



User Guide

Ver 4.6

Clavister AB
Torggatan 10,
SE-891 28 ÖRNSKÖLDSVIKE,
SWEDEN
www.clavister.com

Copyright and Trademarks

Clavister Insight End User License Agreement.

Important - BEFORE OPENING OR INSTALLING THE SOFTWARE PACKAGE(S), CAREFULLY READ THE TERMS AND CONDITIONS OF THE FOLLOWING Clavister Insight LICENSE AGREEMENT. OPENING OR INSTALLING THE SOFTWARE PACKAGE(S) INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THE AGREEMENT. THIS IS A LEGAL AGREEMENT BETWEEN YOU, AS LICENSEE, AND EIQNETWORKS, INC. ("EIQNETWORKS") AS OWNER. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THE AGREEMENT, RETURN THE UNOPENED AND UNINSTALLED SOFTWARE PRODUCTS AND THE ACCOMPANYING ITEMS TO THE PLACE YOU OBTAINED THEM. PROMPTLY RETURN THE UNOPENED AND OR UNINSTALLED SOFTWARE PACKAGE(S) AND ALL OTHER MATERIALS WITH PROOF OF PAYMENT TO YOUR PLACE OF PURCHASE, AND YOUR LICENSE FEE WILL BE REFUNDED.

SOFTWARE LICENSE

1) GRANT OF LICENSE. This License Agreement ("License") gives you a nonexclusive, nontransferable license to install one copy of the software per contained in the sealed software package or electronic package and may include electronic documentation or paper documentation, (the "SOFTWARE") on one (1) workstation, or server ("HOST"). Base license allows the user to collect, analyze and report on log / event / activity data from ten(10) licensed devices. An additional license is needed for each additional device beyond the base license to collect, analyze and report on log / event / activity data from licensed network device or licensed host. A Base License is required before additional licenses can be purchased. A device is defined as any supported network switch, router, firewall, IDS / IPS / Proxy / Anti Virus Server / any network device or appliance. A host is defined as any Windows or Linux/Solaris or Unix node.

The SOFTWARE is in "use" on a computer when it is loaded into the temporary memory (RAM) or installed into the permanent memory (HARD DISK /CD ROM, or other storage device) of that computer. A separate license is required for each physical device on which the licensed software will be used to collect, analyze, monitor and report.

Clavister Insight is licensed based on Device IP address, Device ID, and or Device Name. Customers who wish to purchase Clavister Insight license are required to provide the Systems Identifier (System ID of the system on which Clavister Insight will be installed) so that eIQnetworks can generate the appropriate license key. Customers who subsequently change their System are required to submit a written letter (on your company letterhead) requesting eIQnetworks to issue a new license key. eIQnetworks at its sole discretion will determine if it will issue a new license key.

2) UPGRADES. If the SOFTWARE is a valid upgrade you may use or transfer the SOFTWARE only in conjunction with the prior version(s) of the SOFTWARE.

3) COPYRIGHT. The SOFTWARE (including any images, photographs and text incorporated into the SOFTWARE) is owned by eIQnetworks, and is protected by United States, Canadian and international copyright laws and international treaty provisions. No title to the Software shall be transferred to you. Therefore you must treat the SOFTWARE like any other copyrighted material and not reproduce it except that you either (a) make one copy of the SOFTWARE solely for backup or archival purposes, or (b) transfer the SOFTWARE to a single hard disk

provided you keep the original solely for backup or archival purposes, and the copy contains all of eIQnetworks' proprietary notices. You may not copy the printed materials accompanying the SOFTWARE.

4) TITLE. Clavister Insight and the information it contains, any updates and all copies are eIQnetworks property and title to such Software Program remains with eIQnetworks.

5) Other Restrictions. You may not reverse engineer, decompile, disassemble, or translate the SOFTWARE, except to the extent such foregoing restriction is expressly prohibited by applicable law. You may not permit other individuals to use the Software Program except pursuant to the terms and conditions herein, reverse assemble, decompile, modify or create derivative works based on the Software Program, copy the Software Program except as provided above, rent, lease, assign or otherwise transfer any rights with respect to the Software Program or remove any proprietary notices on such Software Program. It is illegal to copy or distribute Clavister Insight software or its accompanying documentation, including programs, applications, data, codes, and manuals, or to run a copyrighted software program on two or more computers simultaneously unless this is specifically allowed by the license agreement, without permission or a license from eIQnetworks.

6) Dual-media Software. You may receive the SOFTWARE in more than one medium. Regardless of the type or size of medium you receive, you may use only the medium appropriate for your single-user computer. You may not use the other medium on another computer or loan, rent, lease, or transfer the disks to another user except as part of the permanent transfer (as provided above) of all SOFTWARE and printed materials, nor print copies of any user documentation provided in "online" or electronic form.

7) EXPORT CONTROLS. The Software Program and/or any underlying information or technology may not be exported or re-exported into or to a national or resident of Cuba, Libya, North Korea, Iran, Syria or any other country to which the United States has effected an embargo, or to anyone on the U.S. list of Specially Designated Nationals.

8) TERMINATION. eIQnetworks may terminate the license granted you hereunder at any time if you fail to comply with any terms and conditions of this Agreement. Upon termination of the license, you must destroy or dispose of the Software, any copies of the Software and manual and other materials provided with the Software.

9) THIRDPARTY SOFTWARE. The Software Program uses certain third-party libraries/software. The license agreements of the same are provided with *THIRDPARTYLICENSEREADME.txt* under application install path.

LIMITED WARRANTY. eIQnetworks warrants that the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of thirty (30) days from the date of receipt. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you. This warranty may not be assigned.

CUSTOMER REMEDIES. eIQnetworks and its suppliers' entire liability and your exclusive remedy shall be, at eIQnetworks option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet eIQnetworks Limited Warranty and which is returned to eIQnetworks with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or twenty-one (21) days, whichever is longer.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, eIQnetworks and its suppliers disclaim all other warranties, either or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, with regard to the SOFTWARE and the accompanying printed materials. This limited warranty gives you specific legal rights. You may have others which vary from state/jurisdiction to state/jurisdiction.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable laws, in no event shall eIQnetworks or its suppliers be liable for any damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of information, or other pecuniary loss) arising out of the use of or inability to use Clavister Insight, even if eIQnetworks has been advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Should you have questions concerning this Agreement, or if you desire to contact eIQnetworks please visit our Web site: www.eIQnetworks.com

I have read and agree to the terms and conditions above.

Clavister InSight™, eIQnetworks™, The Power of Security Intelligence, Security Analysis Center™ and Instant Reports™ are trademarks and or Service marks of eIQnetworks, Inc.

Contents

INTRODUCTION	10
COMPONENTS IN CIS	10
<i>Clavister Insight 4.6 helps you</i>	11
<i>Icons in the Documentation</i>	11
GETTING STARTED	12
STARTING CLAVISTER INSIGHT	12
<i>Navigating through CIS</i>	13
<i>Help</i>	13
SYSLOG SERVER	14
UPGRADING REMOTE SYSLOG SERVER(S)	16
Steps: Upgrading Syslog Server(s)	17
DASHBOARD	18
EVENTS GRAPH	21
MANAGE DASHBOARD	22
<i>How to Manage?</i>	22
<i>Creating New Dashboard</i>	23
ALERTS	26
WORKBENCH	30
<i>Monitoring</i>	32
<i>Forensic</i>	33
<i>Apply Filter</i>	35
<i>Drill Down</i>	36
POLICIES	37
CREATE POLICY	38
<i>Load Rule from the template</i>	43
<i>Create New Rule</i>	43
<i>Edit Policy</i>	43
<i>Make Copy of the Policy</i>	44
<i>Delete Policy</i>	44
CREATING DEVICE BASED RULE	44
<i>Applying filters to a Rule</i>	47
<i>Editing a Device based Rule</i>	52
<i>Making a Copy of the Device based Rule</i>	53

<i>Deleting Device based Rule</i>	53
<i>Configuring a Device based Rule</i>	54
ALERT DELIVERY	54
<i>E-mail Notification</i>	55
<i>SNMP Trap</i>	56
RULE TEMPLATE	57
CREATING RULE TEMPLATES	57
<i>Device Based Rule Templates</i>	58
<i>Editing a Template</i>	58
<i>Deleting a Rule Template</i>	58
SET THREAT LEVELS	59
<i>Change threat levels</i>	60
PROFILES	61
CREATING A NEW PROFILE	62
<i>CIS Syslog as Source Input</i>	63
<i>File as Source Input</i>	64
<i>Selecting Groups and Devices</i>	67
<i>DNS Lookup</i>	68
<i>Filter Templates</i>	69
<i>Scheduler</i>	80
Add Task	81
<i>Report Type</i>	86
Query By	88
<i>Report Style</i>	88
<i>Customizing Reports</i>	89
Editing a Report	90
Deleting a Report	91
<i>Save Report</i>	91
E-mailing Reports	94
FTP Reports	94
EDIT PROFILE	95
COPY PROFILE	96
DELETE PROFILE	96
FORENSICS	97
LOG COLLECTION	102
CONFIGURING SEARCH	102
<i>Device Based New Search</i>	103
<i>Archived Search Data</i>	104

<i>Log Files from Selected Devices</i>	105
<i>Date & Time Range</i>	105
Scheduler	106
<i>Scheduling Forensics Search</i>	106
Add Task	107
<i>Device Based Forensic Search</i>	107
<i>Search Filters</i>	108
Save Report	111
<i>Forensics Options</i>	112
EDIT SEARCH	113
COPY SEARCH	113
DELETE SEARCH	113
MANAGING DEVICES AND GROUPS	114
THE GROUPS SCREEN	114
The Global Group	115
Adding a Group	116
Editing a Group	116
Moving a Device from Default Group	116
Regional and Group drop-down lists	117
THE DEVICES SCREEN	117
Adding a Device	118
Configuring the Intrushield devices:	118
Adding a Virtual Device or Interface	119
Deleting a Device	119
Configure Devices	120
Licensing Criteria	121
Policies	122
Collection Policy	123
Add Collection Policy	123
Policy Synopsis	125
Edit Collection Policy	125
OPTIONS	126
GENERAL SETTINGS	126
Monitoring Options	128
Selecting a admin user who can Create/Modify Event Classes	128
ADMIN ALERTS	129
Add Admin Alert	129
PROTOCOL SETTING	131

E-MAIL SETTINGS	132
MONITORING	134
ADVANCED SETTINGS	135
APP STATUS	137
SYSLOG STATISTICS	137
MONITORING STATISTICS	138
TRACKING LOGS	139
SCHEDULER	140
SYSTEM INFO	140
USERS	142
USERS	143
<i>Create a New User</i>	144
<i>Option to customize the Security Center view</i>	145
EDITING A USER	146
<i>Add Active Directory User</i>	147
<i>Import Active Directory Users</i>	148
<i>Importing Active Directory Server User Accounts:</i>	149
USER SESSIONS	150
GROUPS	150
POLICIES	152
AUDIT TRIGGERED ALERTS	153
<i>How to create and assign privileges to an Audit User?</i>	153
LICENSES	155
LICENSE REQUIREMENTS	155
LICENSING DEVICES IDENTIFIED BY CIS SYSLOG SERVER	155
LICENSING AN UNCONFIGURED DEVICE	156
THE LICENSE MANAGER SCREEN	156
<i>Licenses</i>	157
Adding a License	158
Managing a License	158
Adding a Device	159
Editing a Device	159
Updating a License	160
<i>Licensed Devices</i>	161
<i>Options</i>	161
Export Identifier	162
Export License	162

SECURITY CENTER	163
SECURITY CENTER- REPORTING	163
<i>Calendar Frame</i>	165
<i>Table of Contents Frame</i>	165
<i>Report Frame</i>	166
<i>Exporting a Report</i>	166
<i>Utility Options</i>	166
<i>Pane Options</i>	167
<i>Options</i>	168
<i>Manage Views</i>	170
Creating a Custom View	170
Export Report	172
<i>Export Report-Filters</i>	174
<i>Filters</i>	174
SECURITY CENTER - MONITORING	176
Views	176
Creating a Custom View	177
Monitors	178
The Add Monitor Wizard	179
ADDING A DEVICE BASED MONITOR	179
Selecting Device Based Entities	179
EVENT VIEWER FILTERS	184
Selecting Entities to Filter	184
APPENDIX	186
BACKING UP CIS 4.6	186
<i>Backing Up Data from an CIS 4.6 Server</i>	186
<i>Backing Up Data from an CIS 4.6 Syslog Server</i>	186

Introduction

This chapter provides a description of the Clavister Insight and its components.

What is CIS?

CIS provides a platform to manage security information and events effectively. This requires the collection of log files from devices, normalizing the data across disparate devices, aggregation of the data into a database and correlating the data for monitoring, alerting, reporting and forensic tasks. CIS automates all these tasks meticulously so that the IT or security administrators valuable time can be spent analyzing the networks security posture rather than the tedious manual process of managing log files.

Components in CIS

CIS constitutes of 2 main components:

- ❖ [CIS Server](#)
- ❖ [Syslog Server](#)

CIS Server: All the network devices to be analyzed are added, profiles and alerts are configured so that when syslog server fetches the event logs in a live environment, it can report on the event logs. These reports help the security administrator to take proactive actions and safeguard networks.

Syslog Server: Collects event logs automatically from all the configured network devices, compresses them into delta files and sends it across to the CIS Server for generating reports.

Clavister Insight 4.6 helps you

- ❖ Meet HIPAA, GLBA, Sarbanes-Oxley, FISMA and PCI regulatory compliance.
- ❖ Monitor and visualize hacker and virus attacks and behavior patterns.
- ❖ Minimize or eliminate false positives with correlated alerting.
- ❖ Identify intrusions, viruses and security breaches, including blended attacks.
- ❖ Identify attack type, source, destination, port, protocol, severity, rules, etc. in real-time.
- ❖ Obtain details on virus activity such as virus source, virus type, virus details, virus impact, etc.
- ❖ Using forensic analysis, vector an attack for investigating a hacker's behavior and attack path.
- ❖ Understand protocol usage by device, user and department.
- ❖ Understand blocked website access and allowed/denied traffic.
- ❖ Bandwidth utilization by department, client and protocol.
- ❖ Identify inappropriate Internet usage by employees.
- ❖ Understand and obtain details on SPAM and spyware activity.
- ❖ MSSPs can provide role based access to reporting and monitoring portals.

Icons in the Documentation

There are three icons used to call your attention to additional helpful information.



The "Important!" icon points out important information regarding data or system security.



The "Note" has information that should be considered.



The "Tip" has information that may aid in performing a procedure or in solving a problem.

Getting Started

This chapter provides instructions how to start, configure default options, and create profiles using Clavister Insight 4.6.

Starting Clavister Insight

This section explains how to start Clavister Insight (registered version or a trial version).

Once you install the software successfully, start CIS by double clicking on the Clavister Insight icon created on the desktop.



CIS Desktop Icon

Alternatively, you can start Clavister Insight by typing the installed Web site URL in the address bar of the browser window.

Provide the default user credentials created during the CIS install on the login screen.

The first time you start your CIS software, a 21 days evaluation period begins, good enough to understand the application, test its operation, and purchase the product. During the evaluation period, Clavister Insight is as competent as the purchased product. At the end of the evaluation period, the evaluation license expires, thereby ceasing the CIS operations.


To ensure uninterrupted Security Information and Event analysis and to protect your network, you should purchase the product at the earliest.

Navigating through CIS

By default, CIS starts the Dashboard console. The following list highlights important features of the product to evaluate.

1. **Dashboard:** View security events data from 100s of heterogeneous and multi-vendor network devices.
2. **Alerts:** Template driven Alert Manager allows creation and definition of any number of alerts.
3. **Forensics:** Provides the ability for forensics search of 100s of GB of log data for security audits.
4. **Policies:** Rule based policies, where the user can decide to deliver alerts via e-mail or group the required events in an event class to set threat levels.
5. **Security Center:**
 - ❖ **Reporting:** Delivers powerful custom and pre-defined reports for security including reports for antivirus, spam, spyware, and regulatory compliance.
 - ❖ **Monitoring:** Provides a quick, consolidated real-time view of the security posture of the network.
6. **Device Manager:** Provides central platform to configure all devices.

Help

Extensive online help is available for all the modules by clicking  on the top right-hand corner of each screen. If you have any questions about Clavister Insight, our [support](#) team will be glad to assist you.

Syslog Server

The Clavister Insight syslog server helps you do away with manual configuration of devices. While some devices can export log files in a readable format, others typically do not write log information to a readable file. In such cases, Clavister Insight relies on a syslog server to capture log information. The Clavister Insight syslog server helps eliminate the need for manual configuration of devices, automatically detects and configures devices. The syslog server can be installed on any machine in the network.

One of the first things you should do after installing Clavister Insight is configure a syslog server. While doing this, you can choose to load balance it by indicating a secondary syslog server that will take over from it once a specified threshold value is reached. You can also backup all the logs that are streamed to the syslog server from various devices by configuring a backup syslog server.



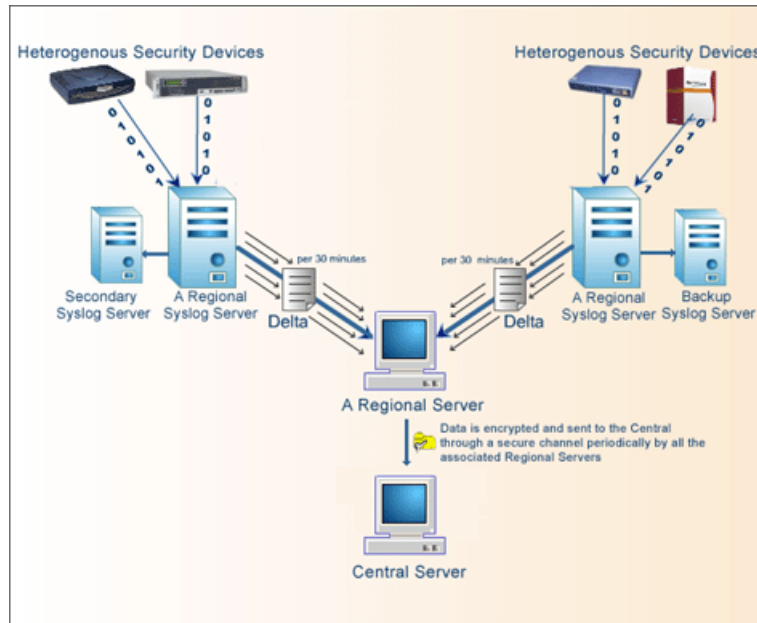
The backup syslog server can be a non-CIS or CIS syslog server. The CIS Syslog server forwards all the packets that it receives from the configured devices to the backup syslog server. Please note that a backup syslog server cannot forward any data to the CIS syslog server and in case that happens, the CIS syslog server drops all such data packets.

When you create a profile, you can choose to collect your log files from any of the following:

- ❖ CIS Syslog Server
- ❖ File

CIS Syslog Server: The CIS syslog server streams log file data to the data collector service installed on the Clavister Insight machine, where it is parsed and stored in the database.

Regional-Central Architecture



Once the syslog server is installed on the machine local to the network of the device, it automatically updates delta file to the database on a regular basis without any intervention from the administrator.

File: Use this option to report on static log files obtained from a manually added device (device that is not configured to send data to the syslog server).



Since the Clavister Insight syslog server runs as a Windows service, make sure it is installed on Windows NT, 2000, XP or 2003.



To configure CIS syslog server, you must have administrator privileges.

Windows XP with SP2 has strict Windows Firewall rules, so it blocks all external applications. Make sure that the default settings of your Windows Firewall are changed to unblock the following:

- a. Allow remote administration for CIS Apache Server from the Group Policy Settings.
- b. Provide exception for syslog server, CIS Apache Server, and other related executable files.

c. Provide exception for the following ports.

Add following TCP ports: open up the following ports between the remote syslog servers and CIS server.

- ❖ 230 → for Secure Socket File transfer
- ❖ 10616 → CISServer.exe
- ❖ 10617 → SyslogServer.exe
- ❖ 10618 → DataCollector.exe
- ❖ 10626 → for receiving commands from syslog server, if the syslog server is installed on a remote machine.
- ❖ 10817 → CIS communication

Add following UDP ports: 10624 (for Monitoring EXE to receive data from syslog server, if the syslog server is installed on remote machine), 514 (if the syslog server is installed locally)

To make device log files accessible in a consistent log file format, the Clavister Insight Syslog server collects log data from the device and writes it in a usable format to an IP address on the machine running Clavister Insight. The default port number is 514 using UDP protocol. The log files collected by the Clavister Insight syslog server are stored locally on the machine running Clavister Insight and log files created by the device remain there.

By default, the Clavister Insight syslog server is configured to start when the Clavister Insight starts and continues to run as long as the machine is running. The syslog service collects log data in real-time, and up-to-date logs are available for reporting. If the syslog service is not running, any log data generated will be lost.

Upgrading Remote Syslog Server(s)

During the upgrade you are prompted to upgrade the following components.

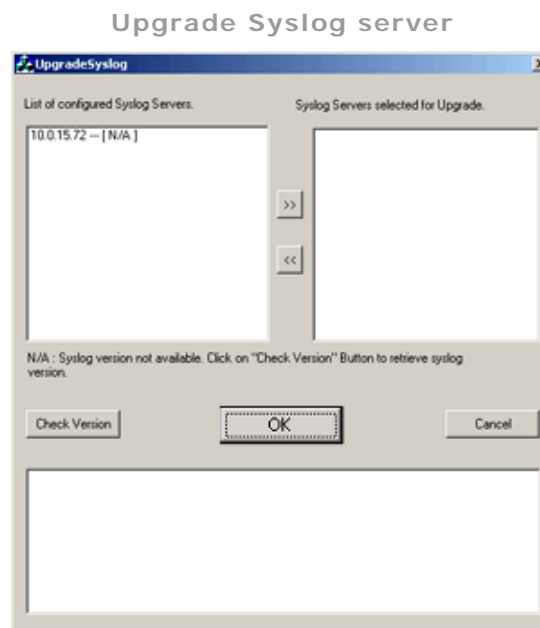
- ❖ CIS Server
- ❖ Syslog Server

You can directly upgrade both the components over the previous versions if installed on the local machine. When you select to upgrade, UpgradeSyslog window is displayed along with the list of associated Syslog Servers. The


following section provides information on how to upgrade the remote CIS Syslog server.

Steps: Upgrading Syslog Server(s)

1. **UpgradeSyslog** window is displayed with the list of all the Syslog servers associated with the CIS server.
2. To check the version number of the listed Syslog servers, select a Syslog and click **Check Version** button. Version number of the selected Syslog is displayed.
3. After you check the version numbers of the listed Syslog servers, move the Syslog servers that are to be upgraded to the selected list.
4. Click **OK**. All the selected Syslog servers will be upgraded to the latest version.



After the upgrade, all the selected syslog servers will be upgraded to the latest version.

Important: Clavister Insight notifies the admin user of any failed upgrades through a flashing icon  on the main screen. Admin user can acknowledge it and can retry to upgrade.






Dashboard

The dashboard tab brings up a list of real-time events occurring at each device. Each event displayed expatiates upon Source IP, Destination IP, Virtual Device, Rule, User Name, Category, Date & Time, Group Name, Device Type, BII, Flow, Protocol, Event description, Event ID, Destination Port, Attack ID, Virus Name, Interface, URL, Virus ID, and Device Name.

Using the real-time Event Viewer, details on all requests that result in an emergency are readily available, such as the requests that triggered it, where it came from, what device was attacked and the port of attack. You can choose the lowest severity up to which monitoring can be performed. This helps you quickly take corrective actions to protect your network perimeter.



The Event Viewer console on a CIS Central displays recent events from all the CIS regional servers.

Severity	Description
 Emergency	An Emergency Event indicates a significant problem, such as a loss of functionality or data, and the user should pay immediate attention.
 Alert	An Alert Event is a security event fired when an alert message is received from the server and is immediately displayed to the user.
 Critical	A Critical Event indicates a problem that is not immediately significant but may cause future complications
 Error	An Error Event indicates a significant problem the user should know about, such as a loss of functionality or data.
 Warning	A Warning Event indicates a problem the user should know about, like attempts to perform a task that he is not permitted to.

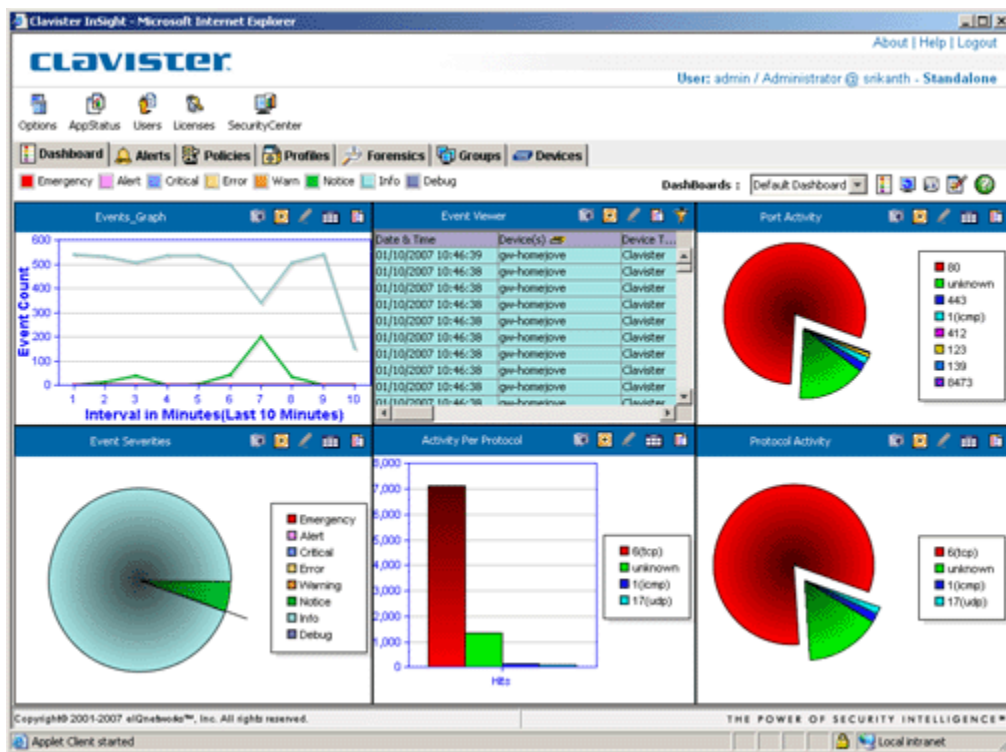
- Notice

A Notice event indicates a normal but significant condition has occurred such as when a user login fails or when a session closes.
- Information

An Information event indicates a significant action that takes place such as when a user successfully logs on or off or creates or renames a mailbox.
- Debug

Debug events indicates all actions performed during an operation and lists all individual steps within each process or task, to pinpoint problems.

Dashboard View



The default Dashboard screen comprises of six distinct frames giving you an overview of the activity in your network.

Each frame has the following options for each monitor.



- ❖ **Snap:** Allows you to take a snap of the monitor and analyze it.

- ❖ **Zoom:** Allows you to maximize the view of the monitor.
- ❖ **Edit:** Allows you to edit the settings of user defined monitors only.
- ❖ **Table:** Place the cursor on the table icon and it displays the information of the selected monitor in a tabular format.

Event Severities Table Data								
	Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
Event Count(Last 60 Minutes)	110.0	187.0	300.0	231.0	88.0	166.0	10.0	266.0

Note: If the number of Graph attributes for a monitor is more than twelve, its corresponding information cannot be shown in tabular format.

- ❖ **List Of Monitors:** Allows you to see the list of default and user defined monitors.

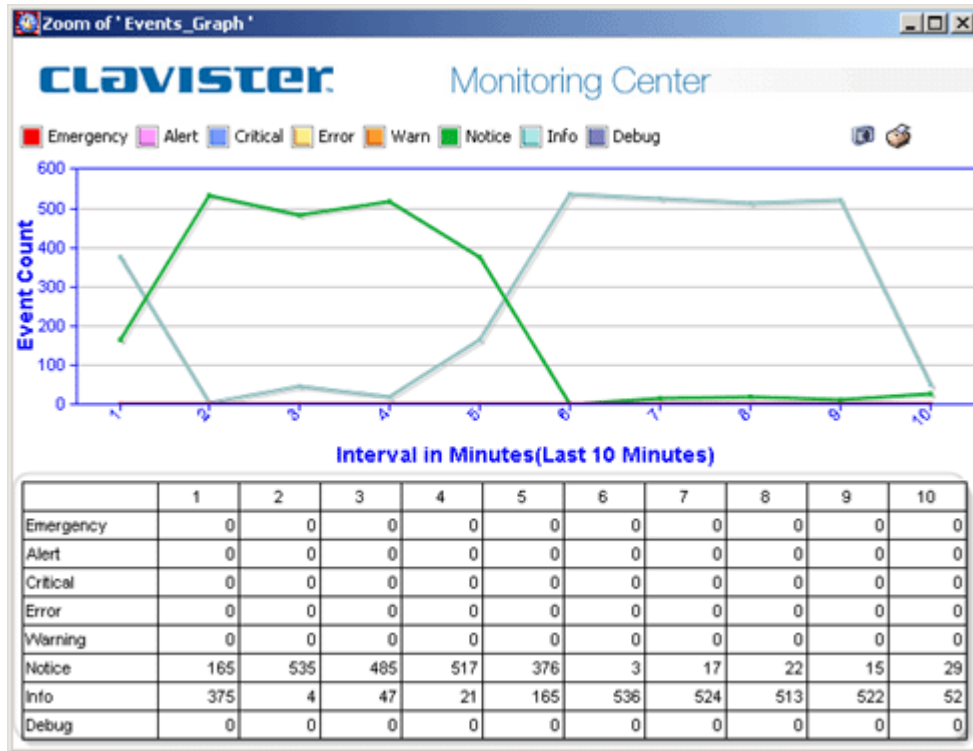


Note: You can change the monitor to be displayed in the each frame by selecting one from the list.

Events Graph

You can view the rate of events that are generated from all the configured devices.

Events Graph View



From this screen, view all event severities occurring for Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug events triggered from the configured devices in the last 10 minutes.

Note: Severity level of the events is listed in the table as integers ranging from 0 to 7.

This graph provides event count details of all severity types from all the configured devices and facilitates you to obtain a quick view on the status of the events that can lead to complications.



Manage Dashboard


A dashboard is a user interface that organizes and presents complex information in a way that is easy to comprehend. Clavister Insight comes with an interactive, user friendly Dashboard comprising of viewing panes—Real-Time Events, Event Graphs, and Alert Graphs...

To change the dashboard view, create your own dashboard view with custom preferences from the Manage Dashboard wizard.

How to Manage?

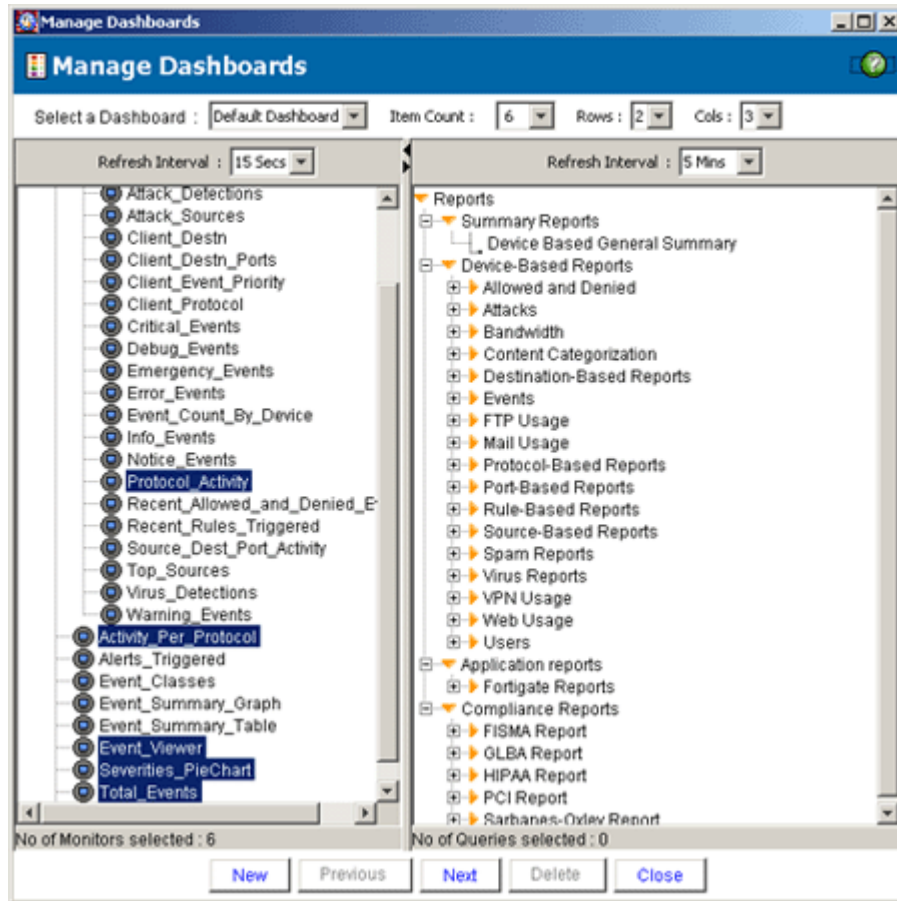
On the dashboard main screen, the Dashboards drop-down lists containing all the dashboard views is available to the user.

To set a view as the default, select from the drop-down list and click the set as default icon . To restore the default dashboard view, click the restore dashboard view icon .

From the dashboard main screen, click the list icon  placed right to the **DashBoards** drop-down list to create a custom dashboard view.

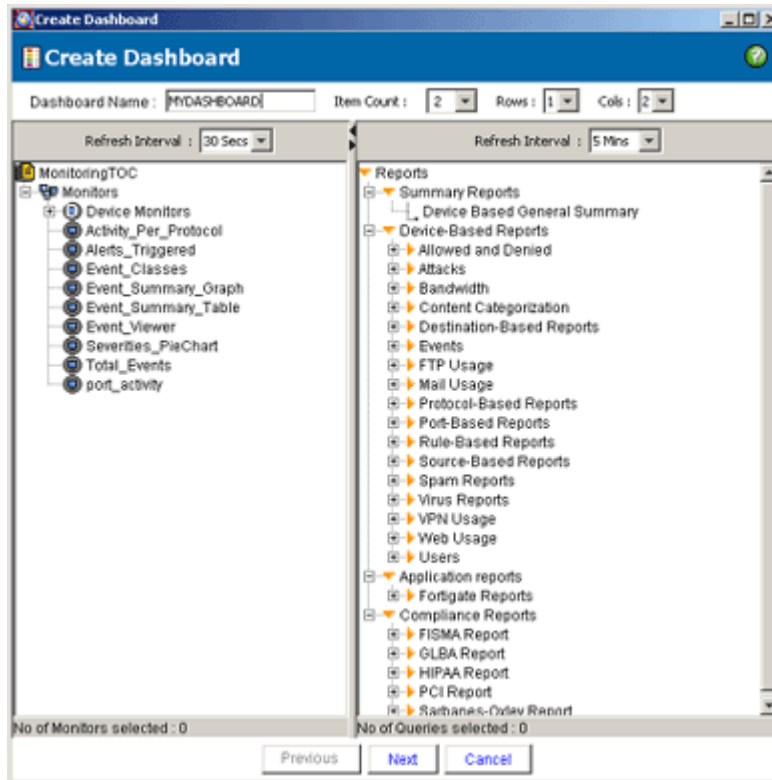


The manage dashboard wizard opens. It highlights the six monitors that are currently set in the dashboard view. You can change the way you want to arrange rows and columns to appear in the view. See the image below.

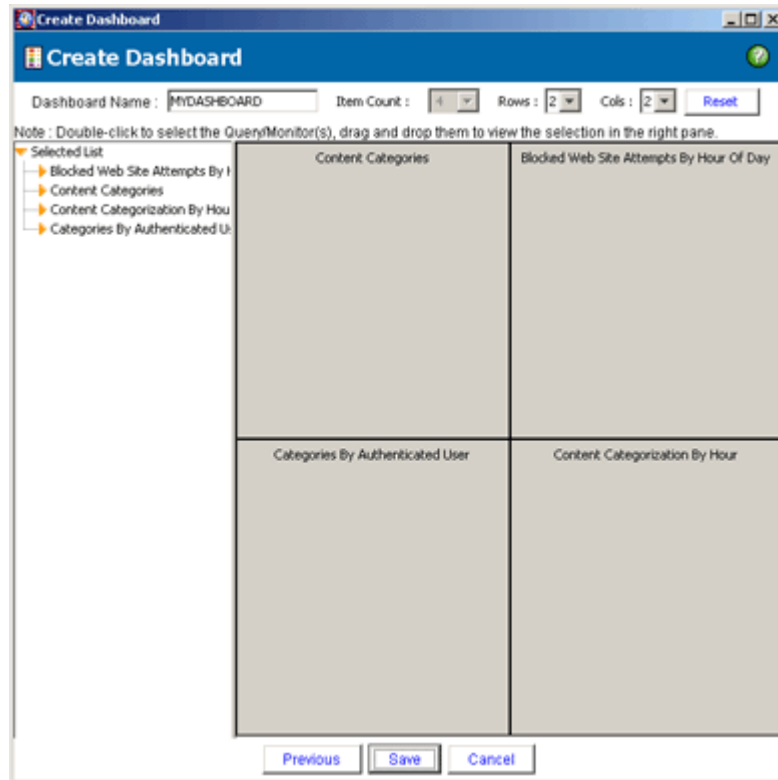



Creating New Dashboard

1. Click on the **New** button from the **Manage Dashboard** window. The Create Dashboard window is displayed.
2. Select from the **Item Count** drop-down list, number of monitors you want to see in the view.
Note: Sum of Monitors and Reports selected must be equal to the Item count.
3. You can change the way you want to arrange rows and columns to appear in the view. For example if you want to see eight monitors in your view, it can be selected as 2 rows and 4 columns or 4 rows and 2 columns.
4. Select the monitors you want to set in the dashboard view from the **Monitoring TOC**.



5. Select the query(s) to generate a report on the selected monitor from the Reports pane.
6. Click **Next** button. Create dashboard wizard displays a custom dashboard based on your selection.
7. Selected **Query/Monitor(s)** list is seen in the left pane. Double-click to choose your selection from the list, drag and drop it in one of the available panes on the right-hand side.
8. Click **Save**. The dashboard view is saved and listed in the dashboards drop-down list.



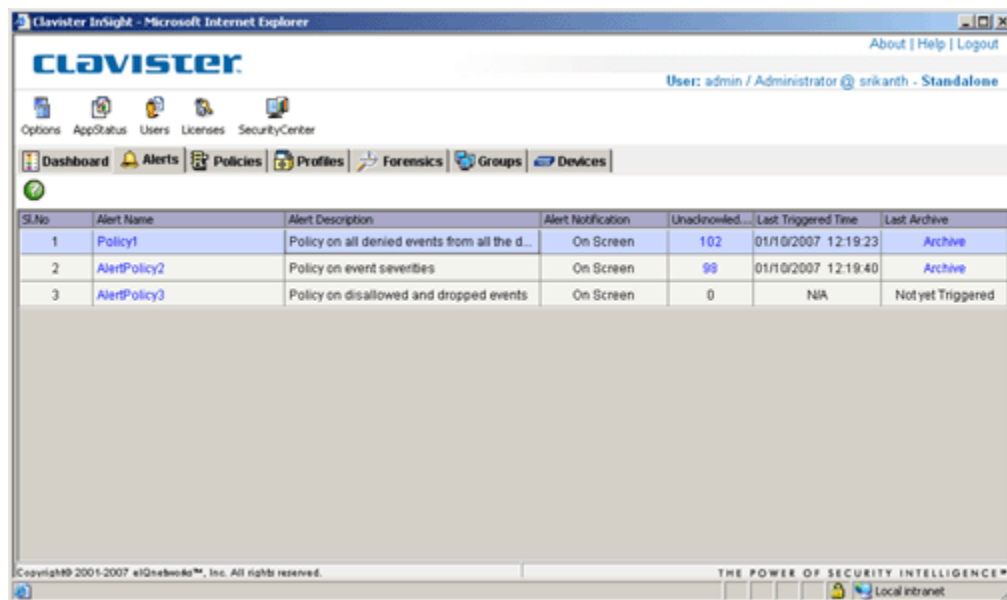
By default, dashboard view is opened in the Run Mode. To change the mode to Design Mode, click the  mode icon, resize the monitors available on your dashboard view and then click on the mode icon to restore the run mode.

Alerts

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, where the information is monitored; others are active, where the information is altered with intent to corrupt or destroy the data or the network itself. The Alerts feature of Clavister Insight provides warning in advance so you can respond proactively.

The Alert Manager displays the list of all the Alerts configured to the Policies. The Alert Name corresponds to the name of the Policy for which it is enabled. The alerts warn you whenever a specified event type or attack activity is detected or if the total number of attack attempts exceeds a specified value.

The Alert Manager



The screenshot shows the Clavister Insight Alerts Manager interface. The page title is "Clavister Insight - Microsoft Internet Explorer". The user is logged in as "admin / Administrator @ srikanth - Standalone". The navigation menu includes Dashboard, Alerts, Policies, Profiles, Forensics, Groups, and Devices. The Alerts section is active, displaying a table with the following data:

Sl.No	Alert Name	Alert Description	Alert Notification	Unacknowled...	Last Triggered Time	Last Archive
1	Policy1	Policy on all denied events from all the d...	On Screen	102	01/10/2007 12:19:23	Archive
2	AlertPolicy2	Policy on event severities	On Screen	99	01/10/2007 12:19:40	Archive
3	AlertPolicy3	Policy on disallowed and dropped events	On Screen	0	N/A	Not yet Triggered

Copyright © 2001-2007 aQnebo™, Inc. All rights reserved. THE POWER OF SECURITY INTELLIGENCE™ Local intranet

Important: A Console user, given the Access Using Console privilege to monitor alerts of a specific user will only see triggered alerts for that user.

An alert Manager displays the following information pertaining to an Alert:

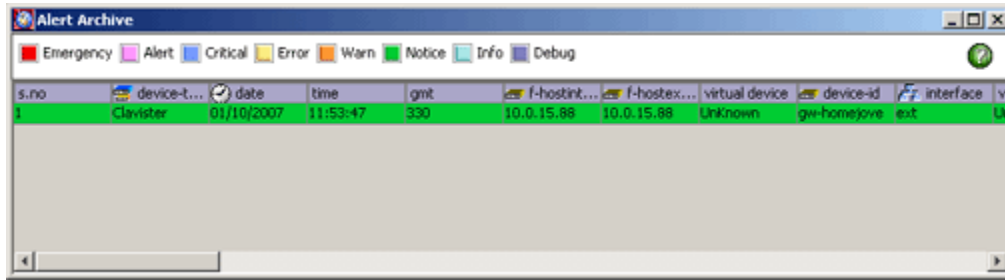
- ❖ **Alert Name:** The Alert name corresponds to the Policy name. For example, if an Alert is configured on a policy called Policy1, the Alert name will also be Policy1.
- ❖ **Alert Description:** Alert description displays the description of the corresponding Policy.
- ❖ **Alert Notification:** This displays the method of Alert notification opted by you in the Policies. You can either notify Alerts via e-mail or by SNMP trap; if none is specified then “on screen” notification is displayed.
- ❖ **Unacknowledged Events:** Once the Alert is triggered, the numbers of events that are filtered through Rules to be a part of the Policy are displayed. As CIS encounters these events they are marked unacknowledged and are displayed here. You can acknowledge each event by clicking on that field (number). With every event you acknowledge the count decreases by one. Alternatively you can acknowledge all events at once. Go to “Alert Events” for details.
- ❖ **Last Triggered Time:** This column displays the date and time when the Alert was last triggered.
- ❖ **Last Archive:** This column informs about the status of the Alert. If the Alert criterion is not met then “Not yet triggered” message is displayed. The triggered Alert is archived and the message shown in that case is “Archive”. You can click on “Archive” to see the corresponding details of the archived Alert. Go to “Alert Archive” for more details.

Alert Events

Once an Alert is triggered, the total count of events which meet the Policy settings are displayed on the ‘**Unacknowledged events**’ column in the main Alert window. Here are the points entailing the use and scope of Alert events:

1. If the Alert has triggered, click on the count displayed in Unacknowledged Events column to open the Alert Events window.
2. The **Alert Events** window displays the Alert Name along with the associated list of Archived events in a timestamp format on the left pane.
3. Select a triggered Archived Event, the corresponding event details like – device type, device ID, Interface, Priority, event code, event type, event category and so on ... are displayed on the right pane.
4. Click the **Acknowledge** button to take notice of that particular event. With every archived event you acknowledge the event count reduces simultaneously on the main Alert window.
5. You can also opt to acknowledge all the triggered events at one go, if you don’t foresee any threat associated with the triggered alert by clicking on the **Acknowledge All** button.

Alert Archive Screen



The screenshot shows a window titled "Alert Archive" with a toolbar containing buttons for Emergency, Alert, Critical, Error, Warn, Notice, Info, and Debug. Below the toolbar is a table with the following data:

s.no	device-t...	date	time	gmt	f-hostint...	f-hostex...	virtual device	device-id	interface	v
1	Clavister	01/10/2007	11:53:47	330	10.0.15.88	10.0.15.88	Unknown	gw-homejve	ext	lt

Note: You can access workbench from any event by double clicking on it.

Workbench

Workbench is a platform to display all the entities attributed to any single event compiled in the report or event viewer along with the respective 'value' details.

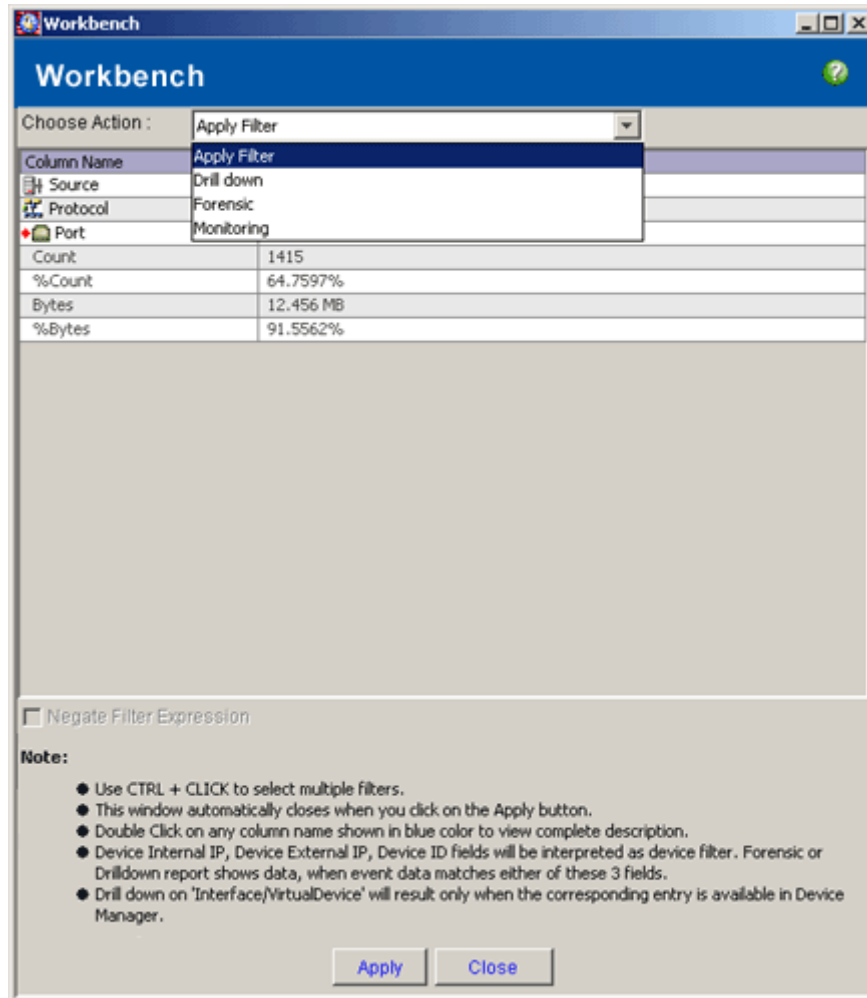
The Event Viewer displays all the real-time events occurring at the devices configured on CIS. You can drill-down and narrow your scope to excavate further details of any event displayed on the event viewer. Right or double-click on any event from the Event Viewer. The Workbench dialog box opens and displays the details associated with the selected event.

Other than Event Viewer, users can launch workbench from different modules of the application:

- ❖ Monitoring
- ❖ Reporting
- ❖ Forensics
- ❖ Alerts

The following options are available on the workbench combo-box to obtain further details of the selected columns (entities):

- ❖ Monitoring
- ❖ Forensic
- ❖ Apply Filter
- ❖ Drill Down



Note: You can drill-down only up to level 1 by using Drill Down option and **Forensic** option allows you to drill-down up to level 2.

Editing Event Attribute Values

You can edit the event attribute values from the Workbench. This saves the cumbersome task of going back to the Events and sifting through reams of data to select the desired event value. Follow the steps given below to edit attribute values and perform the required action on them.

1. Double-click on the desired event to open the Workbench.
2. Select the action to be performed from the **Choose Action** combo-box.

3. Double-click on the event attribute value that you want to edit. Modify the value and press enter to save the edited value.
4. Click the **Apply** button for executing the action with the edited value.

Note: You can perform the Drill-down and Forensic drill down action on IP address and Port range by entering the specific range in the respective value columns.

Monitoring

Select the action type as Monitoring from the Workbench to view further details of the events associated with the selected column(s) (entities) bearing specific values.

1. Select Column Name(s) you want to view the details for.
2. Now click on the Apply button. Only those events which are associated with the chosen column(s) (entities) are displayed in a new window.

Date & Time	Device(s)	Device T...	Group	Virtual D...	Interface	User Na
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:34	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:33	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:59:33	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:39	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown
01/10/2007 16:57:40	gw-homejove	Clavister	Default Group	Unknown	int	Unknown

Applied Filter Expression
Device=gw-homejove

By selecting the Monitoring action from the Workbench, you can further drill information on the desired entities and obtain the events view on them. By right or double clicking any event from the Events View, you can again access the Workbench and excavate further details. You can continue excavating into events until you find the required details as you can go back to the workbench from any event on the Events View window.

Event Cache For Devices

For events generated from Cisco PIX/ASA, Cisco IOS/CatOS, FortiGate, NetScreen and TopLayer devices, double-clicking on Event ID attribute will result in opening an event cache URL page containing the Error Message description, Explanation and Recommended Action that should be taken if the event messages persist from the same source.

You can also access the event cache by choosing Start -> Programs -> Clavister Insight v4.6-> Event Cache Index.

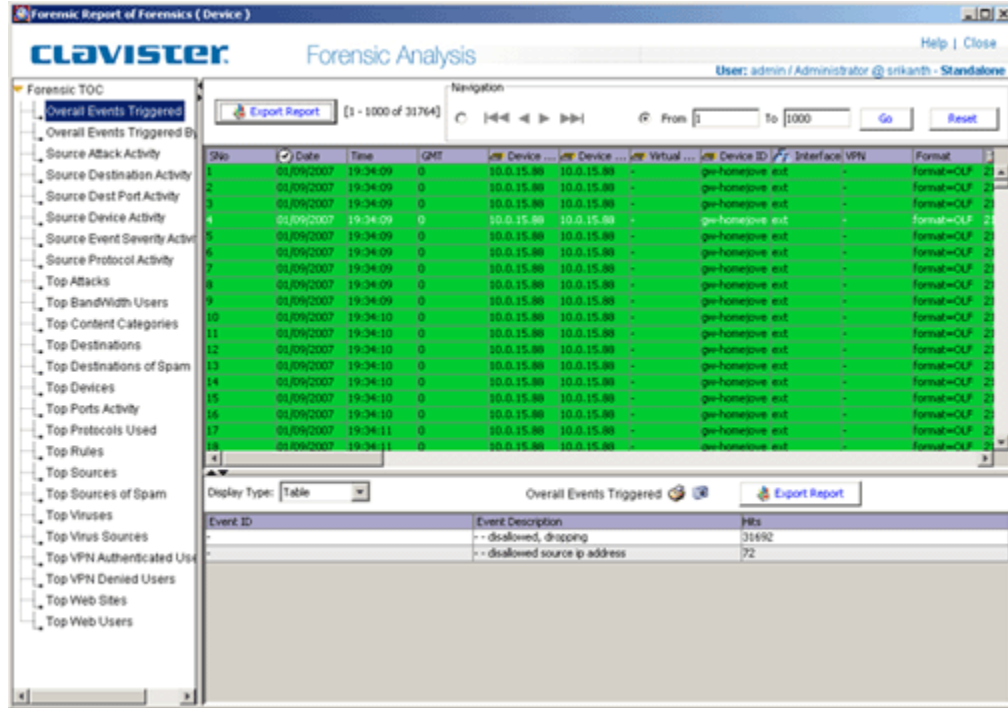
Important: In case of Cisco IOS device, to view the event details associated with the selected Event ID, manually create the eventcacheURL.ext file in the application path containing the information of CISCO Network Security Database Documentation in the following format: 29~<URL of CISCO Network Security Database Documentation>.

Forensic

Select the action type as Forensic from the workbench combo-box to see the Forensic report on the selected event attribute.

Select any event attribute from the workbench column and then click the Apply button. A window opens displaying the forensic report based on the applied filter expression (event attribute), for example, event code, protocol, event id and so on.

You can investigate on the event details by using the Forensic option up to two levels. The Forensic report generated from the workbench is similar to the one generated from the Forensics main module.



The Forensic report on the selected filter expression can be exported to desired location in a customized view. Use the following options to customize your report view:

- ❖ **From-To** - To specify records within a range. By default only 25 records are displayed in the forensic drill-down report. To specify a different range, you need to modify the number of records from forensicDrillCol.ext file found in the installation path.

Note: The specified range cannot exceed more than 1000 records.

- ❖ **Export Report** - You can export the forensic report to a specific location and in HTML or Text format. To customize the view of the exported report, select the fields you want to include in the report that is being exported.

Information: Values in a report saved in text format are separated by a comma separator.

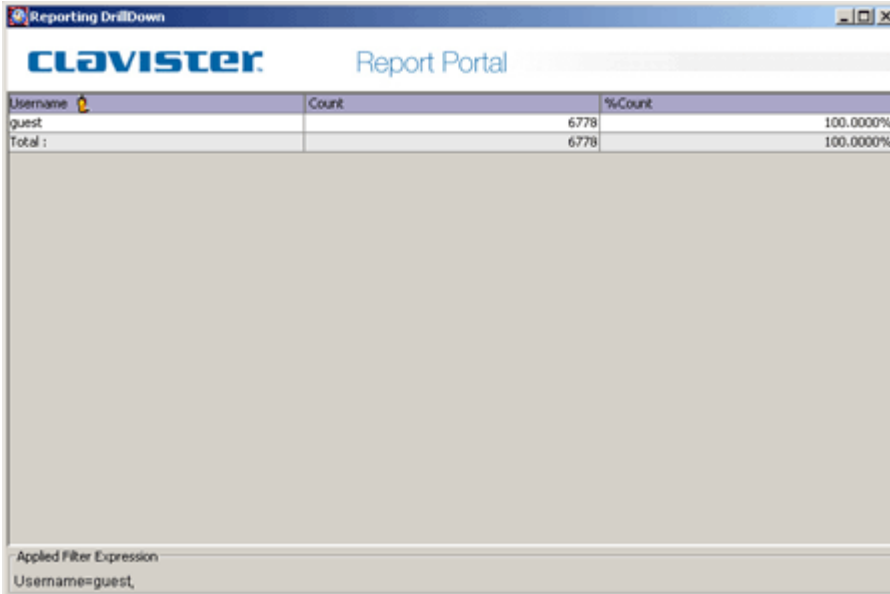
Forensic drill-down from Workbench is almost similar to the main Forensic Search module, in addition to the regular features it also supports the regular expressions like- '*' . For example, you can edit the attribute value and insert a regular expression to track down the events that contain a common string in their event attribute values.

This support is available for forensic search from Workbench for following filters:

- ❖ Content Category
- ❖ Spam Source Mail
- ❖ Spam Destination Mail
- ❖ URL

Apply Filter

On the Workbench selecting the action type as Apply Filter provides the ability to drill-down into a report to obtain further details. This is extremely useful when you want to study the behavior of a specific user or find out what contributed to the numbers present in the reports.



The screenshot shows a window titled "Reporting DrillDown" with the Clavister logo and "Report Portal" header. It displays a table with the following data:

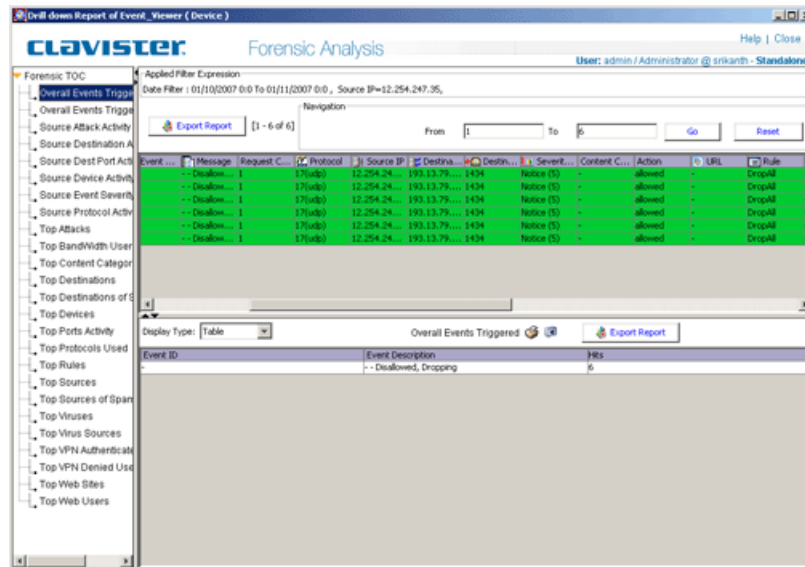
Username	Count	%Count
guest	6778	100.0000%
Total :	6778	100.0000%

At the bottom of the window, the "Applied Filter Expression" is shown as "Username=guest,".

You can select the event attributes from the workbench column, apply them as filters and generate a report on it. You can perform hierarchical investigation only up to one level. After accessing the workbench the second time from the consecutive report, you cannot delve and investigate any further.

Drill Down

From the Choose Action combo-box, select the Drill Down option to drill down further on the event attributes. This is extremely useful when you want to generate a quick report and find out what contributed to the numbers present in the reports.



Information: As the Drill-down takes place on the data present in the Forensic Summary files, therefore it is faster than the forensic drill-down.

You can investigate on the event details by using the Drill Down option only up to first level. After you access the workbench the second time from the consecutive Drill Down report, you cannot perform investigate any further.

Note:

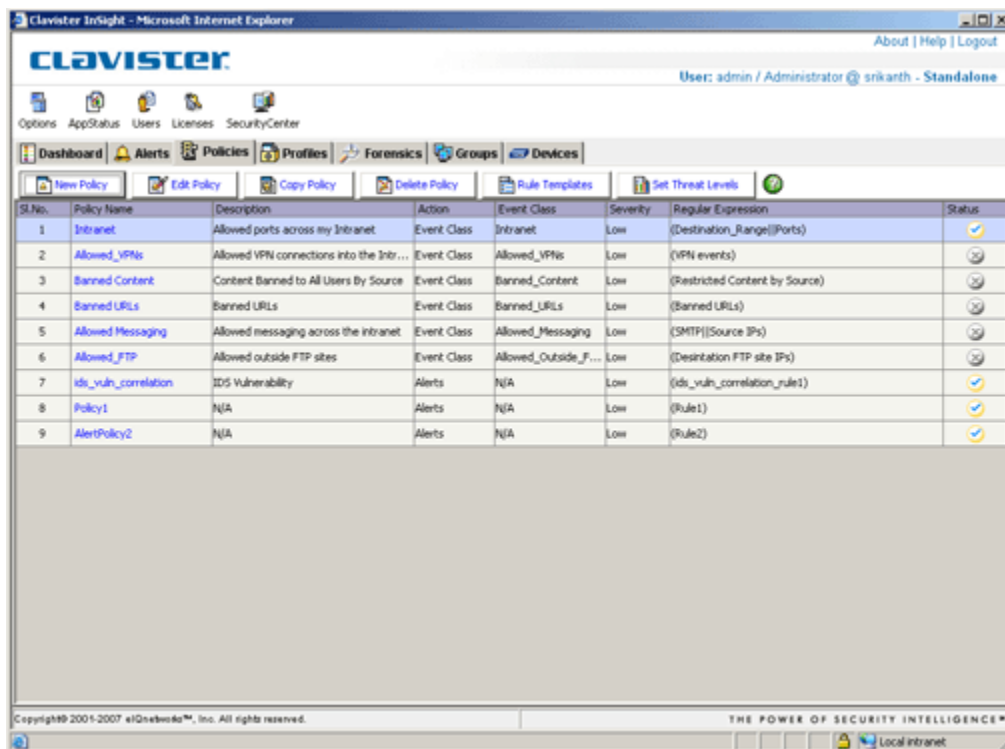
- ❖ For events occurring on devices that belong to more than one group, drill-down cannot be performed.
- ❖ Filter attributes in grey color (fading) background cannot be selected to drill-down further. For example Date & Time, Event Description and Native Log filter attributes cannot be selected in the workbench image seen on this page.
- ❖ Double-click on filter attributes shown in blue color to see the description in a dialog box.

To negate the filter in the reports, select the Negate Filter check box on the workbench.

Policies

In simple words, a Policy is a systematic set of statements to govern the upcoming decisions and actions of the user.

In CIS, a policy is a formal set of rules to define the course of action that the user needs to take under specific circumstances. A rule can dictate-- which devices to consider, what event type to filter or negate, which entities with what values to add... The user can associate a severity level to the Policy created. A policy is founded on the customized device based rules or the existing rule templates. On implementation of a policy, the user can choose to either trigger an alert notification, or simply classify the Policy under an Event class by associating it to a report query. A user can add, edit, copy or delete a Policy.



S.No.	Policy Name	Description	Action	Event Class	Severity	Regular Expression	Status
1	Intranet	Allowed ports across my Intranet	Event Class	Intranet	Low	{(Destination_Range){Ports}}	✓
2	Allowed_VPNs	Allowed VPN connections into the Intranet	Event Class	Allowed_VPNs	Low	{VPN events}	⊘
3	Banned_Content	Content Banned to All Users By Source	Event Class	Banned_Content	Low	{(Restricted Content by Source)}	⊘
4	Banned_URLs	Banned URLs	Event Class	Banned_URLs	Low	{(Banned URLs)}	⊘
5	Allowed_Messaging	Allowed messaging across the intranet	Event Class	Allowed_Messaging	Low	{SMTP{Source IPs}}	⊘
6	Allowed_FTP	Allowed outside FTP sites	Event Class	Allowed_Outside_F...	Low	{(Desination FTP site IPs)}	⊘
7	ids_vuln_correlation	IDS Vulnerability	Alerts	N/A	Low	{ids_vuln_correlation_rule1}	✓
8	Policy1	N/A	Alerts	N/A	Low	{(Rule1)}	✓
9	AlertPolicy2	N/A	Alerts	N/A	Low	{(Rule2)}	✓

The main menu bar of the Policy window contains the buttons to add a New Policy, Edit Policy, Copy Policy and Delete Policy. It also includes a button to create Rule Templates.

As and when you create and save a Policy the related details are listed on the main screen of this window. The following bottom line information is displayed in the columns:

1. Name of the Policy
2. The description of the Policy as entered by the user while creating it
3. The type of action to take on implementation of the Policy as prescribed by the user
4. The Event Class details
5. The Severity level associated with the Policy, as marked by the user while creating it
6. The regular expression, depicting the Rule(s) and how they are associated with the Policy by using operators

Create Policy

1. Click **New Policy** from the Policies main window, the **Create Policy** window opens.
2. Enter a Policy Name.
3. Enter a short description of the Policy properties for future reference.
4. Associate a Severity level to the Policy. The severity level is reflected in the main Policy window, once you create and save the Policy. The options available are as follows:
 - ❖ Low
 - ❖ Medium
 - ❖ High.
5. The Policies are dependant on rules. You can assign rules to a policy from two different sources, they are as follows:
 - ❖ [Load Rule from the template.](#)
 - ❖ [Create New Rule](#)
6. Before creating a Policy, define what mode of action to take on implementation for that Policy. The Type of Actions that a user can take are as follows:

- ❖ **Trigger Alert:** Select this option to notify the successful execution of this Policy through an e-mail. Click on the Alert Delivery button to configure the e-mail options. Click [here](#) to know "How to configure Alert Delivery via e-mail"?
- ❖ **Event Class:** An Event Class represents one type of events used by CIS for alerting and reporting purposes. You can classify the events based on specific network areas (DMZ, internal or external networks), operating systems, IDS or IPS systems by grouping them under one Event Class.

Here is how to set Event Class:

1. Select Event Class.
2. Enter a unique Event Class name.
3. Click the Configure button. The Configure window opens. Select the Threat level and furnish the threat level from the in-built list. The available options are:
 - ❖ Emergency
 - ❖ Alert
 - ❖ Critical
 - ❖ Error
 - ❖ Warning
 - ❖ Notice
 - ❖ Info
 - ❖ Debug
4. Select the **Update Database for Selected Categories** option to save the matching events in the Database. Select the event categories that you want to send to the database.
5. Press Ctrl + Select the category(s) that you want to send to the database under the created **Event Class**.
6. Click **Save** to save the Event Class, else **Close** the window.

Note:

- ❖ Selection of Database correlation will increase database size because all the matched events are saved in the database.
- ❖ By Configuring the Event Class on a Policy you can generate Reports, both complete and selective as defined in the Event Class settings
- ❖ An Alert action is based on the Rule expression; where as the Event Class is independent of it.

- ❖ **Negation:** Use this operator to negate or exclude a particular Rule and apply the rest to the Policy. The negated Rule appears prefixed with an exclamation symbol -"!" in the existing rules list.
- ❖ **And:** Use the "And" operator to select and combine more than one Rule to apply in unison to the Policy.
 - Select a Rule from the existing rules list. For example - Select RULE 1.
 - Click the "And" operator.
 - Select the supplementary Rule from the existing rules list. For example, select RULE 2.
 - Click Finish.
 - The Operator settings appear in the Summary text box. In this case, (RULE1&&RULE2). This combines both the rules and both will be executed when their respective criteria is met.

The "And" operator is denoted by an ampersand symbol (&&)

 - Click Clear to undo the Operator settings.
- ❖ **Or:** Use the "Or" operator to select two Rules and apply one of them to the Policy.
 - Select a Rule from the existing rules list. For example - Select RULE 1.
 - Click the "Or" operator.
 - Select the complementary Rule from the existing rules list. For example-select RULE 2.
 - Click Finish.
 - The Operator settings appear in the Summary text box. In this case - (RULE1||RULE2). Now both the rules are combined and the one which meets the criteria first will be executed and the other stands void.

The "Or" operator is denoted by a pipe (vertical bar) symbol (||)

 - Click Clear to undo the Operator settings.

Press the Ctrl key and select the more than one Rule at a time from the existing Rules list and click the operator you want to apply from the available operators except the negate filter, as the Negate operator works on one filter at a time.

By default the "Or" Operator is applied to the filter.

- ❖ Set Precedence: Use Set Precedence to establish an order of importance to execute the rules. This will set the priority on the rules in a descending order. Follow the steps given below to set precedence on the Rules :
 - Select a Rule that is of utmost importance to be considered in the Policy. Let's say RULE 1 and then Set Precedence on it.
 - Subsequently, after RULE1 if your want to consider either RULE3 or RULE4. Apply a "Or" operator on RULE3 and RULE4. Select RULE3|RULE4 from the existing rules and Set Precedence on that.
 - Next, Lets assume you set Precedence on RULE2.
 - The Set Precedence feature will establish an order of importance to execute these selected rules. The order is summarized in the Precedence Order text box. In this case the Precedence Order will appear as:
RULE1, RULE3|RULE4, RULE2
The importance associated is in a descending order:
RULE1 > RULE3|RULE4 > RULE2

Note: You can Set Precedence on the Rules even after applying the operators.

Create Policy

Policy Name : POLICY_ONE Severity: Low Medium High

Policy Description :

Mode of Action:

Trigger Alert: Event Class:

Note: An Alert action is based on the Rule expression, while Event Class is independent of it.

Status	Rule Name	Description	Base	Filter Expression
<input checked="" type="checkbox"/>	Rule_A	On the allowed and denie...	Device	{Action={Allowed,}}
<input checked="" type="checkbox"/>	Rule_B	On any attack type	Device	{Attack Type={All}}{Attack Type={All}}

Existing Rules:

- Rule_A
- Rule_B

Available Operations:

Precedence Order : Rule_A,Rule_B Alert Correlation Interval: 30 Sec

Summary:

(Rule_A)(Rule_B)

- Set an Alert Correlation interval between Rules.

Note: When the Rule patterns or the data is complex, the Correlation Interval might timeout while executing these Rules.

- Click the Finish button to end the Rules setting on your Policy.
- The Summary box displays the Rules and the respective operators applied.

Note: The expressions on Rules which appear in the summary box can be as complex as you want them to be, in order to get down to the crux of the Rules for the Policy.

For Example:

RULE1: Based on Device Destination Port and IP range

((Destination Port= [306,]&&Destination IP= [10.00.79.01-10.00.79.15,])

RULE2: Based on only Device Destination port

(Destination Port= [402,])

RULE3: Based on Device Source IP

(Source IP= [10.78.00.97,])

Now you can set an expression like the following where you negate RULE1 and add RULE2 or negate RULE3.

((! RULE1&&RULE2) ||! RULE3)

10. To undo the Rules settings click the Clear button. This will clear the Summary details and you can apply new settings.
11. Click Save. The saved Policy is populated in the Policy main window along with its allied details like-- Description, Action, Event Class, Severity and Regular Expression.
12. Else, Click Cancel to abort the task.

Load Rule from the template

1. Click the Load Rule from Templates button from the Create Policy window.
2. The list of custom made Rule Templates available to load appears.
3. Select the Rule Template from the list that you want to load. To load more than one templates press the Ctrl key and select the Rule templates.
4. Click Finish to complete loading the rule template to the Policy or click Close to abort the task.
5. The Loaded Rule finally appears in the Create Policy window and is available to use in the Policy.

Create New Rule

- ❖ [Device Based Rule](#)

Edit Policy

1. Select the Policy that you want to edit from the Policy list from the main Policies window.
2. Click on the Edit Policy button.
3. The Create Policy window opens.
4. The Policy name is non-editable.
5. You can edit the description of the Policy.

6. Make the necessary changes-- you can edit all the Rules created in the list and also load/delete rules from the templates.
7. You can change the way the operators are working on the sets of filters.
8. You can also edit the type of action to take on implementation of this Policy.
9. Edit the Event Class and the associated queries if needed.
10. Click Save to save the edited Policy.
11. Click Previous to revert back to the earlier screen to alter or recheck the filter settings.
12. Click Cancel to abort the task.

Make Copy of the Policy

1. Select the Policy to make a copy of, from the Policy list on the main Policies window.
2. Click on the Copy Policy button from the main Policies menu bar.
3. The copy of the Policy is saved with a prefix "Copy_of" followed by its original name in the main Policies window.
4. You can edit the name of the Copy of the Policy created.
5. You can edit the Rules and the settings of the Copy of Policy created.

Delete Policy

1. Select the Policy to delete from the main Policies window.
2. Click the Delete Policy button on the main menu bar.
3. The dialog box prompts you for a confirmation. Click Yes to delete, Cancel to abort the task.
4. The Policy is permanently deleted from the CIS.

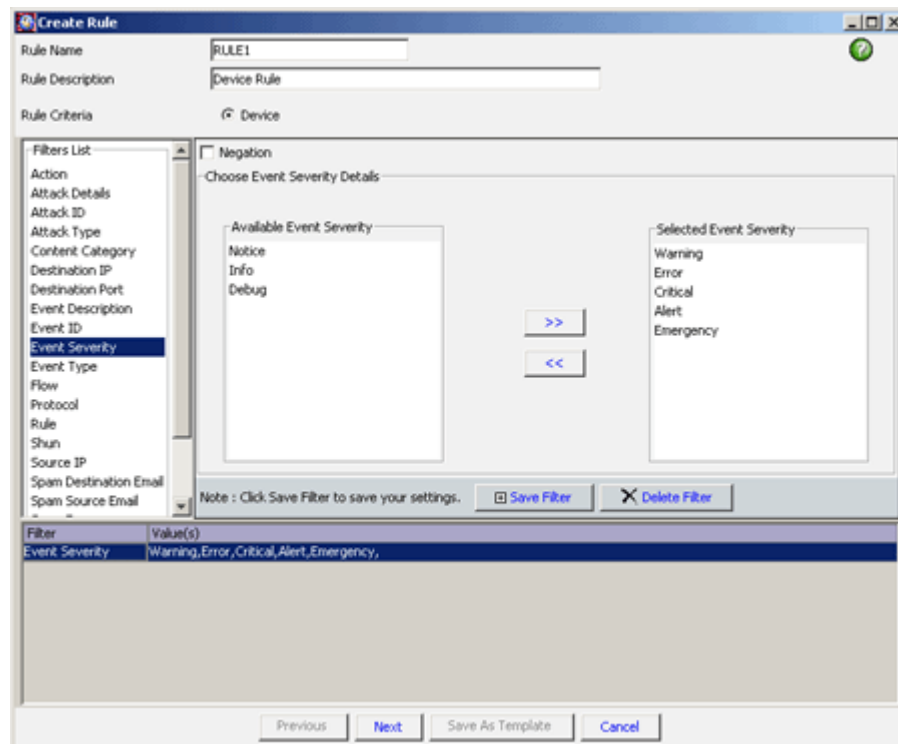
Creating Device based Rule

1. On the Create Policy window, click New Rule (Device) button.
2. The Create Rule window opens
3. Enter an appropriate Rule Name.
4. Enter a short but apt description about the rule in the Rule Description box.

5. A comprehensive Device based Filter List is available on the left hand side column of the Create Rule window. The list comprises of the following filters:

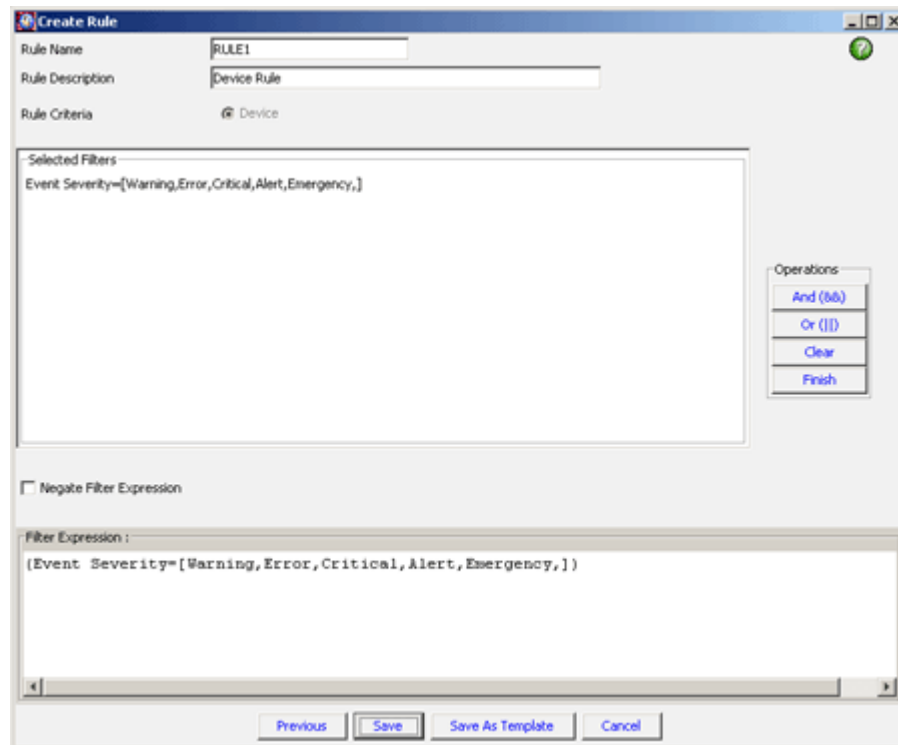
- ❖ [Action](#)
- ❖ [Source IP](#)
- ❖ [Destination IP](#)
- ❖ [Destination Port](#)
- ❖ [Protocol](#)
- ❖ [Event Severity](#)
- ❖ [Event Type](#)
- ❖ [Event ID](#)
- ❖ [Attack Type](#)
- ❖ [Attack ID](#)
- ❖ [Virus Type](#)
- ❖ [Virus ID](#)
- ❖ [URL](#)
- ❖ [Rule](#)
- ❖ [Content Category](#)
- ❖ [Flow](#)
- ❖ [Event Description](#)
- ❖ [Attack Details](#)
- ❖ [Shun](#)
- ❖ [Spam Destination Email](#)
- ❖ [Spam Source Email](#)
- ❖ [Spam Type](#)

6. Select a Filter to apply to the rule.



7. If you want to negate the selected filter, select the Negation check box.
8. Fill in all the details pertaining to the selected filter. The gist of the filter settings appear on the right hand corner box.
9. Click on the Save Filter button to save the settings, or click Delete Filter to cancel the filter settings.

10. Repeat the above steps to add more filters to the rule.
11. An executive summary of the filters created appears on a horizontal bottom box displaying the Filter names and their respective values.
12. Click the Next button to continue with the Filter settings or click Cancel to abort the task.
13. The Next screen displays all the created filters available to apply to the rule.



14. You can use the operators "And" and "Or" to select the filters in combinations or to choose one of the selected two. Press Ctrl and select the filters and then specify the operator.

The "And" operator is denoted by an ampersand symbol (&) in the filter expressions.

The "Or" operator is denoted by a vertical bar (pipe) symbol (|) in the expressions.

By default the "Or" Operator is applied to the filter.

15. The Filter Expression summary is displayed in the bottom most horizontal box. The summary displays the way the operators are applied on the filters using the "&" and "|" symbols.

Note: The filter expressions on Rules can be as complex as you want them to be, in order to get down to the crux of the Rules.

For Example: You can negate a Destination Port and a Destination IP Range or particular source IP. The filter expression in this case will be as follows:

```
! ((Destination Port= [402,] &&Destination IP= [10.00.79.01-10.00.79.15,]) ||Source IP= [125.99.78.90,])
```

16. Use the Negate expression to exclude the set filter expression on the rule. The negated filter expression is prefixed with an exclamation mark-"!"
17. Use the Clear button to undo the operator settings on the filter expressions.
18. Click Finish to accept the Filter Expression.
19. Click the Previous button to revert back to the earlier page to add or modify the filter settings.
20. Click Save to save the rule under the newly created Rules.
21. Click Save As Template to save the rule as a template to load in future policies.

The Rule created is in the disabled state, therefore it is imperative to enable it first from the Configure Rule option from the Create Policy window.

22. Click the Cancel button to abort the task.

Applying filters to a Rule

As described above there is an in-built list of device filters available to apply on the rule. Let us consider each filter at a time and figure out how they can be applied to the Rule.

Action

1. Select either Allowed or Denied to filter events that are allowed or denied in a device.
2. Click the Save Filter button. The filter is added to the Filter list.

3. Click the Delete Filter button to clear the settings.

Source IP

1. Enter the **Source IP/Name** of the device you want to filter and report on only those events originating from the specified source.
2. To filter on events originating simultaneously from a series of devices, specify the IP Range by selecting the **Source IP Range** check box.
3. Select the option **Any** to consider all the source IP addresses.
4. Add the **Source IP/Name** by clicking the **Add** button.
5. Click the **Add/Edit** button. The filter is added to the Filter list.


Destination IP

1. Enter the **Destination IP/Name** of the device you want to filter and report on only those events having the specified Destination IP/Name.
2. To filter on events from a series of devices at a time, provide the IP Range by selecting the **Destination IP Range** check box.
3. Add the Destination IP/Name of the device or the range by clicking the **Add** button.
4. Select the option **Any** to consider all the destination IP addresses.
5. Click the **Add/Edit** button. The filter is added to the Filter list.

Destination Port


1. Enter the destination port number you want to filter for an event displayed in the **Event Viewer** console.
2. To filter on events from a series of devices at a time, provide the IP Range by selecting the **Destination Port Range** check box.
3. Click **Add**, and the port number you entered is added to the list.
4. Select the option **Any** to consider all the destination ports.
5. Click the **Add/Edit** button. The filter is added to the Filter list.

Protocols


1. Select the protocols you want to filter and click  to move them into the Selected Protocols list. You can also add new protocols.
2. You can add a new protocol by clicking the Add button.

3. Click the Add/Edit button. The filter is added to the Filter list.


Events Severity

1. Select the Event Severity from the following list:
 - ❖ Emergency
 - ❖ Alert
 - ❖ Critical
 - ❖ Error
 - ❖ Warning
 - ❖ Notice
 - ❖ Information
 - ❖ Debug
2. Select the protocols you want to filter and click  to move them into the Selected Protocols list.
3. You can also add a new severity by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.


Events Type

1. Select the Event Types from the following list:
 - ❖ TRAFFIC
 - ❖ IPSEC
 - ❖ DROP
 - ❖ BLOCKED
 - ❖ IDS
 - ❖ VPN
 - ❖ SYSTEM
2. Select the event types you want to filter and click  to move them into the selected event type list.
3. You can also add a new event type by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.

Event ID


1. Select the Event IDs from the available list.
2. Select the event IDs you want to filter and click  to move them into the selected ID list.
3. You can also add a new event ID by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.

Attack Type


1. Select the Attack Types from the available list.
2. Select the attack type you want to filter and click  to move them into the selected attack type list.

3. You can also add a new attack type by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.


Attack ID

1. Select the Attack IDs from the available list.
2. Select the attack IDs you want to filter and click  to move them into the selected attack ID list.
3. You can also add a new attack ID by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.


Virus Type

1. Select the Virus Types from the available list.
2. Select the virus types you want to filter and click  to move them into the selected virus type list.
3. You can also add a new virus type by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.


Virus ID

1. Select the Virus IDs from the available list.
2. Select the virus IDs you want to filter and click  to move them into the selected virus ID list.
3. You can also add a new virus ID by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.

URL


1. Select the URLs from the available list.
2. Select the URLs you want to filter and click  to move them into the selected URL's list.
3. You can also add a new URL by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.

Rule

1. Select the rules from the Available list.
2. Select the rules you want to filter and click  to move them into the selected rule list.
3. You can also add a new rule by clicking the Add button.

4. Click the Add/Edit button. The filter is added to the Filter list.

Content Category

1. Select the Content Categories from the available list.
2. Select the content categories you want to filter and click  to move them into the selected content category list.
3. You can also add a new content category by clicking the Add button.
4. Click the Add/Edit button. The filter is added to the Filter list.

Flow

1. Select either Inbound or outbound to filter events that are allowed or denied in a device.
2. Click the Add/Edit button. The filter is added to the Filter list.



Set your device interfaces correctly from the Devices/Groups user interface for this filter to work properly.

Event Description

1. Enter the event description you want to filter in the Event Description box. You can also use wild card '*' to filter any specific word or sentence in the description.
2. Click Add/Edit Filter button. The filter is added to the Filter list.

Attack Details

1. Enter the details of the attack to filter in the Attack Details box. You can also use wild card '*' to filter any common string in the description.
2. Click the Save Filter button. The filter is added to the Filter list.
3. Click the Delete Filter button to clear the settings.

Shun

1. Select Yes to filter Shun events or No to ignore Shun events occurring at the device(s).
2. Click the Save Filter button. The filter is added to the Filter list.

3. Click the Delete Filter button to clear the settings.


Spam Destination Email

1. Enter the email address of the Spam Destination in the Spam Destination Email text box. You can also use wild card '*' to filter any common string.
2. Click the Save Filter button. The filter is added to the Filter list.
3. Click the Delete Filter button to clear the settings.

Spam Source Email

1. Enter the email address of the Spam Source in the Spam source Email text box. You can also use wild card '*' to filter any common string.
2. Click the Save Filter button. The filter is added to the Filter list.
3. Click the Delete Filter button to clear the settings.

Spam Type

1. Select the Virus Types from the available list.
2. Select the Spam types to filter from the available entities list and click  to move them into the selected entities list.
3. Click the Save Filter button. The filter is added to the Filter list.
4. Click the Delete Filter button to clear the settings.

Editing a Device based Rule

1. Select the Rule that you want to edit from the Rule list populated on the Create Policy window. The column Base identifies whether the Rule is based on a Device or Messaging Server.
2. Click on the Edit Rule button from the Create Policy menu bar.
3. If you have selected a Device based rule to edit, the corresponding window opens.
4. The Rule name is non-editable.
5. You can edit the description of the Rule.
6. Make the necessary changes-- you can edit the settings on all the filters available in the list and also add new filters.
7. Click the next button to proceed with editing process, else click the Cancel button to abort the task.

8. On the next screen if needed, you can change the way the operators are working on the sets of filters.
9. Click Save to save the edited Rule on the Create Policy window
10. Click Save As Template to save the edited rule as a template in the Rule Templates repository accessible from the Policies main window.
11. Click Previous to revert to the earlier screen to alter or recheck the filter settings.
12. Click Cancel to abort the task.

Making a Copy of the Device based Rule

1. Select the Device based Rule to make a copy of, from the Rule list populated on the Create Policy window. The column Base identifies whether the Rule is based on a Device or Messaging Server.
2. Click on the Copy Rule button from the Create Policy menu bar.
3. A copy of the selected rule is created.
4. The copy of the Device Rule is saved with a prefix "Copy_of_" followed by its original name.
5. You can edit the name and the description of the copy of the Device Rule.
6. You can edit any or all the Device filter settings followed by the operator settings pertaining to the original Device Rule and can also add new Device filters.
7. Click Save to save the Copy of the Device Rule on the Create Policy window
8. Click Save As Template to save the Copy of the Device Rule as a template in the Rule Templates repository accessible from the Policies main window.
9. Click Previous to revert to the earlier screen to alter or recheck the Device filters settings.
10. Click Cancel to abort the task.

Deleting Device based Rule

1. Select the Rule to delete from the Rule list populated on the Create Policy window.
2. Click the Delete Rule button from the Create Policy menu bar.
3. The dialog box prompts you for a confirmation. Click Yes to delete, Cancel to abort the task.
4. The Rule will be permanently deleted from the Policy.

Configuring a Device based Rule

The Rule is created in a disabled state therefore; you ought to enable it first in order to apply it to the Policy.

1. Select the Device Rule that is in disabled state, from the Rule list populated on the Create Policy window.
2. Click on the Configure Rule button on the Create Policy menu bar.
3. The Configure Rule window opens.
4. The window displays the name of the Device Rule along with all the Devices licensed to the CIS application.
5. From the complete list of licensed Devices select a Device(s) to configure the rule on.
6. Set a threshold value on the Rule.
7. Set the Refresh interval by selecting a value from the drop-down list.
8. Select Correlation to establish correlation between the selected Device(s).
9. Click Set Correlation button, the Set Correlation window opens.
10. Select the Devices(s) to correlate to the Device selected on the previous window.
11. Enter a Correlation Threshold value.
12. Click Save to save the correlation settings, else click cancel to abort the task.
13. The Created Device Rule is now configured and is ready to apply on the Policy.

Alert Delivery

When an alert is generated, you can view it straight away on the Alert Manager by leaving the Alert Notification check box clear in the Configure Alert window or alternatively have it delivered by using any one or both the ways of notification, they are:

- ❖ E-mail
- ❖ SNMP Trap

The Alert Delivery Screen

E-mail Notification

Select the E-mail check box for receiving alerts via e-mail. You can choose to not to include events in the generated alert. Also you can select to include events in the body of the e-mail or as an attachment. The alert details will be attached as an HTML file.

Select any one of the options given below:

- ❖ Do Not Include Events
- ❖ Include Events In Body
- ❖ Include Events as Attachment

Leave the check box clear and the alerts notified through e-mail will contain only the time, alert name, alert description, and a message.



An alert message can be configured to be sent in either HTML or Text format.

E-mail Details

You can set the time period with in which if an alert is generated, it should be notified to a specific e-mail address.

Follow the steps described below to add an e-mail recipient:

1. Enter the time **From** to time **To** in the hh:mm format and the recipient's e-mail address. If an alert is generated within the specified time bounds, the alert message will be sent to the specified recipient.

2. Click the **Add** button. The e-mail ID is added to the recipient list.
3. Enter the subject and the message that should be appended to the alert notification.
4. Enter the threshold figure for the number of e-mails that you want to receive in an hour. For receiving e-mails first configure the SMTP server.
5. To configure the SMTP server, click the **Configure SMTP** button which will take you to the Mail Preferences dialog box in the Options tab.
6. Specify the SMTP (Simple Mail Transfer Protocol) mail server name and user ID for Clavister Insight to send an e-mail alert whenever a specified event type or attack activity is detected or if the total number of attack attempts exceeds a specified value.
7. Finally, click **Save**.

SNMP Trap

SNMP (Simple Network Management Protocol) allows you to instantiate a trap-directed alert notification called the SNMP Trap. Trap-directed notification can help you save network and agent resources by eliminating the need for SNMP requests, and through minimized SNMP polling.

To configure Clavister Insight to send traps to the SNMP server, follow the steps described below:

1. Select the **SNMP Trap** check box
2. Enter the appropriate details of the SNMP server **IP/Name**, **SNMP Port**, and **Community Name**.

The idea behind trap-directed notification is as follows: if a large number of devices are configured to send alerts, and each device has a large number of objects, it is impractical to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the Alert Manager without solicitation. It does this by sending a message known as a trap. After receiving the event, the Alert Manager may choose to take an action based on the threshold set for the event.

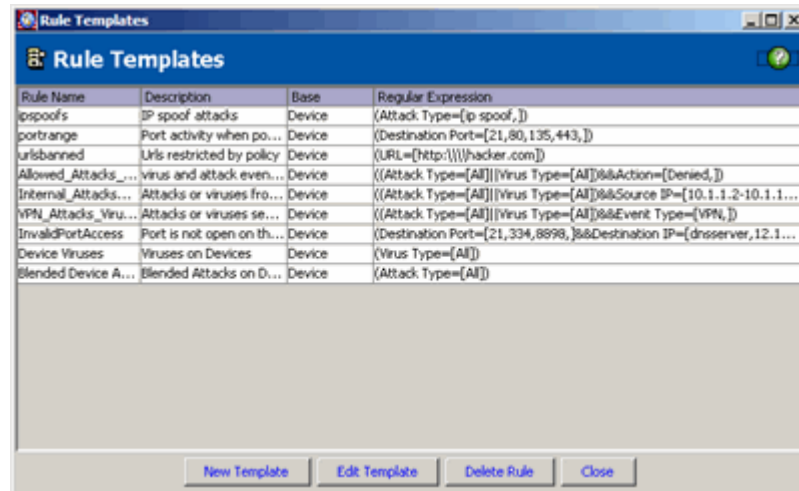
Rule Template

A Policy is based on Rules. You can create and save Rules as templates in one common repository. Every time you want to apply a Rule to the Policy you can select from the pre-formatted Rule templates. The Rule Templates can be applied in combinations, across all the policies.

Creating Rule Templates

1. On the main Policies window, click Rule Templates button.
2. The Rule Template window opens.
3. By default there are Rule templates available in the CIS repository, which can be loaded on Policies. They are:
 - ❖ IP spoof attacks
 - ❖ Portrange
 - ❖ Urlsbanned
 - ❖ Allowed_Attacks_Viruses
 - ❖ Internal_Attacks_Viruses
 - ❖ VPN_Attacks_Viruses
 - ❖ InvalidPortAccess
 - ❖ Device Viruses
 - ❖ Blended Device Attacks

From here you can also create customized templates based on devices.



Device Based Rule Templates

1. Click the New Device Template on the Rule Templates window.
2. The Create Rule window opens.
3. See "Creating Device based Rule" for details.

Editing a Template

1. Select the Rule template that you want to edit from the Rule template list from the Rule Templates window.
2. Click on the Edit Template button.
3. If you have selected a Device based rule to edit, the corresponding device window opens. And if you have selected a Messaging Server based rule to edit, the corresponding Messaging Server window opens.
4. The Rule name is non-editable but can edit the description of the Rule.
5. Make the necessary changes-- you can edit the settings on all the filters available in the list and also add new filters.
6. Click the next button to proceed with editing process, else click the Cancel button to abort the task.
7. On the next screen if needed, you can change the way the operators work on the sets of filters.
8. Click Save to save the edited Rule Template.
9. Click Previous to revert back to the earlier screen to alter or recheck the filter settings.
10. Click Cancel to abort the task.

Deleting a Rule Template

1. Select the Rule template to delete from the list on the Rule Template window. Click the Delete Rule button.
2. The dialog box prompts you for a confirmation. Click Yes to delete, Cancel to abort the task.
3. The Rule Template will be permanently deleted from the repository.

Set Threat Levels

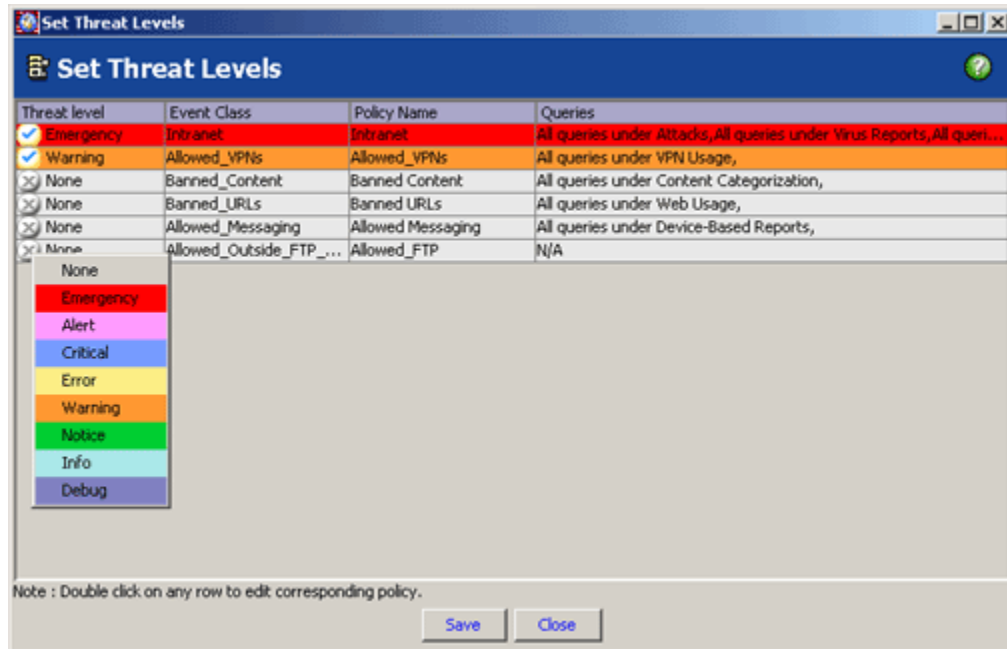
A potential adverse event which is malicious by nature or is incidental and that can put the network and system assets at stake can be classified as a THREAT to the network security of an enterprise.

Event Logs from vendor specific devices come with pre-assigned severity levels for each event depending upon the potential or incidental degree of associated threat. Each severity level is depicted in a different color, which is vendor specific.

There are eight Threat levels, each identified by a corresponding color. From lowest to highest, the levels and colors are:

- ❖ Debug = Violet
- ❖ Info = Cyan
- ❖ Notice = Green
- ❖ Warning = Orange
- ❖ Error = Yellow
- ❖ Critical = Blue
- ❖ Alert = Pink
- ❖ Emergency = Red

Now, CIS gives the flexibility to the Super Admin User to change the threat level associated with a class of events and set it according to his perception of the threat. For example, if the severity level of an Event Class is 'Emergency' and is depicted in red in the vendor logs, but the administrator does not consider them as high level threat events, he can use the Set Threat Level option and change the threat from 'Emergency' to say 'Warning'. Henceforth the severity of events which belong to this Event Class will be marked as Warning and will be depicted in orange. The altered threat level is updated in Event Viewer for real-time monitoring and is also reflected in all graph types and reports.



Change threat levels

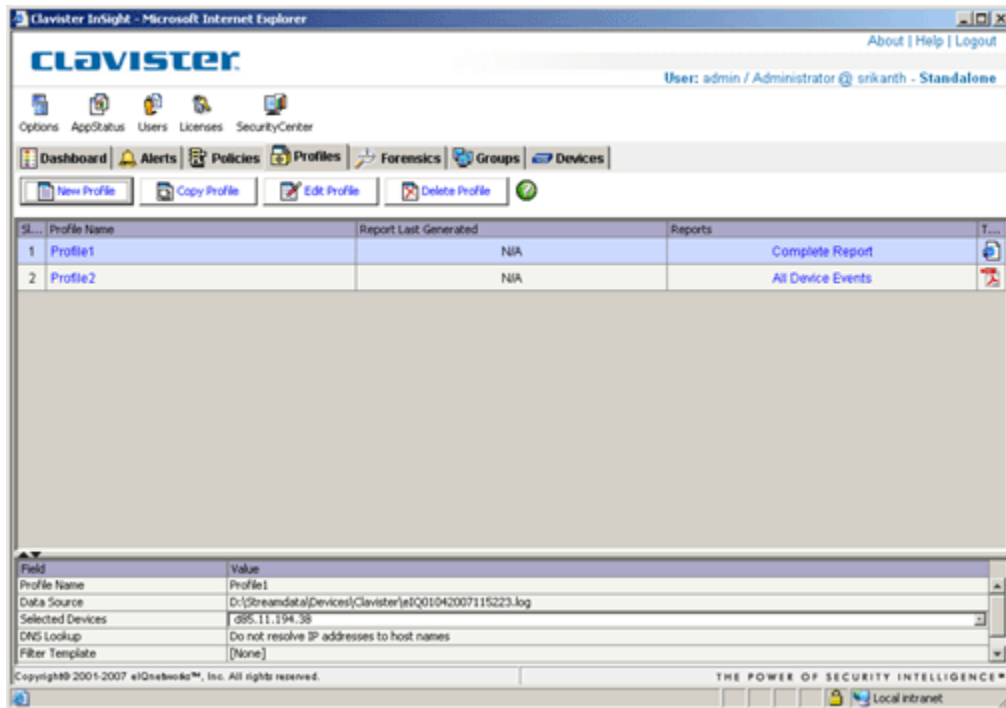
1. Select the Event Class on which you want to change the threat level.
2. Click on the select Threat Level icon to select any of the threat level which you want to apply to an event class.
3. Click Save.

Profiles

A profile is a set of instructions identifying the locations of your device logs, how data must be accessed, the method followed to analyze data, how IP addresses must be resolved, and customization of reports. Profiles also facilitate you to choose filters that help you narrow down your data to the information you need most, which can save time and resources. Profiles can be created using the **New Profile** wizard. When the wizard completes, the profile appears in the profile list.

The Profile Manager main window contains the New Profile, Edit Profile, Copy Profile, and Delete Profile buttons.

The Profile Manager Screen



Creating a New Profile

A profile is a group of settings configured to complete a specific task. Once configured, you can use it repeatedly to generate reports whenever necessary. You can also edit or delete a profile as necessary. The first step towards creating a new profile is to assign a unique name. To do this, carry out the following steps.

To create a profile, follow these steps:

1. On the main Profile Manager window, click **New Profile**. The **New Profile** wizard opens.
2. Type in a name in the **Profile Name** text box.
3. Select the input source for the profile to be created:
 - ❖ Select CIS Database if the CIS syslog server or a DB agent has been configured to collect log file data and store it in the built-in database. OR
 - ❖ Select File to migrate log file data to the database and generate a report.
4. Specify the Date Range to configure the Profile to consider data of only the specified dates.
5. Select the devices you want to report on. If you want to report on all devices, select the **All Licensed Devices** check box and click **Next**.
6. The **DNS Lookup** screen opens. Select a resolution option and click **Next**.
7. Add the filter template you want to apply and click **Next**. To use a pre-defined template, select a filter from the list. To add a new filter template, click **Add** and enter the required filter settings on the desired filters and save the filter template.
8. Schedule the Profile task to run hourly, daily, weekly, monthly or only once depending on your need.
9. Select the type in which you want to generate the profile based report.
10. Select the report format, the template, the table format (for HTML reports only), the organization name and the logo file to use and click **Next**. The **Save Report** screen opens.
11. To e-mail your report, select the **Mail To** check box and specify the recipient addresses in the text box. To upload your report to a remote site, select the **FTP** check box, specify host name, user name, and password and click **Finish**.

Note:

- ❖ CIS supports McAfee Intrushield logs collected by the Syslog Server and not from the Log File as source option.

- ❖ Creating File based profiles on a Central Server is possible only when it has at least one syslog server configured/reporting to it.
- ❖ A Normal user cannot create profiles based on File option.
- ❖ Once a profile is created, the Profile Name and the log source (CIS Syslog Server/File) cannot be edited.
- ❖ Use of wildcards is not supported in the FTP retrieval path.
- ❖ Clavister Insight receives log data once every 30 minutes (from the CIS syslog server) and the database is updated once every hour. So a user cannot generate any report within the first hour.
- ❖ Use the File option instead of CIS Syslog Server to generate reports. In this case, the report is generated immediately.

CIS Syslog as Source Input

Select this option if CIS syslog server is collecting the log data from the Devices.

New Profile

Profile Name

CIS Database : Select this option to report on Devices from CIS database.
Use this if CIS Syslog Server is collecting your log data.

File : Select this option to migrate log data to CIS database and generate a report.
Use this if CIS Syslog Server is NOT configured to collect your log data.

File as Source Input

Select this option if you want to parse and move the log file data to CIS data store. To generate a report on the parsed log data immediately, select the check box **Generate Report after Parsing the Log Data** and proceed with creating a profile.

We suggest using this option only when a syslog server is not configured to collect the log data.

New Profile

Profile Name:

CIS Database: Select this option to report on Devices from CIS database. Use this if CIS Syslog Server is collecting your log data.

File: Select this option to migrate log data to CIS database and generate a report. Use this if CIS Syslog Server is NOT configured to collect your log data.

Log File Source:

Device Identifier:

(This identifier will be used if the log files do not specify any.)

Generate Report after parsing Log data.

Note:

1. Select File if the log file resides on the CIS Server.
2. Select FTP if the log file resides on an FTP site.
3. Make sure that the device you want to report on is licensed.

Log File Source:

A source file can reside on the local machine where CIS is installed or on a FTP site. Select the File or FTP option based on the location of the log file.

Device Identifier: Select this option to identify, license and further generate a report on the data present in the log file, which is henceforth represented with the string provided in the Device Identifier text box.

Generate Report after Parsing the Log Data: Select this option if you want to parse the log file and subsequently generate a report immediately.

Leave the check box clear if you want the data present in the log file only to be parsed. The report on this profile can be generated only after the next aggregation cycle.

Generic File Names

Clavister Insight provides a generic method for specifying input and output file names in the profile. You can enter generic file names directly in name text box or you can use the Grammar Syntax feature to specify input and output file names. This feature is useful in scheduling repetitive tasks for which the log file name is structured on a timestamp format.

File Specification Grammar Macros

<i>File Specification Grammar Macros</i>		
Macro (Code)	Description	Format
%b%	Abbreviated month name	(Jan-Dec)
%B%	Full month name	(January-December)
%m%	Month	(01 – 12)
%d%	Day of month	(01 – 31)
%H%	Hour in 24-hour format	(00 – 23)
%y%	Year without century	(00..99)
%Y%	Year with century	(2000-2099)

Clavister Insight allows you to use wild card specification in the file name specification, and understands standard DOS directory wild cards (i.e., *). You can specify the relative day, week, month or year by decreasing or increasing the specific value. The same syntax is used to specify file names for output reports.

Grammar Syntax Examples

<i>Generic Naming – Grammar Syntax Examples</i>		
File Name Specification	Sample File Name+	Represents
eIQ%m%%d%%y%.log	eIQ062005.log	June 20, 2005
eIQ%m%%d%%Y%.log	eIQ06202005.log	June 20, 2005
eIQ%Y%%d%%B%.log	eIQ200520June.log	June 20, 2005
eIQ%*%%m%%y%.log++	eIQ*0605.log	June 20, 2005
<p>+ Assuming current date is June 20th, 2005</p> <p>+ + In this example, all files created in June 2005 that are in the specified directory will be processed by the scheduler. This is because of the wild card specification * in the File Name. Note that Clavister Insight will not limit itself to files with only the day of the month. The wild card is a system wild card, and as in the DOS directory command, it will pick up all files with any matching string in place of the asterisk.</p>		

To specify file names using the Grammar syntax, follow the steps below:

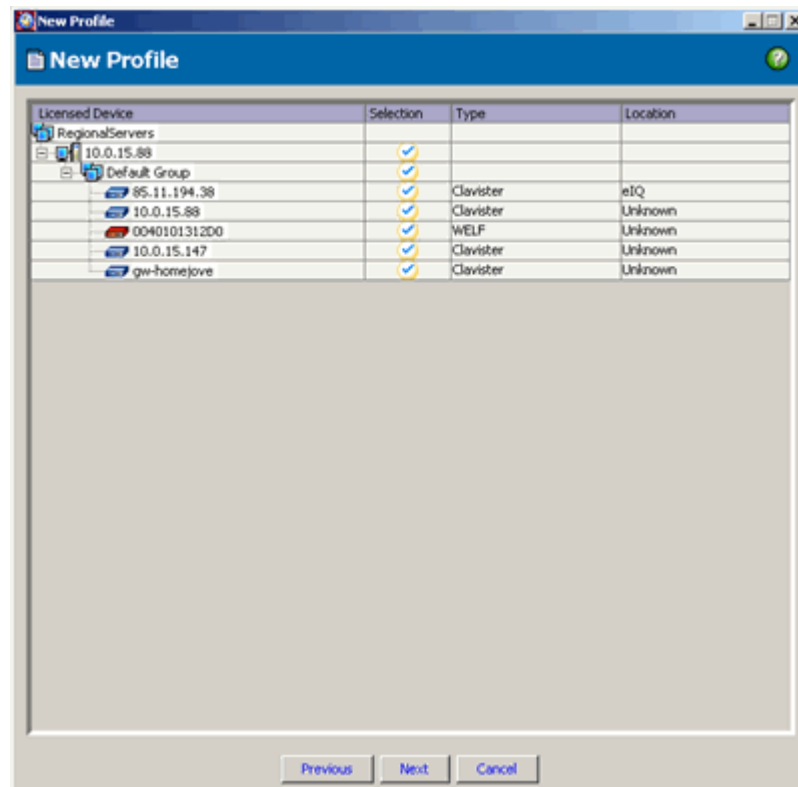
1. Click **New Profile** and select **File** to migrate log file data to the Clavister Insight database and generate a report. Click **Next**.
2. Click **Grammar** to display the **Grammar** screen.
3. Click **Browse** and go to the location where generic log files are stored.

4. Select the timestamp format for the generically named files. Based on the log file naming convention of your log file, select the appropriate date format from the **Date Format** drop down list. You can add an alphabetical prefix to the format and select from different file extensions in the suffix box.
5. In the **Add/Subtract** text box (Year, Month, and Day/Weeks) specify the time stamped log file that you want to use as the input. For example, to attach to yesterday's log file, enter **-1** in the **Day** text box with respect to the current system date.
6. The selected file syntax is automatically displayed at the bottom of the screen.

Selecting Groups and Devices

This screen lists all devices that are licensed and you can select the ones that you want to report on. A device can be added and configured from the **Devices** tab. If your devices are configured to write log data into a single log file, you can select only those licensed devices you want to report on.

The Devices Selection Screen



 This icon represents a configured licensed device.

Follow the steps described below to select the devices you want to report on from amongst the licensed network devices:

7. To report on all network devices logging data into the log file, select the **Select All** check box. OR select a group or device from the list.
8. Click **Next**.

DNS Lookup

Clavister Insight can resolve the IP address, as found in the collected device log data, into meaningful host names using Domain Name System (DNS) resolution. Each Internet address can be resolved (if defined in the DNS of the owner of the IP number) into a domain name, which is easier to remember and makes the Clavister Insight reports more readable. Should the domain name not be defined for a specific IP address, the resolution will fail and only return the IP number to Clavister Insight, which is displayed in the report.

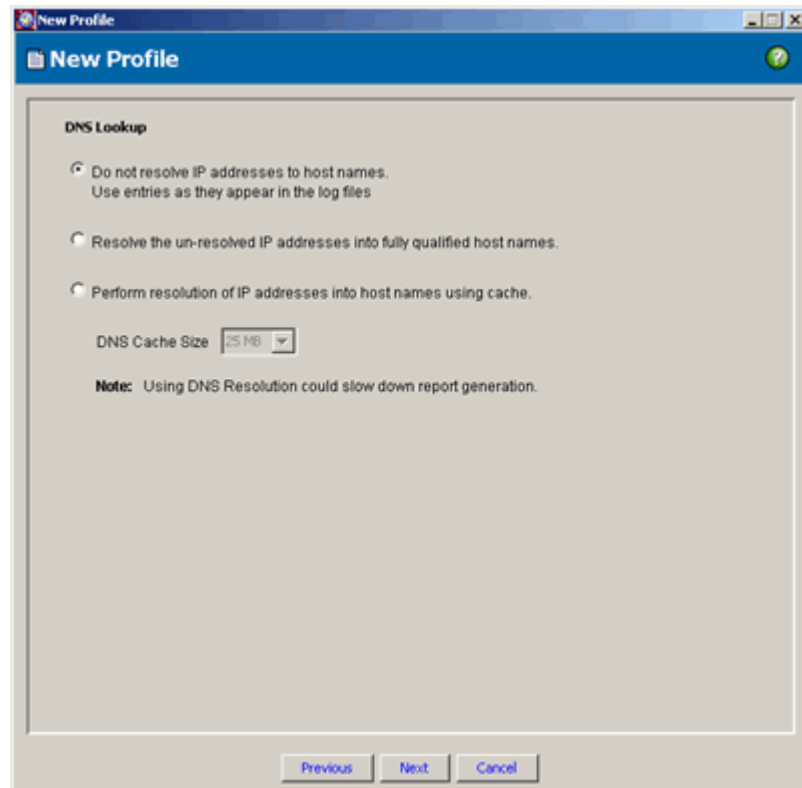
It is a good idea to increase the size of the DNS cache that is built into Clavister Insight should the number of unique IP numbers grow. Select the size of cache file from the drop-down list in the New/Edit Profile → DNS Lookup tab if you want Clavister Insight to consider previously resolved IP addresses stored in the cache. An important consideration is that if a cache is very large and never reaches the point of being filled, very old lookup information may be used in the reports.

The working order for DNS lookup in Clavister Insight ...

- ❖ Is the IP number defined as an intranet address?
- ❖ If not, check the DNS cache if it has been resolved earlier and is still stored.
- ❖ If not found in the DNS cache, the lookup will then call the DNS for resolution.

The lookup of IP numbers is based on all of the IP numbers that will be visible in report tables, should a report table contains 100 IP numbers, and these are the ones that will be resolved. As internal addresses normally are the most readily found in the reports, their definition in the intranet section reduces lookups and enhances reporting speed.

The DNS Lookup Screen



Components on the DNS Lookup Screen

- ❖ **Do not resolve IP addresses:** Select this button if you do not want to resolve numeric IP addresses into host names. This will speed up the processing of log files. By default, this option is selected.
- ❖ **Resolve the unresolved IP addresses into fully qualified host names:** Select this button if you want to resolve numeric IP addresses into domain names.
- ❖ **Perform resolution of IP addresses:** Select this button if you want to perform resolution i.e., from domain names to IP addresses and IP addresses to domain names using cache.
- ❖ Click **Next**.

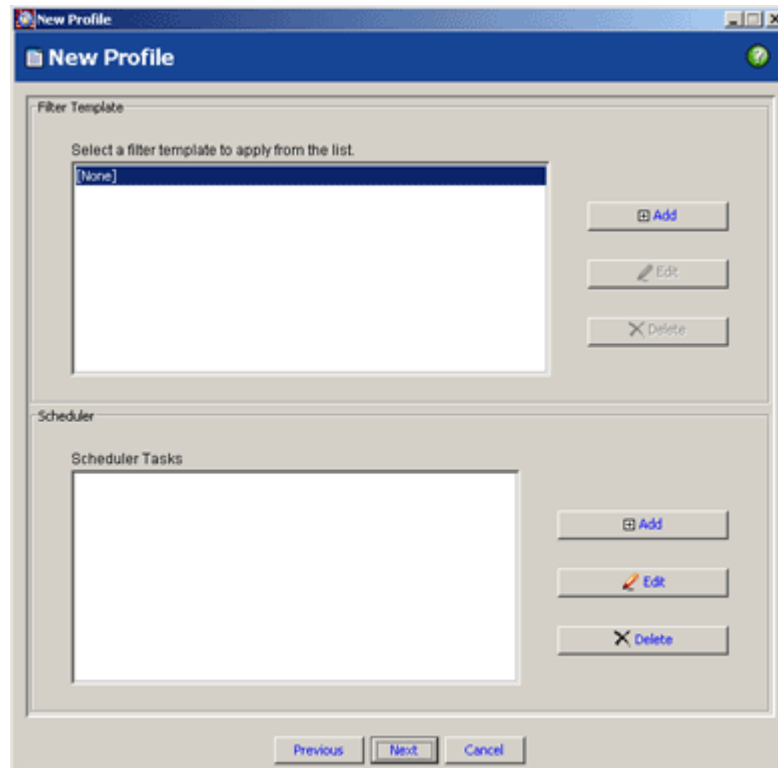
Filter Templates

Profiles look at the results based on the filters you have defined, and ignore everything else. If you want to filter specific information, add a filter template according to your requirement. You cannot use more than

one filter template for a profile. You can create, manage and use filter “templates” across profiles.

To define a new filter template click on the Add button, this will direct you to the **Filter Template** screen, where new filter templates can be created.

The Filter Templates Screen



You can choose to apply only one filter template on a profile.

From the list of available filter templates, select the filter template you want to apply on the created profile.



Make sure that the selected filter template contains all the filter definitions you want to apply on the profile.

Click Next.

Creating a New Filter Template

Clavister Insight provides complex, multi-level filters to sift what data to analyze and present in reports. These filters let you focus on only the data

you need and ignore the rest. For instance, if you want to generate a report on how many visits a particular group of IPs made to your website between two given dates, you can create a filter that limits your report to the IPs for the dates of interest.

This section provides you the information on how to create and set up filter templates for Profiles.

1. Type a descriptive name in the **Template Name** text box. Make sure this name is easy to remember and descriptive of the data you are trying to filter
2. Select the Filter from the available list of filters
3. Select the Include filter button if you want to include the data pertaining to this filter
4. Select the Exclude filter button if you want to Exclude this filter data pertaining to this filter
5. Furnish the required details for the filter settings, Click **Add**
6. Click **Save Filter**. The filter created is listed below along with its respective value. Click **Delete Filter** to clear the filter setting
7. Set all the filters that you want to assign to the Template
8. Click **Save** to save the Filter Template, else Click **Cancel** to abort the task

Filter Elements

The following section provides detailed information on each of the filter elements that can be used to create a filter, and describes how to configure them.

Clavister Insight provides you with the following filter elements:

- | | |
|------------------|--------------------|
| ❖ Protocol | ❖ Sender e-mail |
| ❖ IP/Host Name | ❖ Recipient e-mail |
| ❖ Events | ❖ Event/AttackIDs |
| ❖ Authentication | ❖ Action |
| ❖ Score | |

Each of the elements is discussed in the following sections.

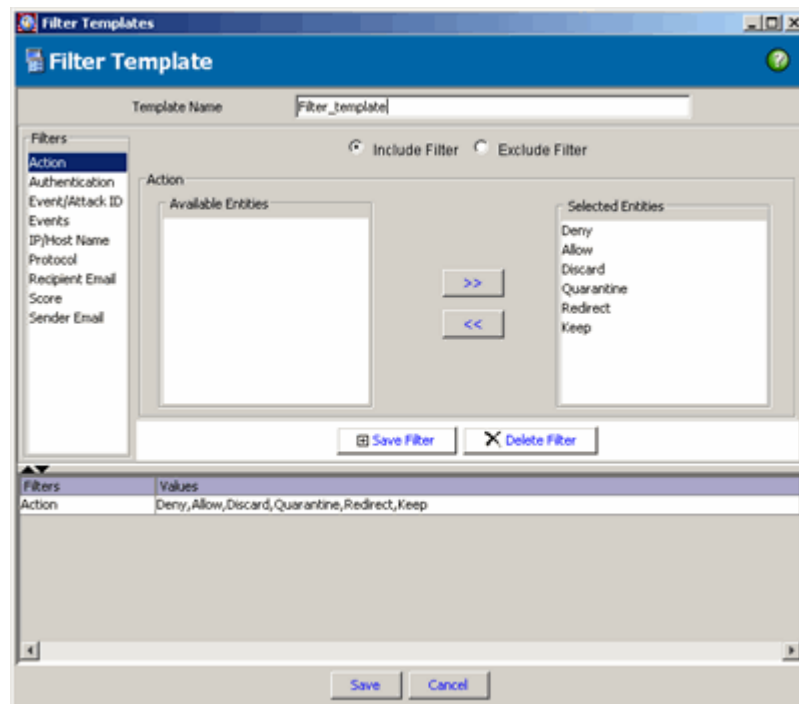
Action


This filter lets you include/exclude information based on the action details which are logged by the devices. Clavister Insight will generate reports

including/excluding information for the selected Action, which are as follows:

- ❖ Keep
- ❖ Redirect
- ❖ Quarantine
- ❖ Discard

Action filter screen



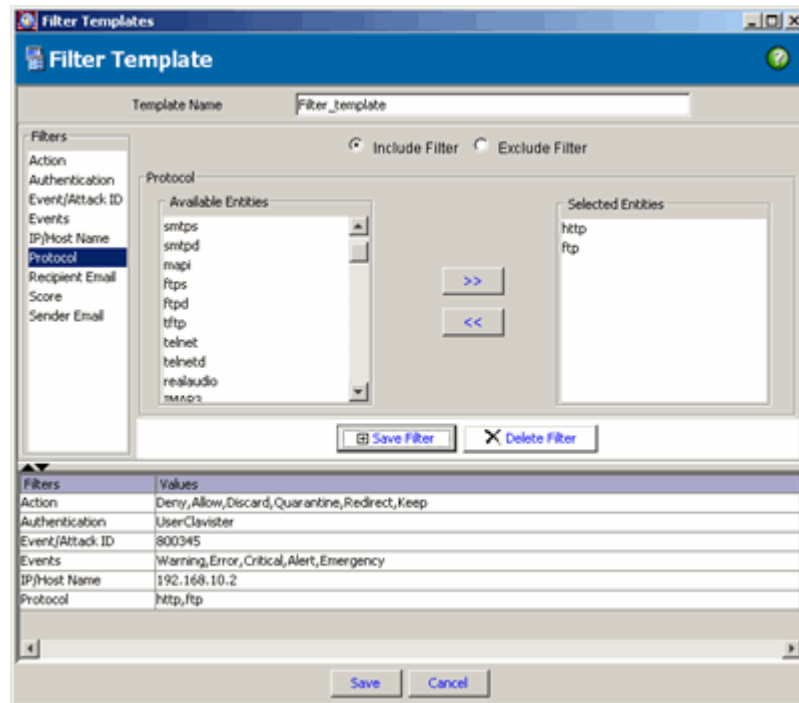
1. Select the actions to be included in the filter template and move them to the selected entities list by clicking the  icon.
2. Click the Save Filter button. The filter is added to the Filter list.
3. Click the Delete button to clear the settings.
4. Press the Save button to save the filter template.

The Protocol Filter

This filter element assists you to include or exclude information based on the protocols selected. If it is used as an Include filter, Clavister Insight

will include data based on the protocols selected and exclude information pertaining to all other protocols. For instance, if you want to select to include all device activity based on the HTTP protocol in a report, Clavister Insight will include all information based on this protocol and exclude all other information. If used as an Exclude filter, data based on the selected protocols will be excluded and that based on all the other protocols will be included.

The Protocol Filter Screen



Follow the steps given below to configure the **Protocol** filter:

1. Type in a name for the filter template in the **Filter Name** box.
2. From the **Filters** list, select **Protocol**. The **Protocol** screen opens in the right pane.
3. Select the protocols you want to filter from the **Available Protocols** box.
4. Click **>** to move the selected protocols into to the **Selected Protocols** box. Use Ctrl+Click to select multiple protocols.
5. Click **Save Filter** to save the filter else **click Delete Filter**.

The IP/Host Name Filter

This filter assists you to include or exclude information based on the IP addresses you specify. For instance, if you want to exclude information pertaining to a group of IP addresses, create an Exclude filter and specify the IP addresses in sequence as shown in the figure to exclude them from the report. If used as an Include filter, this element will include data pertaining to the specified IP(s).

The IP/Host Name Filter Screen

Filters	Values
Action	Deny, Allow, Discard, Quarantine, Redirect, Keep
Authentication	UserClavister
Event/Attack ID	800345
Events	Warning, Error, Critical, Alert, Emergency
IP/Host Name	192.168.10.2

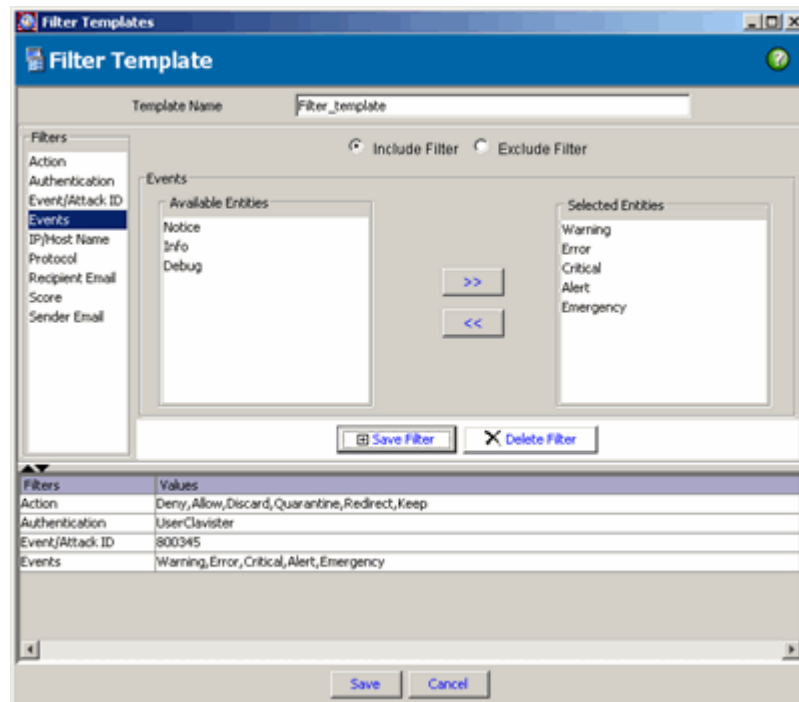
Follow the steps given below to add the IP/Host Name filter:

1. **IP/Host Name:** Select this option if you want to add a single IP address or use wild cards. **Ex** 192.168.100.* to add all devices starting with the given input.
2. Click **Add** to add the IP addresses. To delete an IP Address, select and click Delete.
3. Click **Save Filter** to save the filter else **click Delete Filter**.


The Events Filter

This filter assists you to include or exclude information based on the event types you select. For instance, if you want to include information pertaining to only the Warning, Critical, and Security events, just create an Exclude filter and select the events as shown in the figure to include them in the report. If used as an Exclude filter, this element will exclude data pertaining to selected event types.

The Events Filter Screen



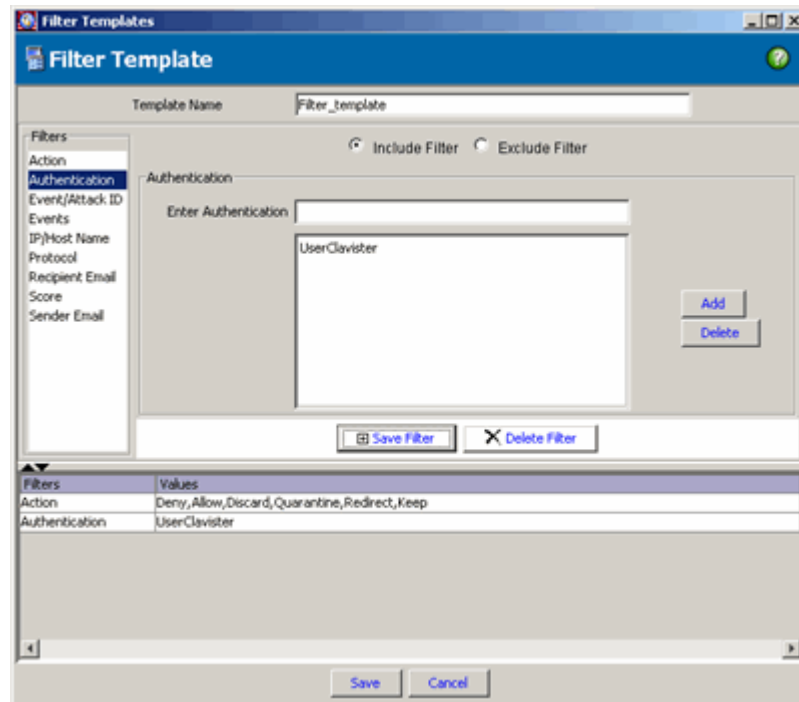
Follow the steps given below to add the Events filter:

1. Type in a name for the filter template in the **Filter Name** text box.
2. Select the **Events** filter.
3. Select the events you want to filter from the **Available Events** box.
4. Click  to move the selected event types into the **Selected Events** box. Use Ctrl+Click to select multiple events.
5. Click **Save Filter** to save the filter else **click Delete Filter**.

The Authentication Filter

This filter assists you to include or exclude information based on the authenticated users you specify. This filter is useful if you have a secure website. If used as an Exclude filter, this element will exclude data pertaining to the specified authenticated users.

Authentication Filter Screen



Follow the steps given below to add an authentication filter:

1. Type in a name for the filter template in the **Filter Name** box.
2. Select the Authentication check box and click **Next**.
3. Enter an authenticated username in the **Authentication** box. Click **Add**.
4. This user is added to the list of authenticated users.
5. Click **Save Filter** to save the filter else **click Delete Filter**.

Score

This filter allows you to specify the score of junk mail intensity encountered based on which Clavister Insight will process log file data and generate reports. Enter the Score for which you want logging included/excluded in your reports.

The Score filter screen

Filters	Values
Action	Deny, Allow, Discard, Quarantine, Redirect, Keep
Authentication	UserClavister
Event/Attack ID	800345
Events	Warning, Error, Critical, Alert, Emergency
IP/Host Name	192.168.10.2
Protocol	http, ftp
Recipient Email	recipient@company.com
Score	100

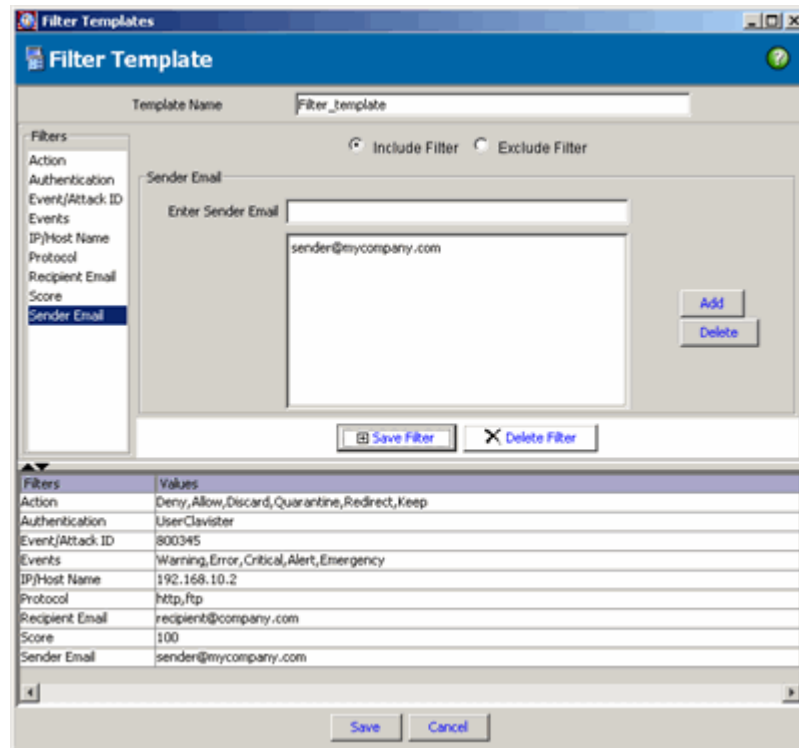
1. Enter the score of junk mail intensity that you want to filter from the logs.
2. Click **Save Filter** to save the filter else **click Delete Filter**
3. Click **Save** to save the filter template.

Sender E-mail

The Sender E-mail filter allows you to specify the email id of the sender which Clavister Insight will filter through the log file data and generate reports. Use the include/exclude check box to consider or negate the

Sender Email filter. To specify the Sender E-mail filter settings, follow the steps given below:

Sender e-mail filter screen



1. Enter the e-mail address of the sender that you want to filter, in the **Sender E-mail** box.
2. Click the **Save Filter** button. The filter is added to the Filter list.
3. Click the **Delete Filter** button to clear the settings.

Recipient E-mail

The Recipient E-mail filter allows you to specify the email id of the recipient which Clavister Insight will filter through the log file data and generate reports. Use the include/exclude check box to consider or negate the Recipient E-mail filter. To specify the Sender E-mail filter settings, follow the steps given below:

Recipient e-mail filter screen

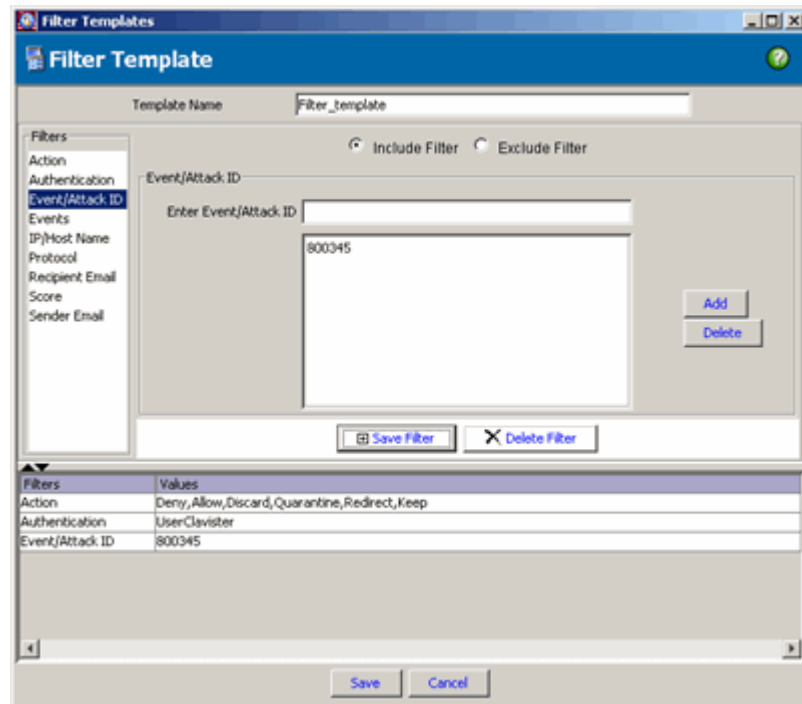
Filters	Values
Action	Deny, Allow, Discard, Quarantine, Redirect, Keep
Authentication	UserClavister
Event/Attack ID	800345
Events	Warning, Error, Critical, Alert, Emergency
IP/Host Name	192.168.10.2
Protocol	http, ftp
Recipient Email	recipient@company.com

1. Enter the e-mail address of the recipient to filter, in the **Recipient E-Mail** text box.
2. Click the **Save Filter** button. The filter is added to the Filter list.
3. Click the **Delete Filter** button to clear the settings.

Event ID/Attack ID

This filter allows you to specify event or attack ID(s) based on which Clavister Insight will process log file data and generate reports. Select the event IDs for which you want logging included/excluded in your reports.

Event/Attack ID filter screen



1. Select the Event ID/Attack ID filter and click Next.
2. To add a new ID, specify the event/attack ID in the Event ID/Attack ID box and click **Add**.
3. Click **Save Filter** to save the filter else **click Delete Filter**.

Scheduler

The Scheduler provides a visual interface to schedule reporting. You can schedule to run profiles automatically at specific date and times, which is particularly advantageous when you are running reports at regular intervals. Using the Scheduler, you can schedule tasks to run on specific dates and at specific times.

Scheduling a Profile

In the new profile wizard, the Scheduler screen opens. The list box contains all the scheduled tasks. Click the Add button to schedule a new task or select an existing task to edit.

Add Task

To schedule a task for a profile to generate reports at regular intervals, create a task using the Add Task wizard.

4. Click **Add**. The **Add Task** wizard opens.
5. Enter a name in the **Task Name** box.
6. Select the frequency of the task, i.e., how frequently you want the task to be executed.
7. Click **Next**.

The Add Task Screen



Only those profiles created by selecting the CIS Syslog Server or File with grammar as the input source can be scheduled.

Scheduling Task by Hour

To schedule the task on an hourly basis select the Hour button and specify the interval.

Schedule by Hour Screen

The screenshot shows a Windows-style dialog box titled "Scheduler". The main heading inside the dialog is "Perform this Task for Specified Interval Daily." Below this heading, there are three input fields:

- Start Time:** A text box containing "11:33:22" with "(24 Hr Notation)" to its right.
- Start Date:** A text box containing "09/19/2006" with a calendar icon and "(MM/DD/YYYY)" to its right.
- After Every:** A dropdown menu showing "1" and the word "Hours" to its right.

 At the bottom of the dialog, there are three buttons: "Previous", "Finish", and "Cancel".

1. The **Start Time** indicates the time at which you want the scheduled task to start. The current time is displayed in the hh:mm:ss by default. To change it, just specify a different time value. For example, 13:49:37.
2. The **Start Date** indicates the day you want the scheduled task to start. Use the **Calendar** button to select the start date or enter a date in the mm/dd/yyyy format.
3. The **After Every** indicates the interval at which you want the scheduled task to start. The intervals are 1, 3, 6, and 12 hours.
4. Click **Finish**.

Scheduling Task by Day

To schedule the task on a daily basis, select the **Daily** button and specify the time. You can also choose to have your tasks performed either every day or on weekdays only.

Schedule by Day Screen

Follow the steps described below to schedule a task by day:

1. Select the **Everyday** button to schedule the daily task and click **Next**.
2. Enter the start time to indicate the time at which you want the scheduled task to start. For example, 18:24:30,
3. The **Start Date** indicates the day you want the scheduled task to start. Use the calendar to select the start date, or type in a date.
4. Click **Finish** to save your settings.

Scheduling Task by Week

Select the **Weekly** button and click **Next** to bring up a dialog box where you can select the days of the week and the start time. This will result in the scheduled job being performed on the selected days of the week. The start time is specified in the Start Time edit box. The scheduled reports will not be generated before this time. Enter the time at which you want the scheduler to begin scheduling your tasks.

Add Weekly Task Screen

Follow the steps described below to schedule a weekly task:

1. Select the **Weekly** button to schedule a weekly task and click **Next**.
2. Enter the start time to indicate the time at which you want the scheduled task to start. For example, 18:24:30.
3. The **Start Date** indicates the day you want the scheduled task to start. Use the calendar to select the start date.
4. Select the days of the week on which you want to run the tasks.
5. Click **Finish** to save your settings.

Scheduling Task by Month

Select the Monthly button and click **Next** to bring up a dialog box where you can select the month, start date, and the day of each month when you want to generate the report. You can also generate the report of a specific day of the week of each month.

Add Monthly Task

The screenshot shows the 'Scheduler' dialog box with the following configuration:

- Start Time:** 11:57:21 (24 Hr Notation)
- Start Date:** 08/07/2006 (MM/DD/YYYY)
- Frequency:** Days (selected), Every (unselected)
- Days of the month:** 1 (selected)
- Months:** Jan, Mar, Jul, Nov, Sep, Dec (checked); Feb, Apr, Jun, Aug, Oct (unchecked)
- Buttons:** Previous, Finish, Cancel

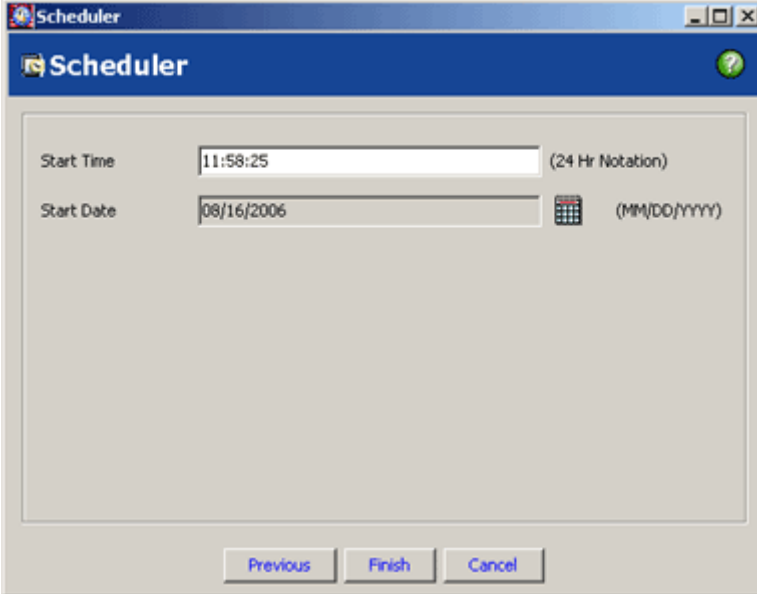
Follow the steps described below to schedule a monthly task:

1. Enter the **Start Time** to indicate the time when you want the task to start.
2. Enter the **Start Date** to indicate the date on which you want the task to start.
3. Click the **Day** button to choose the day of the selected months on which you want the task to run or the **Every** button to choose the day of the week of the selected months on which you want the task to run.
4. Select the months of the year when you want the task to run and click **Finish**.

Scheduling One-Time Tasks

Select **One Time Only** button and click **Next** to bring up a dialog box where you can select the start time and start date when you want to generate the report.

Add One-time Task Screen



The screenshot shows a 'Scheduler' dialog box. The title bar reads 'Scheduler'. The main area contains two input fields: 'Start Time' with the value '11:58:25' and '(24 Hr Notation)' to its right, and 'Start Date' with the value '08/16/2006' and a calendar icon and '(MM/DD/YYYY)' to its right. At the bottom are three buttons: 'Previous', 'Finish', and 'Cancel'.

Follow the steps described below to create a one-time task:

1. The **Start Time** indicates the time when you want the scheduled task to run.
2. The **Start Date** indicates the day you want the scheduled task to start. Use the calendar push button to specify the start date or enter a date.
3. Click **Finish** to save your settings.

Report Type

You can generate a report either for a single device or for all the devices using the Clavister Insight.

- ❖ A single combined report for all selected devices.
- ❖ Individual reports for each selected device
- ❖ Group based report
- ❖ Interface-based report

The Report Type Screen

Single combined report: You can generate a single combined report for all the devices that you have selected in the profile by using this Report Type.

Individual reports for each device: You can generate an individual report for each device that you selected in the profile. Using this option, you can obtain the list of events and individually monitor the occurrence of events on each device and scrutinize the performance of each device and set thresholds specific to devices.

The individual reports are:

- ❖ Generated/stored in separate folders under the Profile. The folder name will be the device IP or host name.
- ❖ The report name will have the suffix '_IP or host name' of the device.

Group based report: Using this option, you can generate a report for the entire group just by creating a profile with the group selected.

Interface based report: Using this option, you can enable reporting only on interfaces and devices and not virtual devices.



If you select your report to be a combination of options other than single combined report, only one report is displayed in the report view and all the reports for other devices are stored in a user-specified location.

Query By

Use the Query By option to generate reports classified By Device, By Group or By Day.

Device: Select this option to generate a report with an additional column that gives the details of the selected Devices.

Group: Select this option to generate a report to query on the Group to which the selected device belongs. For example, if you select two different devices present in more than one group then the report is generated with an additional column-- Group. This appended column gives the Group details of the selected devices. This query is particularly useful when the administrator assigns privileges for the Non-admin users to access only a few Devices configured on the application.

Day: Select this option to generate a report to query on the Day. This report appends a column-Day that gives the details of the day when that particular data came about.

Note: You can query by the above options in the reports from the security center also.

Report Style

You can customize the look and feel of reports as per your choice by selecting from 11 different templates and 10 table formats. You can also choose from HTML, MHTML, MS Word, MS Excel, PDF, and Text reports formats.


- ❖ **Format** — Includes HTML, MHTML, Microsoft Word, Microsoft Excel, PDF, and generic text file formats into which the content of the report will be generated.

Note: MS-Office must be installed before you try to generate

reports in WORD or EXCEL formats. Also Adobe Reader 6.0 and above to view the reports in PDF format.

- ❖ **Template** — You can determine the basic structure of the report. The drop-down box allows you to select from a number of pre-configured report styles that have different fonts and colors. They are Cool, Vintage, Cascade, Serene Arcade, Sand Ribbon, Wise Monk, Capri Blue, Glass Block, Trendy, Standard, and Orange Spice.
- ❖ **Table Format** — Select the format of the tables used to present tabular data in Microsoft Word reports. The table formats are Simple, Colorful, Columns, Grid, Classic Grid, List, Classic List, Contemporary, Elegant, and Professional.
- ❖ **Organization** — This field allows you to select the company name, as it will appear in reports. Typically, this field is used to present the name of the company creating the report.
- ❖ **Logo File** — The Logo text field is where the user can specify the logo file that will be displayed in reports. The default logo is the logo.gif and is picked from the folder [Installation Directory]\htmlfiles\logo.gif. To display your company logo, replace this image with your logo in this folder, or specify the absolute path to your logo file if it is in a different location. For example if your logo file is mylogo.gif and is in a folder named "images" in drive D:, then the absolute path to the file would be D:\images\mylogo.gif.

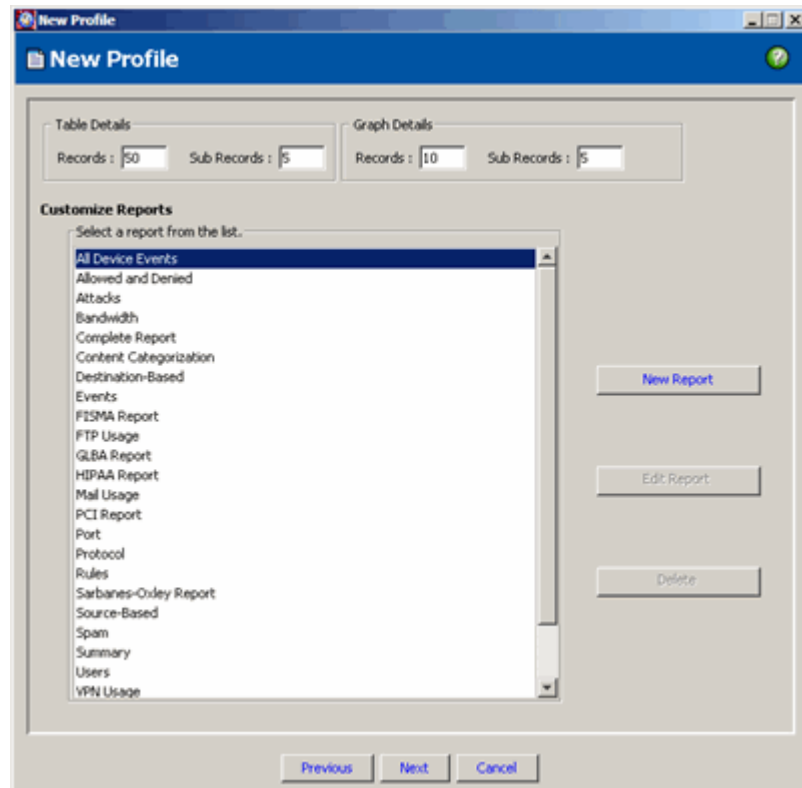
To specify the format of reports, follow these steps:

1. In the **Reports** screen, click **Report Style**. The **Report Style** screen opens.
2. Enter the template name. Click  to select the background, query font, and node font colors.
3. Click **Save**.

Customizing Reports

Clavister Insight enables you to create customized reports tailored to suit your needs. You can choose which queries to include, whether to include graphs, the graph type, and even how many records to include in each table.

The Report Customization Screen



A custom report is a report that you can create by including only selected queries that meet your specific requirements. This helps you focus on only the data you need.

To create a new report, follow the steps below:

1. In the **Customize Reports** screen, click **New Report**.
2. In the **Report Name** box, enter a name for the report.
3. Select the queries you want included in the new report. Click **Save**.

Editing a Report

To edit the settings for a report, follow the steps given below:

1. Select a report and click **Edit**. The **Edit Report** screen opens.
2. After making the changes, click **Save**.



Any changes made will be reflected in the report, the next time it is generated.

Default reports like Complete Report, Bandwidth Report, Protocol Report, Event Report, Intranet Report, and Device Report cannot be edited or deleted.

Deleting a Report

To delete a report, follow the steps given below:

1. Select a report from the report list and click **Delete**.
2. Click **OK** to confirm the deletion.

Save Report

Use this screen to specify the report name, the e-mail addresses to which the reports can be e-mailed automatically, and the remote FTP location to which your report can be uploaded. By default, the generated report is saved on the machine where Clavister Insight is installed in the following location.

```
[InstalledPath]\userprofiles\[user]\ProfileseIQ\[Profile name]\  
[filename]
```



It is recommended that you not use mapped network drives to store generated reports. Instead, use only your local drives to store the reports.

Reports are delivered in the following three ways:

- ❖ Saved on a local system or network neighborhood
- ❖ E-mailed to one or more recipients
- ❖ Uploaded via FTP to a remote location

The following sections explain how to specify the output and delivery of reports in each of these three ways.

The Save Report Screen

New Profile

Save Report

Save As: [Grammar](#)

Mail To:

Cc:

Subject:

Message:

To e-Mail Reports: [Configure SMTP](#) Server

FTP

Host Name:

User Name:

Password:

Use Passive Mode

[Previous](#) [Finish](#) [Cancel](#)

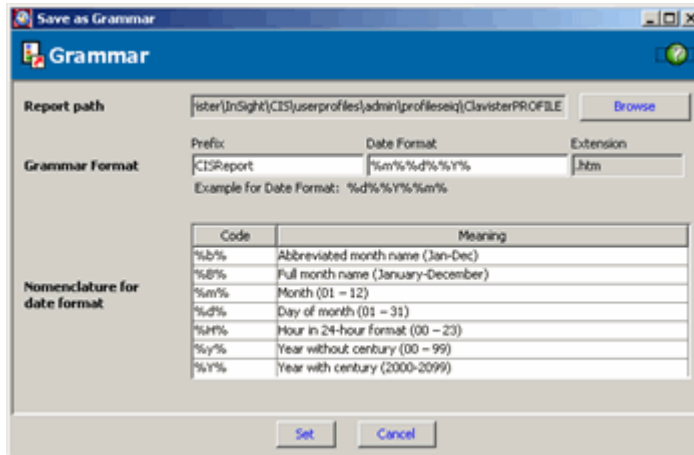
Saving Reports

By default Clavister Insight saves a generated report in the machine where Clavister Insight is installed. Enter a name for the report in the **Save As** text box. For help on using generic file names, see the table below for examples.

Using Generic Names for Reports

Clavister Insight follows a generic method for specifying input and output file names in the profile. You can enter generic file names directly in name text box or you can use the Grammar Syntax feature to specify input and output file names. This feature is useful in scheduling repetitive tasks as the log file name is structured on a timestamp format.

Grammar Settings



Clavister Insight provides the option of using wild card specification in the file name, and understands standard DOS directory wild cards (i.e., *). You can specify the relative hour, day, month or year by decreasing or increasing the specific value. The same syntax is used to specify file names for output reports.

Generic Naming – Grammar Syntax Examples		
File Name Specification	Sample File Name+	Represents
CISReport%m%%d%%y%.htm	CISReport 062006.htm	June 20, 2006
CISReport%m%%d%%Y%.htm	CISReport06202006.htm	June 20, 2006
CISReport%Y%%d%%B%.txt	CISReport200620June.txt	June 20, 2006
CISReport%*%m%%y%.htm+	CISReport *0606. htm	June 20, 2006

+ Assuming current date is June 20th, 2005

+ + In this example, all files created in June 2006 that are in the specified directory will be processed by the scheduler. This is because of the wild card specification * in the File Name. Note that Clavister Insight will not limit itself to files with only the day of the month. The wild card is a

system wild card, and as in the DOS directory command, it will pick up all files with any matching string in place of the asterisk.

To specify file names using the Grammar syntax feature, follow the steps given below:

1. Click **Grammar**. The Grammar dialog box is displayed.
2. In the Grammar dialog box, click **Browse** and go to the location where generic log files are stored.
3. Define the timestamp format for the generically named files. Based on the log file naming convention of your log file, specify the appropriate date format in the **Date Format** text box. Note that you can add an alphabetical prefix to the format and select from several different file extensions in the suffix box.
4. In the **Add/Subtract** text box (Hour, Day, Month and Year) specify which timestamped log file is the input. For example, to attach to yesterday's log file, enter -1 in the Day text box with respect to the current system date.
5. The selected file syntax is automatically displayed at the bottom of the dialog box.

E-mailing Reports

You can e-mail your reports to specified addresses using Clavister Insight. You can enter multiple e-mail addresses separated by semi-colons. Follow the steps given below to e-mail your reports:

1. Select the **Mail To** check box and enter the e-mail address in the text box. To e-mail to multiple recipients, use semi-colon to separate the e-mail addresses.
2. You can enter multiple e-mail addresses separated by semi-colons and send a copy of the report to other users (cc:) if required.
3. Enter the subject in the **Subject** box.



This feature will work only if your SMTP server is configured.

FTP Reports

You can also choose to upload your report to a remote FTP location. Follow the steps given below to upload your reports:

1. Select the **FTP** check box and enter the host name to send the file, user name, and password to configure FTP. The machine that is to receive the reports must be running an FTP service.
2. Select the Passive Mode check box if you want Clavister Insight to use "**passive FTP**" to initiate FTP connections.
3. Passive FTP connections provide more security for the network that hosts the FTP server to which Clavister Insight will connect. Clients that use passive FTP send a PASV command, which allows the server to specify which data port it wants to use, rather than sending a standard POST command to specify a control channel and data channel port.

Edit Profile

You can edit or delete a profile as required. To edit a profile, follow the steps described below:

1. From the menu bar, click **Edit Profile**.
2. On the **Edit Profile** wizard you can edit the configuration settings made in **Device**, **DNS Lookup**, **Filter Templates** and **Reports** tab respectively.

The Edit Screen

3. Click **Save to** save the settings.

Copy Profile

If you want to create profiles that are similar, use the copy profile option.

1. To create a copy of a profile, select an existing profile and click the **Copy Profile** button on the main screen.
2. The Copy Profile window opens displaying the newly created profile. The profile created is identical with the former except the profile name.

Delete Profile

If you want to delete a profile, select an existing profile and click the **Delete Profile** button on the main window of Profile Manager.

Forensics

Forensics analysis involves capturing, recording, and analyzing network events in order to discover the source of security attacks or other problem incidents.

It involves capturing of all data packets passing through a certain traffic point and written onto a storage area (file archive) with analysis being done subsequently in batch mode. This approach requires large amounts of memory storage (SAN or NAS), involving a file system.

Clavister Insight's forensics analysis uses this approach to perform the forensics analysis and in this the major concern is for privacy as all packet information including user data is captured. Clavister Insight addresses this by using a secure communication channel when collecting forensics logs from the specified devices.

The **Forensics** analysis feature helps you to look up a metadata index for specific information across devices across up to several years. This metadata index contains information such as the device ID and time range that references each log file. This enables Clavister Insight to quickly refer log files that contain the device ID and time range applicable to the search.

A configured search has the following columns associated with it.

- ❖ Search Name
- ❖ Report Generated
- ❖ Archive
- ❖ Generate Report

The Forensics Manager Screen

SI No.	Search Name	Report Generated	Archive	Generate Report
1	Forensics	01/10/2007 14:15:45	ForensicsReport100107.bt	
2	Forensics2	01/10/2007 14:18:42	ForensicsReport100107.bt	

Details of	Forensics
Criteria	Device
Search Description	Search for Dropped and Disallowed Events
Archive Source Path	N/A
Archive Location	C:\Program Files\Clavister\Insight\CS\userprofiles\admin\forensics\forensics\ForensicsReport100107.txt
Selected Devices	All
Date & Time	01/01/2007 00:00 01/10/2007 23:30
Filter(s) Selected	Expression

You can edit, copy, or delete a defined searching criterion.

Report Generated: Click the link under the Report Generated column to view the report. You can also customize the report view by including only those fields you want to view.

The Forensic Report Page

Sno	Date	Time	GMT	Device	Device	Virtual	Device ID	Interface	VPN	Format	Source
1	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
2	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
3	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
4	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
5	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
6	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
7	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
8	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
9	01/09/2007	19:34:09	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
10	01/09/2007	19:34:10	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
11	01/09/2007	19:34:10	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
12	01/09/2007	19:34:10	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
13	01/09/2007	19:34:10	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
14	01/09/2007	19:34:10	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
15	01/09/2007	19:34:10	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
16	01/09/2007	19:34:10	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
17	01/09/2007	19:34:11	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1
18	01/09/2007	19:34:11	0	10.0.15.99	10.0.15.99		gw-homesive	exit		Format=OUP	212.183.100.1

Event ID	Event Description	Hits
-	-- disallowed, dropping	31692
-	-- disallowed source ip address	72

Use the following options to customize your report view:


- ❖ **Change My View** - To change the view of your report by selecting the fields you want to view.
- ❖ **Number of Records** - To change the number of records you want to display in the report.
- ❖ **From-To** - To specify records within a range.
- ❖ **Export Report** - To save your search result in either HTML/Text formats.

Note: Values in a report saved in text format are separated by a comma separator.

Note: Forensics analysis stops if the available disk space is less than 20% of the total disk space. Once the disk space falls below this level, the following message appears: *Stopped Forensics searching due to unavailability of free disk space.*

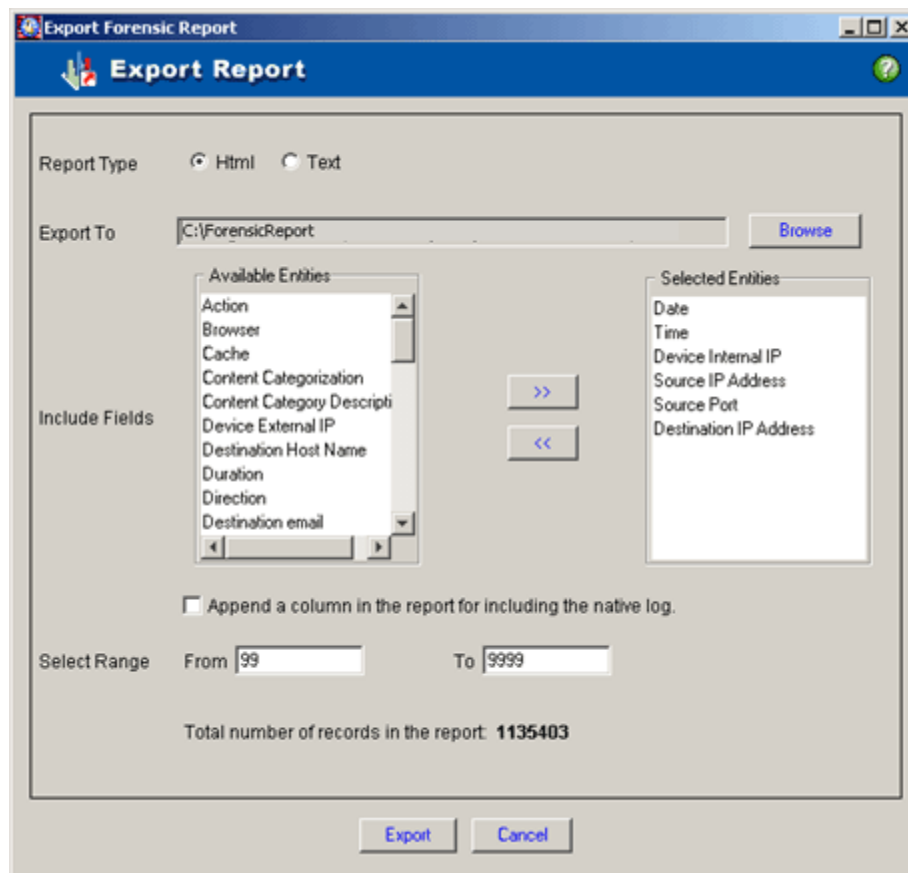
Change My View: This option lets you change the report view by selecting the necessary fields that you want to see in your report.

1. Click **Change My View**. The **Fields** screen opens.
2. Change the report view by adding or removing the fields.

3. Select the fields you want to view from the **Available Report Fields** list and click  to move them into the **Selected Report Fields** list.
4. To include a column in the forensics report for including the native log, select the check box **Append a column in the forensics report for including the native log**.
5. Click **Save**.

Export Report:

You can export the forensic report to be saved onto a specific location and in HTML or Text format. To customize the view of the exported report, select the fields you want to include in the report that is being exported.



Follow the steps described below to export a report:

1. Click **Export Report**. The Export Report screen opens.
2. Select the **Report Type** you want it to be exported to.

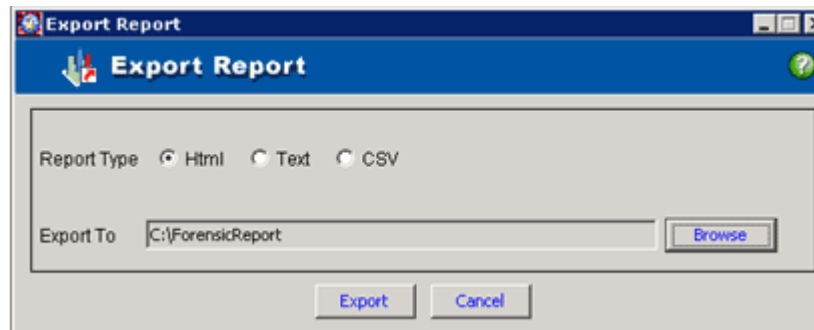
3. Select the fields you want to view from the **Available Fields** list and click to move them into the **Selected Fields** list.
4. Select the range of records that you want to export from the generated forensic report.
5. Click **Export**.

Single Query-Export Report

1. You can export the forensic report on a single query from the TOC to a specific location in HTML, Text or CSV format.
2. Click Export Report for the selected query. The Export Report screen opens.
3. Select the Report Type you want it to be exported in:
 - ❖ Html
 - ❖ Text
 - ❖ CSV*

The CSV* (comma-separated values) file format contains the values in a table as a series of ASCII text lines where each column value is separated by a comma from the next column's value and each row starts a new line.

Export Forensic Report of Top Events




4. Browse to the location where you want to export the Forensic Report based on a single query.
5. Click OK to export or Cancel to abort the task.

Display Type: You can select the Top Events to be depicted in any one of the display types:

- ❖ Table
- ❖ Pie
- ❖ Horizontal
- ❖ Bar
- ❖ Tape

Note: In Forensics reporting, number of records displayed in graphs is limited to 11.

Archive: This column displays the details of the latest results of the configured search. Once a new update for this search is triggered, search results for this search are transferred to the archives.

Generate Report: This column displays the report icon. Click  to generate a report for the configured search.

Log Collection

Using forensics analysis, you can specify from what devices to search log files. In addition, you can do the following:

1. Collect log files from all configured devices.
2. Store logs in OLF (Open Log Format) and compress them into delta files.
3. Transfer delta files from the Syslog Server to the Forensics Analyzer database.
4. Select the format and the location where you want the logs saved from the Options screen.
5. Select a time period to search for specific information.

Configuring Search

For example, if you want to search for events that occurred between 1st and 14th February in 2005 use forensics analysis as follows:

1. Click **New Search** from the Forensics Manager.
2. Enter a name and description for the New Search.
3. Select the criteria of your search: Device or Mirapoint Device.
4. Select the source as **Archived Search Data** and click **Next**.
5. Browse to the specific location where you have stored the raw log files from all the devices, specify the file, click **OK** and click **Next**.
6. Select the devices you want to report on and click **Next**.
7. Specify the Date and time range for which you want to generate a forensics report.
8. Select the filters you want to apply to this search and click **Next**.

9. Select from the available fields, the fields you want in the report and click **Next**.
10. Click **Finish**.

Device Based New Search

Follow the steps described below to add an alert:

1. On the Forensics main window, click New Search. The New Search wizard opens.
2. Enter a name and description for the search in the Name and Search box respectively.
3. Select the search criteria as Device
4. Select from one of the following log sources you want to search from:
 - ❖ Log Files from Selected Devices
 - ❖ Archived Search Data
5. Once all the fields in the window are filled in, click Next.

New Search Screen

The screenshot shows the 'New Search' dialog box in the 'Forensic Search' application. The dialog has a blue header with the title 'New Search'. It contains several input fields and radio buttons. The 'Name' field contains 'ForensicNew', and the 'Description' field contains 'Forensic search for auditing reports'. Under 'Criteria', the 'Device' radio button is selected. Under 'Source', the 'Log Files from Selected Devices' radio button is selected, and the 'Archived Search Data' radio button is unselected. Below the 'Source' section, there is a text prompt 'Specify saved search file name' followed by an empty text box and a 'Browse' button. At the bottom of the dialog, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

Archived Search Data

If you have selected this option as the log source for your search, your search confines to the data present in the reports previously generated. This helps you save time, as you need not search the entire log database.


Follow the steps described below to perform an archive search:

Browse to the archive location of previous reports to search for the required data and click **Next**.

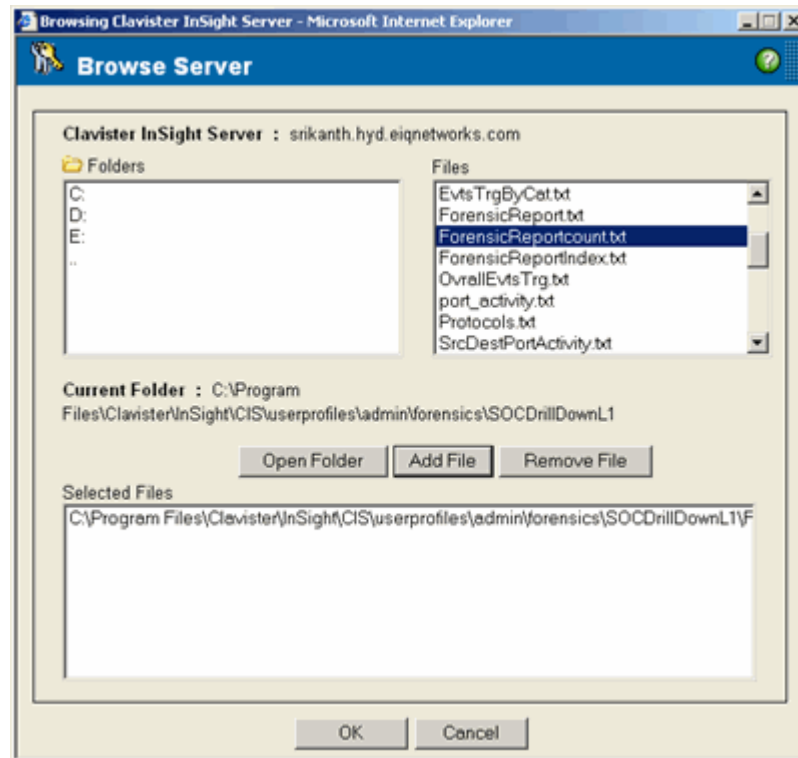


If no report is generated prior to this search, archived data is not available for you to lookup. So this option will not be functional.

Browse Server

1. Click **Browse** and the **Browse Server** Window opens.
2. This window gives you the directory hierarchy of the CIS Server installation.
3. You can select a folder by double-clicking any item or by selecting the folders under  icon and click **Open Folder** to view the files within the folder in the under Files section.
4. Similarly, you can select and add a file within a selected folder by double-clicking it or by clicking the **Add File** button.
5. Selected Log Files section will show the selected log files.
6. To remove a selected file, click **Remove File** button.
7. You can see the path of your selected file or folder in the Selected Log Files section and click **OK**.

The Browse Server Screen



Log Files from Selected Devices

If you have selected this option as the log source for your search, follow the steps described below:

- ❖ Click **Next**.

Date & Time Range

You can enter the time period to configure your search. Follow the steps described below:

1. Click the calendar icon and enter the **Date From** to **Date To** in the appropriate text area provided.
2. Select the hours of a day from the drop-down list available.
3. Click **Next**.

The Date & Time Range Screen

Scheduler

A Forensic search can be scheduled to run the task either daily, weekly or for one-time only.

1. Click on the **Add** button to define a new schedule or click **Edit** button to change the existing schedules.
2. Select a scheduled task from the list.
3. Click **Next**.

Scheduling Forensics Search

The Scheduler facilitates you to run the forensics search reports automatically, at specific times, which is particularly advantageous when you are running reports at regular intervals.

In the new profile wizard, select the Scheduler tab and the scheduler screen opens. The list box contains all the tasks that are scheduled. Click the Add button to schedule a new task or select an existing task to edit.

Add Task

1. Click the **Add** button. The Scheduler Frequency Selection screen opens.
2. On this screen, you can select the frequency at which you want the forensics report to run.
3. Specify a unique name for the task in the **Task Name** box. This name The Scheduler Main Window displays this name under the column Scheduled Tasks.
4. Select the frequency from the options given. The available frequencies are:
 - ❖ Daily
 - ❖ Weekly
 - ❖ One Time Only
5. The forensics report schedule you just created is added to the list of scheduled tasks in the Scheduler screen of configure forensics search wizard.

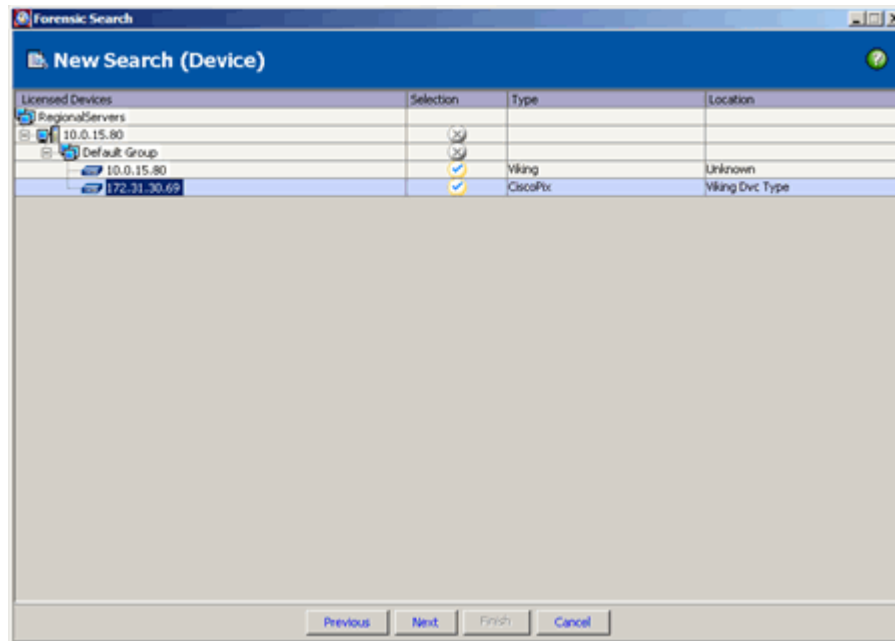
Note: Hourly and Monthly tasks configured in the earlier versions become obsolete after the upgrade and you need to edit them to acquire a different frequency to run the scheduled task.

Device Based Forensic Search

You can select Group/Devices and analyze their logs from this screen.

1. Select all the available devices in one go by selecting the check box in the **Group Name/Device IP** column.
2. To select individual network devices, just select the check box against the device name and once you are done, click **Next**.

The Device Group



Search Filters

You can select the filters you want to apply on your search from here.

1. Select the **Select All** check box to apply all the available filters on your search. To select individual filters, select the check box against that filter.
2. The following are the available filters:
 - ❖ Source
 - ❖ Destination
 - ❖ Destination Port
 - ❖ Rule
 - ❖ Protocol
 - ❖ Event ID
 - ❖ Expression
 - ❖ Severity

Source Filter

If you have selected **Source** in the **Search Filters** window, follow the steps described below:

1. Enter the **Source IP/Name** of the device you want to filter from the rest and report on only those events originating from the specified source.
2. To filter on events originating simultaneously from a series of devices, specify the IP Range by selecting the **Source IP Range** check box.
3. Add the **Source IP/Name** by clicking the **Add** button.
4. Click **Next**.

Destination Filter

If you have selected **Destination** in the **Search Filters** window, follow the steps described below:

1. Enter the **Destination IP/Name** of the device you want to filter from the rest and report on only those events having the specified Destination IP/Name.
2. If you have to filter on events from a series of devices at one time then you can provide the IP Range by selecting the **Destination IP Range** check box.
3. Add the **Destination IP/Name** of the device or the range by clicking the Add button.
4. Click **Next**.

Destination Port Filter

If you have selected **Destination Port** in the Search Filters window, follow the steps described below:

1. Enter the **Destination Port** number in a device that you want to filter and report on only those events ending up in the specified port.
2. Add the port number by clicking the **Add** button.
3. Click **Next**.


Rule Filter

If you have selected **Rule** in the **Search Filters** window, follow the steps described below:

1. Enter the **Rule ID** you want to filter and click **Add** to move them into the **Selected Rules** list.
2. Click **Next**.

Protocol Filter

If you have selected **Protocol** in the **Search Filters** window, follow the steps described below:

1. Select the protocols you want to filter and click  to move them into the **Selected Protocols** list. You can also add new protocols.
2. Click **Next**.

Event ID

If you have selected **Event ID** in the **Search Filters** window, follow the steps described below:

1. Select the **Event IDs** you want to filter from the available list below.
2. Click **Add** button to add a new event ID to the list.
3. Click **Add** to open the **New Event ID** screen.
4. Enter an appropriate name and the ID of a new event you want to add to the list.
5. Click the **Add** button and click **Save**. The new event ID is added to the list of existing event IDs.
6. Click **Next**.

Expression/Phrase Filter


You can search for any string containing a specific word or phrase from the database on this screen.

Do one of the following:

1. Select **Use words** to search for the specified words in the database. You can apply the conditional operators **AND/OR** on the words specified as index for your search.
2. Select **Use phrase** to search for a given phrase from the log files in the database.
3. Click **Add** and then click **Next**.

Severity Filter

You can select the severity types which you want to filter in your search from this screen.

1. Available severity types are:
 - ❖ Emergency
 - ❖ Alert
 - ❖ Critical
 - ❖ Error
 - ❖ Warning
 - ❖ Notice
 - ❖ Information
 - ❖ Debug
2. Select from the Available severity types and click  to move them into the Selected Severity Types list.
3. Click Next.

Save Report

You can save the Forensics Reports for devices in the following two ways:

- ❖ E-mailed to one or more recipients
- ❖ Uploaded via FTP to a remote location

You can save the report to the specified location in either Text or HTML formats.

Follow the steps given below to e-mail your forensic reports:

1. Select the Mail To check box and enter the e-mail address in the text box. To e-mail to multiple recipients, use comma to separate the e-mail addresses.
2. You can enter multiple e-mail addresses separated by comma and send a copy of the report to other users (cc:) if required.
3. Enter the subject of the mail.

Follow the steps given below to FTP your forensic reports:

1. Select the FTP check box and enter the Host name to send the file, User Name, and password to configure FTP. The host machine should have FTP service running in it.
2. Select the Passive Mode check box if you want Clavister Insight to use "passive FTP" to initiate FTP connections.

Note: Take caution in using Mail To and/or FTP options for saving the forensic report as the report can be voluminous.

Forensics Options

With the Forensics options, you can specify the path where you want to store the forensics logs. You can choose to trigger an alert whenever your secondary storage device falls below the specified level and option to forward forensic logs to the Central server.

The following are the forensics options:

- ❖ Disk Space Alert
- ❖ Forward Forensic Logs

Disk Space Alert: Forensics analysis may stop due to unavailability of free disk space. To restart it, free up the disk space or specify a different location from the **Forensics → Options** tab.

Note: Forensics analysis will stop if the available disk space is less than 20%.

Follow the steps described below to set your options for forensics analysis:

1. On the main screen, click **Options**. The Options dialog box opens. Select the **Forensics** tab.
2. Specify the Path where you want to store the forensic logs.
3. Click **Browse**. The **Browse Folder** window opens.
4. Select the folder where log files are stored and click **OK**.
5. Select the **Disk space Alert** check box to raise an e-mail alert if the memory available is less.
6. Enter the recipient e-mail address in the **Mail To** box. To add a copy, enter an e-mail address in the CC box. Use comma to separate multiple e-mail addresses.
7. Click **Save**.



To be able to send an e-mail alert, your SMTP server must be configured. For detailed instructions on how to configure your SMTP server, click [here](#).



To see the mapped network drives created by the user, change the service logon properties from Local System account to **This account** with a valid username and password from the Service Control Manager.

Forward Forensic Logs: You have the option to forward the Forensics logs to the central machine and at what time of the day.

On a regional if you change the storage path of forensics logs, you can forward only the deltas collected into the newly defined storage path, to the central.

Note: This functionality is available only with regional CIS Servers.

Edit Search

Follow the steps described below to edit a configured search:

1. Click a search under the column **Search Name**. The **Edit Search** window displays.
2. Make the necessary changes and click **Next**.
3. Verify the altered settings and click **Finish**.

Copy Search

To create a copy of an already existing search, use the Copy Search option.

Follow the steps described below to create a copy:

1. To create a copy of a search, select an existing search and click the **Copy Search** button on the main screen.
2. The **Copy Search** window opens displaying the newly created search.



The search just created is identical to the former except the search name.






Delete Search

To delete a search, select an existing search and click the **Delete Search** button on the main window of **Forensics** manager.

Managing Devices and Groups

This section describes how to manage your devices and Clavister Insight syslog server. Once you configure the syslog server, Clavister Insight accesses device logs using the syslog service for processing and storage. Log file data is stored in either the built-in database or an enterprise database. Configure the enterprise database from the **Options → General** tab. You can add as many devices as permitted by your license.

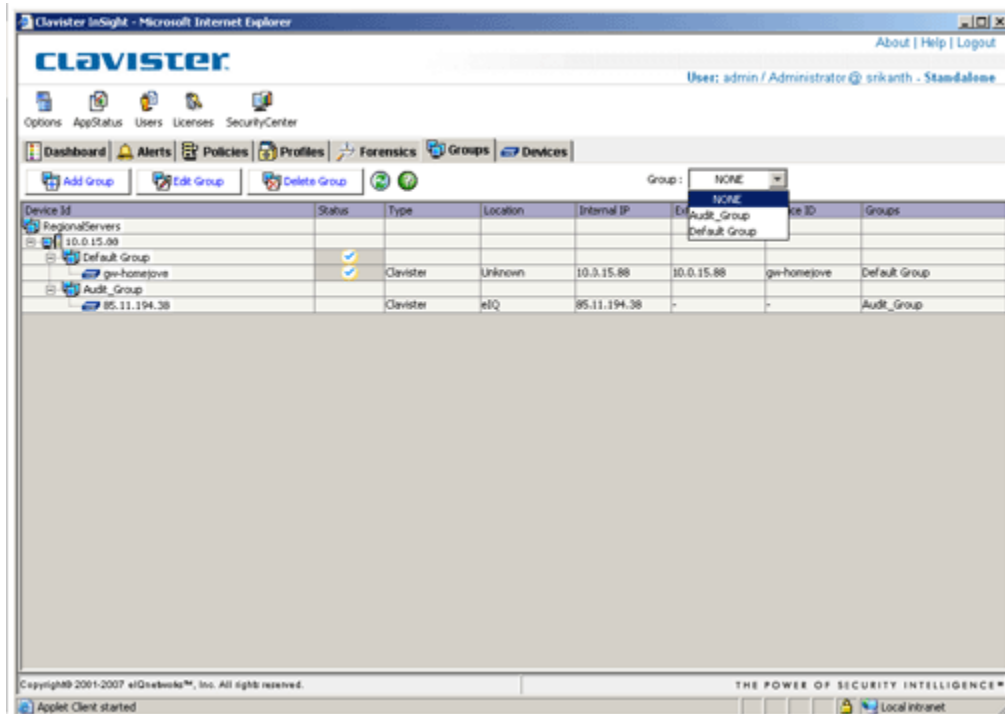
Clavister Insight assigns a unique symbol to the configured Device for easy identification. The following table gives the details of the symbols used in the Groups/Devices screen display:

	Represents a configured licensed device
	Represents a configured licensed device that is inactive
	Represents group or a regional server
	Represents an active syslog server
	Represents a syslog server that is not in the network

The Groups Screen

The **Groups** screen displays the list of groups you created and the devices under each group. You can view details of each device by clicking on the device IP and specifying which group to monitor. You can also add or delete groups from this screen.

The Groups Screen



In this screen, you can view all the configured regional servers. To view all the groups created on it, just select a regional server from the **Regional** drop-down list. The list displays all the existing groups.

The Global Group

Why Global Group?

When you add a new device, automatically it shows under the Default Group for that specific CIS regional. To group devices configured on the CIS Central via the regional syslog server, place them under a predefined group called the Global.

Default Group:

Clavister Insight automatically creates the default group. You can also create new group and allocate devices under that group. If you delete a group, all the devices in that group are automatically shifted to the default group.

Adding a Group

Follow the steps described below to add a group:

1. On the **Groups** screen, click **Add**. The **Add Group** screen opens.
2. Enter a name for the group in the **Group Name** box.
3. Select the parent group from the **Sub-Group** drop-down list.
4. Select the importance, importance factor, and the severity factor from the appropriate drop-down lists.
5. Select the devices you want to add to the group and click **Create Group**.

Editing a Group

Follow the steps described below to edit a group:

1. On the Groups screen, click the group you want to edit. The Edit Group screen opens.
2. Edit the values in the **Importance**, **Importance Factor**, and the **Severity Factor** lists as required.
3. Select the devices you want to add or remove from the existing group and click **Save**.

Moving a Device from Default Group

When you add a new device, it falls under the Default Group. You can move the added device from the default group to any other existing group by following the steps described below:

1. Select the Groups tab.
2. Click on the group to which you want to move the device. The screen displays the list of all the devices.

3. Now select the device you want to move under the selected group.
4. Click **Save**.

Regional and Group drop-down lists

On CIS Central, you can view all the configured regional servers. Select a regional server from the Regional drop-down list to view all the groups existing on that regional.

The Devices Screen

The **Devices** screen lists the syslog servers, configured/unconfigured and manually added devices. You also can add or delete an unconfigured device/virtual device from this screen.

Devices Screen

The screenshot shows the Clavister Insight web interface. The top navigation bar includes links for Dashboard, Alerts, Policies, Profiles, Forensics, Groups, and Devices. The main content area displays a table of devices. The table has the following columns: Device, Type, Location, License, Monitoring, Groups, Policy, Internal IP, External IP, and Device ID. The data is organized into a tree view under 'RegionalServers'.

Device	Type	Location	License	Monitoring	Groups	Policy	Internal IP	External IP	Device ID
RegionalServers									
10.0.15.88									
10.0.15.88	Syslog Server								
gw-homejove	Clavister	Unknown	21 Days Left	<input checked="" type="checkbox"/>	Default Group	Collect All	10.0.15.88	10.0.15.88	gw-homejove
Manually Added Devices									
85.11.194.38	Clavister	eIQ	21 Days Left		Default Group		85.11.194.38	-	-

Adding a Device

Follow the steps described below to add a device:

1. On the **Devices** screen, click **Add Device**. The **Add Device** wizard opens.
2. Select an identifier by which you want your device identified. A device can be identified by its either external IP address, internal IP address, or device ID.
3. Enter the device name in the **Device** box.
4. Select the device type from the **Device Type** drop-down list.
5. Enter the location in the **Location** box and click **Save**.



To display an unconfigured in the **Add Device** window, click on the IP of the device under the Syslog Server or under the Manually Added Devices and click **Save**.



Important: If the device is of type Intrushield, you need to perform the following configuration changes to obtain reports from the Intrushield device.

Configuring the Intrushield devices:

To enable CIS Server generate reports on the log events streamed from the Intrushield devices, edit the intrushield.ext file found in the application path (Apppath ...\CISSyslogSrv\Syslog) folder.

The file has the following information:

<device IP> <Column names>

Format of the IntruShield device log columns must be semicolon separated and each column Identifier would begin and end with \$.

Edit the device IP column with the IP address of the Intrushield device that is streaming data to the CIS Server via the syslog. For example, if 192.168.1.99 is the Intrushield devices IP address, which you want to report upon, uncomment <device IP> tag and provide the respective IP address as <192.168.1.99> with respective columns in the intrushield.ext.

To report on more intrushield devices, append the intrushield.ext file with the device IP and respective Intrushield columns to be included in the report.



CIS supports McAfee Intrushield logs collected by the syslog server and not from the Log File as the data source option.

Adding a Virtual Device or Interface

Follow the steps described below to add a virtual device:

1. Select a primary device from the devices regional server list and click **Add Interface/VD**.
2. To add a virtual device or interface, select any one of the available options:
 - ❖ Virtual Device
 - ❖ Interface
3. Select **Virtual Device** and enter the IP address of the virtual device and click **Save**.



You must select a primary device to monitor its virtual device or an interface.

Follow the steps described below to add an Interface:

1. Select a primary device from the devices regional server list and click **Add Interface/VD**.
2. To add a virtual device or interface, select any one of the available options:
 - ❖ Virtual Device
 - ❖ Interface
3. Select **Interface** and specify the Interface Direction.
 - ❖ Internal
 - ❖ External
4. Enter the IP address of the Interface and click **Save**.

Note: Interface name will have the prefix as Iface-.

Deleting a Device

Follow the steps to delete a device:

1. Select the device/s that you want to delete.

Note: By default, CIS selects all the un-configured devices to delete.

2. Click **Delete** to delete the list of devices.



Deleting a device will also remove data pertaining to that device from the database.

3. This device is now displayed under the category **Unconfigured Devices**.



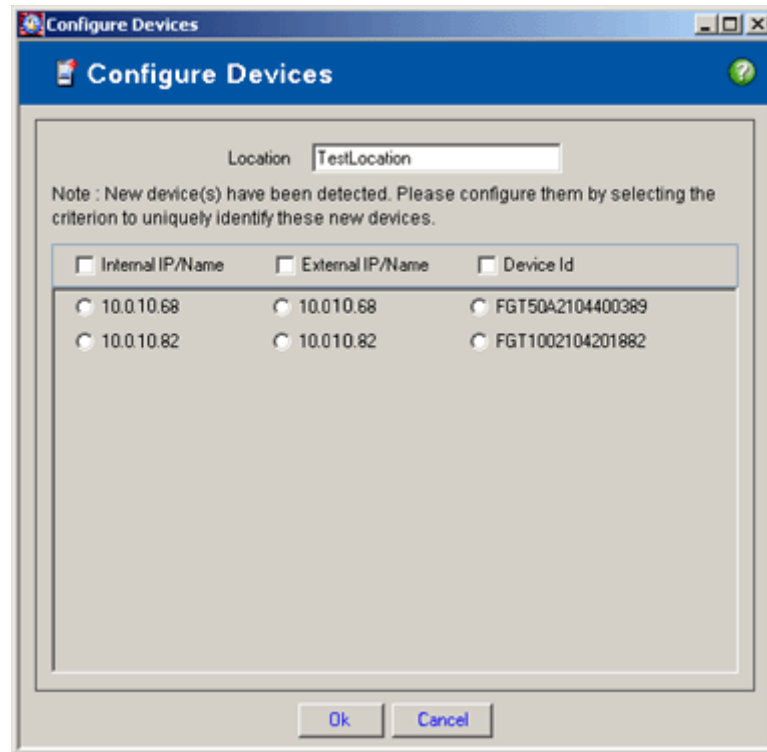
The ability to dynamically add or delete a device is important for MSSPs who often keep adding and deleting devices.

Configure Devices

1. While using the trial license, CIS configures all the devices automatically.
2. Under a permanent license, the Devices added from the Add Device wizard, appear under **Manually Added Device**. The Device manager displays the devices that are auto detected as **UnknownDeviceID**. You can configure these manually added and unknown devices from the Configure Devices screen.
3. On the Configure Devices screen, you can enter the Location Name where you want to associate all the devices.

The Configure Devices screen displays information about

Configure Device screen



- ❖ **Internal IP/Name:** This column displays information about the Internal IP/Name of the added devices.
 - ❖ **External IP/Name:** This column displays information about the IP addresses of the added devices.
 - ❖ **Device Id:** This column displays information about the Device Id of the added devices.
4. Select the any one of the above three options for the devices you want to configure and click **OK**.
 5. You can now License the manually added and unknown devices from the license manager or from the pop-up screen displaying the unlicensed devices.

Licensing Criteria

If the **Device Manager** identifies a new device ID in the log file, it adds the device ID under the syslog server as UnknownDeviceId, and if you add a device using the Add Device Wizard, it shows under **Manually Added Devices**.

To specify the licensing criteria for the newly associated devices click the **UnknownDeviceId/Manually Added Device** link, the **Licensing Criteria** dialog opens. Specify the criteria based to License the Device.

You can identify the Device by any of the following three identifiers:

- ❖ Internal IP/Name
- ❖ External IP/Name
- ❖ Device ID

Select any one of the identifiers and click **Save**. When you do this, CIS prompts you to license the device immediately, later, or never. If you select Now, The device immediately displayed as licensed on the **Devices** screen.

Note: Trial License automatically licenses the Devices.



You can report on a device only if it is licensed. Once you delete the device, you can reuse the License for another device. Click [here](#) to know how.

Policies

Clavister Insight offers a visual interface to enforce collection policy. If you have installed CIS as the Central Server, select the regional servers from the Regional drop-down list and enforce the policies. Policy defined on the Central server reflects back on the regional server.

Important: Policies defined in the policy Manager are not applicable to ISA and AV devices.

Collection Policy

This window displays the list of collection policy names. You can also Add, Edit and Delete a policy.

By default, the application provides you with the following policies:

- ❖ Default
- ❖ Collect All
- ❖ No Collection

You cannot edit/delete the default policies.

Add Collection Policy

1. To add a collection policy, click Add button. The Add Collection Policy window opens.
2. Specify the name of the policy.
3. Select a group/device under Syslog Server/Device column and choose specific devices in that group on which you want to enforce the policy.
4. Click Next. The Event Collection window opens.
5. In the Event Collection window, you can specify the severity of events to write into the delta files, specify the severity of events, which you want to stream to the monitoring console and the storing of the logs with respect to different activities occurring on the devices.
 - ❖ **Event Collection:** Specify the events to consider and save in the deltas while the raw log files are compressed into delta files and specify what events should be logged onto the Event Viewer from the raw log data that is fetched by the syslog server.
 - ❖ **Important:** By default, the **Monitoring** option is unchecked. Only if you select this option, CIS sends the log events for monitoring.

The Event Collection Screen

The screenshot shows a web-based configuration window titled "Add Collection Policy". It is divided into two main sections. The first section, "Event Collection", has two rows: "Syslog: Write" with a dropdown menu set to "Debug" and the text "and higher severity events to Delta.", and "Monitoring: Stream" with a checked checkbox and a dropdown menu set to "Warning" followed by "and higher severity events to Monitoring.". The second section, "Append Raw Log in Delta", has three rows: "Severity" with a checked checkbox and a dropdown menu set to "Warning", "Attack" with a checked checkbox, and "Virus" with a checked checkbox. At the bottom of the window are three buttons: "< Previous", "Finish", and "Cancel".

Follow the steps below to enable monitoring and to specify delta severity.

- To enable the streaming of events to the Event Viewer or to specify the events to consider for writing into the delta file, select from the drop-down list respective event severities. To view all events or to write all events in the delta file, select Debug. The available severity types are:
 - ❖ Emergency
 - ❖ Alert
 - ❖ Critical
 - ❖ Error
 - ❖ Warning
 - ❖ Notice
 - ❖ Information
 - ❖ Debug
- Append Raw Log in Delta:** In this section, you can specify to append the native or raw logs to deltas until the selected severity level from the drop-down list. CIS will not consider or append other events that do not come under the selection.

Note: CIS appends raw logs for only those devices that can stream their logs to CIS syslog server.

3. You can specify to store Events till a specific severity, Attack events, and Virus events. The available severity types are:
 - ❖ Emergency
 - ❖ Alert
 - ❖ Critical
 - ❖ Error
 - ❖ Warning
 - ❖ Notice
 - ❖ Information
4. Finally, click **OK**.

Policy Synopsis

1. Default and new Collection Policies added are populated on the main Policy Name list-box.
2. Select a policy name. The complete synopsis of the policy settings is displayed on the right pane of the same window. You can view the complete details of the events written to syslog and the events appended to the raw log data on the same screen.
3. If you want to modify the collection policy, click the Edit button.

Edit Collection Policy

Edit your selection of Group Name/Device and choose specific devices in that group on which you want to enforce the policy. Edit your preferences for collection policy as required and click **Save**.

Configure

With the Configure button, you can configure multiple devices at one time. This is useful when you have a large number of devices streaming logs to the syslog server

Options

You can specify global settings on all the profiles you create or on individual profiles by using the Options tab. This helps you to control the way Clavister Insight operates and optimize its functionality.

- ❖ **General:** You can configure the database to save the log data and check for new devices identified by the syslog server by using this tab.
- ❖ **Admin Alerts:** You can select the criterion to trigger an alert by CIS by using this tab.
- ❖ **Monitoring:** This tab shows up only on a regional server and you can switch off local monitoring on a regional server and forward all the events to the Central server by using this tab.
- ❖ **Protocol:** This tab lists the most common protocols and services categorized into families. This is helpful in protocol-based analysis of device activity. You may also add new protocols and families.
- ❖ **E-mail:** Use this option to specify the e-mail protocol SMTP to configure your messaging system.
- ❖ **Advanced:** This tab enables you to add, edit, and delete devices and syslog servers. After adding a device for analysis, you can import its logs using the syslog service and begin generating reports.

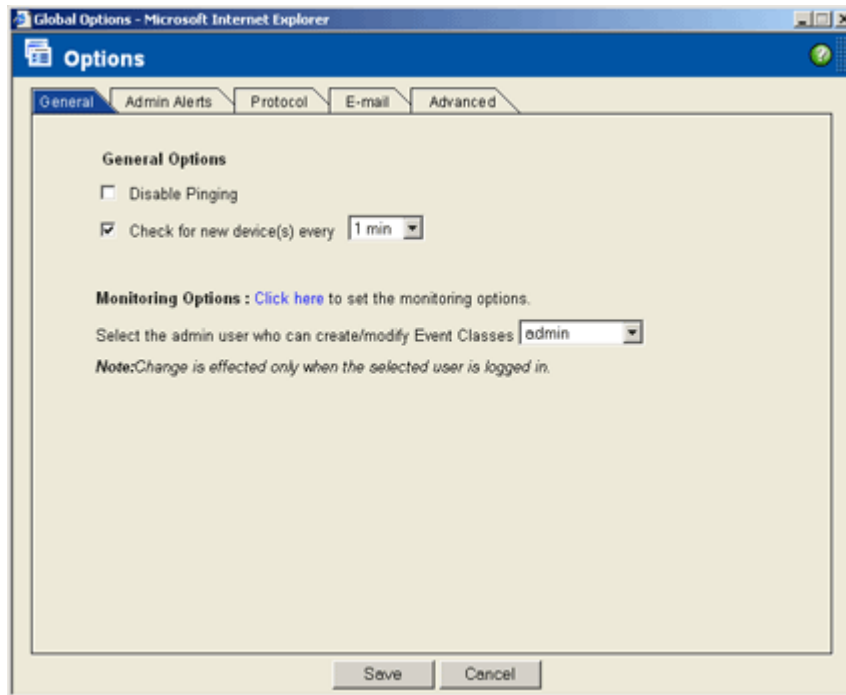


A Power User can only access the E-mail and Advanced tabs.

General Settings

You can specify the database that you want to use for storing processed log data by using the General Settings tab. By default, the device log data is stored in the built-in database but you can also choose to store log data in an enterprise database. You can configure an enterprise database from the **Options** → **General** screen.

The General Settings Tab



Disable Ping: You can enable or disable ping activity from the syslog server, which at times occurs frequently and hence makes the network busy. By disabling ping, you can keep a check on the ping operation performed by the Syslog Server to identify the status of devices configured to Syslog Server.

Check for new devices every: Select this check box to check for the unconfigured devices every:

- ❖ 1 min
- ❖ 10 min
- ❖ 30 min
- ❖ 1 hour

Based on the interval selected, a pop-up window displaying the Unlicensed Devices show up whenever CIS finds a new device and prompts you to configure and license it.

Monitoring Options

Click on the link here and the Set Monitoring Options window opens where you can set the monitoring options. You can set the monitoring based on the following:

- ❖ Maximum number of records for a Monitor
- ❖ Maximum number of records for Event Viewer

Maximum number of records for a Monitor: This option lets you specify the maximum number of records to consider for a monitor at a given instance of time. If there are more Alert Events then all of the events occurring within the period and exceeding the specified Maximum Number of records are dropped.

Maximum number of records for Event Viewer: This option lets you specify the maximum number of records that you want the event viewer to display.

Note: Restart the CIS server for the changes to take effect.

Selecting a admin user who can Create/Modify Event Classes

Select an admin user account from the drop-down list to assign the privilege to create/modify Event Classes also can change/reset the threat level associated with an event displayed in the event viewer, graph types and reports.

Selecting the admin user:

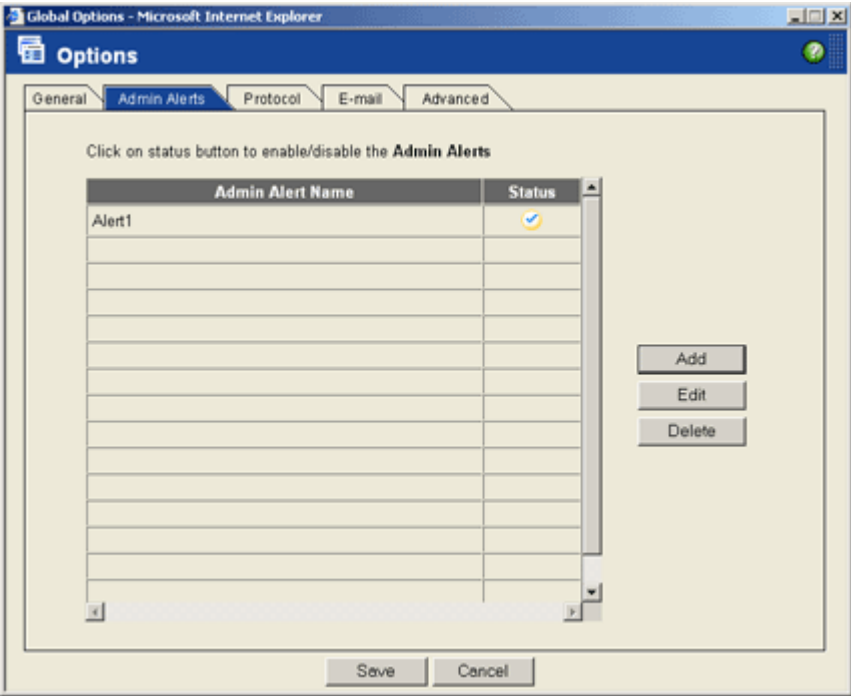
All the admin user accounts defined from the User manager are shown in the drop down list.

1. Select a user account to grant the privilege to create/modify Event Classes.
2. Save your settings, logout from the application and login with selected admin user credentials to be able to reset the threat levels.

Admin Alerts

Use the **Admin Alerts** screen to select the criterion on which you want to trigger an Alert. To specify the alert criterion, follow the instructions given below:

Admin Alerts



Add Admin Alert

1. On the Alerts main screen, click the Add button. The Configure Admin Alerts window opens.
2. Enter the alert details (Alert Name and Alert Description) in the Alert Details section.

3. To specify the alert criteria, select any one of the following criterion:
 - ❖ Alert when user account is locked.
 - ❖ Alert when the specified device or devices are down.
 - ❖ Alert when the event count from specified devices exceeds a specified threshold.
 - ❖ Alert when the storage space is less than the specified disk space. You can set either Warning or Critical e-mail alerts based on the availability of the storage space.
4. Select the devices on which you want to generate admin alerts. Click Next.

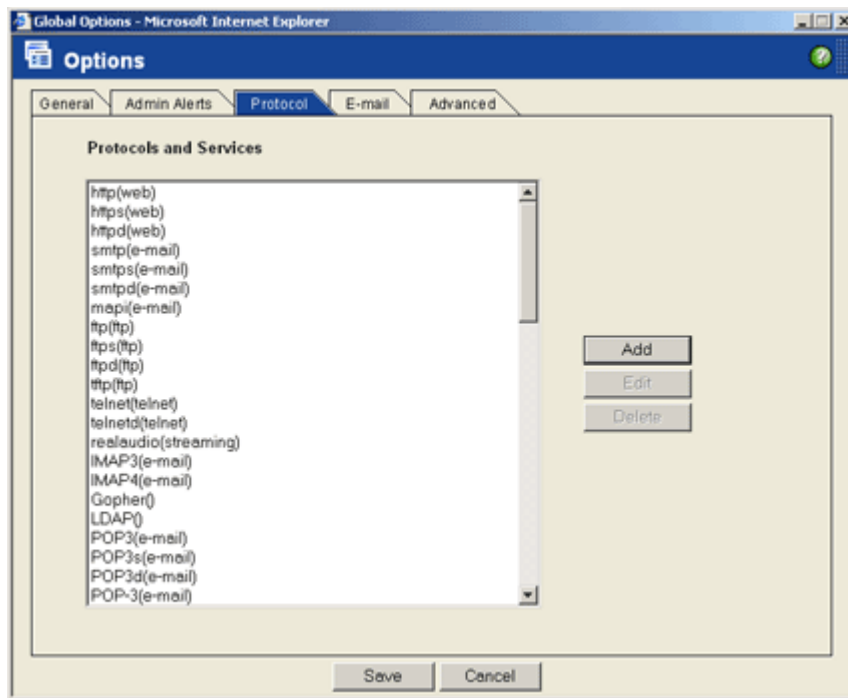
Alert Notification

1. Enter details of the method by which you want to be notified. Click **Add** to add a mail recipient.
2. Enter the time **From** to time **To** in the hh:mm format and the recipient's e-mail address. If an alert triggers within the specified time bounds, the specified recipient receives the Alert message.
3. Click the **Add** button. This adds the e-mail ID to the recipient list.
4. Enter the subject and the message that should appended to the alert notification.
5. To configure your SMTP server, go to the E-mail dialog box in the **Options** tab. Click **Save**.
6. Click **Finish**.

Protocol Setting

The **Protocols and Services** list box displays all the protocols that Clavister Insight analyzes and reports on, according to their group category. For instance, the protocols POP3, SMTP, and IMAP4 fall under the group 'E-mail' since they deal with sending and receiving e-mail. You can add additional protocols and assign them to existing or new groups, and generate a report on the protocol usage in where the protocols are categorized according to the groups to which you have assigned them.

The Protocol Settings Tab



A protocol is a set of rules for transferring data over the Internet. Some common protocols used are HTTP, FTP, SMTP, and TCP/IP. Clavister Insight reports on activity by protocol and on protocol families, which are groups of related protocols.

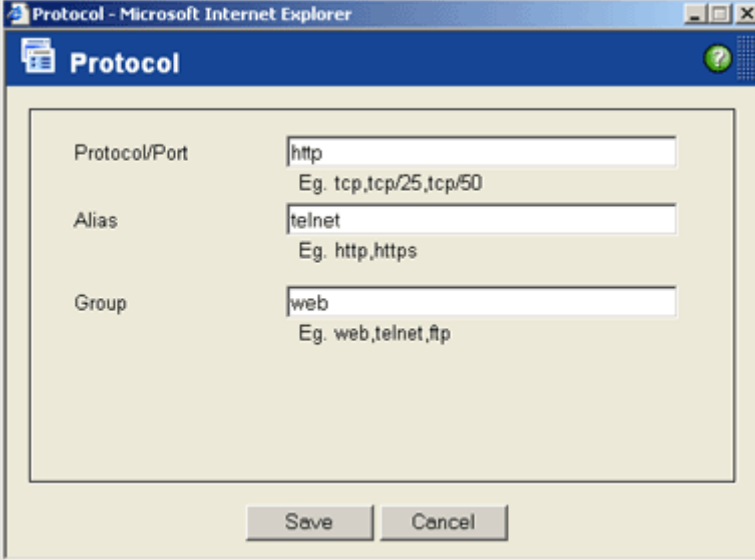
To add a protocol: Click **Add**. Enter the name of the protocol and the type of traffic the protocol represents. For example, the protocol POP3 categorizes under e-mail since it is a protocol used to send and receive e-mail.

1. **Protocol/Port:** Enter the name of the protocol.

2. **Alias:** Enter the alias name in the Alias box.
3. **Group:** Enter the name of the protocol group to which the protocol belongs.
4. Click **Save**.

You can see the protocol populated in the protocol list.

The Add Protocol Screen



The screenshot shows a web browser window titled "Protocol - Microsoft Internet Explorer". The main content area is a form titled "Protocol". It contains three input fields with labels and examples:

- Protocol/Port:** The input field contains "http". Below it, the example text reads "Eg. tcp,tcp/25,tcp/50".
- Alias:** The input field contains "telnet". Below it, the example text reads "Eg. http,https".
- Group:** The input field contains "web". Below it, the example text reads "Eg. web,telnet,ftp".

At the bottom of the form are two buttons: "Save" and "Cancel".

To edit a protocol: You cannot edit the Default protocols but user-defined protocols are editable. Make any changes needed in the protocol name as necessary. The edited name should be exactly as you want it to appear in the Clavister Insight reports.

To delete a protocol: Select a protocol from the list and click **Delete**. This will remove the protocol from the list.

Click **Save**.

E-mail Settings

Enter the required information for your SMTP mail server in the appropriate boxes.

The E-mail Settings Tab

Global Options - Microsoft Internet Explorer

Options

General Admin Alerts Protocol **E-mail** Advanced

SMTP

Server sysadmin@clavister.com Settings

User ID user@clavister.com

SMTP Server requires authentication

Test SMTP

Recipient's mail id Send Test Mail

Save Cancel

- ❖ **SMTP:** Simple Mail Transfer Protocol is a protocol for sending e-mail messages between servers. An e-mail client using either POP or IMAP can then retrieve the messages.
- ❖ **Server:** Domain name of the e-mail server supporting the Post Office Protocol (POP) protocol and saving mails e.g. www.hotmail.com.
- ❖ **User ID:** Enter the user name of the authorized administrator user ID.
- ❖ **SMTP Server Requires Authentication:** If your SMTP server requires authentication, select the SMTP server requires authentication check box and enter the server name and user ID in the text spaces provided.
- ❖ **Test SMTP:** To verify your SMTP settings, you can send a test mail. To do this, enter the intended recipient's e-mail ID in the **Recipient's mail ID** box and click the **Send Test Mail** button.

The E-mail Settings Screen

The screenshot shows a web browser window titled "SMTP Authentication - Microsoft Internet Explorer". Inside the browser is a dialog box titled "Options". The dialog box has a light beige background and a blue header. It contains the following fields:

- Type:** A dropdown menu with "LOGIN PLAIN" selected.
- User Name:** A text box containing "User".
- Password:** A text box with 10 black dots for masking.
- SMTP Port:** A text box containing "25".

At the bottom of the dialog box are two buttons: "Save" and "Cancel".

Follow the steps described below to specify the e-mail settings:

1. Specify the authentication type to login to the SMTP server from the **Type** drop-down list.
1. Enter the **User name** and **Password**.
2. Specify the SMTP port number in the **SMTP Port** box.
3. Click **Save**.

Monitoring

Forward: Select this option to forward all events to the CIS Central. When you do this, events are monitored at both the regional and Central. On the Central, you can monitor all events forwarded by the Regional, on the regional, whereas you can monitor all events above the selected severity level on Regional.

Forward Only Mode: Select this option to turn off monitoring on the regional. Then you can monitor all events on Central.

Click **Save**.



This option is available only on CIS regional server.

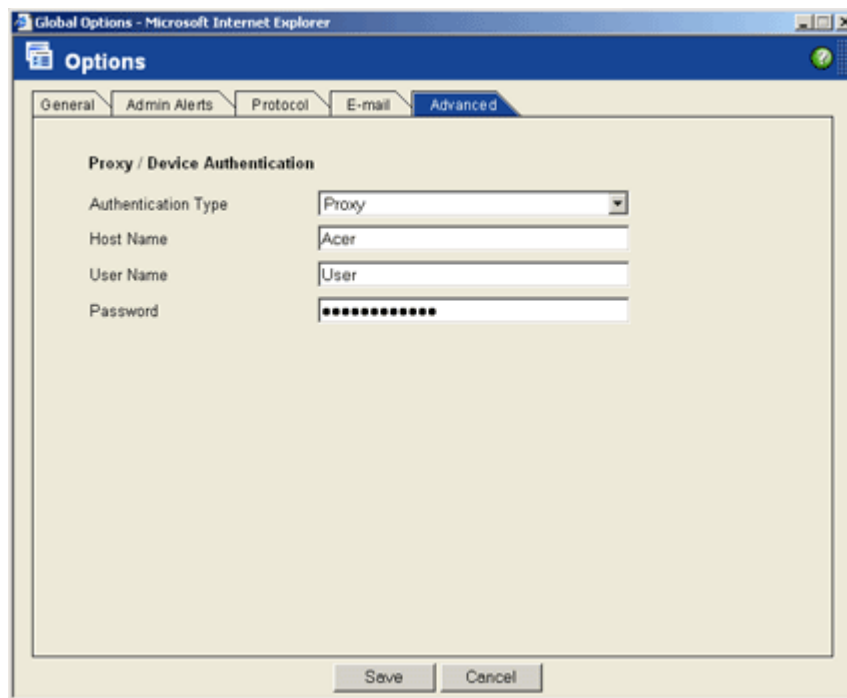
Advanced Settings

Some organizations separate their local networks from the rest of the Internet by installing a device or "gateway." A device is a system or software configured to prevent particular types of access or information from entering the network. Most devices block the flow into the local area network, but allow individuals to access most resources outside of the network.

Clavister Insight lets you enter details of a device in the Device Configuration screen, which you can then use when connecting to an FTP site from behind that device. You can configure the device once, and then assign that device configuration to those sites that require it.

The following table lists all conventional device types and the information about each that you will need to procure and enter into Clavister Insight.

The Advanced Settings Tab



The screenshot shows a web browser window titled "Global Options - Microsoft Internet Explorer" with a tab labeled "Options". The "Advanced" tab is selected, and the "Proxy / Device Authentication" section is visible. It contains the following fields:

Field	Value
Authentication Type	Proxy
Host Name	Acer
User Name	User
Password

At the bottom of the dialog box are "Save" and "Cancel" buttons.

Select the authentication type from the Authentication Type drop-down list. They are

Type of Device	Information you must specify
Site	Host Name (or Address), User Name (ID)
User after logon	Host Name (or Address), User Name (ID), Password
Proxy	Host Name (or Address)
Transparent	User Name (ID), Password
User with no logon	Host Name (or Address)
User FwID@remoteHost	Host Name (or Address), User Name (ID), Password
User RID@HostFwID	Host Name (or Address), User Name (ID), Password
User RID@FwID@Host	Host Name (or Address), User Name (ID), Password

1. Enter the **Host Name** in the text box.
2. Enter the User Name and the Password in the text boxes provided.
3. Click **Save**.

To enter device information, get information about your device from your administrator.

App Status

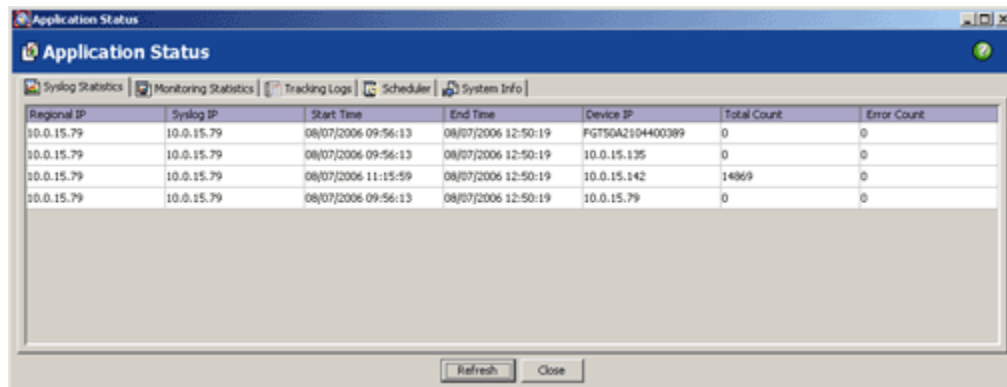
The **App Status** (Application Status) screen displays information on various components that are important to manage and keep the Clavister Insight up and running. You can view information about the delta files transmitted from the syslog server. It also provides you with information on the status of log files, device IPs, log file names, last updated date and time, file sizes, components required by Clavister Insight for the installation, and scheduled tasks.

The **Application Status** screen provides information on the following.

Syslog Statistics

This tab displays details of the syslog server on a regional CIS server that includes:

Syslog Statistics



Regional IP	Syslog IP	Start Time	End Time	Device IP	Total Count	Error Count
10.0.15.79	10.0.15.79	08/07/2006 09:56:13	08/07/2006 12:50:19	FGT50A2104400389	0	0
10.0.15.79	10.0.15.79	08/07/2006 09:56:13	08/07/2006 12:50:19	10.0.15.135	0	0
10.0.15.79	10.0.15.79	08/07/2006 11:15:59	08/07/2006 12:50:19	10.0.15.142	14869	0
10.0.15.79	10.0.15.79	08/07/2006 09:56:13	08/07/2006 12:50:19	10.0.15.79	0	0

- ❖ **Regional IP:** Displays the IP address of the regional CIS server on which the syslog server is installed.
- ❖ **Syslog IP:** Displays the IP address of the syslog server. The screen displays the Syslog server statistics.
- ❖ **Device IP:** Displays the IP address of the device configured under a specific Syslog IP.

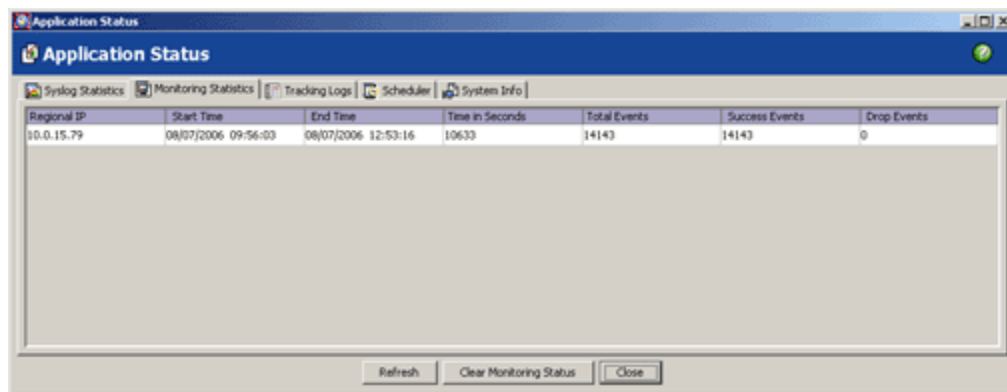
- ❖ **Start Time:** Displays the start time of the refresh interval.
- ❖ **End Time:** Displays the end time of the refresh interval.
- ❖ **Total Count:** Displays the total number of events parsed.
- ❖ **Error Count:** Displays the total number of events that failed to parse.

Use the Refresh button to update the status of statistics displayed for the Syslog Server.

Monitoring Statistics

This tab displays details the monitoring statistics by a regional server that includes:

Monitoring Statistics



The screenshot shows a window titled 'Application Status' with a tabbed interface. The 'Monitoring Statistics' tab is active, displaying a table with the following data:

Regional IP	Start Time	End Time	Time in Seconds	Total Events	Success Events	Drop Events
10.0.15.79	08/07/2006 09:56:03	08/07/2006 12:53:16	10633	14143	14143	0

At the bottom of the window, there are three buttons: 'Refresh', 'Clear Monitoring Status', and 'Close'.

- ❖ **Regional IP:** Displays the IP address of the device on which the CIS Regional is installed.
- ❖ **Start Time:** Displays the start time when monitoring began.
- ❖ **End Time:** Displays the end time where the monitoring has finished.
- ❖ **Time in Seconds:** Displays the total time in seconds, for which these statistics are displayed.
- ❖ **Total Events:** Displays the total number of events monitored in a given time period.
- ❖ **Success Events:** Displays the total number of events successfully monitored in a given time period.
- ❖ **Drop Events:** Displays the total number of events dropped in a given time period.

Use the Refresh button to update the status of statistics displayed for Monitoring module of the regional server.

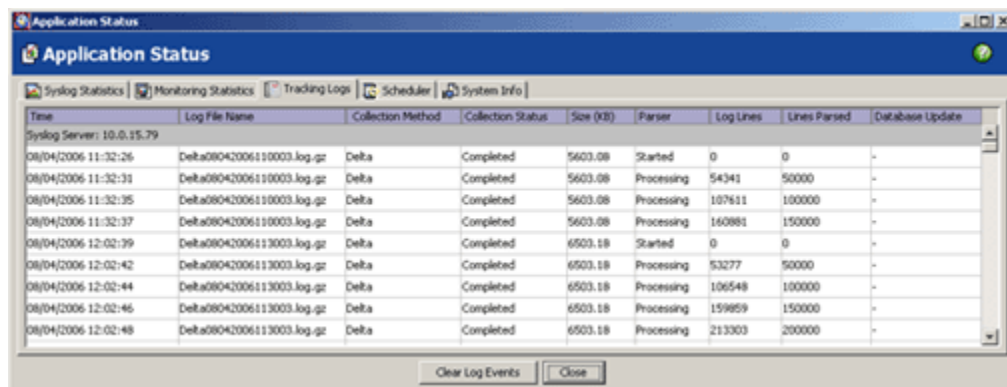
Tracking Logs

This tab displays information on the delta log files successfully received by Clavister Insight from a syslog server and updated to the database. If a single delta file saves records of multiple devices, corresponding device names are displayed. The following information can be viewed on the **App Status** screen:

- ❖ **Event Time:** This field displays the timestamp of occurrence of the status event.
- ❖ **Log File Name:** The name of the log files.
- ❖ **Log Collection Method:** Displays the File collection method for example Syslog Delta, FTP, Local File etc.
- ❖ **Log Collection Status:** Informs you the status of log collection for example:
 - ❖ Started collecting from ftp://ftp.mysite.com
 - ❖ Completed etc.,
- ❖ **Size:** This is the total size (in Kilobytes) of the collected file.
- ❖ **Parser:** The status of parsing activity is shown here as Started, Completed, or Failed.
- ❖ **Log Lines:** Displays the total number of lines in the log file.
- ❖ **Lines Parsed:** This field displays the total number of lines that are parsed successfully. The number of lines that could not be parsed can be calculated from the Log Lines minus Lines Parsed.
- ❖ **Database Update:** The status of Update is displayed as Started, Completed, and Failed.

Use the **Clear Log Events** button to delete content about old log files so that the details of new log files updated to the database can be displayed.

Tracking Log Status



The screenshot shows the 'Application Status' window with the 'Tracking Logs' tab selected. The window title is 'Application Status' and it contains a table with the following columns: Time, Log File Name, Collection Method, Collection Status, Size (KB), Parser, Log Lines, Lines Parsed, and Database Update. The data in the table is as follows:

Time	Log File Name	Collection Method	Collection Status	Size (KB)	Parser	Log Lines	Lines Parsed	Database Update
Syslog Server: 10.0.15.79								
08/04/2006 11:32:26	Delta08042006110003.log.gz	Delta	Completed	5603.08	Started	0	0	-
08/04/2006 11:32:31	Delta08042006110003.log.gz	Delta	Completed	5603.08	Processing	54341	50000	-
08/04/2006 11:32:35	Delta08042006110003.log.gz	Delta	Completed	5603.08	Processing	107611	100000	-
08/04/2006 11:32:37	Delta08042006110003.log.gz	Delta	Completed	5603.08	Processing	160881	150000	-
08/04/2006 12:02:39	Delta08042006113003.log.gz	Delta	Completed	6503.18	Started	0	0	-
08/04/2006 12:02:42	Delta08042006113003.log.gz	Delta	Completed	6503.18	Processing	53277	50000	-
08/04/2006 12:02:44	Delta08042006113003.log.gz	Delta	Completed	6503.18	Processing	106548	100000	-
08/04/2006 12:02:46	Delta08042006113003.log.gz	Delta	Completed	6503.18	Processing	159859	150000	-
08/04/2006 12:02:48	Delta08042006113003.log.gz	Delta	Completed	6503.18	Processing	213303	200000	-

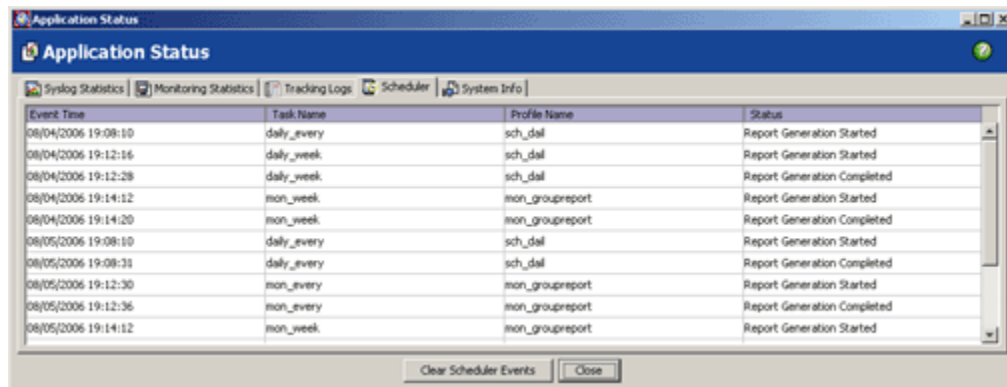
At the bottom of the window, there are two buttons: 'Clear Log Events' and 'Close'.

Scheduler

This tab provides information on the status of the regularly scheduled tasks configured for different profiles. The Scheduler records a history of how an event fares when it runs — whether it runs successfully or not, what errors, if any, occur and related information. It provides you with an overview of the tasks and their schedules. It contains a listing of all the reports scheduled to run, the profiles they are associated with, and their status. Use the **Clear Scheduler Events** button to delete all the old events and display only the latest events created by the Scheduler tasks.

- ❖ **Event Time:** Lists the date and time on which the scheduled report generation started.
- ❖ **Task Name:** Lists the name of the task generating the report.
- ❖ **Profile Name:** Lists the profile name associated with the task.
- ❖ **Status:** Reports whether the task ran successfully or that one or more errors occurred. The error messages will explain any problems that the scheduled events encountered. This column also reports whether the scheduled report has been mailed and/or uploaded to ftp site.

The Scheduler Tab



Event Time	Task Name	Profile Name	Status
08/04/2006 19:08:10	daly_every	sch_dal	Report Generation Started
08/04/2006 19:12:16	daly_week	sch_dal	Report Generation Started
08/04/2006 19:12:28	daly_week	sch_dal	Report Generation Completed
08/04/2006 19:14:12	mon_week	mon_groupreport	Report Generation Started
08/04/2006 19:14:20	mon_week	mon_groupreport	Report Generation Completed
08/05/2006 19:08:10	daly_every	sch_dal	Report Generation Started
08/05/2006 19:08:31	daly_every	sch_dal	Report Generation Completed
08/05/2006 19:12:30	mon_every	mon_groupreport	Report Generation Started
08/05/2006 19:12:36	mon_every	mon_groupreport	Report Generation Completed
08/05/2006 19:14:12	mon_week	mon_groupreport	Report Generation Started



Only Administrators and Normal users have access to App Status information.

System Info

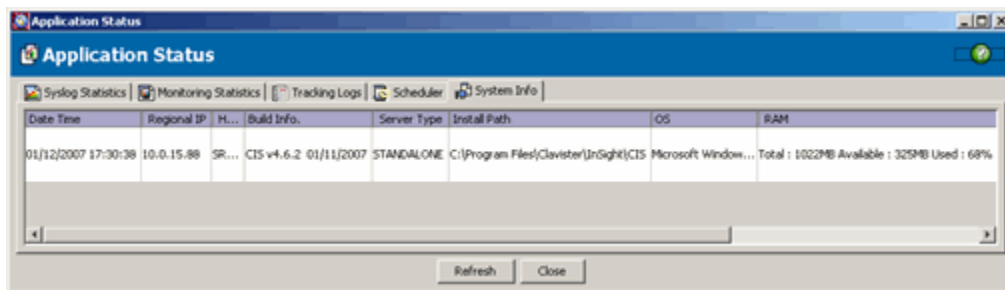
This tab displays details of the following:

- ❖ **Date Time:** Displays the timestamp of when the status event occurred.

- ❖ **Regional IP:** Displays the IP addresses of the regional to which this device is configured.
- ❖ **Host Name:** Displays the hostname of the system.
- ❖ **Build Info:** Displays the build number of the CIS which is currently installed on this system.
- ❖ **Server Type:** Displays if the server type is of Central, Regional, or a Standalone.
- ❖ **Hard Disk:** Displays the information of total disk space and available disk space for each drive on the system and the type of file system existing on this drive.
- ❖ **OS:** Displays the operating system of the system running CIS server.
- ❖ **RAM:** Displays the value for size of RAM on this system.
- ❖ **CPU Usage:** Displays the value for percentage of CPU resources used for accomplishing a given task.

Install Path: Displays the installation path of CIS server on this system.

System Information



Use the Refresh button to update on any changes in the system information.

Users

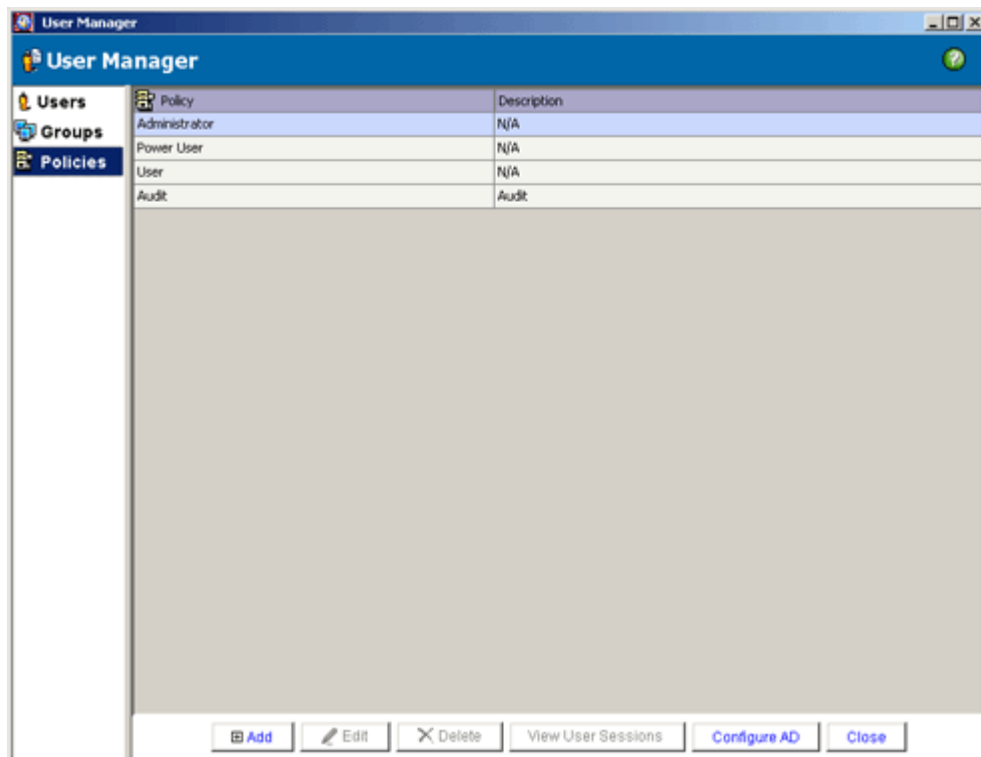
You can create users with different access rights through the User Manager. This helps you manage and ensure security of your profiles and associated policy settings. Important: Only an admin user can access User Manager.

Important: Only an admin user can access User Manager.

User Manager UI in CIS 4.6 mainly comprises of the following 3 categories

- ❖ Users
- ❖ Groups
- ❖ Policies

User Manager Main Screen

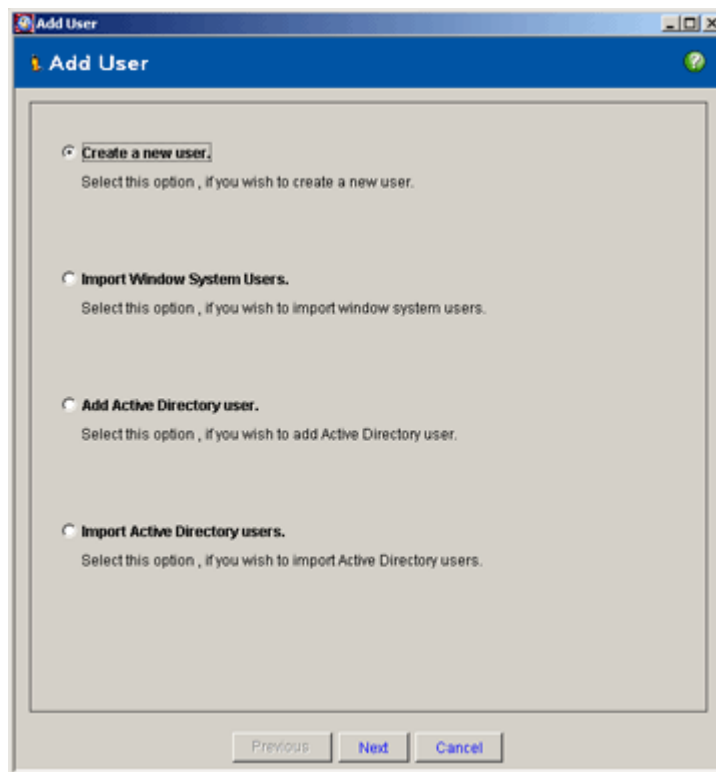


Users

An administrator can create Administrator, User and Power User accounts. If you are a default admin user, only then you have access to all the modules of the application. Power user can access all the other functionalities except Devices, Groups, Users, Licenses, Alerts, and AppStatus. However, the administrator defines his scope. A User (Report user) can only run and view all/some of instant reporting sections as specified by the administrator.

You can add new user accounts to CIS by the following ways:

- ❖ Create a new user
- ❖ Import Windows System Users
- ❖ Add Active Directory User
- ❖ Import Active Directory users



Create a New User

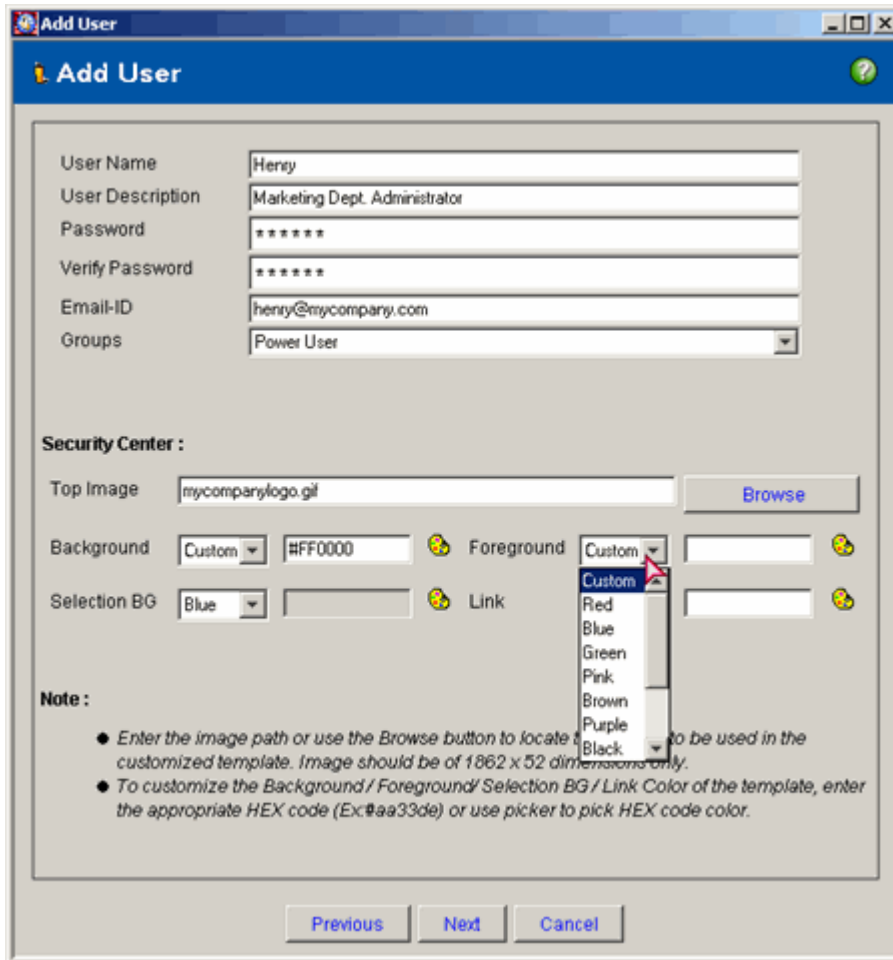
Clavister Insight provides three levels of access rights: Administrator, Power User, and User.

Each of the user types and the rights it enjoys are as follows:

- ❖ **Administrator:** Users in this group have total control and can create, delete or edit any user with any right (administrator or normal), edit configuration settings, modify schedules, and add or delete licenses.
- ❖ **Power User:** Users in this group can create, edit, delete, view profiles, schedule tasks and generate reports. A Power User can access the settings in the **Options** dialog. However, this user is restricted from Groups, Devices, Users, Licenses and Alerts.
- ❖ **User:** User accounts in this group can only generate all or some instant reports sections according to the assigned privileges in the policy to which the user is associated. While creating a policy, you can specify the report categories of devices accessible to the users associated with the policy. Note that there are separate reporting sections for devices.

Follow the steps described below to add a user:

1. On the main screen, click **Users**. The User Manager screen opens.
2. Select the Users option and click **Add**. The Add User dialog opens.
3. Specify a login name for the user in the **User Name** in the text box.
4. Specify the description for the user account you want to add.
5. Enter the corresponding password in the **Password** text box and re-enter it again in the **Verify Password** text box.
6. Specify the valid e-mail ID of the user.
7. From the **User Group** drop-down list, select a group that defines the privileges for the user.



If you are creating a Power user then you need to specify the device groups and devices that he will have the privilege to access and report on, and for a report User, you need to specify the device groups and the report categories that he will be able to generate reports. Click **Save**.

Note: Any Normal User account carried forward from previous versions of CIS shows up as a Power User, which is non-editable and you cannot delete him.

Option to customize the Security Center view

Users have the option to change the look and feel of both the reporting and monitoring portals.

Follow the steps described below to customize:

1. Browse to select the top image you want to be present on the reporting and the monitoring portals.
2. To define the text and link colors to be used in Security Center UI, specify the **Text/Link** color from the available drop-down lists OR select the Custom option and specify the HEX code or use the picker option, for the following:
 - ❖ **Background**: To set the Background color for the Security center tree.
 - ❖ **Foreground**: To set the colors of the Text.
 - ❖ **Link**: To select the color the Link should change to on a mouse hover.
 - ❖ **Selection BG**: To set the color of the background when a tree node is selected.
3. Click **Save**.

Editing a User

While editing a user on the Edit User screen, you can change all of the available fields except the User Name.

Import Windows System Users

Native OS user authentication allows you to leverage single sign-on thereby eliminating the need to maintain separate security credentials.


Note: You can only import the user accounts present in the windows operating system.

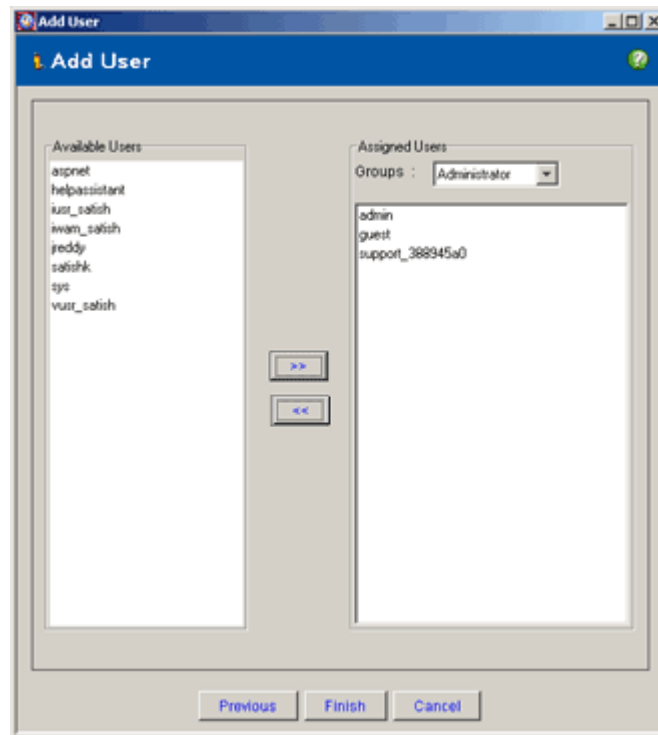
So to create and import a new windows user account into CIS, define a new user for Windows operating system from Control Panel → Administrative Tools → Computer Management → System Tools → Local Users and Groups.

The user account that you have just created is displayed in the **Add User** window and can be imported into the CIS application.

Importing User Accounts from Windows Operating System

1. Select **Import Windows System Users** from the **Add User** wizard. Click **Next**.
2. A window is opened displaying all the existing user accounts from the windows operating system.

3. Select the User accounts that you want to import into CIS and into which Group.
4. Configure at least one device for the user on which he can monitor or report on.
5. Click  icon to move the user into the assigned user list.
6. Click **Finish**.



Note: By default, users cannot report on any devices. Administrator must grant them the privilege to access device and report sections.

Add Active Directory User

CIS facilitates to add a new domain user into the specific groups. In this case, no domain privileges are necessary and you can directly add a new user with the domain account credentials.

Add Active Directory User:

1. Select **Add Active Directory User** wizard. Click Next.
2. A window is opened where you need to enter the active directory server details.
3. Specify the name of the Domain and the Server Name/IP of the domain.
4. Enter the **Active directory port** for the server. By default port 389 is used in connecting to AD server.
5. Specify the User Name and Password for the new user account using which the respective user would login into the CIS application.
6. Click **Validate User** to check the entered user account details.
7. Click **Next**.

Import Active Directory Users

Clavister Insight supports the use of an external LDAP-enabled directory to authenticate and authorize users on a per group basis.

LDAP group-based authentication for the CIS Appliance can be configured to support Microsoft Active Directory By keeping the authentication centralized on your directory, a security administrator can always know

who is accessing network resources and can define user/group-based policies to control access.

Active Directory natively supports a fully integrated public key infrastructure and Internet secure protocols, such as LDAP over SSL, to let information being accessed beyond their firewall to extranet users.


Important: Configure your Active directory Server details before you import its user accounts to CIS.

The screenshot shows a window titled "Add User" with a sub-header "Add User". Below this is a section titled "Active Directory Server Details" containing several input fields:

- Domain:** A dropdown menu with "eignetworks.com" selected.
- Server Name/IP:** A text box containing "10.0.15.199". Below it is an example: "Example: dir.company.com".
- Active Directory Port:** A text box containing "389".
- Group DN:** A text box containing "cn=users,dc=hyd,dc=eignetworks,dc=com". Below it is an example: "Example: ou=groups,dc=dir,dc=mycompany,dc=com".
- Administrator Name:** A text box containing "venkatesh".
- Password:** A text box with masked characters "*****".

Below the fields is a **Note:** "Please review the above Active Directory Server details." At the bottom of the dialog are three buttons: "Previous", "Next", and "Cancel".

Importing Active Directory Server User Accounts:

1. Select Importing Active Directory Server Users from the Add User wizard. Click Next.
2. A window is opened displaying all the existing user accounts from the Active Directory server.
3. Select the user accounts that you want to import into CIS and into which Group.
4. Click  icon to move the user into the assigned user list.
5. Click Finish.

User Sessions

Click View User Sessions to open the User Sessions screen. This screen records a history of users accessing Clavister Insight and provides you an overall view of the user activity. It enlists all the users who logged on to Clavister Insight, the client machine name and the data and time they logged in. The admin user who has currently logged in can clear all the recorded user sessions by clicking the Clear Sessions button.

- ❖ Status: This reports the operation (login or logout) that the user performed.
- ❖ User Name: This lists the user name with which the user logged on to Clavister Insight.
- ❖ System: This lists the client machine from which the user logged on to Clavister Insight.
- ❖ Date: This lists the date and time on which the operation was performed.

Status	User Name	System	Date
Login	admin	127.0.0.1	4/12/2006 9:55:22
Logout	admin	127.0.0.1	4/12/2006 9:55:42
Login	admin	127.0.0.1	4/12/2006 9:56:0
Logout	admin	127.0.0.1	4/12/2006 11:9:29
Login	admin	127.0.0.1	4/12/2006 11:13:19
Logout	admin	127.0.0.1	4/12/2006 13:12:36
Login	admin	127.0.0.1	4/12/2006 13:12:53
Logout	admin	127.0.0.1	4/12/2006 13:19:28
Login	admin	127.0.0.1	4/12/2006 13:19:32
Logout	admin	127.0.0.1	4/12/2006 13:36:47
Login	admin	127.0.0.1	4/12/2006 13:36:58
Logout	admin	127.0.0.1	4/12/2006 14:2:32
Login	admin	127.0.0.1	4/12/2006 14:2:42
Logout	admin	127.0.0.1	4/12/2006 14:4:10
Login	admin	127.0.0.1	4/12/2006 14:4:35
Login	admin	127.0.0.1	4/12/2006 14:5:14
Login	admin	127.0.0.1	4/12/2006 14:6:44

Groups

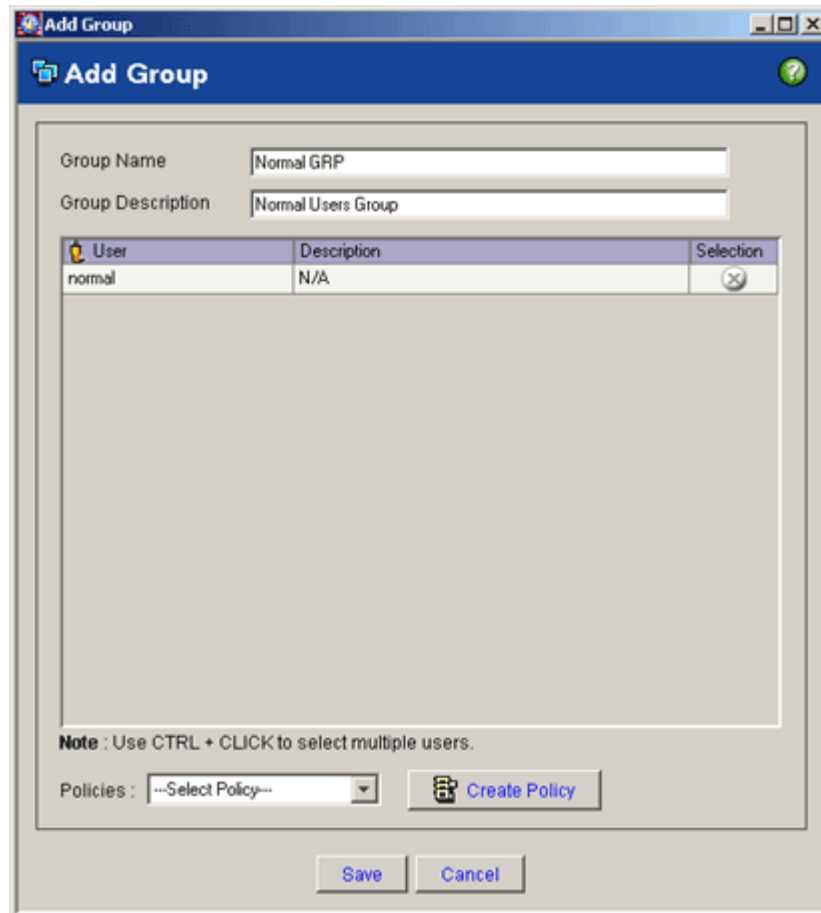
Using the Groups option, an administrator can create and define policy bound users who will be a part of the group. You can even select to define a policy from


the groups' option, which subsequently can be associated with the users who belong to the selected group.

Add Group

Using the Add Group wizard, an administrator can create a group; add existing users to the group and associate policies.

1. Specify a Group Name that you want to define and give an appropriate Group Description.
2. Add Group window lists all the existing user accounts added in the application.
3. Select the users whom you want to make part of this group.
4. Select a policy you want to associate with from the Policies drop-down list or define a new policy for the group.
5. Click Save.



User	Description	Selection
normal	N/A	

Policies

Using the policies option, an administrator can define the criteria on granting permission to use the Monitoring and Reporting modules.

Add Policy

Using the Add Policy wizard, an administrator can define the criteria on granting permission to use the Monitoring and Reporting modules.

1. Specify a Policy Name that you want to define and give an appropriate Policy Description.
2. Select the modules that a user can access associated with this policy.
3. If Reporting module is selected, click Next and the query selection screen opens.
4. Select the query sections, a user associated with this policy could report on.
5. Finally, click Finish.

Audit Triggered Alerts

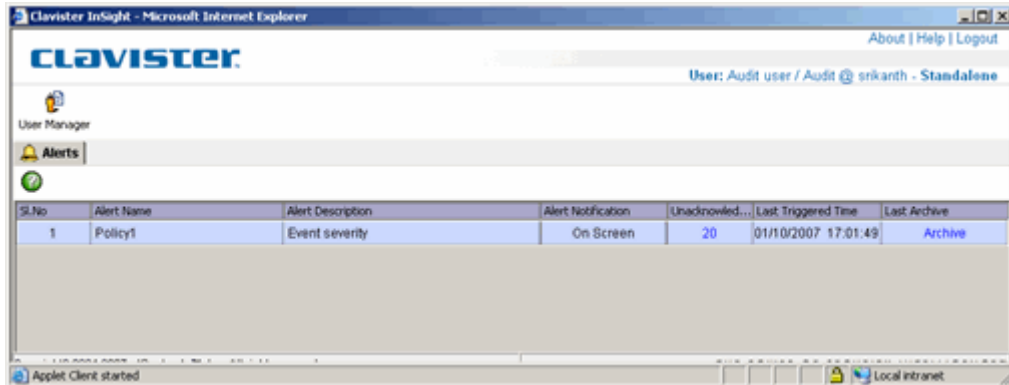
Using this option, admin user has the option to create a user account whose sole priority is to monitor the alerts generated for a specific user.

How to create and assign privileges to an Audit User?

1. Create a Sample user account from the user manager with Monitoring privileges.
2. Create another user account (Audit User) that is only created to monitor/audit the alerts triggered for the policies created by the sample user.
3. While assigning a policy, select Access using Console module and select the Sample user (created in step 1) from the drop-down list for which the Audit User account will monitor and acknowledge the triggered alerts.

- When the Audit User (created in step 2) logs in to the application, he would be able to audit and acknowledge the alerts triggered by the policies created by the Sample user.

Alerts UI for the Audit User



The screenshot displays the Clavister Insight Alerts UI for the Audit User. The interface includes a header with the Clavister logo, navigation links (About | Help | Logout), and the user information (User: Audit user / Audit @ srikanth - Standalone). Below the header, there are tabs for User Manager and Alerts. The Alerts tab is active, showing a table with one alert entry.

Sl.No	Alert Name	Alert Description	Alert Notification	Unacknowledged...	Last Triggered Time	Last Archive
1	Policy1	Event severity	On Screen	20	01/10/2007 17:01:49	Archive

Licenses

This chapter provides information on how to license your copy of Clavister Insight and the devices you want to report on. It also explains how to manage your licenses.



In a distributed setup, devices can be licensed only from the License Manager on the CIS Central.

License Requirements

At the time of first installation, Clavister Insight automatically creates a machine-specific trial license key using the MAC address. Once the license key is generated, you cannot use it to run Clavister Insight on any other machine. The trial license key can be used to license 10 devices. Each device can be analyzed for 21 days after it is licensed and the trial will expire 21 days after the last device is licensed. If your evaluation has been satisfactory, write to Clavister requesting for a permanent license.

For a permanent license, use the Export Identifier to create a text file `C:\Program Files\Clavister\Insight\CIS\CISSystemIdentifier.txt` that stores the device identifier information. Send the file to Clavister, and we will generate a license key for you.

If you have more than one device to license, let us know the number and we will generate an appropriate license key.

Licensing Devices Identified by CIS Syslog Server

When a new device ID streamed by the syslog server is detected, it is added under the syslog server as `UnknownDeviceId`. Click the `UnknownDeviceId` link and specify the criteria based on which you want this device licensed.

Note: In case you are evaluating the trial copy of CIS, streaming devices are automatically licensed.

A device can be identified by any of the following three identifiers:

- ❖ Internal IP
- ❖ External IP
- ❖ Device ID

Select an identifier and click **Save**. The device can be licensed immediately, later or you can choose not to license it for ever.

If you select the option to license it **Now**, the device is immediately licensed. But if your CIS installation is of type Regional, the device that is identified by the syslog can be only added from there. Licensing all such devices added from the CIS regional servers is only possible from the CIS Central.



Only licensed devices can be reported on.

Licensing an Unconfigured Device

Follow the steps described below to license an unconfigured device:

1. Identify the IP address in the log file and add it in the **Devices/Groups**.
2. On the **License Manager** screen, select the **Licenses** tab.
3. Select a license key and click **Manage**.
4. Click **Add Device**. The **Add Device** screen opens. Select the device you want to license and click **Save**.



The specified ID that is either internal/external IP or device ID must match the one provided by the device in the log files.

The License Manager Screen

The License Manager comprises of three tabs, each of which is explained in the sections below:

- ❖ Licenses
- ❖ Licensed Devices
- ❖ Options

Licenses

On this screen, you can add, manage, update, or delete a license. It also displays the following information:

- ❖ License Key
- ❖ Devices
- ❖ Used Licenses
- ❖ Remaining Licenses
- ❖ Type

The Licenses Screen

License Key	Devices		Type
	Used	Remaining	
G11DOGM2DKHE3DCGU4TOG4DCGO	2	8	Trial(21 Days)

Adding a License

You can add a new license on this screen. A license can be added in any of the two following ways:

- ❖ Select file
- ❖ Enter Manually

Follow the steps described below to add a license:

1. Click **Add**. The **Add License** screen appears.
2. If you have selected the Select file option, browse to the path where the .lic file is located.
3. If you have selected the Enter manually option, enter the license and the corresponding signature key in the text area.
4. Click **Add**.



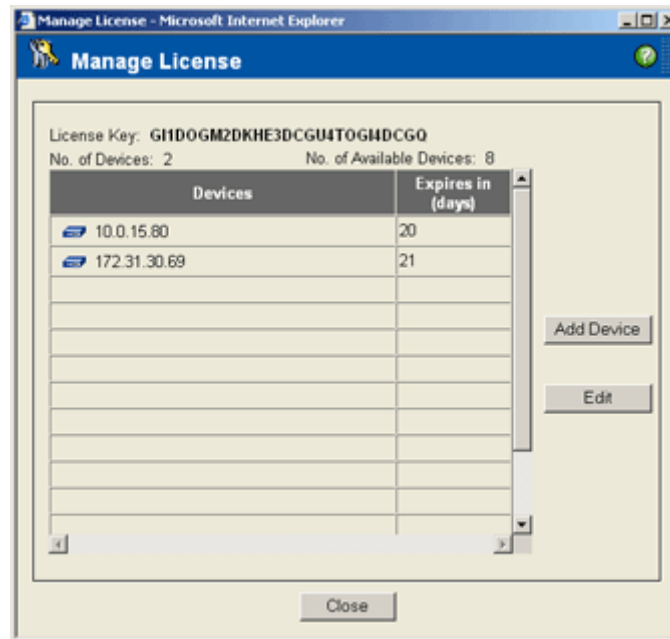
Before licensing a device, make sure it is configured.

Add License Screen

Managing a License

You can manage an existing license key from here. You can also view the count of devices that have been licensed and also those yet to be licensed.

Manage License



To manage license key, select the license key and click the **Manage** button available in the **License Manager** → **Licenses** tab.

Adding a Device

Follow the steps described below to add a device:

1. Click **Add Device**. The **Add Device** screen appears.
2. Select the device that you want to license from the list of unconfigured devices.
3. Click **Save**.

Editing a Device

You can replace an existing device with a new device. Before doing this, make sure that the device that you want in place of the existing device is added in the Devices/Groups and available in the License Manager as an unconfigured device.

Follow the steps described below to edit a device:

1. In the **Manage License** window, select a device and click **Edit**.
2. Enter the IP address of the device you want in place of the existing device.
3. Click **OK** to confirm.



You can edit a primary device license not more than twice.

Updating a License

On the **Update License** screen you can update the current license with a new one. You can update a license in two ways:

- ❖ Select file
- ❖ Enter manually

Update License

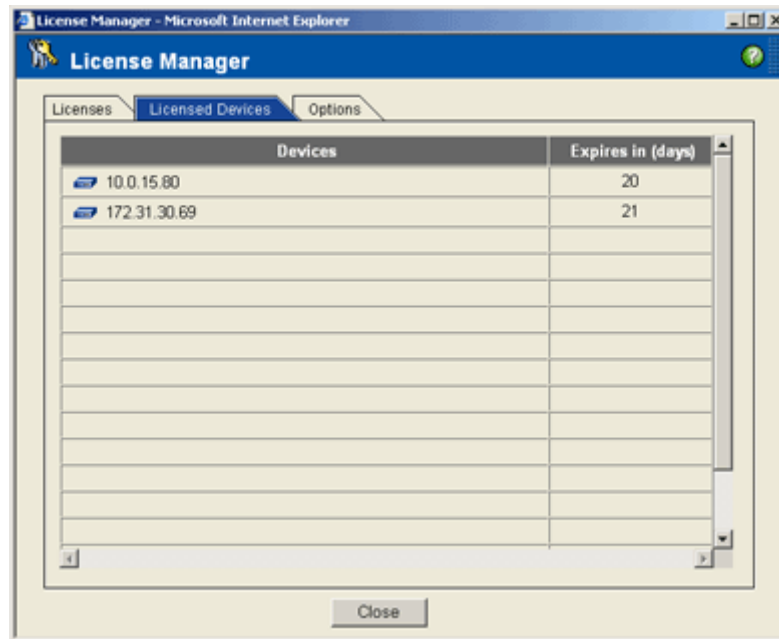
Follow the steps described below to update a license:

1. In the **License** tab, select a license and click **Update**.
2. If you have selected the Select file option, browse to the path where the .lic file is located.
3. If you have selected the Enter manually option, enter the license and the corresponding signature key in the text area.
4. Click **Update**.

Licensed Devices

This screen displays all the licensed devices, and number of days left before the license for each device expires.

Licensed Devices

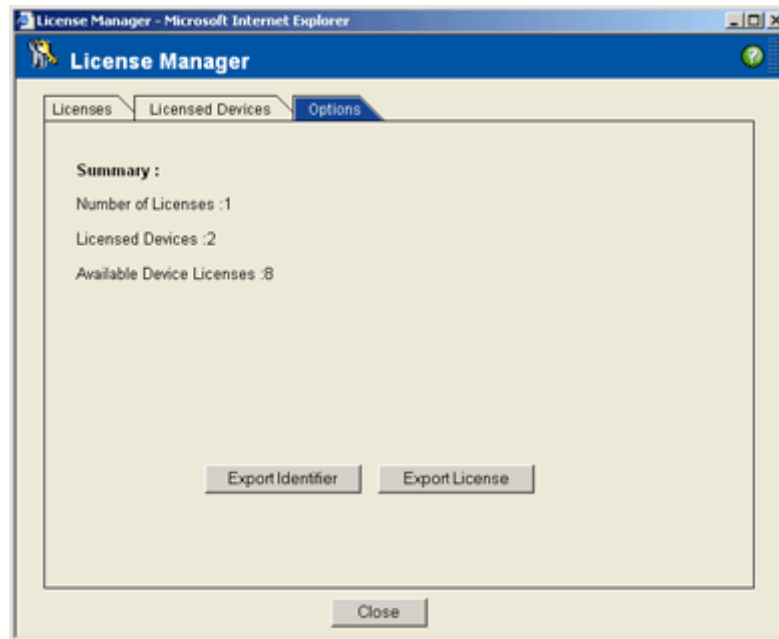


- ❖ Click **Close** to close the **Licensed Devices** screen.

Options

This section describes the options available on your license.

Licensing Options



Export Identifier

Click this button to save the Network Identifier to a text file. The Export Identifier file is located in the Clavister Insight installation directory. The identifier is exported to `C:\Program Files\Clavister\Insight\CIS\CISSystemIdentifier.txt`. To generate the license key, you must export this file to Clavister manually.

Export License

Use this option to keep a backup copy of your license.

For additional information, please contact the reseller from whom you purchased the software, or contact our support team at support@clavister.com

Security Center

On the GUI of the Clavister Insight, you have the Security Center button that will take you to the Monitoring and Reporting portals.

Reporting: This feature allows you to configure and generate reports. In addition to default reports that are non-editable, you can create custom reports tailored to meet your unique requirement. You can drill-down and obtain additional details for a selected top-level query.

Monitoring: This feature allows you to monitor predefined criteria and giving insight into essential system events. You can create your own views to monitor recent viruses detected, attack detections, emergency events, alert events, warning events, average events per second, port activity, protocol activity, and more.

Security Center- Reporting

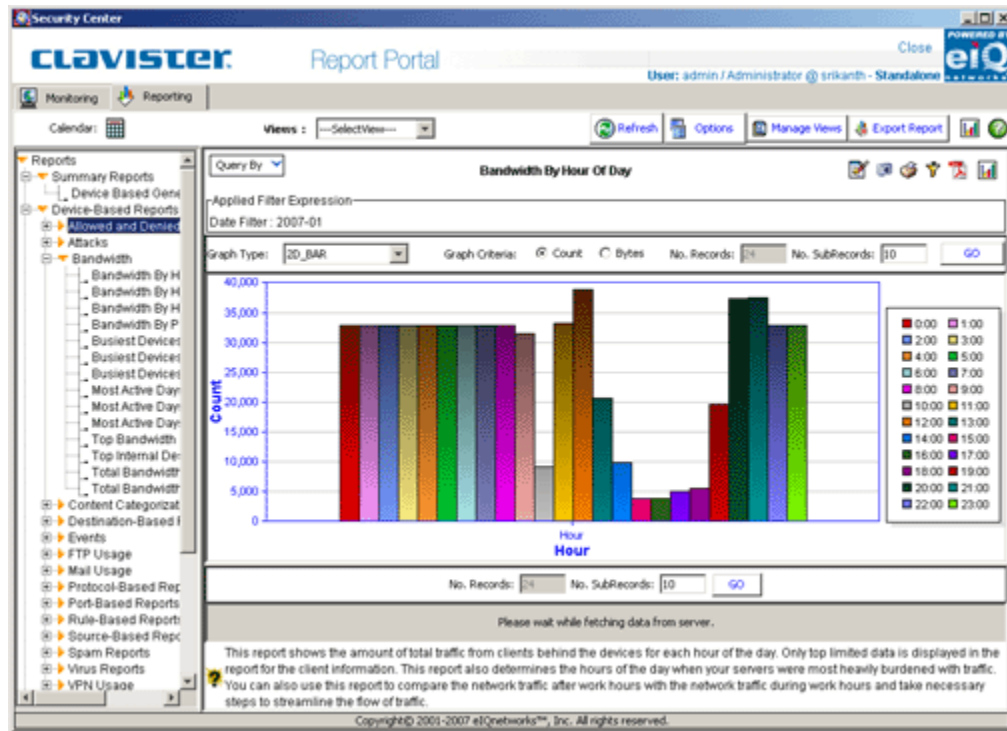
The Security Center is the platform where you can create and generate a report to view a single query on the fly without creating a profile. This is helpful when you want to view data for a single query quickly.

Reports generated on a Central machine will contain information about only the top records for each query type from all the Regional servers.

Access to the Security Center depends on the login privileges of the user. Click [here](#) for information on the types of users and privileges associated with each user type.

If you have logged in as a Power User or User account, you are allowed to report on only those devices/reporting sections you have permissions for.

The Reporting Portal




There are seven distinct time periods for which you can generate a Security Center report:

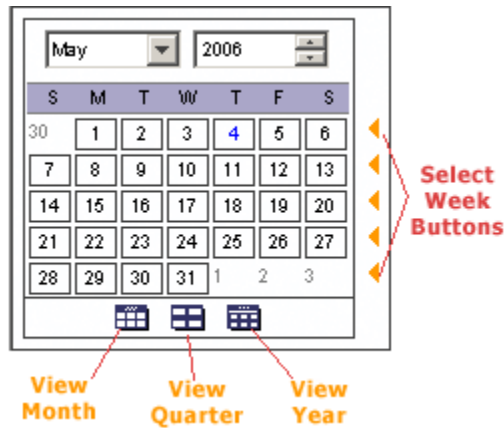
- ❖ Most recent completed hour
- ❖ Cyclic aggregate by the 24 hours of the day
- ❖ Most recent completed day
- ❖ Cyclic aggregate by the seven days of the week
- ❖ Most recent completed week
- ❖ Most recent completed month
- ❖ Longer sequences of months.

When you click on report link, the top-level report in the main section of the Security Center is replaced by a new report. An Instant Report generated by Security Center consists of three major sections:

- ❖ The calendar frame, from where you can specify the time period.
- ❖ The table of contents frame, which controls the report or the dashboard being viewed.
- ❖ The report frame, which displays the results.

Calendar Frame

The  icon on the top left corner of the Reporting window is the toggle switch to access the complete Calendar Frame, which can be used to apply time filters across the available reports. The different buttons on the Calendar facilitate selection of different time periods. With the Month Selector button you can change the month that appears in the Calendar. Along the right-hand side of the calendar are the Select Week buttons. Clicking one of these buttons selects the corresponding week. There are four buttons along the bottom of the calendar. These four buttons are View Month, View Quarter and View All.



By using the Calendar, you can select custom date ranges. To select a contiguous date range, hold down the Shift key and click the desired days. To select non-contiguous days, hold down the Ctrl key and select the desired days.

Table of Contents Frame

The Table of Contents displays a list of the available Report Chapters. To expand or collapse a Chapter, click the arrow to the left of the Chapter name. Some Chapters contain sub-Chapters. Sub-chapters can also be expanded and collapsed by clicking on the corresponding arrow. Click the Report Name to view the report.

All the queries that come under a common category are grouped under a single section. Now, you can see all the related queries under the required category and can obtain more precise information from the log data.




e.g., all the queries related to devices are shown under one single section

Report Frame

The report frame on the left hand-side of the screen displays either the report or dashboard chosen in the table of contents for the time frame chosen in the calendar. The default item to appear in the report frame is usually the dashboard for the default template.

Use the Calendar, the Table of Contents, or click on the title of a graph or table in the Dashboard to navigate to the content you want to view.

Exporting a Report

You can export each instant report to a PDF file by clicking  found at the top right-hand corner of the report frame.

The Back button is especially useful to perform drill-down function. (See the Additional Function Bar).

Reading a Report

All reports consist of a title, a short description, and a table of results. In most reports, each table and graph is color-coded to help you relate items in the table to items in the graph if there are more results than that can be displayed in the table or graph. Each report has a unique help card, which you can view from the top of the report by clicking the Help button on the report title bar. The help card contains information to help you interpret and make use of the information displayed in the report.

Utility Options

In the upper right-hand corner of the Reporting Portal, you can find the commonly used utility options of the reporting center. They are

- ❖ [Options](#)

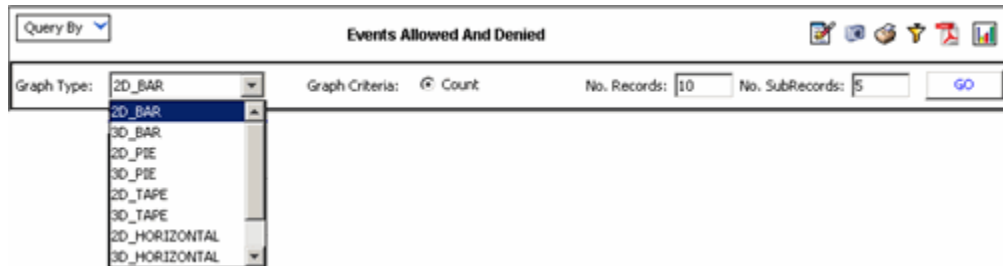
- ❖ [Manage Views](#)
- ❖ [Export Report](#)

Additional options available on the reporting center:

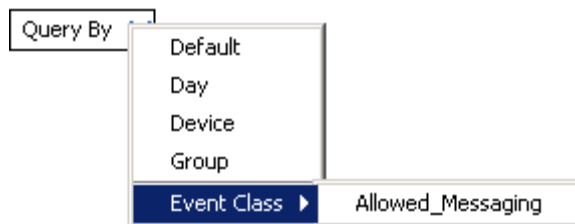
Refresh: Click the Refresh button to show the current available data on the Reporting Window.

Help: The Help icon brings up a Help window with additional information about the Reporting center.

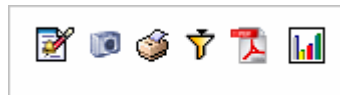
Pane Options



Query By: Click on the Query By button to change the selected query to generate report classified By Day or By Device or By Group. Please note that some queries are classified only by device.




Snap: With the snap icon you can maximize the view of the pane.



Print: With the print icon the user can print the displayed report.

Filters: With the filter icon the user can narrow the scope of the displayed report, expand the number of records displayed and also change the graph type.

Export to PDF: You can export each instant report to a PDF file by clicking the PDF icon found at the top right-hand corner of the selected pane.

Hide Graph: by default, the Reporting Pane is divided into two horizontal halves. The Graph type Report is displayed on the upper half and the table type Report is displayed on the lower half of the Reporting Pane. Click on the Hide Bar toggle switch depicted by  icon to hide the Graph and get a better view of the associated tabular report.

Graph Type: By default, the graph type displayed is the 2D BAR graph. You can select to view the graph type in the following formats:

- ❖ 2D_BAR
- ❖ 3D_BAR
- ❖ 2D_PIE
- ❖ 3D_PIE
- ❖ 2D_TAPE
- ❖ 3D_TAPE
- ❖ 2D_HORIZONTAL
- ❖ 3D_HORIZONTAL
- ❖ 2D_AREA
- ❖ 3D_AREA

The type of graph is dependant on the kind of data available for that Query.

Graph Criteria: You can select to view the graphs based on event count or by bytes transferred for each query selected.

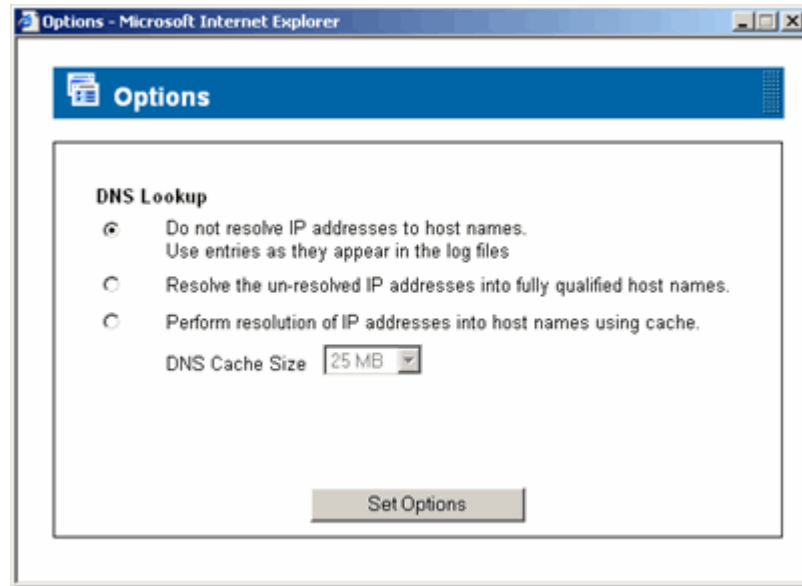
- ❖ Count
- ❖ Bytes

Most of the queries support only the count criteria. Queries based on Data transfer support both Count and Bytes graph criteria.

No. Records & Sub-Records: From here, you can specify the number of records and sub records that you want to view in your selected report.

Options

Use the report Options to change the DNS settings and logged in non-admin user password settings.



The DNS Lookup settings affect the reports that display IP address. The default setting is not to resolve IP addresses. The second option is to resolve IP addresses always, into fully qualified host names by looking up values from the local DNS server. The third option is to perform the IP resolution from a DNS cache that is built and maintained locally.

Note: Since the results from DNS resolution are not stored in the database, you will not find any resolved names when applying a host name filter or any other filter on the resolved IP addresses.

The Change Password option (available only when logged in as non-admin user) allows the Non-Admin users to change their login password.

Follow the steps described below to define a new password:

1. Select the Change Password check box. The new password field is enabled.
2. Enter a new password for the user currently logged in.
3. Click Set Options.

Make sure you provide the same password when you login into the application next time.

Manage Views

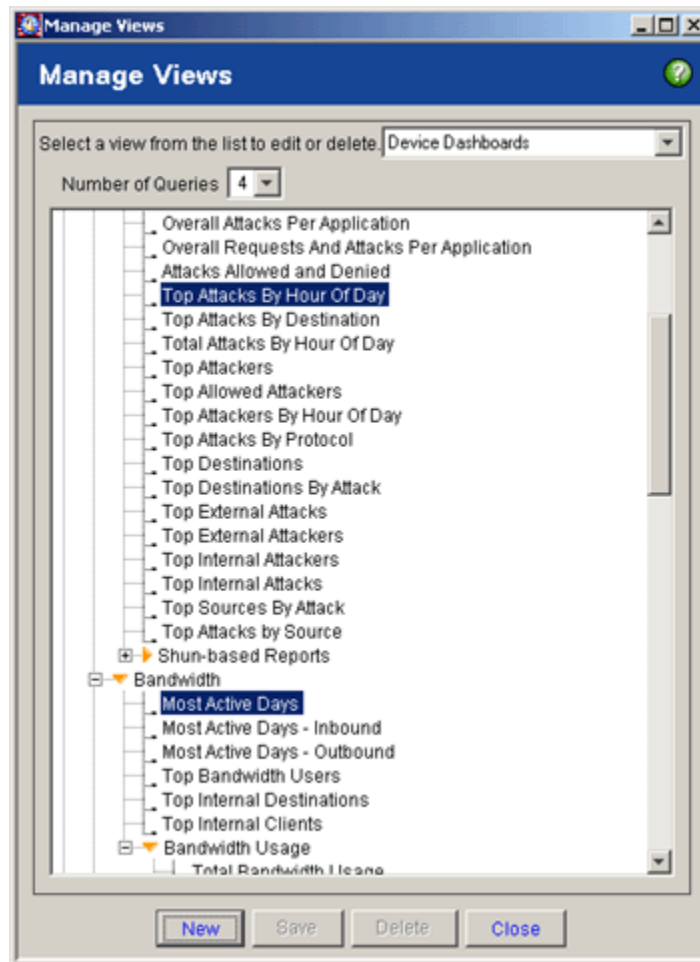
In Security Center of CIS you can create your own customized views. By default CIS Security Center Device Dashboard view has the following queries:

- ❖ Most Active Days
- ❖ Overall Events Triggered
- ❖ Bandwidth By Hour Of Day
- ❖ Top Attacks By Hour Of Day

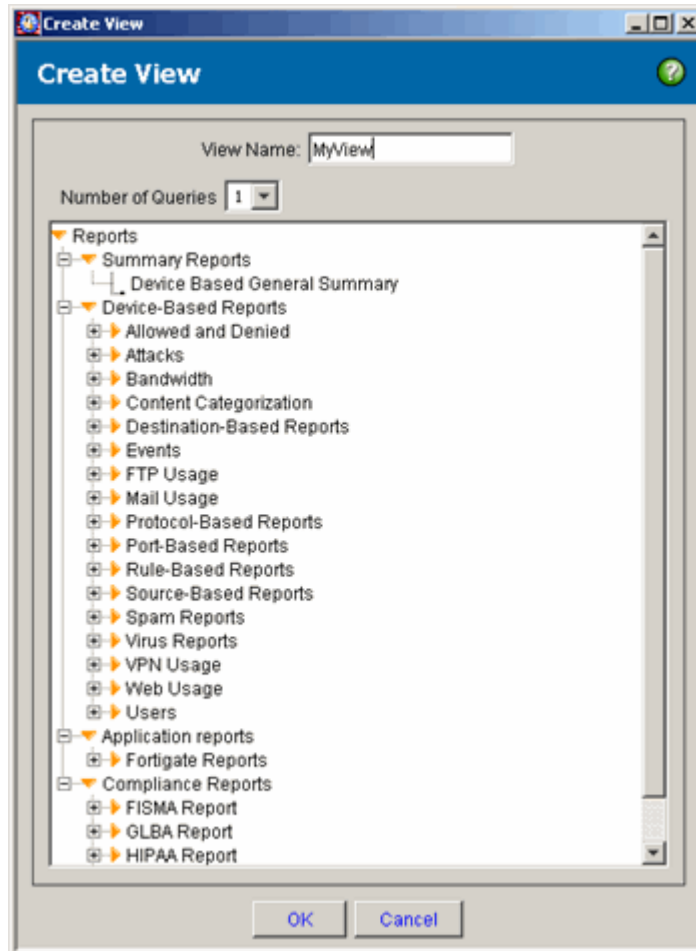
Creating a Custom View

Follow the steps described below to create your own view by selecting the queries you want to view:

1. Click **Manage Views** from the main screen. The **Manage Views** window opens.



2. It will show the default views available with the application and the corresponding queries for the selected view.
3. To define a new view, click **New**. The **Create View** window opens.



4. Enter a name for the view in the **View Name** box. Select the number of queries you want to assign to this view from the drop-down list.
5. Select the required queries from the list and click **OK**.
6. To make this view as your default view, Select the view from the Views drop-down list on the Security Center and click **Set as my default**.
7. Click **Restore default** to revert back to dashboard views.

Note: Only user-defined views can be edited or deleted.

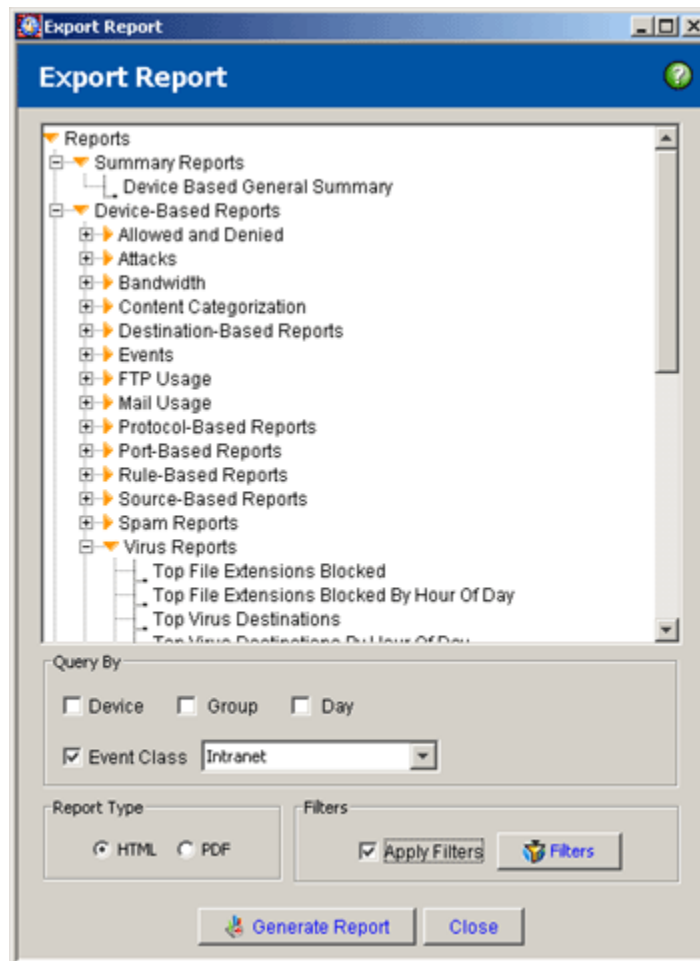
Export Report

To export a report, select the queries and a rendering format from the available options and click Generate Report. The report based on the selected queries is generated and it subsequently opens in the application

associated with the format rendered. For example, choosing PDF opens the report in Adobe Acrobat Reader.

Follow the steps described below to export a report by selecting the queries to report on:

1. Click Export Report from the main window. The Export Report window opens.



2. In the reporting sections available in the application and the corresponding queries for the selected section are listed in the Export Report window.
3. The selected reports can be exported to either HTML or PDF formats.
4. Select the queries to export and generate report for and click Generate Report.

Note: Power User and user are not allowed to define/apply the Global Filters.

5. A comprehensive report is compiled based on all the selected queries and is exported to the specified format.

Export Report-Filters

Global Filters can be used to apply filters uniformly across the selected queries from the 'Export Report' window. The global filters will be applied to the reports, which are to be exported to either HTML or PDF formats. You can narrow down the scope of report, specify the number of records to be displayed and even change the graph type in the report by applying these filters.


Follow the steps below to configure Global Filter settings.

1. Click on the **Filters** button in the Export Report window. The Filters dialog box is displayed.
2. Specify under **Max # of records to display**, details for **Number of Records** and **Number of SubRecords**.
3. To filter unique or a range of **Client Name/IP addresses**, specify the details in the **Range** and **IP/Name** fields and click Add button to enlist them.
4. To save the filter settings, click **OK**.

Filters

Use Filters to narrow down the scope of the report, increase the number of records displayed, and change the graph type. The sections of the filter vary depending on the selected report.

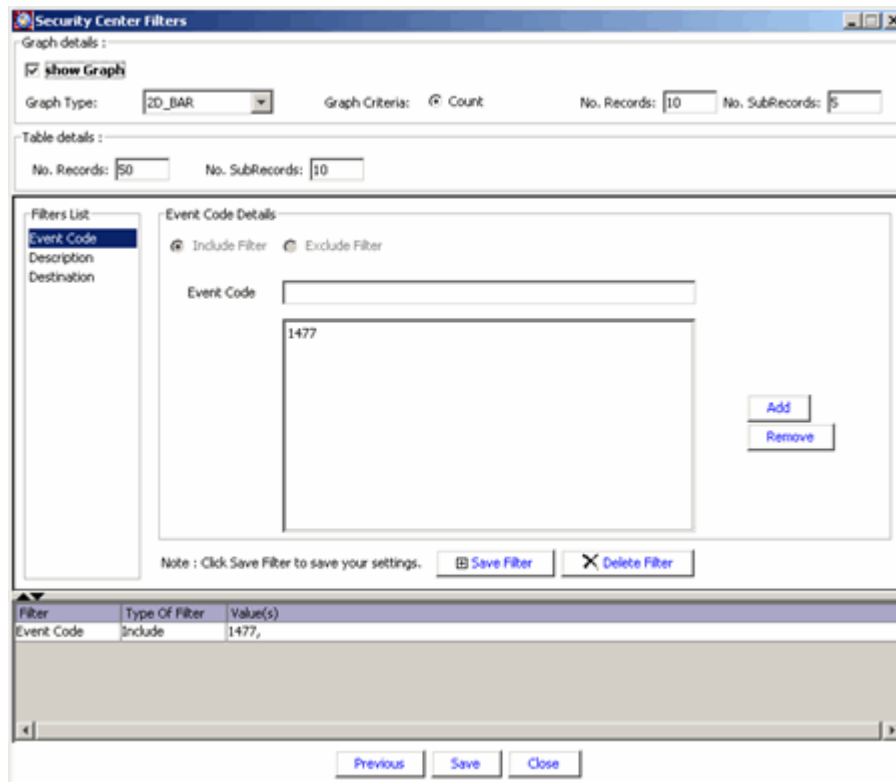
Follow the steps below to configure filter settings.

1. Select a Report query from the list displayed on the left pane, click on the filter  icon on the right pane and the corresponding Filters window is displayed.
2. On this window, you can select the devices you want to report on and the filters that can be applied for the selected query.

For example, in the image below represents the filters for **Top Receiving Domains By Message count**.

- ❖ Define the filters, Number of Records and Sub Records to display for the selected report.
- ❖ Specify the **Client Details**.

Query Filter



Filter	Type Of Filter	Value(s)
Event Code	Include	1477,

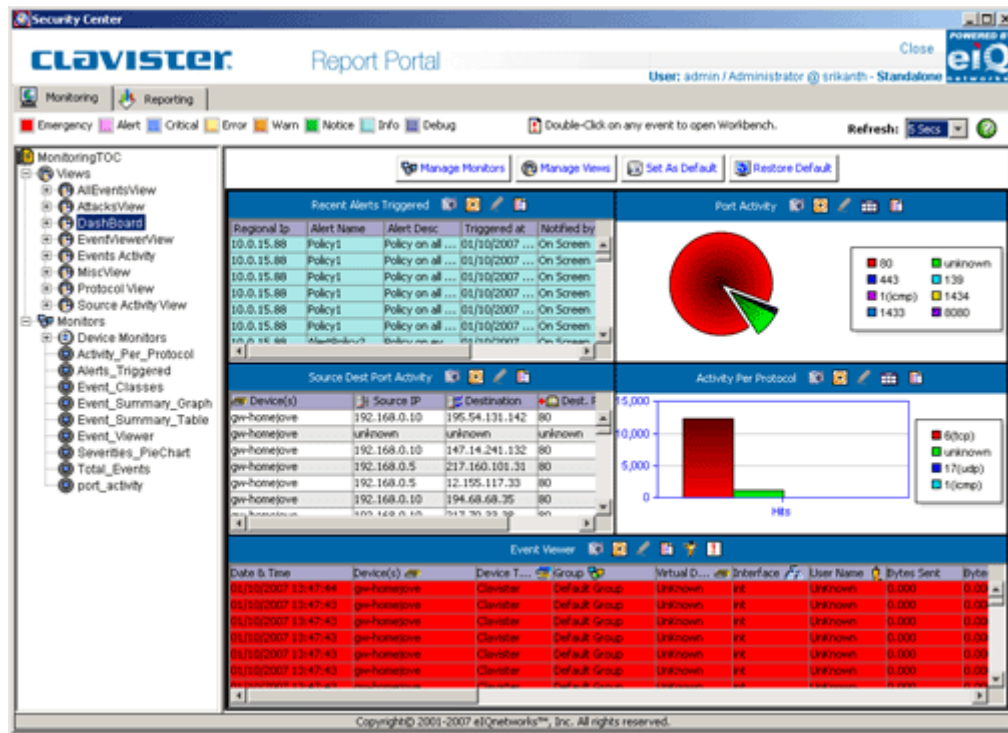
3. Click Next, give the domain details and save the filter.
4. Add more domains if required and Click save.
5. Similarly all the queries have corresponding filters to generate custom reports.

Note: Not all reports are associated with graphs.

Security Center - Monitoring

The real-time monitoring feature of Clavister Insight facilitates monitoring on predefined criteria. This gives you an insight into the essential system events. You can also set filters on some predefined performance metrics and proactively act to prevent problems.

Monitoring Portal – Security Center



Note: Graphs displayed in the Monitoring portal are seen as 2D by default. To change them to view as 3D images, override the property `MON_Use3D=no` to `MON_Use3D=yes` in the `GraphOptions.ext` found in the `(Apppath ... \Clavister Insight\CIS)`.

Views

A view is a custom defined portion of the monitoring window where you can create your own view.

By default you have the following views available in the application. They are:

- ❖ DashBoard
- ❖ EventViewerView
- ❖ AllEventsView
- ❖ AttacksView
- ❖ MiscView
- ❖ Events Activity
- ❖ Protocol View
- ❖ Source Activity View

The default view is the dashboard view which comprises of:

- ❖ Recent Alerts triggered
- ❖ Port Activity
- ❖ Source Destination Port Activity
- ❖ Activity Per Protocol
- ❖ Event Viewer

Note: Data displayed in the Event Viewer monitor depends on the filters applied in the Event Manager and the level selected in the Enable Monitoring list in the Options tab of the Syslog Configuration window.

Save As: Follow the steps described below to associate an alias name to save the selected view with a different name.

1. Select any of the existing views from the list and click Save As button.
2. Enter a name in the View Name box.
3. Click OK.

A view is added to the list with the name you have just added, which is a replica of the view which was your primary selection.

Creating a Custom View

Follow the steps described below to create your own view by selecting only those monitors that you want to view:

1. Click Manage Views from the main menu of the Monitoring Center. The **View Manager** window opens.
2. To define a new view, click New. The **Add View** window opens.
3. Enter a name for the view. Select the number of monitors you want to assign to this view from the drop-down list.
4. To select the monitors from the list, select the monitors and click to move them into selected list. Click **Save**.

5. To make this view as your default view, select the view from the Select view drop-down list and click **Set** this as my default view.
6. Click **Restore default** view to revert back to dashboard view.

Note: The number of monitors should be exactly equal to number of monitors assigned in this view. User-defined views can be edited and deleted.

Monitors

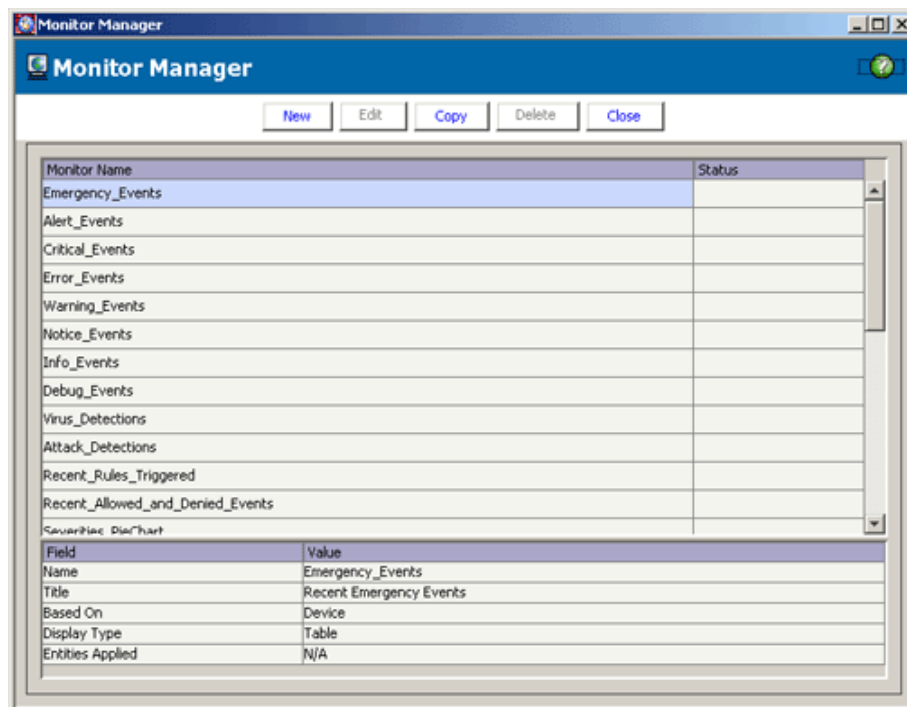
On the TOC pane of the Monitoring center, you can see the list of default and user-defined monitors.

Select a monitor from the list and click on it to see its details.

If you want to add and configure a new monitor, click Manage Monitors from the main menu of monitoring center. The Monitor Manager screen opens from where you can add monitors.

Adding a Monitor

This section provides instructions on how to add a monitor.



Note: Data from the entities to be monitored can be enabled/disabled by checking the corresponding status button.

The Add Monitor Wizard

Follow the steps described below to add a monitor:

1. From the **Security Center** main menu, click Monitoring. The Monitor Center screen opens.
2. Click **Manage Monitors** button. The Monitor Manager window opens. Click **New**.
3. Enter a name for the monitor in the **Monitor Name** box.
4. Enter a title for the monitor in the **Title** box.
5. There are two ways displaying information in the monitor. They are
 - ❖ Table
 - ❖ GraphTo customize the view, under the section **Display Type**, specify the graph type and number of graph items to associate with it.
6. Click **Next**.

Note: Pie charts can be generated only if the monitor is created for a single entity.

Adding a Device Based Monitor

To add a Device based Monitor, select the entities to monitor from the in-built list and move them from the available entities list to the selected entities list. Click **Next**.

Note: If all the available entities are selected, the monitor does not display any information even if any of one of the selected entity does not have data.

Selecting Device Based Entities

The following are the entities available, click on the filter to see the steps specific to each one of them:

❖ Client IP

❖ Device IP

- ❖ Destination IP
- ❖ Destination Port
- ❖ Protocol
- ❖ Priority
- ❖ Attacks
- ❖ Virus
- ❖ Event Id
- ❖ Event Type
- ❖ Event Description
- ❖ Attack Details
- ❖ Virus Details
- ❖ Rule
- ❖ Flow
- ❖ Spam Destination Email
- ❖ Spam Source Email
- ❖ Spam Type
- ❖ Bytes Sent
- ❖ Bytes Received
- ❖ Shun

Summary

The Summary sheet displays the summary of the settings that you chose for the monitor. To make any changes before saving it, click the **Previous** button. To finish, click Finish.

Device Based Entities

The following sections explain how to select device-based entities to monitor.

Client IP

If you have selected Client IP, follow the steps described below:

1. Enter the client IP you want to monitor.
2. To monitor events from a series of devices at one time, select the Range check box and enter the IP Range.
3. Click Add to add the client IP or range and click Next.

Device IP

You can select the Group Name/Device IP - Device Type for which you want to create a monitor.

1. Select the devices you want to create a monitor for. You can select all devices at a time or individual groups and devices.
2. Click Next.

Destination IP

If you have selected Destination IP, follow the steps described below:

1. Enter the Destination IP of the device you want to monitor.
2. To monitor events from a series of devices at a time, select the Range check box and enter the IP Range.
3. Click Next.

Destination Port

If you have selected Destination Port, follow the steps described below:

1. Enter the destination port number you want to monitor.
2. Click Add to add the port number to the list.
3. Click Next.


Protocol

If you have selected Protocol, follow the steps described below:

1. Enter the protocol you want to monitor.
2. Click Add to add the protocol to the list.
3. Click Next.

Priority

If you have selected Priority, follow the steps described below:

1. Select the priority you want to associate with the monitor from the Available Priorities list.
 - ❖ Emergency
 - ❖ Error
 - ❖ Critical
 - ❖ Alert
 - ❖ Warning
2. Click  to transfer the selected priorities to the Selected Priorities list.
3. Click Next.

Virus

If you have selected Virus, follow the steps described below:

1. Enter the virus name you want to associate with this monitor.
2. Click Add to add the virus to the list.
3. Click Next.


Virus Details

If you have selected Virus, follow the steps described below:

1. Enter the virus name you want to associate with this monitor.
2. Click Add to add the virus to the list.
3. Click Next.


Attacks

If you have selected Attacks, follow the steps described below:

1. Select the attacks you want to associate with the monitor from the Available Attack list.
2. Click  to transfer the selected attack types to the Selected Attacks list.
3. Click Next.

Attack Details

If you have selected Attacks, follow the steps described below:

1. Select the attacks you want to associate with the monitor from the Available Attack list.
2. Click  to transfer the selected attack types to the Selected Attacks list.
3. Click Next.


Event ID

If you have selected Event ID, follow the steps described below:

1. Enter the event ID you want to monitor.
2. Click Add to add the event ID to the list.
3. Click Next.

Event Types


If you have selected Event Types, follow the steps described below:

1. Select the Event Types you want to associate with the monitor from the Available Event Types list.
2. Click  to transfer the event types to the Selected Event Types list.

3. Click Next.

Event Description

If you have selected Event Description, follow the steps described below:

1. Select the Event Types you want to associate with the monitor from the Available Event Types list.
2. Click  to transfer the event types to the Selected Event Types list.
3. Click Next.

Rule

If you have selected Rule, follow the steps described below:

1. Select the rules you want to monitor from the list.
2. Click Next.

Flow

If you have selected Flow, follow the steps described below:

1. Select from the following
 - ❖ Allowed
 - ❖ Denied
2. Select Allowed if you want monitor only allowed events.
3. Select Denied if you want monitor only denied events.

Spam Type

If you have selected Spam, follow the steps described below:

1. Select the Spam types you want to monitor from the predefined spam list.
2. Click Next.

Event Viewer Filters

Filters help you to filter the view on the Event Viewer console. You can select the entities you need as columns in the display. Click the Filters in the Event Viewer screen to select the entities you want to filter.

Selecting Entities to Filter

In the Event Viewer console, all events are displayed with color code based on its severity. Event Viewer filters allows you to select specific severity types from the Select at least one severity check box.

The available severity types are:


- ❖ Emergency
- ❖ Alert
- ❖ Critical
- ❖ Error
- ❖ Warning
- ❖ Notice
- ❖ Information
- ❖ Debug

To select the entities you want to filter, follow the steps described below:

Select the entities you want to filter from the list of available entities:

- ❖ Date & Time
- ❖ Group Name
- ❖ Device Name
- ❖ Device Type
- ❖ BII
- ❖ Flow
- ❖ Source IP
- ❖ Destination IP
- ❖ Protocol
- ❖ Event ID
- ❖ Destination Port
- ❖ Event Description
- ❖ Attack ID
- ❖ Virus Name
- ❖ Interface
- ❖ URL
- ❖ Virus ID

- ❖ Virtual Device
- ❖ Rule
- ❖ User Name
- ❖ Severity
- ❖ Shun
- ❖ From Attacker
- ❖ Bytes Sent
- ❖ Native Log
- ❖ Bytes Recv
- ❖ From Victim

Click on  to move the selected entities into the selected list. Click Next to enter details for the selected filters.

Appendix

Backing up CIS 4.6

Although CIS 4.6 has file replication (auto backup) when running in a distributed mode it is still a good idea to backup your data.

Backing Up Data from an CIS 4.6 Server

To backup data from a CIS standalone or distributed environment, follow the instructions below.

1. Logon to your CIS Server. If you have a distributed environment you will need to follow step 2 for all regional and central servers.
2. The default install path for CIS is Root://Program Files/Clavister/Insight/CIS. If you did not install CIS in the default path then you will need to change the path to the appropriate location. You will need to backup the following files and directories from the CIS directory:
 - ❖ Database
 - ❖ DBAudit
 - ❖ ForensicLogs
 - ❖ Profiles
 - ❖ Userprofiles
 - ❖ Devices.xml (Only if you have devices)
 - ❖ Groups.xml

Backing Up Data from an CIS 4.6 Syslog Server

1. The CIS Syslog Server may be installed on the same physical server as the CIS Server or it may be installed on a separate server. Please be sure to backup all instances of the CIS Syslog Server within your environment.
2. The default install path for the CIS Syslog is Root://Program Files/CISSyslogSrv/Syslog. If you did not install the CIS Syslog Server in the default path then you will need to change the path to the appropriate location. You will need to backup the following files and directories from the Syslog directory.

- ❖ Logs
- ❖ DeviceLicInfo.txt
- ❖ FirewallList.txt (Only if you have network devices)
- ❖ Leaffirewalls.txt (Only if you have Check Point Firewalls)
- ❖ RDEPDevices.txt (Only if you have RDEP Devices)