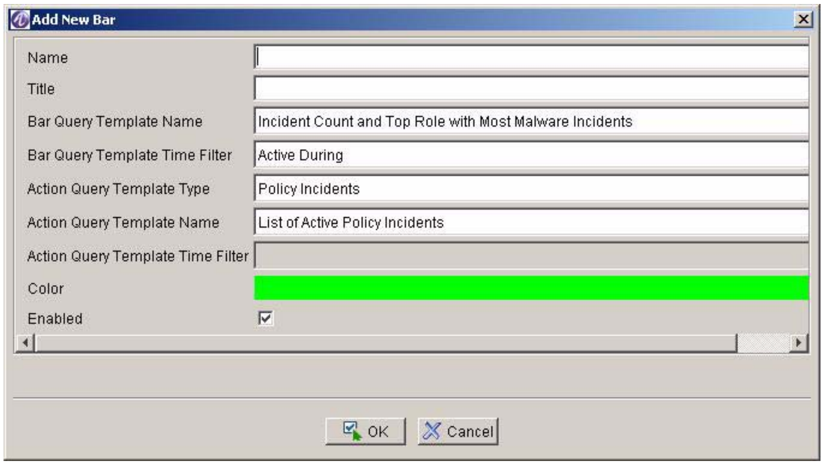
Figure 51 Dashboard Configuration - Bars



Name	Title	Query Tem...	Query Tem...	Action Que...	Action Que...	Action Query T...
activeMalw...	Active Wor...	Number of ...	Detected D...	Malware In...	List of Unbl...	Detected During
allPolicyInc...	All	Number of ...	Occurred D...	Policy Incid...	List of Activ...	Occurred During
authFailures	Captive Por...	Number of ...	Connected ...	User Sessi...	Captive Por...	Connected Dur...
authFailure...	Kerberos	Number of ...	Connected ...	User Sessi...	Kerberos A...	Connected Dur...
authFailure...	RADIUS	Number of ...	Connected ...	User Sessi...	RADIUS Au...	Connected Dur...
bypassPos...	Bypass	Number of ...	Detected D...	Posture Inc...	List of Host...	Detected During
imPolicyInc...	IM	Number of ...	Occurred D...	Policy Incid...	List of IM P...	Occurred During
malwareBl...	DoS (Block...	Number of ...	Detected D...	Malware In...	List of DoS ...	Detected During
malwareBl...	IP Scan (Bl...	Number of ...	Detected D...	Malware In...	List of IP S...	Detected During
malwareBl...	Port Scan (...	Number of ...	Detected D...	Malware In...	List of Port ...	Detected During

2 Click **New** if you want to add a new bar. The Add New Bar screen displays (*Figure 52*).

Figure 52 Add New Bar



Name	
Title	
Bar Query Template Name	Incident Count and Top Role with Most Malware Incidents
Bar Query Template Time Filter	Active During
Action Query Template Type	Policy Incidents
Action Query Template Name	List of Active Policy Incidents
Action Query Template Time Filter	
Color	🟩
Enabled	☑

3 Enter the bar configuration as follows:

Table 9 Add New Bar Attributes

Attribute	Description
Name	Name for the bar.
Title	Title for the bar.
Bar Query Template Name	From the dropdown list, select a query template that will retrieve data from the database.
Bar Query Template Time Filter	Specify a time filter for the bar, this is the time filter that will be applied when collecting counts, for example top 10.
Action Query Template Type	From the dropdown list, select the visualization data type: User, Malware incidents, Policy incidents, and so forth.
Action Query Template Name	From the dropdown list, select an action type: All active users, Kerberos authentication failures, List of users with active worms, and so forth.
Action Query Template Time Filter	Identify the time filter for the action query. This attribute is only available if a time filter was not set during the query definition.
Color	Click the color bar. A color template is displayed where you can select the bar color.
Enabled	Select the Enabled checkbox to enable the bar.

4 Click **OK** for the configuration to apply.

5 Select a bar in the Bar tab of the Dashboard Configuration screen and click **Edit** to modify an existing bar configuration.

6 Select a bar and click **Clone** to copy the configuration of an existing bar.

7 Select a bar and click **Delete** to remove the bar from a given module.

NOTE: You can only delete a user-configured bar. However, if the bar properties are being used in another bar or module, an error message is displayed and deletion will not occur.

Viewing Visualization Data

Visualization allows administrators to track what a user is doing, what applications are being used, and what is being done to a network. Such tracking is useful for forensic and postmortem purposes, that is, for debugging and ensuring that the network is performing at its optimum and there are no threats to the network. SafeGuard collects this data (traffic flow, Layer 7, malware events from the CPU, policy events from policy, and authentication events from Auth) and periodically pushes it in tabular format to OmniVista SafeGuard Manager as visualization data.

Visualization data can be viewed in tabular format for the following objects:

Table 10 Visualization Data Objects

Table Type	Description
Policy Incidents	Displays a list of all policy incidents against a user. For more information, see *Viewing Policy Incidents*.
Malware Incidents	Displays a list of malware incidents. This table also displays the counts of various severities of the infection events. For more information, see *Viewing Malware Incidents*.
Posture Incidents	Displays all posture incidents, including EPV incident ID, host IP and MAC addresses. For more information, see *Viewing Posture Incidents*.
User Sessions	Displays user authentication and bandwidth usage that is aggregated for each user. Typically this has a navigation tree on the left panel that helps finds users belonging to a specific group/role or connected to a specific port of a specific device. For more information, see, Viewing User Sessions.
Application Type	Displays the user bandwidth usage that is aggregated for each type of application. For more information, see *Viewing Application Types*.
Application Instance	Displays the user bandwidth usage for each user, application type, destination port, and destination IP address. For more information, see *Viewing Application Instances*.
Application Flows	Allows an administrator to view application flows for a selected user or application. For more information, see *Viewing Application Flows*.

Viewing Policy Incidents

When policy conditions are matched for any given user, policy incidents are created. To view policy incidents:

1 Click the View Policy Incidents icon from the Page Bar or select *View > Go To > Policy Incidents* (Ctrl + 1) menu item. The All Events view displays with the following information

Table 11 Policy incidents Attributes

Attribute	Description
Username	Username in violation of a policy.
First Occurrence	Time the violation first occurred.
Last Occurrence	Displays the time of the last policy violation.
# of Occurrences	Number of times the violation occurred.
Policy Name	Name of the policy that is applied.
Policy Filter	Applicable policy filters.
Policy Action	Action taken when the policy violation occurred.
Application Name	Application that was being used when the policy violation occurred.
Protocol	Protocol being used, TCP or UDP.
MAC Address	MAC address of the user's machine.
Source IP Address	Originating IP address of the machine at which the policy violation was detected.
Destination IP Address	Destination IP address of the machine to which the policy violation is reaching.
Severity	Identifies if the policy violation is major.
Policy Category	Category for the policy violation. Can be one of two pre-defined categories (resource access, application control) or can be a user-defined string. If a category is not defined, this column displays blank.
Violation Status	Violation status, whether the violation has been cleared.
Authentication Status	Authentication status for the user, authenticated or unauthenticated.
Authentication Role	Authentication role for the user.
User Status	Status for the user, active or inactive.

2 Search the data displayed locally in the table view by clicking the Find icon in the Action Bar. A free-form text search field is displayed. Enter a keyword in the text field to define your search. To search the database, click the **Database Search**

button in the Find field. For more information on using the search and sort features, see Chapter 3, General Navigation.

3 To view specific incidents by status, location, role, or category, use the attributes in the left column. For more information on using the left column fields, see Chapter 3, General Navigation.

4 Select a row and click **Clear** to clear the policy violation and put it in history.

5 Select a row and click **Delete** to delete the violation record from the database.

6 Click **User Details** in the Action Bar to get a detailed view of the user activity.

7 Highlight a row to get a detailed view of the selected policy violation in the bottom half of the screen. The details view shows a detailed view of the user and machine in violation, including policy name, policy severity, action taken, and so on.

8 Highlight a policy incident and right-click to select **Show Policy Config** to display the policy configuration screen for the selected incident. A confirmation dialog box displays before you can view the configuration information. See *Policies* for more information on policy configuration.

9 Click **Refresh** to get the latest policy incidents from the server.

10 Click **Export** to export the table details into a CSV file that can easily be exported into an Excel worksheet.

11 Click **Print** to print the data to a networked printer.

Viewing Malware Incidents

The term *malware* is derived from *malicious software*, which is any program or file that is harmful to a computer system. Common types of malware include computer viruses, worms, Trojan horses, and spyware.

When SafeGuard OS detects malware on the system, malware policies specify how the infection is handled. For more information on how SafeGuard OS detects and isolates malware security threats, see the *OmniAccess SafeGuard OS Administration Guide*. These malware policies specify how much or how little access a user or an application has to the network when it is suspected of being infected. OmniVista SafeGuard Manager allows administrators to view all malware incidents and clear or whitelist any incidents on a per-user or per-application basis, if necessary.

To view all malware incidents:

1 Click the View Malware Incidents icon from the Page Bar or select *View > Go To > Malware Incidents* (Ctrl + 2) menu item. The All Malware Incidents view displays the following information:

Table 12 Malware Attributes

Attribute	Description
Time	Time the malware incident was detected.
Malware Action	Action taken against the malware incident.
Severity	Severity level of the malware incident.
Category	Category to which the malware incident belongs.
Algorithm	Algorithm used to identify whether the suspected malware is actually malware.
Application	Application that was being used at the time of malware detection.
Application Group	The name of the application group to which the infected application belongs. An application group is a collection of application protocols.
# of Connections	Number of connection attempts.
Time taken to Detect	Time it took to detect the malware incident.
Username	User name that created the malware violation.
Computer Name	Name of the computer from which the malware incident originated.
MAC Address	MAC address of the computer from which the malware incident originated.
Source IP Address	Originating IP address where malware was detected.
Destination IP Address	Destination IP address.

Table 12 Malware Attributes *(continued)*

Attribute	Description
Protocol	Protocol being used: TCP or UDP.
History	History of the last 8 malware incidents. When you place your cursor on the history column, a tooltip displays up to 8 IP addresses related to the specific incident. This is very helpful for diagnostic purposes, to see what algorithm was used to determine that this is actually an incident and what other IP address are impacted.
Cleared Time	Time the malware is cleared. The cleared time is shown in History view only.
Authentication Status	Authentication status for the user, authenticated or unauthenticated.
Authentication Role	Authentication role for the user.
User Status	User Status: Active or inactive.

2 Search the data displayed locally in the table view by clicking the Find icon in the Action Bar. A free-form text search field is displayed. Enter a keyword in the text field to define your search. To search the database, click the **Database Search** button in the Find field. For more information on using the search and sort features, see Chapter 3, General Navigation.

3 Use the navigation tree to the left to view malware incidents by the type of infection (quarantined, action taken, malware category, detection algorithm), role, or location. For more information on using the left column fields, see *Chapter 3, General Navigation*.

4 Select a row and click **Clear** to clear the infection event and enable the device. For example, if the option was set to block the host and the host is infected, the device sends an alert. OmniVista SafeGuard Manager takes the appropriate action to either just log or block it. When you select Clear, you remove the malware event and tell OmniVista SafeGuard Manager to let the host pass through.

NOTE: A malware event can be cleared either at the device level or through OmniVista SafeGuard Manager. After the device detects that the malware does not exist, it can send a clear event or the user can clear the event from OmniVista SafeGuard Manager.

5 Select a row and click **Whitelist**, which adds a white list to the user and any traffic from the user will not be considered for malware detection. A confirmation dialog box displays asking you to select **Yes** to proceed or **No** to cancel.

6 Click **User Details** to get a detailed view of the user activity.

7 Highlight an incident to get a detailed view of the selected malware instance. The Infection Details view at the bottom of the screen shows the detailed view of the

user machine, allowing you to traverse through the details and see what applications the user is using, the infections and the policy incidents against the user. This is helpful in diagnostics purposes and can help the administrator to narrow down the problem and identify where the problem exists.

8 Click **Refresh** to get the latest malware events.

9 Click **Application Flows** in the Action Bar to view application flows affected in the neighborhood (plus or minus time specified) of the malware event. For more information, see *Malware Incident Tracking and Troubleshooting*.

Malware Incident Tracking and Troubleshooting

OmniVista SafeGuard Manager allows administrators to view application flows related to malware incidents. This feature helps administrators to narrow down the time window in which a specific malware incident occurred, highlight the application flow in proximity to that incident, and thus troubleshoot the incident as needed.

To view application flows in relation to a malware incident:

1 Select View Malware Incidents from the Page Bar.

2 Highlight the malware incident for which you want to see application flow detail.

3 Click **Application Flows** in the Action Bar. The Application Flows screen displays.

4 In the left-hand navigation column, select the status of Active for all active application flows, Inactive for all inactive application flows, and Active or Inactive for all flows.

5 Reference Time displays the time the malware incident occurred; this helps you to specify the time range for the application flows in reference to the malware incident.

6 Use the Time Range field to configure a time in seconds of plus or minus 5, 10, 30, or 60 seconds in which you want to see all application flows in relation to the selected malware incident. For example, if you select +/- 5 seconds, all application flows in proximity of the selected malware incident (+/- 5 seconds) will display.

7 Apply a time filter of Any Occurrence, First Occurrence, or Last Occurrence.

8 Click **Refresh** to view the updated data.

Viewing Posture Incidents

The term "*posture*" refers to a collection of attributes that play a role in the conduct or health of a device that is seeking network access. Some of these attributes relate to the endpoint device-type and operating system; and other belong to various security applications that might be present on the endpoint, such as anti-virus (AV) scanning software.

Posture validation refers to the act of applying a set of rules to the posture data to provide an assessment of the level of trust that you can place in that endpoint. Posture incidents; therefore, are any events that are in violation and suspect the health of an endpoint device.

To view all posture incidents:

1 Click the View Posture Incidents icon from the Page Bar or select *View* > *Go To* > *Posture Incidents* (Ctrl + 3) menu item. The All Posture Infections view displays the following information:

Table 13 All Posture Incidents Attributes

Attribute Name	Description
State	State, active or inactive.
Host IP	IP address for the host.
Host MAC	MAC address for the host.
Time	Time the posture incident occurred.
Status Message	Status Message
Device IP	IP Address for the device.
EVP Incident ID	Identifier for the EVP incident.

2 To view specific incidents by status, location, role, or category, use the attributes in the left column. For more information on using the left column fields, see Chapter 3, General Navigation.

3 Click **Refresh** to see the updated incidents.

4 Click **Find** to apply a textual or advanced search in the table shown in All Posture Incidents. For more information on using the search and sort features, see Chapter 3, General Navigation.

Viewing User Sessions

You can view visualization data, network activity per user or for all users.

To view all users:

1 From the Dashboard, click on the Total Users row in the User panel, click the View Users icon from the Page Bar, or select the *View* > *Go To* > *Users* (Ctrl +4) menu item. The All Users screen displays with the following information:

Table 14 User Attributes

Attribute	Description
Username	User name as detected by the authentication (login ID).
Source IP Address	IP address of the user’s interface.
MAC Address	MAC address of the user’s interface.
Bandwidth	Bandwidth that the user is using.
Authentication Status	Current state of the user: authenticated, unauthenticated, or authentication failed.
Authentication Role	Role derived for this user based on authentication protocol, server, and user name.
Authentication Type	Type of authentication. The values can be: ■ krb: Windows AD/Kerberos v5 passive sniffing ■ captive-portal: HTTP-based active authentication ■ unauthenticated: Guest users
Authentication IP	IP address of the authentication server
Computer Name	Name of the computer the user is using.
Login Time	Time the user logged in.
Device Physical Port	Physical port of the Alcatel-Lucent device (SafeGuard OS) on which the user is detected.
VLAN	VLAN on which the user is detected.
Domain	Name of the domain to which the user is identified.
User ID	Identifier for the user.
Logout Time	Time the user logged out. The logout time is shown in History view only.

2 Search the data displayed locally in the table view by clicking the Find icon in the Action Bar. A free-form text search field is displayed. Enter a keyword in the text field to define your search. To search the database, click the **Database Search**

button in the Find field. For more information on using the search and sort features, see Chapter 3, General Navigation.

NOTE: Some data might be excluded from the display because visualization filters may have been applied. You can disable the filters if you want to store or display all data. Disabling the filters will not retrieve previously filtered data; however, new data will be stored. For more information on visualization filters, see *Setting Visualization Filters*.

3 To view specific users by status, location, role, or category, use the attributes in the left column. For more information on using the left column fields, see *Chapter 3, General Navigation*.

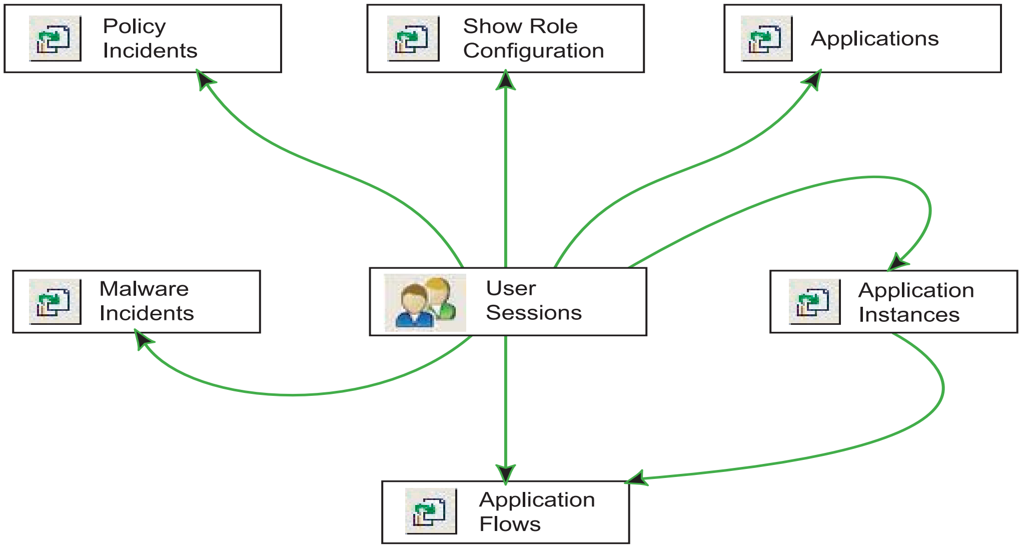
4 Select a user and click **Clear User** to reset the authentication state for the selected user. The user is treated as unauthenticated and needs to be authenticated.

5 Highlight a user to view user details for the selected user in the bottom-half of the screen. The detailed view shows all activity and application instances for the selected user.

6 Highlight a user and click **Show Role Config** in the Action Bar to display the role configuration information for the selected user. See *Roles* for more information on configuring roles.

7 Select a user and click an Action Bar icon to display a different table view for the selected user. *Figure 53* shows the different views you can access from the Users view.

Figure 53 Other Table Views from a Selected User View



8 Click **Refresh** to view the updated visualization data.

9 Click **Export** to export the table details into a CSV file that can easily be exported into an Excel worksheet.

10 Click **Print** to print the data to a networked printer.

Viewing Application Types

The application view displays the type of application being used (HTTP, FTP, and so forth).

To view all application types:

1 Click the View Applications icon from the Page Bar or select *View* > *Go To* > *Applications* (Ctrl + 5) menu item. The All Application Type screen displays with the following information:

Table 15 Application Attributes

Attribute	Description
Application	Application type.
Protocol	Protocol the application is using: TCP or UDP.
Application ID	Identifier for the application.
Bandwidth	Bandwidth that the application is using.

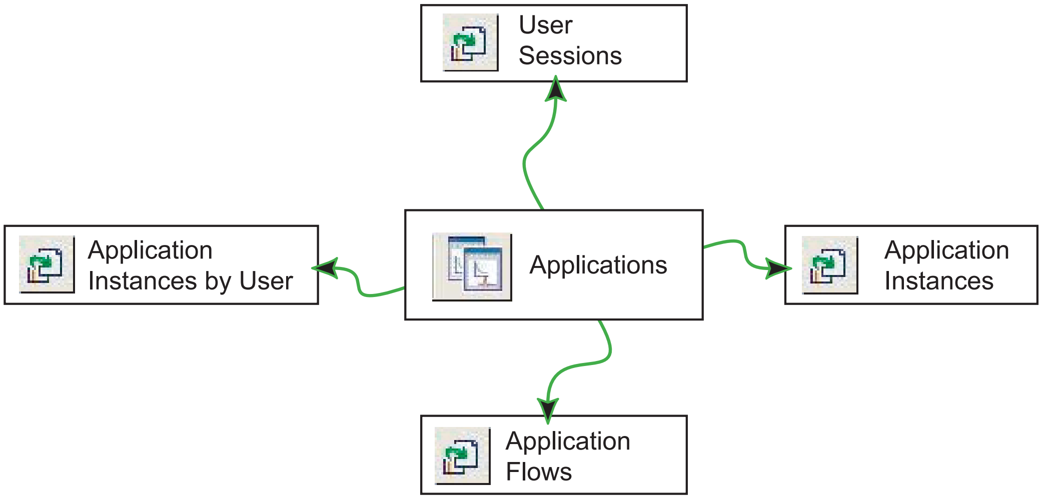
2 Search the data displayed locally in the table view by clicking the Find icon in the Action Bar. A free-form text search field is displayed. Enter a keyword in the text field to define your search. To search the database, click the **Database Search** button in the Find field. For more information on using the search and sort features, see Chapter 3, General Navigation.

3 To view specific incidents by status, location, role, or category, use the attributes in the left column. For more information on using the left column fields, see Chapter 3, General Navigation.

4 Highlight a row to get detailed information on the selected application type. The details appear in the bottom-half of the screen.

5 Select a row and click an Action Bar icon to display a different table view for the selected application. *Figure 54* shows the different views you can access from the Applications view.

Figure 54 Other Table Views from Application View



6 Click **Refresh** to view the updated visualization data.

7 Click **Export** to export the table details into a CSV file that can easily be exported into an Excel worksheet.

8 Click **Print** to print the data.

Viewing Application Instances

To view all application instances:

1 Click the View Application Instances icon from the Page Bar or select *View* > *Go To* > *Application Instances* (Ctrl + 6) menu item. The All Application Instances screen displays with the following information:

Table 16 Application Instances Attributes

Attribute	Description
Username	Name of the user for whom the instance is recorded.
Application	Application type.
Protocol	Protocol the application is using: TCP or UDP.
Source IP Address	IP address where the application instance originated.
Destination IP Address	Destination IP address for the application instance.
Destination Port	Destination port for the application instance.
Bytes In	Total number of incoming bytes.
Bytes Out	Total number of outgoing bytes.

Table 16 Application Instances Attributes *(continued)*

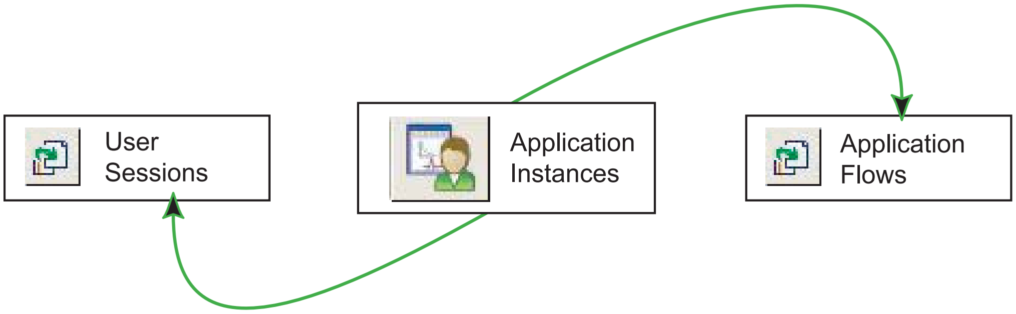
Attribute	Description
Packets In	Total number of incoming packets.
Packets Out	Total number of outgoing packets
Application Instances	Total number of application instances.
Deny Traffic from Host - side IP	Deny traffic originating from host-side IP address.
Deny Traffic to Host-side IP	Deny traffic that is directed to host-side address.

2 Search the data displayed locally in the table view by clicking the Find icon in the Action Bar. A free-form text search field is displayed. Enter a keyword in the text field to define your search. To search the database, click the **Database Search** button in the Find field. For more information on using the search and sort features, see Chapter 3, General Navigation.

3 Highlight a row to get a detailed summary of the selected application instance in the bottom-half of the screen.

4 Select a row and click the App Flows icon from the Action Bar to get application flows for the selected application instance. The Application Flows view gives a detailed view of all application instances for the selected user. For more information on using the Application Flows view, see *Viewing Application Flows*. *Figure 55* shows the other views that you can access for the selected application instance.

Figure 55 Other Table Views from Application Instances View



5 Click **Refresh** to view the updated visualization data.

6 Click **Export** to export the table details into a CSV file that can easily be exported into an Excel worksheet.

Viewing Application Flows

To view application flows:

1 Click the View Application Flows icon from the Page Bar or select *View* > *Go To* > *Application Flows* (Ctrl + 7) menu item. The Application Flows view displays, giving a detailed view of all user activity for the selected user.

2 Search the data displayed locally in the table view by clicking the Find icon in the Action Bar. A free-form text search field is displayed. Enter a keyword in the text field to define your search. To search the database, click the **Database Search** button in the Find field. For more information on using the search and sort features, see Chapter 3, General Navigation.

3 Select a row and click **Layer 7 Events** from the Action Bar to get a detailed Layer 7 view of the application instance, including the event ID, time stamp, event type, and Layer 7 event details.

4 Select a row on the Application Flows view to get a flow summary for the selected user in the bottom-half of the screen.

5 Click **Refresh** to apply any search or sort filters and display the latest data from the database.

6 Click **Export** to export the table details into a CSV file that can easily be exported into an Excel worksheet.

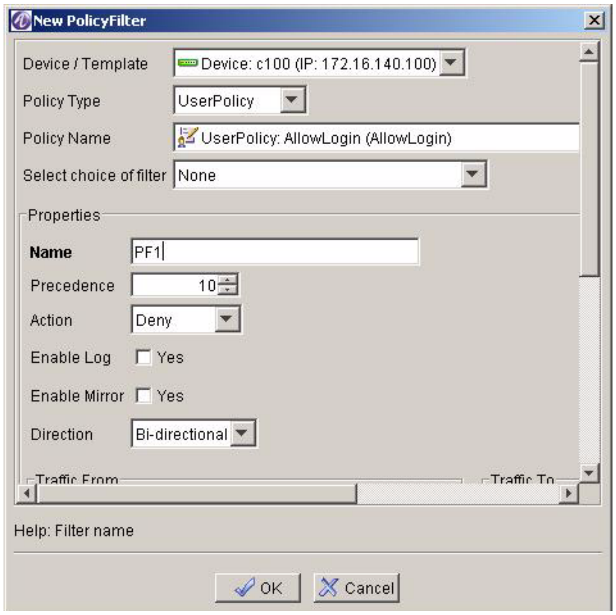
Creating Policy Filters

OmniVista SafeGuard Manager allows you to create a policy filter from data available in an application flow.

To create a policy filter:

1. Click the View Application Flows icon in the Page Bar.
2. Select a data flow line and right-click to select Create Policy Filter. The New Policy Filter screen displays (*Figure 56*).

Figure 56 Create New Policy Filter



Device / Template: Device: c100 (IP: 172.16.140.100)

Policy Type: UserPolicy

Policy Name: UserPolicy: AllowLogin (AllowLogin)

Select choice of filter: None

Name: PF1

Precedence: 10

Action: Deny

Enable Log: □ Yes

Enable Mirror: □ Yes

Direction: Bi-directional

Help: Filter name

3. Enter the information as follows:

Table 17   New Policy Filter Attributes

Attribute	Description
Device/Template	From the dropdown list, select either a device or a template for which you want to define a new policy filter.
Policy Type	Select the type of policy for which you are creating this filter: user, malware, or override.
Policy Name	Select the policy name to which the filter is to be applied.

Table 17 New Policy Filter Attributes

Attribute	Description
Select choice of filter	From the dropdown list, select the type of filter. Valid values are: ■ None ■ Block user ■ Deny traffic originating from user ■ Deny traffic to user ■ Deny traffic from user to network IP ■ Deny traffic from network-side IP to user ■ Deny traffic from network-side IP ■ Deny traffic to network-side IP
Name	Specify a brief name for the new policy filter.
Action	Select an action: Deny, Reset TCP, or Permit.
Enable Log	Select this checkbox if you want a log entry to be created.
Enable Mirror	
Direction	Select the direction in which the policy filter is to be applied, bi-directional, flow-in, or flow-out. For more information on traffic direction, see *Traffic Flow*.

4 Click **OK** to create the filter.

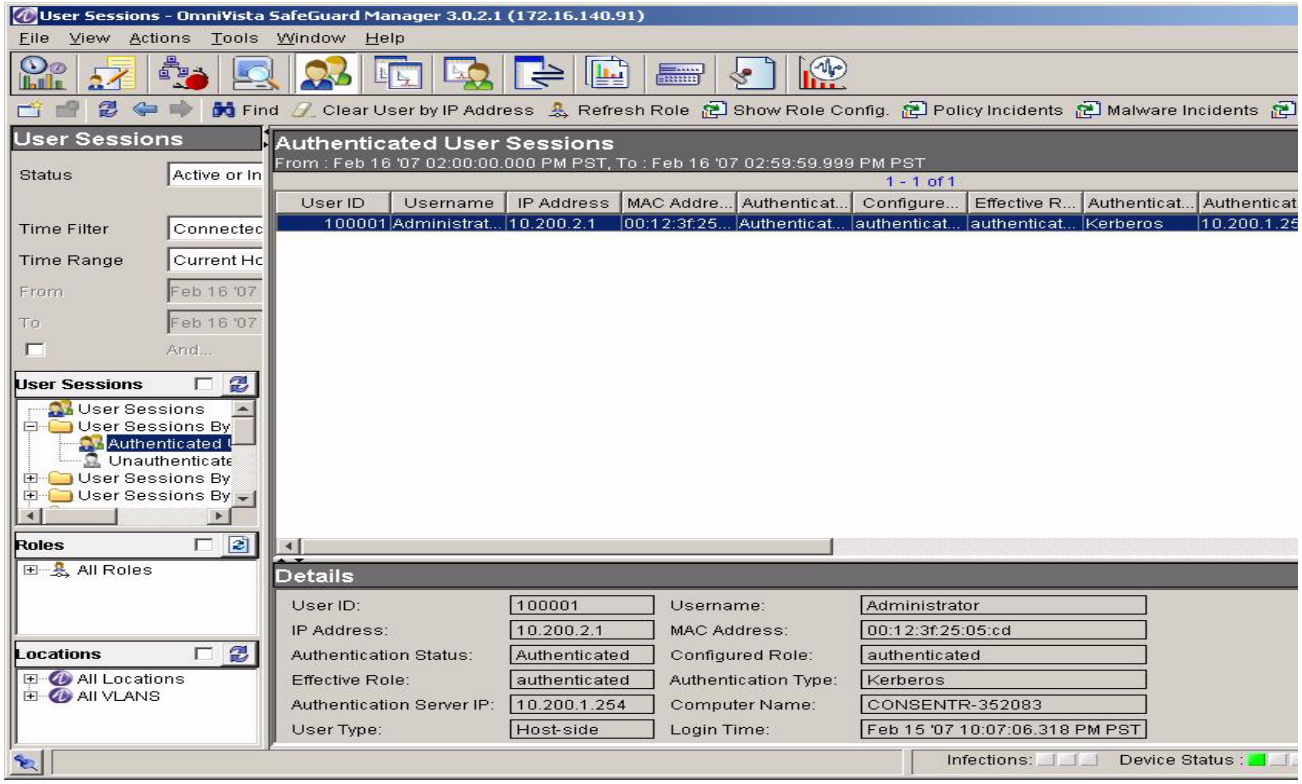
Viewing Time-based Data

OmniVista SafeGuard Manager allows you to apply time filters in the navigational views. Using these time filters, you can specify a time range for which you want to view data. These navigational views also allow you to view data that can be active or inactive and is within the time range specified.

To view data within a specific time range:

1 Click on a Page Bar icon to get a table view (*Figure 57*).

Figure 57 View All User Sessions



User Sessions

Status: Active or In

Time Filter: Connectec

Time Range: Current Hc

From: Feb 16 '07

To: Feb 16 '07

□ And...

Authenticated User Sessions

From : Feb 16 '07 02:00:00.000 PM PST, To : Feb 16 '07 02:59:59.999 PM PST

1 - 1 of 1

User ID	Username	IP Address	MAC Addre...	Authenticat...	Configure...	Effective R...	Authenticat...	Authenticat
100001	Administrat...	10.200.2.1	00:12:3f:25...	Authenticat...	authenticat...	authenticat...	Kerberos	10.200.1.25

Details

User ID: 100001
Username: Administrator
IP Address: 10.200.2.1
MAC Address: 00:12:3f:25:05:cd
Authentication Status: Authenticated
Configured Role: authenticated
Effective Role: authenticated
Authentication Type: Kerberos
Authentication Server IP: 10.200.1.254
Computer Name: CONSENTR-352083
User Type: Host-side
Login Time: Feb 15 '07 10:07:06.318 PM PST

2 In the left column, set the Status as Active to view active data or Inactive to view historical data. You can also select Active or Inactive to view all data.

3 Use the Time Range dropdown list to specify a time period for which you want to view data. Current Hour is selected as the default.

4 Select Custom in the Time Range field to activate the To and From fields. Clicking on this dropdown list brings up a calendar and timestamp that allows you to select a specific date and time for which the data is to be displayed.

5 Use the Time Filter dropdown list to specify the time filter. Connected During Time Range is selected as the default; therefore, whatever you specify in the Time Range field will impact the data displayed.

6 Click **Refresh** to update the view.

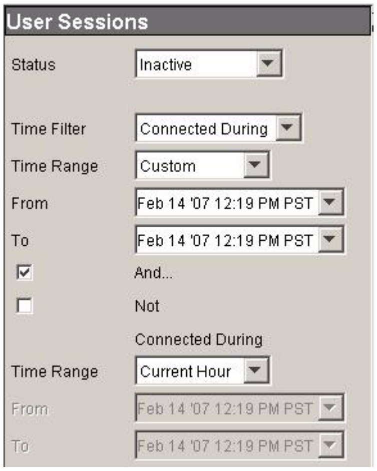
Additional Time-based Filtering

For certain views (application and users), you can apply additional time filters to exclude or include data from the original time-based query. For example, if your initial query was to show users logged in between 4:00pm to 5:00pm, you can use the additional exclude filters to show users not logged in between 3:00pm to 4:00 pm.

To apply additional filtering:

1 Click on the **And...** toggle button in the Time Range specification panel of the navigation tree (*Figure 57*). The time filters are expanded (*Figure 58*).

Figure 58 Additional Time Filters



User Sessions

Status: Inactive

Time Filter: Connected During

Time Range: Custom

From: Feb 14 '07 12:19 PM PST

To: Feb 14 '07 12:19 PM PST

☑ And...

□ Not

Connected During

Time Range: Current Hour

From: Feb 14 '07 12:19 PM PST

To: Feb 14 '07 12:19 PM PST

2 Select the Not checkbox to exclude the data from the original time range, compared to the data specified in the new time range.

3 The Time Filter that you selected previously is displayed as a read-only field. If you need to change the Time Filter, see Viewing Time-based Data.

4 Select a new time range using the Time Range dropdown list. OmniVista SafeGuard Manager validates this selection to ensure that the time range selected is not the same as the original time range.

5 Refresh the page to apply the new time filters.

Viewing Active Data Against Historical Data

Active data is generated while the user is logged in. Data is considered history (inactive) when the user logs out. Whenever any data or events are cleared, they also become part of history.

NOTE: Malware and Posture events are host based; therefore, they are not considered history when the user logs out. These events must be cleared for them to be history.

Searching Active or Inactive Data within a Specified Time Range

OmniVista SafeGuard Manager allows you to search for active or inactive data within a specified time range (*Figure 57*). This example uses a search for active applications and application instances within a specified time range.

Figure 59 Search Active or Inactive Data within Specified Time Range

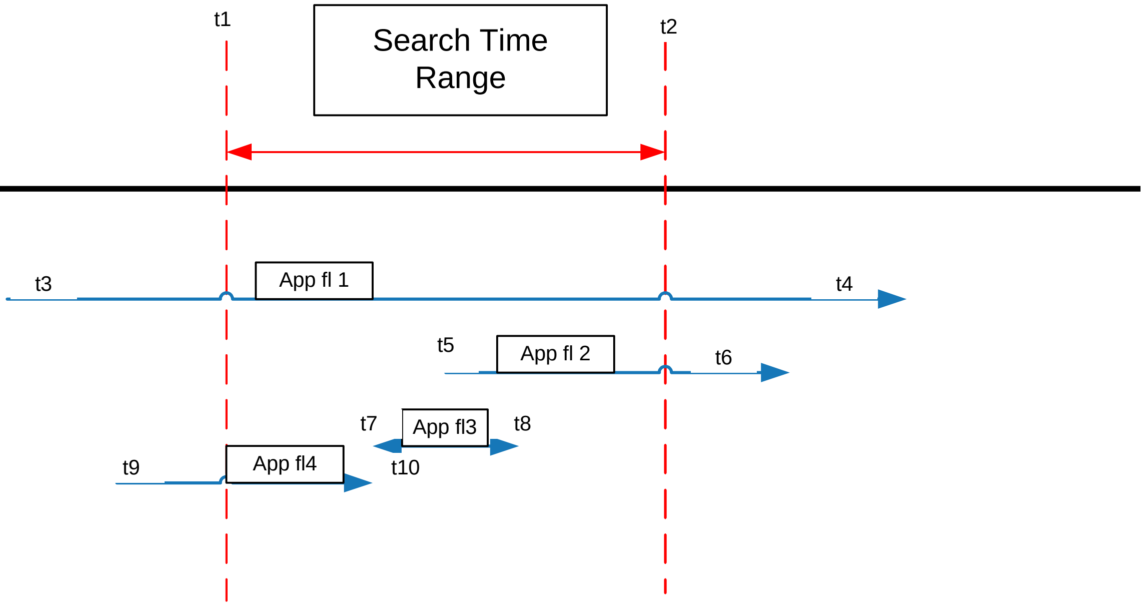


Figure 59 shows that a search for an active application “*App*” between *t1* and *t2* time period results in a sum of bandwidth (bytes, packets) of all the application flows (*fl1* – *fl4*). The start time of the application comes up as *t3* and the last occurrence time shows up as *t4*.

At this point, what users might expect (given the search time range of *t1* – *t2*) is to see data within the time range specified. However, search crosses the time boundaries and displays aggregate data for all the flows of the application “*App*” which either started or ended (or could be both), or active between *t1* and *t2* times.

chapter

5 Device Configuration

This section includes the following:

Managing Devices

This section describes how you can add new devices, delete existing devices, and perform basic device configuration.

Checking a Device

When you add a device, OmniVista SafeGuard Manager checks to ensure that the device is a Alcatel-Lucent device. No other devices are added. The check ensures that:

- the device has a valid Alcatel-Lucent IP address
- SNMP community names match the names configured on the device
- the device added is a Alcatel-Lucent device

If the compatibility check fails, an error message is displayed.

Adding a New Device

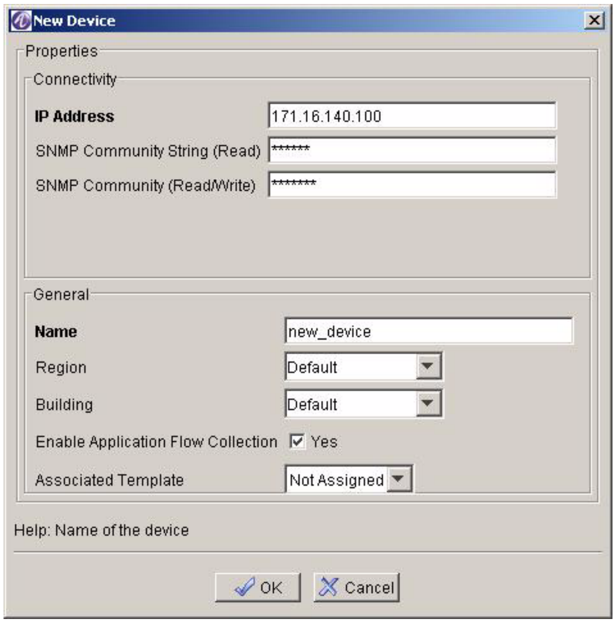
OmniVista SafeGuard Manager allows you to add a single device or multiple devices from a list of devices that you create using a specific format.

Adding a Single Device

To add a single device:

1. Select the Device Configuration icon from the Page Bar or select the *View* > *Go To* > *Config Management* menu item.
2. Click the New icon from the Action Bar.
3. Select Single Device. The New Device (*Figure 60*) dialog box displays.

Figure 60 New Device Dialog Box



New Device

Properties

Connectivity

IP Address 171.16.140.100

SNMP Community String (Read) ******

SNMP Community (Read/Write) *******

General

Name new_device

Region Default

Building Default

Enable Application Flow Collection ☑ Yes

Associated Template Not Assigned

Help: Name of the device

4 Enter the following device attributes:

Table 18 Add Device Attributes

Attribute	Description
IP Address	The Management IP address of the device.
SNMP Community String (Read)	Simple Network Management Protocol (SNMP) read community name that was configured when the device was initially set up.
SNMP Community (Read/Write)	SNMP read/write community name that was configured when the device was initially set up.
Name	Device name.
Region	Name of the region in which the device is located.
Building	Name of the building in which the device is located.
Enable Application Flow Collection	Click this box if you want to collect application flow data.
Associated Template	Select a template from the pull-down list that you want to associate with the device. For more information on templates, see *Templates*.

NOTE: Make sure that the attributes are specified correctly; otherwise, adding a device fails producing one of the following error messages, *"Device unreachable,"* or *"Device is not a Alcatel-Lucent device,"* or *"Unable to communicate with IP Address."*

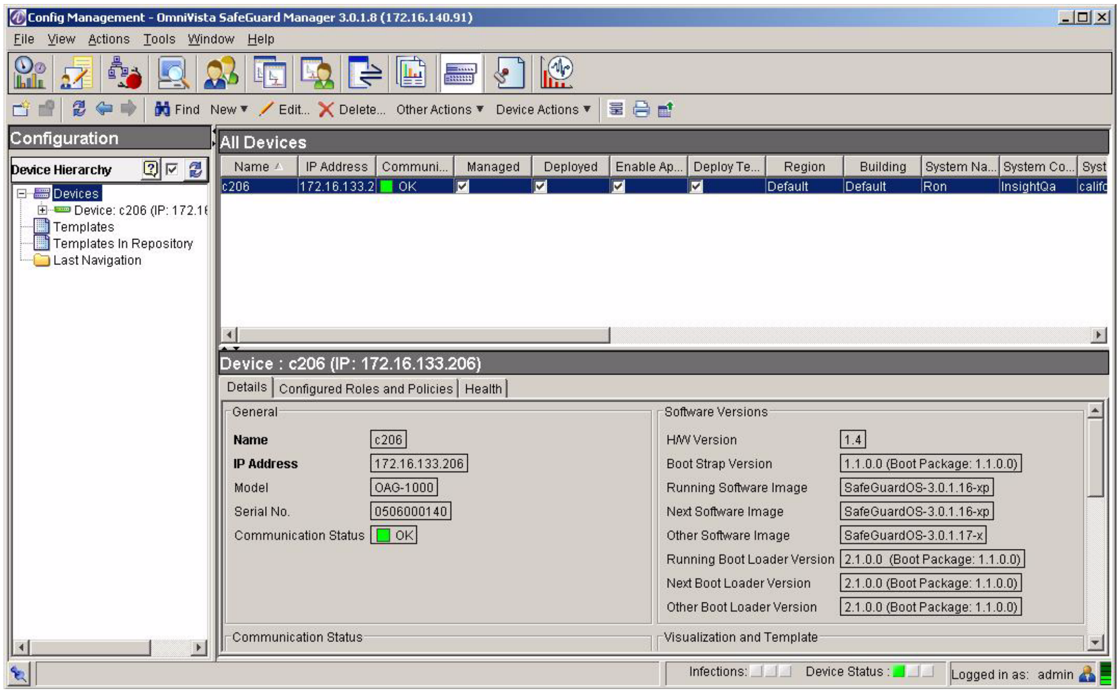
5 Click **OK** to add the device. The add process reads the system configuration and the list of outstanding visualization events from the device using a combination of SNMP and Alcatel-Lucent proprietary OmniVista SafeGuard Manager Visualization Channel.

NOTE: The device periodically ages out the visualization data; therefore, some of the events may be lost by the time you add the device.

The device displays in the All Devices panel and the device objects display in the Device Hierarchy navigation tree (*Figure 61*).

NOTE: The device must be reachable with appropriate community strings for the device to be added.

Figure 61 Device Configuration


Config Management - OmniVista SafeGuard Manager 3.0.1.8 (172.16.140.91)
File View Actions Tools Window Help
Find New ▼ Edit... Delete... Other Actions ▼ Device Actions ▼
Configuration
Device Hierarchy
Devices
Device: c206 (IP: 172.16
Templates
Templates In Repository
Last Navigation
All Devices
Device : c206 (IP: 172.16.133.206)
Details
Configured Roles and Policies
Health

Name	IP Address	Communi...	Managed	Deployed	Enable Ap...	Deploy Te...	Region	Building	System Na...	System Co...	Syst
c206	172.16.133.2	🟩 OK	☑	☑	☑	☑	Default	Default	Ron	InsightQa	califo

General

Name c206

IP Address 172.16.133.206

Model OAG-1000

Serial No. 0506000140

Communication Status 🟩 OK

Software Versions

H/W Version 1.4

Boot Strap Version 1.1.0.0 (Boot Package: 1.1.0.0)

Running Software Image SafeGuardOS-3.0.1.16-xp

Next Software Image SafeGuardOS-3.0.1.16-xp

Other Software Image SafeGuardOS-3.0.1.17-x

Running Boot Loader Version 2.1.0.0 (Boot Package: 1.1.0.0)

Next Boot Loader Version 2.1.0.0 (Boot Package: 1.1.0.0)

Other Boot Loader Version 2.1.0.0 (Boot Package: 1.1.0.0)

Adding Multiple Devices

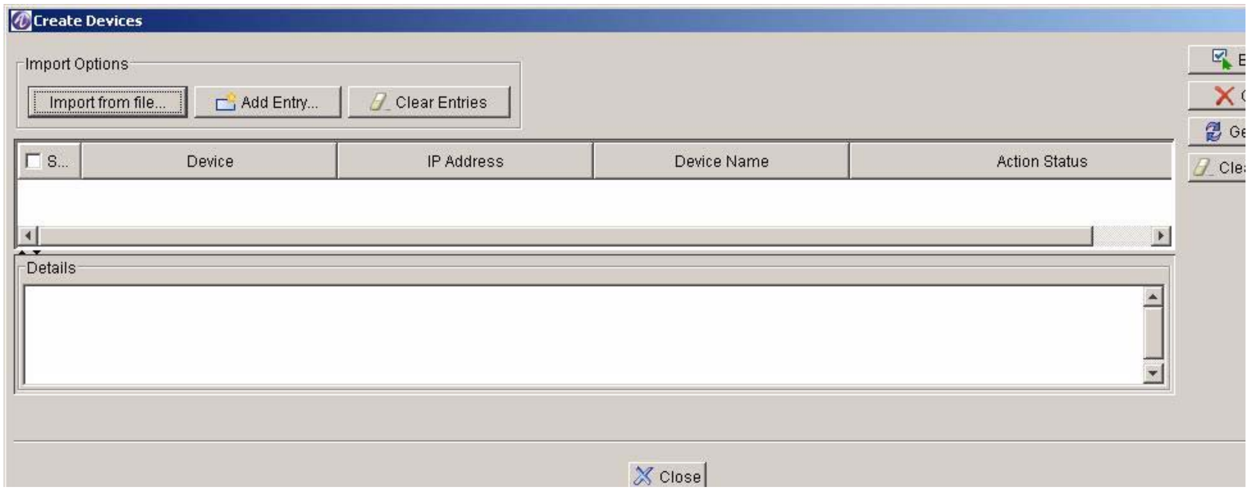
To add multiple devices:

1 Select the Device Configuration icon from the Page Bar or select the *View* > *Go To* > *Config Management* menu item.

2 Click the New icon from the Action Bar.

3 Select Multi Device. The Create Devices (*Figure 62*) dialog box displays. You can populate this table using either the **Import From File** or the **Add Entry** option.

Figure 62 Add Multiple Devices



4 Click **Import From File** to import a list of devices written in a specific format. For example:

```
##########################################################################
Name: Device List File #Purpose: For bulk device addition into OmniVista
SafeGuard Manager Syntax of each line: #
ip,read,readwrite,name,region,building,enable-flow-collection-in-true-
false # # Example: 172.16.3.125,public,private,controller,R1,B1,true
##########################################################################
172.16.3.125,public,private,controller,R1,B1,true
172.16.1.53,public,private,switch,R1,B2,true
```

5 Click **Add Entry** to add another entry in the table. This can be used to create a list.

6 The following device attributes are displayed:

Table 19 Add Device Attributes

Attribute	Description
Select Device	Select the Select Device checkbox to select all devices in the list.

Table 19 Add Device Attributes *(continued)*

Attribute	Description
Device	Show the device name with its IP address.
IP Address	The Management IP address of the device.
SNMP Community String (Read)	Simple Network Management Protocol (SNMP) read community name that was configured when the device was initially set up.
SNMP Community (Read/Write)	SNMP read/write community name that was configured when the device was initially set up.
Device Name	Device name.
Action Status	Status of the action you selected.

7 Click **Clear Entries** to clear all entries from the table.

8 Click **Execute**. The server schedules and processes each entry and provides feedback and action detail in the Action Status column.

Configuring Device Objects

After you have added the device, you must now configure the device objects. OmniVista SafeGuard Manager allows you to configure the following device objects:

- *Application Groups*
- *Application Filters*
- *Network Zones*
- *Policies*
- Role Derivations
- *Roles*
- *LDAP Servers*

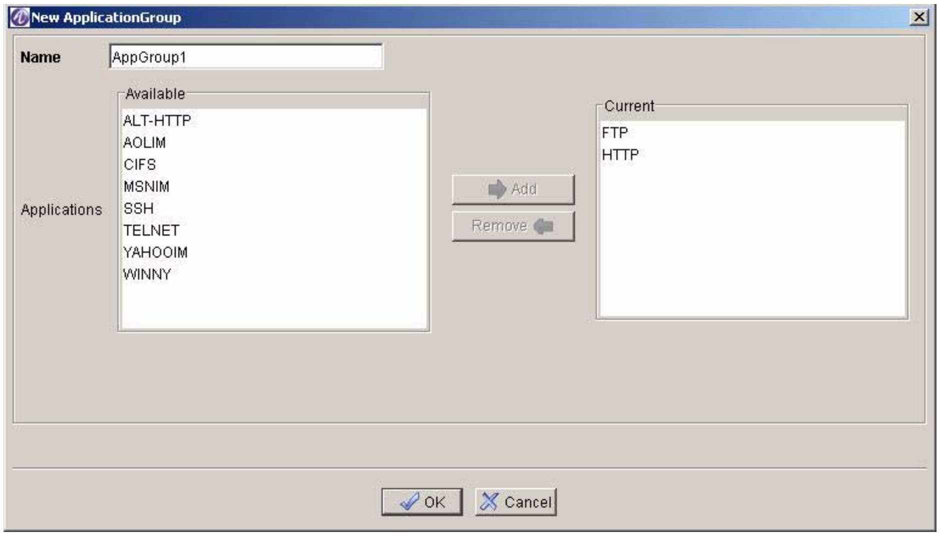
Application Groups

An *Application group* is a collection of application protocols used to filter Layer 4 or Layer 7 applications in rules and policy filters. You can define application groups to restrict vendors or contractors from using a specific application, for example, FTP. You can even refine application traffic to permit or deny certain file types.

To define custom application groups:

1 Select Application Group from the navigation tree (*Figure 61*) and click **New** New... in the Action Bar. The New ApplicationGroup dialog box displays (*Figure 63*).

Figure 63 New Application Group



Name: AppGroup1

Applications

Available:
ALT-HTTP
AOLIM
CIFS
MSNIM
SSH
TELNET
YAHOOIM
WINNY

Current:
FTP
HTTP

2 Enter the Application Group attributes as follows:

Table 20 Application Group Attributes

Attribute	Description
Name	Specify a name for the application group you are creating.
Available Applications	Highlight an application in the *Available Applications* column and click **Add** to add the selected application to the application group.
Current	Highlight an application in the **Current** column and click **Remove** to delete the selected application from the application group.

3 Click **OK**. The application group is added and displayed under the Application Group object in the navigation tree. You can add more than one application groups using the same process. The maximum number of groups that you can add is 32.

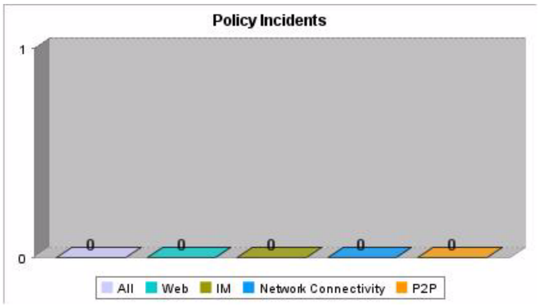
Application Group:P2P

A new application group (P2P) is available that allows you to collate all policy events related to peer-to-peer (P2P) applications. Currently, SafeGuard supports the following P2P applications:

- WinNY—a Japanese file sharing program

P2P is available in the following System Dashboard layouts:

- Incidents
- User Incidents



NOTE: P2P application groups are also available in the Policy Incidents and Applications views.

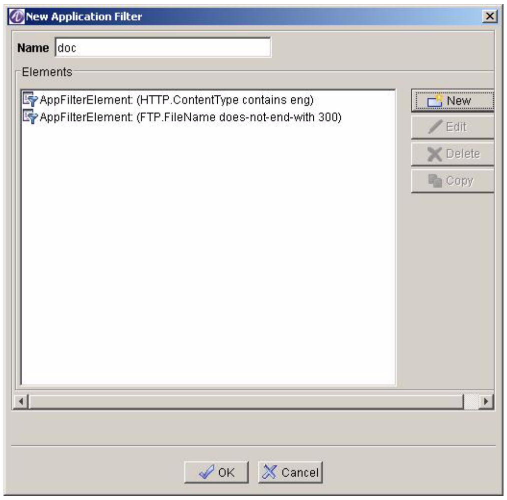
Application Filters

An *application filter* is a further refinement of an application. Application filters block an application depending upon an action the user performs. For example, you might allow contractors to use FTP, unless they attempt to upload any document that has the string “spec” in the filename. So when the traffic comes in, SafeGuard matches the FTP traffic against the “spec” parameter in the filename.

To define application filters:

1 Select Application Filters from the navigation tree (*Figure 61*) and click **New** New... in the Action Bar. The New AppFilter dialog box displays (*Figure 64*).

Figure 64 New Application Filter



Name doc

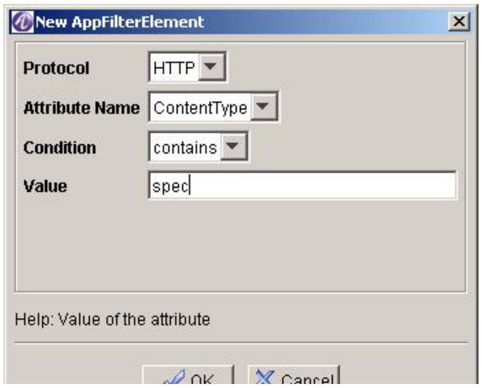
AppFilterElement: (HTTP.ContentType contains eng)
AppFilterElement: (FTP.FileName does-not-end-with 300)

2 Specify a name for the filter in the Name field.

3 Select an operator (Or, And) from the dropdown Operator list. The operator indicator indicates whether to use either, or a combination of the filter elements.

4 Click **New** to add a filter element. The New App Filter Element dialog box displays (*Figure 65*).

Figure 65 New AppFilter Element



New AppFilterElement

Protocol: HTTP

Attribute Name: ContentType

Condition: contains

Value: spec

Help: Value of the attribute

5 Specify the application filter attributes as follows:

Table 21 Application Filter Elements Attributes

Attribute	Description
Protocol	Select an application protocol from the Protocol drop-down list, for example, HTTP, FTP, or CIFS.
Attribute Name	Select an attribute name (Content type, Host, or User Agent) from the Attribute Name dropdown list.
Condition	Select a condition for the filter element from the Condition dropdown list, for example, starts with, contains, and so forth.
Value	Specify a value, for example if you chose the condition of starts with in the Condition field, you can say “spec” in this field.

6 Click **OK**. The filter element displays in the Elements field of the New AppFilter dialog box (*Figure 64*).

7 Click **OK** on the New AppFilter dialog box to create a new application filter. The application filter is added and displayed under the Application Filters object in the navigation tree. You can add more than one application filters using the same process.

8 Select a filter element and click **Edit** to change the values of an existing filter element.

9 Select a filter element and click **Delete** to remove a filter element.

10 Select a filter element and click **Copy** to clone the filter elements.

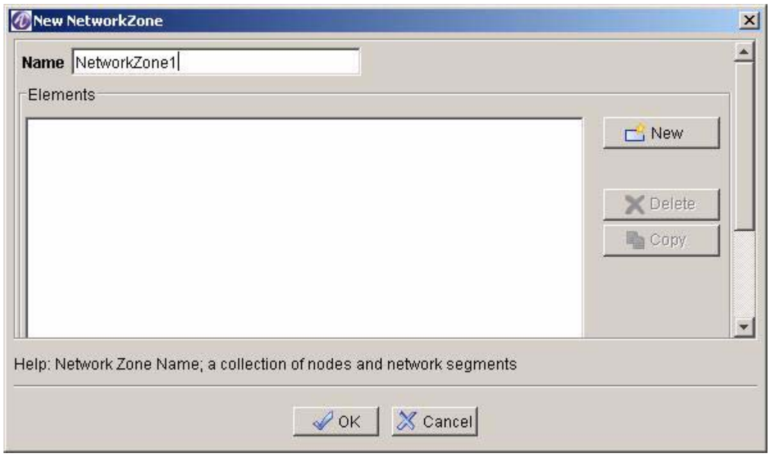
Network Zones

Network resources can be organized into *network zones*. These zones or logical groups are collections of nodes and network segments. A zone is an easy way to define the resources for a group and naming that entity. For example, you can define a network zone for the servers for the Finance organization or for the resources that you want to allocate to unauthenticated users. Zone filtering has two major benefits for the device administrator. It simplifies administration by eliminating the entry of separate numbers for each device or network segment. If a new resource is added within an existing network zone, it is available to any user that already has access to that zone.

To define a network zone:

1 Select Network Zones from the navigation tree (*Figure 61*) and click **New** New... in the Action Bar. The New NetworkZone dialog box displays (*Figure 66*).

Figure 66 New NetworkZone



New NetworkZone

Name NetworkZone1

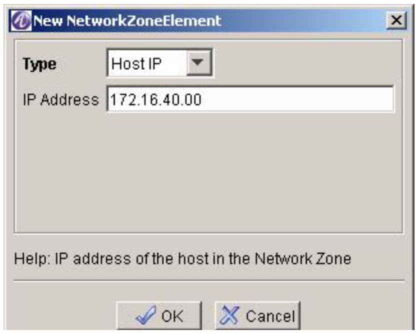
Elements

Help: Network Zone Name; a collection of nodes and network segments

2 Specify a name for the network zone in the Name field.

3 Click **New** to add a new element for the network zone. The New NetworkZoneElement dialog box displays (*Figure 67*).

Figure 67 New Network Zone Element



New NetworkZoneElement

Type Host IP

IP Address 172.16.40.00

Help: IP address of the host in the Network Zone

4 Specify the network zone attributes as follows:

Table 22 Network Zone Elements Attributes

Attribute	Description
Type	Select a network type from the Type dropdown list, Host IP, Network, IP Range, Host MAC, MAC Mask.
IP Address	Depending on what you selected in the Type field, enter the IP or the MAC address.

5 Click **OK**. The network zone element displays in the Elements field of the New NetworkZone dialog box (*Figure 66*).

6 Click **OK** on the New NetworkZone dialog box to create a new network zone. The network zone is added and displayed under the Network Zones object in the navigation tree. You can add more than one network zones using the same process.

7 Select a network zone element and click **Edit** to change the values of an existing network zone element.

8 Select a network zone element and click **Delete** to remove a zone element. Select a network zone element and click **Edit** to change the values of an existing network zone element.

9 Select a network zone element and click **Delete** to remove a zone element.

10 Select a network zone element and click **Copy** to clone the attributes of the selected element.

Policies

Policies are the rules that govern user access and resources. Policies are used to establish the boundaries and enforce a security philosophy for these users and resources. OmniVista SafeGuard Manager supports the following policies:

- Malware policies—Specify how the infection is handled when SafeGuard detects malware on the host. These policies allow you to set how little or how much access a user or an application can have on the network when an infection is suspected.

  You can set up malware policies to block the infected user or application, or allow the end device to communicate to an IT server or Internet website for automatic upload of the most recent anti-virus software or OS patch. When the infection is specific to a particular application, malware policies allow traffic from other applications to continue unimpeded.

- User policies—Allow user access to network resources and applications based on the authentication state of the user. When a user logs on to the network, the machine starts authentication using the username, password credentials, IP address, MAC address, authentication state, and user role. Using a set of configured role mapping rules and information intercepted from the authentication server, a user role is derived for the user. The system uses the role and the configured role mapping rules. Using a role hierarchical system, it applies all of the policies or rules for that particular user based on the *user role*. A user role is a designation for the user, usually a job classification such as a software engineer.

  Each policy comprises of multiple rules (filters), which is how the traffic is matched. A rule has two parts: a filter and an action. When a filter condition is true, its action might be to allow access or deny access to a resource. For example, all engineers might be allowed access to the engineering servers but restricted from accessing Finance or Human Resources servers.

- System policies—SafeGuard has a set of default policies and roles that are primarily used by internal routines. These policies cannot normally be configured by the user.

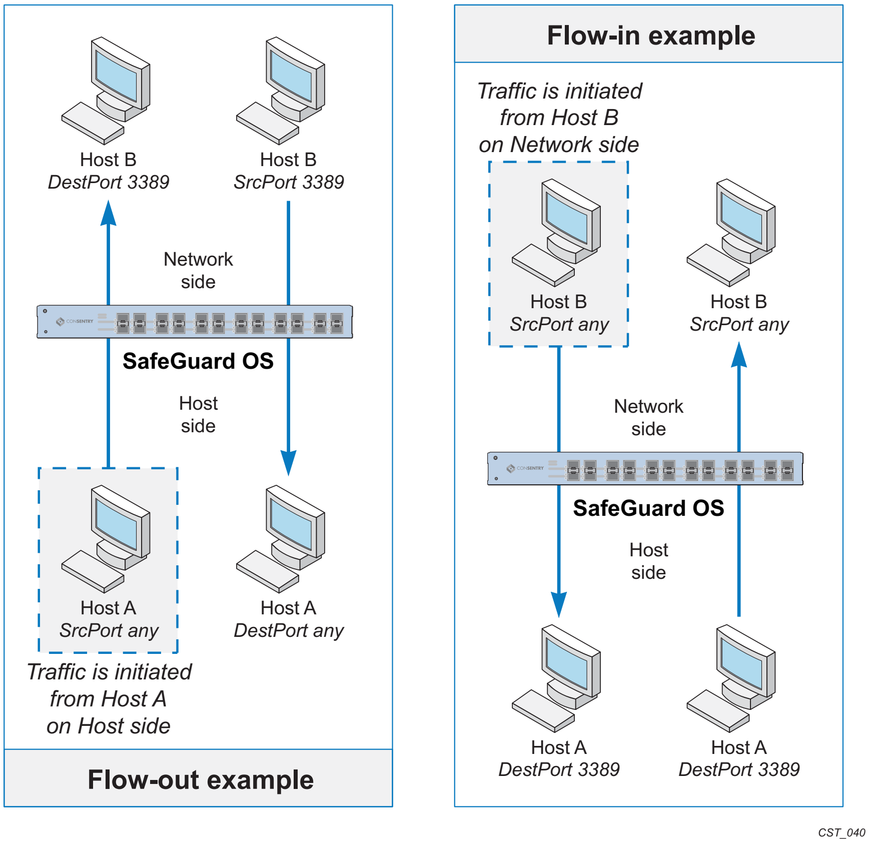
- Override policies—Policies that take precedence over system policies. In the rare case where it is necessary to temporarily override a system policy, create an override policy. These policies have a higher ranking than system policies and are executed after malware policies

- EPV policies—EPV helps ensure that a user's system and virus software are kept up-to-date. End point Posture Verification (EPV) is a component of SafeGuard OS that validates software compliance. EPV policies are the mechanisms that control whether a user's machine is scanned (checked) or whether the user is allowed to bypass the check. EPV policies cannot be assigned to a role.

NOTE: Only Malware and User policies can be assigned to a role. For more information on roles, see *Roles*.

Traffic Flow

Unlike competitive products, Alcatel-Lucent devices are not packet-based or packet-based control mechanisms. Instead, the system initiates policy enforcement on TCP connections or groupings of UDP packets. These connections are called *flows*. The upper physical ports of the Alcatel-Lucent devices are called the *network side* of the device and the lower physical ports the *host side*. In the default policy configuration, you express a policy from the host side perspective, but the policy is applied to traffic in both directions. This bidirectional behavior is unlike traditional Access Control Lists (ACLs) that require explicit CLI configuration for each direction.



However, there are occasions when you want to control a flow from the network side of the device. You can change the flow direction using the flow-in and flow-out attributes in the Filter Direction field when defining policy filters. For more information on traffic filters, see *Table 25*.

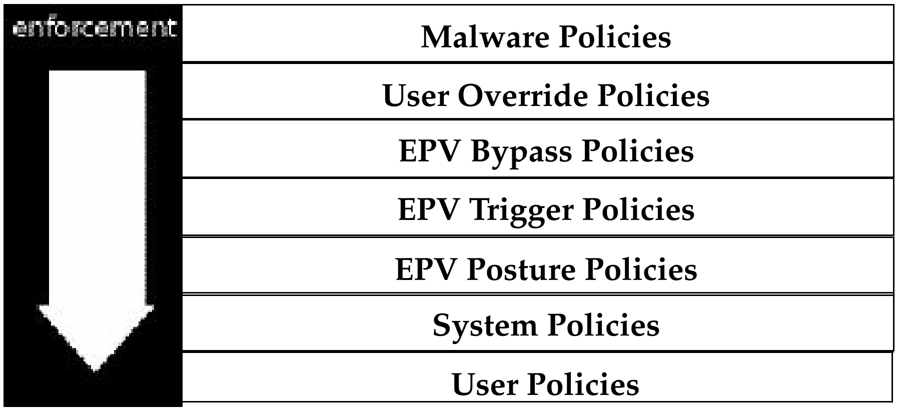
Policy Enforcement

The order in which a policy is enforced depends on two factors:

1. Ranking of the policy
2. Precedence of the policy

Policies have an internal ranking system that stacks the policies in the order shown in *Figure 68*.

Figure 68 Order of Policy Enforcement



This ranking is done within the system and cannot be overridden by users. However, within malware and user policies, you can assign a priority level or precedence to a policy. You can also assign a precedence number to the rules within a policy.

Precedence

Malware and user policies allow you to assign a precedence number to rule and policies. These precedence numbers are secondary to the overall ranking of the policies.

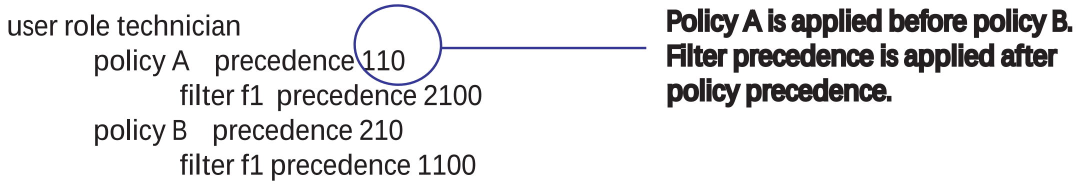
Filter Precedence

A policy can have many rules; therefore, you can assign a precedence number to the filter statements of a rule. The precedence of a filter determines the order in which the rule is applied for a specific user. Precedence numbers can be in the range of 1 to 65535, where 1 has the highest precedence and 65535 the lowest.

Policy Precedence

When a user policy is applied to a role, it too can have a precedence. Policy precedence comes before rules precedence. *Figure 69* shows an example of policy precedence. *Figure 70* shows an example of configured role and policies.

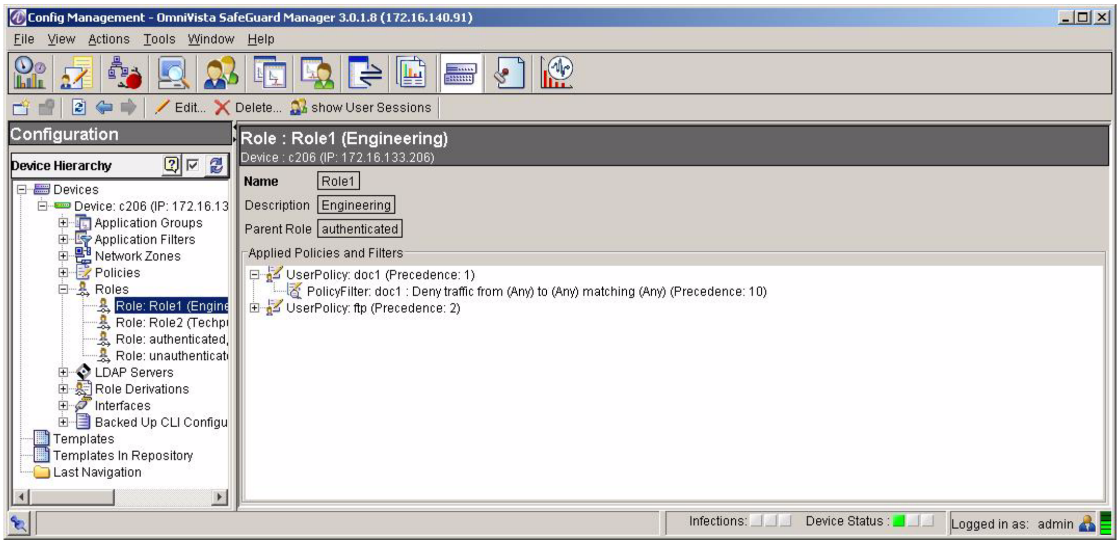
Figure 69 Policy and Filter Precedence



```
user role technician
        policy A   precedence 110
                filter f1  precedence 2100
        policy B   precedence 210
                filter f1 precedence 1100
```

Policy A is applied before policy B. Filter precedence is applied after policy precedence.

Figure 70 Configured Roles and Policies



Config Management - OmniVista SafeGuard Manager 3.0.1.8 (172.16.140.91)
File View Actions Tools Window Help
Edit... Delete... show User Sessions
Configuration
Device Hierarchy
Infections:
Device Status :
Logged in as: admin

Devices
- Device: c206 (IP: 172.16.13
  - Application Groups
  - Application Filters
  - Network Zones
  - Policies
  - Roles
    - Role: Role1 (Engine
    - Role: Role2 (Techp
    - Role: authenticated,
    - Role: unauthenticat
  - LDAP Servers
  - Role Derivations
  - Interfaces
  - Backed Up CLI Configu
- Templates
- Templates In Repository
- Last Navigation

Role : Role1 (Engineering)
Device : c206 (IP: 172.16.133.206)

Name: Role1
Description: Engineering
Parent Role: authenticated

Applied Policies and Filters
- UserPolicy: doc1 (Precedence: 1)
  - PolicyFilter: doc1 : Deny traffic from (Any) to (Any) matching (Any) (Precedence: 10)
- UserPolicy: ftp (Precedence: 2)

Precedence numbers fall into three ranges. User policies are divided into two bands to provide flexibility of overriding system policies, if needed. *Table 23* lists policy precedent ranges. Malware policies are enforced first, followed by override policies, system policies, and lastly user policies. This enforcement order parallels the precedence ranges shown in *Table 23*.

Table 23 Policy Precedence Ranges

Policy Type	Precedence Range
Malware policies	1–65535
Override user policies	1–65535
System policies	10–99
User policies	1–65535

Designing a Policy Workflow

A policy workflow is simply an approach to planning, organizing, and implementing a policy management strategy. Before configuring your rules, roles and policies, it is helpful to do some ground work.

1. Determine your corporate philosophy to security.

   There are two schools of thought on how to execute a policy system. One method creates a wall where all users are initially denied access. You then punch holes, or exceptions into the wall. The other method is to allow everything through and then to block specific network resources and applications.

2. Using your existing corporate security plan and documents for organizing your role hierarchy, organize your users, servers, and other resources into logical groups.

   As mentioned before, users are organized by role. But you can also organize resources into *network zones*, which are collections of nodes and network segments. A network zone is an easy way to take all of the resources for a group and naming that entity. For example, you can define a network zone for the servers for the Finance organization or for the resources that you want to give unauthenticated users. For more information on defining network zones, see *Network Zones*.

3. Determine what applications and what files you want to monitor or block.

4. Define the list of permissions (rules) based on the access criteria. For more information, see *Defining Policies*.

5. Order the filters within each role by precedence. For more information on roles and role hierarchy, see *Roles*.

Defining Policies

A policy is a set of rules that define a set of permissions for the user. For each policy you define:

1. Select the type of policy definition you want to create (User, Malware, EPV, or User Override).

2. Assign the policy a name.

3. Add a description for the policy (optional).

4. Add a severity for the policy (optional).

5. Add a category for the policy (optional).

6. Configure the rules which are comprised of filters and actions. For more information on application filters, see *Application Filters*.

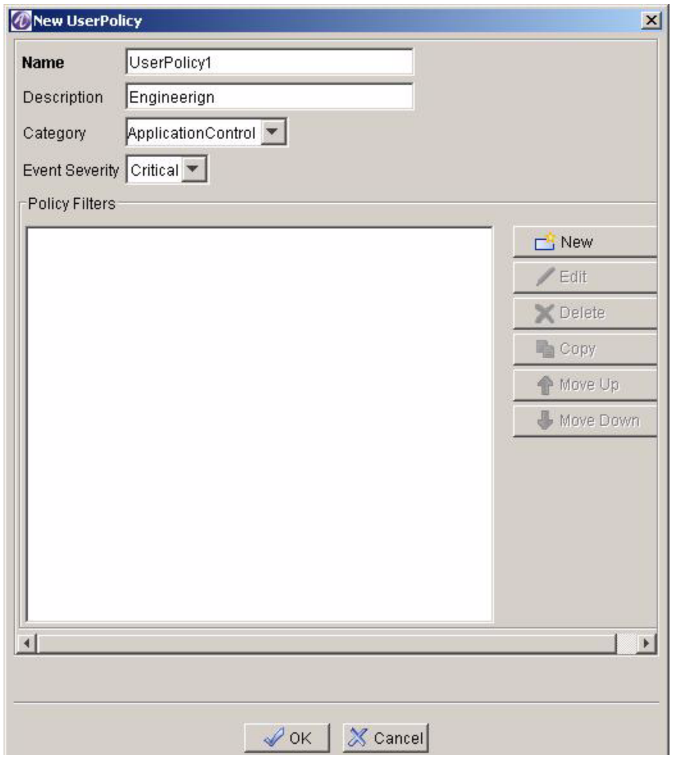
7 Configure the roles that apply to the policies and associate the policy to the user. For more information on roles, see Role Derivations and *Roles*.

Creating a New Policy

To create a new policy:

1 Select Policies from the navigation tree (*Figure 61*) and select User Policy, Malware Policy, EPV Policy, or User Override Policy from the New dropdown list in the Action Bar. For this example, we have selected User Policy. The New UserPolicy dialog box displays (*Figure 66*).

Figure 71 New User Policy



Name: UserPolicy1

Description: Engineerign

Category: ApplicationControl

Event Severity: Critical

2 Enter information in the user-configurable fields as follows:

Table 24 Policy Attributes

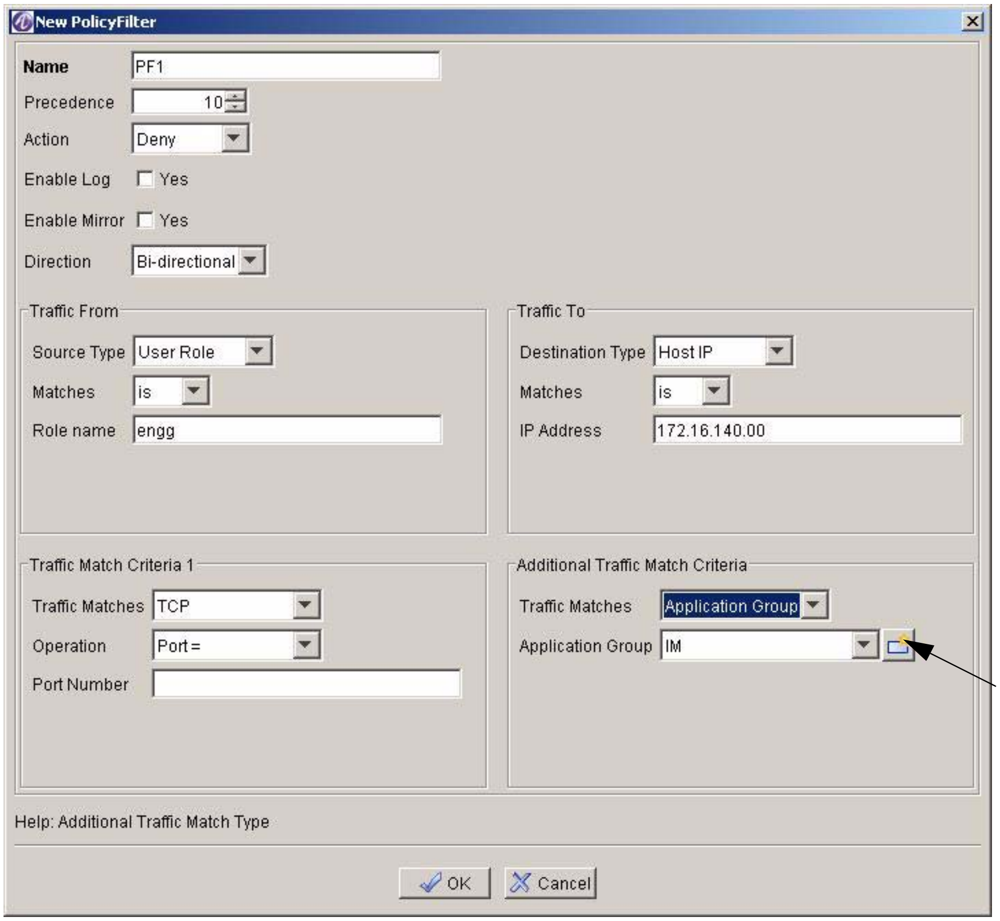
Attribute Name	Description
Name	Specify a name for the policy event you are creating.
Description	Specify a description for the policy event.
Category	From the dropdown list, select an existing category or specify a new one for the policy event.

Table 24 Policy Attributes *(continued)*

Attribute Name	Description
Event Severity	Specify a severity level for the policy event from the dropdown list, Critical, Major, Minor, or Informational.

3 Filter expressions improve the accuracy and consistency of configuration commands deployed to the network. Click **New** to define policy filters. The New Policy Filter dialog box displays (*Figure 72*).

Figure 72 New Policy Filters



New PolicyFilter

Name PF1

Precedence 10

Action Deny

Enable Log ☐ Yes

Enable Mirror ☐ Yes

Direction Bi-directional

Traffic From

Source Type User Role

Matches is

Role name engg

Traffic To

Destination Type Host IP

Matches is

IP Address 172.16.140.00

Traffic Match Criteria 1

Traffic Matches TCP

Operation Port =

Port Number

Additional Traffic Match Criteria

Traffic Matches Application Group

Application Group IM

Help: Additional Traffic Match Type

Create New Objects

4 Enter information in the user-configurable attributes as follows:

Table 25 Policy Filter Attributes

Attribute Name	Description
Name	Specify a name for the policy filter.

Table 25 Policy Filter Attributes *(continued)*

Attribute Name	Description
Precedence	Use the up and down arrows to assign a priority level or precedence to the policy. Each policy filter has an associated precedence which sorts the filters within the policy. The precedences have a valid range of 1 (highest) to 65535 (lowest). If a precedence number is not specified, the system assigns a precedence.
Action	From the dropdown list, assign an action for the policy filter. **Note:** The policy filter actions displayed in the Action dropdown list depend on the type of policy you select. Following values are available: ■ Deny—drop the packet and deny access ■ Reset TCP—drop the packet and reset the denied connection ■ Permit—permit access ■ Bypass—bypass the packet
Enable Log	Select the Enable Log checkbox if you want to log the events.
Enable Mirror	Select the Enable Mirror checkbox if you want to mirror the traffic.
Filter Direction	Traffic flow direction in which the filter is to be applied, In, Out, or both directions (InOut). For more information on traffic flow, see *Traffic Flow*.
Traffic From/Source Type	Select a source type from which to restrict traffic. Following values are available: ■ Any—any source type ■ User Name—source type with this user name ■ User Role—source type that belongs to this user role ■ Network Zone—source type that belongs to this network zone ■ IP Address—source type with this IP address ■ IP Address/Mask—source type with this IP address and net mask ■ IP Address Range—source type with this IP address range ■ MAC Address—source type with this MAC address ■ MAC Address/Mask—source type with this MAC address and mask

Table 25 Policy Filter Attributes *(continued)*

Attribute Name	Description
Traffic To/Destination Type	Select a destination type to which you want to restrict traffic. Following values are available: ■ Any—any destination type ■ IP Address—destination type with this IP address ■ IP Address/Mask—destination type with this IP address and mask ■ IP Address Range—destination type with this IP address range ■ MAC Address—destination type that with this MAC address ■ MAC Address/Mask—destination type with this MAC address and mask ■ Network Zone—destination type that belongs to this network zone
Traffic Match Criteria 1	Depending on your selection in this field, the traffic match criteria will display different fields. Following values are available: ■ Any—any application protocol ■ TCP—matches the criteria for Transport Control Protocol (TCP). If you select TCP, additional fields are displayed for specifying the operation (less than, equal to, and so forth) and the port number. ■ UDP—matches the criteria for User Datagram Protocol (UDP). If you select UDP, additional fields are displayed for specifying the operation (less than, equal to, and so forth) and the port number. ■ Application Group—matches the criteria for the specified application group. If you select Application Group, a dropdown list of application group you defined earlier is displayed. For more information on specifying application groups, see Application Groups on page 103. ■ Application Filter—matches the criteria for the specified application filter. If you select Application Filter, a dropdown list of application filters you defined earlier is displayed. For more information on specifying application filters, see Application Filters on page 105.
Additional Traffic Match Criteria	This field is configurable only if you select TCP or UDP as the traffic match criteria. When you do so, you get a dropdown list of traffic matches (application group, application filter). Select the application group or filter you want to use as a policy filter.

5 Click **OK**. The policy filter you defined displays in the Policy Filters panel of the New User Policy dialog box.

6 Click **OK**. The new user policy displays in Policies object of the navigation tree. You can create more than one policy using the same process.

7 Select a policy and click **Edit** to change the values of an existing policy.

8 Select a policy and click **Delete** to remove a policy. A confirmation box is displayed asking you to confirm the deletion.

9 Select a policy and click **Copy** to clone the attributes of the selected policy.

10 If you want to change the precedence of the policy you just created or an existing policy, use the **Move Up** and **Move Down** buttons.

NOTE: Policies only apply if they are assigned to roles. For information on assigning policies to roles, see *Roles*.

Role Derivations

Role derivation for a user is achieved by matching a set of authentication protocol-specific attributes and their values to a role. The attributes are obtained by user authentication against an external RADIUS, Kerberos, or another server. These attributes are sent by the authentication server to the network access device when an access request is successfully accepted. Role derivation rules are not applied when authentication fails. Roles can also be derived against user names.

The role derivation rules are defined in a rule map, which can be configured for each authentication protocol type. Every rulemap has a factory default role based on the type of authentication protocol for which the rule map is configured. The default role in a rule map can be modified to a role by user choice. The default role is assigned when no rule in the rule map matches the attributes of an authentication session.

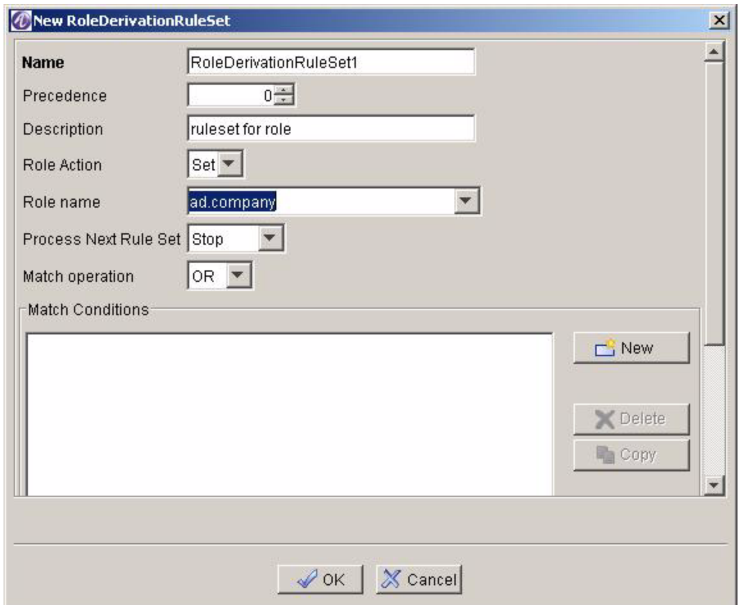
In addition, the position of a rule in the rule map determines the priority of the rule in the rule map. The first rule that is matched drives the role derivation for the authenticating user. If no match occurs on the attribute list, then the default role specified in the rule map is assigned to the authenticating user. When a rule map is defined or created, the “default role” is set to the factory default role, which in turn is based on the auth attribute type for which the rule map is defined. This default role is authenticated.

You set up users in the authentication database by assigning them a set of roles usually defined first by department and then by mapping a set of authentication protocol-specific attributes and their values to a role. The attributes are obtained by user authentication against an external RADIUS, Kerberos, or another server.

To define a role derivation rule set:

1 Select Role Derivations from the navigation tree (*Figure 61*) and click **New** New... in the Action Bar. The New Role Derivation Rule Set dialog box displays (*Figure 73*).

Figure 73 Role Derivation Rule Set



New RoleDerivationRuleSet

Name: RoleDerivationRuleSet1

Precedence: 0

Description: ruleset for role

Role Action: Set

Role name: ad.company

Process Next Rule Set: Stop

Match operation: OR

Match Conditions

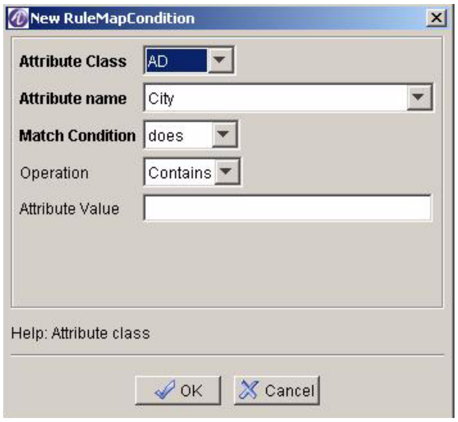
2 Enter information in the user-configurable fields as follows:

Table 26 Role Derivation Rule Set Attributes

Attribute Name	Description
Name	Rule map name in character string.
Precedence	Use the up and down arrows to assign a priority level or precedence to the rule map.
Apply Rule Set	Check this box if you want to apply the rule set.
Description	Description for the role derivation rule set in a character string.
Role Action	From the dropdown list, select Set.
Role Name	Role name in character string. Role names are case sensitive. The 'software engineer' role is not the same as the 'Software Engineer' role.
Match Operation	From the dropdown list, select a match operation of OR or AND.
Match Conditions	Displays the conditions set in the New Rule Map Condition dialog box (*Figure 74*).

3 Click **New** to set match conditions. The New Rule Map Condition dialog box displays (*Figure 74*).

Figure 74 New Rule Map Condition



New RuleMapCondition

Attribute Class: AD

Attribute name: City

Match Condition: does

Operation: Contains

Attribute Value:

Help: Attribute class

4 Enter information as follows:

Table 27 New Rule Map Condition Attributes

Attribute Name	Description
Attribute Class	From the dropdown list, select an attribute class of System, RADIUS, or AD.
Attribute Name	From the dropdown list, select an attribute name.
Match Condition	From the dropdown list, select a condition of does or does not.
Operation	From the dropdown list, select an operation for the match condition.
Attribute Value	Specify a value to match the attribute condition.

NOTE: The **OK** button is grayed out unless or fields are appropriately configured.

5 Click **OK**. The rule set conditions are set and display in the Match Conditions panel of the Role Derivation Rule Set dialog box.

6 Click **OK** on the Role Derivation Rule Set dialog box. The role derivation is created and displays under Role Derivation in the navigation tree.

7 Select a role derivation and click **Edit** to change the configuration of an existing role derivation.

8 Select a role derivation and click **Delete** to remove it from the list. A confirmation box is displayed asking you to confirm the deletion.

9 Select a role derivation and click **Copy** to clone the configuration of the selected role derivation.

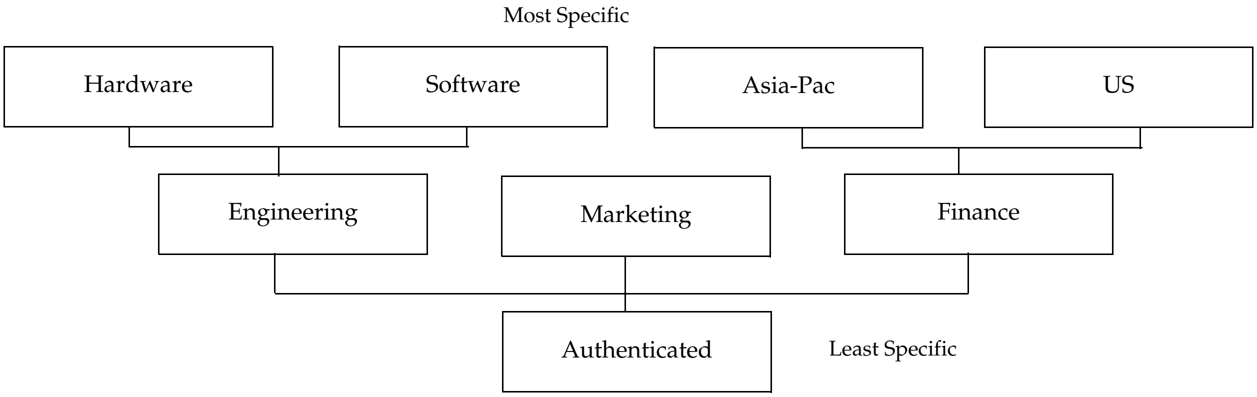
Roles

You set up users in the authentication database by assigning them a set of roles, usually defined first by department and then by mapping a set of authentication protocol-specific attributes and their values to a role. The attributes are obtained by user authentication against an external RADIUS, Kerberos, or another server. Each role has a different set of privileges. There are two hardcoded roles for the system: authenticated and unauthenticated. Any user who is unauthenticated is assigned the unauthenticated role. Any policies that you define for that role are assigned to all users having that role.

Any user-defined role, by default, has the authenticated role as the parent. A role can be designated as a child of other roles, except for the authenticated and unauthenticated roles.

Policies are applied from the bottom of the hierarchy to the top of the hierarchy. In other words, policies are applied from the most specific to the least specific role. *Figure 75* shows a simple role hierarchy.

Figure 75 Role Hierarchy



Some rules for configuring roles:

- By establishing a role hierarchy, you can avoid having to duplicate policies throughout each role.
- The chain within a role hierarchy cannot be cyclical.
- A child role can have only one parent role.
- All user-defined roles are assumed to be children of the authenticated role, unless the new role is designated to be a child of another role.
- The default role of unauthenticated cannot be a parent of other user configured roles.

- Default roles cannot be deleted.

For more information on how policies are applied, see the *OmniAccess SafeGuard OS Administration Guide*.

NOTE: Role names are case sensitive. The “software engineer” role is not the same as “Software Engineer” role.

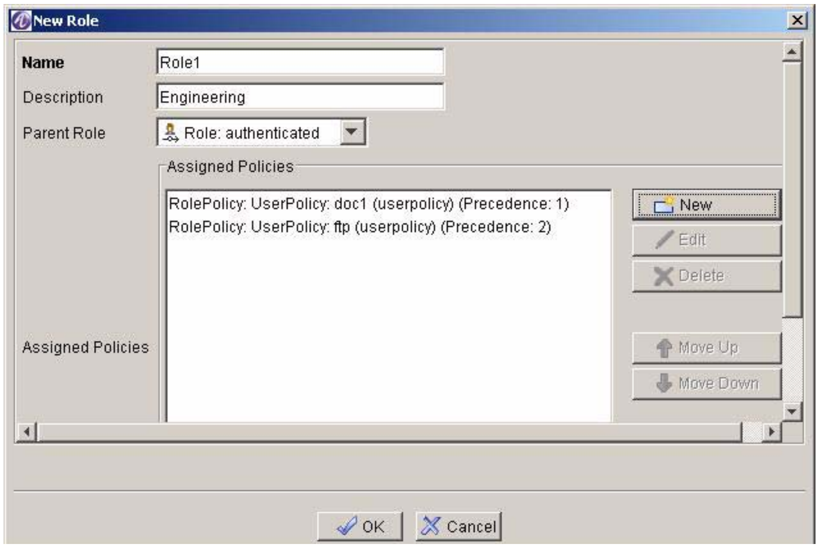
The procedure for creating a role is:

1. Create the role by giving it a name.
2. Define the parent role, if necessary.
3. Apply either a user policy or a malware policy to the role.

To create a new role:

1. Select Roles from the navigation tree (*Figure 61*) and click **New** New... in the Action Bar. The New Role dialog box displays (*Figure 76*).

Figure 76 New Role



Name: Role1

Description: Engineering

Parent Role: Role: authenticated

Assigned Policies:

RolePolicy: UserPolicy: doc1 (userpolicy) (Precedence: 1)
RolePolicy: UserPolicy: ftp (userpolicy) (Precedence: 2)

2. Enter information in the user-configurable fields as follows:

Table 28 Role Derivation Rule Set Attributes

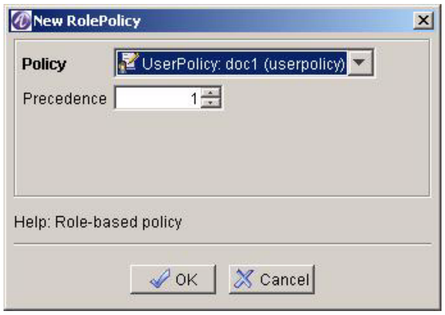
Attribute Name	Description
Name	Role name.
Description	Role description in character string.

Table 28 Role Derivation Rule Set Attributes

Attribute Name	Description
Parent Role	From the dropdown list, select a role to be assigned as a parent role.
Assigned Policies	Displays the policies assigned using the New Policies dialog box.

3 Click **New** to assign policies for this role. The New RolePolicy dialog box displays (*Figure 77*).

Figure 77 New Role Policy



4 Enter information as follows:

Table 29 New Role Policy Attributes

Attribute Name	Description
Policy	From the dropdown list, select a user or malware policy that you defined earlier. For more information, see *Defining Policies*.
Precedence	Use the up and down arrows to assign a priority level or precedence to the policy. For more information on precedence, see *Policy Precedence*.

NOTE: The **OK** button is grayed out unless or fields are appropriately configured.

5 Click **OK**. The policy is assigned and displays in the Assigned Policies panel of the New Role dialog box.

6 Click **OK** on the New Role dialog box. A new role is created and displays under Roles in the navigation tree.

7 Select a role and click **Edit** to change the configuration of an existing role.

8 Select a role and click **Delete** to remove it from the list. A confirmation box is displayed asking you to confirm the deletion.

9 Select a policy and click **Up** or **Down** to change the precedence.

LDAP Servers

LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information from a server. The LDAP protocol defines how to store structured data. For example, corporations may want to store employee contact information, categorize employees into various groups (QA, Docs, Engineering, and so forth).

LDAP servers are used to authenticate users when Active Directory (AD) is used as an authentication mechanism. AD is an implementation of LDAP directory services by Microsoft for use in Windows environments.

Configuring LDAP Servers

When SafeGuard authenticates a user, during the process of role derivation, and if conditions set use AD attribute class, LDAP servers that are configured are contacted to get the value of desired attribute. For example,

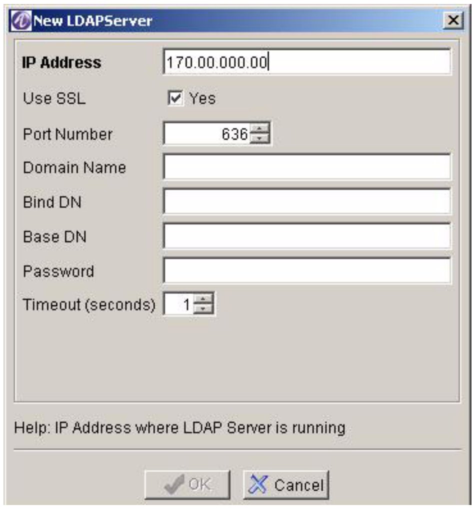
If you set a rule-map with a condition `(set role=”offshore” if AD.country=INDIA)`

When authenticating a user, SafeGuard obtains the value of `AD.country` and matches it using that value. If the match is successful, the role of `“offshore”` is assigned.

To configure an LDAP server:

1 Select LDAP Servers from the navigation tree (*Figure 61*) and click **New** New... in the Action Bar. The New Role Derivation Rule Set dialog box displays (*Figure 78*).

Figure 78 New LDAP Server



New LDAPServer

IP Address: 170.00.000.00

Use SSL: ☑ Yes

Port Number: 636

Domain Name:

Bind DN:

Base DN:

Password:

Timeout (seconds): 1

Help: IP Address where LDAP Server is running

2 Enter information in the user-configurable fields as follows:

Table 30 New LDAP Server Attributes

Attribute Name	Description
IP Address	Enter an IP address for the LDAP server.
Use SSL	Select the checkbox if you want LDAP to use the Secure Socket Layer (SSL) encryption to secure data transmissions.
Port Number	Use the up/down arrows to specify a port number for the LDAP server.
Domain Name	Enter an alphanumeric name for the domain name.
Bind DN	Enter a distinguished name to be used in the LDAP bind.
Base DN	Enter a distinguished name.
Password	Enter a password for the LDAP server.
Timeout (seconds)	Use the up/down arrows to select timeout in seconds.

3 Click **OK** to apply and save the server settings.

4 Select an existing LDAP server and click **Delete** in the Action Bar to delete the selected server. A confirmation dialog box displays asking for verification.

5 Select an existing LDAP server and click **Edit** in the Action Bar to modify the server settings.

6 Select an existing LDAP server and click **Copy** in the Action Bar to copy the settings of the selected server.

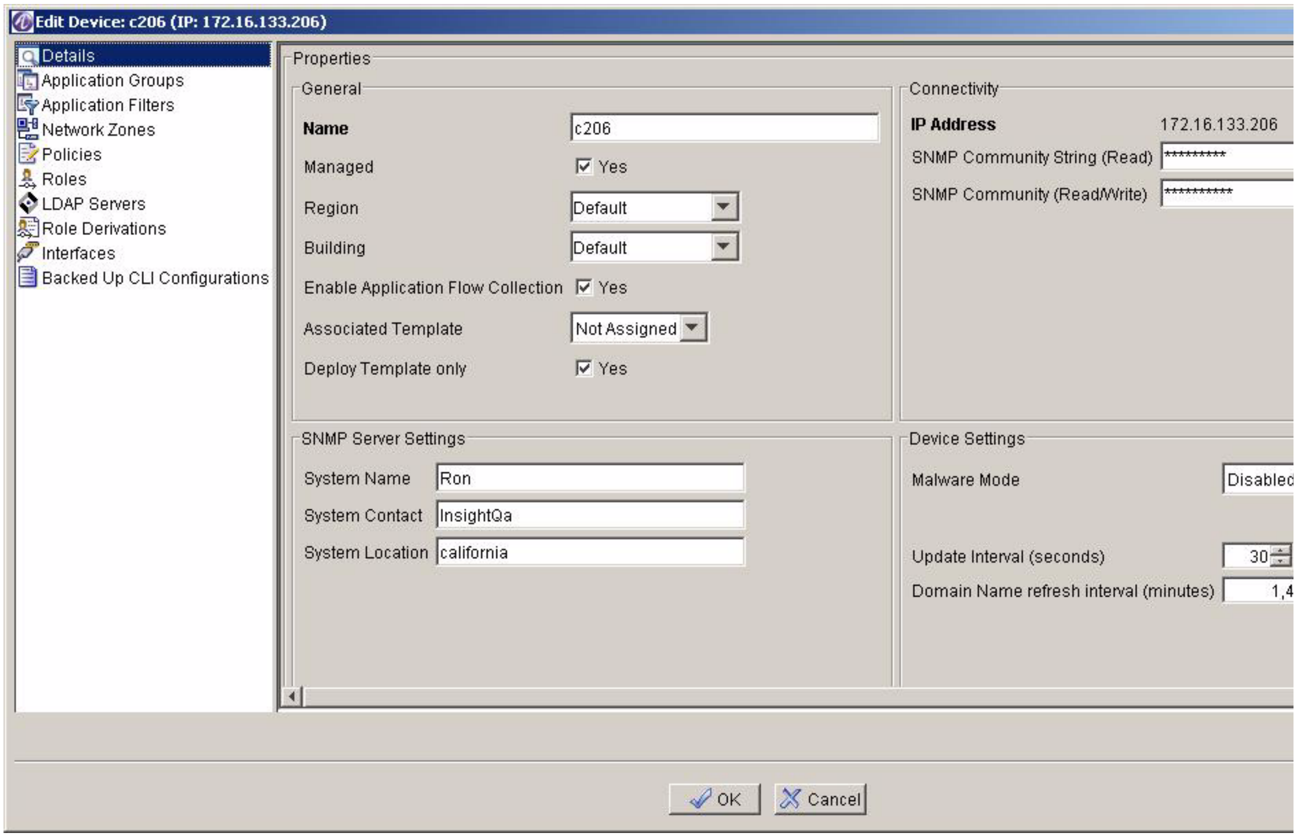
Editing Device Objects

To edit a device:

1 Select the Device Configuration icon from the Page Bar or select the *View* > *Go To* > *Config Management* menu item.

2 Click the Edit icon from the Action Bar. The Edit Device (*Figure 79*) dialog box displays.

Figure 79 Edit Device



Edit Device: c206 (IP: 172.16.133.206)

Properties

General

Name c206

Managed ☑ Yes

Region Default

Building Default

Enable Application Flow Collection ☑ Yes

Associated Template Not Assigned

Deploy Template only ☑ Yes

Connectivity

IP Address 172.16.133.206

SNMP Community String (Read) *********

SNMP Community (Read/Write) ***********

SNMP Server Settings

System Name Ron

System Contact InsightQa

System Location california

Device Settings

Malware Mode Disabled

Update Interval (seconds) 30

Domain Name refresh interval (minutes) 1,4

3 You can edit the device properties: general, connectivity, SNMP server settings, and device settings using the following attributes:

Table 31 Edit Device Attributes

Attribute Name	Description
General Properties:	
Name	A unique name of the device that you are editing.
Managed	Select the Yes checkbox if the device is to be managed. If you deselect the box, the device will not be polled, basically the device is disconnected from OmniVista SafeGuard Manager without deleting.
Region	Name of the region where the device is located. Mapped to SysLocation.
Building	Name of the building in which the device is located. Mapped to SysLocation.
Enable Application Flow Connection	Select the Yes checkbox if you want to collect the application flow data. This is useful for diagnostic purposes.
Associated Template	From the dropdown list, select a template to associate to this device.
Deploy Template Only	Select the Yes checkbox if you want the device to be configured only with the associated template. Selecting this checkbox ensures that only the objects that are associated with the selected template are deployed on the selected device and objects that are associated with the device are ignored. If you deselect the box, the device is configured with the template objects and also with the device objects.
Connectivity Properties:	
IP Address	IP address of the device you are adding.
SNMP Community String (Read)	Simple Network Management Protocol (SNMP) read community name that was configured when the device was initially set up.
SNMP Community (Read/Write)	SNMP read/write community name that was configured when the device was initially set up.
SNMP Server Settings:	
System Name	Name of the SNMP server.
System Contact	Name of the device administrator.
System Location	Location of the SNMP server.

Table 31 Edit Device Attributes *(continued)*

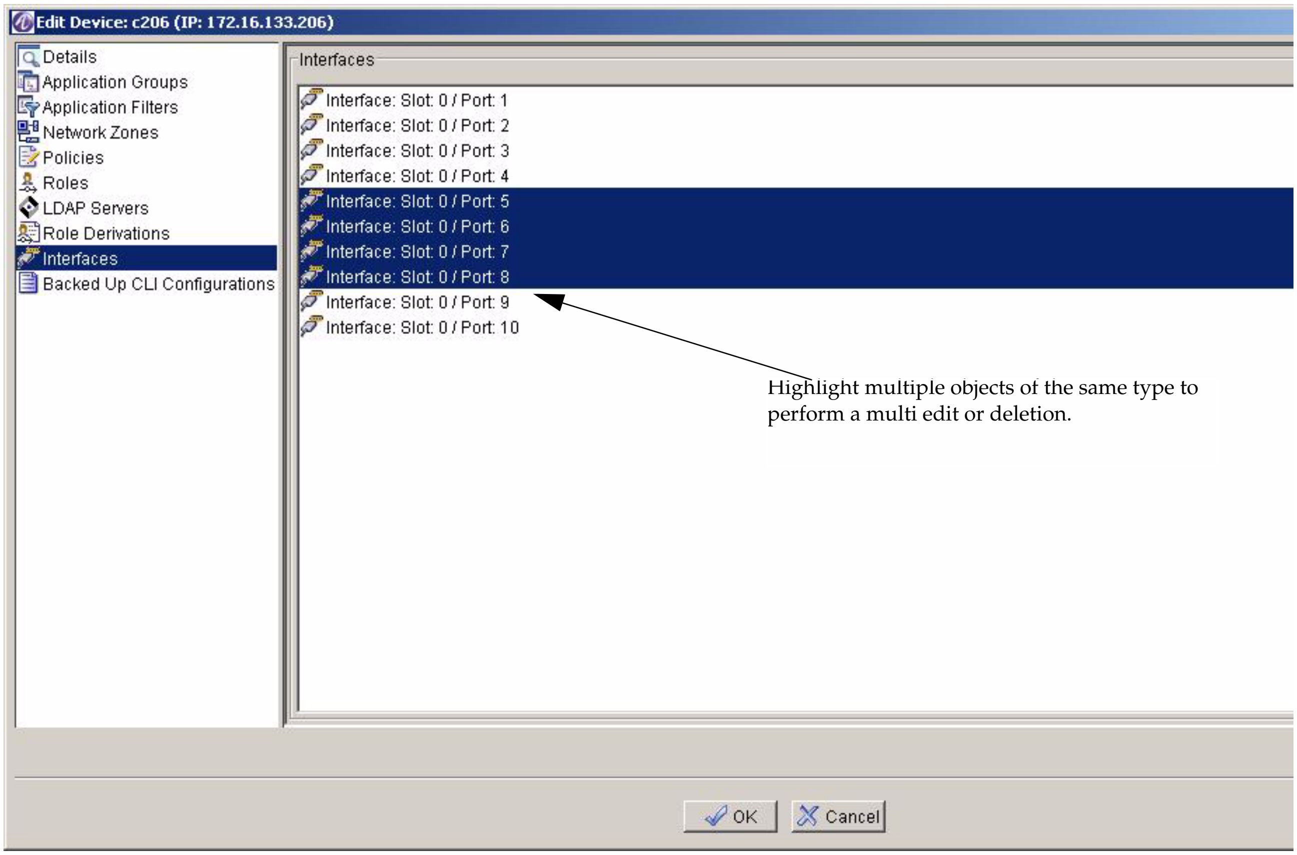
Attribute Name	Description
Device Settings:	
Malware Mode	From the dropdown list, select one of the following malware modes: ■ Disabled—Disables malware detection in the switch. Malware processing will be bypassed. ■ Log Only—Enables malware detection in the device but no action is taken. Only logs are created. ■ Block Host—Blocks the entire host. ■ Block Application—Blocks only the application group (destination ports) on the host. The rest of the application groups running on the host will have network access as determined by the user's policy.
Protection Mode (only for switches)	From the dropdown list, select one of the following protection mode: ■ Pass-Thru—Performs no monitoring. ■ Monitor—Monitors for policy visualization based on user-defined policy controls; however, no enforcement actions are taken. ■ Protect—Monitors and enforces policies on user-defined policy controls.
Update Interval (seconds)	Use the up and down arrows to specify the update interval.

4 Select an object in the navigation tree and click **New** create a new object of the selected type. See *Configuring Device Objects* for more information on creating and configuring new objects.

5 Select an object in the navigation tree and click **Edit** to modify an existing object. OmniVista SafeGuard Manager allows you to edit multiple objects (of the same type).

6 To edit objects of the same type, highlight multiple objects (*Figure 80*) and click **Edit**. The Edit Object dialog box displays. If the objects that you selected are not of the same type, the error message, *"There are no common editable fields for the selected objects"* displays.

Figure 80 Editing or Deleting Multiple Device Objects


Edit Device: c206 (IP: 172.16.133.206)
Details
Application Groups
Application Filters
Network Zones
Policies
Roles
LDAP Servers
Role Derivations
Interfaces
Backed Up CLI Configurations
Interfaces
Interface: Slot: 0 / Port: 1
Interface: Slot: 0 / Port: 2
Interface: Slot: 0 / Port: 3
Interface: Slot: 0 / Port: 4
Interface: Slot: 0 / Port: 5
Interface: Slot: 0 / Port: 6
Interface: Slot: 0 / Port: 7
Interface: Slot: 0 / Port: 8
Interface: Slot: 0 / Port: 9
Interface: Slot: 0 / Port: 10
OK
Cancel

Highlight multiple objects of the same type to perform a multi edit or deletion.

7 To delete objects of the same type, highlight multiple objects (*Figure 80*) and click **Delete**. The Confirm Deletion dialog box displays. If the objects that you selected for deletion are not of the same type, the error message, *“There are no common editable fields for the selected objects”* displays.

Editing Interfaces

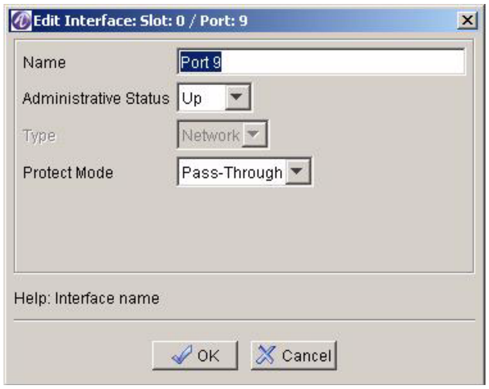
Interface is the slot or port associated with the device. To edit an interface:

1 Select the Device Configuration icon from the Page Bar or select the *View > Go To > Config Management* menu item.

2 Select Interfaces in the navigation bar and highlight a port that you want to edit.

3 Click the **Edit** icon from the Action Bar. The Edit Interface (*Figure 79*) dialog box displays.

Figure 81 Edit Interface



Name: Port 9
Administrative Status: Up
Type: Network
Protect Mode: Pass-Through
Help: Interface name

4 Edit the attributes as follows:

Table 32 Edit Interface Attributes

Attribute Name	Description
Name	Name of the port you want to modify.
Administrative Status	From the dropdown list, select an administrative status for the port: up or down.
Type	From the dropdown list, select the type of the interface to be edited: Host or Network.
Protect Mode	From the dropdown list, select a protect mode. Applicable for Controllers only.

5 Click **OK** to apply the changes.

6 Click **Refresh** to display the changes in the interface view.

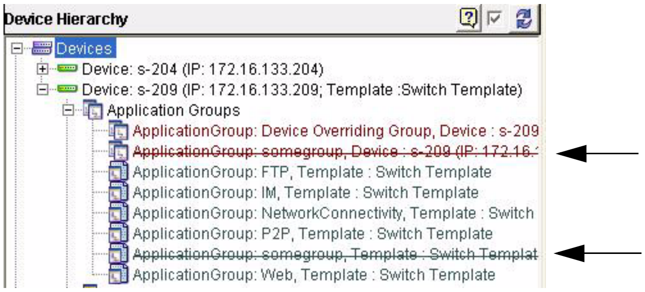
NOTE: You can edit or delete multiple interfaces of the same type (*Figure 80*) by multi-selecting them. If the interface type is not the same, an error message *"There are no common editable fields for the selected objects"* displays.

Templates

Templates are a convenient way to create a boilerplate for objects that share many of the same attributes. Templates consist of template definitions and template data. The template definition contains the logic and variables to be populated with template data. It defines the actions that need to be taken for any device to which the template is attached. The template helps in creating the configuration that is downloaded to a device. Basically, device templates are a collection of configuration elements that you want to keep consistently same across multiple devices. The following considerations should be considered when viewing template objects in the navigation tree:

- Template objects appear in italics and have a blue background. If you change a template object, all devices associated with that template are impacted.
- Objects that are not italicized are applicable to the selected device only.
- Objects that have a strike through them are also template objects but there is an overriding device object that has the same key. For example, a similar object may have been created using the CLI.
- Objects that are maroon in color and have a strike through them are deleted device objects. These objects exist in the template but not in the device.

Figure 82 Device/Template Objects Legends



Device Hierarchy

Devices
Device: s-204 (IP: 172.16.133.204)
Device: s-209 (IP: 172.16.133.209; Template :Switch Template)
Application Groups
ApplicationGroup: Device Overriding Group, Device : s-209
~~ApplicationGroup: somegroup, Device : s-209 (IP: 172.16.~~
ApplicationGroup: FTP, Template : Switch Template
ApplicationGroup: IM, Template : Switch Template
ApplicationGroup: NetworkConnectivity, Template : Switch
ApplicationGroup: P2P, Template : Switch Template
~~ApplicationGroup: somegroup, Template : Switch Templat~~
ApplicationGroup: Web, Template : Switch Template

deleted device object

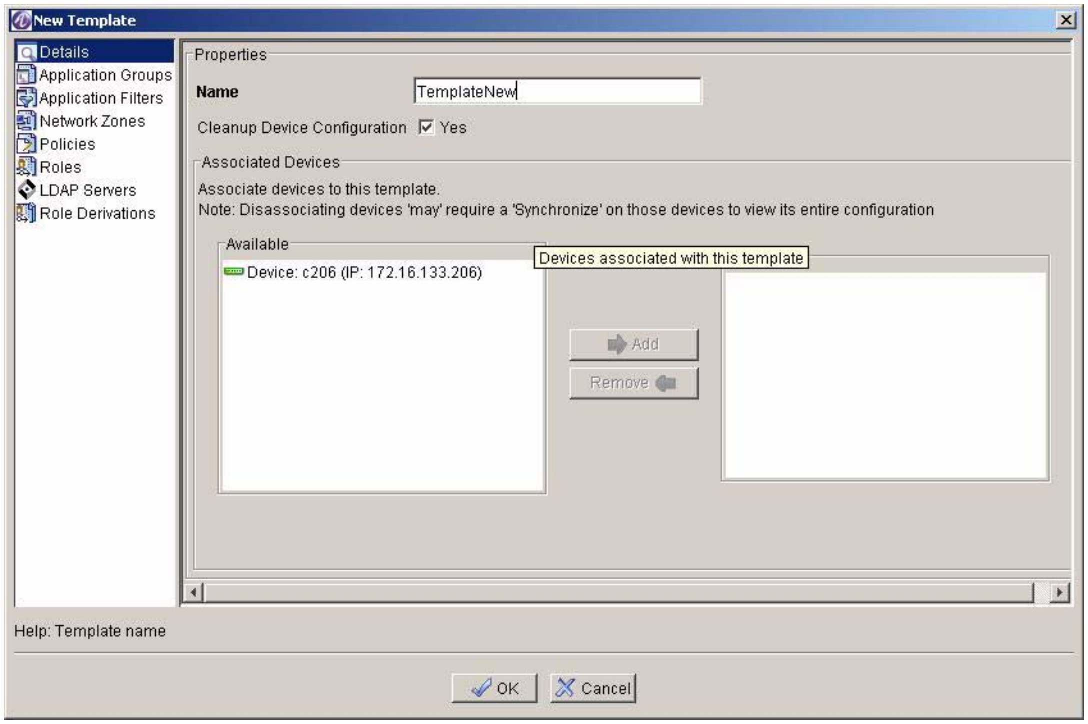
template object with overriding device object

Creating a New Template

To create a new template:

1 Select Templates from the navigation tree (*Figure 61*) and click **New** New... in the Action Bar. The New Template dialog box displays (*Figure 83*).

Figure 83 New Template



Name: TemplateNew

Cleanup Device Configuration ☑ Yes

Associate devices to this template.

Note: Disassociating devices 'may' require a 'Synchronize' on those devices to view its entire configuration

Device: c206 (IP: 172.16.133.206)

Help: Template name

2 The new template comprises of the template objects (application group, application filters, policies, and so forth) you have already defined. Specify the name for the template in the Name field.

3 For the **Cleanup Device Configuration**, select **Yes** if you want to cleanup device configuration. Selecting yes cleans up the device-only objects so that the template-only objects are configured.

NOTE: Select the Yes checkbox if you want the device to be configured only with the associated template. When Deploy Template only is used, the device is updated only with template objects. If you deselect this box, the device is configured with the template objects and also with the device objects.

4 From the Available column choose the devices to which you want to apply the template.

5 From the current column, choose the devices that you want to disassociate from the template.

6 Click **OK**. The new template is now associated with the selected devices.

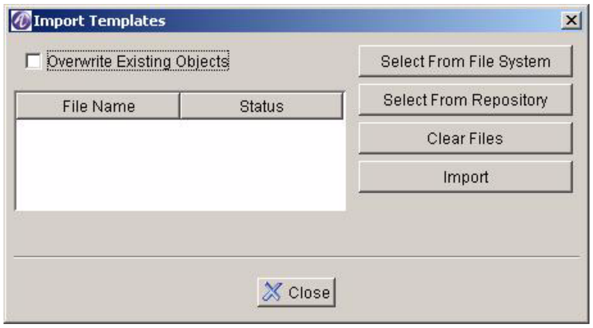
Importing Templates

To import a new template:

1 In Device view, select Templates from the Navigation Tree.

2 Select Import from the Page Bar. The Import Template dialog box appears (*Figure 84*).

Figure 84 Import Template



3 Select **Overwrite Existing Objects** if you want the device objects to be overwritten.

4 Click **Select from File System** to select a template that you have saved previously as a file.

5 Click **Select from Repository** to select a template from the template repository. The selected template displays under File Name. For more information, see *Template Repository*.

6 Click **Clear Files** to remove all selected files.

7 Click **Import** to import the selected template.

Template Repository

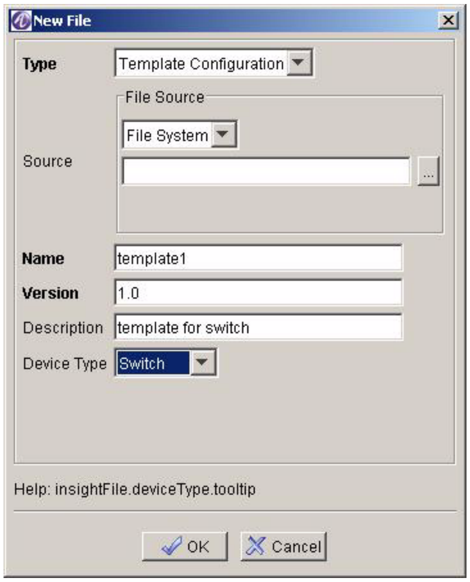
OmniVista SafeGuard Manager allows you to save templates in a repository, such that you can select from a list of templates for importing or deploying templates.

To save a template to the repository:

1 Select Template Repository from the Navigation Tree.

2 Click New. The New File screen displays (*Figure 85*).

Figure 85 New File



Type: Template Configuration

Source: File System

Name: template1

Version: 1.0

Description: template for switch

Device Type: Switch

Help: insightFile.deviceType.tooltip

3 Enter the attributes as follows:

Table 33 Edit Interface Attributes

Attribute Name	Description
Type	From the dropdown list, select Template Configuration.
Source	From the dropdown source list, select Template. Browse for the source where you saved your templates.
Name	Enter a descriptive name for the template.
Version	Provide a version so template cannot be overridden.
Device Type	Select a device type: Switch, Controller, or any.

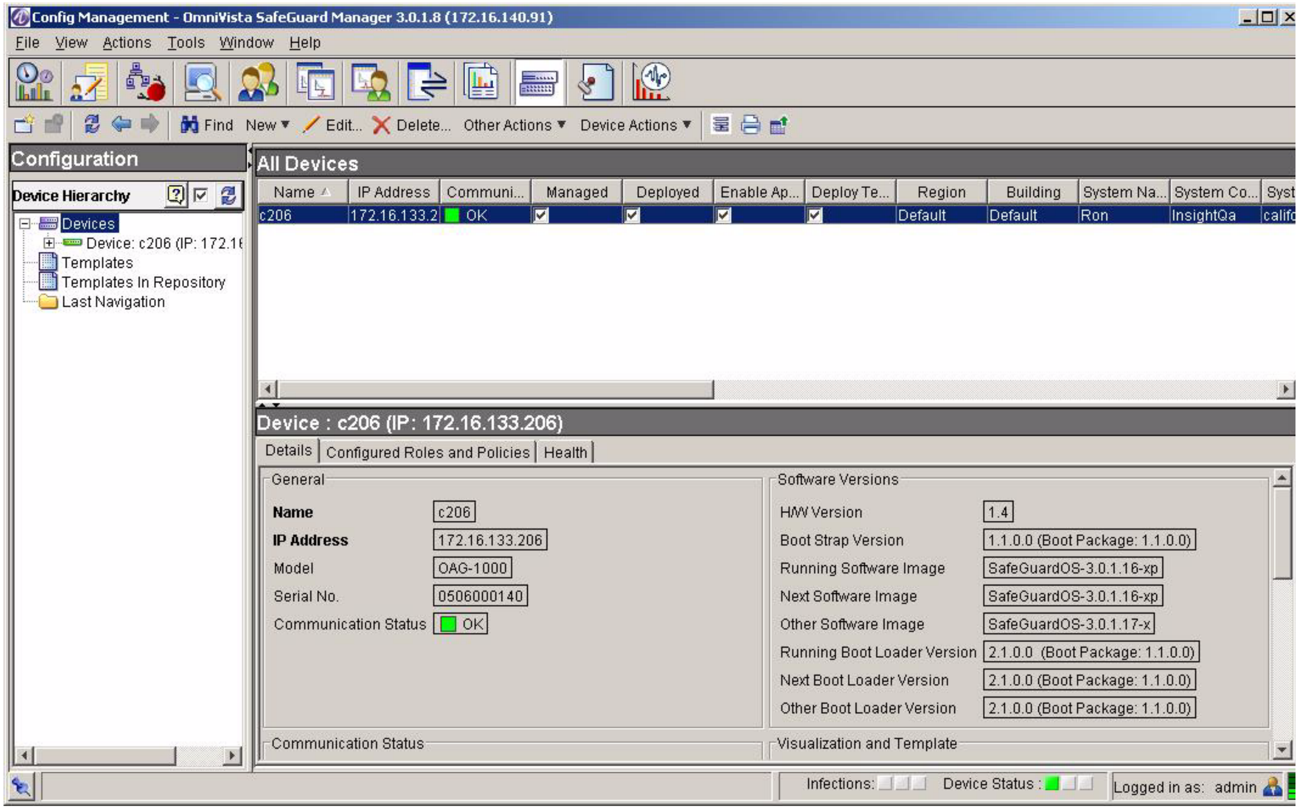
4 Select OK to save the template in the template repository.

Deleting an Existing Device

To delete an existing device:

1 Click the Device Configuration icon from the OmniVista SafeGuard Manager Page Bar. The Config Management panel displays (*Figure 86*).

Figure 86 Config Management


Config Management - OmniVista SafeGuard Manager 3.0.1.8 (172.16.140.91)
File View Actions Tools Window Help
Find New ▾ Edit... Delete... Other Actions ▾ Device Actions ▾
Configuration
Device Hierarchy
Devices
Device: c206 (IP: 172.1€
Templates
Templates In Repository
Last Navigation
All Devices

Name	IP Address	Communi...	Managed	Deployed	Enable Ap...	Deploy Te...	Region	Building	System Na...	System Co...	Syst
c206	172.16.133.2	🟩 OK	☑	☑	☑	☑	Default	Default	Ron	InsightQa	califo

Device : c206 (IP: 172.16.133.206)
Details Configured Roles and Policies Health

General

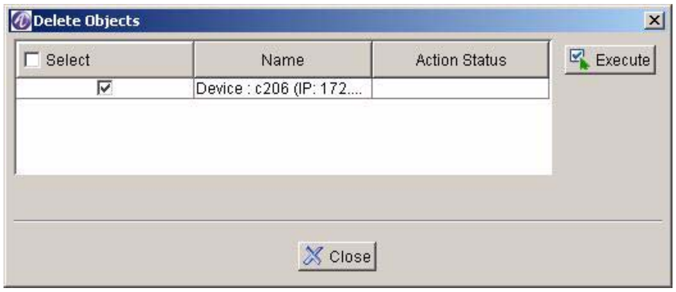
Name	c206
IP Address	172.16.133.206
Model	OAG-1000
Serial No.	0506000140
Communication Status	🟩 OK

Software Versions

H/W Version	1.4
Boot Strap Version	1.1.0.0 (Boot Package: 1.1.0.0)
Running Software Image	SafeGuardOS-3.0.1.16-xp
Next Software Image	SafeGuardOS-3.0.1.16-xp
Other Software Image	SafeGuardOS-3.0.1.17-x
Running Boot Loader Version	2.1.0.0 (Boot Package: 1.1.0.0)
Next Boot Loader Version	2.1.0.0 (Boot Package: 1.1.0.0)
Other Boot Loader Version	2.1.0.0 (Boot Package: 1.1.0.0)

2 In the navigation tree, select the device you want to delete, and click the **Delete** icon from the Action Bar. The Delete Objects dialog box displays (*Figure 87*).

Figure 87 Delete Confirmation Dialog Box



□ Select	Name	Action Status
☑	Device : c206 (IP: 172....	

3 Click **Select** checkbox to delete all devices or select the checkbox next to the device you want to delete.

4 Click **Execute** to perform the deletion. The selected device is removed from the list of added devices.

5 Click **Cancel** to cancel the deletion.

Polling a Device

Polling is done automatically; no user interface exists. OmniVista SafeGuard Manager checks to see if the connection to the device still exists and if the SNMP agent is running. If the device cannot be reached, OmniVista SafeGuard Manager pings the device through an OmniVista SafeGuard Manager Visualization Channel to ensure that the device is reachable. If the ping fails, a device-unreachable alarm is generated and the device health indicator is changed accordingly. OmniVista SafeGuard Manager continues to poll the device and if the device responds to SNMP requests, the alarms are cleared and an ICC connection is initiated. The device status shows the state of the device.

Synchronizing a Device

Synchronization is performed to ensure that you are viewing the latest data from the device, to collect the latest device health and status statistics, and server statistics. Synchronization can be performed in one of the following ways:

- Manually—The administrator clicks Sync Device in the device table view which synchronizes the device and port configuration data that could have changed asynchronously through the CLI. The visualization data is not synchronized because it is TCP based and OmniVista SafeGuard Manager client should already have this data. For more information on how to manually synchronize a device, see *Manually Synchronizing a Device*.
- Automatically after a communication loss—If an OmniVista SafeGuard Manager poll detects that communication was lost and then regained, a full synchronization is automatically performed, which synchronizes both the configuration and the visualization data.
- Automatically after device reboot—When a device is rebooted, polling detects that communication was lost and regained and a full synchronization is automatically performed. OmniVista SafeGuard Manager detects the device reboot based on the `sysUpTime` of the device. A device reboot synchronizes both the configuration and the visualization data. As the device clears the visualization data on a reboot, the corresponding data is pushed to history.

Manually Synchronizing a Device

To manually synchronize a device from the Config Management window:

1 Click the Config Management icon from the Page Bar or select the *View* > *Go To* > *Config Management* menu item.

2 From the list of devices, select the device from which you want to synchronize data.

3 Select *Device Actions* > *Synchronize Configuration* from the Action Bar. A confirmation dialog box displays.

4 Select **Yes** to proceed with the synchronization. The synchronization process begins, and you see a "*sync device in progress*" message in the status bar. After synchronization is completed, the status bar displays a "*Sync Device status: Succeeded*" message in the status bar. Device configuration data is now successfully synchronized.

Device Actions

OmniVista SafeGuard Manager's Config Management allows you to perform the basic configuration, file, and refresh actions on devices.

NOTE: From the Config Management view, you can access Device Actions menu items from the Action Bar, or using a key sequence, or by selecting a device and right-clicking. The menu and the key sequence are provided with each device action discussed below.

To access the pull-down Device Actions menu:

1 Select the Device Configuration icon from the Page Bar or select the *View* > *Go To* > *Config Management* menu item.

2 Click the down arrow next to the Device Actions menu in the Action Bar to see the menu items.

The following menu items are available:

Table 34 Device Actions Menu

Menu Item	Available Actions
Manage Configuration	■ Synchronize Configuration (**Ctrl**+**Shift**+**Y**)—synchronizes the configuration such that you see the latest data from the device. ■ Deploy Changes (**Ctrl**+**Shift**+**D**)—deploys the configuration changes. ■ Save Running Config (**Ctrl**+**Shift**+**S**)—saves the running configuration such that the configuration changes persist after a device reboot. ■ Back up Configuration (**Ctrl**+**Shift**+**V**)—saves the CLI configuration in the repository.
Manage Files	■ Upgrade Software (**Ctrl**+**Shift**+**U**)—allows you to upgrade a selected device or all devices to the next available software version. ■ Upgrade BootLoader (**Ctrl**+**Shift**+**L**)—allows you to distribute a bootloader image as an ordinary file. ■ Distribute File (**Ctrl**+**Shift**+**F**)—allows you to select a file to be downloaded to the selected device.
Reboot Device	(**Ctrl**+**Shift**+**B**) Reboots the selected device.
Refresh	■ Refresh Policies (**Ctrl**+**Shift**+**P**)—refreshes policies on the device. ■ Refresh Roles (**Ctrl**+**Shift**+**O**)—refreshes roles.

Manage Configuration

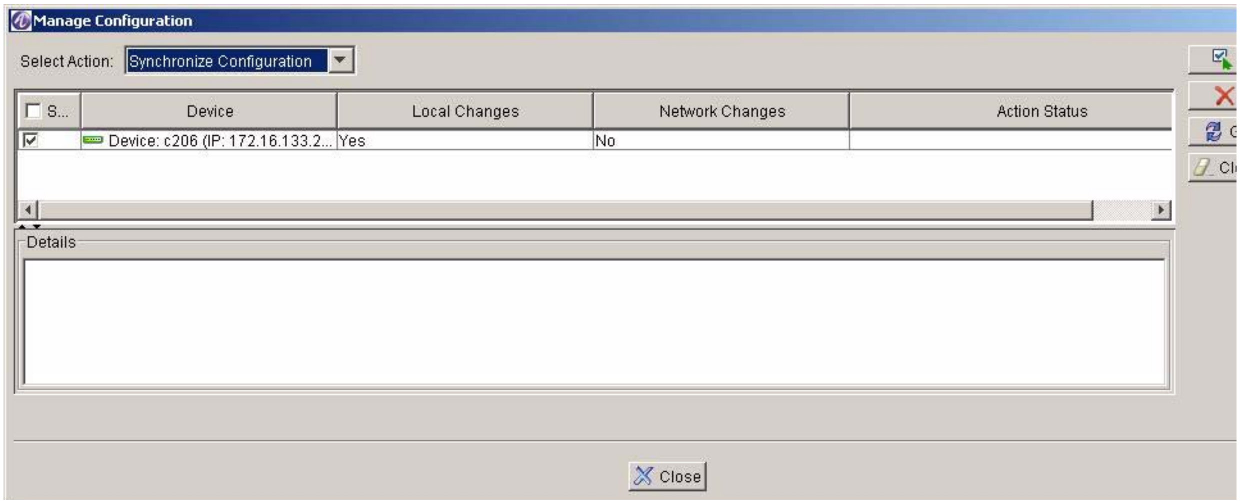
OmniVista SafeGuard Manager allows you to synchronize, deploy changes, save a running configuration, and to retrieve a version configuration on a device using the Manage Configuration dialog box.

Synchronize Configuration

To synchronize configuration on a device:

1 Select *Device Actions* > *Manage Configuration* > *Synchronize Configuration* (**Ctrl**+**Shift**+**Y**) from the Config Management window. The Manage Configuration dialog box displays (*Figure 88*).

Figure 88   Manage Configuration Dialog Box (Synchronize Configuration)



Select Action: Synchronize Configuration

☐ S...	Device	Local Changes	Network Changes	Action Status
☑	Device: c206 (IP: 172.16.133.2...	Yes	No	

2 From the Select Action dropdown list, select Synchronize Configuration.

3 Select the device for which you want to synchronize data.

4 Click **Execute**. Data synchronization begins and synchronization details are shown in the Action Details (lower-half) section of the screen.

5 Click **Cancel** to cancel the synchronization.

6 Click **Get Status** to get the current device status.

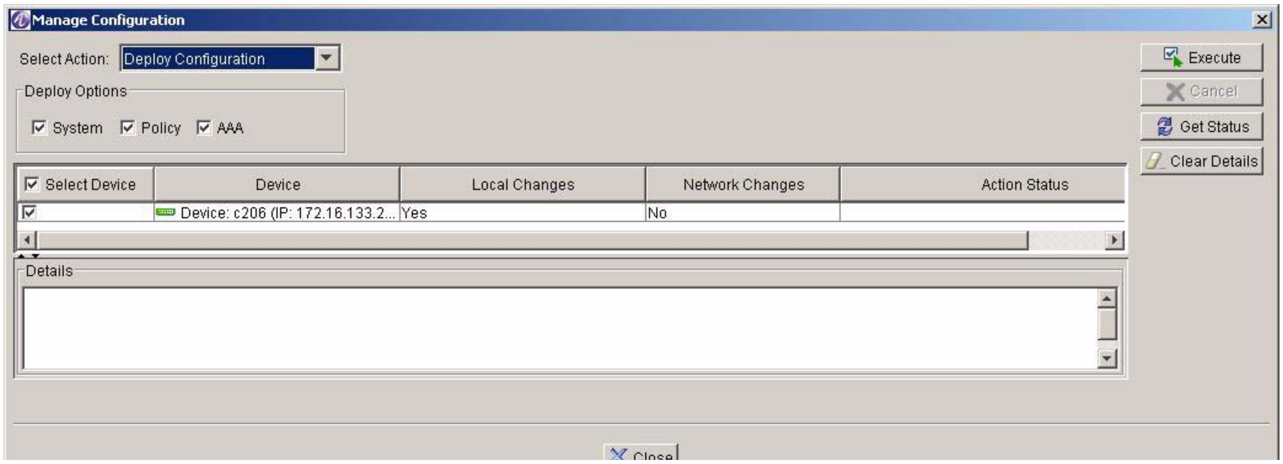
7 Click **Clear Details** to clear status details.

Deploy Changes

To deploy changes on a device:

1 Select *Device Actions* > *Manage Configuration* > *Deploy Changes* (**Ctrl**+**Shift**+**D**) from the Config Management window. The Manage Configuration dialog box displays (*Figure 89*).

Figure 89 Manage Configuration Dialog Box (Deploy Changes)



Select Action: Deploy Configuration

Deploy Options

☑ System ☑ Policy ☑ AAA

☑ Select Device	Device	Local Changes	Network Changes	Action Status
☑	Device: c206 (IP: 172.16.133.2...	Yes	No	

2 Select the deploy options (system, policy, or/and AAA) that you want to apply.

3 Select the device to which you want to deploy the changes.

4 Click **Execute**. Changes are deployed and the status is displayed in the Action Details (lower-half) section of the screen.

NOTE: Changes can be template-based or device-based. If you deploy template only changes, the template is changed and all devices associated with the template are updated. If you deploy device-only changes, only the selected device is updated.

5 Click **Cancel** to cancel the deployment.

6 Click **Get Status** to get the current device status.

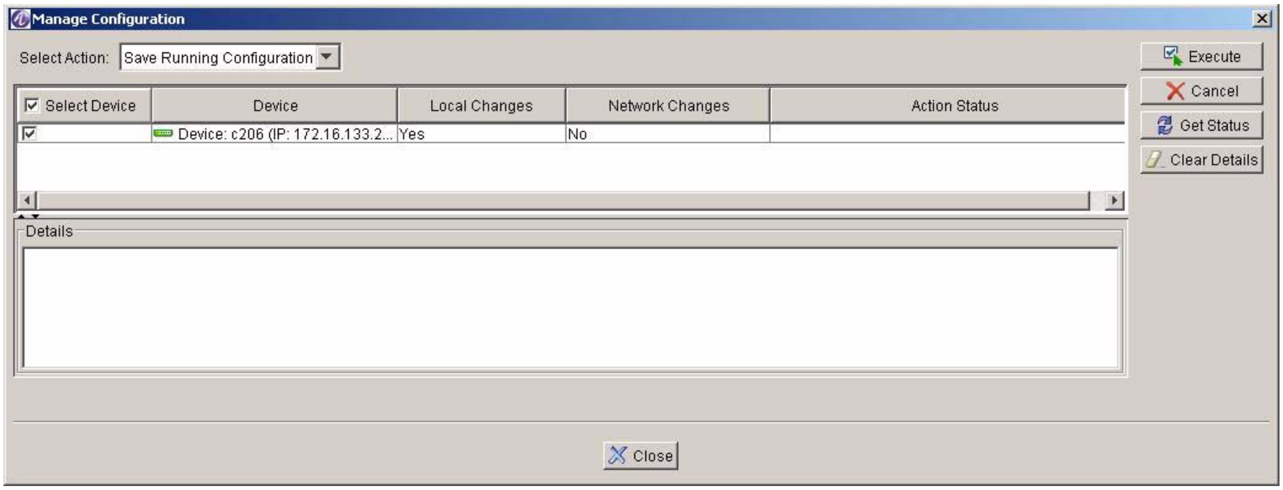
7 Click **Clear Details** to clear status details.

Save Running Config

To save a running config:

1 Select *Device Actions* > *Manage Configuration* > *Save Running Config* (**Ctrl**+**Shift**+**S**) from the Config Management window. The Manage Configuration dialog box displays (*Figure 90*).

Figure 90 Save Running Config



Select Action: Save Running Configuration

☑ Select Device	Device	Local Changes	Network Changes	Action Status
☑	Device: c206 (IP: 172.16.133.2...	Yes	No	

2 Select the device for which you want to save the running config.

3 Click **Execute**. The status is displayed in the Action Details (lower-half) section of the screen.

4 Click **Cancel** to cancel saving the running configuration file.

5 Click **Get Status** to get the current device status.

6 Click **Clear Details** to clear status details.

Backup CLI Configuration

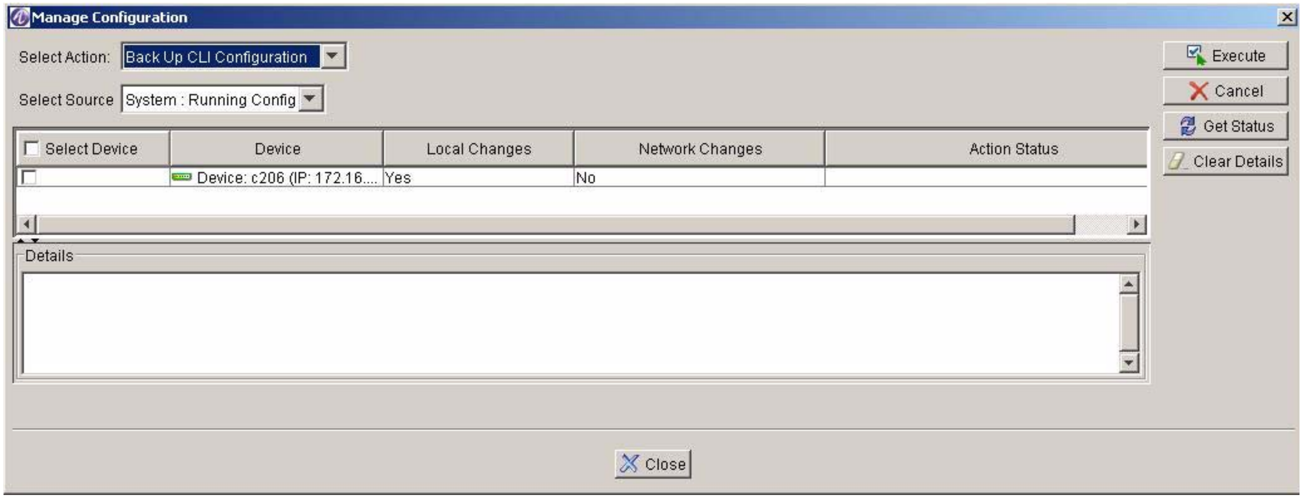
OmniVista SafeGuard Manager allows you to create configuration versions for a device and distribute a specific version to the device when needed. You can create configuration versions for a specific device using one of the following two ways:

- Multiple devices, using *Device Actions* > *Manage Configuration* > *Backup CLI* Configuration.
- Individual device, by clicking "**Backed Up CLI Configurations**" on the tree node under the selected device in the tree and then clicking **New**.

To create a configuration version:

1 Select *Device Actions* > *Manage Configuration* > *Backup CLI Configuration* (**Ctrl**+**Shift**+**V**) from the Config Management window. The Manage Configuration dialog box displays (*Figure 91*).

Figure 91 Backup CLI Configuration



Manage Configuration

Select Action: Back Up CLI Configuration

Select Source: System : Running Config

☐ Select Device	Device	Local Changes	Network Changes	Action Status
☐	Device: c206 (IP: 172.16....	Yes	No	

Details

2 Select Backup CLI Configuration from the Select Action dropdown list.

3 Select the configuration file you want from the Select Source dropdown list.

4 Click the Select box to select all the devices in the list. For individual device, select the checkbox next to the device for which you want to save the configuration version.

5 Click **Execute**. The status is displayed in the Action Details (lower-half) section of the screen.

NOTE: OmniVista SafeGuard Manager contacts each selected device for its `nvram:startup-config` and copies it as a file that belongs to the selected device.

6 Click **Cancel** to cancel the backup.

7 Click **Get Status** to get the current device status.

8 Click **Clear Details** to clear status details.

Viewing CLI Configuration Versions

Any CLI configuration versions that you have created can be viewed under the device hierarchy tree.

To view CLI configuration versions:

1 Select the device for which you want to view CLI configuration versions.

2 In the device hierarchy, select the **Backed Up CLI Configuration** tree node. Any created versions are shown in the right-hand side of the screen.

3 Select a file and click **Show Contents** to view the contents of the selected file.

Manage Files

OmniVista SafeGuard Manager allows you to upgrade or rollback software on devices.

To manage files:

1 Select the Device Configuration icon from the Page Bar or select the *View > Go To > Config Management* menu item.

2 Select Manage Files from the Device Actions pull-down menu. The following options are available:

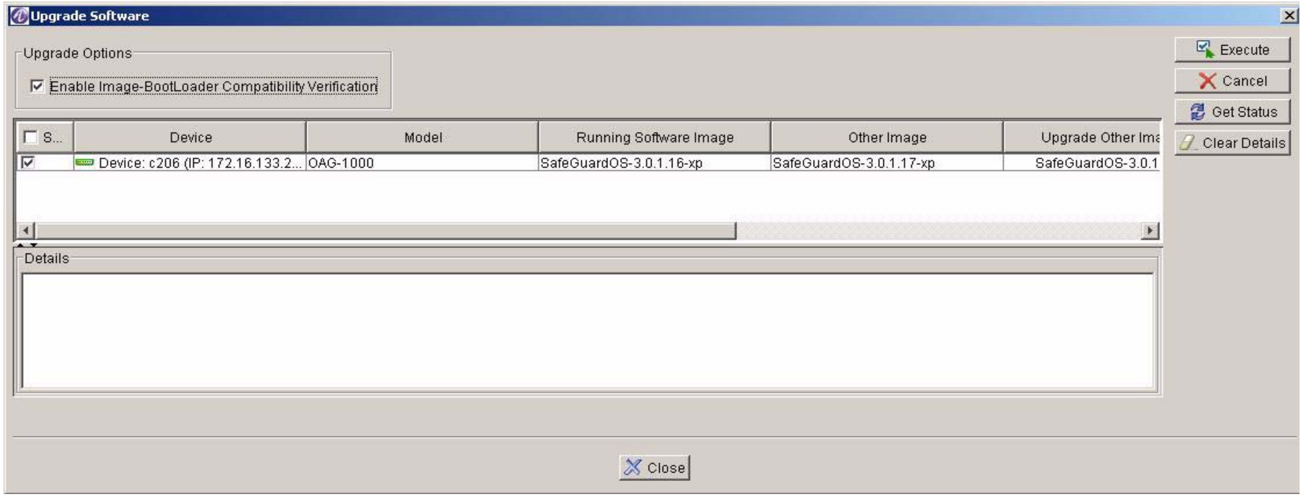
- Upgrade Software—allows you to upgrade the software version on the device.
- Upgrade bootloader—allows you to upgrade a bootloader image.
- Distribute file—allows you to manage files in a repository and distribute as necessary.

Upgrade Software

To upgrade a software image:

1 Select *Device Actions > Manage Software > Upgrade Software* (**Ctrl+Shift+U**) from the Config Management window. Or, right-click on any device and select *Device Actions > Distribute Image*. The Software Upgrade dialog box displays (*Figure 92*).

Figure 92 Software Upgrade Dialog Box



Upgrade Options

☑ Enable Image-BootLoader Compatibility Verification

□ S...	Device	Model	Running Software Image	Other Image	Upgrade Other Ima
☑	Device: c206 (IP: 172.16.133.2...	OAG-1000	SafeGuardOS-3.0.1.16-xp	SafeGuardOS-3.0.1.17-xp	SafeGuardOS-3.0.1

2 Enter the information as shown below:

Table 35 Software Upgrade Dialog Box Attributes

Column Name	Description
Select Device	Select the Select Device checkbox to upgrade all devices in the list. You can upgrade on a per device basis by selecting the checkbox next to each device.
Device	Displays the device name with its IP address.
Model	Specifies the type of device: controller or switch. The software images displayed in the “Next Software Image” column depend on the device type.
Running Software Image	Shows the current software image that is running on the device.
Upgrade Image	Shows the software image to be copied to the device.
Boot	Select this checkbox if you want to boot the device after the image is copied. Default is for all devices to be booted after a software upgrade.

Table 35 Software Upgrade Dialog Box Attributes

Column Name	Description
Action Status	Shows the upgrade status. Possible values are: ■ Scheduled ■ In progress ■ Copying ■ Booting ■ Success ■ Failure

3 Click **Execute** to start copying the new software image.

4 Click **Cancel** to cancel the upgrade.

5 Click **Get Status** to get the current device status.

6 Click **Clear Details** to clear status details.

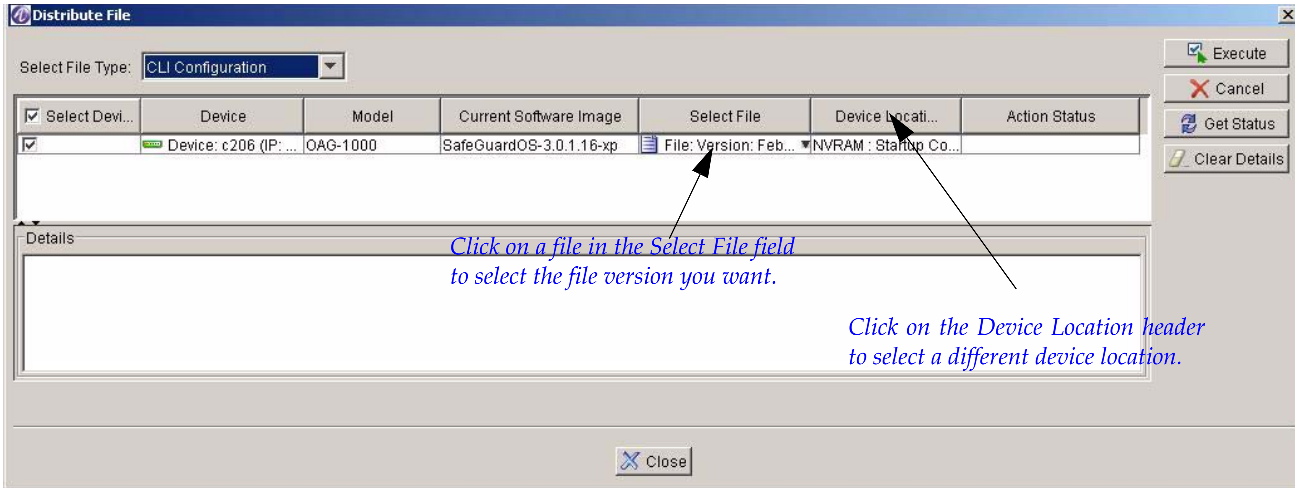
Distribute File

OmniVista SafeGuard Manager allows you to create, store, and manage template configuration, boot loader, ICS portal configuration, ICS policy configuration, and captive portal web page files in a repository. The simplest way to manage files and distribute them is to create a file for a specific device, store it in the repository, and then distribute the file. For more information on file management and to see the types of files that can be managed, see *File Repository*. Once the files are available in the repository, you can select a file to be downloaded or distributed to a selected device or a list of devices.

To distribute a file:

1 Select *Device Actions* > *Distribute File* (**Ctrl**+**Shift**+**F**) from the Config Management window. Or, right-click on any device and select *Device Actions* > *Distribute File*. The Distribute File dialog box displays (*Figure 93*).

Figure 93 Distribute File Dialog Box



Select File Type: CLI Configuration

☑ Select Devi...	Device	Model	Current Software Image	Select File	Device Locati...	Action Status
☑	Device: c206 (IP: ...	OAG-1000	SafeGuardOS-3.0.1.16-xp	File: Version: Feb...	NVRAM : Startup Co...	

Click on a file in the Select File field to select the file version you want.

Click on the Device Location header to select a different device location.

2 Enter the user configurable fields as shown below:

Table 36 Distribute File Dialog Box Attributes

Column Name	Description
Select File Type	Select the type of file you want to distribute. Following file types are supported: ■ CLI Configuration ■ Boot Loader ■ ICS Portal Configuration ■ ICS Policy Configuration ■ Captive Portal Web Page ■ Other
Select Device	Select the Select Device checkbox to select all devices in the list to which the file is to be downloaded. You can select the file to be downloaded on a per device basis by selecting the checkbox next to each device.
Device	Displays the device name with its IP address.
Device Type	Specifies the type of device: controller or switch.
Current Software Image	Shows the current software image that is running on the device.
Select File	This is a user-selectable field that shows a list of all applicable files, including date and version, that are available for distribution. Click on a file name to get the version you want to distribute.

Table 36 Distribute File Dialog Box Attributes

Column Name	Description
Device Location	Clicking on this field brings up a dialog box that lets you choose the device location to which you want to distribute the file. Select the appropriate location from the dropdown list and click OK. The new location will display in the Device Location column.
Action Status	Shows the file download status.

3 Click **Execute** to distribute the file.

NOTE: The Distribute File feature uses the “copy” CLI command to copy the file to the selected devices.

4 Click **Cancel** to cancel the distribution.

5 Click **Get Status** to get the current device status.

6 Click **Clear Details** to clear the status details.

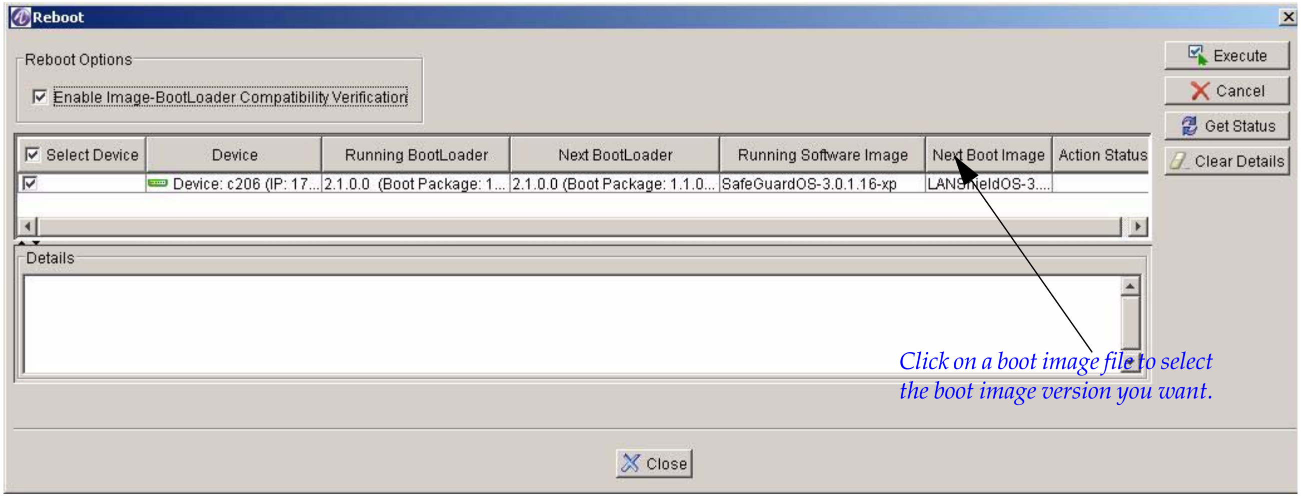
Reboot Device

You can reboot a single device or multiple devices from the OmniVista SafeGuard Manager Configuration Management window.

To reboot a device:

1 Select *Device Actions* > *Reboot Device* from the Config Management window. Or, right-click on any device and select *Device Actions* > *Reboot Device* (**Ctrl**+**Shift**+**B**). The Reboot Device dialog box displays (*Figure 94*).

Figure 94 Reboot Device Dialog Box



☑ Enable Image-BootLoader Compatibility Verification

☑ Select Device	Device	Running BootLoader	Next BootLoader	Running Software Image	Next Boot Image	Action Status
☑	Device: c206 (IP: 17...	2.1.0.0 (Boot Package: 1...	2.1.0.0 (Boot Package: 1.1.0...	SafeGuardOS-3.0.1.16-xp	LANShieldOS-3....	

Click on a boot image file to select the boot image version you want.

2 Enter the user configurable information:

Table 37 Reboot Device Dialog Box Attributes

Column Name	Description
Select Device	Select the checkbox next to the device that needs to be rebooted or select the Select Device checkbox for all devices in the list.
Device	Displays the device name with its IP address.
Running BootLoader	
Next BootLoader	Shows the image name that is going to be used when the server boots up. The next boot image is determined based on “Image selected.” Click on the next boot image file to get a list of boot images available for the selected device.
Running Software Image	Shows the current software image that is running on the device.
Next Boot Image	

Table 37 Reboot Device Dialog Box Attributes

Column Name	Description
Action Status	Shows the reboot status.

3 Click **Execute** to reboot the selected device.

> **NOTE:** If the software image is not found to be compatible with the bootloader image, OmniVista SafeGuard Manager will not execute boot on the selected device.

4 Click **Cancel** to cancel reboot.

5 Click **Get Status** to get the current device status.

6 Click **Clear Details**

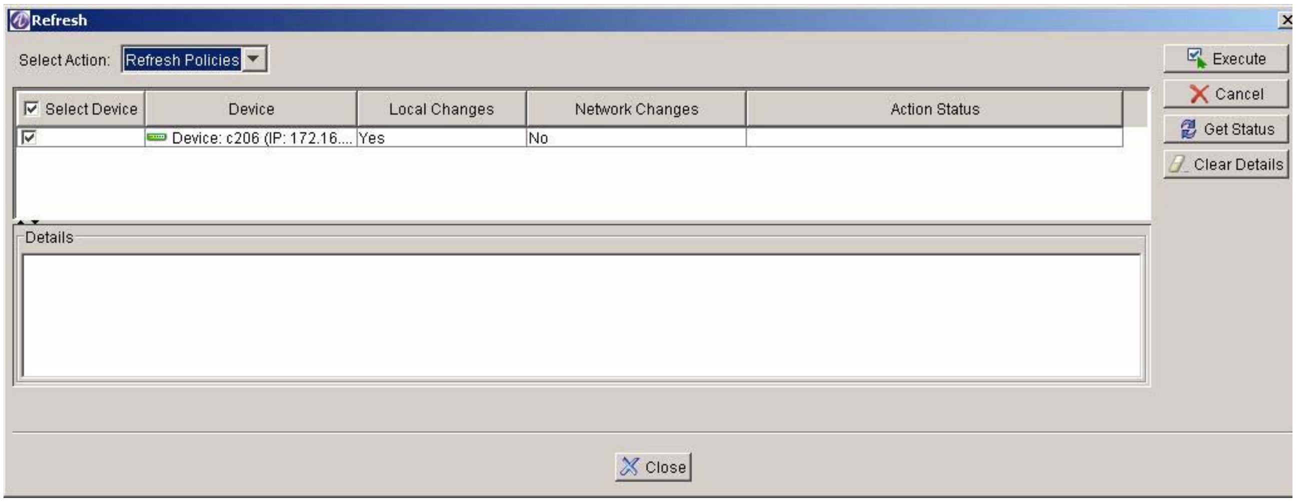
Refresh

OmniVista SafeGuard Manager allows you to refresh policies and/or roles on a selected device.

To refresh policies or roles:

1 Select *Device Actions* > *Refresh* > *Refresh Policies* (**Ctrl**+**Shift**+**P**) from the Config Management window if you want to refresh policies. Or, to refresh roles, select *Device Actions* > *Refresh* > *Refresh Roles* (**Ctrl**+**Shift**+**O**). The Refresh dialog box displays (*Figure 95*).

Figure 95 Refresh Dialog Box



Select Action: Refresh Policies

☑ Select Device	Device	Local Changes	Network Changes	Action Status
☑	Device: c206 (IP: 172.16....	Yes	No	

2 Enter the information as shown below:

Table 38 Refresh Dialog Box Attributes

Column Name	Description
Select Action	Select “Refresh Roles” if you want to refresh roles or select “Refresh Policies” to refresh all policies on the selected device.
Select Device	Select the checkbox next to the device for which you want to refresh policies or roles.
Device	Device name, including the IP address.
Local Changes	Shows if the device changes were made locally to a device.
Network Changes	Shows if the device changes are applicable network-wide.
Action Status	Shows the refresh status.
Action Details	Shows the refresh details.

3 Click **Execute** to refresh the roles or policies.

4 Click **Cancel** to cancel refreshing roles or policies.

5 Click **Get Status** to get the current device status.

6 Click **Clear Details** to clear the status details.

Other Actions

You can execute show commands, delete visualization, create or update templates, using the Other Actions menu available through Config Management.

To access the pull-down Other Actions menu:

1 Select the Device Configuration icon from the Page Bar or select the *View* > *Go To* > *Config Management* menu item.

2 Click the down arrow next to the Other Actions menu in the Action Bar to see the menu items.

The following menu items are available:

Table 39 Other Actions Menu

Menu Item	Available Actions
Execute Show Command	Execute a show command on a selected device. For more information, see *Execute Show Commands*.
ICS Admin	Save the ICS portal configuration. For more information, see *ICS Admin*.
Delete Visualization Data	Delete visualization records. For more information, see *Delete Visualization Data*.
Create Template	Create a new template. For more information, see *Creating a New Template*.
Update Template	Update an existing template. For more information, see *Update Template*.
Discard Non-template changes	Ignore non-template changes made to the device. For more information, see *Discard Non-template Changes*.
Show Device Health	Displays device health and statistics. For more information, see *Viewing Device Health Statistics*.
Show Interface Statistics	Displays interface statistics. For more information, see*Viewing Server Health Statistics*.

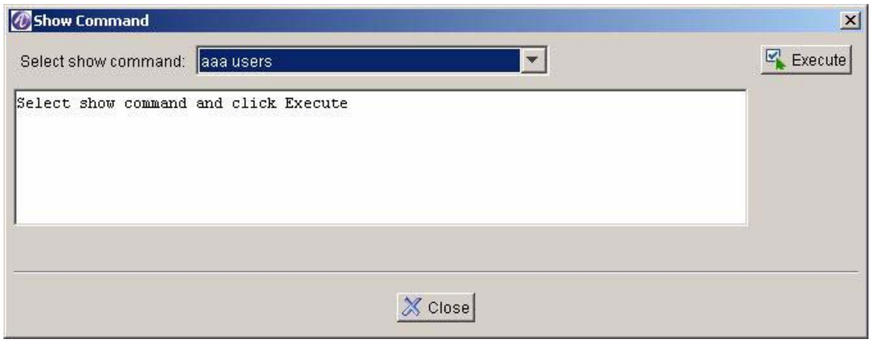
Execute Show Commands

OmniVista SafeGuard Manager allows you to execute a show command on any of the selected devices.

To execute a show command:

1 Select *Other Actions > Execute Show Command* from the Config Management window. Or, right-click on the device for which you want to execute a show command to access the Other Actions menu. The Show Command dialog box displays (*Figure 96*).

Figure 96 Show Command



```
Select show command and click Execute
```

2 Select a show command from the dropdown list.

NOTE: Certain show commands are not available if 4-eye mode is enabled. These commands are only visible if the administrator logs in the 4-eye mode. For more information on 4-eye mode, see *Enabling Dual-Admin or 4-Eye Mode*.

3 Click **Execute**. The show command results display in the text area in the bottom half of the screen. An error message will display if OmniVista SafeGuard Manager is unable to communicate to the selected device.

ICS Admin

When you first reboot the device, OmniVista SafeGuard Manager uploads the ICS portal configuration along with the device configuration. This configuration persists in the OmniVista SafeGuard Manager server as a file that allows you to deploy the configuration at a later stage.

To change the ICS configuration:

1. Select the device for which you want to save the ICS configuration file.
2. Select *Other Actions* > *ICS Admin*. OmniVista SafeGuard Manager takes a few seconds to connect to the device and a web page is displayed where you can directly change the ICS configuration for the selected device.

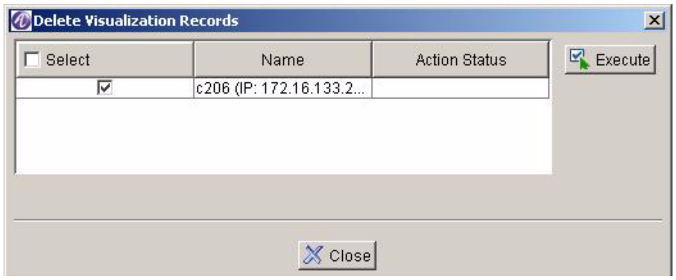
Delete Visualization Data

OmniVista SafeGuard Manager allows you to delete visualization records (flow summary and layer 7 details) for any of the selected devices.

To delete visualization records:

1. Select *Other Actions* > *Delete Visualization Data* from the Config Management window. Or, right-click on the device for which you want to delete visualization records. The Delete Visualization Records dialog box displays (*Figure 97*).

Figure 97 Delete Visualization Records



□ Select	Name	Action Status
☑	c206 (IP: 172.16.133.2...	

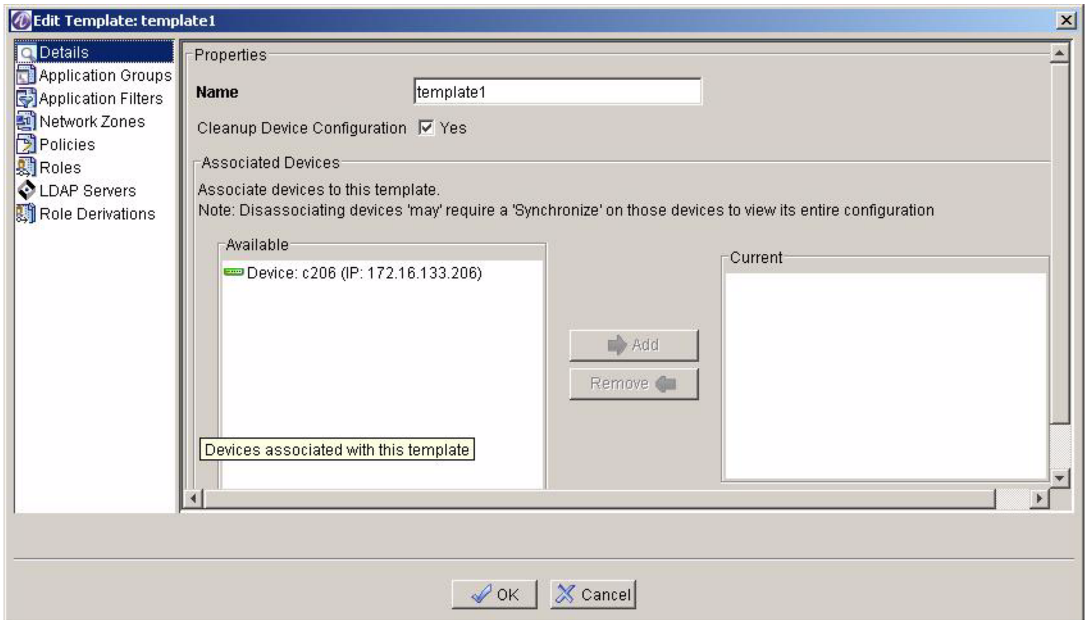
2. Click the Select checkbox to select all devices in the list or click the checkbox next to the device for which you want to delete visualization records.
3. Click **Execute**. The deletion results are shown in the text box. If OmniVista SafeGuard Manager is unable to communicate with the device, an error message is displayed.

Update Template

To update or make any changes to an existing template:

1 Select *Other Actions* > *Update Template* from the Config Management window. Or, in the navigation tree, select the template you want to update and click **Edit**. The Edit Template dialog box displays (*Figure 98*).

Figure 98 Edit Template



Name: template1

Cleanup Device Configuration ☑ Yes

Associate devices to this template.

Note: Disassociating devices 'may' require a 'Synchronize' on those devices to view its entire configuration

Device: c206 (IP: 172.16.133.206)

2 For the **Cleanup Device Configuration**, select **Yes** if you want to cleanup device configuration. Selecting yes cleans up the device-only objects so that the template-only objects are configured.

NOTE: Select the Yes checkbox if you want the device to be configured only with the associated template. When Deploy Template only is used, the device is updated only with template objects. If you deselect this box, the device is configured with the template objects and also with the device objects.

3 From the Available column choose the devices to which you want to apply the template.

4 From the current column, choose the devices that you want to disassociate from the template.

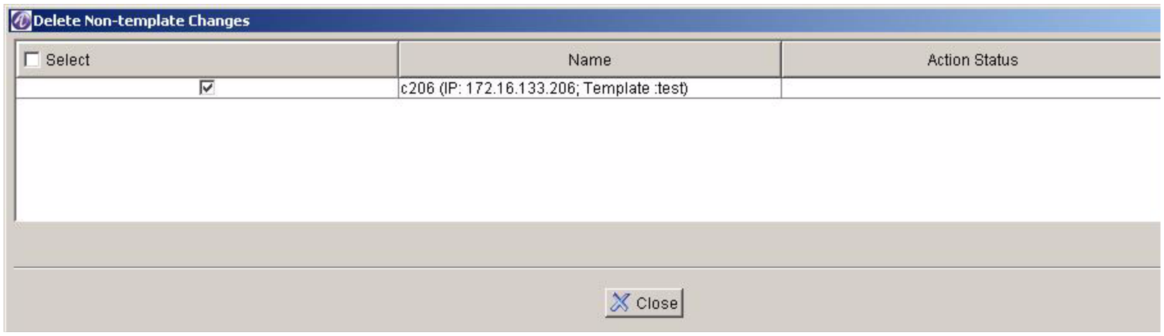
5 Click **OK**. The updated template is now associated with the selected devices.

Discard Non-template Changes

To discard any changes that were made to the device but not to the template:

1. Select *Other Actions > Discard Non-template Changes* from the Config Management window. The Discard Non-template Changes dialog box displays (*Figure 99*).

Figure 99 Discard Non-template Changes



Delete Non-template Changes

□ Select	Name	Action Status
☑	c206 (IP: 172.16.133.206; Template :test)	

2. Select the device on which you want to discard any non-template changes.

3. Click **Execute** to discard changes.

Understanding Device Management Display

OmniVista SafeGuard Manager can be used to manage partial configuration of SafeGuard devices. The configurable objects fall under the following two categories:

- Policy
  - Application Group
  - Application Filter
  - Network Zone
  - User Policies
  - Roles
- Authentication, Authorization, and Accounting (AAA)
  - Role Derivation
  - LDAP Server

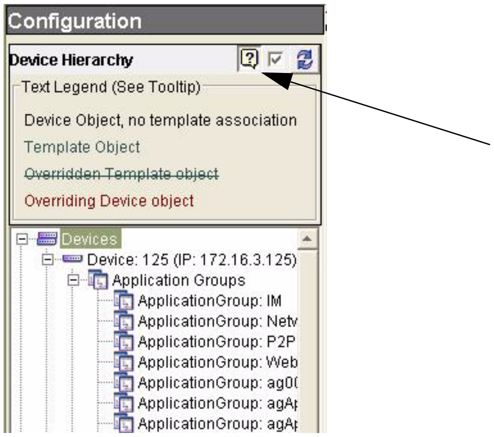
The navigation tree depicting the device/template hierarchy uses different legends to differentiate between template objects. It is important to understand the visual differences between these objects in order to simplify the management of templates across several devices. *Table 40* shows the legends and what they mean:

Table 40 Template Objects

Legend	Description
Device object, no template association	Objects that appear in black belong to a device when the device is not associated with a template.
Template object	Objects that appear in blue belong to a template.
~~Overridden template object~~	Objects that have a strike through them are also template objects but there is an overriding device object that has the same key.
~~Deleted Device Object~~	Device objects that have been deleted have a strike through them and appear in maroon color. These objects exist in the template but not in the device
Overriding device object	Objects that appear in red are device objects that potentially override a similar object in the template. The object was probably created or modified using other interfaces into SafeGuard, for example, CLI. to accept this change to the template, select the object and right-click and select **Add to Template**.

You can show or hide the legend by clicking on the ? icon as shown in *Figure 100*.

Figure 100 Show Device Hierarchy Legend



Show/Hide icon

Strike through objects denote changes observed on a template object. You can either accept or discard this change. To discard this change, select the changed object, right click, and select **Delete** to delete the selected object. To accept the changed object and add it to a template, select the object, right-click, then select the **Add to Template**.

NOTE: Alcatel-Lucent recommends that you do not perform the “Add to Template” action on Policy and Role objects.

To effectively apply all changes to a template, in the Config Management view, select a device and click on **Update Template**. This ensures that all device changes are moved to the template by creating or updating the objects in the template.

Recommended Device Management Workflow

You can create and share workflows across several devices. The following steps help you create a simple workflow that can be shared across devices:

1. Add the device from which you want to share the configuration. For more information on adding devices, see Adding a New Device.

2. Create a template from that device. To create a template, select the device and click **Create Template** in the Action Bar. For more information on creating templates, see *Creating a New Template*.

3. Add all other devices that should share this configuration.

4. Deploy the configuration to those devices. Select *Device Actions* > *Manage Configuration* > *Deploy Changes* to deploy the configuration. This step ensures that all devices are deployed with the same configuration.

5. If you want to make any changes across all devices, edit the template and make the required changes.

6. Redeploy the configuration to all associated devices.

It is recommended that you use OmniVista SafeGuard Manager to make any configuration changes. However, if you are using a template, you can perform the following steps to update the template with any device changes:

1. Synchronize the device. For more information on synchronizing devices, see *Synchronizing a Device*.

2. Visually inspect all changes that you want to accept. Discard the changes that are not needed by highlighting them and then right-click and select **Delete** to delete any unwanted changes.

3. Select the device and click **Update Template** in the Action Bar.

4. Deploy the changed configuration to all associated devices. Select *Device Actions* > *Manage Configuration* > *Deploy Changes* to deploy the configuration.

5. Save the running configuration. Select *Device Actions* > *Manage Configuration* > *Save Running Config* to save the running configuration.

chapter

6 Query and Reports

This section includes the following:

- *Query*
- *Reports*

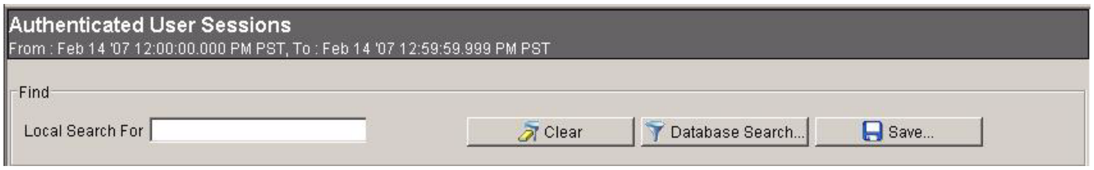
Query

Queries are available in OmniVista SafeGuard Manager for querying visualization data, reporting, and for creating bars in dashboard configuration. You can create additional queries using the Save Query Template. OmniVista SafeGuard Manager provides you with an easy way of using these queries in customized dashboards. You can create a bar then assign it to a module that was created prior to saving the new query.

To define a query template:

1 Select *View* > *Go To* > *Users* (or any other menu item, or click an icon from the Page Bar to get to a table view). In a table view, click the Find Find icon. A free-form text search field displays (*Figure 101*).

Figure 101 Free-Form Search Fields



Authenticated User Sessions
From : Feb 14 '07 12:00:00.000 PM PST, To : Feb 14 '07 12:59:59.999 PM PST

2 Click **Save**. The Save Query Template displays (*Figure 102*).

Figure 102Save Query Template - General Tab

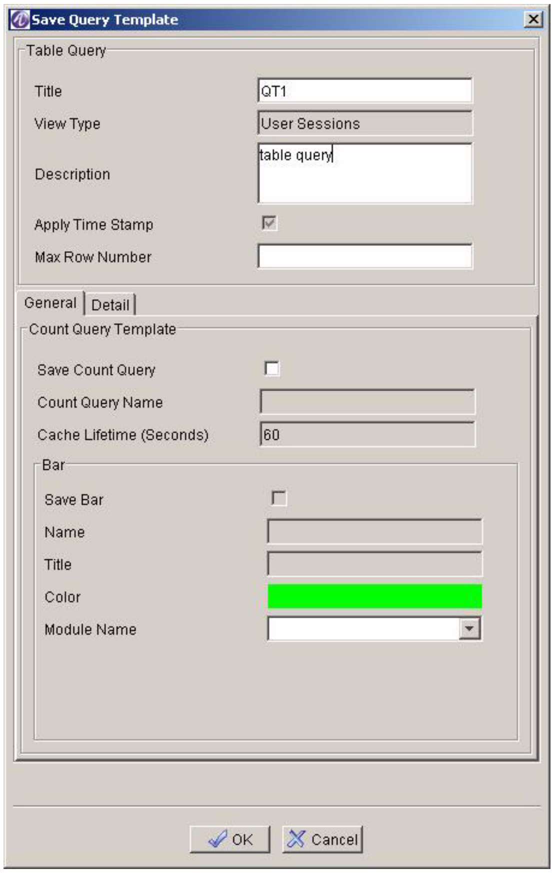


Table Query

Title: QT1

View Type: User Sessions

Description: table query

Apply Time Stamp: ☑

Max Row Number:

Count Query Template

Save Count Query: ☐

Count Query Name:

Cache Lifetime (Seconds): 60

Bar

Save Bar: ☐

Name:

Title:

Color: 🟩

Module Name:

3 Enter the template settings on the Save Query Template - General tab as follows:

Table 41 Save Query Template Settings

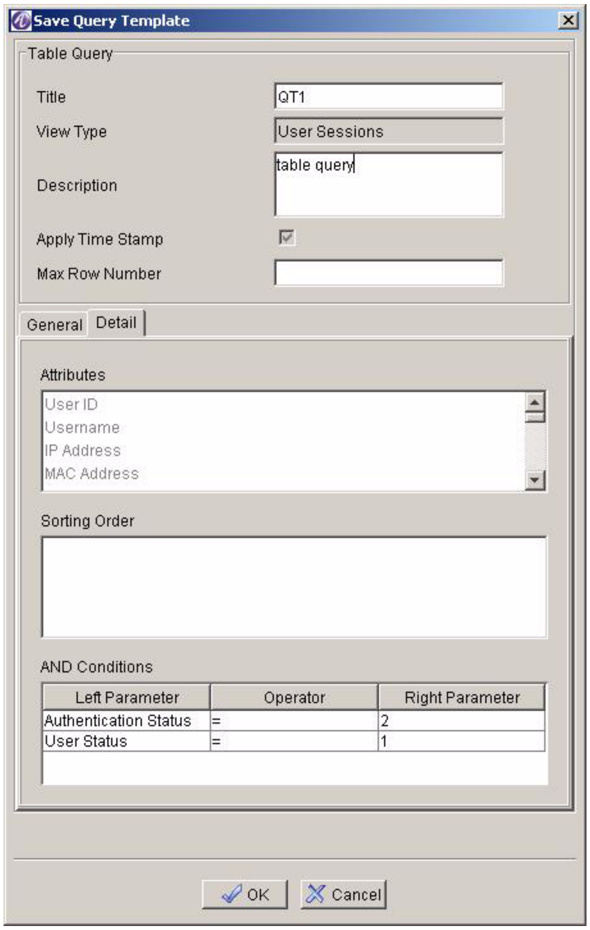
Setting Name	Description
Table Query:	
Title	Name by which the query template is to be saved.
Description	Brief description for the query template.
Apply Time Stamp	If this checkbox is selected, the time range filters you specify are applied. This checkbox is selected as a default. If you de-select this checkbox, the time filters are not applied and an existing timestamp is used. **Note:** When you execute this saved query, the time conditions in the navigation panel are applied or ignored depending on the selection you make on this screen.

Table 41 Save Query Template Settings

Setting Name	Description
Max Row Number	Specify the number of rows you want displayed as the query result.
Count Query Template:	
Save Count Query	Select the Count Query checkbox if you want the count query to be used in dashboard configuration to create a bar. The rest of the fields will be enabled only if this checkbox is selected.
Count Query Name	Name by which the count query is to be saved.
Cache Lifetime (Seconds)	Cache lifetime specified here is what is used as the refresh value when configuring dashboards. The default setting is 60 seconds.
Bar:	
Save Bar	Select the Save Bar checkbox if you want to save the bar information to the dashboard.
Name	Name for the bar.
Title	Title for the bar.
Color	Color for the bar.
Module Name	Module name to which the bar belongs.

4 Click the Details tab. The Save Query Template - Details displays (*Figure 103*).

Figure 103Save Query Template - Details Tab



Title	QT1
View Type	User Sessions
Description	table query
Apply Time Stamp	☑
Max Row Number	

Attributes

User ID
Username
IP Address
MAC Address

Sorting Order

AND Conditions

Left Parameter	Operator	Right Parameter
Authentication Status	=	2
User Status	=	1

5 The Details tab shows the template settings as follows:

Sorting Order	Sorting order that has been previously set using the Database Search button of the Find feature.
Conditions	Conditions that have been previously set using the Database Search button of the Find feature.

6 Click **OK** to save the template settings. The newly created Query template displays under the Custom Queries node in the Navigation Tree.

7 Refresh the tree node and the new query shows up under custom queries.

8 Select a query and right-click it to delete the selected query. A confirmation box will display to verify deletion.

NOTE: Monitoring users cannot create or delete queries. Queries are not available for Layer 7 events.

Reports

Reports use the existing Query mechanism to represent the high-level network health. Administrators can use reports to view the top destinations visited and then decode at the application layer. They can also create user-specific reports that indicate policy incidents, machine malware state, login and logout times, and the type and number of applications in use. The following tasks need to be performed before you can view or analyze a report:

- *Defining a Report*
- Scheduling a Report
- Generating a Report

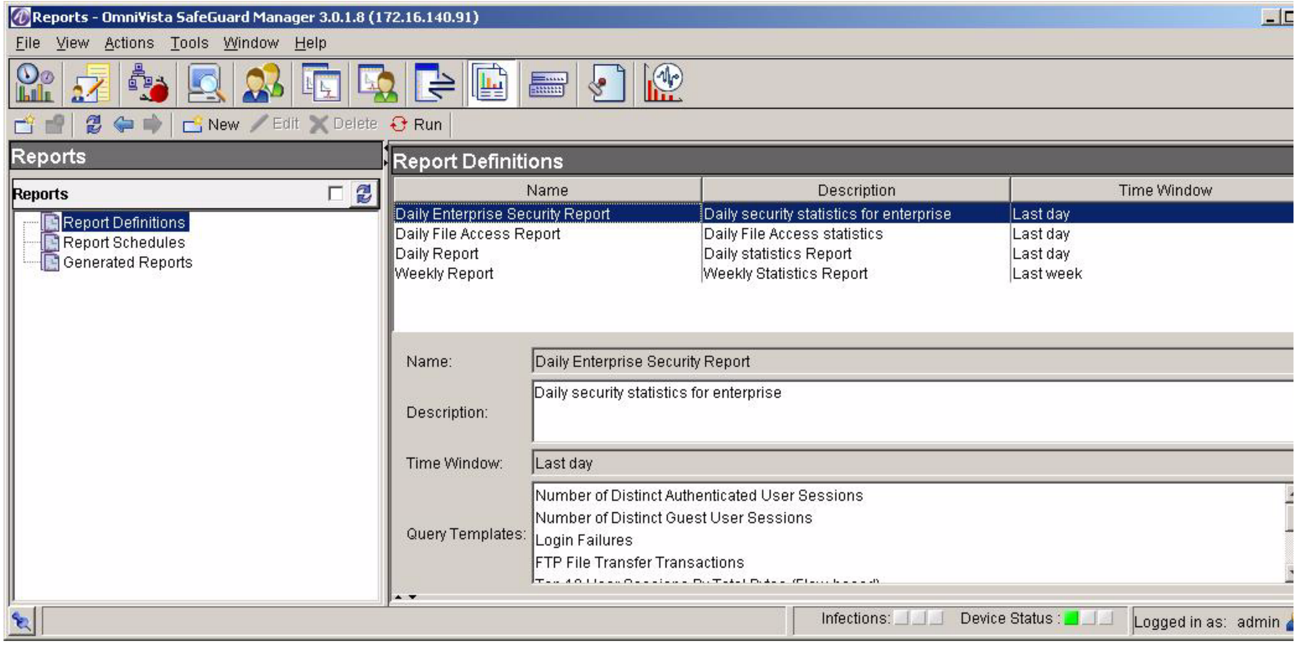
Defining a Report

Report definition is the building block for creating a report. Before you can schedule or view the output from any report, you have to define templates or create new definitions for a template that is to be used for creating a report.

To define or create a report:

1 Click the Reports icon from the Page Bar, or select the *View* > *Go To* > *Reports* (**Ctrl +9**) menu item. The Reporting screen displays (*Figure 104*).

Figure 104 Reports Screen



Name	Description	Time Window
Daily Enterprise Security Report	Daily security statistics for enterprise	Last day
Daily File Access Report	Daily File Access statistics	Last day
Daily Report	Daily statistics Report	Last day
Weekly Report	Weekly Statistics Report	Last week

Name: Daily Enterprise Security Report

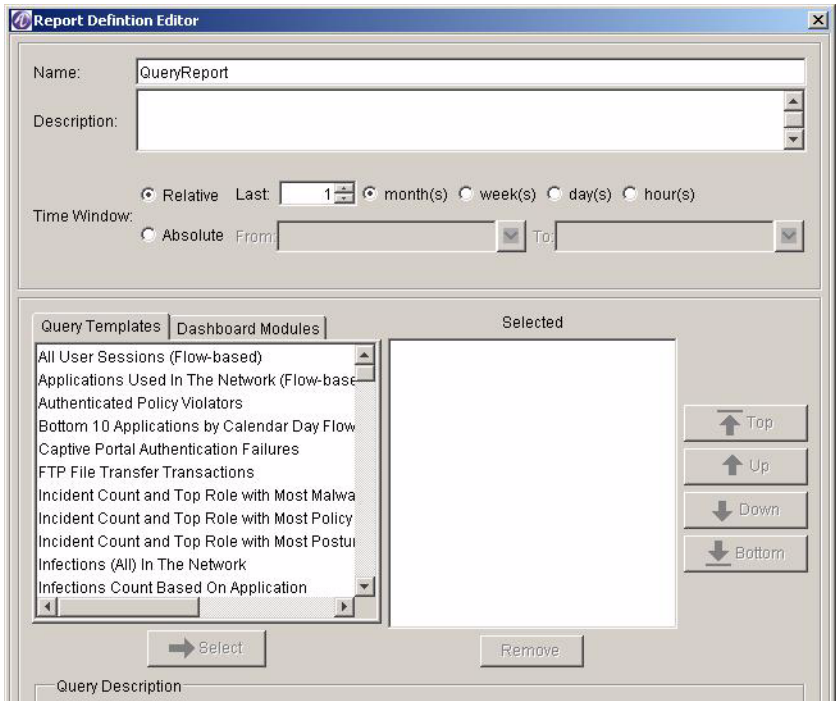
Description: Daily security statistics for enterprise

Time Window: Last day

Query Templates: Number of Distinct Authenticated User Sessions
Number of Distinct Guest User Sessions
Login Failures
FTP File Transfer Transactions

2 Select Report Definitions in the navigation tree and click **New** in the Action Bar. The Report Definition Editor displays (*Figure 105*).

Figure 105Report Definition Editor



Name: QueryReport

Description:

Time Window: ● Relative Last: 1 ● month(s) ○ week(s) ○ day(s) ○ hour(s)
○ Absolute From: To:

All User Sessions (Flow-based)
Applications Used In The Network (Flow-base
Authenticated Policy Violators
Bottom 10 Applications by Calendar Day Flow
Captive Portal Authentication Failures
FTP File Transfer Transactions
Incident Count and Top Role with Most Malwa
Incident Count and Top Role with Most Policy
Incident Count and Top Role with Most Postu
Infections (All) In The Network
Infections Count Based On Application

3 Enter the information as shown below:

Table 42 Report Definitions

Define	Description
Name	Specify a textual name for the report.
Description	Specify a description for the report you are creating.
Time Window	Select **Relative** to specify a relative time for the query: daily, hourly, weekly, or monthly. You can also select how many hours per day for which you want the reporting data. Select **Absolute** to enter a specific time. Use the dropdown lists in the **From** and **To** fields to enter a specific calendar date and time to be used as the start date and time and end date and time for the query.
Query Templates	The Query Templates tab shows a list of available queries. Highlight the query on which you want reporting to be done and click **Select** to add the query to the Selected box. When you select a query template and click **Select**, an Add Template to Report dialog box displays that allows you to configure **Time Filter** and **Active Status** on the report. Use the up/down arrows to select a Time Filter (Occurred During, First Occurred During, Last Occurred During). Configure the Active Status as Active, Inactive, or Active or Inactive. **Note:** Depending on the query you select, the choices for Time Filter might be different. After you have added all the queries you want in your report, you can arrange the order in which you want to view the data: **Top**: to move a query to the top of the list. **Up**: to move a query one level up. **Down**: to move a query one level down. **Bottom**: to move a query to the bottom of the list.
Dashboard Modules	The Dashboard Modules tab shows a list of all available predefined dashboard modules that can be included in a report. Select the module that you want to include and click Add. After you have added all the modules that you want in your report, you can adjust the placeholders for the module chart by using the **Top**, **Up**, **Down**, and **Bottom** buttons.
Query Description	Displays the description for the selected query.

4 Click **Apply**. The next time you run your scheduled or ad hoc report, this query definition is applied.

5 Click **Run** in the Action Bar to start the reporting process.

NOTE: Reports can be generated directly by clicking **Run** or can be scheduled by creating report schedules. The same report definition can be used in more than one schedule. Reports typically process a large set of data and can be slow.

To edit an existing report definition:

1 Click the Reports icon from the Page Bar, or select the *View* > *Go To* > *Reports* (Ctrl +9) menu item. The Reporting screen displays (*Figure 104*).

2 Select an existing report and click Edit in the Action Bar. The Report Definition Editor displays (*Figure 105*).

3 Change the attributes as necessary. For more information on report definition attributes, see *Defining a Report*.

4 Click **Apply**. The next time you run a report, your new definition will be applied.

Scheduling a Report

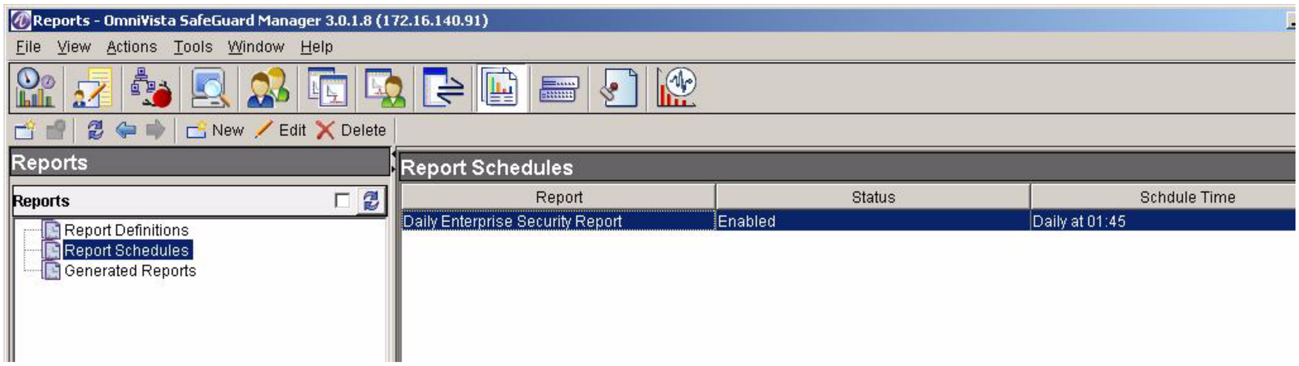
You can schedule a report either while setting definitions (see *Reports*), or you can modify or create new schedules using the Report Schedules Editor.

To schedule a report:

1 Click the Reports icon from the Page Bar, or select the *View* > *Go To* > *Reports* (Ctrl +9) menu item. The Reporting screen displays (*Figure 104*).

2 Select Report Schedules from the navigation tree in the left-hand side of the panel (*Figure 106*).

Figure 106 Report Schedules


Reports - OmniVista SafeGuard Manager 3.0.1.8 (172.16.140.91)
File View Actions Tools Window Help
New
Edit
Delete
Reports
Reports
Report Definitions
Report Schedules
Generated Reports

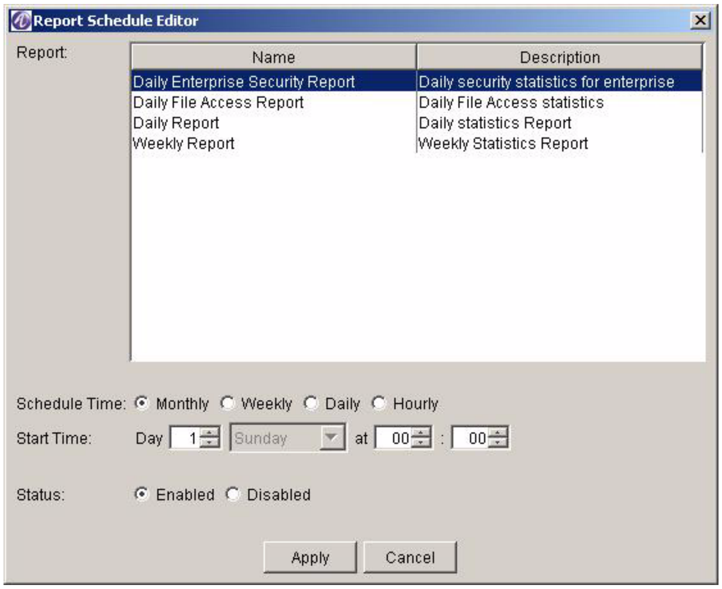
Report Schedules

Report	Status	Schdule Time
Daily Enterprise Security Report	Enabled	Daily at 01:45

3 Select the report for which you want to set the schedule.

4 Click **New** to create a new schedule or **Edit** to modify an existing schedule. The Report Schedule Editor displays (*Figure 107*).

Figure 107Report Schedule Editor



Report:

Name	Description
Daily Enterprise Security Report	Daily security statistics for enterprise
Daily File Access Report	Daily File Access statistics
Daily Report	Daily statistics Report
Weekly Report	Weekly Statistics Report

Schedule Time: ● Monthly ○ Weekly ○ Daily ○ Hourly

Start Time: Day 1 Sunday at 00 : 00

Status: ● Enabled ○ Disabled

5 Select the schedule frequency: Monthly, Weekly, Daily, or Hourly.

6 Specify the start time by using the up and down arrows.

7 Select Enabled or Disabled for the status.

8 Click **Apply** to save the schedule changes. The next time you run a report, the new schedule is used.

Generating a Report

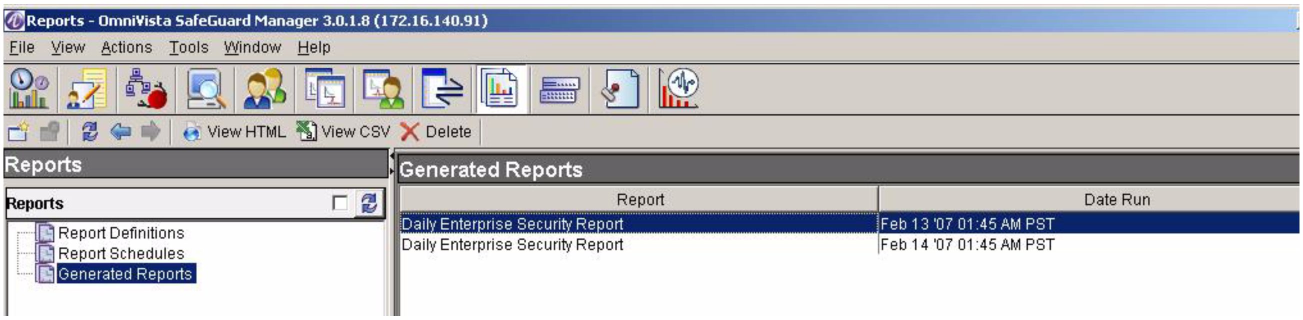
After you have scheduled and run a report, you can view a report in either an HTML or a CSV (Comma Separated Value) format.

To view a report:

1 Click the Reports icon from the Page Bar, or select the *View* > *Go To* > *Reports* (Ctrl +9) menu item. The Reporting screen displays (*Figure 104*).

1 Select Generated Reports from the navigation tree in the left-hand side of the panel (*Figure 108*).

Figure 108 Generated Reports

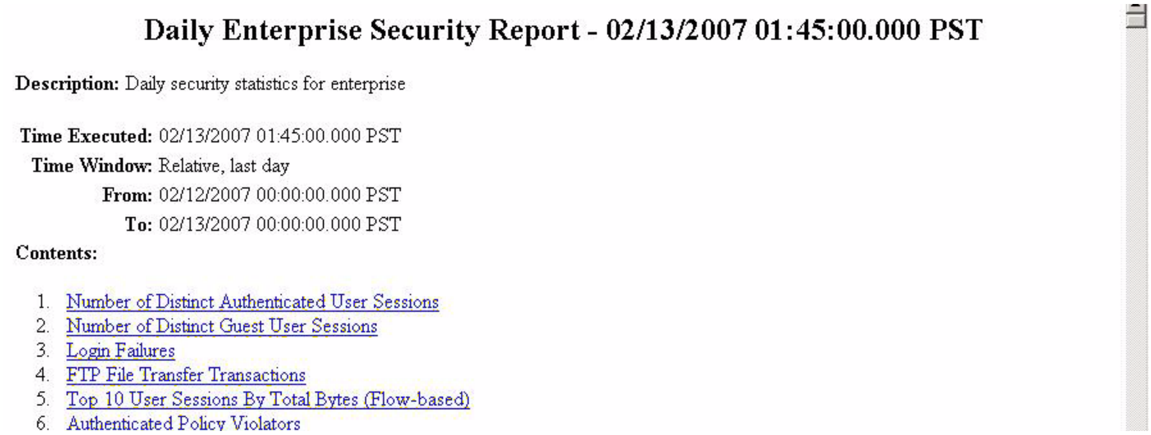


Report	Date Run
Daily Enterprise Security Report	Feb 13 '07 01:45 AM PST
Daily Enterprise Security Report	Feb 14 '07 01:45 AM PST

2 Select the report you want to view.

3 Select View HTML from the Action Bar to view the report in HTML format.

Figure 109 Report in HTML Format



Daily Enterprise Security Report - 02/13/2007 01:45:00.000 PST

Description: Daily security statistics for enterprise

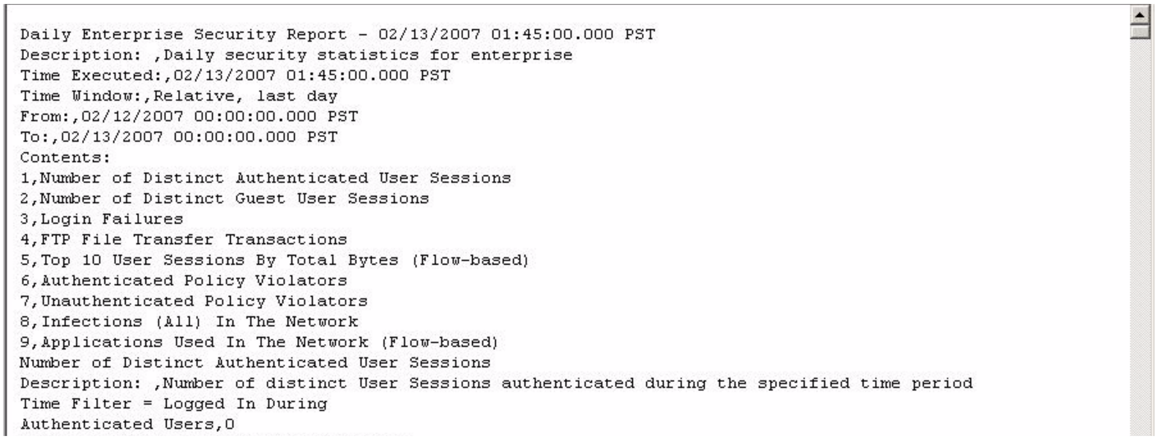
Time Executed: 02/13/2007 01:45:00.000 PST
Time Window: Relative, last day
From: 02/12/2007 00:00:00.000 PST
To: 02/13/2007 00:00:00.000 PST

Contents:

1. Number of Distinct Authenticated User Sessions
2. Number of Distinct Guest User Sessions
3. Login Failures
4. FTP File Transfer Transactions
5. Top 10 User Sessions By Total Bytes (Flow-based)
6. Authenticated Policy Violators

4 Select View CSV from the Action Bar to view the report in CSV format.

Figure 110 Report in CSV Format



```
Daily Enterprise Security Report - 02/13/2007 01:45:00.000 PST
Description: ,Daily security statistics for enterprise
Time Executed:,02/13/2007 01:45:00.000 PST
Time Window:,Relative, last day
From:,02/12/2007 00:00:00.000 PST
To:,02/13/2007 00:00:00.000 PST
Contents:
1,Number of Distinct Authenticated User Sessions
2,Number of Distinct Guest User Sessions
3,Login Failures
4,FTP File Transfer Transactions
5,Top 10 User Sessions By Total Bytes (Flow-based)
6,Authenticated Policy Violators
7,Unauthenticated Policy Violators
8,Infections (All) In The Network
9,Applications Used In The Network (Flow-based)
Number of Distinct Authenticated User Sessions
Description: ,Number of distinct User Sessions authenticated during the specified time period
Time Filter = Logged In During
Authenticated Users,0
```

NOTE: When you generate a report either through a schedule or interactively, if **Enable Report Delivery** is checked in the Mailer tab of Server Settings, then an email is sent. This email can be in a zip format if any graphs are included in the report definition. You have to open the zip file and select View HTML to view the report. For more information on mailer settings, see *Mailing Malware and Report Notifications*.

chapter

7 Managing the Server

This section includes the following:

- *User Authentication*
- *User Accounts*
- *File Repository*
- *Client Settings*
- Server Settings
- *General*

User Authentication

An integral part of any security solution is access control, which is the way you control user access into the network and what services users are allowed to use after they have access. Authentication, Authorization, and Accounting (AAA) is an industry accepted framework that implements access control. This section focuses on the authentication component and how an administrator can set user authentication using OmniVista SafeGuard Manager.

SafeGuard OS has a local authentication mechanism built-in to the authentication manager. You can use SafeGuard OS' authentication in stand-alone mode or use it with external authentication servers such as RADIUS. The local system also serves as a local mechanism to derive the role for a given user.

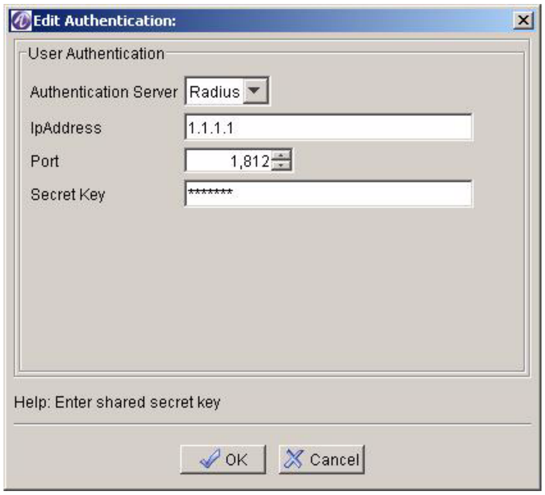
The database contains an entry for each user, which includes the user name, password, and the role being assigned to the user. The user role can be derived based on the rule map configured for the authentication protocol.

In addition to local database authentication, OmniVista SafeGuard Manager users can be authenticated using an external RADIUS server. The OmniVista SafeGuard Manager administrator logs in for the first time and configures OmniVista SafeGuard Manager to a RADIUS server. The administrator sets up user accounts requiring all subsequent log ins by all users to be authenticated by RADIUS.

To change user authentication to an external authentication server (RADIUS):

1 Select *Tools* > *OmniVista SafeGuard Manager Users* > *User Authentication*. The Edit Authentication dialog box displays (*Figure 111*).

Figure 111 Edit Authentication



Edit Authentication:

User Authentication

Authentication Server: Radius

IpAddress: 1.1.1.1

Port: 1,812

Secret Key: *******

Help: Enter shared secret key

2 By default the users are authenticated locally. Select RADIUS from the Authentication Server dropdown list.

3 Enter the user configurable fields as follows:

Table 43 Edit User Authentication Attributes

Attribute	Description
Authentication Server	Select RADIUS to apply an external authentication server.
IpAddress	Enter the IP address on which the communication to the RADIUS server can be established.
Port	Enter the port number on which the communication to the RADIUS server can be established.
Secret Key	Enter the shared secret key.

NOTE: Whenever, the authentication method is changed from “Local” to “RADIUS,” all logged in clients are logged out.

4 Click **OK** to apply the new settings. This ensures that further authentication is performed by the RADIUS server.

Authentication Guidelines

- The default “admin” account is always authenticated locally.
- When a user logs in, and if RADIUS is the authentication type, then OmniVista SafeGuard Manager checks to ensure that the user exists in the local database and validates the password using RADIUS. This means that the administrator must have already created a user account locally for the user to be authenticated through RADIUS.
- As part of creating or modifying a user appropriate roles are selected that are only known to OmniVista SafeGuard Manager.
- In the Add User/Modify User dialog box, the password and confirm password fields are not displayed if the authentication type is selected as “RADIUS” when setting the authentication for that particular user. The only exception to this rule is when you modify the default “admin” account because the default admin account is always authenticated locally.

- If you choose to change the authentication method from “RADIUS” to “Local,” the password has to be set explicitly for all users before the users can log in.

NOTE: Whenever, the authentication method is changed from “RADIUS” to “Local,” all user accounts, except the admin account, are put in a “*disabled*” state. These accounts will stay in a disabled state unless the administrator resets the passwords for these accounts. For more information on enabling accounts, see *Modifying Your Password*.

User Accounts

OmniVista SafeGuard Manager users can be one of the following types:

- Monitor—users designated with the role of monitors can only view data; they are not allowed to change any data or execute any commands. The Monitor role cannot create, modify, or add users or change a user’s role. Action buttons are disabled for this role.
- Configurator—users designated with the role of configurators can view data as well as change data and also execute commands. However, they cannot create, modify, or add users. They also cannot change a user’s role.
- Administrator—users designated with the role of administrators can view and edit data, as well as execute commands. They can create, modify, and add users and also change a user’s role, if needed.

  There are two types of administrator login settings: *Standard* or *Dual-admin*. The Standard administrator login requires a single password and login. The Dual-admin or 4-Eye admin cannot log in to the client on their own but can enable another administrator role to enter the 4-Eye mode. For more information on the dual-admin role, see *Enabling Dual-Admin or 4-Eye Mode*.

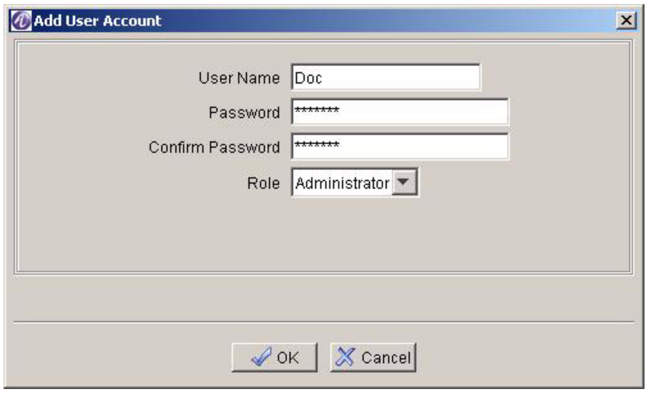
Adding a New User

To add a new user:

1 Select *Tools > OmniVista SafeGuard Manager Users > User Accounts...* The Account Management window displays.

2 Click **Add** on the Account Management window to add a new user. The Add User Account dialog box displays (*Figure 112*).

Figure 112 Add User Account



User Name: Doc
Password: ********
Confirm Password: ********
Role: Administrator

3 Enter a name in the User Name field.

4 Enter a password for the user in the Password field and then confirm it in the Confirm Password field.

5 From the dropdown list in the Role field, select one of the following:

Role Type	Description
Monitor	This role has read-only privileges.
Configurator	This role has read-write privileges but cannot change a user's role.
Administrator	This role has all read-write privileges and can also change a user's role. If you select this role type, then also select whether it is a standard administration or dual-admin login setting.
4-Eye Admin	This role can view the following information: username, computer name, application details, and reports.

6 Click **OK**. The new user role is added.

Enabling Dual-Admin or 4-Eye Mode

The dual-administrator or 4-Eye administrator role cannot log into the client on their own. However, if another user with a different administrator role logs into the client, then the 4-Eye admin role is required to enable an administrator role to enter the 4-Eye admin mode. Only in this mode, an administrator can view the following data:

- Username
- Computer name
- Application details
- Reports

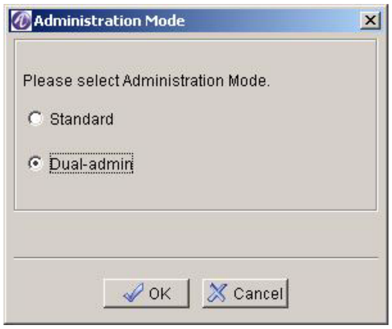
To enable 4-Eye mode:

1 Select *Tools* > *OmniVista SafeGuard Manager Users* > *User Accounts*.

2 Add a new user and select the role as “4-Eye Admin.” For more information on adding a user, see *Adding a New User*.

3 Select *Tools* > *OmniVista SafeGuard Manager Users* > *Administration Mode*.

Figure 113 Administration Mode



Administration Mode

Please select Administration Mode.

○ Standard

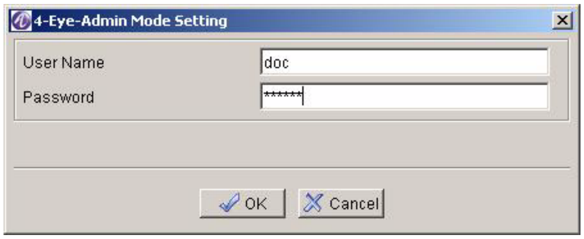
● Dual-admin

4 Select **Dual-admin**. This creates the dual-admin/4-Eye administrator role.

NOTE: The Enabled checkbox shows the status of the user account. For all user accounts, except admin, when an authentication method is changed from RADIUS to local, the account is set to “*disabled*”. The account remains in a disabled state until the administrator resets the password for the account.

5 Select *Tools* > *OmniVista SafeGuard Manager Users* > *Enter 4-Eye-Admin Mode* to enter this mode. The 4-Eye-Admin Mode Settings dialog box displays (*Figure 114*).

Figure 114 4-Eye-Admin Mode Settings



User Name: doc

Password: ******

6 Enter the user name and password for the 4-Eye administrator role to log in.

7 Click **OK** to log in. After you log in, you can view the hidden information.

File Repository

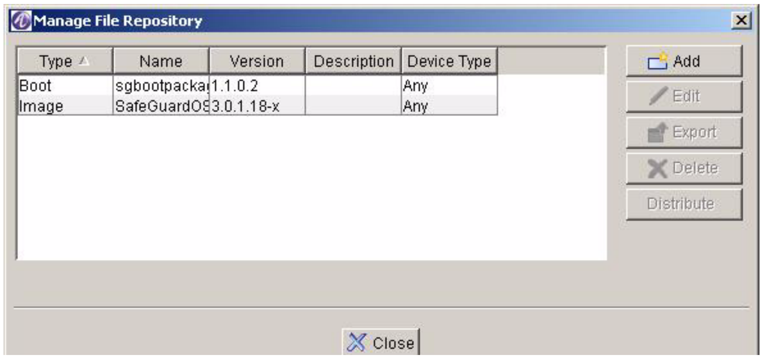
File repository allows you to manage device files in an OmniVista SafeGuard Manager repository. The following file types can be managed:

- Software image
- Boot Loader
- ICS portal configuration
- ICS policy configuration
- Captive portal web page
- Other

To manage device files:

1 Select *Tools* > *File Repository*. The Manage File Repository screen displays (*Figure 115*).

Figure 115 Manage File Repository



Type	Name	Version	Description	Device Type
Boot	sgbootpacka	1.1.0.2		Any
Image	SafeGuardOS	3.0.1.18-x		Any

2 The Manage File Repository screen displays the following information:

Table 44 Manage File Repository Columns

Column Name	Description
Type	Type of file in the repository.
Name	Name of the file. When the file type is image, the file name is automatically translated to <version>.img. For example “SafeGuardOS-2.2.1.5-cp.img. The translation is required to avoid duplication of images.
Version	Shows the version of the image on the device. Applicable only to “image” file type.
Description	Brief description for the file. This is added when the file is added to the repository.
Device Type	Device type to which the file is applicable. Possible values are: ■ Controller ■ Switch ■ Any

3 Select an existing file and click **Edit** to update or change file attributes.

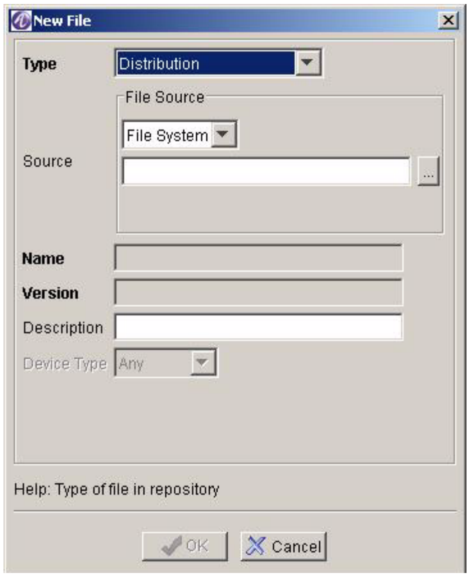
4 Click **Export** to export an existing file.

5 Select an existing file and click **Delete** to delete the file.

6 Select an existing file and click **Distribute** to distribute the selected file to a device.

7 Click **Add** to add a new file. The New File screen displays (*Figure 116*).

Figure 116 New File



8 Enter the required information as follows:

Table 45 New File Attributes

Attribute Name	Description
Image	Select the type of file you want to add to the repository using the dropdown list. Following file types are available: ■ Image ■ Boot loader ■ ICS portal configuration ■ ICS policy configuration ■ Captive portal web page ■ Other
File Source	Shows if the file is available in the network files system.
Source	Click the ellipses (...) next to the text box to browse for a file.
Description	Brief description of the file.

9 Click **OK**. The selected file is added to the repository and displays in the Manage File Repository screen.

NOTE: You can distribute these files to one or many devices at the same time. For more information, see *Distribute File*.

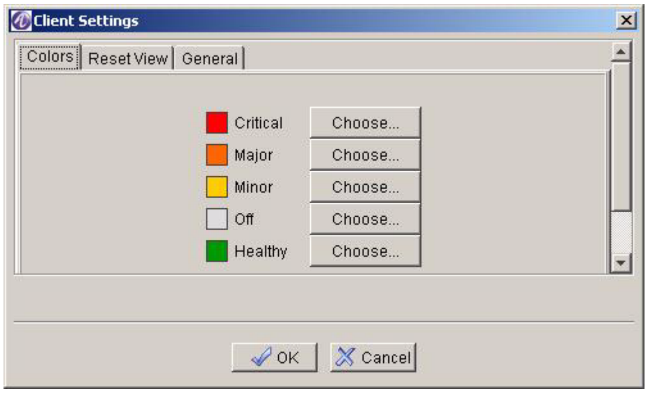
Client Settings

OmniVista SafeGuard Manager allows you to choose and set the order in which you view the columns in a given table view. These settings are remembered in Windows for each user and are applied when you visit the same table again. You can also change the color display for any alarms.

To change the client settings:

1 Select *Tools* > *Client Settings*. The Client Settings dialog box displays (*Figure 117*).

Figure 117 Client Settings - Colors



🟥 Critical Choose...
🟧 Major Choose...
🟨 Minor Choose...
□ Off Choose...
🟩 Healthy Choose...

2 Select the Color tab to change the color scheme.

3 Select the Reset View tab to reset the column order to its previous view.

4 Click **OK** to apply the changes.

Server Settings

The following server settings can be performed from the OmniVista SafeGuard Manager client:

- *Setting Visualization Filters*
- *Exporting the Database*
- *Backing Up the Database*
- *Restoring the Database*
- *Mailing Malware and Report Notifications*

Setting Visualization Filters

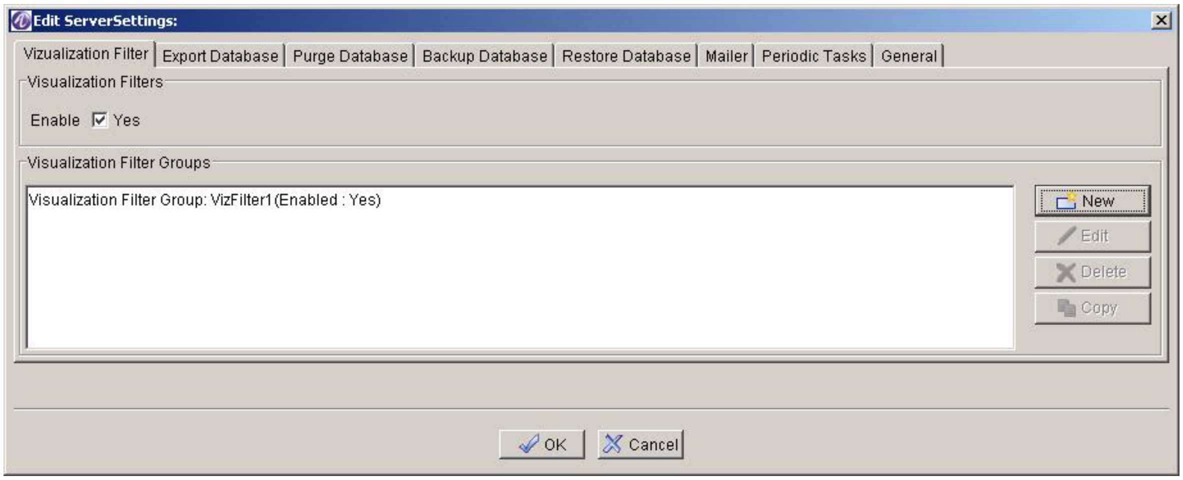
OmniVista SafeGuard Manager allows you to set up visualization filters. Filters allow you to selectively view events based on VLAN ID, application type, or user role. Once a filter is applied and you enable the filter, all the flows matching the filter conditions are either excluded or included as specified in the filter.

To configure a visualization filter:

1 Select *Tools* > *Server Settings*. The Edit Server Settings screen displays (*Figure 121*).

2 Select the Visualization Filter tab (*Figure 118*).

Figure 118 Edit Server Settings - Visualization Filter



Visualization Filters

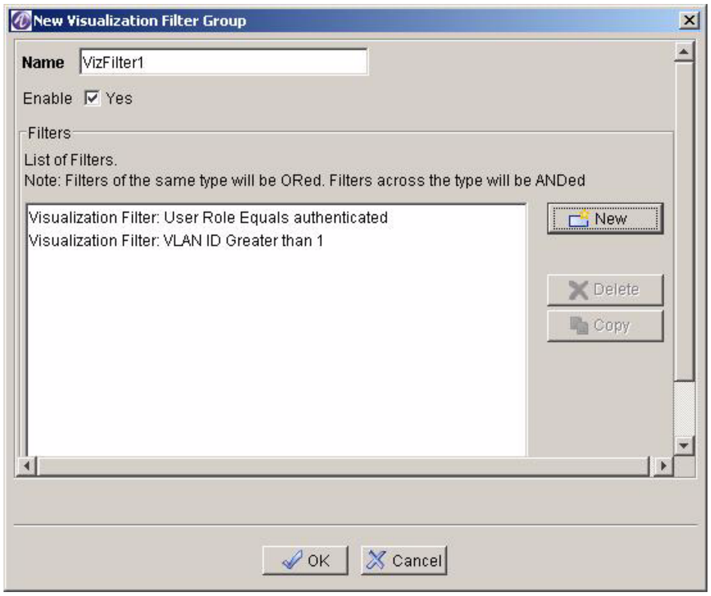
Enable ☑ Yes

Visualization Filter Groups

Visualization Filter Group: VizFilter1 (Enabled : Yes)

3 Click **New** to add a new visualization filter group. The New Visualization Filter Group dialog box displays (*Figure 119*).

Figure 119 New Visualization Filter Group



Name VizFilter1

Enable ☑ Yes

Filters

List of Filters.

Note: Filters of the same type will be ORed. Filters across the type will be ANDed

Visualization Filter: User Role Equals authenticated

Visualization Filter: VLAN ID Greater than 1

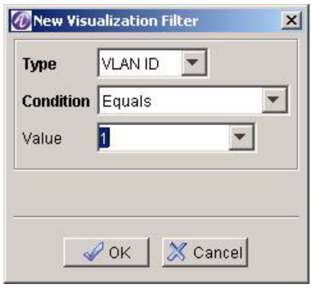
4 Specify a name for the new visualization filter group.

NOTE: A filter group can contain one or more filter depending on the filter type: VLAN, Application, or User Role. A filter group name is unique and two filter groups cannot have the same name. Filters apply only to Layer 7 and flows data.

5 Select the Enable checkbox if you want the visualization filters to be enabled. If this checkbox is selected, any flows matching the filters will be excluded or included depending on how the filter is set up.

6 Click **New**. The New Visualization Filter dialog box displays (*Figure 120*).

Figure 120 New Visualization Filter



Type VLAN ID

Condition Equals

Value 1

7 Specify the filter information as shown below:

Table 46 New Visualization Filter Attributes

Attribute	Description

Type	From the dropdown list, select whether the visualization filter is to be based on VLAN ID, Application, or User Role.
	Note: Filters of the same type have the OR condition applied, whereas filters across different types have the AND condition applied. For example, if FilterGroup1 is created with filters:
	■ VLANID In Range 2-5
	■ Application like HTTP%
	The above filters are translated to:
	`( ((VLANID >=2) AND (VLANID <=5)) AND`
	`((application type.startsWith(‘HTTP’)>0)) )`
	The flows satisfying this condition will be dropped.

Condition	From the dropdown list select a condition that excludes or includes the values that you specify in the value field.
Value	Specify a value to go with the entry in the condition field.

8 Click **OK**. The new filter displays in the Visualization Filter Group. You can specify multiple filters using the same process.

9 To delete a filter, select the filter and click **Delete**.

Exporting the Database

The Database Export feature allows you to export Visualization data that includes user details, user application usage details, flow data, Layer 7 data, devices and corresponding ports details. The following configuration data is not exported:

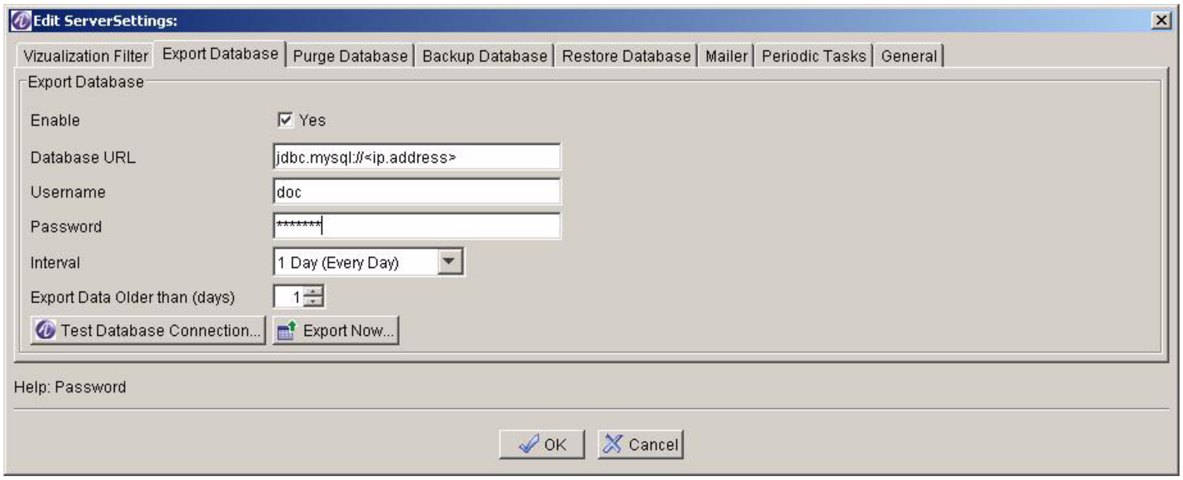
- Policy template objects
- Report definitions and their schedules
- OmniVista SafeGuard Manager server settings (Purge, Export, Backup, Mailer)
- Custom queries
- Custom modules, bars, and layouts in dashboards

You can export the visualization data and then use your own tools to analyze or display the data.

To export the database:

1. Select *Tools* > *Server Settings*. The Edit Server Settings screen displays.
2. Select the Export Database tab (*Figure 121*).

Figure 121 Edit Server Settings - Export Database



Export Database

Enable ☑ Yes

Database URL jdbc.mysql://<ip.address>

Username doc

Password *******

Interval 1 Day (Every Day)

Export Data Older than (days) 1

Help: Password

3. In the Export Database tab, specify the settings as follows:

Table 47 Export Database Settings

Setting Name	Description
Enable	Select the Enable checkbox to periodically export the database at the specified interval: daily, weekly, and so on.

Table 47   Export Database Settings

Setting Name	Description
Database URL	URL for the database to which you want to export.
Username	Name for the user authenticated to perform the database export.
Password	Password associated with the username.
Interval	Use the dropdown list to specify a time interval for the database export.
Export Data Older than (days)	Use the up/down arrows to specify (number of days) if you want to export current data or data older than the specified days.

4 Click **Test DB Connection** to verify database connectivity.

5 Click **Export Now** to export the database immediately. The bottom-half of the screen (Last Action Status) shows the status of the last export or if you used **Export Now**, the status of the current export.

6 Click **OK** to apply the settings.

Purging the Database

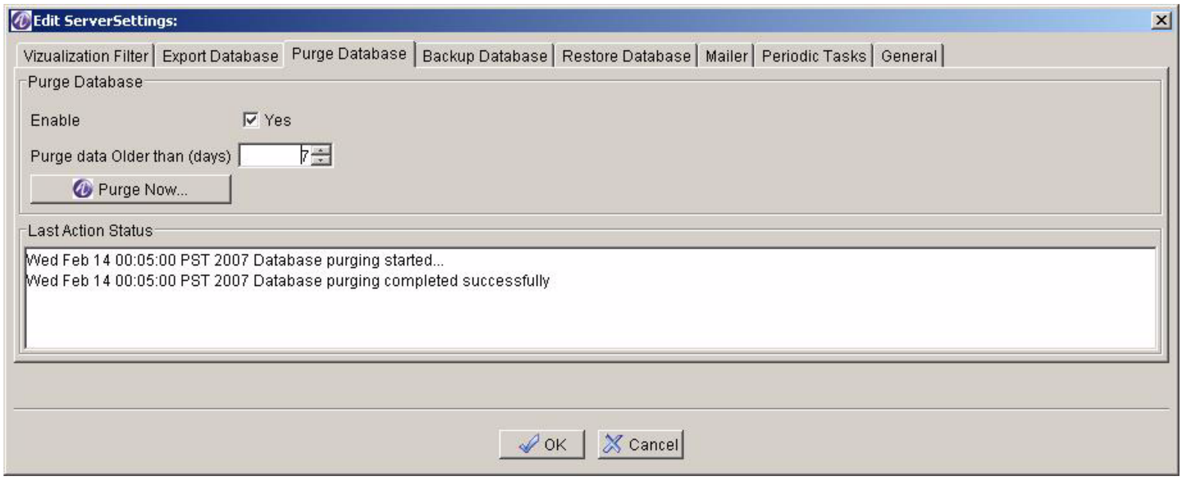
Database purge performs a cleanup of user data, application usage details, flow and Layer 7 data.

To cleanup or purge the database:

1 Select *Tools* > *Server Settings*. The Edit Server Settings screen displays.

2 Select the Purge Database tab (*Figure 122*).

Figure 122 Edit Server Settings - Purge Database



Enable ☑ Yes

Purge data Older than (days) 7

```
Wed Feb 14 00:05:00 PST 2007 Database purging started...
Wed Feb 14 00:05:00 PST 2007 Database purging completed successfully
```

3 Select the Enable checkbox to enable the database purge. The checkbox is selected as the default.

4 Use the Purge Data Older than (days) up/down arrows to specify (in number of days) the data that you want to purge. Range is 1–30 days and the default is 14 days.

5 Click **OK** to enable the purging process. The bottom half of the screen (Last Action Status) shows the status of the last purge.

Backing Up the Database

The Database Backup feature allows you to backup Visualization data that includes user details, user application usage details, flow data, Layer 7 data, devices and corresponding ports details and any generated reports.

You may want to back up your database periodically to protect its integrity or for historical purposes. Data can be backed up to the OmniVista SafeGuard Manager server or an outside server as long as it is accessible to the OmniVista SafeGuard Manager server.

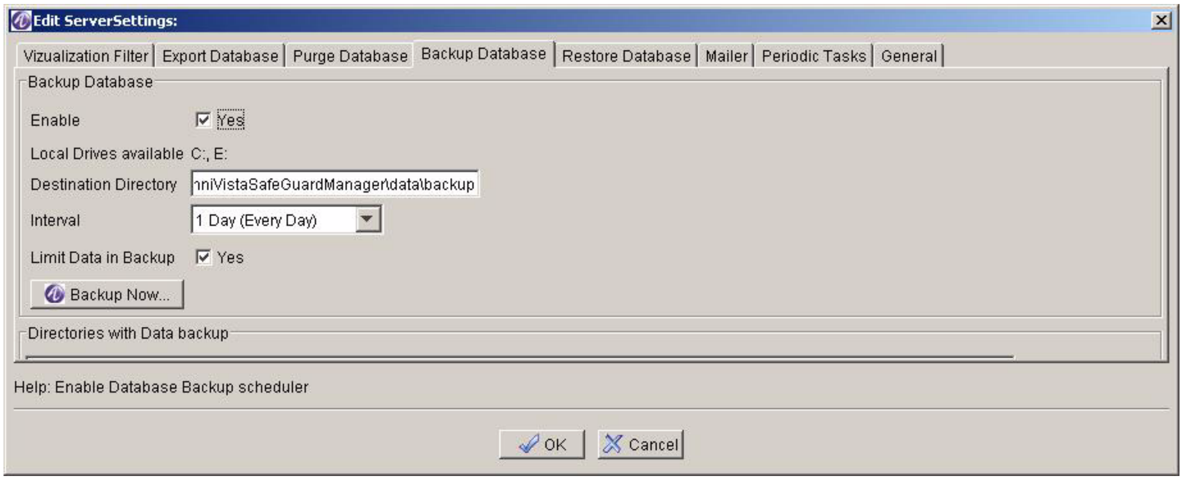
Database backup is performed to save a known good state of the system in case of disaster recovery.

To back up the database:

1 Select *Tools* > *Server Settings*. The Edit Server Settings screen displays.

2 Select the Backup Database tab (*Figure 123*).

Figure 123 Edit Server Settings - Backup Database



Edit ServerSettings:

Backup Database

Enable ☑ Yes

Local Drives available C:, E:

Destination Directory niVistaSafeGuardManager\data\backup

Interval 1 Day (Every Day)

Limit Data in Backup ☑ Yes

Directories with Data backup

Help: Enable Database Backup scheduler

3 Specify the settings as follows:

Table 48 Backup Database Settings

Setting Name	Description
Enable	Select the Enable checkbox to enable backups. The checkbox is not selected as a default.
Destination Directory	Specify the location of the directory on the server where the backed up files are to be stored.
Interval	Use the up/down arrows to specify whether data is to be backed up daily, weekly, and so forth.

4 Click **Backup Now** to back up the database immediately. The bottom-half of the screen (Last Action Status) shows the status of the last backup or if you used **Backup Now**, the status of the current backup.

5 Click **OK** to apply the settings.

Deleting backed up directories

OmniVista SafeGuard Manager server keeps track of the backup destination directories. You can either delete these directories or use them for restoring the database.

To delete backed up directories:

1 *Select Tools* > *Server Settings*. The Edit Server Settings screen displays (*Figure 121*).

2 Select the Backup Database tab (*Figure 123*).

3 Select the backed up directory that you want to delete.

4 Click **Delete**. The selected directories are deleted.

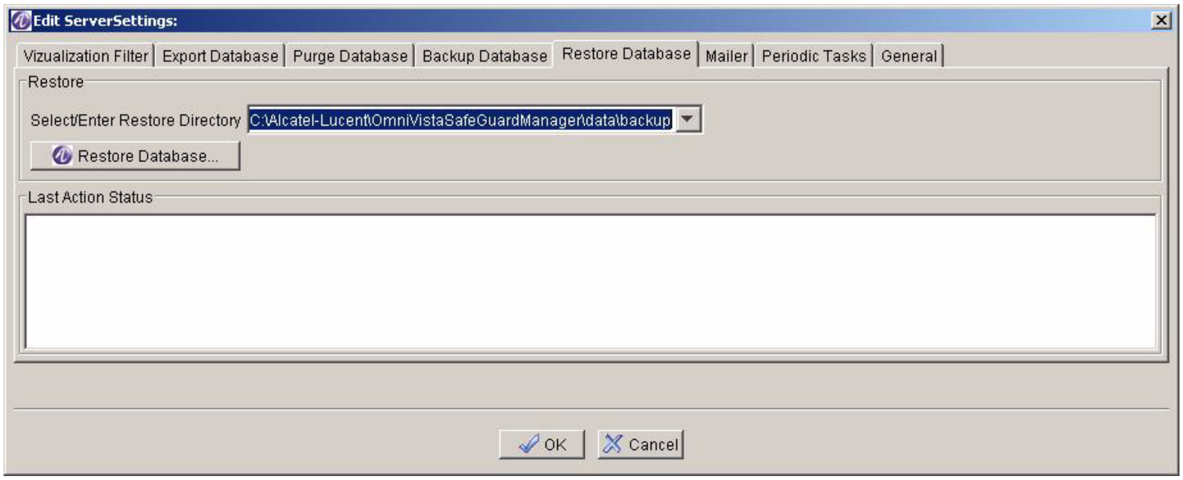
Restoring the Database

You can restore data from a previously backed up directory.

To restore the database:

1. Select *Tools* > *Server Settings*. The Edit Server Settings screen displays.
2. Select the Restore Database tab (*Figure 124*).

Figure 124 Edit Server Settings - Restore Database



Select/Enter Restore Directory C:\Alcatel-Lucent\OmniVistaSafeGuardManager\data\backup

3. From the Select/Enter Restore Directory dropdown list, select an existing backup directory or enter a new directory.
4. Click **Restore Database** to begin restoring data from the specified backup directory.

NOTE: OmniVista SafeGuard Manager client will lose connection to the OmniVista SafeGuard Manager server while the server is restarted and the data is restored from the specified directory. After you have reconnected to the client, the restore status will display in the Last Action Status section of the Restore Database screen.

Mailing Malware and Report Notifications

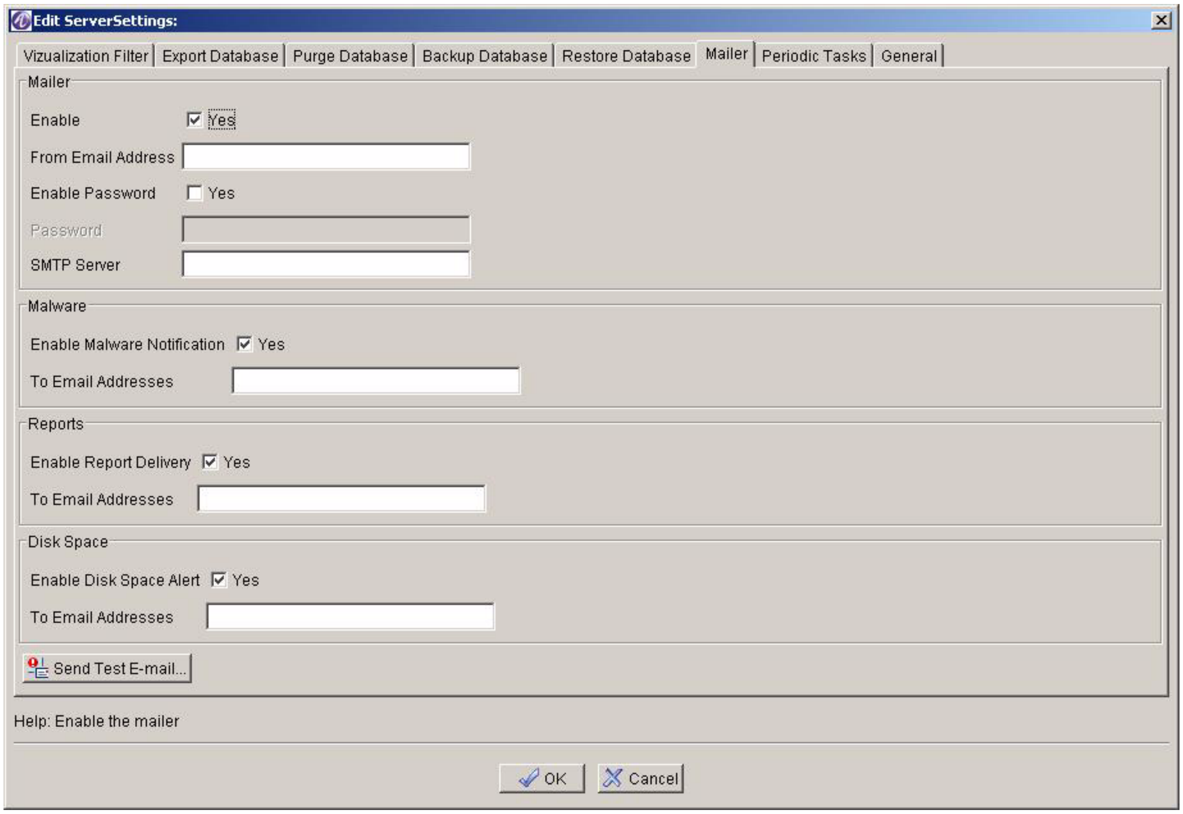
The OmniVista SafeGuard Manager server has emailing capabilities that allow the administrator to set up the mailer such that automatic email notifications are sent to a specified user/administrator. The following two types of data events automatically trigger an email notification:

- when malware incidents are detected
- when reports are generated

To set up the mailer:

1. Select *Tools* > *Server Settings*. The Edit Server Settings screen displays.
2. Select the Mailer tab (*Figure 125*).

Figure 125 Edit Server Settings - Mailer



Mailer

Enable ☑ Yes

From Email Address

Enable Password ☐ Yes

Password

SMTP Server

Malware

Enable Malware Notification ☑ Yes

To Email Addresses

Reports

Enable Report Delivery ☑ Yes

To Email Addresses

Disk Space

Enable Disk Space Alert ☑ Yes

To Email Addresses

Help: Enable the mailer

3 Specify the settings as follows:

Table 49 Mailer Settings

Setting Name	Description
Mailer:	
Enable	Select the Enable checkbox to make sure that the mailer is enabled.
From Email Address	Email address of the server administrator.
SMTP Server	URL for the SMTP server.
Malware:	
Enable Malware Notification	Select the Enable Malware Notification checkbox if you want to send automatic email notifications upon malware detection.
To Email Addresses	Specify the comma separated email addresses for the recipients of the email notifying them of malware incidents.
Reports:	
Enable Report Delivery	Select the Enable Report Delivery checkbox if you want to send automatic email notifications upon report generation.
To Email Addresses	Specify the comma separated email addresses for the recipients of the email notifying them of report generation.

4 Click **Send Test E-mail** if you want to verify that the email address and the SMTP server names are accurate.

5 Click **OK** to apply the settings.

NOTE: Once the mailer is set up, email notifications upon malware detection and report generation are delivered directly to the email addresses specified.

Periodic Tasks

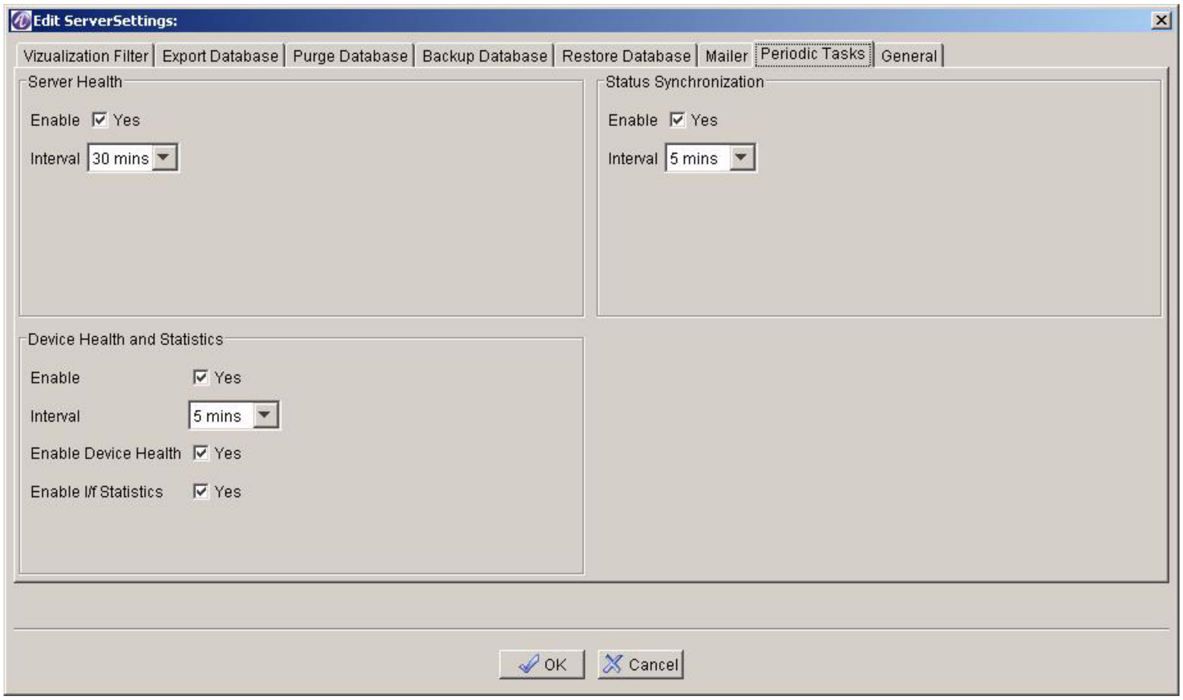
OmniVista SafeGuard Manager allows you to configure device health statistics collection interval and enable or disable statistics data collection.

To enable statistics data collection:

1 Select *Tools* > *Server Settings*. The Edit Server Settings screen displays.

2 Select the Periodic Tasks tab (*Figure 126*).

Figure 126 Periodic Tasks



Server Health

Enable ☑ Yes

Interval 30 mins

Status Synchronization

Enable ☑ Yes

Interval 5 mins

Device Health and Statistics

Enable ☑ Yes

Interval 5 mins

Enable Device Health ☑ Yes

Enable I/f Statistics ☑ Yes

3 **Server Health:** Select the Enable checkbox to activate collection of statistics and specify an interval in minutes when data is to be collected.

4 **Status Synchronization**: Select the Enable checkbox to activate status synchronization and specify an interval in minutes when status is to be synchronized.

5 **Device Health**: Select the Enable checkbox to activate collection of device health data and select Device Health and Device I/F Statistics checkboxes to activate collection of device health and interface statistics. Specify the collection interval (in minutes) for data collection using the Device Health Statistics Collection Interval dropdown list. Valid values are: 5, 10, 15, 30, or 60 minutes.

6 Click **OK** to apply the settings.

NOTE: Statistics are collected only for active devices. If a device is deleted, all associated statistics are deleted from the device health table. For more information on viewing device health and statistics, see *Device Health*.

General

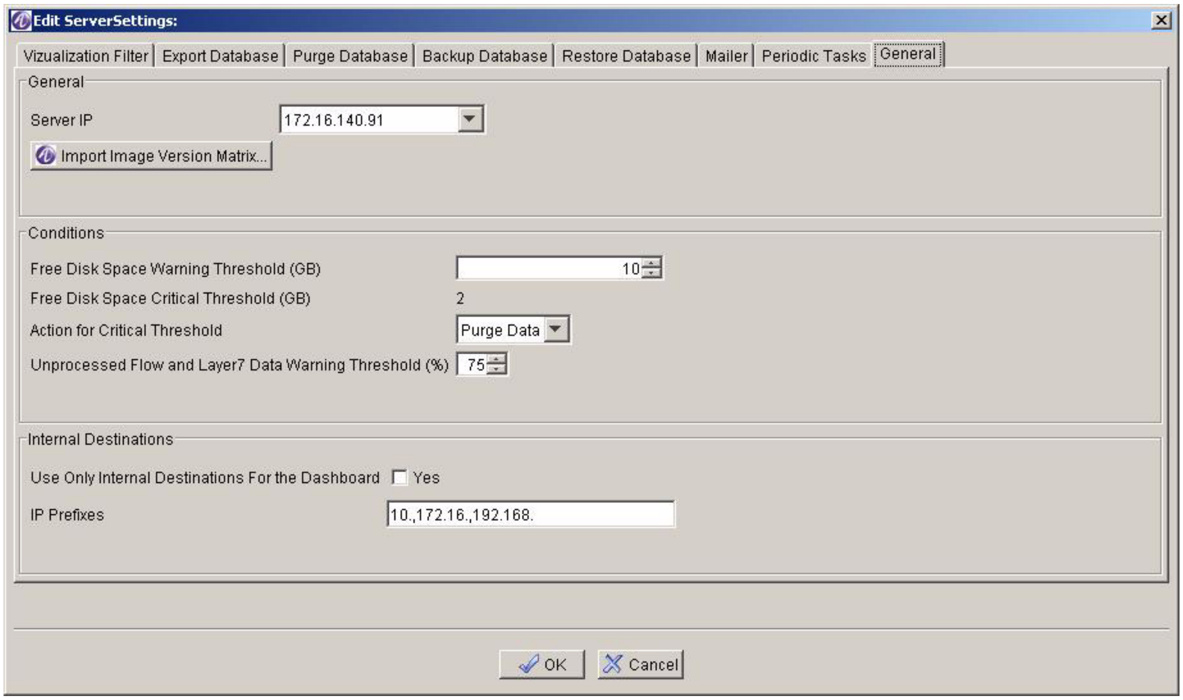
The General tab in the Server Settings allows you to set free disk space thresholds and import image version matrix.

To set free disk space thresholds and import image version matrix:

1 Select *Tools > Server Settings*. The Edit Server Settings screen displays.

2 Select the General tab (*Figure 127*).

Figure 127 Edit Server Settings - General



Edit ServerSettings:

Vizualization Filter | Export Database | Purge Database | Backup Database | Restore Database | Mailer | Periodic Tasks | General

General

Server IP: 172.16.140.91

Import Image Version Matrix...

Conditions

Free Disk Space Warning Threshold (GB): 10

Free Disk Space Critical Threshold (GB): 2

Action for Critical Threshold: Purge Data

Unprocessed Flow and Layer7 Data Warning Threshold (%): 75

Internal Destinations

Use Only Internal Destinations For the Dashboard: □ Yes

IP Prefixes: 10.,172.16.,192.168.

3 Select the server IP address from the dropdown list. This field is used in case OmniVista SafeGuard Manager is installed on a machine that has two Ethernet interfaces. For more information on starting the OmniVista SafeGuard Manager server with the proper interface, see *Starting OmniVista SafeGuard Manager Server in a Multiple Interface Scenario*.

4. Click **Import Image Version Matrix** if you want to import the matrix that gives image version and bootloader compatibility matrix.
5. From the dropdown list, select a Free Disk Space Warning Threshold.
6. Select an action for Critical Threshold. Valid choices are Purge Data and Stop Server.
7. Specify an Unprocessed Flow and Layer7 Data Threshold.
8. If you want to use only internal destinations for the dashboard, select this checkbox.
9. Enter the IP prefixes that these attributes are applicable to.
10. Click **OK** to apply the settings.

Starting OmniVista SafeGuard Manager Server in a Multiple Interface Scenario

When OmniVista SafeGuard Manager is installed on a system that has multiple IP addresses and the OmniVista SafeGuard Manager server is started for the first time, it binds itself to the IP address chosen by Windows OS. However, if this default IP address is not accessible from the OmniVista SafeGuard Manager client and the SafeGuard devices, then this address needs to be changed.

Use the following procedure to ensure that the correct interface is used when starting the OmniVista SafeGuard Manager server:

1. Login to OmniVista SafeGuard Manager using the local client installed on the OmniVista SafeGuard Manager server using the desktop shortcut.
2. Go to *Tools >Server Settings*, General Tab. For more information, see *General*.
3. Select the IP address that is accessible from both the OmniVista SafeGuard Manager clients and the SafeGuard devices using the dropdown list in the Server IP field.
4. Click **OK** to apply the settings.
5. Exit out of the client.
6. Restart the server.

chapter

8 Audit Logs and Statistics

This section includes the following:

- *Audit Logs*
- *Device Health*
- *Server Health*

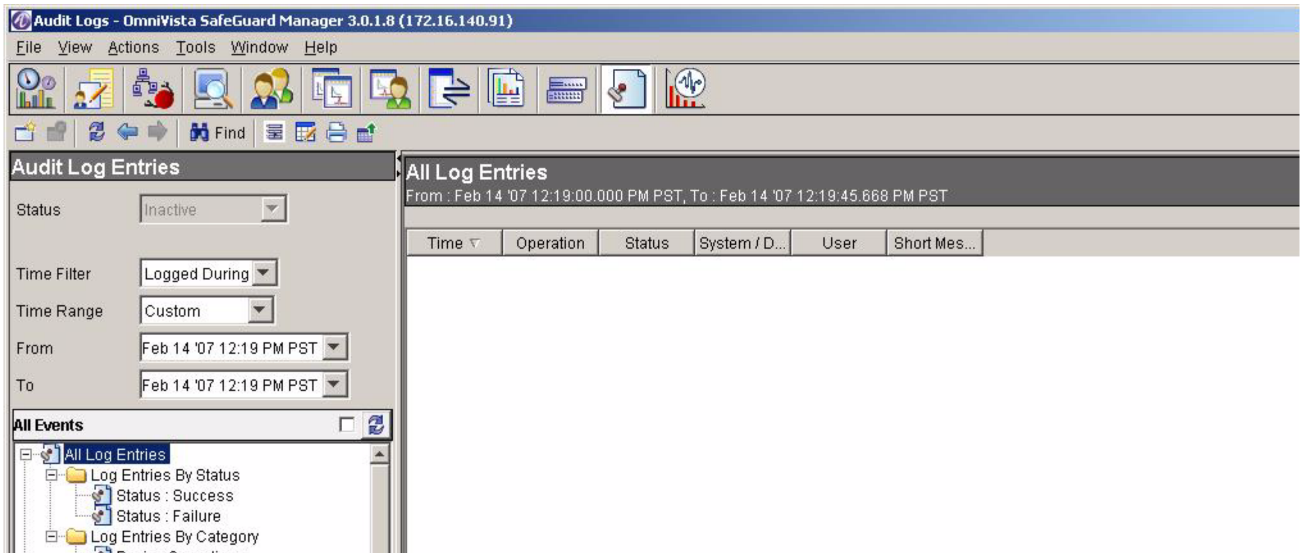
Audit Logs

OmniVista SafeGuard Manager provides logs that indicate who did what and when and on which device. These logs are for user and device operations and can be helpful for auditing purposes. You can choose to view these log entries by time, status, or category. Audit log does not log any debugging log messages.

To view audit logs:

1 Click the Audit Log icon in the Page Bar. The Audit Logs screen displays (*Figure 128*).

Figure 128 Audit Logs



Status: Inactive

Time Filter: Logged During

Time Range: Custom

From: Feb 14 '07 12:19 PM PST

To: Feb 14 '07 12:19 PM PST

All Log Entries

From : Feb 14 '07 12:19:00.000 PM PST, To : Feb 14 '07 12:19:45.668 PM PST

2 You can choose to view audit logs either by status or by category by highlighting the appropriate logs in the navigation tree. The following information is displayed:

Table 50 Audit Log Attributes

Attribute	Description
Time	Time the entry was logged.
Category	Type of log message: authentication, OmniVista SafeGuard Manager action, device action. For more information on message type, see OmniVista SafeGuard Manager Log Messages.
Operation	Type of operation executed.
Status	Success/Failed to indicate the status of the operation performed. If it is not applicable, no value will be shown.

Table 50 Audit Log Attributes

Attribute	Description
System/Device	Provides the context of the operation.
User	User ID.
Short Message	Brief message description of the log.

3. In the details panel, you can view the details of the message logged in by the operation.
4. Click **Print** in the Action Bar to print the log data or click **Export** to export the log into a CSV format.

OmniVista SafeGuard Manager Log Messages

Following list shows some of the type (category) of messages that OmniVista SafeGuard Manager logs:

- Authentication
  - Login
  - Enable or disable 4-eye mode
  - Add, modify, or delete user
- OmniVista SafeGuard Manager Actions
  - Database purge
  - Database export
  - Database import
  - Clear policy incidents
  - Delete policy incidents
  - Change configuration of server settings
- Device Actions
  - Any device action executed in Config Management
  - Clear user
  - Refresh user role
  - Clear malware incident(s)
  - White list malware incident(s)

  - Delete visualization records
  - Delete device
  - Manage or unmanage a device
  - Communication status change (SNMP, ICC, CLI/GSOAP)
- Reports
  - Definition: Add/Modify/Delete
  - Schedule: Add/Modify/Delete
  - Report generation
  - Report email
- Dashboards
  - Configuration change

Device Health

OmniVista SafeGuard Manager allows you to collect, view, and store statistics relating to device health. These statistics are helpful in analyzing each device's performance and its current connections. Administrators can use this drill-down capability to view device CPU and memory performance, fan or power failure, and any device operation success or failure messages. For more information on enabling device health statistics and the collection interval, see *General*. The following parameters are collected as part of device health:

- Current CPU Usage
- Current memory usage
- Disk I/O
- Hardware status (fan failure, power supply failure, temperature

You can view device health in one of the following ways:

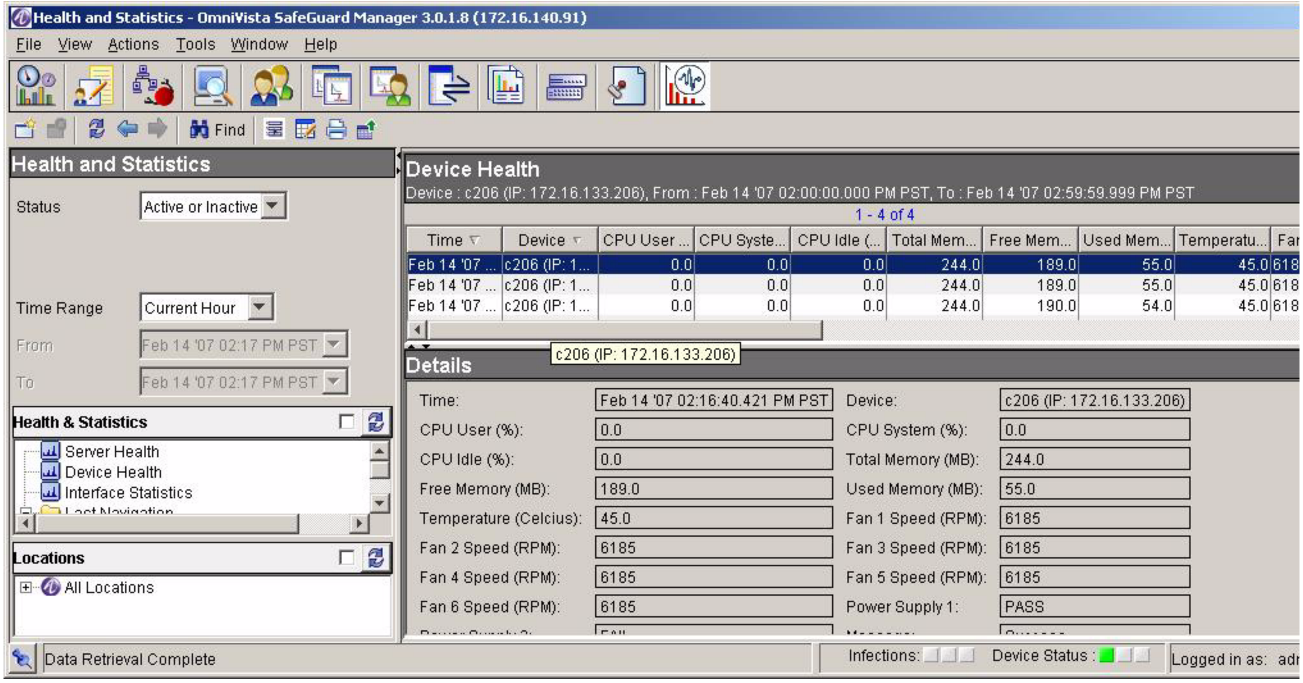
- Click on the View Statistics icon in the Page Bar. This view displays the statistics for both OmniVista SafeGuard Manager server health and device health.
- Click on the Device Heath Statistics node in the navigation tree. You can expand this node to view all devices. Select an individual device to view the most recent statistics or statistics for a specified time range.
- Select the Health tab from on the Device Configuration screen. This tab displays the most recent device health statistics for the selected device. Once the tab is active, data is automatically refreshed every 5 minutes.

Viewing Device Health Statistics

To view device health:

1 From the Config Management view, click on the Device Health Statistics node in the navigation tree, or from the Page Bar, select *Other Actions > Show Device Health*. The Device Health Statistics screen displays (*Figure 129*).

Figure 129 Device Health Statistics



Status: Active or Inactive

Time Range: Current Hour

From: Feb 14 '07 02:17 PM PST

To: Feb 14 '07 02:17 PM PST

Device Health

Device : c206 (IP: 172.16.133.206), From : Feb 14 '07 02:00:00.000 PM PST, To : Feb 14 '07 02:59:59.999 PM PST

1 - 4 of 4

Time	Device	CPU User ...	CPU Syste...	CPU Idle (...	Total Mem...	Free Mem...	Used Mem...	Temperatu...	Far
Feb 14 '07 ...	c206 (IP: 1...	0.0	0.0	0.0	244.0	189.0	55.0	45.0	618
Feb 14 '07 ...	c206 (IP: 1...	0.0	0.0	0.0	244.0	189.0	55.0	45.0	618
Feb 14 '07 ...	c206 (IP: 1...	0.0	0.0	0.0	244.0	190.0	54.0	45.0	618

Time:	Feb 14 '07 02:16:40.421 PM PST	Device:	c206 (IP: 172.16.133.206)
CPU User (%):	0.0	CPU System (%):	0.0
CPU Idle (%):	0.0	Total Memory (MB):	244.0
Free Memory (MB):	189.0	Used Memory (MB):	55.0
Temperature (Celcius):	45.0	Fan 1 Speed (RPM):	6185
Fan 2 Speed (RPM):	6185	Fan 3 Speed (RPM):	6185
Fan 4 Speed (RPM):	6185	Fan 5 Speed (RPM):	6185
Fan 6 Speed (RPM):	6185	Power Supply 1:	PASS

2 The following statistics are displayed:

Table 51 Device Health Statistics

Attribute	Description
Timestamp	Time the statistics were collected.
User CPU	CPU utilization for the user.
System CPU	CPU utilization by the system.
Idle CPU	
Total Memory	Total memory in MB.
Free Memory	Total free memory in MB.
Used Memory	Total used memory in MB.
System Internal Temperature	System internal temperature measured in Celsius.

Table 51 Device Health Statistics

Attribute	Description
Fan 1 Speed - Fan 6 Speed	Speed of the various fans from fan 1 to fan 6.
Power Supply 1	Status of the primary power supply.
Power Supply 2	Status of the secondary power supply.
Message	Message relating to the device operation performed.

These values are collected periodically from each device and stored in the database.

3 Specify times in the Time Range field to view statistics for a specific time.

NOTE: You can further fine tune statistics collection interval and other configuration using *Tools > Server Settings > General Tab*. For more information, see *General*.

4 Click **Refresh** to see the updated device health and statistics.

Server Health

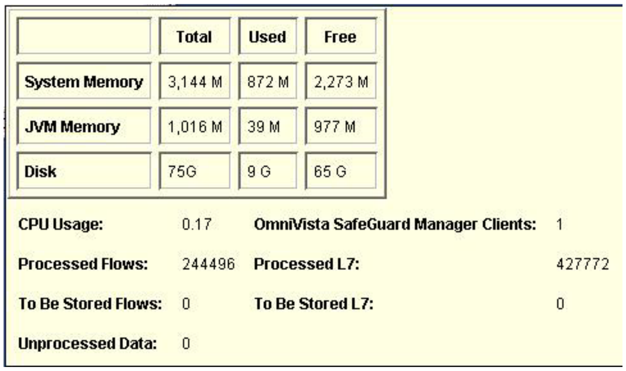
OmniVista SafeGuard Manager allows you to collect, view, and store statistics relating to server health. These statistics are helpful in analyzing server performance. Administrators can use this drill-down capability to view server CPU and memory performance, OmniVista SafeGuard Manager client connections, Layer 7 events, and any application or flows processed. The following parameters are collected as part of server health:

- Memory
- CPU
- Disk
- Number of OmniVista SafeGuard Manager users
- Number of flows processed
- Number of Layer 7 events processed

Server statistics are collected periodically and stored in the database on a daily basis. The default rate at which the statistics are collected is 1 minute and is controlled by the `ServerHealth_Interval_In_Minutes` parameter in *application.conf*. Each day current data replaces the data in the server health table, while earlier data is moved to the previous day's health table. The purging of the server health tables is performed based on the settings you specified in the server settings. For more information, see *Purging the Database*.

You can view server health in one of two ways:

- Place your cursor on the settings icon located at the bottom-right corner of the OmniVista SafeGuard Manager client window. Most recent server health information is available as a tooltip for this icon. A sample display of current values using tooltip is shown below.



	Total	Used	Free
System Memory	3,144 M	872 M	2,273 M
JVM Memory	1,016 M	39 M	977 M
Disk	75G	9 G	65 G

CPU Usage: 0.17

OmniVista SafeGuard Manager Clients: 1

Processed Flows: 244496

Processed L7: 427772

To Be Stored Flows: 0

To Be Stored L7: 0

Unprocessed Data: 0

- Click the Statistic View icon from the Page Bar. For a detailed description of these values, see *Viewing Server Health Statistics*.

Viewing Server Health Statistics

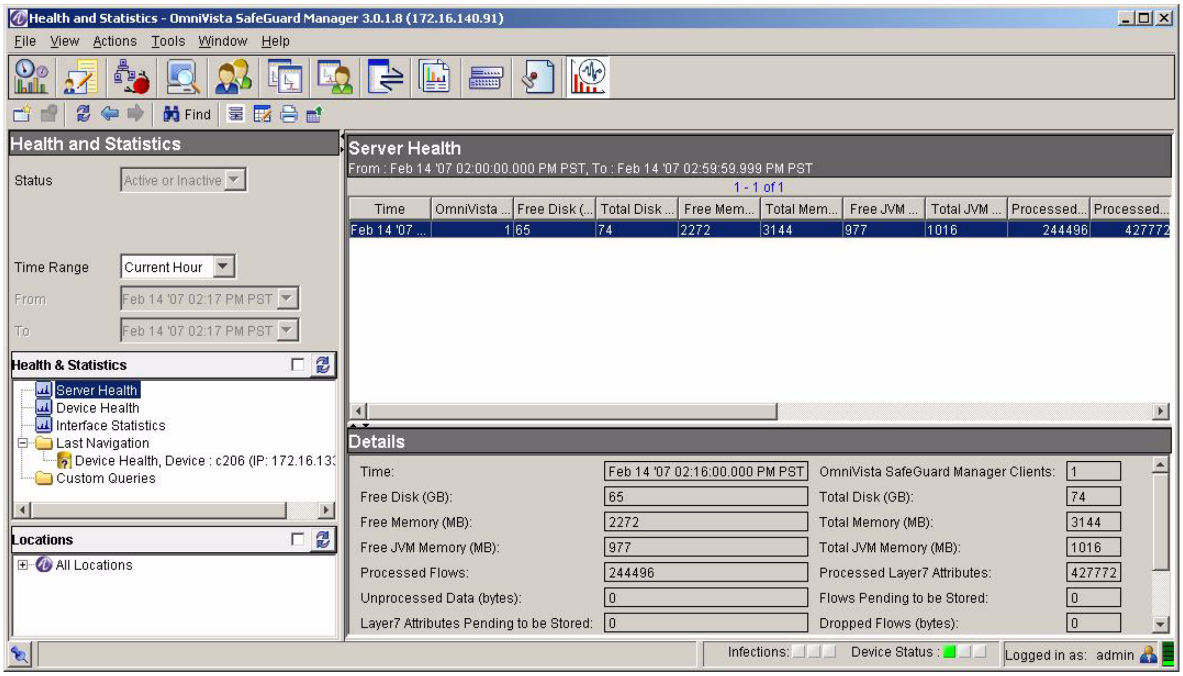
You can choose to view server health statistics over a specific period of time or the most recent values available.

To view server health statistics:

1 Click the Statistic View icon in the page bar.

2 The OmniVista SafeGuard Manager Server Health screen displays (*Figure 130*).

Figure 130 OmniVista SafeGuard Manager Server Health



Status: Active or Inactive

Time Range: Current Hour

From: Feb 14 '07 02:17 PM PST

To: Feb 14 '07 02:17 PM PST

Server Health

From : Feb 14 '07 02:00:00.000 PM PST, To : Feb 14 '07 02:59:59.999 PM PST

1 - 1 of 1

Time	OmniVista ...	Free Disk (...	Total Disk ...	Free Mem...	Total Mem...	Free JVM ...	Total JVM ...	Processed...	Processed...
Feb 14 '07 ...	1	65	74	2272	3144	977	1016	244496	427772

Details

Time:	Feb 14 '07 02:16:00.000 PM PST	OmniVista SafeGuard Manager Clients:	1
Free Disk (GB):	65	Total Disk (GB):	74
Free Memory (MB):	2272	Total Memory (MB):	3144
Free JVM Memory (MB):	977	Total JVM Memory (MB):	1016
Processed Flows:	244496	Processed Layer7 Attributes:	427772
Unprocessed Data (bytes):	0	Flows Pending to be Stored:	0
Layer7 Attributes Pending to be Stored:	0	Dropped Flows (bytes):	0

3 Use the Time Range fields to specify a specific time period for which you want to view server statistics. The following statistics are displayed:

Table 52 Server Health Statistics

Attribute	Description
Time	
OmniVista SafeGuard Manager Clients	Number of OmniVista SafeGuard Manager clients connected.
Free Disk (GB)	Free disk space on the server in GB.
Total Disk (GB)	Total disk space on the server in GB.
Free Memory (MB)	Memory in MB that is free and available on the server.

Table 52 Server Health Statistics

Attribute	Description
Total Memory (MB)	Total memory in MB on the server.
Total JVM Memory (MB)	Memory allocated to Java Virtual Machine (JVM).
Application Flow Events	Number of application flow events processed in the specified time.
Layer 7 Events	Number of layer 7 events processed in the specified time.
CPU Usage (%)	Percentage of CPU being used on the server.
Disk Reads	
Disk Writes	

Index