

# Operational Documentation

| Version 1.0 | 13/08/02



CORE SECURITY TECHNOLOGIES

# Table of Contents

<b>TABLE OF CONTENTS</b>	<b>2</b>
<b>1. INTRODUCTION</b>	<b>5</b>
WHAT IS WISDOM ?	5
<i>Advantages of the graphical approach</i>	6
APPLICATION AUDIT TRAILS	7
Type of events	7
<b>2. WISDOM INSTALL</b>	<b>9</b>
Workstation requirements:	9
<i>Install procedure</i>	9
<i>Un-install procedure</i>	11
<b>2. ANALYSIS WITH WISDOM</b>	<b>13</b>
2.1 LOG DATA HANDLING	14
Connectors	14
Adding objects to the Analysis Flowchart sector	14
Deleting objects	14
<i>Selecting Input Sources</i>	15
Single-File container	15
FileSet container	16
ODBC queries	17
NT Event Logger	17
CORE Audit logs	18
<i>Parsing Input sources</i>	18
Low-level parsing rules	19
Application specific details	21
Attribute-type definition	22
Adding categories	22
Adding attributes	23
Moving components to a different category	24
<i>Filtering information</i>	24
Filtering by criteria	24
Sampling	26
<i>Creating Output Repositories</i>	27
Previewing log contents	27
Updating the repository contents	28
Renaming a repository	28
Visualization options on Repository containers	28
Using Default views	28
Selecting Visualization modes	29
<i>Saving workspace definitions</i>	30
2.2 STARTING THE ANALYSIS	31
2.3 GRAPHICAL INTERFACE DESCRIPTION	32
<i>Visualization Modes</i>	35
Summary Graph	35
Scatter Plot Graphs	35
Complex Scatter Plot Graphs	36
Parallel Coordinates	37
<b>3. ANALYSIS PROCEDURES</b>	<b>38</b>
3.1 COMMON ANALYSIS PROCEDURES	38
Context Menu	38
Selecting events	39
Event selection on Parallel Coordinates graph	39



Selection procedure in other visualization modes	40
Exporting Data Panel events	40
Focusing on timeframes	41
Resizing procedure	41
Time slide procedure	42
Changing Data Panel display options	43
Adding new columns	43
Resizing of columns	44
Changing column ordering	44
Opening a new Visualization Area	44
Using charts	45
Configuring chart settings	45
Exporting chart data	47
Visually filtering views	48
Filtering by Color References	48
Filtering by Chart Element	49
Commenting events	50
Using comments to keep track of events	50
Creating templates	50
To create a new Analysis Graph template	50
<b>3.2 SPECIFIC PROCEDURES AND SETTINGS</b>	<b>52</b>
3.2.1 Using Summary view	52
3.2.2 Using Scatter Plot view	54
To select Y-axis value	55
How to hide Y-axis references legend	55
Selecting coloring options	55
How to show the palette references	56
Selecting random value	57
Changing transparency	58
3.2.3 Using Complex Scatter plot view	58
Changing border colors	58
Changing transparency on border color	59
Changing width on border line	59
Setting size	60
Changing default size value	61
Changing shape settings	61
3.2.4 Using Parallel coordinates views	62
Handling multiple y-axes	62
How to hide Y-axis references legend	63
Selecting coloring options	63
Highlighting an event rail	64
<b>4. CREATING THE ANALYSIS REPORT</b>	<b>65</b>
To create a report:	66
Related tasks	66
<b>INDEX OF FIGURES</b>	<b>68</b>
<b>ALPHABETICAL INDEX</b>	<b>70</b>



## Disclaimer

Copyright © 1998 - 2002, CORE ST S.A. or its subsidiaries (CORE ST). All rights reserved. This documentation may be printed and copied solely for use with CORE FORCE solution. Two (2) copies of this documentation may be made for archival and backup purposes. Except for the foregoing, no part of this documentation may be reproduced or transmitted in any form or by any means or used to make any derivative work (such as translation, transformation or adaptation) without express written consent from CORE ST.

CORE ST reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of CORE ST to provide notification of such revision or changes. CORE ST MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE DOCUMENTATION IS FREE OF ERRORS OR THAT THE DOCUMENTATION IS SUITABLE FOR YOUR USE. THE DOCUMENTATION IS PROVIDED ON AN "AS IS" BASIS. CORE ST MAKES NO WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. TO THE FULL EXTENT ALLOWED BY LAW, CORE ST ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR DIRECT, INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THIS DOCUMENTATION, EVEN IF CORE ST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CORE ST, the CORE ST logo, WISDOM and WISDOM are registered trademarks. SAP and the SAP logo mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brand and product names may be registered trademarks or trademarks of their respective holders.

IF THIS DOCUMENTATION IS PROVIDED ON A COMPACT DISK, THE OTHER SOFTWARE AND DOCUMENTATION ON THE COMPACT DISK ARE SUBJECT TO THE LICENSE AGREEMENT ACCOMPANYING THE COMPACT DISK.

# 1. Introduction

---

The purpose of Information Visualization is to use perception to amplify cognition. But what has this concept to do with Security Logs? Tasks related to log retrieval and meaningful exploitation of data are usually a heavy burden for the auditor. The amount and variety of the information contained in logs is sometimes an impediment for obtaining conclusions and developing a 10,000 feet view on the real events hidden behind the traditional text representations of log trails. In other words, the crystallization of log events in WISDOM's visual representation could lead to a higher-quality security analysis than one obtained from the text-based reports and even from more traditional graphical approaches as pie or bar charts.

Using a graphical approach to interpret the log contents turns easier to identify patterns and trends on the data. Even more important, anomalous events that could have been missed are quickly identified due to the graphical approach of the analysis, where each single event is considered as part of the complete activity of the systems in relation to all events taking place in a period of time.

Another clear advantage of the visual representation is that while it is not natural for us to remember patterns expressed on a text list, it is fairly easy to remember spatial objects as pictures and maps or, in CORE Wisdom's case, visual diagrams based on event logs. Then anomalous behavior can be expressed as an event that occurs outside predefined limits (easy to difference on the graph) or by a complete change on the normal pattern, with a very different "behavioral map" of the system activity.

Auditing tasks involve frequent analysis in the events registered on the security and application logs. The traditional approach to the information contained there is mainly based in text-format representation of the data. But as we considered on the previous paragraphs these limits can be overcome. It is important to note the iterative nature of the analysis, where each graphical construction on the logs can initiate a line of research to direct the analysis by visually navigating a specific timeframe in the log trails.

Pattern recognition thru graphical visualization can be used to profile system utilization in terms of security events. The net gain on information reduction comparing against the unmanageable amount of events on the audit trails provides with aggregated forms of information handling when the auditor intends to do a meaningful analysis on the logs.

## What is WISDOM ?

WISDOM presents the auditor with a framework to analyze the information contained on audit trails thru a more abstract approach that permits a deeper exploitation of the events in order to discover interrelations otherwise hidden in the maze of text-format logs.

The main advantage obtained with WISDOM's visual representation strategy is given by the fact that the analysis performed by the auditor is not based primarily on the events in the audit trails, but on the patterns and trends emerging from them. The auditor can now move from the graphical visualization of the aggregated data towards a meaningful analysis of the data detailed on the logs. The process performed on the original logs is shown in Figure 1.

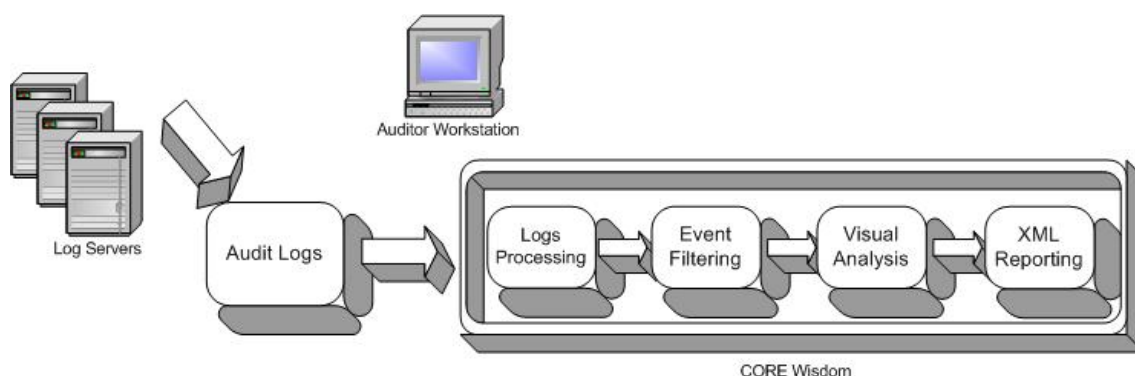


Figure 1: Analysis life-cycle in WISDOM

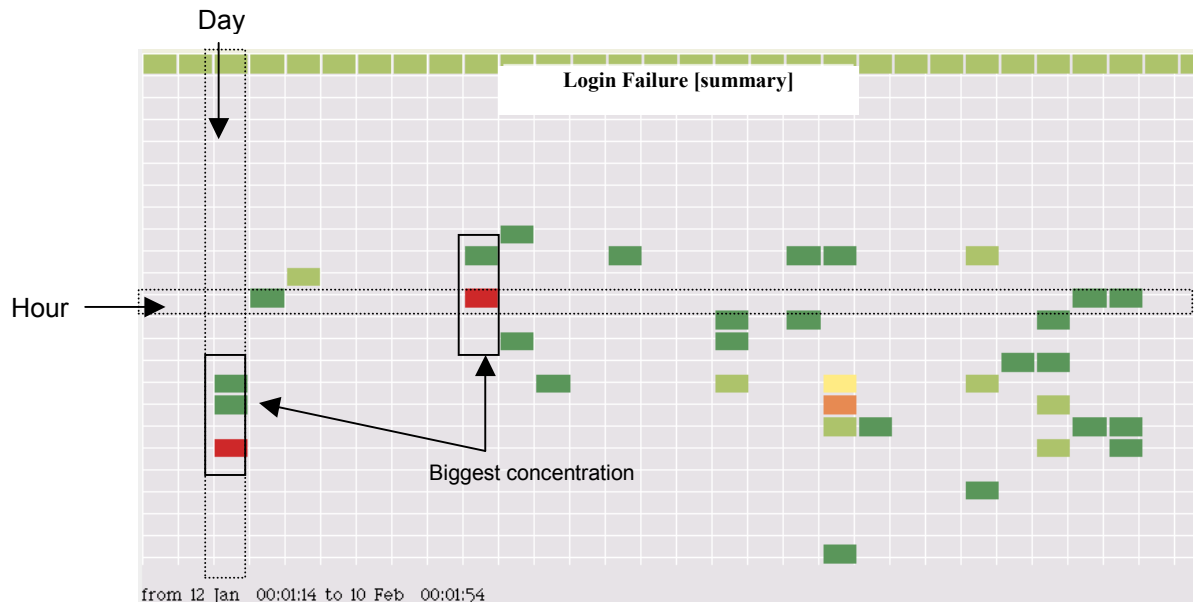
## Advantages of the graphical approach

Security logs can be analyzed with WISDOM to obtain, for example, information on failed logins. Let us compare the advantages of the graphical analysis over the limited conclusions that could be drawn from its text report counterpart. Table 1 presents us with Logon Failed events taking place during five consecutive days. This is a subset of the actual contents of this log, some of the columns have been omitted to simplify the review. Even with this caution, when we compare the effort involved on the analysis to discover trends from the text table with the immediate conclusions drawn from the graphical representations provided by WISDOM, the result is clear.

Date	Time	User	Terminal	Text
01.02.2002	0:01:36	JOHNB		Logon Failed (Reason = 1, Type = B)
01.02.2002	0:01:36	JOHNB		Logon Failed (Reason = 1, Type = B)
01.02.2002	17:04:27	ANNC	ANNC	Logon Failed (Reason = 1, Type = A)
02.02.2002	0:01:36	JOHNB		Logon Failed (Reason = 1, Type = B)
02.02.2002	0:01:36	JOHNB		Logon Failed (Reason = 1, Type = B)
03.02.2002	0:01:37	JOHNB		Logon Failed (Reason = 1, Type = B)
03.02.2002	0:01:37	JOHNB		Logon Failed (Reason = 1, Type = B)
04.02.2002	0:01:38	JOHNB		Logon Failed (Reason = 1, Type = B)
04.02.2002	0:01:38	JOHNB		Logon Failed (Reason = 1, Type = B)
04.02.2002	9:52:49	KIMS	KIMS	Logon Failed (Reason = 1, Type = A)
04.02.2002	9:53:05	KIMS	KIMS	Logon Failed (Reason = 1, Type = A)
04.02.2002	15:33:38	HARRYS	HARRYS	Logon Failed (Reason = 1, Type = A)
04.02.2002	15:33:41	HARRYS	HARRYS	Logon Failed (Reason = 1, Type = A)
04.02.2002	20:58:48	MPAZ	pcrcolor	Logon Failed (Reason = 1, Type = A)
05.02.2002	0:01:38	JOHNB		Logon Failed (Reason = 1, Type = B)
05.02.2002	0:01:38	JOHNB		Logon Failed (Reason = 1, Type = B)
05.02.2002	14:58:50	ANNC	ANNC	Logon Failed (Reason = 1, Type = A)

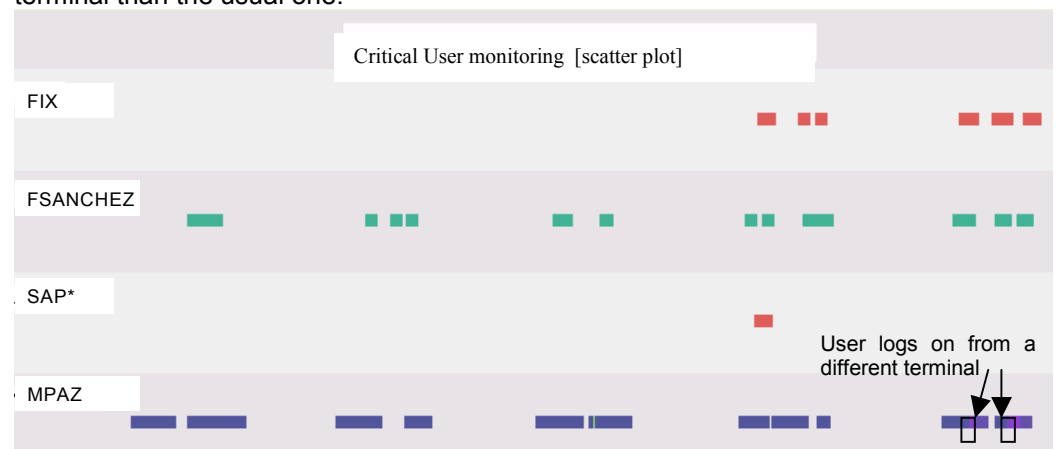
Table 1: System Security Log - Text view

In the graphical representation of similar data that is shown in Figure 2, the events emerge in an obvious pattern, showing the biggest concentration of events occurs around the starting and ending of each week, which is a normal pattern for login failure.



**Figure 2: Graphical representation for visual analysis**

Another example is shown in Figure 3. In this diagram you not only can easily identify login patterns for critical accounts, but also you can detect other usage patterns: the color used to depict the login event adds information about the terminal used at each attempt. In this way you graphically visualize that some users always login from the same terminal. And in the last day of event accounting user MPAZ logs on from a different terminal than the usual one.



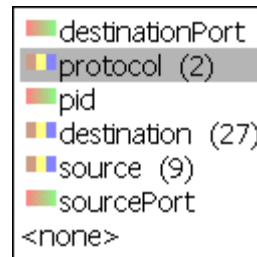
**Figure 3: Critical user login pattern – Graphical visualization**

As result of the visual approach the entities and actions contained on log trails such as transactions identifiers, user names, login terminals become elements of the visualization graph.

## Application Audit trails

### Type of events

Events are comprised of two different types of attribute values assigned to fields. The type of the attribute value determines the behavior and some of the actions available for use on WISDOM visualizations.



**Figure 4: Attribute types identifiers**

- (1) **Discrete attributes:** We include as discrete attributes those values representing categories as well as ordinal values. These are the attributes used, for example, for chart generation. Discrete attributes are identified by preceding them a three-colored icon and followed by the number of distinct values it takes enclosed in parenthesis. Examples in Figure 4 are *protocol*, *destination* and *source*.
- (2) **Continuous attributes:** These values represent numeric entities such as quantities, totals, single numbers. Some procedures are only available in the case of continuous attributes: for example, you can only use the *Size* option present in Complex Scatter Plot graphs with values of this kind, as described in section *Setting size* on page 60. A continuous-colored icon precedes continuous attributes. Examples in Figure 4 are *destinationPort*, *pid* and *sourcePort*.

#### *Related information*

For information about importing these logs into WISDOM analysis environment, see section *Selecting Input Sources* on page 15.

For information about the procedures that can be used in the analysis, see section 3. *Analysis procedures*, on page 38 and section 4. *Creating the analysis report* on page 65.



## 2. Wisdom Install

The installation of the software is made through the installation wizard, which will install all required components in the Analyst workstation.

### Workstation requirements:

In order to use CORE Wisdom, the workstation should have available:

- At least 60 MB of free disk space for the software installation.
- The required space for log handling (depends on the file size of the logs to analyze)
- Microsoft Internet Explorer 6.x or newer
- Pentium III 750 Mhz processor
- 128 MB RAM

Make sure your workstation complies with the minimum hardware requirements before proceeding.

### Install procedure

1. Double-click on the setup.exe installation file in order to execute the *Installation Wizard*.

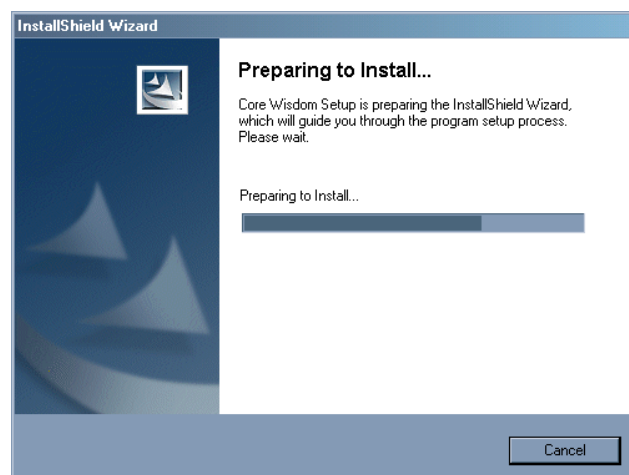


Figure 5: Preparing to install

2. When the *Welcome* window shown on Figure 6 appears, select *Next* to continue.

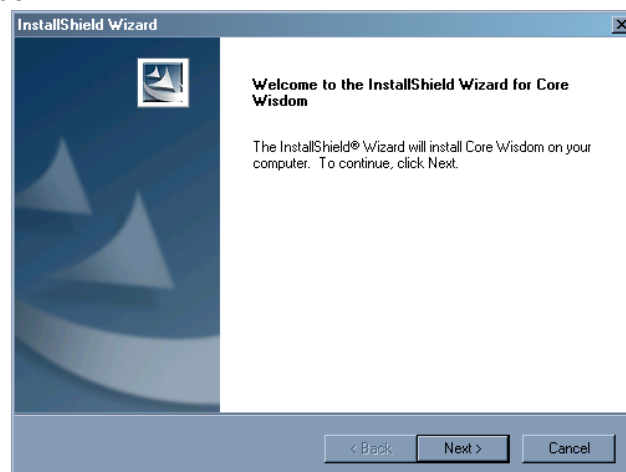
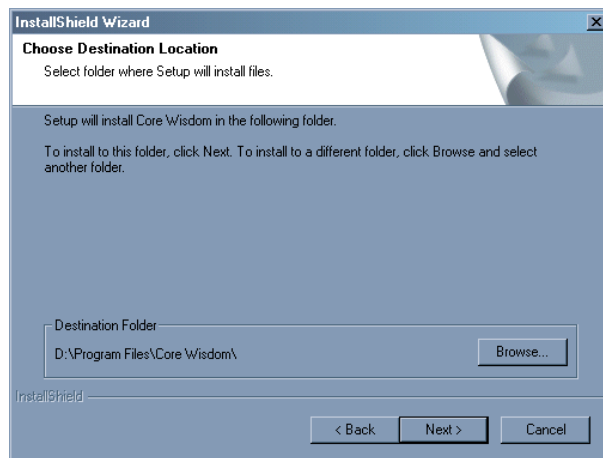


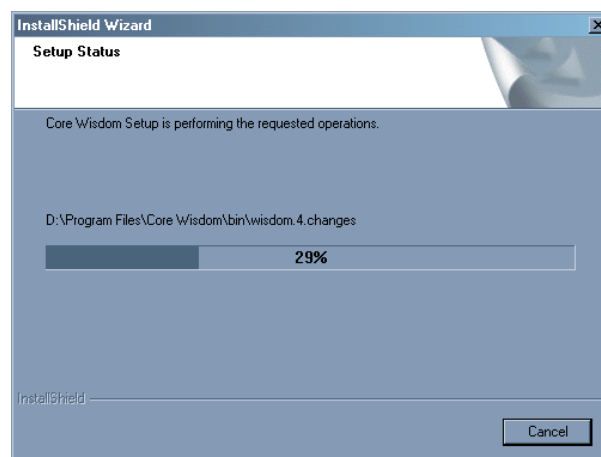
Figure 6: Welcome to the install wizard

3. The next step is to select the installation directory. If you need to change the default option, browse to the appropriate folder using the *Browse* button in the *Choose Destination Location* window. After you have selected the destination folder click *Next* to proceed with the setup.



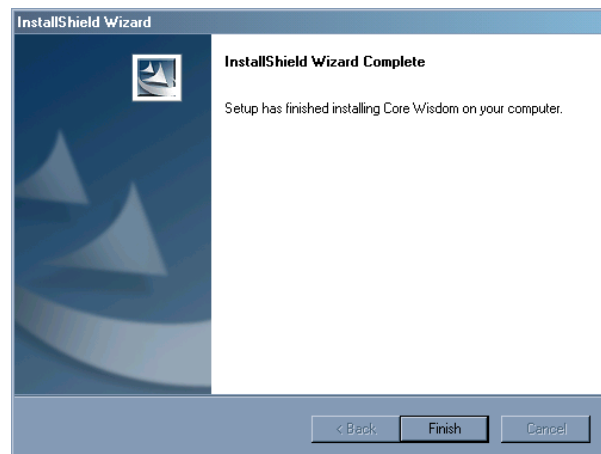
**Figure 7: Choose destination location**

4. Setup process begins. Required files are copied onto the destination folder.



**Figure 8: Setup status**

5. Installation process completes. Press *Finish* in the *InstallShield Wizard Complete* window to finish the setup.



**Figure 9: Wizard Complete**

## Un-install procedure

In order to uninstall CORE Wisdom from the auditor's workstation, you should perform the following steps:

1. Select the *Add/Remove Programs* applet in the Windows *Control Panel*. You can access the *Control Panel* from the *Settings* options located in the *Start Menu*. The window shown on Figure 10 displays.

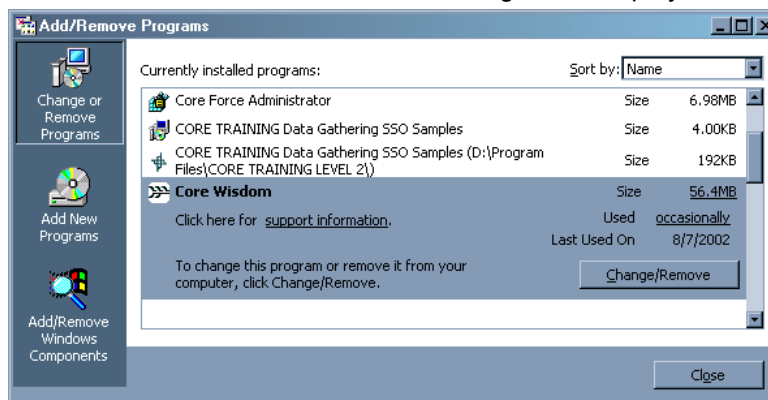


Figure 10: Add/Remove programs

2. Select the *Change/Remove* button on the *Add/Remove Programs* window. This will present on screen the *InstallShield Wizard* screen presented on Figure 11 with the options available. Select the *Remove* radio button in order to start the un-install process.

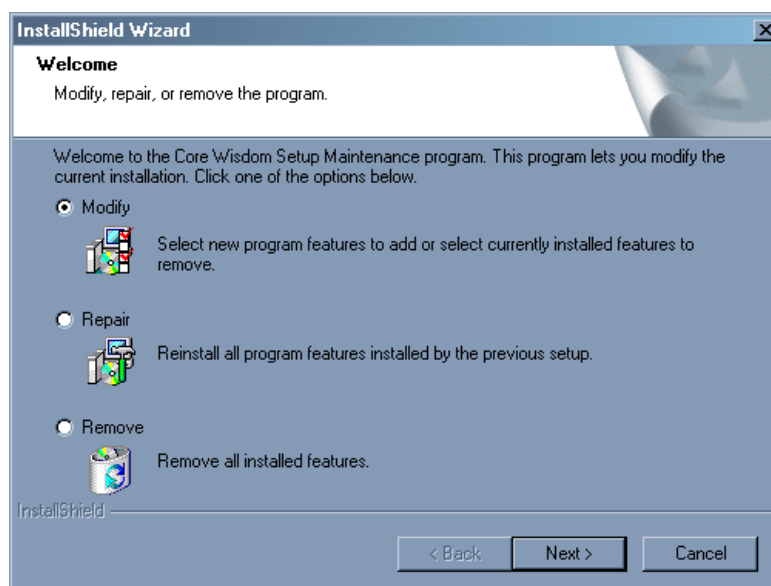


Figure 11: Install Wizard options

3. Confirm the un-install by selecting the *OK* button on the *Confirm Uninstall* window.

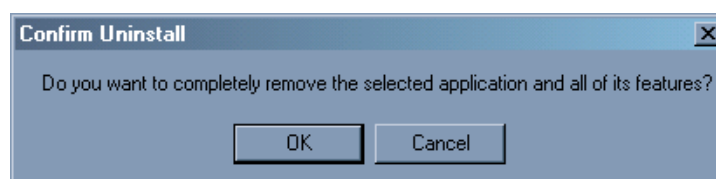
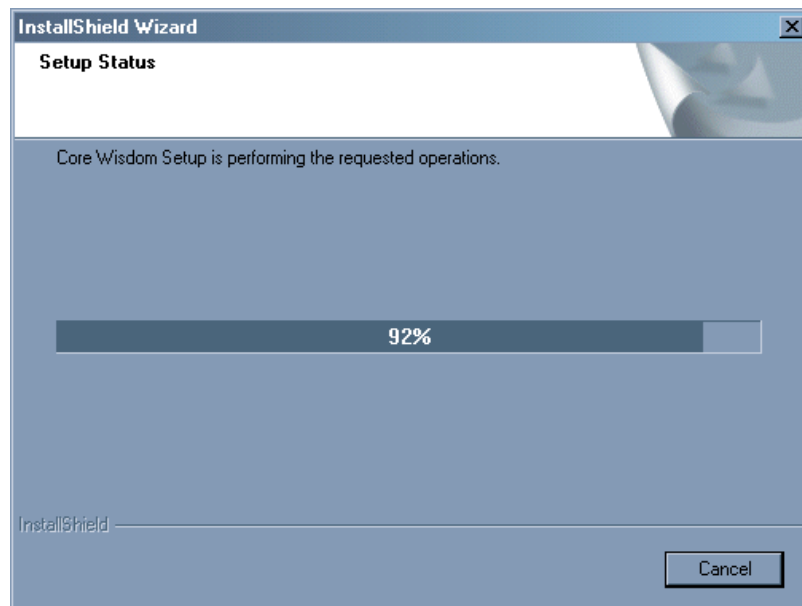


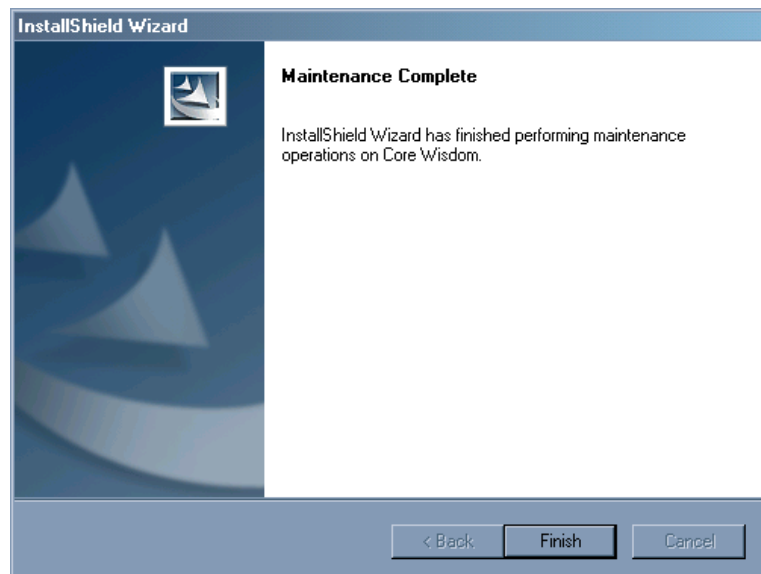
Figure 12: Confirm Uninstall

4. The uninstall proceeds, deleting all CORE Wisdom files and registry entries created during the install process. During this stage the window shown on Figure 13 will be displayed on screen with the status information.



**Figure 13: Setup status information**

5. The uninstall finishes. Click on the *Finish* button to end the InstallShield Wizard.

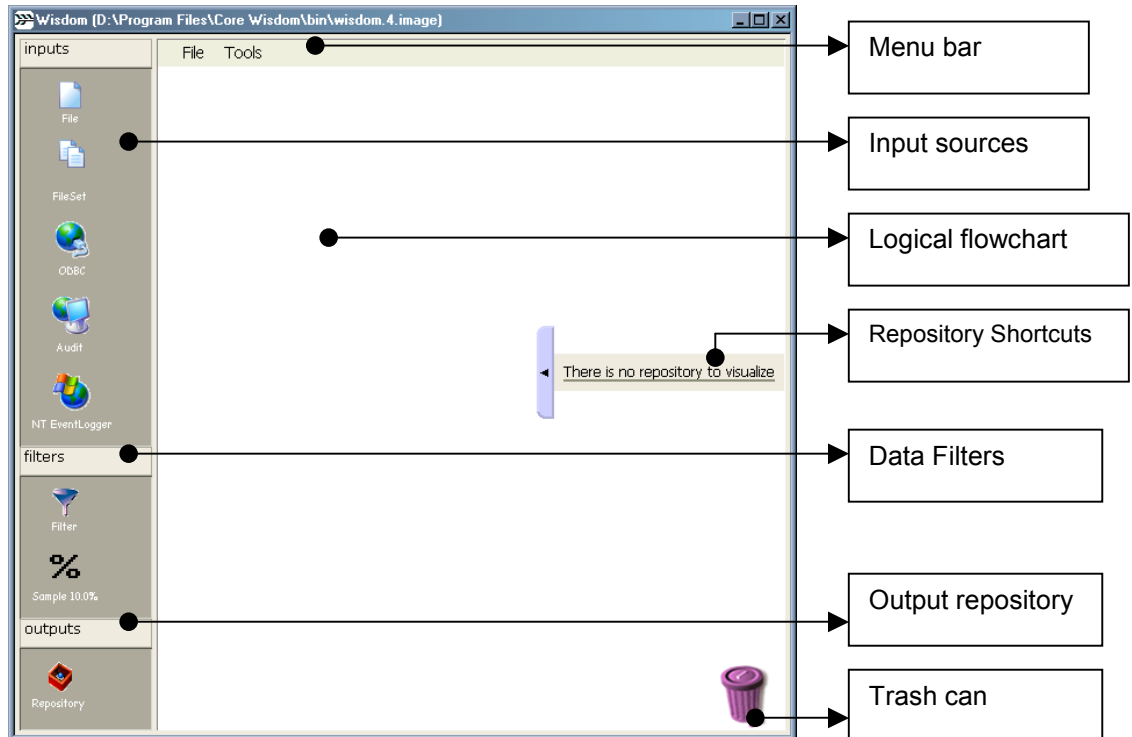


**Figure 14: Maintenance complete**

6. Close the Add/Remove Programs window.

## 2. Analysis with WISDOM

To access *CORE Wisdom*, go to the Windows *Start Menu* and select the *Programs* folder. Click on the *CORE Wisdom* program icon. The main window (Start-up window) appears (see Figure 15), ready to start the analysis process. No data is selected for analysis yet.



**Figure 15: CORE Wisdom Start-up window**

- a) **File:** This menu contains options for the export of data and particular settings on the Visualization area to maintain them. Use the *exit* option in order to end the current CORE Wisdom session.
- b) **Tools:** The *Tools* menu contains the options to define log format and parsing structures. Additionally, you can use it in order to update the CORE Wisdom software version.

Wisdom will parse log entries for a variety of formats, including but not limited to: text-based, database stored and Windows event logs. The log format will be defined first as *low level* parsing rules in order to allow Wisdom to identify the general log format for the application. After that, *application-specific* rules will parse the entry fields. A set of built-in parsing rules are included for the most common log formats. The auditor can define additional rules as is required. See section *Parsing Input sources* on page 18 for a detailed explanation of the rules creation process.

From the raw input log format to the parsed tables that are stored in the *repository* objects, the event data will pass through as many filters as required to build the analysis visuals and reports. This logical flowchart will be assembled by the auditor as is detailed on the *2.1 Log data handling* section on page 14.

Finally, the auditor will access the Visualization graphs, in order to carry on the visual analysis of the information contained on the event logs. See section 3. *Analysis procedures* on page 38 for a detailed explanation on these procedures.

## 2.1 Log data handling

The initial data acquisition and handling process includes the following steps:

1. Select the Input source that will be used in the analysis. Each of the different inputs that can be used involves its own particular features. See section *Selecting Input Sources* on page 15 for additional information on this subject.
2. Filter the information contained on the original logs. Filters can be applied either on Input Sources or Output Repositories. See section *Filtering information* on page 24 for more information on filter usage.
3. Select the Output Repository that will be used to visualize the data.

Actions allowed on the containers are divided in general actions (available for all sources) and specific actions featured only for a specific category.

General Actions are:

- Add a data connector between two containers
- Add an object to the Analysis Flowchart screen sector
- Delete an object in the Analysis Flowchart screen sector

### Connectors

This process can be viewed as a chaining of information containers (Inputs, Filters and Outputs) that will actually define the visualization scope for the analysis. The linking of each element in the chain is done through container connectors. Connectors appear as arrows with red control marks, which you can use to select the arrow's source and destination (see Figure 16).



**Figure 16: Connectors**

1. To add a connector, right-click on the source container and select the *add connection* option from the context menu.
2. The default source of the connector is the original container that was selected. To change the default source click on the source red mark and drag it to a different source container.
3. The destination container has to be manually selected. Click on the destination red mark and drag it to a different destination container.

To update the destination container with the data from the recently connected source, left-click the destination container and select the *update* option from the context menu.

### Adding objects to the Analysis Flowchart sector

To create the Analysis Flowchart you will have to add multiple data containers, filters and connectors in order to select the data source and the event scope that will be analyzed. You can also combine data sources.

1. To add objects (containers and filters) to the Logical Flowchart sector, perform a single left-click on the object or click and drag the object onto the sector.

### Deleting objects

1. To delete an object on the Analysis Flowchart screen, either:
  - a. Right-click the object and select the *delete* option in the context menu or
  - b. Click and drag the object to the Trash Can, located on the lower right section of the Analysis Flowchart screen.

## Selecting Input Sources

These files are read by the parsing component in WISDOM and visually presented on screen. Five different Input types can be used:

### Single-File container



This container allows the inclusion of single-file log sources. In order to attach a log file to this container:

1. Right-click the *File* container and select the *choose file* option from the context menu (see Figure 17).

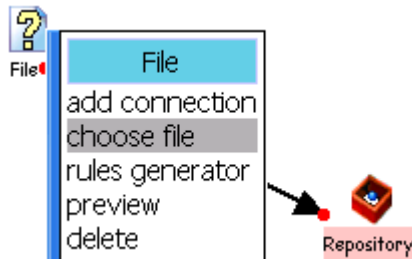


Figure 17: Choose single-file input

2. Browse to select the file that you wish to use as a source (see the window shown on Figure 18).

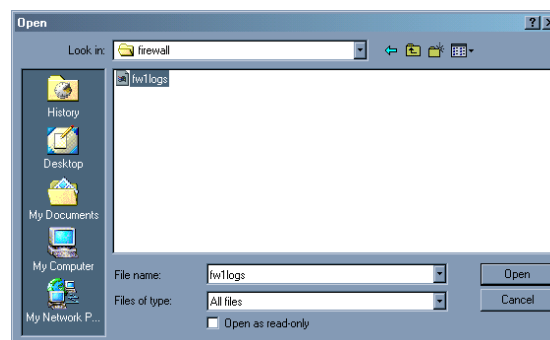


Figure 18: Locate single-file log

3. Once the file is selected, the container icon changes (the question mark disappears) and the icon label describes the file name, log format detected and log size. A sample icon is shown in Figure 19.



Figure 19: File selected icon

- You can also access the raw log entry by right-clicking the container and selecting the *preview* option from the context menu. See Figure 20 for a sample preview window.

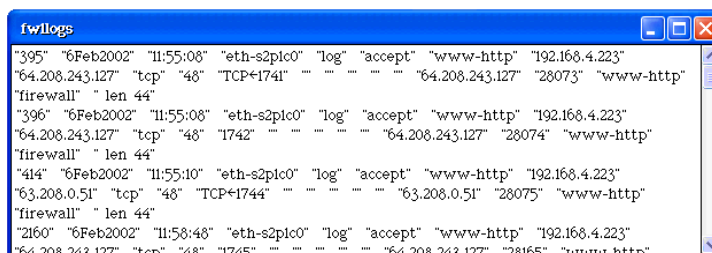


Figure 20: Sample log preview



### FileSet container

Multiple source files can be selected, given they share the same format and naming convention. Source events are grouped by day in each file in the source folder and named after the following syntax, *Logtype**date* (YYYYMMDD; year, month, day). The log type is represented by the initial letters in the file name and is required to be shared by all files in the log set.

- Right-click the FileSet container and select the *choose file path* option from the context menu to select the location of the folder that stores the log set files.
- A dialog box shows on-screen asking for the folder path and common string for the set. For instance, the example in Figure 21.

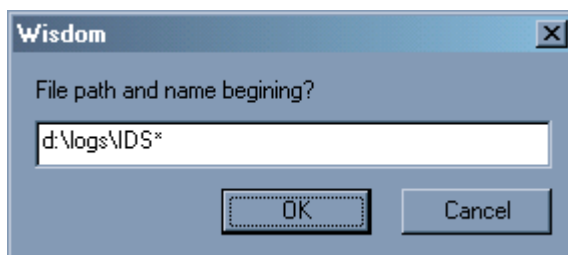


Figure 21: File path and name beginning for log set

- Select the timeframe interval for the events that will be included on the container. In order to do this, right-click the *FileSet* container and select the *default interval* option. You can manually select the start and end dates by selecting *Other...* from the Interval drop-down list.

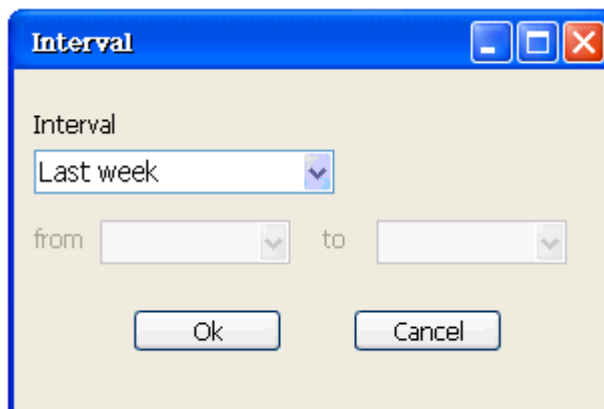


Figure 22: Setting the event interval



4. The container icon changes, showing the path and log type that was selected.



FileSet d:\logs\IDS\*

**Figure 23: Fileset selected icon**

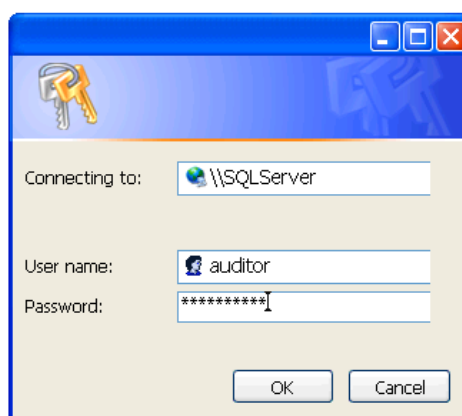
### ODBC queries

ODBC sources can also be used to acquire the log entries. If an application that is to be audited accepts ODBC queries on the entries, this container can be used to configure and establish the connection through the ODBC source. Note that the ODBC driver should be installed previously to the connection attempt.

1. To configure parameters for the connection, right-click the ODBC query container end select the *parameters...* option. Enter the machine name and user credentials in the form fields.

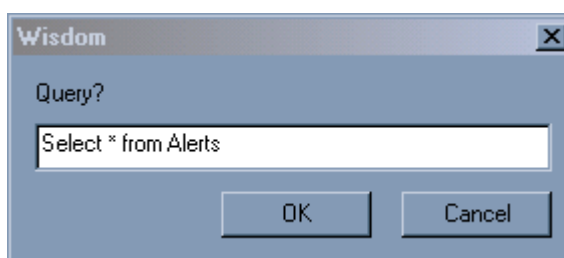


ODBC



**Figure 24: Parameters for the ODBC connector**

2. To perform a query on the data, right-click on the ODBC container and select the *set query* option from the context menu. Type in the query string, following the format accepted by the connection and click the OK button.



**Figure 25: Enter query**

3. When the connection completes successfully, the log entries stored on the data source are downloaded to the CORE Wisdom workstation.



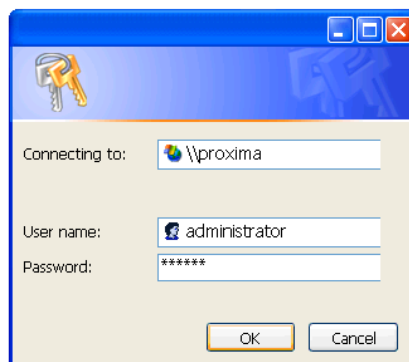
NT EventLogger

### NT Event Logger

NT Event Logger can be accessed and used as data input. All three log types can be accessed remotely from the source machine (System, Application and Security).

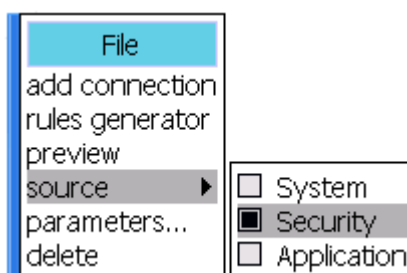
1. The first step to configure the NT Event Logger connection is to enter the connections credentials indicating destination machine's name, user

name and password. Right-click the NT Event Logger container and select the *parameters...* option from the context menu in order to access this configuration dialog.



**Figure 26: Enter connection credentials**

- Next, you can select the specific log type (Application, Security and System). In order to do this, right-click the NT Event Logger container and select the *source* option in the context menu (see Figure 27). Choose the log type that you wish to import.



**Figure 27: NT Event logger context menu**

- The container icon changes, indicating the machine name and log type for the chosen source, as shown on Figure 28.



**Figure 28: Selected log NT Event icon**



### CORE Audit logs

Audit is a client/server tool that allows remote system logs auditing and centralizing, it supports standard and modular syslog output formats. The server (auditd) runs on audited machines and the client (audit) runs on the auditors workstations. Support for importing Audit logs will be implemented in the next release of CORE Wisdom.

## Parsing Input sources

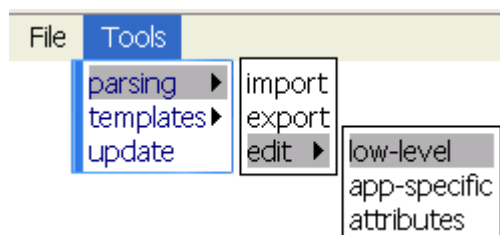
After you select an Input source to analyze, CORE Wisdom will attempt to parse the entries and interpret the field format. This will be used to build the attribute list for the log that will be available during the analysis.

Parsing rules are used to recognize the log format and fields. Several rules come included with the default CORE Wisdom installation, but you can build your own rules to parse a custom log file generated by any given application. Parsing rules are build in two separate levels:

### Low-level parsing rules

These rules refer to the general log format and their format is usually in the form: {monthName} {day} {hour}:{minutes}:{seconds} {host} {application}[{pid}]: {message}.

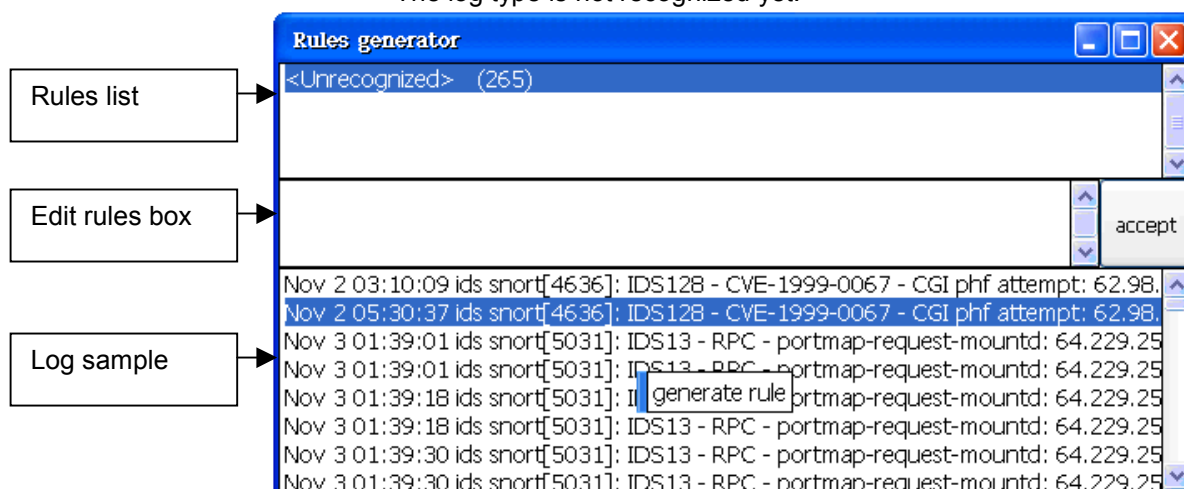
- a. In order to add custom Low-level rules access the *Tools* menu on the Start-up window and select the *edit* option on the *parsing* submenu. This will display the *edit* submenu option list. Select the *Low-level* option from the list (see Figure 29). Alternatively, you can right-click on the Input container and select the *Rules generator* option from the context menu.



**Figure 29: Edit low-level parsing rules**

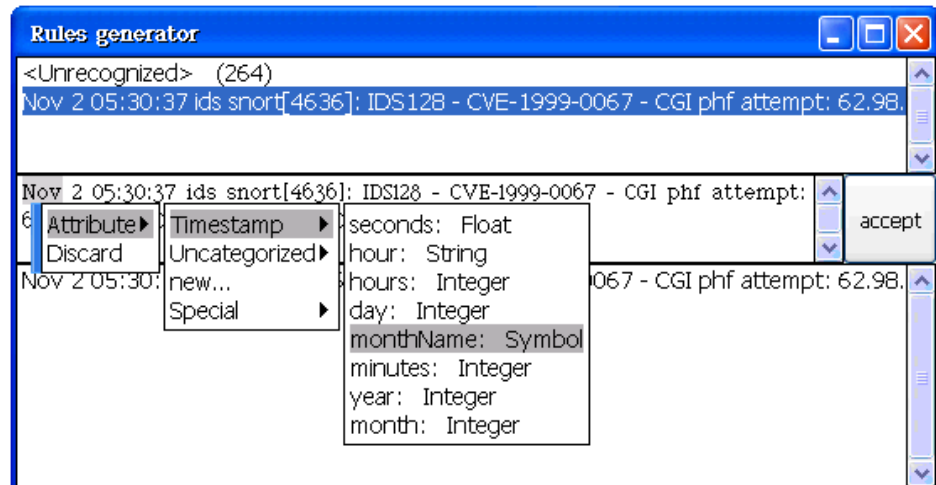
**Note:** The second option is recommended when you have a sample of the log entries that can be taken as a model to build the parsing rules definitions. We will use this option for our sample rule.

- b. This opens up the *Rules generator* window shown on Figure 30. The log type is not recognized yet.



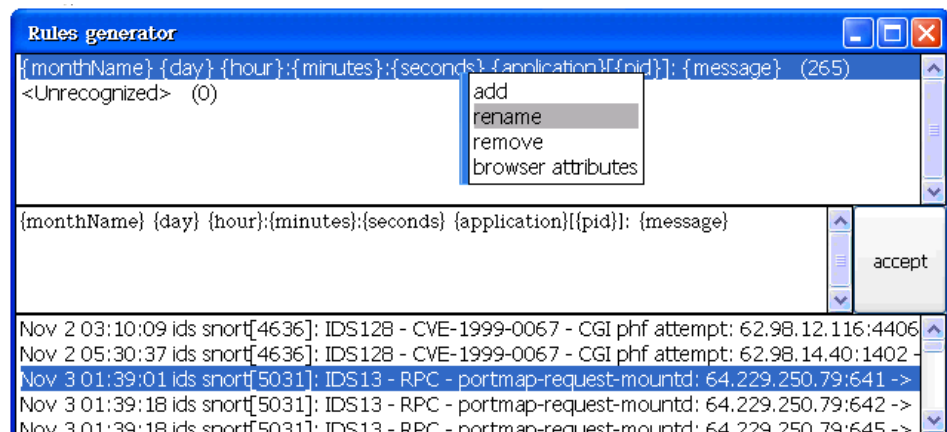
**Figure 30: Rules Generator for low-level parsing**

- c. Create the new parsing entry by right-clicking on one of the log entries and select the *generate rule* option from the context menu. This will create a new rule entry in the Rules list. In the Edit rules box you can assign a type for each field, as it will be recognized for each application. Here should be labeled all common fields for the application. All the remaining text strings that will vary will be described as *message* field for the application. See Figure 31.



**Figure 31: Assigning attribute type to low-level rules**

- d. After the entry is created, right-click on the entry name and select the *rename* option from the context menu. You will be asked to enter the name for the rule. Choose a name that help to identify the application later, like SnortRule.



**Figure 32: Rename the rule entry**

### *Application and Message field types*

Two special fields will be used when defining low-level parsing rules, and will be used later by the Application-level rules.

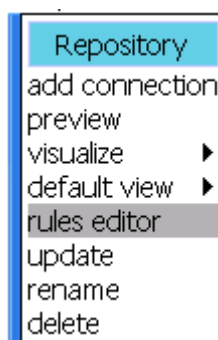
1. **Application:** The field defined as *application* field will be used as the pattern name in the Application-level rules. See section *Application specific details* on page 21 for more details on this.
2. **Message:** When you define a section of the entire log entry as being of *message* field, this means that this particular section will be parsed as part of the Application parsing rules. For instance, this can happen with an application that generates entries of different format. Although some sections of the entries must share a common structure. The common

structure will be defined in the low-level parsing rules and the sections that varies will be parsed as Application type rules.

## Application specific details

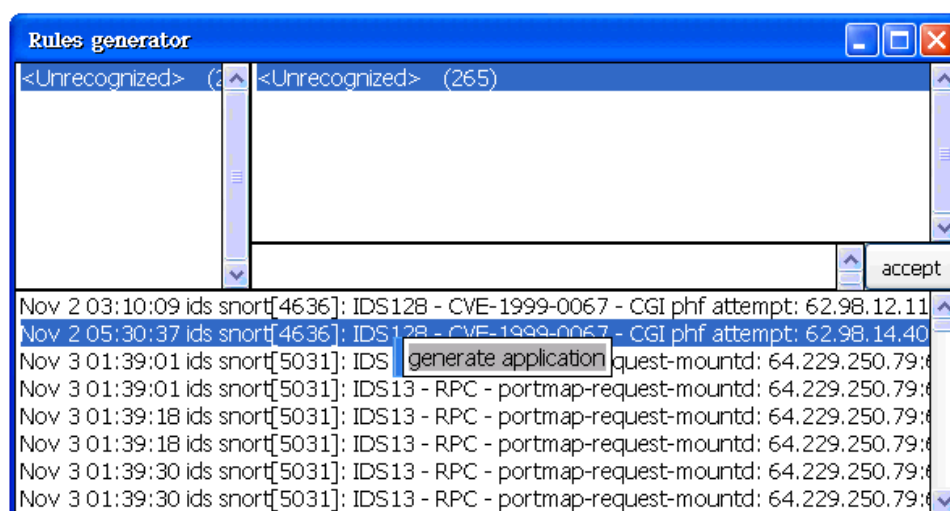
These rules further detail the different entries that could be generated by a given application. For instance, possible rules for the Snort Lightweight IDS could be:

- e. A rule that parses all Port Scan preprocessor entries, such as:  
`spp_portscan: PORTSCAN DETECTED from {sourceHost} (STEALTH)">spp_portscan: PORTSCAN DETECTED from {sourceHost} (STEALTH)`
  - f. A rule that parses all TCP/IP-related alerts, such as:  
`{attactType}: {sourceHost}:{sourcePort} -&gt; {destinationHost}: {destinationPort}">{attactType}: {sourceHost}: {sourcePort} -&gt; {destinationHost} :{destinationPort}`
1. In order to define these rules, you must create a Repository container that will contain all events for a given Input source. Right-click the Repository container and select the *rules editor* option from the *Repository* context menu shown on Figure 33.



### Figure 33: Edit Application-specific parsing rules

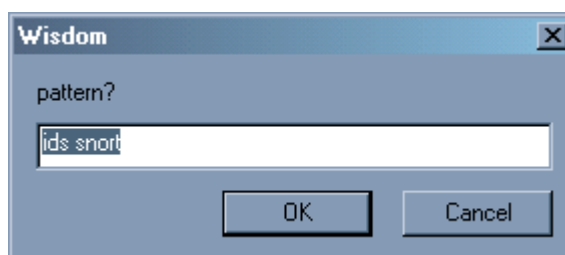
2. The *Rules generator* opens up. Initially there are no rules defined for the Repository container that could parse the *message* substring for the log entries. Right click on one of the entries to start the definition of the application-level parsing rules. Select the *generate application* option in the context menu, as shown on Figure 34.



### Figure 34: Generate application-level parsing rules

3. You will be asked for the pattern name, which must be defined as the content string for one of the *application*-type fields defined for the low-

level parsing. In our example it will be “ids snort”. Click the *OK* button to accept the pattern name.



**Figure 35: Enter pattern name**

- Now you will have to generate the rules for this particular application, as was explained on the *Low-level parsing rules* section on page 19. In this case, the text string that will be defined for parsing will be the defined as *message* for the low-level parsing.

## Attribute-type definition

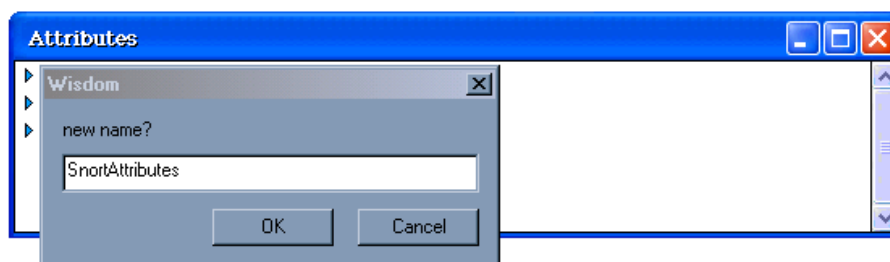
You can define custom attributes, in order to define custom fields for any given application that will be available for selection in the Visualization area during the analysis.

In order to access the Attribute tree, select the *edit* options list in the *parsing* submenu on the *Tools* menu located in the Start-up window to access the *attribute* option. This will open the Attribute window, where two basic components can be defined:

- Categories:** These are groups of attributes and other subcategories. Categories are useful to organize the attribute tree and allow for a quick access to the attribute field name. By default the only categories that exist in the default installation are TimeStamp and Uncategorized.
- Attributes:** Attributes are the base component of the attribute tree and will be used as building blocks for the parsing rules. Each attribute is defined by the field name and data type (string, integer, etc).

## Adding categories

- To add a new category, right-click on the attribute tree window and select the *new category* option from the context menu. You will be asked to assign a name to the new category, as shown on Figure 36.



**Figure 36: Assign a name to the new category**

- In order to create a new subcategory of the selected category, right click the higher-level category and select the *add subcategory* option from the context menu. Enter the name for the new subcategory. See Figure 37.

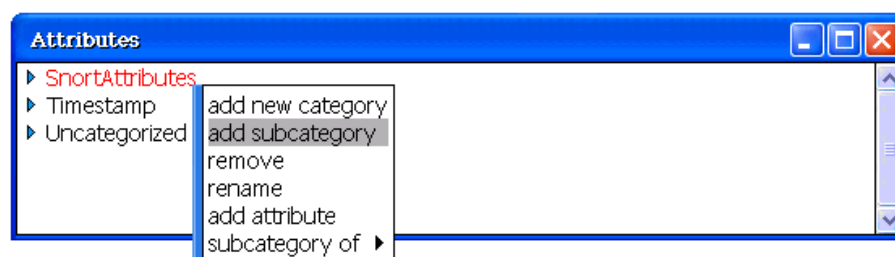


Figure 37: Category context menu

### Adding attributes

1. To add a particular attribute to a category or subcategory, right-click the category container and select the *add attribute* option from the context menu (see Figure 38).

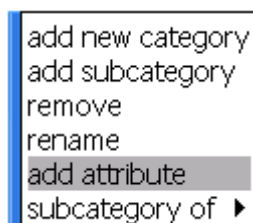


Figure 38: Adding attribute types

2. You will be asked to assign a name to the attribute. Enter the name and press the OK button.

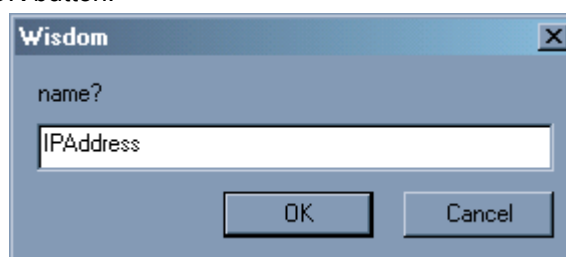


Figure 39: Enter attribute's name

3. By default, attribute fields are considered text strings, but you can assign a different type by right-clicking on the attribute and select the proper type from the *type* option list, as shown on Figure 40.

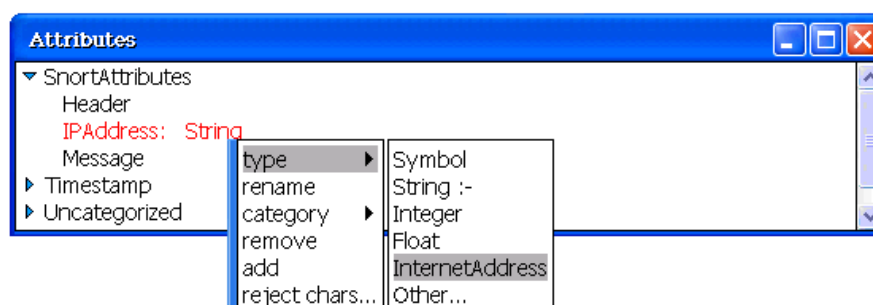


Figure 40: Select attribute type

4. You can also select to reject specific characters from the attribute field contents, to make for an accurate detection on the log type. To do this, right click the attribute name and select the *reject chars...* option from the context menu. Enter the characters that will be excluded in the dialog window shown on Figure 41.

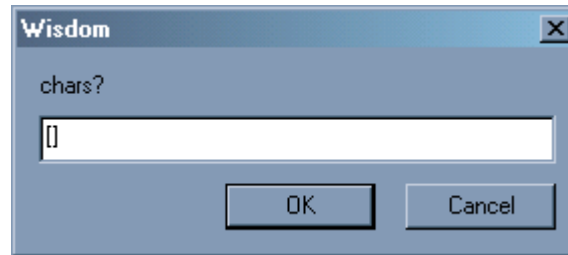


Figure 41: Excluding bracket chars from the attribute' contents

### Moving components to a different category

1. In order to move the currently selected category or attribute to be part of an existing category, right-click the component and select the *Subcategory of* (for categories) or *Category* (for attributes) option from the context menu. Select from the list the higher-level category where you wish to move the component to. The initially selected component will now be part of the destination category.

## Filtering information

CORE Wisdom offers two different filter types, in order to reduce the amount of events that will be used as input. This will speed up the processing of the logs.

1. Filter by criteria (Filter)
2. Sampling filter (Sample)



Filter

### Filtering by criteria

The Filter object can be added to the flowchart in order to reduce the amount of objects that the Repositories will receive by applying a logical filter by one of the attributes present on the log (log fields).

1. Add a Filter object in the Analysis Flowchart sector and connect it to an existing container (either an input source or a repository).
2. Right-click the Filter object and select the *Attribute* option from the context menu. A list with all log fields detected is displayed. Select the field name which you will use to filter the information. In the example shown on Figure 42 the selected field name is *sourceHost*.

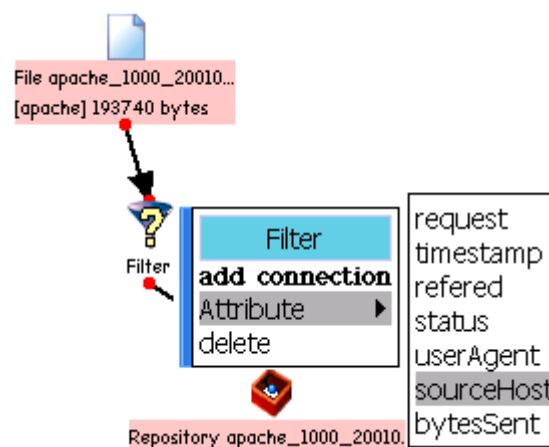


Figure 42: Select the field name

3. You can select two different filtering operations:



- a. Include values: which will transfer to the downstream container only log entries that matched the chosen value for the selected attribute.
- b. Exclude values: If you select to exclude certain values, only the entries that did not match the filtering criteria will be sent to the downstream container.

To toggle between both operations, right click the Filter object and select the *toggle include/exclude* option from the context menu.

4. Select the value that you wish to use as the filtering criteria. Most representative values are shown on the *Include values* (or the *Exclude values* option, depending on the selected operation), as is shown on Figure 43.

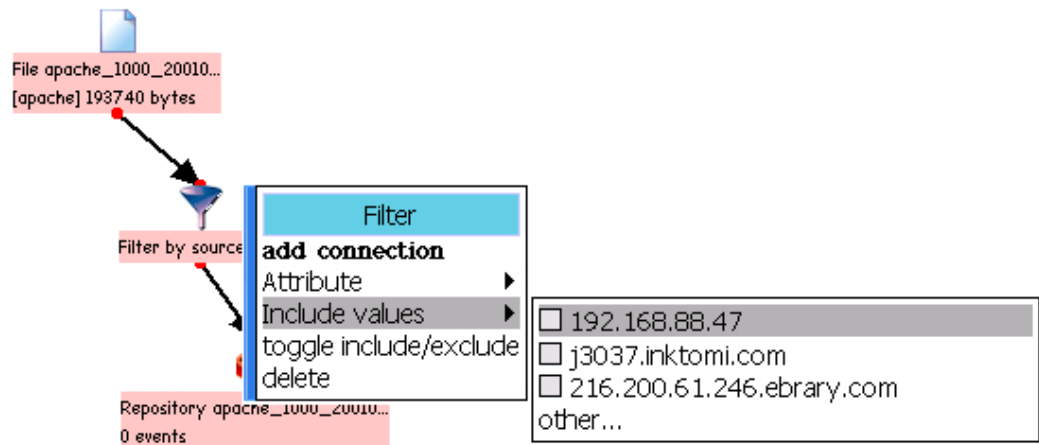
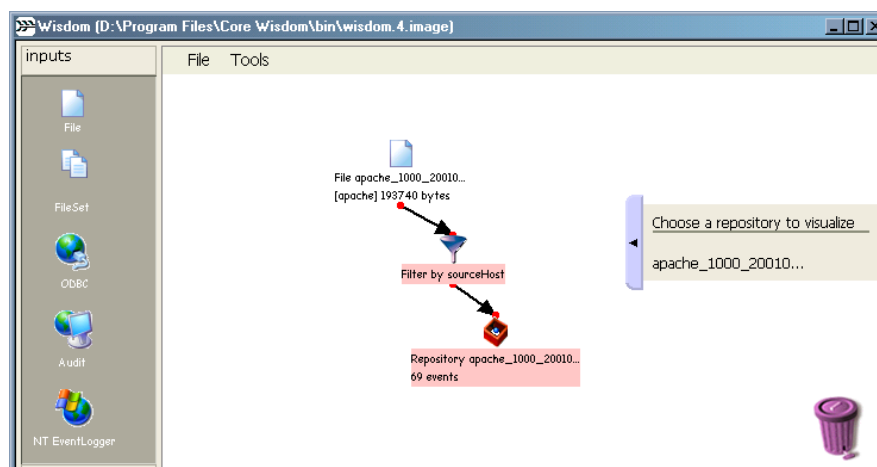


Figure 43: Selecting the field value

- Right-click on the downstream Repository and select the *update* option from the context menu in order to transfer the filtered events to the container. The downstream repository will now show the amount of events that matched the criteria, as is shown on Figure 44.



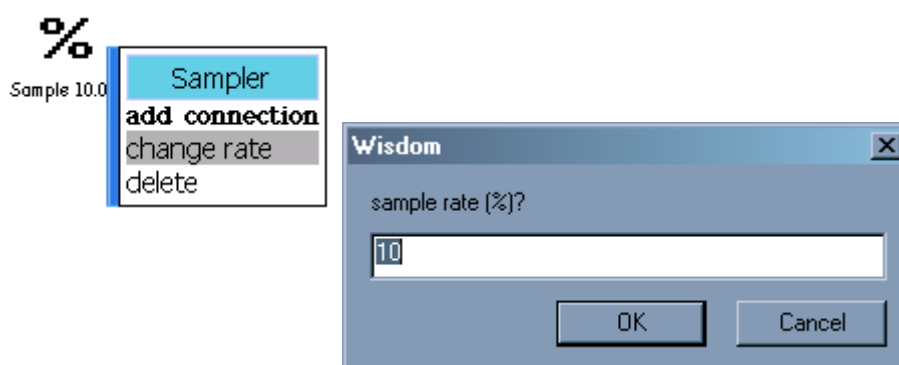
**Figure 44: Filter applied – Repository was updated**

**Note:** The *Repository Shortcuts* menu now shows the Repository name on the list. You can click the repository name to access the default view that was defined for that container. See section *Creating Output Repositories* on page 27 for more information on data repositories.

## Sampling

These filters allow to reduce the source log information to a custom percentage of the original number of events (default is 10%). Sampling filters will actually discard all other events in order to give the auditor a general idea of the event distribution during the graphical analysis of the log information.

- Add a Sampler object in the *Analysis Flowchart* sector and connect it to an existing container (either an Input source or a Repository).
- Right-click the Sampler object and select the *change rate* option from the context menu if you want to modify the default percentage value (see Figure 45).



**Figure 45: Change sampling rate**

- Next, update the downstream repository to transfer the event sample to the destination container. In Figure 46 two different Output repositories are shown, one with the sample events and other with the original source log.

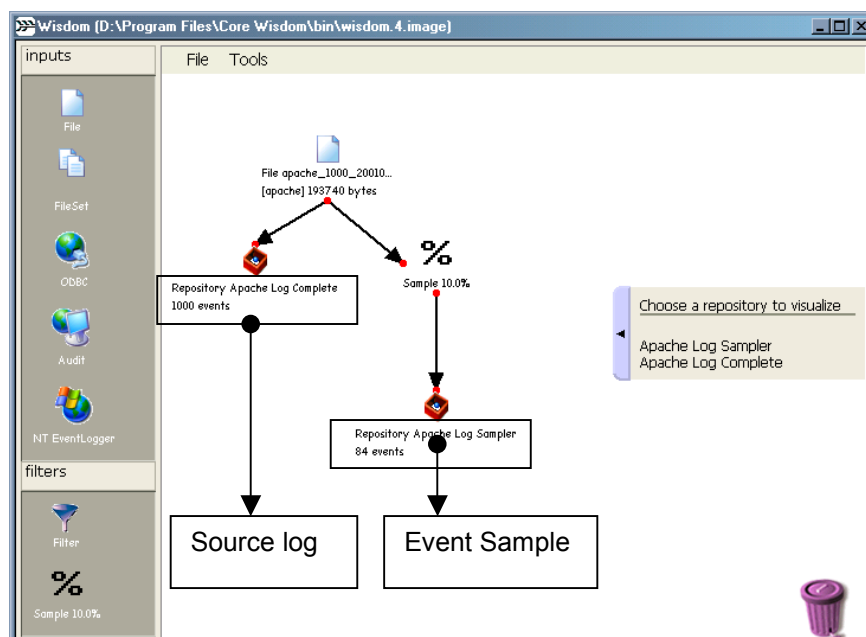


Figure 46: Sampled logs

## Creating Output Repositories

Output repositories provide the means to visualize the log information and are always the leaf objects in the logical trees build in the *Analysis Flowchart* sector.



### Previewing log contents

Similar to the action that can be performed on Input log sources, you can preview the raw log entries, although in the case of data repositories the logs are differentiated down to the field level, not by the entire log entry.

- In order to preview the log table, right-click the Repository object and select the *preview* option from the context menu. The log table is displayed on screen, as shown on Figure 47.

Apache Log Complete					
status	referred	sourceHost	request	bytesS	userAgent
200	http://www.cc	192.168.E	GET /in	43	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	http://www.cc	192.168.E	GET /in	5197	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	http://www.cc	192.168.E	GET /in	5197	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	http://www.cc	192.168.E	GET /in	5197	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	-	192.168.E	GET /h	14347	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	http://www.cc	192.168.E	POST /	1200E	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	http://www.cc	192.168.E	POST /	1200E	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	http://www.cc	192.168.E	POST /	50497	Mozilla/4.77 [en] (Windows NT 5.0; U)
200	-	192.168.E	GET /h	14347	Mozilla/4.77 [en] (Windows NT 5.0; U)
404	-	j3037.inkt	GET /ei	214	Mozilla/3.0 (Slurp/cat; slurp@inktomi.com; http://www.ink
302	-	dyn-wirele	GET /a	274	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
200	-	dyn-wirele	GET /c	7234	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
200	-	dyn-wirele	GET /p	3893E	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
200	-	dyn-wirele	GET /js	614	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
200	-	dyn-wirele	GET /in	185	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
200	-	dyn-wirele	GET /in	186	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
200	-	dyn-wirele	GET /in	369	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

Figure 47: Log table for the selected repository

## Updating the repository contents

Every time you change either the filtering settings or information sources, you will be required to update the downstream repositories in order that the changes take effect and the new data set can be transferred to the downstream repositories.

1. To do this, right-click the data repository object and select the *update* option from the context menu.

**Note:** The repository label will update the event count to the number of actual events.

## Renaming a repository

By default, repositories maintain the name of the original input source. In order to make easy the analyst task, you can rename the repository to a more meaningful name.

1. Right-click the repository and select the *rename* option from the context menu. The dialog window shown on Figure 48 appears, asking for the Repository new name.

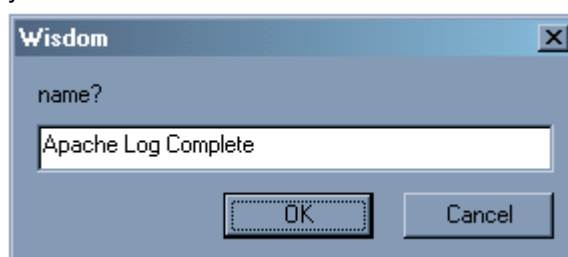


Figure 48: Enter repository new name

2. Enter the new name and click the *OK* button for the changes to have effect on the repository label.

## Visualization options on Repository containers

CORE Wisdom offers several features which you can select to begin with the visual analysis of the information contained on the log data.

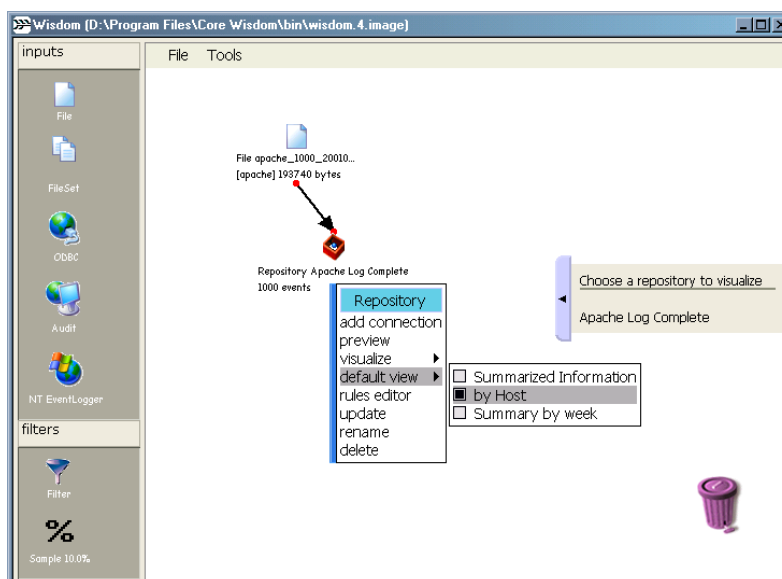
- Define default views for using with Repository Shortcut
- Select a Visualization mode (see Visualization Modes on page 35 for a detailed description on the available modes)

## Using Default views

Default views are customized templates that you can predefine to be opened each time you access the repository. When you select a default view for a given repository, it will be used each time that:

- a. You perform a double-click on the Repository container
- b. You select the repository name on the *Repository Shortcuts* menu

1. In order to select the default view for the repository, right-click on the repository container and select the *default view* option. The list of available templates is shown. See a more detailed explanation on templates creation and usage on the *Creating templates* section on page 50.



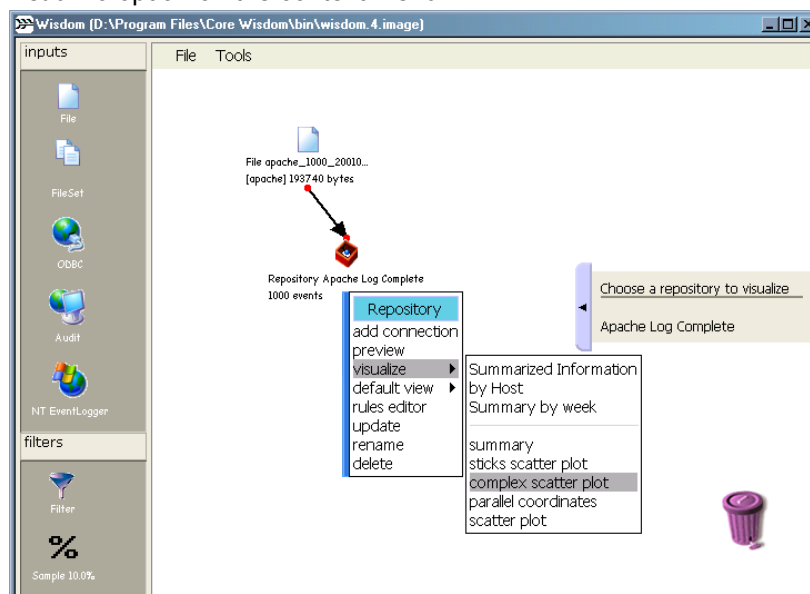
**Figure 49: Selecting the default view for a repository**

2. To open the repository' default view, perform a double-click on the repository or select the repository name on the *Repository Shortcut* list.

### Selecting Visualization modes

CORE Wisdom offers several Visualization modes that will be used to visually analyze the log information. Visualization modes are described in greater detail on the *Visualization Modes* section on page 35.

1. In order to access the Visualization Area where you will be performing the analysis tasks, right-click the repository container and select the *Visualize* option on the context menu.



**Figure 50: Select the Visualization mode or template**

2. Select the Visualization mode or template name that the new Visualization Area will have from the list of available views. (See the *Opening a new Visualization Area* section on page 44 for additional information).

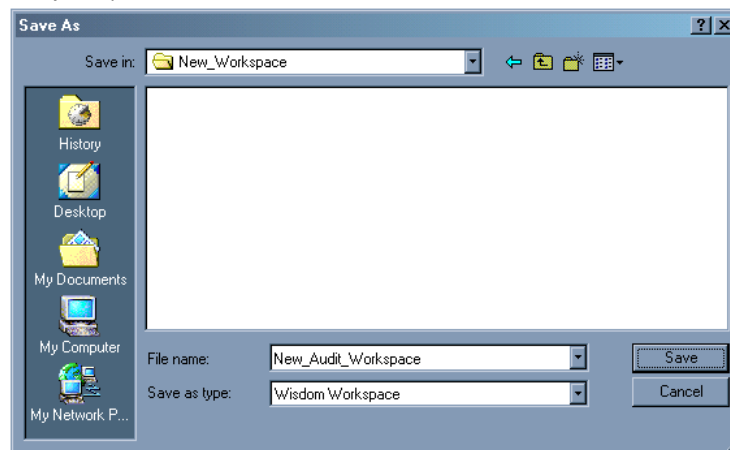
## Saving workspace definitions

One of the most relevant features of CORE Wisdom is the capability to maintain the Logical Workflow you have created available for later usage. In order to do this, you are required to save the settings into a Workspace-definition file.

1. Once you created the Logical Workflow by following the procedures described in the previous sections, select the *Save* option in the *File* menu.

**Note:** If you are working on a Workspace definition file that has already been saved, you can save the definition file under a different name by selecting the *Save As...* option in the *File* menu.

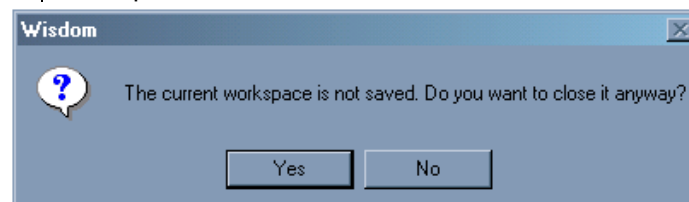
2. You will be asked for the folder path and the filename of the Workspace definition file in the *Save As* dialog window as shown on Figure 51. All Workspace definition files are stored with an *.ww* file extension (Wisdom Workspace).



**Figure 51: Select Workspace file path**

3. Next time that you need to use a previously stored Workspace definition, select the *Open...* option from the *File* menu.

**Note:** If you are currently working on a workspace, you will be warned that the changes to that workspace will be lost (see Figure 52). Click the *No* button and save the changes if you wish to preserve the current Workspace definition for later usage. Otherwise, click the *OK* button to open a different Workspace definition file.



**Figure 52: Warning: Workspace definition was not saved**

4. Indicate the file name of the saved Workspace definition file in the *Open* dialog window.



## 2.2 Starting the analysis

When you access CORE Wisdom the initial interface is the Start-up window that allows you to choose which type of visual representation you will start working with. The selection you make here starts a predefined query comprised of information contained on the selected Input source and the filters applied through the repository chain in the Analysis Workflow.

Once you have selected the initial visualization settings, you will access the Visualization Area with the default parameters (Graphic Display, Axis values, timeframe, criteria for filtering of events, etc.) for the query already set. While working in the workspace for the selected query you navigate the initial Visualization Area, opening additional Areas as needed to focus on a specific timeframe or set of events as shown in the scheme on Figure 53. You will also be presented with additional options for changing each particular view to further adjust it in order to obtain a clearer layout of the data.

For a detailed description of the options available for each Graphic Mode see section 3.2 *Specific procedures and settings* on page 52. You will use the Visualization options offered by the product to create customized views on log trails and gather insight on normal patterns and anomalous or unauthorized behavior that could be taking place on your company's application systems.

**Note:** As we stated before, the initial Visualization mode settings are automatically selected, based on the default values of the query chosen in the Start-up window.

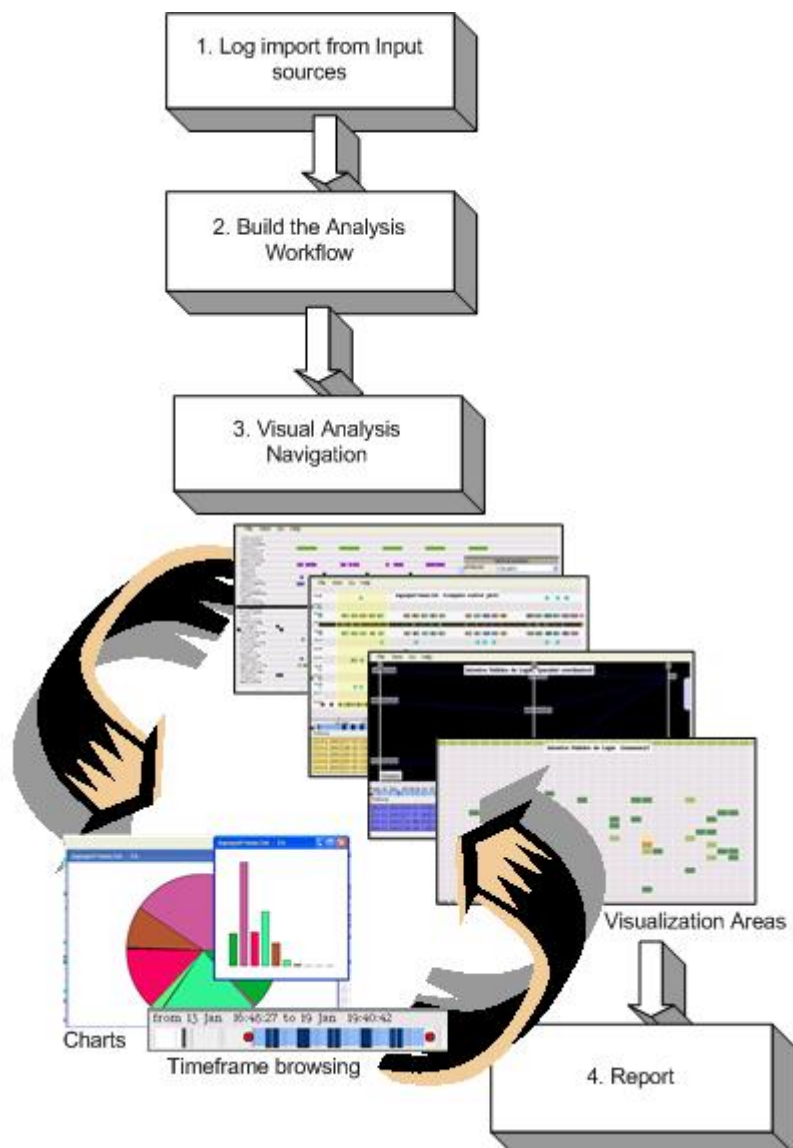


Figure 53: Analysis process – life cycle

## 2.3 Graphical interface description

The graphical interface used for log analysis in WISDOM is called the Visualization Area. Inside this area, where most of the analysis tasks are performed, the log information is shown and the auditor can visually explore the logs in order to discover anomalous events and patterns of activity. In Figure 54 you can see the general structure of the Visualization Area.



A: Menu Bar

B: Browsing Panel

C: Time Frame Control

D: Data Panel

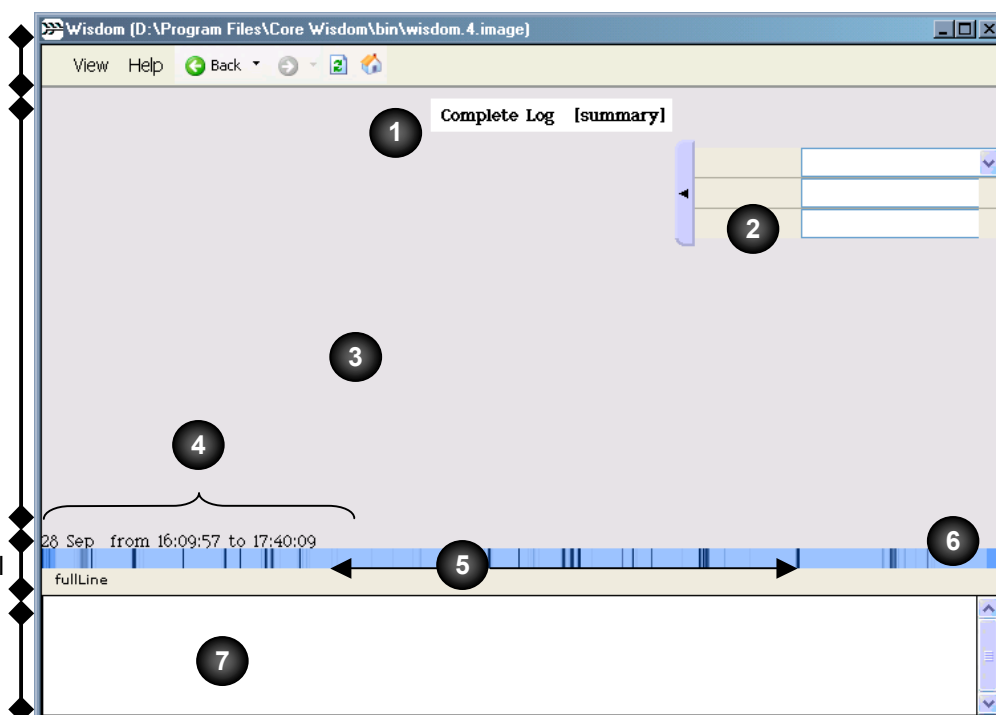


Figure 54: Visualization Area schema for all Visualization Modes

**Visualization Area:** You will start the analysis with the default Visualization Area for the query initially selected. When you move forward on the security analysis process you eventually could end up with multiple Visualization Areas opened. Inside the Visualization Area you can differentiate various sectors:

**B. Menu bar:** The menu bar contains the options available for all general operations performed on the analysis process.

The Menu bar has the following submenus (see Figure 55)

- a) **View:** The options available on this menu controls the visualization on screen. You can select through this menu the visualization mode which will be used as well as the user-defined or built-in templates to be applied on the visualization.
- b) **Help:** Gives access to WISDOM's on-line help.
- c) **Back and Forward buttons:** Permits the auditor to navigate through the Visualization Areas opened in the analysis.
- d) **Refresh:** Refreshes the contents of the Visualization Area.
- e) **Home:** Goes back to the Start-up screen.

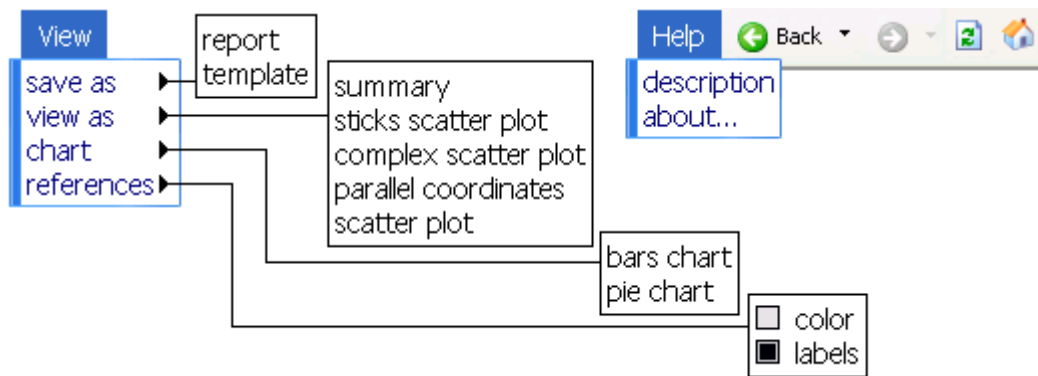


Figure 55: Complete menu bar

## B. Browsing Panel

(1) **Title:** This element shows the Repository name that was used as source of the information identifying the log which will be parsed and analyzed. The title also identifies the Visualization mode (Summary, Scatter Plot, Complex Scatter Plot or Parallel Coordinates) chosen by the auditor.

(2) **Settings Configuration Flap:** This control can be hidden or displayed by performing a click on the left bar of the object. Its content varies with each Visualization mode and allows for additional customization of the graphic shown on the Browser Panel. See the description on each visualization mode for the Configuration Settings flap values.

(3) **Analysis Graph:** This sector shows the graphical representation of the data comprised on the logs. WISDOM offers four different visualization modes to represent the events contained in the logs, namely Summary, Scatter Plot, Complex Scatter Plot and Parallel Coordinates. Each Visualization mode gives the auditor a different perspective to explore the events. See additional information about each Visualization Mode on section *Visualization Modes* on page 35

**C. Time Frame Control.** In this sector you can see three components: the *Slider Controls*, the *Data Time-frame display* and the *Event Density view*. See section *Focusing on timeframes* on page 41 for more information about procedures related to this control.

(4) **Data Timeframe display:** It shows the time interval where the analysis takes place. The initial Visualization Area shows at session start the complete period of time comprised by all events on the selected log. When the auditor starts navigating through the Visualization Area this component will only show the time frame of the selected events. See section *Selecting events* on page 39.

(5) **Event Density view:** The vertical black lines show the concentration of events around the selected time period.

(6) **Slider Controls:** The purpose of this component is to permit the auditor focalize on certain time interval in the logs, notably improving the visibility of some portion of the graphic.

**D. Data Panel:** The lower sector of the screen shows the raw log records that represent all events selected on the Analysis Graph sub area. There is no data in this area until a selection is made on the Browsing Panel, see additional information about this in section *Selecting events*, on page 39.

## Visualization Modes

### Summary Graph

By using **Summary Graphs**, as shown in Figure 56, you have a quick access to the distribution of events (total or filtered by some chosen criteria), and the analysis centers around specific periods in which the events occurs and what the occurrence rate is on the time unit selected for review. This allows the auditor to detect behavioral patterns exhibited by objects in the logs.

It is important to note that each mosaic in the graph represents the summatory of events and is differentiated by a color scale in relation to the amount of events represented in the box, as shown on the *Color* reference palette shown in Figure 56.

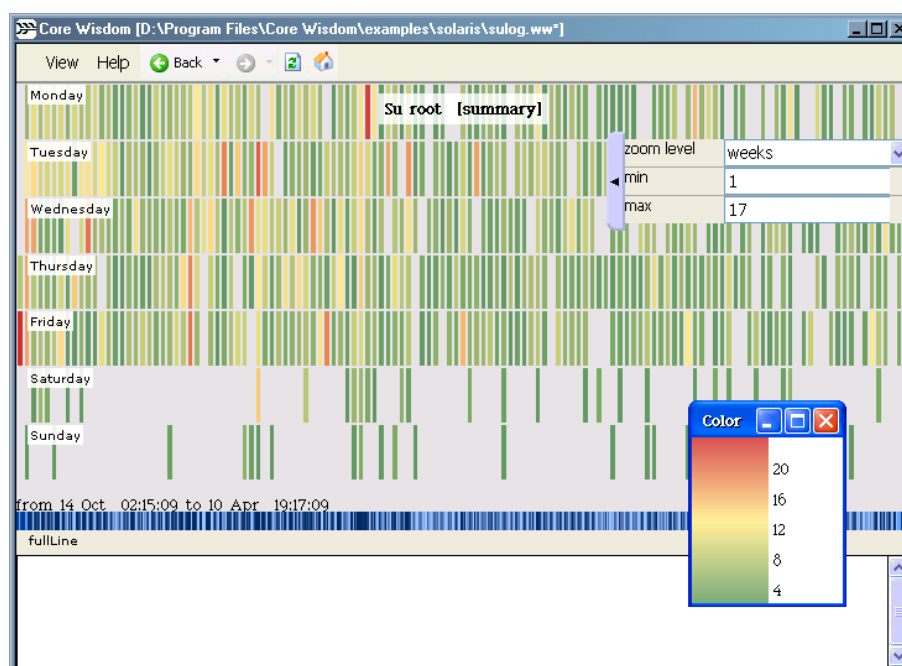


Figure 56: Summary graph

### Scatter Plot Graphs

With **Scatter Plot Graphs**, shown on Figure 57, you will find additional settings to adjust the information displayed on the Analysis graph. Each event is represented in this visualization mode as a colored box. The analysis features are expanded by introducing a user-configurable y-axis and the option to recolor the events based on specific categories. See section 3.2.2 *Using Scatter Plot view* on page 54 for detailed information about the procedures related with this graph.



Figure 57: Scatter plot graph

### Complex Scatter Plot Graphs

**Complex Scatter Plot Graphs**, shown on Figure 58, adds new dimensions that will improve the amount of information presented on screen for analysis. Each event is represented in the Analysis Graph as a colored dot. The auditor maintains in this visualization mode all the configuration options available with Scatter Plot views, plus the ability to change the *Border color*, *Size* and *Shape* relative to each attribute value. For additional information on the procedures available for use in this graph see section 3.2.3 *Using Complex Scatter plot view* on page 58.



Figure 58: Complex Scatter plot

## Parallel Coordinates

The **Parallel Coordinates** graph presents multiple y-axes interrelated by lines that show the correlation of multiple attributes in the events. Each single line correlates the occurrence of attributes for the same event. The auditor can discover possible patterns of grouping for the attributes of each selected y-axis variable. More information about the related procedures can be found on 3.2.4 *Using Parallel coordinates* views on page 62.

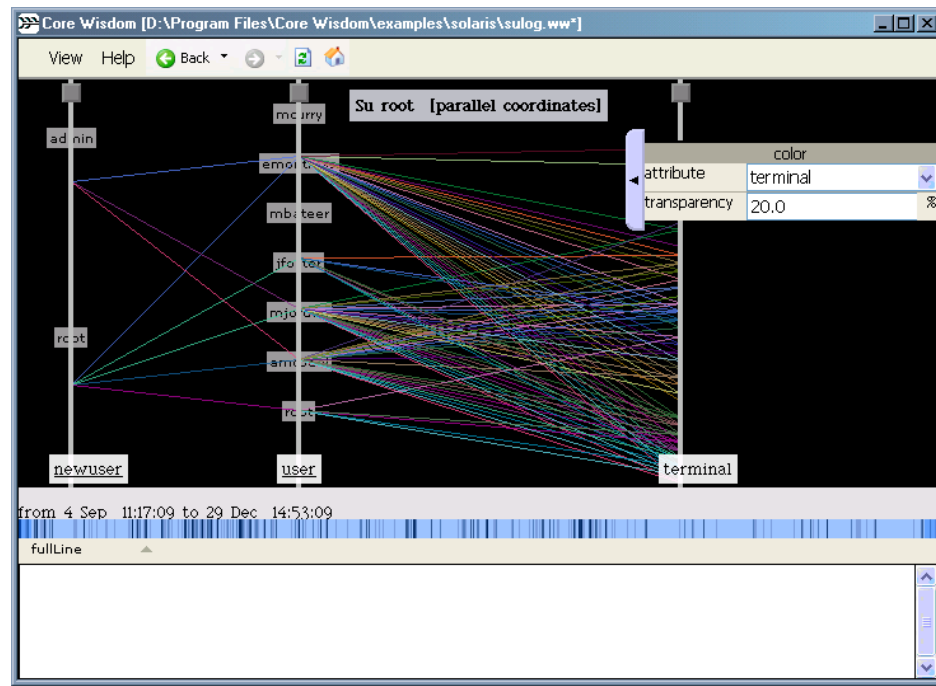


Figure 59: Parallel coordinates

## 3. Analysis procedures

In this section we will in first term review the general options available for manipulating the visualization options included on all graphs (see section 3.1 *Common analysis* procedures below) and then we will focus on the specific features of each different Analysis Graph (see section 3.2 *Specific procedures and settings* on page 52) used in the workspace for the analysis of system activity and anomalous events detection.

### 3.1 Common analysis procedures

The procedures described on the current section comprise general actions that apply to all Visualization modes (Summary, Scatter Plot, Complex Scatter Plot and Parallel coordinates).

#### Context Menu

When the auditor visually analyses the information, he or she interacts with multiple objects on screen (components described in section 2.3 *Graphical interface description* on page 32), but there are also other equally important graphic tools, used to perform actions on the objects in the Analysis graph and the Data Panel. They are the various context menus available to the auditor and one of the primordial tools in Wisdom graphical interface.

1. **Window Menu:** When the auditor performs a right-click **over a non-selected area** of the Analysis graph the *Window Menu* is displayed. This is used to generate new views or charts based on all events present in the current Visualization area, as described in sections *Opening a new Visualization Area* on page 44; *Using charts* on page 45 and *Creating templates*, on page 50. The *Window Menu* is shown on Figure 60.

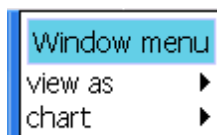


Figure 60: Window Menu

2. **Selection Menu:** When you right-click with the mouse **over a selected sector of the screen**, the *Selection menu* is shown. The actions available in this menu refer to the generation of new views or charts based only on the information present in the selected event range, as described in sections *Opening a new Visualization Area* on page 44; *Using charts* on page 45. It also contains the *Comment* option to insert the auditor's comments on the selected range in order to keep track of the events as described in the section *Commenting events* on page 50. The *Selection Menu* is shown on Figure 61.

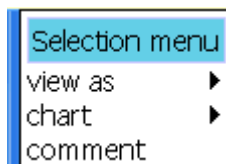


Figure 61: Selection Menu

3. **Chart Menu:** By right-clicking **on the charts objects displayed on screen**, the *Chart menu* pops up and presents the auditor with all actions related to chart handling, as the option to change the attribute

that bases the chart drawing as is described in section *Configuring chart settings* on page 45. The *Chart Menu* is shown on Figure 62.

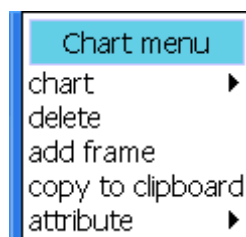


Figure 62: Chart Menu

4. **Data Panel - Add/remove attribute menu:** You will find this menu available by right-clicking the column name for a specific field in the log records shown on the Data Panel. This menu contains a list of the fields available for displaying on the current view. For information about the uses of this menu see section *Adding new columns* on page 43. *Add/remove attribute* menu is shown on Figure 70.

## Selecting events

You can graphically select a group of events to focus the analysis only on a subset of the entire log.

There are two different methods for selection of data, depending on the type of visualization mode in use at the time.

### Event selection on Parallel Coordinates graph

On Parallel Coordinate visualization modes you can select one of the values for the y-axes with a mouse left-click on the selection point for the value (example is circled in white), as shown in Figure 63. This action highlights all the lines going out from the selected category to the remaining axis in the graph. All log records related to this event rail are shown on the Data Panel.

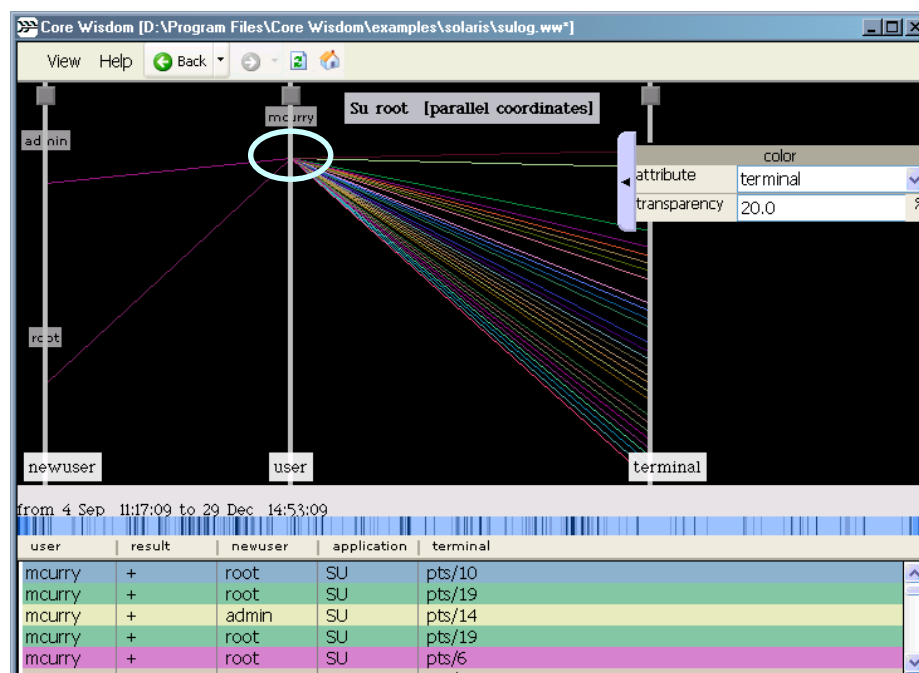
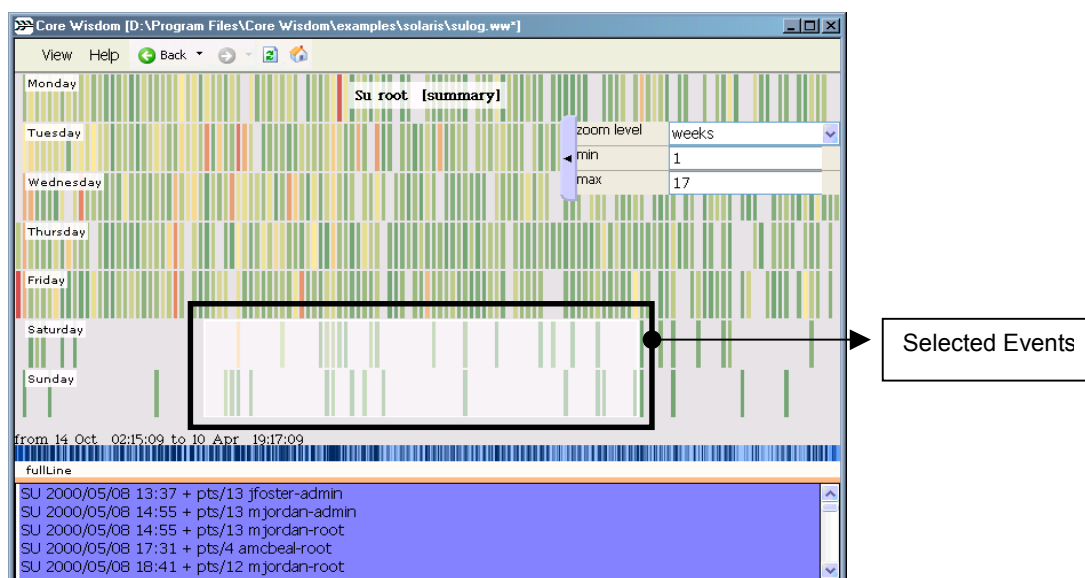


Figure 63: Selecting events in Parallel Coordinates visualization

### Selection procedure in other visualization modes

The other method for selection applies to both Simple and Summary graphic visualization modes. You can select events by performing a click-and-drag on any section of the graph. The selected portion of the display appears highlighted, as shown in Figure 64.



**Figure 64: Selecting events in Summary graphs**

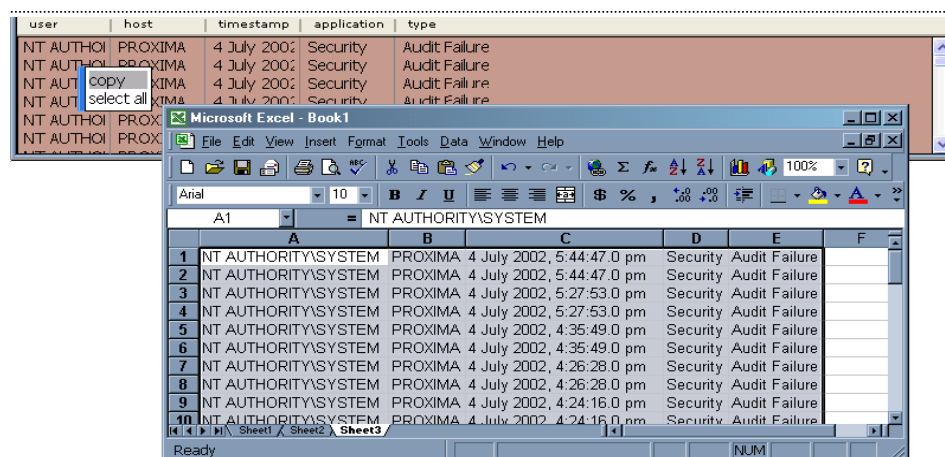
In all visualization modes, when you select a group of events the data contained in the log appears in the Data Panel for reviewing. In this way the auditor directly access the raw events that were used to construct the information depicted on the graphic in order to obtain the data values.

### Exporting Data Panel events

You can export the events shown on the Data Panel grid to third party applications, such as Microsoft Excel. Exported data will follow the same column format as in the current Data Panel settings and will be separated by TAB characters.

1. Select the entries that you wish to export by clicking on them. In order to select all entries shown on the Data Panel, right-click on the Data Panel sector and select the *Select all* option from the context menu.
2. Right click on any selected event and choose the *Copy* option to copy the data to the clipboard.





**Figure 65: Exporting Data Panel entries**

3. Paste the data on any application such as Microsoft Excel or Windows Notepad.

#### *Related tasks*

Changing Data Panel display options. See on page 43

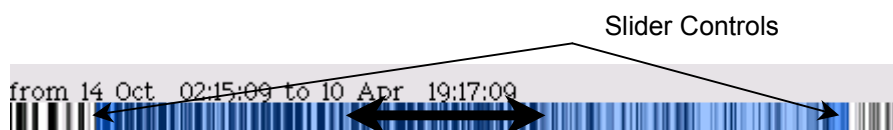
Opening a new Visualization Area. See on page 44

Using comments to keep track of events. See on page 50

Commenting events. See on page 50

Using charts. See on page 45

#### **Focusing on timeframes**



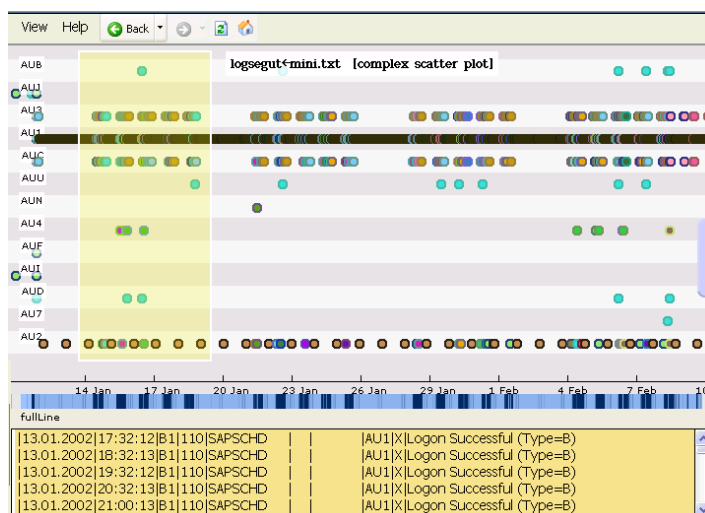
**Figure 66: Slider Controls resizing analysis interval**

Although newly opened visualizations start with the complete event range for their related query, you have the option of navigate through this timeframe with the Time Frame Control. This browsing control allows you to focus on certain periods of occurrence of the logged events by reconfiguring the Analysis Graph to only show a subset of actions. In this way the auditor can zoom on the data for the selected time segment and have access to additional details that could otherwise be missed. There are two options available: resizing and sliding of the controls.

#### **Resizing procedure**

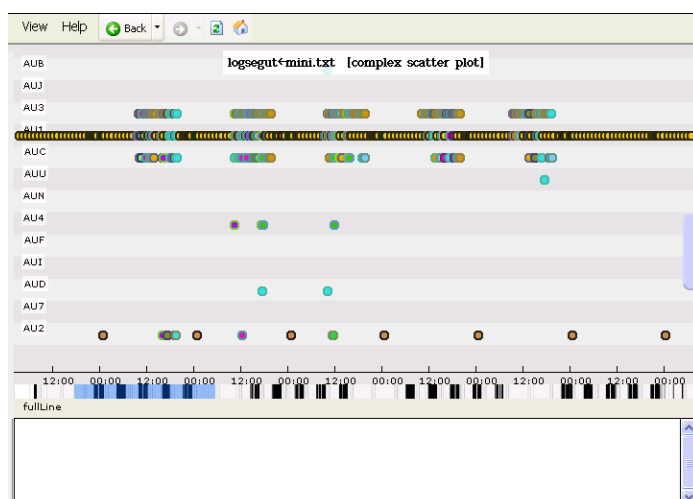
1. Select with a click-and-drag one of the sliding controls on the slider
2. Move the selected control to the right or left in order to extend or reduce the time segment
3. You will see that the Analysis graph is adapted to the new time frame

As you can see on Figure 67, the original Visualization Area shows the entire timeframe covered by the log. Four weeks of events are shown on the graph. A first analysis shows that the event are clustered around four groups, each one identifying one week. The Event Density view also shows this grouping as a concentration of vertical black lines around each cluster of five days in the four weeks.



**Figure 67: Analysis graph before zoom (four weeks interval)**

The analyst can zoom in the first week, by reducing the Slider controls as shown in Figure 68. In this fashion, the events for each day are easily identified in the general picture. The **Event Density View** keeps displaying the whole four weeks, but the **Analysis Graph** is focused on the first week only (selected area in Figure 67).



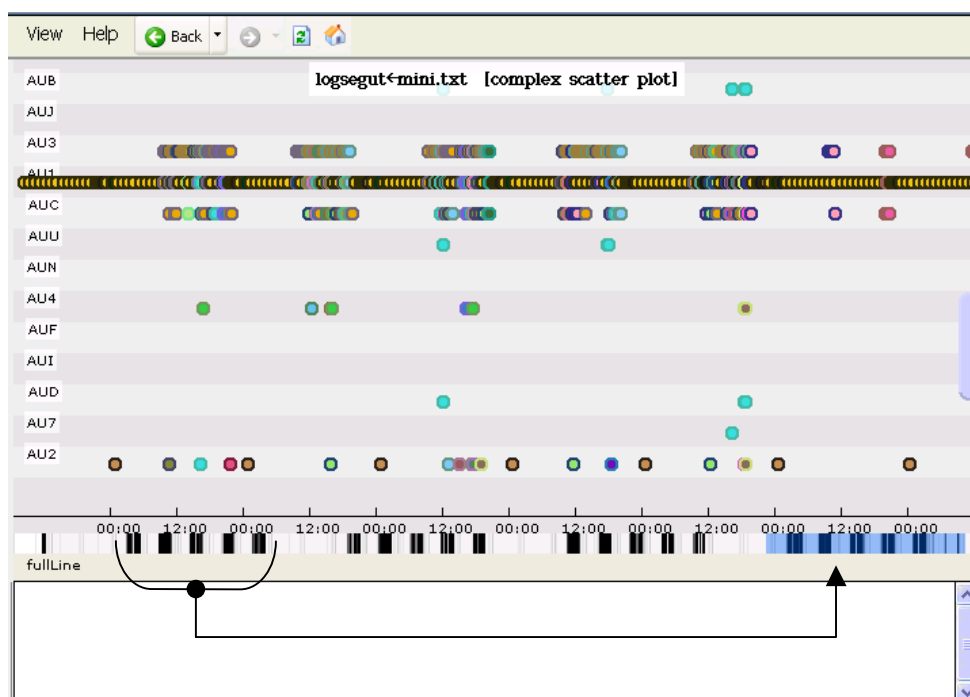
**Figure 68: Analysis graph after zoom (one week interval)**

### Time slide procedure

You can move forward or backward over a sub segment of the timeframe, to do this:

1. Click-and-drag on any section of the Slider Control.
2. Slide the control to the right for going forward in time or to the left to access the previous events.
3. You will see that the Analysis graph is adapted to the new sub segment of time frame.

In the new Analysis graph, as shown in Figure 69, the last week is now displayed.



**Figure 69: Analysis graph after moving forward in time (last week)**

### Related tasks

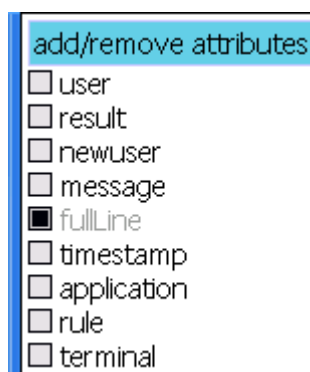
- 3.2.1 Using Summary view . See on page 52
- 3.2.2 Using Scatter Plot view. See on page 54
- 3.2.3 Using Complex Scatter plot. See on page 58

## Changing Data Panel display options

When you perform an event selection on the graphic the raw event from the logs appears on the Data Panel section of the visualization area. On the initial view each record shows the *full line* containing every field on the event record.

## Adding new columns

1. Perform a right-click on the field header of the Data Panel. When you do this the context menu (see on Figure 70) appears,
2. Select the checkbox labeled with the field name, and the selected field will be displayed before the first column.
3. To hide a particular field, clear the checkbox labeled with the field name.

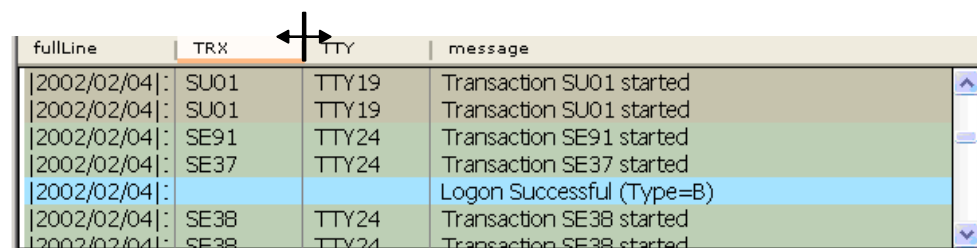


**Figure 70: Adding columns on Data Panel**

## Resizing of columns

The auditor can also resize the column width for each of the selected records on the Data Panel. To do this:

1. Position the mouse on the division line at the right side of the column name as shown in Figure 71.
2. Perform a click-and-drag to extend or reduce the column width until you can see all the data.
3. Release the mouse button.



fullLine	TRX	TTY	message
[2002/02/04]:	SU01	TTY19	Transaction SU01 started
[2002/02/04]:	SU01	TTY19	Transaction SU01 started
[2002/02/04]:	SE91	TTY24	Transaction SE91 started
[2002/02/04]:	SE37	TTY24	Transaction SE37 started
[2002/02/04]:			Logon Successful (Type=B)
[2002/02/04]:	SE38	TTY24	Transaction SE38 started
[2002/02/04]:	SE38	TTY24	Transaction SE38 started

Figure 71: Column resizing in Data Panel

## Related tasks

Creating the analysis report. See on page 65

## Changing column ordering

In order to allow for a clear arrange of the event field on the Data Panel, the auditor can reorder the columns.

1. Position the mouse on the field name in the Data Panel's heading line.
2. Perform a click-and-drag, dragging the field name to the new location in the event grid.
3. Release the mouse button.

## Opening a new Visualization Area

You can also use the selection made as the baseline for a new Visualization Area to focus on the data.

1. Perform a selection as described in section *Selecting events*, on page 39.
2. Perform a right-click with the mouse inside the selected area. This opens up the *Selection Menu* that is shown on Figure 72.
3. In this context menu select the *View as* option.
4. In the submenu select the desired visualization mode

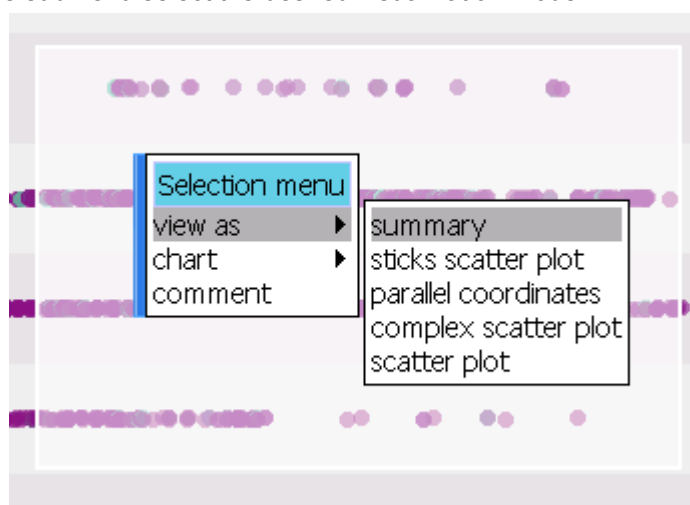


Figure 72: Opening new visualization on a selected area

The events comprised by the selected section will be shown on the new visualization. This could be very useful when you use multiple visualization modes to analyze the data from different perspectives.

If you do not select an area on the Analysis graph, the new visualization contains all events on the present time frame. This could be used either with the objective of preserving the original Analysis graph and perform the additional analysis in a copy of the current visualization.

### Related tasks

Selecting events. See on page 39

Creating templates. See on page 50

## Using charts

While working with events in the Analysis graph, you can choose to create a Chart to display a summary of the values for one attribute, using a Bar or Pie chart to analyze further the event distribution.

This can be done either on a selection of events, or on the whole range.

1. If you want to chart a selected range of events, first select the range of events you will chart and then perform a right click on the selection. This will open up the *Selection Menu*. Otherwise, if you want to create a chart on the whole range of events you can do a right-click on any area of the Analysis Graph that does not contain a selected range. This will open up the *Window Menu*.
2. On the context menu, select *Chart* submenu.
3. In the submenu choose the type of graph you want to create. The options available are *Bars chart* or *Pie chart*, as shown in Figure 73.
4. The chart appears on the Visualization area.
5. Once the chart is present on the screen, you can move it by using drag and drop.

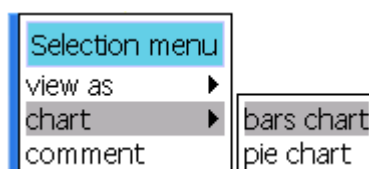


Figure 73: Selection menu used to open a chart

## Configuring chart settings

When you create a new chart, its drawing is based on the attribute selected on the *Color* configuration setting (located in the Settings Configuration Flap). The default attribute used for drawing the chart is the one selected on the *Color* option in the *Settings Configuration Flap*. If the *Color* option is not in use, the initial chart will be blank and you will be asked to select an attribute first, as shown on Figure 75. After the chart is created, however, you can change this attribute.

To change the chart attribute:

1. Perform a right-click on the chart object. This will show the context menu.
2. Select the *Attribute* option in *Chart menu*.
3. Select the desired attribute in the sublist. Only attributes present in the current query used for the analysis will be shown, as shown in Figure 74.

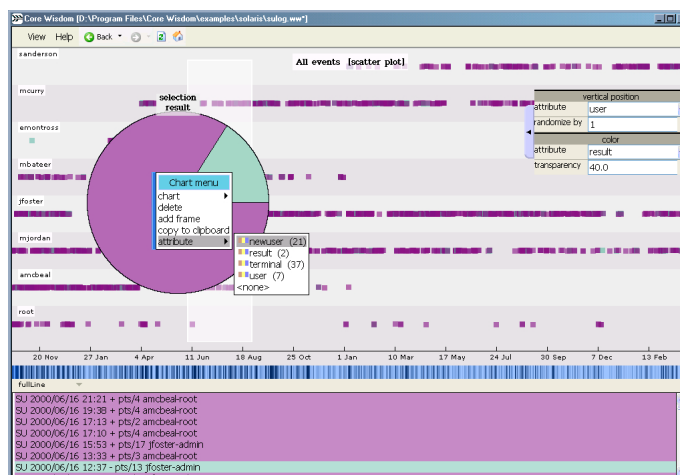


Figure 74: Changing chart settings

To show additional information on chart components:

You can hover with the mouse on each component (either sectors for Pie charts or bars in Bar charts) to display the information about how many events the component represents and what the percentage against the total amount of events is.

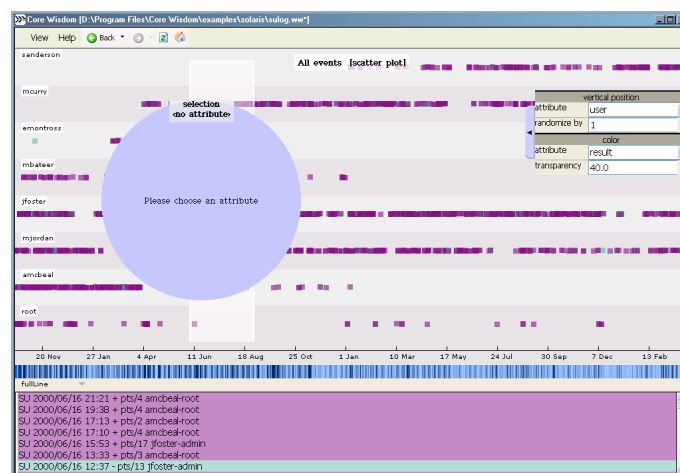
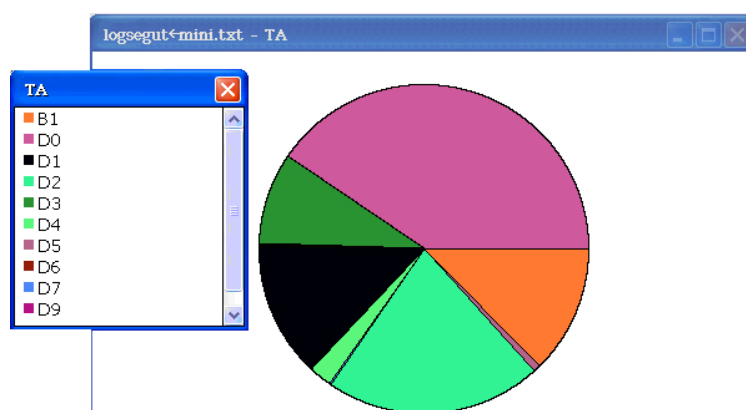


Figure 75: No attribute used to create a chart

To frame charts:

You can also add a frame for better displaying of the chart in the Analysis graph. To do this:

1. Right-click the chart object area. This will show the context menu for the chart.
2. Select the *Add frame* option in the *Chart menu*. The chart appears now in its own window as shown in Figure 76.



**Figure 76: Frame chart and Color Reference palette**

3. To make the picture clearer you can open the *Color* reference palette and maintain it in the same view. You do this by selecting the *Color* option in the *Reference* option of the View menu, as shown on Figure 77. This action causes the *Color* reference palette to pop up as shown previously in Figure 76.



**Figure 77: Opening the Color reference palette**

#### *Related tasks*

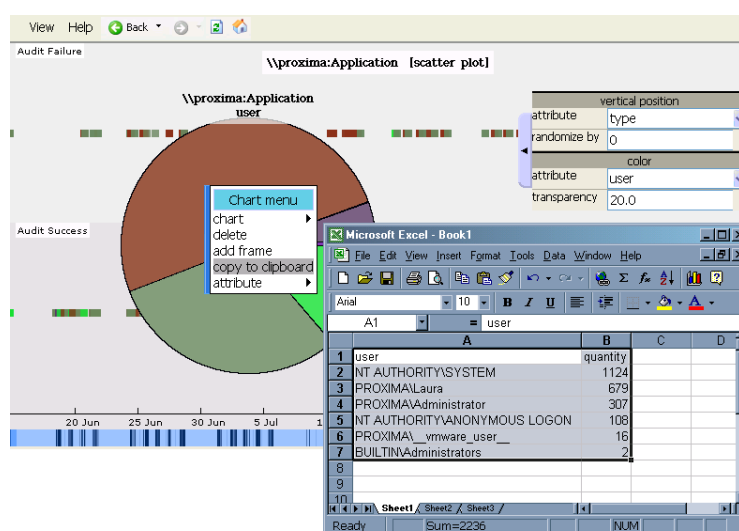
Selecting events. See on page 39

Creating the analysis report. See on page 65

### **Exporting chart data**

CORE Wisdom allows you to export the summary data used to create the charts. With this feature, you can manipulate the data with third party applications such as Microsoft Excel, thereby extending CORE Wisdom's charting and filtering features.

1. Create a pie or bars chart. Right-click on the chart object and select the *copy to clipboard* option from the context menu.
2. You can now paste the data table to any application such as Microsoft Excel, with the regular *Paste* command option found in Windows-based applications. See Figure 78 for an example showing the export of a data table to MS Excel.



**Figure 78: Exporting chart data to MS Excel**

### Related tasks

Selecting events. See on page 39

## Visually filtering views

There are two different options to visually filter the events shown on the Visualization Areas without removing them.

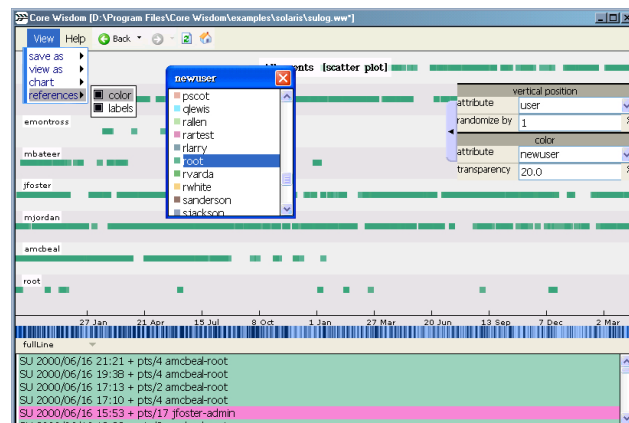
### Filtering by Color References

On Summary, Simple and Complex Scatter Plot visualization modes, you can use the option *References* → *Color* on the *View* menu to display only one category of events on screen. For example, if you work on a Scatter Plot graph depicting User Logins you can apply a graphic filter to show only those events that include login attempts for any user sitting on Terminal JKASEI. The filter will apply on the categories reflected by the attribute selected in *Color* configuration setting (located on Settings Configuration Flap) for the current Analysis Graph.

1. Determine which color is used by the event category you want to display on the analysis graph, hovering the mouse on an event of the same category color. This will reveal the category value content.
2. Left-click *View* on the Menu bar. This displays the *View* menu.
3. Select the *References* → *Color* option. A palette showing each color and category pops up on screen. The window title for the palette is the attribute name selected in the *Color* configuration setting (located on the Settings Configuration Flap).
4. Select the category you want to apply the filter on. In this example, the chosen category is the root user.



- The Analysis Graph will only show events within the same category (root user in this case).



**Figure 79: Filtering by Color References**

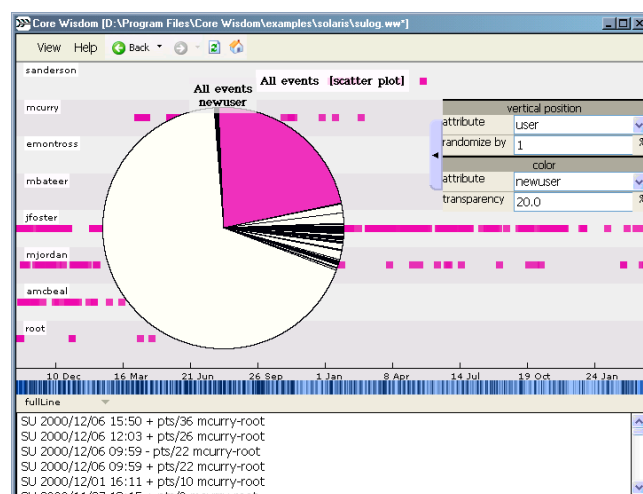
All other events are hidden but they are still shown on the Data Panel. To remove the filter by *Color References*:

- Re-selecting the category by left-clicking it will remove the filter and show all events again.
- If you close the Palette window the filter is removed and all events are shown.

### Filtering by Chart Element

You have another option for filtering events on the graph, by means of the use of a chart (Pie or Bars) to filter categories in the displayed events. You do this by selecting one element in the chart with a double-click on it (see section *Using charts* on page 45 for additional information)

- Left-click one of the sections in the chart (either a portion of the pie in Pie Charts or a bar in Bar Charts)
- The Analysis Graph will now only show events in such category as that one selected on the chart.
- Perform a new left-click on the chart section corresponding to the filtered category to remove it. This will cause all events to be shown.



**Figure 80: Filtering attribute category by chart sectors**

### Related tasks

Selecting events. See on page 39

Using charts. See on page 45

## Commenting events

You can assign a comment detailing your conclusions and findings. These comments will be shown each time you hover the mouse pointer over the commented events. Every comment you assign to the events will be shown on the Analysis Report for the current visualization. To comment a group of events:

1. Position the mouse on an area of the Analysis graph containing a selected range of events
2. Perform a right-click with the mouse inside the selected area. This opens up the Selection Menu.
3. In this context menu select *Comment*.
4. To show the comments, hover on the selected events. A yellow banner will appear containing the text with your comments.

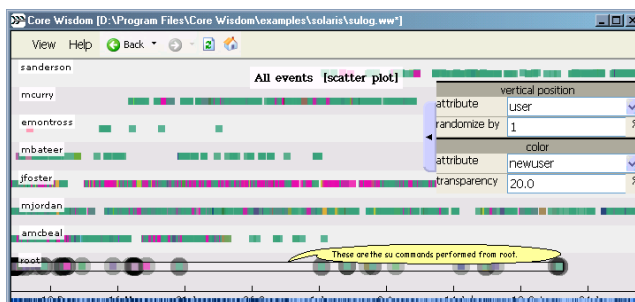


Figure 81: Showing comments

## Using comments to keep track of events

By commenting some events on the screen, you can mark a group of events that will be highlighted through different visualization modes. This is useful to track the behavior of the events from various perspectives as they vary with each Visualization mode.

### Related tasks

Opening a new Visualization Area. See on page 44

Creating the analysis report. See on page 65

## Creating templates

You can create a template to maintain your preferences and settings about the data displaying on the current Visualization Mode. The templates are a quick way to apply a predefined format to the data in order to obtain a meaningful view. Default queries open in their own default template, but it could also be used in any other view that contains the fields in the log required for the template.

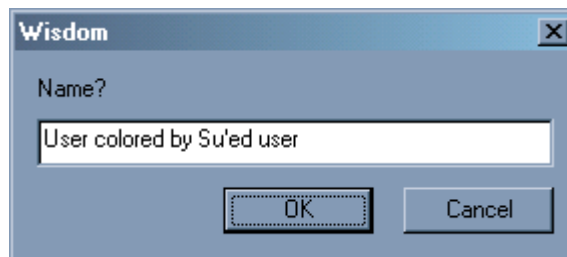
### To create a new Analysis Graph template

1. On the visualization mode selected on the screen configure the specific options for displaying the data on the Settings Configuration Flap. For additional detail on what the specific parameters of each visualization mode are, see section 3.2 *Specific procedures and settings* on page 52.



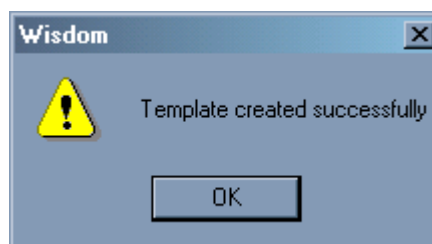
**Figure 82: Creating a Visualization Area template**

2. On the *View* Menu select the *Save as* → *Template* option.
3. Assign a new representative name to the template in the template name dialog box, shown in Figure 83.
4. Click the OK button.



**Figure 83: Visualization area Template name dialog box**

5. The message shown in Figure 84 indicates that the template was created successfully. Click OK.



**Figure 84: The template was created successfully**

**Note:** The newly created template can be applied in the initial Visualization Area selected from the Start-up window, the selected Repository should include the same fields that you used on the template's definition procedure: in our example, **User colored by Su'ed user**. You will not find listed on the context menu templates that use fields other than those present in the Template's definition.

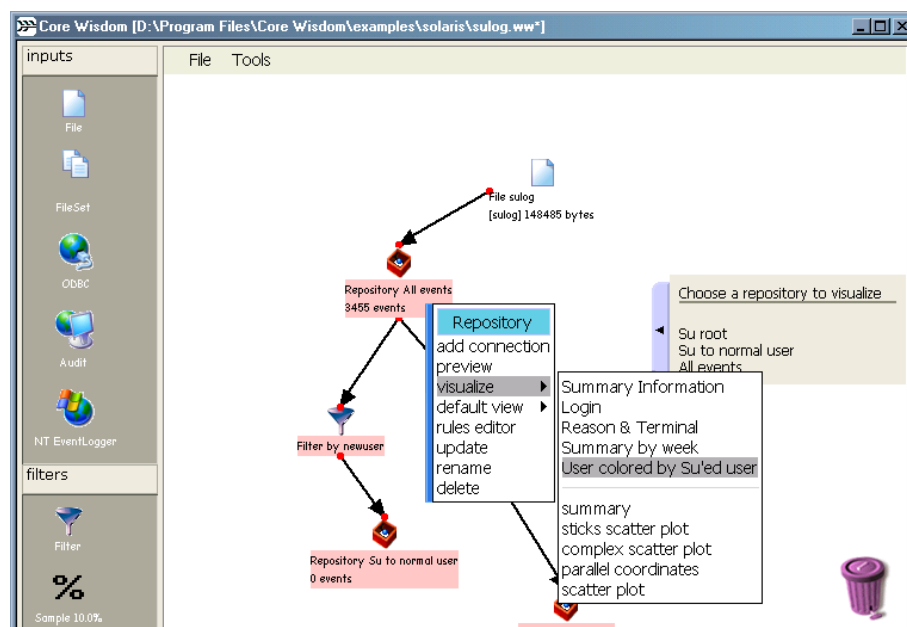


Figure 85: Selecting the new template

#### Related tasks

Selecting events. See on page 39

Opening a new Visualization Area. See on page 44

Using charts. See on page 45

Configuring chart settings. See on page 45

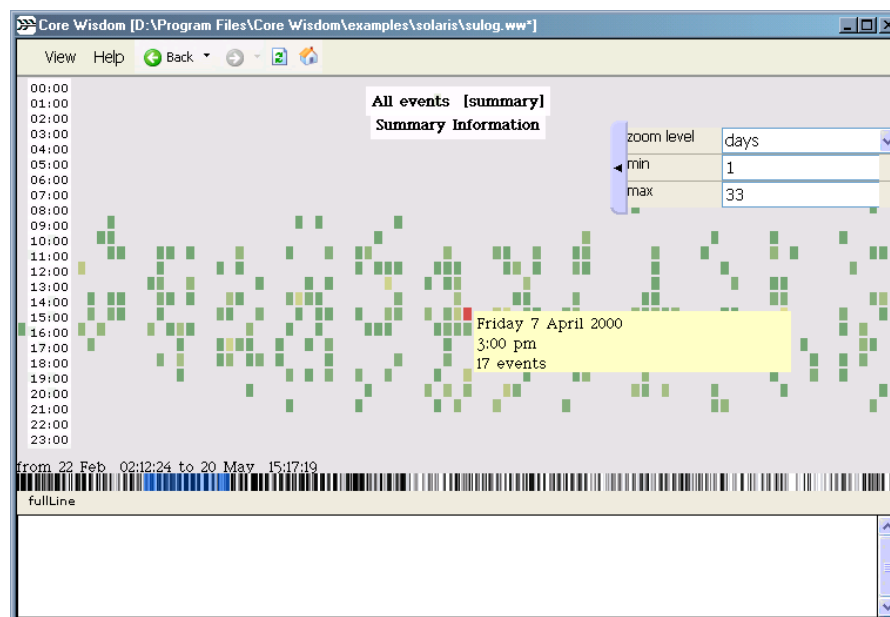
## 3.2 Specific procedures and settings

The following set of procedures describes the use of the particular configuration options available for the presentation of information for each of the four Visualization modes.

### 3.2.1 Using Summary view

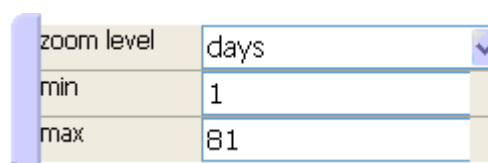
We can see in Figure 86 the initial Summary visualization for a Day Graph obtained from the entire data repository analyzed by the auditor. This is a Day Graph where each column of the grid represents the values for one day, and each row contains hourly values. The Data Timeframe displays the log interval, several months in this case; the first event happening on February 22nd and the last event was recorded on May 19th.

Each hour is shown as a box, colored in relation to the amount of events happening at the moment. In this case, you can see a Details Box showing more information while the auditor hovers the mouse on those events.



**Figure 86: Visualization mode for Summary graph**

There are two possible zoom levels that determine the time units in which the events are grouped on the screen. You can select the *Zoom Level* on the *Settings Configuration Flap*. The possible options are *days* and *weeks*.



**Figure 87: Drill down control for zoom level**

By changing the *Zoom Level* value to **Week** the representation changes to the visualization shown on Figure 88, where each column shows the aggregation of events for one week of the month, and each line is one day in the week.

The values of the Event Range (min-max) show the lowest and highest values represented by the amount of events occurring on the smallest time unit (minute, hour or day), depending on the zoom level chosen.

In this view you also maintain the whole picture by inspecting the Event Density view, where you are presented with the continuous representation for each day and you still keep in mind the succession of events for all the weeks comprised in the Visualization Area.

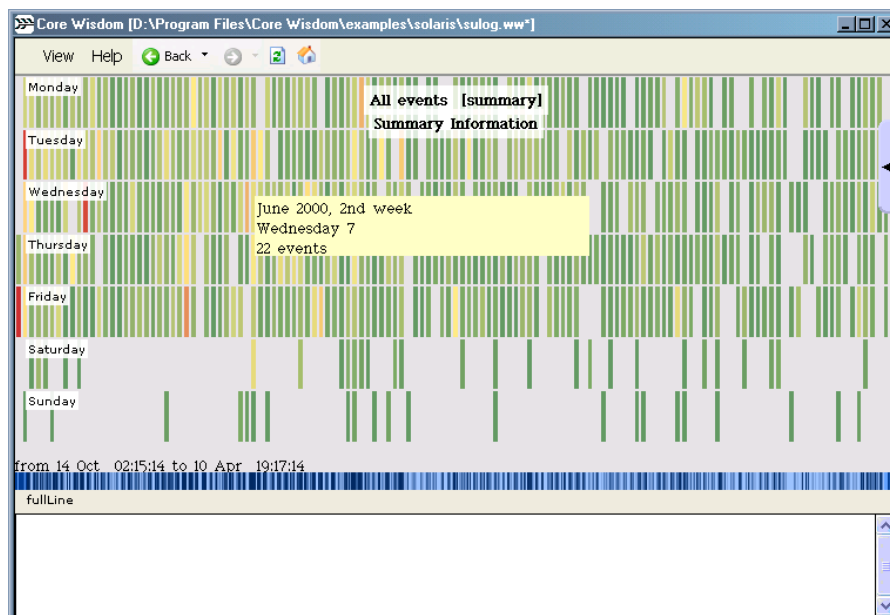


Figure 88: Zoom Level (Week) Graph

### 3.2.2 Using Scatter Plot view

The Scatter Plot view can provide visual answers to the analysis questions about the existence of relationships between pairs of log entities. Each of these entities in the Analysis Graph represents now a single event as an squared box, instead of the sum of all events in the time range as we had seen in Summary graphs. In the case of those relationships taking place, the auditor can explore their nature in a visual environment, to discover anomalies as variable values out of place or clustering patterns for occurrences of the events in the time frame that is being analyzed. Figure 89 shows a typical visualization for Scatter Plot graphs.



Figure 89: Visualization mode for Scatter Plot graph

### To select Y-axis value

The key advantage that this visualization mode features compared to Summary view, is the possibility of defining a value for the Y-axis. The X-axis always remains as the occurrence time of the events plotted on the Analysis Graph. Each element of the view, represented by a squared box, will now be a single event.

1. Display on the screen the Settings Configuration flap by performing a left-click on the control border of this element.
2. Expand the drill-down list in the *vertical position* (Y-axis) in order to show the available field values.
3. Select the desired field with a left-click on the list element, for example User Name as shown previously on Figure 89.
4. This will show every value for the User Name field on the *vertical position* (Y-axis).

### How to hide Y-axis references legend

You can hide or show the references shown on the Y-axis by using the checkbox present in the *references* → *labels* option located in the View menu.

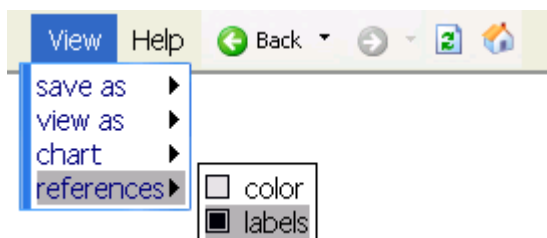
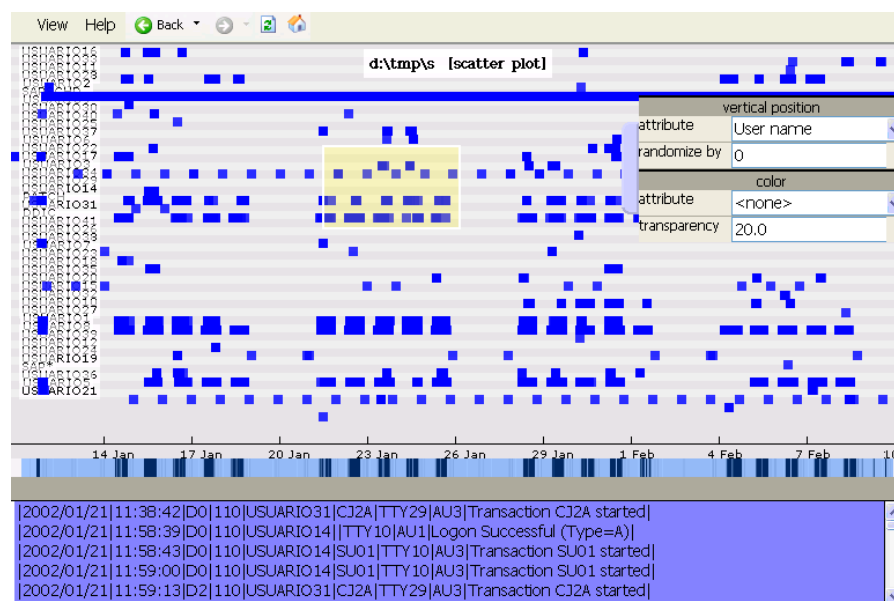


Figure 90: Hiding Y-axis references

### Selecting coloring options

Another useful configuration value is the option to color each event. With this feature you can analyze in the graph another dimension of the data, associating each value for a specified attribute of the events with a different color. This could be the case of user terminal, giving a quick glimpse to the auditor of the source login terminals that each user is working with. Any

change in the normal user's login pattern to their assigned terminal will be shown as an event with a different color on the Analysis graph. On Figure 91 you will see an Analysis Graph showing the selection of User Name as Y-axis.



**Figure 91: Default view with no Color by attribute selected**

To do this:

1. Display on the screen the Settings Configuration flap by performing a left-click on the control border.
2. Select an *attribute* name from the drill-down list containing the relevant log field values.
3. Select the desired field with a left-click on the list element, in this example the user terminal.
4. This will show each terminal with a different color on the Analysis Graph.



**Figure 92: Selecting attribute to color by**

### How to show the palette references

You can hide or show the palette references by using the checkbox present in the *References* → *Color* option located in the View menu.



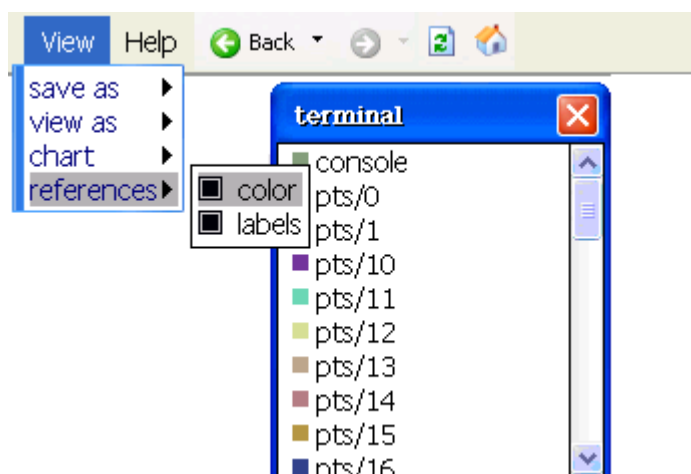


Figure 93: Showing Color references

### Selecting random value

An advanced configuration option present in Scatter Plot views is the opportunity to differentiate the data on screen. If the events cluster around very close time slots, then information about the amount of events occurring on almost the same time is lost to the view of the auditor. To further add the dimension of quantities of events to the Scatter Plot diagram you can use the *Randomize by* value with the purpose of add noise to the visualization. This will cause the events to separate in random intervals defined by the setting's value, creating a vertical dispersion on the events that would turn into visible clusters of activity. The results are shown in Figure 94. To do this:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Left-click on the default *Randomize by* value option for the initial view. This will position the text cursor on the text box.
3. Write in the text box the percentage of separation desired. Press enter for the value to take effect.
4. This will cause the diagram to be redrawn with the events now separated by the random interval. Higher values will create a greater dispersion. With 100% dispersion, the y-position is randomly chosen.



Figure 94: Randomizing event display

## Changing transparency

Another configuration setting available to make easier the visualization task on the events is the *Transparency* value, which can also be used to convey the idea of event clustering levels to the auditor. In this way, events with a higher clustering level will appear solid and more visible, meanwhile single events will have a transparency outlook. To do this:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Left-click on the default *Transparency* value option for the initial view. This will position the text cursor on the text box.
3. Write the percentage of desired transparency in the text box. Press enter for the value to take effect.
4. This will cause the diagram to be redrawn with lone event segments dimmer than clusters of activity. Higher values will generate a greater transparency and contrast.



Figure 95: Setting transparency value for event display

## 3.2.3 Using Complex Scatter plot view

This graph type adds three additional dimensions to the information represented by the events depicted in the Analysis graph. The auditor maintains in this Visualization mode all the configuration options available with Scatter Plot views (*Vertical Position* and *Color*), plus a series of new tools that offers more dimensions to enhance the analysis process. They are Border color, Size and Shape.

The selection of *vertical position* (Y-axis) and *Color* fill are still available, as in the Scatter Plot graph. See about these procedures on sections: *To select Y-axis value* on page 55, *Selecting coloring options* on page 55, *Selecting random value* on page 57 and *Changing transparency* above

## Changing border colors

In Complex Scatter plot you will be offered the additional option to select a different attribute to recolor the borders or the objects representing each event. In this way, events are categorized by assigning a different color to each of the attribute values. To do this:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.

2. Select *Attribute* in the *Border Color* configuration. This will show a drill-down list containing all field values present in the log.
3. Select the desired field with a left-click on the list element, in this example the results for the *su* command execution.
4. This will show the command's outcome with a different border color on the Analysis Graph.



Figure 96: Setting border color

### Changing transparency on border color

You can also change the transparency of the border line, to detect the partial overlapping of multiple events in the Analysis Graph. The procedure to do this is the following:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Left-click on the default *Transparency* value option located in the *Border Color* configuration from the initial view or template. This will position the text cursor on the text box.
3. Write the percentage of desired transparency in the text box. Press enter for the value to take effect.

This will cause the diagram to be redrawn with lone event segments dimmer than clusters of activity represented by the overlapping of borders. Higher values will generate a greater transparency and contrast.

### Changing width on border line

You can also change the border-line width, to highlight the relation between event fill and event border colors in the Analysis graph. The procedure to do this is the following:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Left-click on the default *Width* value option in the *Border Color* configuration from the initial view or template. This will position the text cursor on the text box. See Figure 96.
3. Write the new value for the width in the text box. Press enter for the value to take effect.

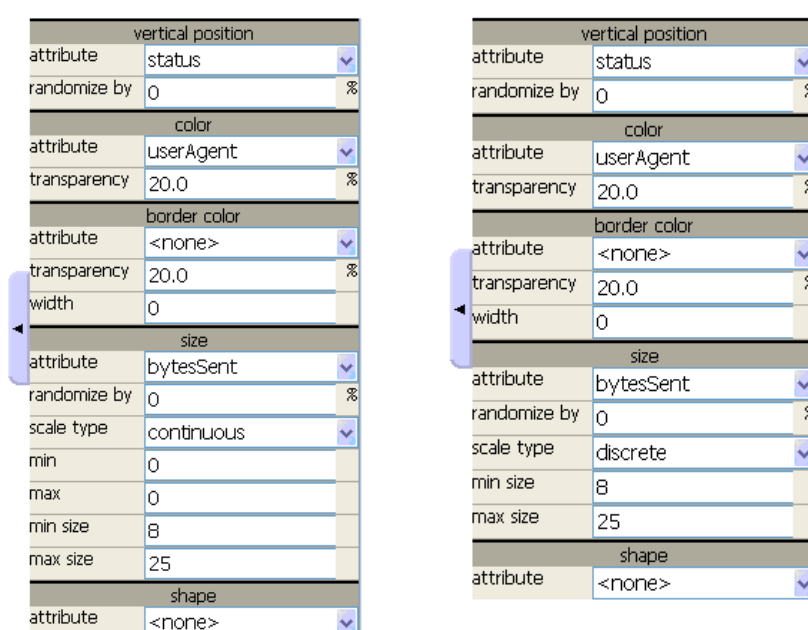
This will cause the diagram to be redrawn. Higher values will generate thicker borders, while lower values will show thinner ones.

## Setting size

You can choose to visually differentiate attribute values for a specific field by changing their size ratio. This option presents different behavior given that a continuous or discrete attribute is selected for the setting (see discussion on attribute types on page 8).

For continuous attributes:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Select *Attribute* in the *Size* configuration. This will show a drill-down list containing all field values present in the log.
3. Select the desired field with a left-click on a **Continuous** attribute. The configuration options changes, as shown on Figure 97.



vertical position	
attribute	status
randomize by	0 %
color	
attribute	userAgent
transparency	20.0 %
border color	
attribute	<none>
transparency	20.0 %
width	0
size	
attribute	bytesSent
randomize by	0 %
scale type	continuous
min	0
max	0
min size	8
max size	25
shape	
attribute	<none>

**Figure 97: Size settings for continuous attributes**

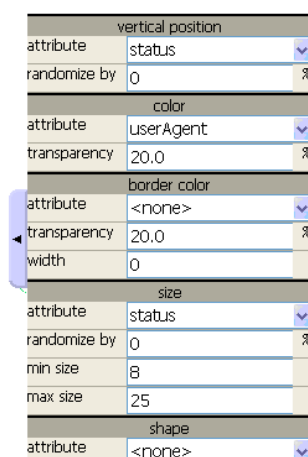
4. Fill in the *min size* option text box with the value in pixels that will take the smallest attribute value.
5. Fill in the *max size* option text box with the value in pixels that will take the higher attribute value.

**Note:** This will cause each event to display with a different size, proportional to the attribute value on the Analysis Graph, the sizes between the min and values will be interpolated by WISDOM.

6. Two different *scale type* can be selected.
  - a. Continuous scale type: Two additional settings are presented on the *Settings Configuration flap*, *min* and *max*. They limit the values that will be shown, filtering out all those values smaller than the *min* and greater than the *max* settings.
  - b. Discrete scale type: Presents the same behavior and settings that when you select discrete attributes, see section For discrete attributes: on page 61.

For discrete attributes:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Select *Attribute* in the *Size* configuration. This will show a drill-down list containing all field values present in the log.
3. Select the desired field with a left-click on the **Discrete** attribute. The configuration options changes, as shown on Figure 97.



vertical position	
attribute	status
randomize by	0 %
color	
attribute	userAgent
transparency	20.0 %
border color	
attribute	<none>
transparency	20.0 %
width	0
size	
attribute	status
randomize by	0 %
min size	8
max size	25
shape	
attribute	<none>

**Figure 98: Size settings for continuous attributes**

4. Fill in the *min size* option text box with the value in pixels that will take the smallest attribute value.
5. Fill in the *max size* option text box with the value in pixels that will take the higher attribute value.

This will cause each event to display with a different size, proportional to the attribute value on the Analysis Graph, the sizes between the min and values will be interpolated by WISDOM.

### Changing default size value

This option is only available when **no attribute** has been selected in the *Attribute* option. The Default size value is eight pixels. Introducing a new value in the *Default* option for the Size configuration sector will change the size for all events showing on the Analysis Graph.

### Changing shape settings

You can change the shape for each attribute value for a specific field to differentiate and add a new dimension to the information represented by the Analysis Graph. In this fashion, you can have a different shape for each different value of the attribute you have selected to analyze. To do this:

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Select *Attribute* in the *Shape* configuration. This will show a drill-down list containing all field values present in the log.
3. Select the desired field with a left-click on the list element.

This will represent each login terminal with a different shape on the Analysis Graph.



Figure 99: Changing shape settings in Complex scatter plot

### 3.2.4 Using Parallel coordinates views

This visualization mode is useful to maintain a general view about the relationship between multiple entities (user names, login terminals, transaction performed and their status) at the same time. Instead of getting the idea on quantities and distribution through time, as in Summary and Simple views, by working with the Parallel Coordinates visualization the auditor can observe the correspondence between diverse values for each variable.

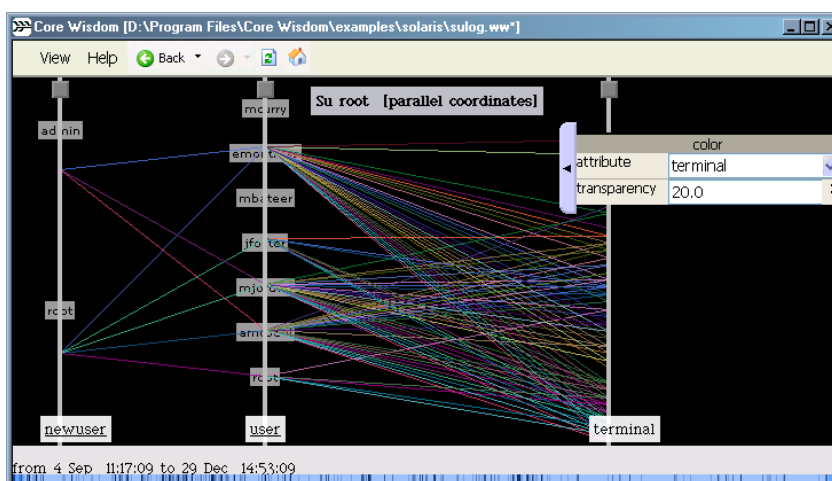


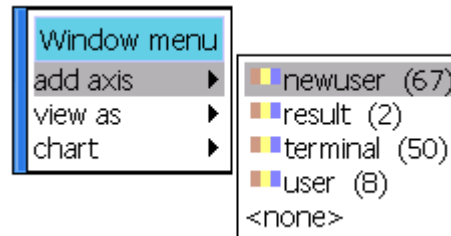
Figure 100: Sample of parallel coordinates graph

#### Handling multiple y-axes

The default visualization produced by the initial query contains normally two or three y-axes depending on the selection. You can add additional axes, remove them or you also can swap them to further customize the analysis environment.

To add new axes:

1. Right-click on any non-selected portion of the Visualization Area to display the *Window menu*.
2. Select the *add axis* option from the context menu.
3. Select the desired field with a left-click on the list element, for example the **result** field, as shown on Figure 101.
4. This will show all values for the User Name field on the new Y-axis
5. Keep selecting other axis until the Analysis Graph presents all the information on screen.



**Figure 101: Adding axes in Parallel Coordinates graph**

To remove existing axes:

1. Perform a right-click on the y-axis that you want to delete
2. Select the *delete* option in the context menu to remove the axis.
3. The visualization graph will be redrawn without the axis.



**Figure 102: Delete option to remove axis on Parallel coordinates graph**

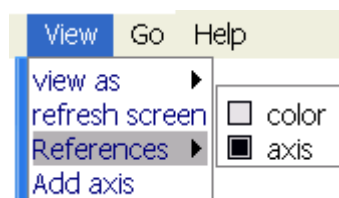
To swap axes location:

You can change the order used to display the axis on the Parallel Coordinates graph. To do this:

1. Position the mouse on the axis and do a click-and-drag to the new position.
2. The visualization mode will be redrawn with the axis on the new position.
3. The event rails will be redrawn to correlate the closest-axis attributes.

### How to hide Y-axis references legend

You can hide or show the references shown on the Y-axis by using the checkbox present in the *References* → *Axis* option located in the View menu.



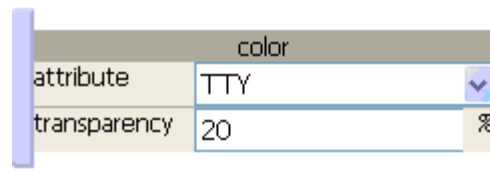
**Figure 103: Hiding axes references**

### Selecting coloring options

By coloring the lines you can also see categories in the data relationships.

1. Display on the screen the *Settings Configuration flap* by performing a left-click on the control border.
2. Select *Attribute* in the *Color* configuration. This will show a drill-down list containing all field values present in the log.

3. Select the desired field with a left-click on the list element, in this example User Terminal.
4. This will display each event rail related to the same terminal with a different color on the Analysis Graph.

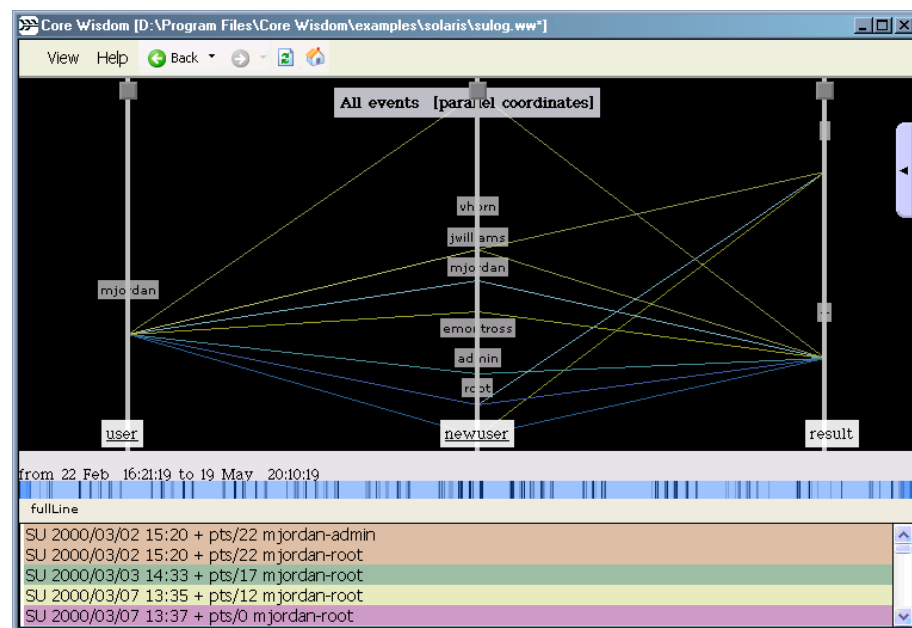


**Figure 104: Select color by attributes on Parallel Coordinates graph**

### Highlighting an event rail

Sometimes the sheer amount of events for analysis turns the graph in an overpopulated image. To get a clear picture of some interesting relationship between the field values you can highlight the relationship path (event rail) that crosses the entire diagram, through each axis. To do this:

1. Locate the label corresponding to the rail in the corresponding y-axis.
2. Perform a left-click onto the value location on the axis. This will highlight all lines going from the value in the selected axis to the immediate axes, and from them on.
3. To toggle off the highlight left-click once more on the attribute label.



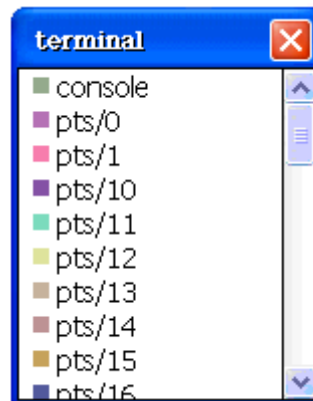
**Figure 105: Highlighting an event rail**



## 4. Creating the analysis report

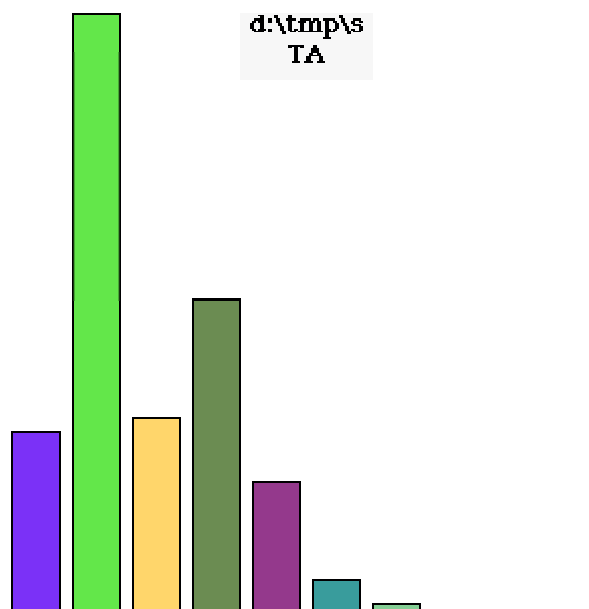
You have the option of create a report with all significant data from the current visualization. The report is the output of the whole analysis process. Sections on the report include:

1. Visualization graph: Includes the Analysis graph, as also the Time Frame Control.
2. Axis information (x-axis and y-axis) and reference table palette for the values configured in the Analysis Graph. See Figure 106 for an example showing the TTY attribute reference palette.



**Figure 106: Reference table palette**

3. All active charts, as shown on Figure 107.



**Figure 107: Sample chart shown in Report**

4. All comments on the graph and the raw event records from the logs as they are shown on the Data Panel, as shown next.

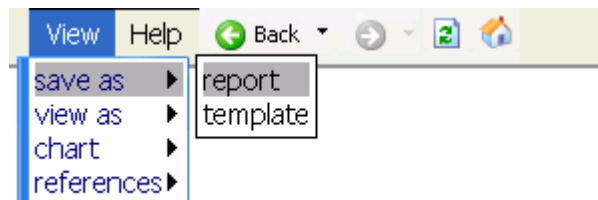
These are some events of interest

**message**

Logon Failed (Reason = 1, Type = A)
Logon Failed (Reason = 1, Type = A)
Logon Failed (Reason = 1, Type = A)
Logon Successful (Type=A)
Transaction ZV12 started
User Logoff
Logon Successful (Type=A)
Transaction SPRO started

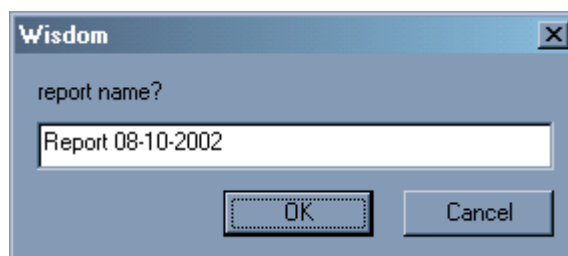
**To create a report:**

1. Select the Visualization mode which will be exported to the report (Summary, Scatter Plot, Complex Scatter Plot or Parallel Coordinates).
2. If needed, create graphs to display data in Pie or Bar format.  
See section Using charts on page 45.
3. Ensure that the Data Panel has the appropriate format, with all required fields included on it.  
See sections *Selecting events* on page 39 and *Changing Data Panel display options* on page 43.
4. Comment every event or range of events you considerate relevant on the Analysis graph.  
See sections *Selecting events* on page 39 and *Commenting events* on page 50.
5. On the *File* menu, select the *Save as* option. In the *Save as* submenu, select *Report*, as shown on Figure 108.



**Figure 108: Saving Visualization mode information as Report**

6. Assign a name in order to identify the report later. Click OK, as shown on Figure 109.



**Figure 109: Report name dialog box**

7. The Report will open in the default Internet browser (this should be Microsoft Internet Explorer 6.x or newer)
8. You can save it to review it later, or print it with the regular procedures to do this on the browser application.

**Related tasks**



Using comments to keep track of events. See on page 50  
Commenting events. See on page 50  
Using charts. See on page 45

# Index of Figures

Figure 1: Analysis life-cycle in WISDOM	6
Figure 2: Graphical representation for visual analysis	7
Figure 3: Critical user login pattern – Graphical visualization	7
Figure 4: Attribute types identifiers	8
Figure 5: Preparing to install	9
Figure 6: Welcome to the install wizard	9
Figure 7: Choose destination location	10
Figure 8: Setup status	10
Figure 9: Wizard Complete	10
Figure 10: Add/Remove programs	11
Figure 11: Install Wizard options	11
Figure 12: Confirm Uninstall	11
Figure 13: Setup status information	12
Figure 14: Maintenance complete	12
Figure 15: CORE Wisdom Start-up window	13
Figure 16: Connectors	14
Figure 17: Choose single-file input	15
Figure 18: Locate single-file log	15
Figure 19: File selected icon	15
Figure 20: Sample log preview	16
Figure 21: File path and name beginning for log set	16
Figure 22: Setting the event interval	16
Figure 23: Fileset selected icon	17
Figure 24: Parameters for the ODBC connector	17
Figure 25: Enter query	17
Figure 26: Enter connection credentials	18
Figure 27: NT Event logger context menu	18
Figure 28: Selected log NT Event icon	18
Figure 29: Edit low-level parsing rules	19
Figure 30: Rules Generator for low-level parsing	19
Figure 31: Assigning attribute type to low-level rules	20
Figure 32: Rename the rule entry	20
Figure 33: Edit Application-specific parsing rules	21
Figure 34: Generate application-level parsing rules	21
Figure 35: Enter pattern name	22
Figure 36: Assign a name to the new category	22
Figure 37: Category context menu	23
Figure 38: Adding attribute types	23
Figure 39: Enter attribute's name	23
Figure 40: Select attribute type	23
Figure 41: Excluding bracket chars from the attribute's contents	24
Figure 42: Select the field name	24
Figure 43: Selecting the field value	25
Figure 44: Filter applied – Repository was updated	26
Figure 45: Change sampling rate	26
Figure 46: Sampled logs	27
Figure 47: Log table for the selected repository	27
Figure 48: Enter repository new name	28
Figure 49: Selecting the default view for a repository	29
Figure 50: Select the Visualization mode or template	29
Figure 51: Select Workspace file path	30
Figure 52: Warning: Workspace definition was not saved	30
Figure 53: Analysis process – life cycle	32

Figure 54: Visualization Area schema for all Visualization Modes	33
Figure 55: Complete menu bar	34
Figure 56: Summary graph	35
Figure 57: Scatter plot graph	36
Figure 58: Complex Scatter plot	36
Figure 59: Parallel coordinates	37
Figure 60: Window Menu	38
Figure 61: Selection Menu	38
Figure 62: Chart Menu	39
Figure 63: Selecting events in Parallel Coordinates visualization	39
Figure 64: Selecting events in Summary graphs	40
Figure 65: Exporting Data Panel entries	41
Figure 66: Slider Controls resizing analysis interval	41
Figure 67: Analysis graph before zoom (four weeks interval)	42
Figure 68: Analysis graph after zoom (one week interval)	42
Figure 69: Analysis graph after moving forward in time (last week)	43
Figure 70: Adding columns on Data Panel	43
Figure 71: Column resizing in Data Panel	44
Figure 72: Opening new visualization on a selected area	44
Figure 73: Selection menu used to open a chart	45
Figure 74: Changing chart settings	46
Figure 75: No attribute used to create a chart	46
Figure 76: Frame chart and Color Reference palette	47
Figure 77: Opening the Color reference palette	47
Figure 78: Exporting chart data to MS Excel	48
Figure 79: Filtering by Color References	49
Figure 80: Filtering attribute category by chart sectors	49
Figure 81: Showing comments	50
Figure 82: Creating a Visualization Area template	51
Figure 83: Visualization area Template name dialog box	51
Figure 84: The template was created successfully	51
Figure 85: Selecting the new template	52
Figure 86: Visualization mode for Summary graph	53
Figure 87: Drill down control for zoom level	53
Figure 88: Zoom Level (Week) Graph	54
Figure 89: Visualization mode for Scatter Plot graph	55
Figure 90: Hiding Y-axis references	55
Figure 91: Default view with no Color by attribute selected	56
Figure 92: Selecting attribute to color by	56
Figure 93: Showing Color references	57
Figure 94: Randomizing event display	57
Figure 95: Setting transparency value for event display	58
Figure 96: Setting border color	59
Figure 97: Size settings for continuous attributes	60
Figure 98: Size settings for continuous attributes	61
Figure 99: Changing shape settings in Complex scatter plot	62
Figure 100: Sample of parallel coordinates graph	62
Figure 101: Adding axes in Parallel Coordinates graph	63
Figure 102: Delete option to remove axis on Parallel coordinates graph	63
Figure 103: Hiding axes references	63
Figure 104: Select color by attributes on Parallel Coordinates graph	64
Figure 105: Highlighting an event rail	64
Figure 106: Reference table palette	65
Figure 107: Sample chart shown in Report	65
Figure 108: Saving Visualization mode information as Report	66
Figure 109: Report name dialog box	66



# Alphabetical Index

## A

**Add/remove attribute menu** · 39  
 advantage · 5  
 analysis graph · 48  
 Analysis Graph · 34, 38, 41, 42, 45, 48, 49,  
 50, 56, 59, 60, 61, 62, 64, 65  
 anomalous behavior · 5  
 anomalous events detection · 38  
 attribute label · 64  
 Auditing tasks · 5

## B

Bar Charts · 49  
 border color · 58, 59  
 Browsing Panel · 34

## C

Chart Menu · 38, 39  
 charts · 5, 38, 41, 45, 46, 50, 52, 65, 67  
 Color References · 48, 49, 56  
 context menu · 46, 52  
 Context Menu · 38

## D

Data Panel · 34, 38, 39, 40, 41, 43, 44, 49,  
 65, 66  
*Data Time-frame display* · 34

## E

*Event Density view* · 34, 41, 54  
 event rail · 39, 64  
 example · 6, 7, 39, 48, 52, 55, 56, 59, 63,  
 64

## F

filter · 35, 48, 49

## I

Information Visualization · 5

## M

menu bar · 33  
 Menu bar · 33, 48

## P

Parallel Coordinates graph · 37, 39  
 patterns · 5, 7, 31, 32, 35, 37, 54  
 Pie Charts · 49  
 procedure · 41, 42, 52, 59

## Q

query · 31, 32, 33, 41, 45, 62

## R

random value · 57  
 Random value · 57  
 raw events · 40  
 reports · 5

## S

Scattered Plot graph · 58  
**Selection Menu** · 38, 44, 45, 50  
 Settings Configuration Flap · 34, 45, 48, 50,  
 53  
 shape settings · 61  
*Slider Controls* · 34, 41  
 Start-up menu · 31, 32  
 Summary graph · 35, 40, 53, 54  
 System Security Log · 6, 52

## T

Time Frame Control · 34, 41  
 title · 34, 48  
 Title · 34  
 transparency · 58, 59

## V

Vertical References · 55, 63  
 Visualization Area · 31, 32, 33, 34, 38, 41,  
 44, 50, 51, 52, 54  
 visualization mode · 35, 36, 39, 44, 50, 55,  
 58, 62  
 Visualization mode · 34, 38, 50, 52, 53



W

Window Menu · 38, 45, 66  
WISDOM for SAP · 5, 6, 8, 13, 15, 32, 34  
workspace · 31, 38

y-axis · 35, 37, 64

Z

zoom level · 53

Y

y-axes · 37, 39, 62