IPSWITCH

WhatsUp Event Rover v10.x User Guide

CHAPTER 1

WhatsUp Event Rover User Guide

WhatsUp Event Rover Menus

Opening Log Files

Filtering Logs

Grouping and Sorting Event Records

Reporting On and Exporting Event Records

CHAPTER 1

WhatsUp Event Rover User Guide

In This Chapter

WhatsUp Event Rover Overview and User Interface

Overview

You can use Ipswitch's WhatsUp Event Rover to view, sort, and report on event logs. Data is loaded into trees (field groupings) whose structure you control. Different field groupings are summoned with a single mouse click, allowing the same records to be shuffled into views most relevant for the type of information you need. Hands-free sorting of log records eliminates the need for most manual filtering. Finally, to minimize potential harm to active event log stores on computers, WhatsUp Event Rover creates a backup copy of your active event log files before engaging in forensics or routine log review. You can maintain these backup copies in WhatsUp Event Rover's event logs repository, which, by default, is compressed to maximize storage disk space.

Key Features

The ability to review data from active Windows event log (EVT and EVTX) files, regardless of host operating system.

The ability to review data from previously saved event log (EVT and EVTX) files, regardless of host operating system.

The ability to review data from Event Archiver zip-compressed event log (EVT and EVTX) files, regardless of host operating system.

Event log data is ordered into user-customizable trees of field groupings.

Event log data can be dynamically reordered into different trees of field groupings.

Summary information (log size, number of events, number of events of a specific type, user accounts found) is presented to the administrator when a log is first opened.

Related data can be exported to comma-delimited text.

Grouped log data can be exported to an HTML report, and comments explaining the data contained within the report may be added.

Log data may be filtered at load using an absolute or relative date range, or by Event ID.

Other event log fields can be filtered after load, including description-based filters on related data.

The ability to save frequently used filters to a local database.

Common event identifier numbers can be mapped to friendly descriptions explaining their meaning. Most security log identifiers are pre-mapped for the administrator.

Multi-event incident criteria can be defined by the administrator (e.g. more than 3 errors from the same source in less than a minute), and then a loaded log can be scanned for one or more incidents.

NTFS compression of WhatsUp Event Rover's local event logs database minimizes storage requirements for backup copies of event logs.

Local caching of saved event log information speeds future reviewing and allows for offsite review of saved event logs.

Administrators can research event identifiers at eventlogs.com, Ipswitch Software's event logs resource site, from directly within the program.

The WhatsUp Event Rover interface has three components:

WhatsUp Event Rover Menu

Each of the eight WhatsUp Event Rover menus has a different set of commands to help you manage and work with the information inside your event logs. In order to find out more about each menu, click the menu name below:

ERv10 Using the File Menu (on page 18)

ERv10 Using the Edit Menu (on page 19)

ERv10 Using the View Menu (on page 19)

ERv10 Using the Options Menu (on page 19)

ERv10 Using the Field Groupings Menu (on page 20)

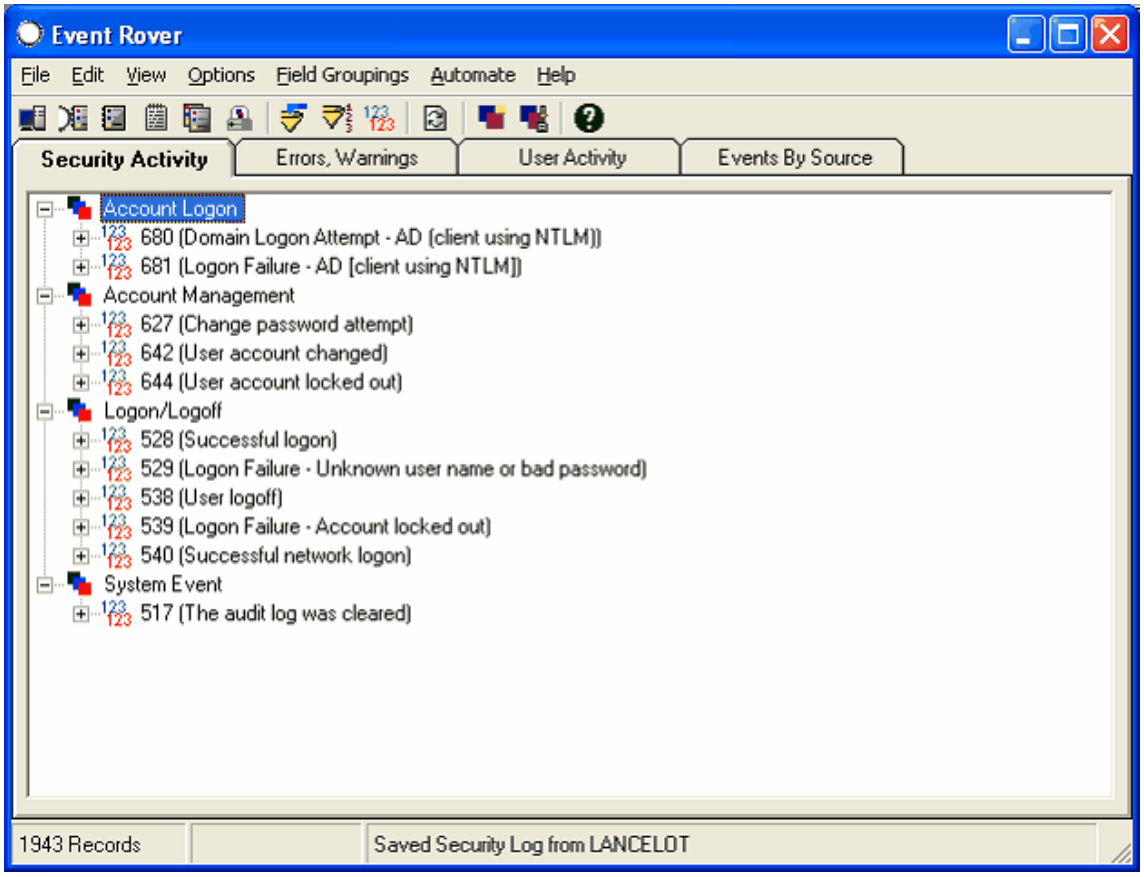
ERv10 Using the Incidents Menu (on page 20)

ERv10 Using the Help Menu (on page 21)

WhatsUp Event Rover Toolbar

The toolbar serves as a quick access mechanism to many of the commands present in most of the WhatsUp Event Rover menus. If you hover over any toolbar button, descriptive text appears, indicating what menu option the button controls.

Log Viewing Tabs



WhatsUp Event Rover's Log Viewing tabs allow you to quickly sort event log data into different field groupings/trees. For instance, an administrator might want to view log data by category and then by event identifier when looking at a security log, but then view system log data by type of event, then source name. Click different tabs in WhatsUp Event Rover to resort and reorder log data into the new field grouping. You can display up to 5 Log Viewing tabs at any one time, but you can define more than 5 field groupings and turn on/off different field groupings as needed. Field groupings can be created and managed from the Field Groupings menu.

At the bottom of any branch of the field groupings tree are related event log records, for example, records that have common fields. Double-click on the bottom of the branch to load the Records Listing Dialog, where you can view related events in a list, export them, and filter them by information in the description field.

System Requirements and Recommendations

WhatsUp Event Rover is designed to run on the following operating systems:

- Microsoft Windows XP
- Microsoft Windows 2003 Server
- Microsoft Windows Vista
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Microsoft Windows 7

For full functionality, install Microsoft's Internet Explorer version 5.0 or later on the machine running WhatsUp Event Rover.

The recommended hardware required to run WhatsUp Event Rover is:

- Dual-core 2GHz or faster
- 2 GB RAM
- 4 GB available hard disk space recommended for saved event log file storage.

Note: Disk space requirements are variable depending on how many backed up event log files you choose to retain inside WhatsUp Event Rover's event log repository. For this reason, it is recommended that you install WhatsUp Event Rover to the largest partition available on a server or workstation.

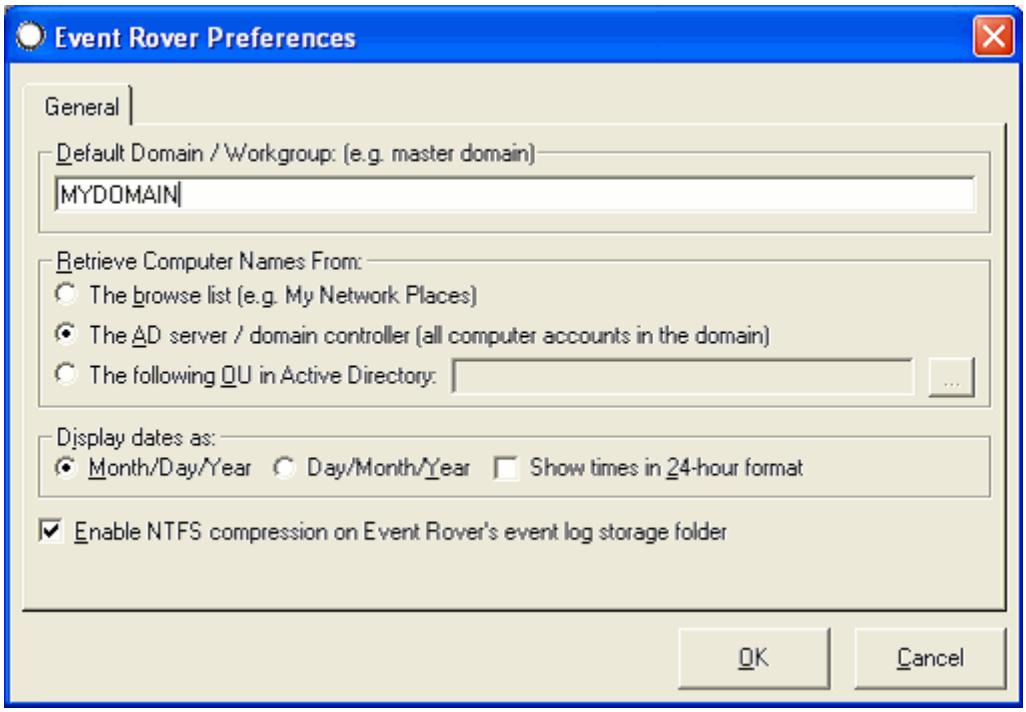
Note: The faster the processor, the quicker the loading and dynamic regrouping of log file data.

To backup active event logs for review in a domain, workgroup, or organizational unit, the user running WhatsUp Event Rover should have local administrative rights on each system and domain administrative rights on domain controllers (AD servers). For proper log conversion and presentation of data, the user running WhatsUp Event Rover should have local administrator rights on the machine where a previously saved event log file originated, if possible.

Before You Begin

1. Install WhatsUp Event Rover to the partition on your hard disk with the most storage space. You may want to retain tens or hundreds of backed up event log files in WhatsUp Event Rover's event log repository, so adequate disk space must be available.

2 Determine which domain(s), workgroup, or organizational units that contain the computers whose logs you plan to backup and review with WhatsUp Event Rover. When running WhatsUp Event Rover for the first time, supply the master domain or workgroup when prompted, and select an appropriate method for retrieving computer accounts.

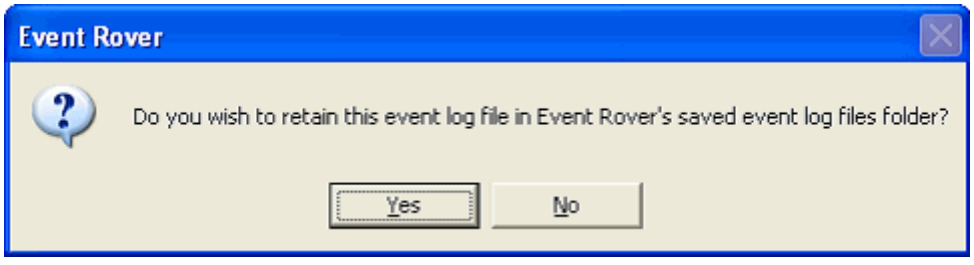


Other Recommendations and Information

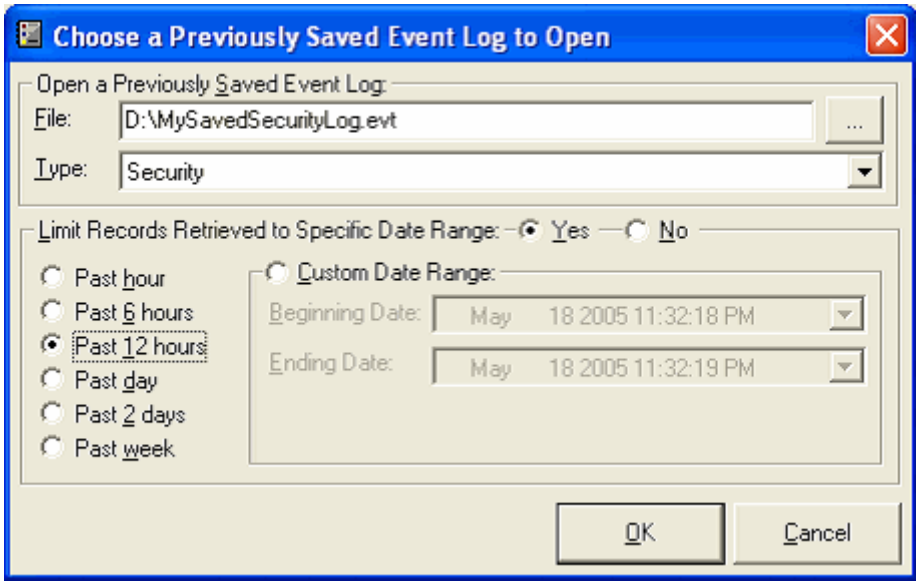
WhatsUp Event Rover works best in a well-connected LAN environment (e.g. 10 Mbit or 100 Mbit Ethernet). Use of WhatsUp Event Rover to backup and review log files across WAN links is not recommended. Rather, in such a scenario, install WhatsUp Event Rover locally on the system at the remote end of the WAN link, and then use remote desktop software (e.g. Terminal Services, VNC, etc) to run WhatsUp Event Rover and view log data.

When you attempt to open an active computer's event log file with WhatsUp Event Rover, WhatsUp Event Rover always creates a backup copy of the active log, without clearing the active log, and transfers that backup copy to your machine running WhatsUp Event Rover. This allows you to review event log information quickly without changing any aspect of the active log file on the remote machine.

To retain an event log file you recently backed up from a system's active event log, answer "Yes" when WhatsUp Event Rover asks "Do you want to retain this event log file in WhatsUp Event Rover's saved event log files folder?"



When opening large event log files (e.g. EVT files containing more than 75,000 records), such as security logs from domain controllers, strongly consider applying a date range filter or an Event ID filter. Restricting log records with a date range or Event ID range greatly reduces the number of events that WhatsUp Event Rover must load, group, and sort. This speeds up WhatsUp Event Rover's operation when a log viewing tab is clicked to present the log data in a new grouping.

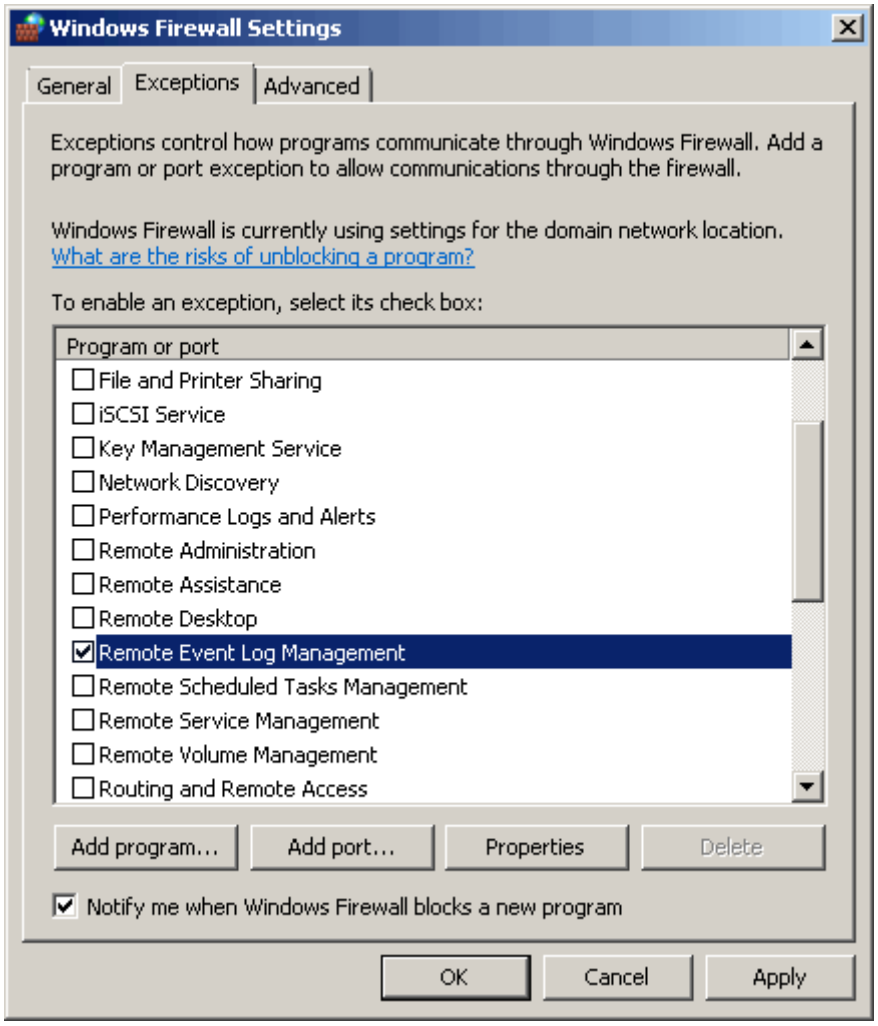


Windows Vista, Windows Server 2008, and Windows 7 Requirements/Recommendations

WhatsUp Event Rover can open and review EVTX files saved from Windows Vista, Windows Server 2008, Windows Server 2012, and Windows 7 operating systems when installed on legacy operating systems, such as Microsoft Windows 2000, XP, or 2003. In addition, WhatsUp Event Rover can review legacy EVT files when installed on Windows Vista, Windows Server 2008, Windows Server 2012, and Windows 7. The forward and reverse compatibility between these two log formats is powered by Ipswitch's LogRefiner technology. As has been the case in the past, if you can remotely view and manage your event logs with the Microsoft Event Viewer, our software should have no issues operating on them.

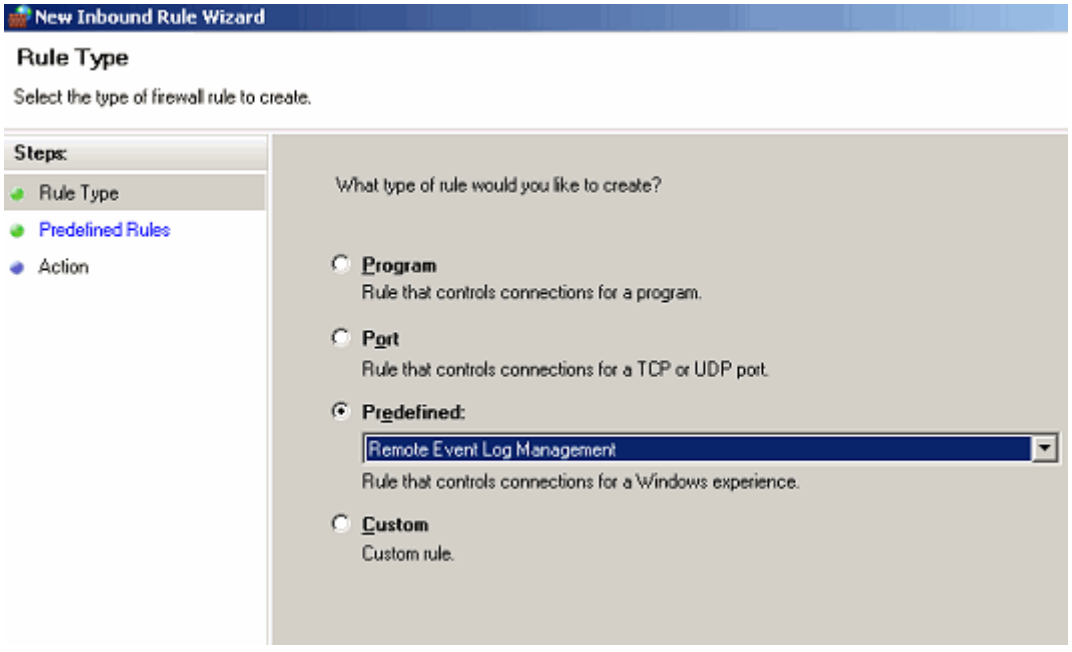
If you are reviewing EVTX log files from newer operating systems with WhatsUp Event Rover installed on Windows 2000, Windows XP, or Windows 2003, make sure the Windows Firewall settings on the target systems support Remote Administration access and Remote Registry access to view the logs properly.

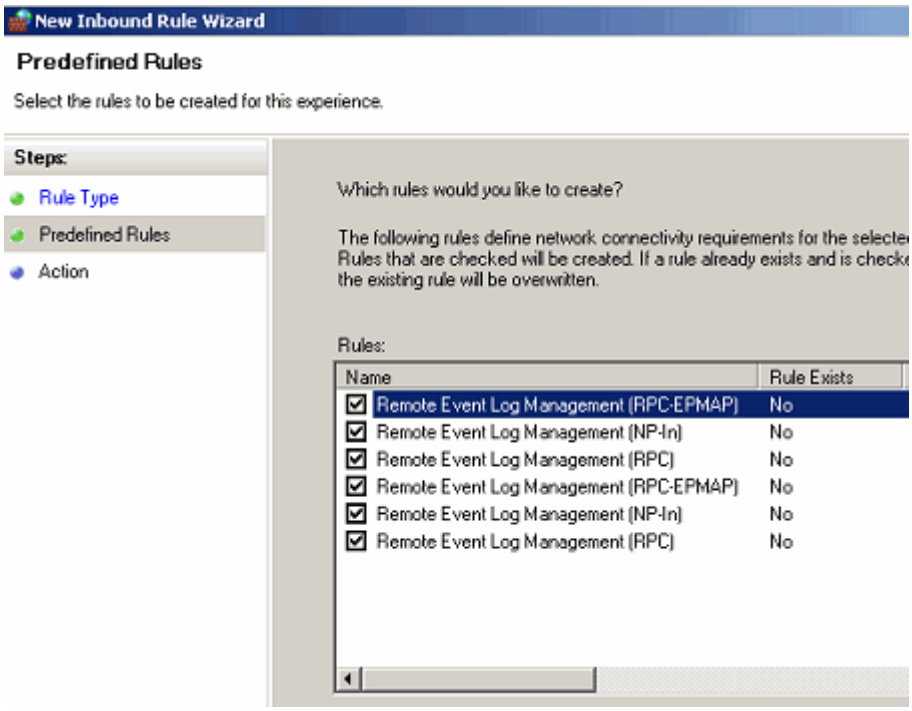
If you are reviewing EVTX log files from newer operating systems with WhatsUp Event Rover installed on Windows Vista, Server 2008, Server 2012, or Windows 7, allow the Remote Event Log Management exception in the Windows Firewall in order for WhatsUp Event Rover to successfully read and work with EVTX logs. The easiest way to do this in a domain is to use a Group Policy Object that governs all Vista, Windows 7, Server 2008, and Server 2012 computers. On workgroup or standalone machines, you can either manually set the exception under the Windows Firewall Exceptions tab on each computer, or you can create a Local Security Policy template targeting the Windows Firewall with Advanced Security area and apply it to the Local Security Policy on each machine with the **secedit** command line tool.

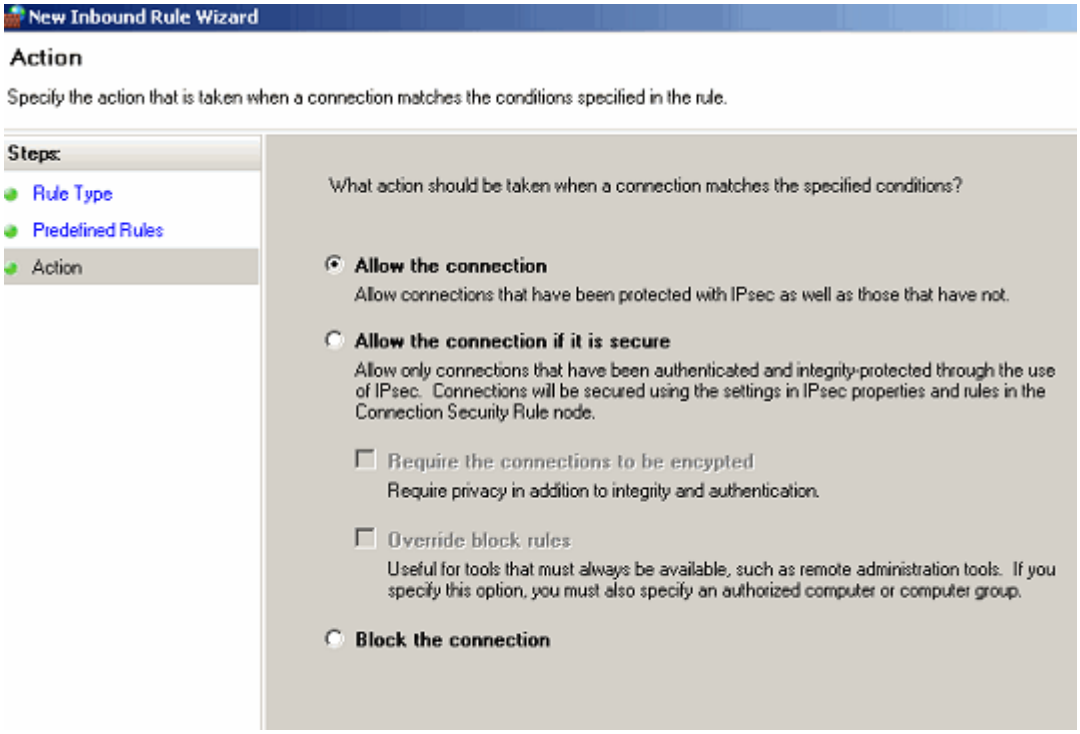


Note: Ipswitch recommends creating both an inbound and outbound rule allowing Remote Event Log Management.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - Local Group Policy Object
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Public Key
IP Security


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Predefined Rules
Action
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Remote Event Log Management
Rule that controls connections for a Windows experience.
Custom
Custom rule.


New Inbound Rule Wizard
Predefined Rules
Select the rules to be created for this experience.
Steps:
Rule Type
Predefined Rules
Action
Which rules would you like to create?
The following rules define network connectivity requirements for the selecte
Rules that are checked will be created. If a rule already exists and is checke
the existing rule will be overwritten.
Rules:
Name
Rule Exists
Remote Event Log Management (RPC-EPMAP) No
Remote Event Log Management (NP-In) No
Remote Event Log Management (RPC) No
Remote Event Log Management (RPC-EPMAP) No
Remote Event Log Management (NP-In) No
Remote Event Log Management (RPC) No


New Inbound Rule Wizard
Action
Specify the action that is taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Predefined Rules
Action
What action should be taken when a connection matches the specified conditions?
Allow the connection
Allow connections that have been protected with IPsec as well as those that have not.
Allow the connection if it is secure
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Require the connections to be encypted
Require privacy in addition to integrity and authentication.
Override block rules
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.
Block the connection

Setting WhatsUp Event Rover Preferences

You can set or change your preferences using the Event Rover Preferences dialog. The Preferences dialog allows you to set the default domain/workgroup WhatsUp Event Rover uses when listing computers, where WhatsUp Event Rover retrieves computer names from (which are used when opening event logs), regional preferences for date/time settings, and whether WhatsUp Event Rover's event log storage folder is compressed.

To adjust your WhatsUp Event Rover preferences, click the **Options** menu, and then select **WhatsUp Event Rover Preferences**. The WhatsUp Event Rover Preferences dialog box displays.

WhatsUp Event Rover Preferences dialog field descriptions:

Default Domain / Workgroup. Determines which domains WhatsUp Event Rover uses to display computers for event log selection. If you have a multiple domain model with several trusting domains and a master domain, this domain should be the master domain so that all other domains are selectable. If you do not have a domain, use the Workgroup name instead and retrieve computer names from the browse list.

Retrieve Computer Names From. For the purpose of connecting to computers to examine their event log information, WhatsUp Event Rover utilizes a variety of methods to list available computers to the administrator. Obtaining computer names from **the browse list** displays all computers registered with the Master Browser in a workgroup or domain. If your domain is segmented, all computers may not be listed in the browse list. Retrieving computer names from the **AD Server / Domain Controller** lists all computer accounts in the domain; however, some accounts may reference inactive or decommissioned systems. Finally, in large domains, it may be more useful to only list computer accounts from a given **Organization Unit in Active Directory**. To use this option, click the browse button on the right to browse for the OU in your domain.

Display Dates. Choose the desired format for how dates are displayed in WhatsUp Event Rover.

Enable NTFS compression on WhatsUp Event Rover's event log storage folder. When checked, this option enables compression on WhatsUp Event Rover's event log storage folder (e.g. <INSTALL PATH>\EventLogs). Enabling compression reduces the storage overhead associated with keeping backup copies of event logs, especially large logs from domain controllers. By default, backup copies of active computer logs saved by WhatsUp Event Rover are copied into this location and are stored there until the administrator removes them.

Attempt ICMP Echo (Ping) Testing Before Attempting to Open Active Computer Logs. When checked, WhatsUp Event Rover attempts to ping a remote computer before attempting to save and load a copy of one of its event logs. This action prevents lengthy network timeouts if a machine is no longer on the network.

Refreshing WhatsUp Event Rover

Refreshing your screen reloads and reorders log records into the currently active Log Viewing tab. You can also use **F5** as a keyboard shortcut to perform the same operation.

To refresh your currently active WhatsUp Event Rover screen or tab, click the **View** menu, and then select **Refresh**.

Reading the Current Event Log Summary Report

When WhatsUp Event Rover opens an event log file for the first time, it attempts to create a summary report in HTML format. The Summary report contains useful information about the opened event log. If you want to view the Summary report for your current event log after WhatsUp Event Rover opens, select **Read Current Event Log Summary Information** from the **File** menu.

Date Range. Displays the earliest and latest dates for events in the event log.

Total Number of Events In Log. Indicates the number of records in the event log.

Event IDs Used For Quick Filtering. Displays the event identifier numbers included or excluded from the current review of the log.

Number Of Events Matching Quick Filter. Displays the number of events returned by the filter at load, as opposed to the total number of events actually in the log.

Event Log Size. Displays the uncompressed size of the log file on disk.

Average Event Size. Indicates the average amount of bytes each log record occupies in the file.

Average Daily Size. An estimate of how much data is written to this log file daily on a given server.

Error Events, Warning Events, Information Events, Failure Audit Events, and Success Audit Events. Display how many events of each type are in the log. This is a useful indicator of problems or abnormal activity in a log, if, for instance, the Error Events or Failure Audit Events count was greater than usual.

User Accounts Found. Summarizes all user accounts found in a given log file. This is especially useful if you are attempting to track user or administrator activity, to see if they are present in the User field of any records in the log.

Note: To use the Event Research Window, Microsoft Internet Explorer version 5.0 or later must be installed on your system. In addition, under Advanced Preferences in Internet Explorer, third-party browser extensions must be enabled.

Log Healer Technology

LogHealer™ Technology automatically runs every time you attempt to open an EVTX log file (e.g. a log file saved from a Windows Vista or later operating system) inside WhatsUp Event Rover. If WhatsUp Event Rover detects problems with the EVTX file (such as it being a file recovered from an improperly shutdown system in a forensic investigation), it will notify you of these issues, and ask you if you would like to repair the file and store the repaired version as a new file. If you elect to repair the file, WhatsUp Event Rover attempts to open the repaired version.

In all cases, WhatsUp Event Rover always maintains the original corrupted/problematic EVTX file without modification, which is especially important when using WhatsUp Event Rover for forensic examination of log data.

When in evaluation mode, WhatsUp Event Rover only recovers the first 64KB of log file data to demonstrate proof of concept. After the full version of the software is purchased and activated, a full recovery of the file is attempted. If for any reason log file data cannot be properly recovered, please contact Ipswitch's Support Department promptly, and make arrangements to send a copy of the EVTX log file in question for further examination.

Reviewing Custom Event Logs

Traditionally, there are six standard Windows Event Logs present on Microsoft Windows server and workstation operating system; the Application, System, and Security logs appear on all Windows operating systems, and the DNS Server, Directory Service, and File Replication Service logs are found on server operating systems.

However, various third-party applications are now creating their own custom Windows event logs for error tracking and reporting. WhatsUp Event Rover gives you the option of defining these custom event logs so they can be reviewed alongside the standard logs mentioned above.

To define a custom event log:

1. Click the **Options** menu, then select **Manage Custom Logs**.
2. Browse to various computers to view the custom Windows event logs present on any given system.
3. Select the custom event log from the list, and then click the **Add Custom Log** button. Similarly, if you no longer wish to see a particular custom event log as available throughout WhatsUp Event Rover, select it from the **Custom Event Logs Defined** list and click the **Remove Custom Log** button.

In some instances, you may not be able to enumerate custom logs on a remote machine (e.g. the Remote Registry Service may be disabled, for instance), so you can also choose to add a custom log manually by clicking the **Add Custom Log Manually** button. In the resulting dialog, specify both the **Custom Log Display Name** (e.g. the name of the log as shown in the Microsoft Event Viewer) and the **Custom Log Internal Name** (e.g. the internal registry name for the log). In pre-Microsoft Vista operating systems, such as Windows XP and Windows 2003, the custom log internal name is always the same as the display name. In Vista and later operating systems, the internal name may be different, and you will need to determine the internal name by finding that logs subkey under the HKLM\System\CurrentControlSet\Services\EventLog section of the computer's registry.

WhatsUp Event Rover License Agreement

Legal Information

Ipswitch License Agreement

1. LICENSE GRANT

Ipswitch grants to you, and you accept, a non-exclusive and non-transferable license to use software program(s) provided by Ipswitch, and the accompanying user documentation ("Documentation"), (collectively, the "Software") as purchased by you only as authorized in this Agreement. You may not assign, transfer, rent, or sublicense the Software (any violation of the foregoing will result in automatic termination of the license without any right of refund). The Software consists of proprietary products of Ipswitch or its third party suppliers, and the proprietary rights that protect such property may include, but are not limited to, U.S. and international copyrights, trademarks, patents, and trade secret laws of general applicability. All right, title and interest in and to the Software are and shall remain with Ipswitch or its third party suppliers, as applicable. This Agreement does not convey to you any interest in or title to the Software, but only a limited right of use revocable in accordance with its terms.

You may use the Software on a specific number of computers, as identified at the time of purchase. Each instance of a Virtual Machine (VM) and each instance of a session in an environment where multiple users share computer resources are considered one computer. For Software in which more than one feature set (e.g. "standard", "premium") is available, you may solely use one specific feature set. If you desire a different feature set, you must purchase an upgrade. Feature sets are defined in the Documentation and identified at the time of purchase.

For Software in which more than one level (e.g. "100 users", "300 devices") is available, you may solely use one specific level. If you desire a different level, you must purchase an upgrade. Levels are defined in the Documentation and identified at the time of purchase.

For Software provided to you for an evaluation period, you may use the Software until the completion of the evaluation period.

For Software provided to you as a subscription, you may use the Software until the completion of the subscription period.

For Software acquired by you under a perpetual license, you may use the Software indefinitely.

For Software in which more than one network environment (e.g. "internally owned and operated", "externally owned and operated") is available, you may solely use the Software in a specific network. If you desire a different network environment, you must purchase an upgrade or a separate license. Network environments are defined in the Documentation and identified at the time of purchase.

For Software which includes dynamic content (e.g. anti-virus and anti-spam definitions), said content is sold on a subscription basis and remains current as long as you maintain an active subscription with Ipswitch.

For Software designated as Software Development Kits (SDK), you may create, reproduce and distribute solutions, plug-ins or other derivative works (collectively "applications") solely to end users who have a valid and current license for the associated Software. For SDK Software designated as "Internal Use", you must further restrict distribution solely to end users in your organization.

2. CONSENT TO USE OF DATA

You agree that Ipswitch and its subsidiaries may collect and use technical and related information, including but not limited to technical information about your computer, system and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to you (if any), and to verify compliance with the terms of this License.

3. INSTALLATION AND RESTRICTIONS

You assume responsibility for selection of the Software to achieve your intended results and for the installation, use, and valid operation of the Software. You agree at all times to maintain records specifically identifying the Software and the personal computers on which the Software is being used and to make such records available for inspection by Ipswitch during normal business hours.

You may make copies of the software media solely for backup, disaster recovery, or archival purposes, which copies shall contain Ipswitch's copyright and other proprietary notices. You may not modify, translate, adapt, decompile, disassemble, decrypt, extract, or otherwise reverse engineer or attempt to discover the confidential source code and techniques incorporated in the Software. You may not create derivative software based on any trade secret or proprietary information of Ipswitch.

4. LICENSE FEES

The license fees paid by you are in consideration of the licenses granted under this Agreement. If the Software is under evaluation and no license fees have been paid, this Agreement will expire at the end of the evaluation period unless you have purchased a license key to enable subsequent activation. If the Software is provided on a subscription basis, this Agreement will expire at the end of the subscription period unless you have purchased a renewal subscription.

5. TERMINATION

This License Agreement is effective until terminated. You may terminate this License Agreement at any time. This License Agreement will also terminate if you fail to comply with any terms and conditions set forth elsewhere herein. You agree upon any termination to destroy the Software together with all copies, modifications and merged portions in any form, and certify in writing that you have done so.

6. LIMITED WARRANTY

For twenty one (21) days (the "Warranty Period") from your date of purchase, Ipswitch warrants for your benefit alone, that (i) the Software will substantially conform to the applicable Documentation and (ii) the media on which the Software is distributed and the Documentation (if any) are free from defects in materials and workmanship and, (iii) during the Warranty Period, the Software will operate substantially in accordance with the Documentation. If during the Warranty Period an error in the Software occurs, you may return the Software to Ipswitch for either repair or replacement, or if so elected by Ipswitch, refund of the license fee paid by you under this Agreement. For any breach of the foregoing warranty during the Warranty Period, your exclusive remedy and Ipswitch's entire liability will be as described in the previous sentence. THE FOREGOING ARE THE ONLY WARRANTIES

PROVIDED BY IPSWITCH AND IPSWITCH DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

7. LIMITATION OF LIABILITY

Because computer software is inherently complex and may not be completely free of errors, it is your responsibility to verify your work and to make backup copies, and Ipswitch will not be responsible for your failure to do so. Ipswitch's cumulative liability to you or any party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Ipswitch for the applicable Software.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL IPSWITCH BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, ECONOMIC, EXEMPLARY, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE IPSWITCH PRODUCTS OR SERVICES, INCLUDING, WITHOUT LIMITATION, DAMAGES OR COSTS RELATING TO THE LOSS OF PROFITS, BUSINESS, GOODWILL, DATA, OR COMPUTER PROGRAMS, EVEN IF IPSWITCH HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT RESTRICTED RIGHTS

If the Software is acquired on behalf of a unit or agency of the United States Government this provision applies.

For units of the Department of Defense (DoD), this Software is supplied only with "Restricted Rights" as that term is defined in the DoD Supplement to the Federal Acquisition Regulations, 52.227-7013(c)(1)(ii) and:

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013. Contractor: IPSWITCH, Inc., 10 Maguire Road, Lexington, MA 02421

Government personnel using this Software, other than under a DoD contract or GSA Schedule, are hereby on notice that use of this Software is subject to restricted rights, which are the same as, or similar to those specified above.

9. GENERAL

This Agreement will be governed by the laws of the Commonwealth of Massachusetts without regard to conflict of law principles. The export of this product is governed by the U.S. Bureau of Industry and Security under Export Administration Regulations and may be exported to appropriate countries and end-users based upon their license exception. Export compliance information for each Ipswitch product can be found on the Ipswitch website at http://www.ipswitch.com/company/export_compliance/product.asp. The appropriate classification for each product is specified on Ipswitch's website. It is the responsibility of the exporter to adhere to appropriate Export Administration Regulations. You shall remain fully responsible for and certify compliance with all applicable Export laws and regulations, and you agree to indemnify Ipswitch from all costs, expenses, and liability for such compliance.

Should any term of this Agreement be declared void or unenforceable by any court of competent jurisdiction such declaration shall have no effect on the remaining terms hereof.

IPSWITCH, INC.

10 Maguire Rd.

Lexington, MA 02421

(781) 676-5700

Fax: (781) 676-5710

CHAPTER 2

WhatsUp Event Rover Menus

In This Chapter

Using the File Menu

The File menu allows you to open copies of active event log files, open previously saved event log files, close log files, read summary information about the currently open log, manage WhatsUp Event Rover's local saved event log repository, and export selected branches of information in a Log Viewing tab to an HTML report.

File menu options

Open an Active Computer Event Log File. Opens the Open Active Event Log dialog so you can create a backup copy of an active event log on a remote computer and then transport the copy to WhatsUp Event Rover to view its data.

Open an Event Log File Saved by WhatsUp Event Rover. Opens the Saved Event Log File Manager dialog so you can open an EVT or EVTX file previously saved by WhatsUp Event Rover in its local event log repository.

Open Any Saved Event Log File. Opens the Open Saved Event Log dialog so you can open an EVT or EVTX file saved by a different program, such as Microsoft's Event Viewer. You can also use this dialog to open zip-compressed EVT and EVTX files, such as those saved by Ipswitch's WhatsUp Event Archiver utility.

Close the Open Event Log File. Closes the open event log file.

Read Current Event Log Summary Information. Opens the Summary Report dialog so you can view a summary of information (e.g. number of events, user accounts present, etc) contained in the currently viewed event log file.

Saved Event Log File Manager. The Saved Event Log File Manager dialog allows you to delete event log files in WhatsUp Event Rover's local event logs repository.

Create an HTML Report From Selected Branch. Opens the Report Creation dialog so you may title and add comments to an HTML report containing event records from the currently selected branch in the Log Viewing tab.

Exit. Closes WhatsUp Event Rover.

Using the Edit Menu

The Edit menu allows you to create and manage both filters and friendly event identifiers that WhatsUp Event Rover can use when viewing an event log file.

Edit menu options

- **Create and Apply a Filter**. Opens the Filters dialog, where you can define, and optionally save, a filter to reduce the records displayed in the Log Viewing tabs.
- **Remove Filter**. Removes the currently active filter from the log data being viewed.
- **Apply a Saved Filter**. Displays a submenu containing all previously saved filters, allowing you to choose one to apply to the current log data.
- **Apply a Recent Filter**. Displays a submenu containing the most recently used filters, allowing you to choose one to apply to the current log data.
- **Manage Filters**. Opens the Filters dialog,where you can edit and delete existing saved filters.
- **Manage Custom Event Logs**. Opens the *Custom Event Log Manager Dialog* (on page 12), allowing you to define custom Windows event logs for review within WhatsUp Event Rover.
- **Manage Friendly IDs**. Opens the Friendly Event ID Manager dialog, allowing you to create, edit, and delete Friendly Event ID definitions. A Friendly ID is a textual description for a given Event ID, Log Type, and Source, that WhatsUp Event Rover displays alongside the Event ID number in the program and in HTML reports. The Friendly ID Manager can also be used when electing to quick filter event logs at load by Event ID.

Using the View Menu

Refresh. Reloads and reorders log records into the currently active Log Viewing tab. You can also use F5 as a keyboard shortcut to perform the same operation.

Using the Options Menu

Use the Options menu to configure WhatsUp Event Rover's default operating behaviors and settings.

WhatsUP Event Rover Preferences. Opens a dialog used to customizes WhatsUp Event Rover's various global behaviors, such as the default domain/workgroup to list computers from, where to obtain computer accounts from (e.g. browse list, DC, Organizational Unit on the DC), and regional date/time preferences.

Using the Groupings Menu

Field groupings are at the center of how WhatsUp Event Rover displays log data. Each defined active field grouping is a separate tab in the Log Viewing tabs. While WhatsUp Event Rover ships with several useful, predefined field groupings, the administrator has full control over how they are organized. The administrator can also create their own field groupings, when appropriate. Use the Groupings menu items to create and manage your field groupings.

Groupings menu options:

Create a New Field Grouping. Opens the Define a Field Grouping dialog, where you can create a new field grouping.

Manage Field Groupings. Opens the Manage Field Groupings Dialog, where you can edit and delete field groupings, as well as mark them active or inactive. Only active field groupings are shown among the Log Viewing tabs.

Using the Incidents Menu

The Incidents menu allows you to define patterns of events as incidents, as well providing you with a way to scan the currently loaded log file for those incidents.

Incidents menu options

Incident Manager. Opens the Incident Manager dialog, where you can create, modify, and remove incident definitions.

View Incidents in This Log. Scans the currently loaded event log for occurrences of your defined incidents. If event occurrences are found, the Incident Viewer dialog opens.

Using the Help Menu

The Help menu contains links to the Ipswitch website, WhatsUp Event Rover's online help system, and allows you to register WhatsUp Event Rover and upgrade your total number of licenses.

Help menu options

Visit Ipswitch Software Online. Connect to the Ipswitch, Inc. home page, using your default browser.

Ipswitch Product Catalog. Connect to the Ipswitch, Inc. product catalog web page, where you can find out more information about other Ipswitch software products.

Register WhatsUp Event Rover / Upgrade WhatsUp Event Rover Licenses. Displays the License Manager dialog, where you can initially register WhatsUp Event Rover, and later, add more licenses as needed.

WhatsUp Event Rover Help File. Opens the WhatsUp Event Rover online help system.

About WhatsUp Event Rover. Displays your WhatsUp Event Rover version and splash screen.

CHAPTER 3

Opening Log Files

In This Chapter

Opening an Active Computer Event Log File

Open an active computer event log file to create a backup copy of an active event log file, move the backup copy of the log file into WhatsUP Event Rover's local event log repository, or open the backup copy locally on the machine running WhatsUp Event Rover.

To open an active computer event log file:

1. From the **File** menu, select **Open an Active Computer Event Log File**. The Choose an Active Event Log to Save, Then Open Locally dialog opens.
2. Complete the fields in the Choose an Active Event Log to Save, Then Open Locally dialog, and then click **OK**. When you finish reviewing the backup copy, WhatsUp Event Rover asks whether you want to save it in WhatsUp Event Rover's event log repository.

Choose an Active Event Log to Save, Then Open Locally dialog field descriptions:

- **Domain**. Select the domain/workgroup of the computer whose log you want to view. If this list is disabled, you have selected to retrieve computers from a specific OU in Active Directory. To change this behavior, see the *Adjusting Global Settings* (on page 9) help topic.
- **Computer**. Select the computer for which you want to review log information.
- **Log Type**. Select the log you wish to view.
- **Quick Filter This Log By Event ID**. Opens the Friendly Event ID Manager dialog in Quick Filter Builder mode, allowing you to build and then select a quick filter based on one or more Event IDs. Quick filtering a log by Event ID can greatly reduce the load time needed for opening a large log file, and streamline the time needed to anaylze the resulting log records.

- **Limit Records Retrieved to Specific Date Range**. Useful for opening large log files. If you choose to limit records retrieved to a relative or custom date range, the amount of data that WhatsUp Event Rover must interpret and organize is greatly minimized. This reduces the time necessary to open this event log, as well as the time necessary to reorder data into different Log Viewing tabs. Date range filtering is currently only available when reviewing EVT format logs on legacy operating systems.

Opening a Saved Event Log File

Use the Open Saved Event Log dialog to open a previously saved event log file (.EVT or .EVTX) from disk. You may also open zip-compressed event log files (e.g. such as those saved by Ipswitch Software's Event Archiver product) using this dialog. Only zip files containing a single EVT/EVTX file can be opened, and the file extension must end in .EVT.ZIP or .EVTX.ZIP

Note: Zip-compressed event log files are automatically decompressed into WhatsUp Event Rover's temp directory (e.g. <INSTALL PATH>\Temp), and the temp folder automatically clears when the program exists. The original .ZIP file remains unmodified.

To open any saved event log file saved by WhatsUp Event Rover:

1. From the **File** menu, select **Open Any Saved Event Log File**. The Choose a Previously Saved Event Log to Open dialog opens.
2. Complete the fields in the Choose a Previously Saved Event Log to Open dialog, and then click **OK**.

Choose a Previously Saved Event Log to Open dialog field descriptions:

File. Enter the path to an EVT/EVTX file (.evt/.evtx) or zipped EVT/EVTX file (.evt.zip/.evtx.zip) on disk.

Browse(...). Browse for an EVT/EVTX file or zipped EVT/EVTX file on disk.

Log Type. Select the originating log type of this EVT/EVTX file.

Load message files/metadata from. In some cases, you may have an EVT or EVTX file from a computer on a different network. To properly display data from the log, instruct Event Analyst to load message files and other related data from a "surrogate" computer on your network.

Note: If you choose to load message files from a different computer when working with a security log, the surrogate computer being used must match the Windows platform of the machine that originally generated the EVT/EVTX file. E.g. if you have a security event log from an external Windows 2003 server, you should load message files from a nearby Windows 2003 server, etc.

Quick Filter This Log By Event ID. Opens and displays the Friendly Event ID Manager dialog in Quick Filter Builder Mode, allowing you to build and then select a quick filter based on one or more Event IDs. Quick filtering a log by Event ID can greatly reduce the load time needed when opening a large log file (e.g. one containing more than 75000 records), and streamline the time necessary for analyzing the resulting log records.

Limit Records Retrieved to Specific Date Range. This option is useful for opening large log files. If you choose to limit records retrieved to a relative or custom date range, the amount of data that WhatsUp Event Rover must interpret and organize is greatly minimized. This reduces the time necessary to open this event log, as well as the amount of time necessary to reorder data into different Log Viewing tabs.

Note: Date Range filtering is currently only available when reviewing EVT format logs on legacy (e.g. XP/2003) operating systems.

Opening an Event Log File Saved by WhatsUp Event Rover

The Saved Event Log Files Manager dialog is a graphical representation of WhatsUp Event Rover's event log repository (e.g. the EventLogs subdirectory in the WhatsUp Event Rover installation folder). Here, you can view summary information about logs previously saved by WhatsUp Event Rover, delete old, unneeded logs, and re-open logs for review in the WhatsUp Event Rover program.

To open an event log file saved by WhatsUp Event Rover:

1. From the **File** menu, select **Open an Event Log File Saved by WhatsUp Event Rover**. The Choose a Saved Event Log File to Open dialog opens.
2. Complete the fields in the Choose a Saved Event Log File to Open dialog, and then click **OK**.

Open an Event Log File Saved by WhatsUp Event Rover dialog field descriptions:

Computer Name. Indicates the machine the log originally came from.

Log Type. Indicates the saved log type.

Date Saved. Indicates the date and time when the log was originally saved.

Date Range. Indicates if the log was originally opened with a date range attached, or if all events were examined. If originally opened with a date range, the next time the log is reopened the same date range applies to the displayed information. Viewing the summary report yields more information regarding the exact date range.

Size (MBs). Shows the uncompressed megabyte size of the log on disk. However, if the event log repository folder is compressed with NTFS compression, the actual compressed size will be much lower.

View Summary Report. Opens the *Summary Report* (on page 11) for the currently selected log, which contains valuable information about the number of records and information contained inside the log.

Delete. Deletes the selected event log from WhatsUp Event Rover's event log repository. The delete function only deletes the backup copy of the event log stored locally by WhatsUp Event Rover, not the active event log on a given server.

Closing the Open Event Log File

When you finish viewing the open event log file, close the open event log file by selecting **Close the Open Event Log File** from the **File** menu.

Reading the Current Event Log Summary Report

When WhatsUp Event Rover opens an event log file for the first time, it attempts to create a summary report in HTML format. The Summary report contains useful information about the opened event log. If you want to view the Summary report for your current event log after WhatsUp Event Rover opens, select **Read Current Event Log Summary Information** from the **File** menu.

Date Range. Displays the earliest and latest dates for events in the event log.

Total Number of Events In Log. Indicates the number of records in the event log.

Event IDs Used For Quick Filtering. Displays the event identifier numbers included or excluded from the current review of the log.

Number Of Events Matching Quick Filter. Displays the number of events returned by the filter at load, as opposed to the total number of events actually in the log.

Event Log Size. Displays the uncompressed size of the log file on disk.

Average Event Size. Indicates the average amount of bytes each log record occupies in the file.

Average Daily Size. An estimate of how much data is written to this log file daily on a given server.

Error Events, Warning Events, Information Events, Failure Audit Events, and Success Audit Events. Display how many events of each type are in the log. This is a useful indicator of problems or abnormal activity in a log, if, for instance, the Error Events or Failure Audit Events count was greater than usual.

User Accounts Found. Summarizes all user accounts found in a given log file. This is especially useful if you are attempting to track user or administrator activity, to see if they are present in the User field of any records in the log.

Note: To use the Event Research Window, Microsoft Internet Explorer version 5.0 or later must be installed on your system. In addition, under Advanced Preferences in Internet Explorer, third-party browser extensions must be enabled.

Opening the Report Creation Dialog

The Report Title and Comments dialog opens when a reporting operation is performed in WhatsUp Event Rover. Type a title for the report, as well as comments that may be useful to your target audience for better interpretation of the data.

To create a new HTML report:

1. From the **File** menu, select **Create an HTML Report From Selected Branch**. The Report Title and Comments dialog opens.
2. Type a title in the **Report title** field, and then enter any comments.
3. Click **OK**.

Report Title and Comments dialog field descriptions:

Report title. Type a title for the report you are generating. The title is placed at the beginning of the HTML report you generate and becomes the beginning of the filename when the report is saved to disk (e.g. ReportTitle DATESTAMP TIMESTAMP.html).

Comments. Annotate the report as needed with introductory comments; comments entered here display at the beginning of the report. Comments are not required.

CHAPTER 4

Filtering Logs

In This Chapter

Filters Dialog

The Create A Filter dialog allows you to create a filter, helping you manage the log data you open in WhatsUp Event Rover.

To create a filter:

1. From the **Edit** menu, select **Create and Apply a Filter**. The Create A Filter dialog opens.
2. Complete the fields in the Create a Filter dialog, and then click **OK**. WhatsUp Event Rover creates the filter.

Note: Only enter data in fields you intend to filter. Leave blank all fields you want ignored by the filter.

Create A Filter dialog field descriptions:

- **Filter By Date**. To define a filter with a specific date range, choose **Yes** and configure the **Beginning Date** and **Ending Date** appropriately. If you specified a date range when you first opened the log, make sure these dates are within that range.
- **Source**. Enter the registered application, hardware, or OS subsystem name whose events you want to filter.
- **Category.** Limits events by category.
- **User.** Limits events by user account.

- **Computer**. Limits events by computer.
- **Event ID**. Limits events by source-specific event number (ID).
- **Type**. To filter by type, check only the types you want included in the filter definition. If you do not want to filter by type, leave all check boxes blank.

Note: Perform limited description filtering when viewing related log entries in the Records Listing Dialog. For advanced filtering, such as multiple conditions per field and wildcards, you can read more about our Event Analyst product at http://www.Ipswitchsoftware.com/eventanalyst.

Note: You can also create a filter by clicking the **Add** button on the Manage Filters dialog.

Manage Filters dialog button descriptions

- **Add**. Allows you to add and save a new filter in the local filters database.
- **Edit**. Loads the filter definition of the selected filter, and allows you to modify its fields.
- **Delete**. Deletes the selected filter.
- **Close**. Closes this dialog.

Applying a Recent Filter

You can filter your WhatsUp Event Rover data by applying a recent filter.

To apply a recent filter:

1. Click the **Edit** menu, and then select **Apply a Recent Filter**.
2. From the secondary menu list, select the name of the filter you want to apply. WhatsUp Event Rover applies the selected filter.

Applying a Saved Filter

You can filter your WhatsUp Event Rover data by applying a saved filter.

To apply a saved filter:

1. Click the **Edit** menu, and then select **Apply a Saved Filter**.
2. From the secondary menu list, select the name of the filter you want to apply. WhatsUp Event Rover applies the selected filter.

Editing a Filter

Use the Manage Filters dialog to edit an existing filter. When editing a filter, you can change any of the filter's properties, and the existing filter will take on the attributes you selected. If you want to keep the existing attributes of a filter, you can also *create a new filter* (on page 27).

To edit an existing filter:

1. From the **Edit** menu, select **Manage Filters**. The Manage Filters dialog opens.
2. Select the filter you want to edit, and then click **Edit**. The Create a Filter dialog opens.
3. Edit the properties you want to change, and then click **OK**. The Enter a Filter Name dialog opens.
4. To change the name of the filter, type a new name; to keep the filter name the same, click **OK**. Your edited filter is created.

Manage Filters dialog field descriptions:

Add. Allows you to add and save a new filter in the local filters database.

Edit. Loads the filter definition of the selected filter and allows you to modify its fields.

Delete. Deletes the selected filter.

Create a Filter dialog field descriptions:

Filter By Date. To define a filter with a specific date range, choose **Yes** and configure the **Beginning Date** and **Ending Date** appropriately. If you specified a date range when you first opened the log, make sure these dates are within that range.

Source. Enter the registered application, hardware, or OS subsystem name whose events you want to filter.

Category. Limits events by category.

User. Limits events by user account.

Computer. Limits events by computer.

Event ID. Limits events by source-specific event number (ID).

Type. To filter by type, check only the types you want included in the filter definition. If you do not want to filter by type, leave all check boxes blank.

Adding a Custom Log to WhatsUp Event Rove

Traditionally, there are six standard Windows Event Logs present on Microsoft Windows server and workstation operating system; the Application, System, and Security logs appear on all Windows operating systems, and the DNS Server, Directory Service, and File Replication Service logs are found on server operating systems.

However, various third-party applications are now creating their own custom Windows event logs for error tracking and reporting. WhatsUp Event Rover gives you the option of defining these custom event logs so they can be reviewed alongside the standard logs mentioned above.

To define a custom event log for use within WhatsUp Event Rover:

1. Select the **Edit** menu, then select **Manage Custom Logs**. The Manage Custom Logs dialog opens.
2. Browse to various computers to view the custom Windows event logs present on any given system.
3. To add a custom event log for review by WhatsUp Event Rover, select the custom log from the list, and then click the **Add Custom Log** button.

Removing an Active Filter

You can remove an active filter from currently displayed log information. To remove an active filter, click the **Edit** menu, and then select **Remove Filter**. The active filter is removed.

Note: When you select Remove Filter, the filter is immediately removed without a confirmation message.

Deleting a Custom Log from WhatsUp Event Rover

After adding custom event logs to WhatsUp Event Rover, you can delete any custom logs you no longer need to view.

To delete a custom log from WhatsUp Event Rover:

1. Select the **Edit** menu, then select **Manage Custom Logs**. The Manage Custom Logs dialog opens.
2. Select the custom log(s) you want to delete from the list of custom logs defined in WhatsUp Event Rover.
3. Click **Remove Log(s)**. The selected custom log is deleted from the system.

Adding a Friendly Event ID

Use the Friendly Event ID Manager dialog to create friendly definitions for specific event identifiers that found in various log types. Friendly event IDs allow you to append your own text to event IDs. After a friendly event ID is defined, WhatsUp Event Rover displays your friendly definition beside the event identifier number, as well as in HTML reports you create.

To add friendly event IDs:

1. From the **Edit** menu, select **Manage Friendly Event IDs**. The Manage Friendly Event IDs dialog opens.
2. Click the **Add** button.
3. Complete the fields in the Manage Friendly Event IDs dialog, and then click **OK**. Your friendly event ID is created.

Manage Friendly Event IDs dialog field definitions:

Event ID. Enter the event identifier number for the event to which you want to associate a friendly definition.

Log Type. Select the log type in which this event identifier is found.

Source. Select the source with which this identifier is associated.

Friendly Definition. Enter descriptive text that explains the meaning/purpose of this event.

Editing a Friendly Event ID

Friendly event IDs allow you to append your own text to event IDs. After a friendly event ID is defined, WhatsUp Event Rover displays your friendly definition beside the event identifier number, as well as in HTML reports you create. After adding a friendly event ID, you can edit it to meet your needs.

To edit a friendly event ID:

1. From the **Edit** menu, select **Manage Friendly Event IDs**. The Manage Friendly Event IDs dialog opens.
2. Click the **Edit** button.
3. Complete the fields in the Manage Friendly Event IDs dialog, and then click **OK**. Your edited friendly event ID is changed.

Manage Friendly Event IDs dialog field descriptions:

Event ID. Enter the event identifier number for the event to which you want to associate a friendly definition.

Log Type. Select the log type in which this event identifier is found.

Source. Select the source with which this identifier is associated.

Friendly Definition. Enter descriptive text that explains the meaning/purpose of this event.

Deleting a Friendly Event ID

Use the Friendly Event ID Manager dialog to delete friendly definitions for specific event identifiers that found in various log types. Friendly event IDs allow you to append your own text to event IDs. After a friendly event ID is defined, WhatsUp Event Rover displays your friendly definition beside the event identifier number, as well as in HTML reports you create.

To delete a friendly event ID:

1. From the **Edit** menu, select **Manage Friendly Event IDs**. The Manage Friendly Event IDs dialog opens.
2. Select the friendly event ID you want to delete, and then click the **Delete** button.
3. Complete the fields in the Manage Friendly Event IDs dialog, and then click **OK**. Your friendly event ID is created.

Manage Friendly Event IDs dialog field descriptions:

Event ID. Enter the event identifier number for the event to which you want to associate a friendly definition.

Log Type. Select the log type in which this event identifier is found.

Source. Select the source with which this identifier is associated.

Friendly Definition. Enter descriptive text that explains the meaning/purpose of this event.

CHAPTER 5

Grouping and Sorting Event Records

In This Chapter

Opening the Define a Field Grouping Dialog

Use the Define a Field Grouping dialog to add a new field grouping to WhatsUp Event Rover, or to edit an existing field grouping.

When you adjust field groupings in WhatsUp Event Rover, you control the behavior of the Log Viewing tabs. Each Log Viewing tab represents one of the active Field Groupings in WhatsUp Event Rover. By changing a field grouping, you control how WhatsUp Event Rover groups and sorts log data in a particular tab. For example, the Security Activity field grouping groups all log data first by Category, and then by Event ID. Because these items are checked, they become the first two branches in the tree in the Security Activity Log Viewing tab. The unchecked fields are "remnant" fields, meaning they are not displayed as branches, but are displayed in the Records Listing Dialog when you click the bottom level of a tree; they are also displayed in reports. In addition, the ordering (top to bottom) of the "remnant" fields determines the sorting order when they display in a report.

To create a new field grouping:

1. From the **Groupings** menu, select **Create a New Field Grouping**. The Define a Field Grouping dialog opens.
2. Type a name for the field grouping in the **Field Grouping Name** field.
3. Check the fields you want to see branched in the field groupings tree.
4. Click **OK**. Your new field grouping is created.

Define a Field Grouping dialog field descriptions:

Field Grouping Name. Determines how the corresponding Log Viewing tab is labeled in the WhatsUp Event Rover system.

Field Grouping Order. Check and order the fields to mimic the way you want the log sorted. Checked fields become branches in a Log Viewing tab's tree representation of event log data. Unchecked fields are not present in the tree, but are present in the Records Listing dialog and in reports. All checked fields must be at the top of the field grouping. Among

unchecked fields, make sure their top to bottom order matches how you would like them sorted in HTML reports.

Up and **Down** buttons. Moves fields up and down the list.

Activating a Field Grouping

Use the Manage Field Groupings dialog to indicate whether field groupings are active (e.g. visible as a Log Viewing tab), indicate which field grouping is the default grouping (e.g. the first tab). From here, you can also edit existing groupings or delete unneeded groupings.

To activate a field grouping:

1. From the **Groupings** menu, select **Manage Field Groupings**. The Manage Field Groupings dialog opens.
2. Check the check box next to the field grouping you want to activate. To deactivate a field grouping, uncheck the check box associated with the field grouping you want to deactivate.
3. Click **Close** to close the Manage Field Groupings dialog.

Manage Field Groupings dialog field descriptions:

Checked field groupings are active, meaning they will be represented as one of the five Log Viewing tabs in the WhatsUp Event Rover interface. Only 5 field groupings can be marked as Active or Default at one time. All others must be made inactive, by unchecking them.

Delete. Deletes the currently selected field grouping. You cannot delete the default field grouping, and at least one field grouping must exist in WhatsUp Event Rover at all times.

Default. Marks the selected field grouping the default field grouping. The default field grouping becomes the first (left most) Log Viewing tab in WhatsUp Event Rover and is the first tab that log data is loaded into when a log is opened.

Edit. Opens the Define a Field Grouping dialog so you can edit the currently selected field grouping.

Editing a Field Grouping

Use the Manage Field Groupings dialog to edit an existing field grouping. From here, you can also activate groupings or delete unneeded groupings.

To edit a field grouping:

1. From the **Groupings** menu, select **Manage Field Groupings**. The Manage Field Groupings dialog opens.
2. Select the field grouping you want to edit, and then click **Edit**. The Define a Field Grouping dialog opens.
3. Complete any necessary edits, and then click **OK**.
4. Click **Close** to close the Manage Field Groupings dialog.

Manage Field Groupings dialog field definitions:

Checked field groupings are active, meaning they will be represented as one of the five Log Viewing tabs in the WhatsUp Event Rover interface. Only 5 field groupings can be marked as Active or Default at one time. All others must be made inactive, by unchecking them.

Delete. Deletes the currently selected field grouping. You cannot delete the default field grouping, and at least one field grouping must exist in WhatsUp Event Rover at all times.

Default. Marks the selected field grouping as the default field grouping. The default field grouping becomes the first (left most) Log Viewing tab in WhatsUp Event Rover and is the first tab that log data is loaded into when a log is opened.

Edit. Opens the Define a Field Grouping dialog so you can edit the currently selected field grouping.

Define a Field Grouping dialog field definitions:

Field Grouping Name. Determines how the corresponding Log Viewing tab is labeled in the WhatsUp Event Rover system.

Field Grouping Order. Check and order the fields to mimic the way you want the log sorted. Checked fields become branches in a Log Viewing tab's tree representation of event log data. Unchecked fields are not present in the tree, but are present in the Records Listing dialog and in reports. All checked fields must be at the top of the field grouping. Among unchecked fields, make sure their top to bottom order matches how you would like them sorted in HTML reports.

Up and **Down** buttons. Moves fields up and down the list.

Setting the Default Field Grouping

Use the Manage Field Groupings dialog to set the default field grouping. From here, you can also activate groupings, edit groupings, or delete unneeded groupings.

To set the default field grouping:

1. From the **Groupings** menu, select **Manage Field Groupings**. The Manage Field Groupings dialog opens.
2. Select the field grouping you want to set as default, and then click **Default**. The system sets the selected field grouping as the default.
3. Click **Close** to close the Manage Field Groupings dialog.

Manage Field Groupings dialog field descriptions:

Checked field groupings are active, meaning they will be represented as one of the five Log Viewing tabs in the WhatsUp Event Rover interface. Only 5 field groupings can be marked as Active or Default at one time. All others must be made inactive, by unchecking them.

Delete. Deletes the currently selected field grouping. You cannot delete the default field grouping, and at least one field grouping must exist in WhatsUp Event Rover at all times.

Default. Marks the selected field grouping the default field grouping. The default field grouping becomes the first (left most) Log Viewing tab in WhatsUp Event Rover and is the first tab that log data is loaded into when a log is opened.

Edit. Opens the Define a Field Grouping dialog so you can edit the currently selected field grouping.

Deleting a Field Grouping

Use the Manage Field Groupings dialog box to delete a field grouping. From here, you can also activate groupings or edit groupings.

To delete a field grouping:

1. From the **Groupings** menu, select **Manage Field Groupings**. The Manage Field Groupings dialog box opens.
2. Select the field grouping you want to delete, and then click **Delete**. A confirmation message displays asking if you are sure you want to delete the selected field grouping.
3. Click **Yes** to delete the selected field grouping.
4. Click **Close** to close the Manage Field Groupings dialog box.

Manage Field Groupings dialog box field descriptions:

Checked field groupings are active, meaning they will be represented as one of the five Log Viewing tabs in the WhatsUp Event Rover interface. Only 5 field groupings can be marked as Active or Default at one time. All others must be made inactive, by unchecking them.

Delete. Deletes the currently selected field grouping. You cannot delete the default field grouping, and at least one field grouping must exist in WhatsUp Event Rover at all times.

Default. Marks the selected field grouping the default field grouping. The default field grouping becomes the first (left most) Log Viewing tab in WhatsUp Event Rover and is the first tab data is loaded into when a log is opened.

Edit. Opens the Define a Field Grouping dialog box, so you can edit the currently selected field grouping.

CHAPTER 6

Reporting On and Exporting Event Records

In This Chapter

Opening the Report Creation Dialog

The Report Title and Comments dialog opens when a reporting operation is performed in WhatsUp Event Rover. Type a title for the report, as well as comments that may be useful to your target audience for better interpretation of the data.

To create a new HTML report:

1. From the **File** menu, select **Create an HTML Report From Selected Branch**. The Report Title and Comments dialog opens.
2. Type a title in the **Report title** field, and then enter any comments.
3. Click **OK**.

Report Title and Comments dialog field descriptions:

Report title. Type a title for the report you are generating. The title is placed at the beginning of the HTML report you generate and becomes the beginning of the filename when the report is saved to disk (e.g. ReportTitle DATESTAMP TIMESTAMP.html).

Comments. Annotate the report as needed with introductory comments; comments entered here display at the beginning of the report. Comments are not required.