



IPS W I T C H

WhatsUp Event Archiver
v10.x
User Guide

CHAPTER 1 WhatsUp Event Archiver Help and Users Guide

WhatsUp Event Archiver Overview and Architecture	1
Deployment Scenarios.....	2
Collection Strategies.....	3
Initial Setup	5
Installation Requirements	5
Manually Creating Firewall Exceptions.....	6
Before You Begin.....	6
Microsoft Vista Requirements and Recommendations.....	15
Network and Bandwidth Considerations.....	18
Other Recommendations.....	20
Syslog Configuration	21
Tips and Tricks.....	21
WhatsUp Event Archiver's Feature Areas.....	22
Performing Test Archives.....	24
Setting Up Databases and Making Connections.....	24
Managing Your WhatsUp Event Archiver Licenses.....	30
Troubleshooting / Contacting Technical Support	32
Legal Information and License Agreement.....	35
International Issues and Log File Conversion	39

CHAPTER 2 WhatsUp Event Archiver Menu and Menu Option Descriptions

Using the File Menu	41
Using the Syslog Menu.....	42
Using the IIS/W3C Logs Menu.....	42
Using the View Menu.....	43
Using the Options Menu.....	43
Using the Tools Menu	44
Using the Help Menu.....	45

CHAPTER 3 Scheduling and Managing Logs for Collection

Adding or Editing Log.....	46
Deleting Scheduled Logs.....	50
Using the Archive Now! Option.....	50
Managing Audit Policies	51
Managing Log Settings.....	52
Launching Event Viewer	53

CHAPTER 4 Scheduling Logs for Multiple Computers

Setting-up Archiving for Multiple Computers at Once (Step 1)	54
Setting-up Archiving for Multiple Computers at Once (Step 2)	54
Setting-up Archiving for Multiple Computers at Once (Step 3)	55
Setting-up Archiving for Multiple Computers at Once (Step 4)	56
Setting-up Archiving for Multiple Computers at Once (Step 5)	56
Setting-up Archiving for Multiple Computers at Once (Step 6)	58

CHAPTER 5 Editing Settings on Multiple Computers

Adjusting Settings for Currently Managed Logs (Step 1)	59
Adjusting Settings for Currently Managed Logs (Step 2)	60
Adjusting Settings for Currently Managed Logs (Step 3)	60
Adjusting Settings for Currently Managed Logs (Step 4)	61
Adjusting Settings for Currently Managed Logs (Step 5)	62
Adjusting Settings for Currently Managed Logs (Step 6)	63
Setting Up/Adjusting Automatic Database Maintenance	64
Importing Older EVT/EVTX Files	66
Viewing WhatsUp Event Archiver Log Entries	67
Managing Failed Archives	68

CHAPTER 6 Adjusting Audit Policies Across Multiple Machines

Unifying Audit Policies (Step 1)	70
Unifying Audit Policies (Step 2)	70
Unifying Audit Policies (Step 3)	71

CHAPTER 7 Adjusting Log Retention/Size Across Multiple Machines

Unifying Log Settings (Step 1)	72
Unifying Log Settings (Step 2)	73
Unifying Log Settings (Step 3)	73
Unifying Log Settings (Step 4)	73

CHAPTER 8 Creating Database Tables

Creating Access Tables	74
Creating Microsoft SQL Server Tables	74
Creating Tables on ODBC Servers	75

CHAPTER 9 Setting-up Multiple IIS/W3C Directories at Once

Setting-up Multiple IIS/W3C Directories at Once (Step 1).....	77
Setting-up Multiple IIS/W3C Directories at Once (Step 2).....	78
Setting-up Multiple IIS/W3C Directories at Once (Step 3).....	78
Setting-up Multiple IIS/W3C Directories at Once (Step 4).....	79
Setting-up Multiple IIS/W3C Directories at Once (Step 5).....	80
Setting-up Multiple IIS/W3C Directories at Once (Step 6).....	80

CHAPTER 10 Configuring WhatsUp Event Archiver and Setting Defaults

Setting Up Archiver Preferences.....	81
Configuring the WhatsUp Event Archiver Service Account.....	89
Setting the Default Domain or Workgroup.....	90
Managing Custom Domain to Computer Mappings.....	91
Global Settings - Retrieving Computer Names.....	92
Managing Custom Logs.....	92
Setting Global Import Filters.....	93

CHAPTER 11 Managing Syslog Messages

Syslog Messages in WhatsUp Event Archiver.....	95
About Syslog Direct Write and Syslog Write to CSV File.....	96
Selecting Syslog Direct Write and Syslog Write to CSV File preferences.....	96
Setting up Syslog Direct Write.....	96
Configuring Syslog Direct Write database settings.....	98
Setting up Syslog Write to CSV File.....	101
Configuring Syslog Archiving Settings.....	102

CHAPTER 1

WhatsUp Event Archiver Help and Users Guide

In This Chapter

WhatsUp Event Archiver Overview and Architecture.....	1
Deployment Scenarios.....	2
Collection Strategies.....	3
Initial Setup.....	5
Tips and Tricks.....	21
WhatsUp Event Archiver's Feature Areas.....	22
Performing Test Archives.....	24
Setting Up Databases and Making Connections.....	24
Managing Your WhatsUp Event Archiver Licenses.....	30
Troubleshooting / Contacting Technical Support.....	32
Legal Information and License Agreement.....	35
International Issues and Log File Conversion.....	39

WhatsUp Event Archiver Overview and Architecture

WhatsUp Event Archiver Functionality Overview

WhatsUp Event Archiver removes the network administrator's burden of clearing and consolidating Microsoft Windows event logs. WhatsUp Event Archiver automatically manages the event logs on servers across your domains, clearing them and storing them in a variety of formats at a designated time or when they reach a certain file size. After installing the application, you should no longer receive "Administrator Alert" messages that occur when a server log is full. Moreover, by implementing WhatsUp Event Archiver into your domains, you are effectively boosting your organization's security for several reasons. First, you can prevent your event logs from overwriting entries, since WhatsUp Event Archiver clears them when they approach their size limits. Secondly, you can pursue a more aggressive audit policy strategy without having to worry about the resulting log volume. Finally, by retaining all of your event log entries in a central area (either in files or in database entries), you have a comprehensive record of network actions that can prove invaluable to law enforcement agencies, should a problem arise. In addition, by using Ipswitch's WhatsUp Event Analyst product, you can perform analysis on your stored log entries.

By using WhatsUp Event Archiver, you do not need to install client services to all of the servers whose logs you want to archive. Because the WhatsUp Event Archiver Service runs under a domain admin user account, it clears the logs remotely and move them to a centralized location. Also, you can modify archiving parameters for all of your servers at once using a central console, the WhatsUp Event Archiver Control Panel.

In addition to running as an enterprise application in a domain, WhatsUp Event Archiver can also be installed and run on single, non-domain workstations or servers. This is especially useful in high-security networks such as web server farms and demilitarized zones.

Finally, WhatsUp Event Archiver converts event log entries into a variety of different data formats and platforms, also you are not tied to a particular data storage format, as you can collect log entries into EVT/EVTX or text flat files, as well as Microsoft Access, Microsoft SQL Server, and other ODBC databases.

How Does WhatsUp Event Archiver Work?

WhatsUp Event Archiver can be subdivided into 3 major areas:

The Log Registration Database. This database stores all of the information on how to archive the event logs on one or more computers. Once you place a log in the registration database, the WhatsUp Event Archiver Service attempts to archive it when its scheduling criteria are met.

The WhatsUp Event Archiver Service. This is the true 24/7, 365 day workhorse of the WhatsUp Event Archiver product. Running continuously, even without user interaction, it uses the Log Registration database to determine what event logs on what computers to monitor and archive.

The WhatsUp Event Archiver Control Panel. This is the centralized GUI administration console that you use to manage the event logs you have registered with the WhatsUp Event Archiver Service. In many ways, it is a graphical representation of the Log Registration database. However, it also contains many other useful features, such as allowing you to adjust audit policies on computers, and event log settings like file sizes and retention policies. To read more about its interface, see the *WhatsUp Event Archiver's Main Interface* (on page 22) topic.

Deployment Scenarios

Well-connected Local Area Networks

Deploying WhatsUp Event Archiver in a Local Area Network environment is one of the easiest ways to configure and use the application. If all machines whose logs will be collected reside in the same domain (or trusting domains) and are well connected by 10Mbit, 100Mbit, or Gigabit Ethernet links, simply choose one server or workstation that will run WhatsUp Event Archiver. If you have more than 100 servers whose logs must be archived, consider setting up multiple WhatsUp Event Archiver instances on different servers for better load balancing. Then, from the WhatsUp Event Archiver Control Panel, Click the **Tools** menu, and then select **Step-By-Step Wizards**. From the sub-menu, select **Choose Setup Archiving for Multiple Computers at Once** to establish a log collection strategy across multiple machines.

If you have a well-connected LAN with non-trusting domains, set up an WhatsUp Event Archiver system in each separate domain, or create custom domain mappings in WhatsUp Event Archiver and establish a common local administrator account across all systems under which the WhatsUp Event Archiver Service runs.

Wide Area Networks (WANs) or Demilitarized Zones (DMZs)

Deployment of WhatsUp Event Archiver in a WAN environment or DMZ setting is a little more complex, but still manageable.

Starting in Version 7 of WhatsUp Event Archiver, you can also utilize a "Working Directory" that is local to the machine where WhatsUp Event Archiver is installed. If you plan to do a lot of processing to a log after it is archived, such as creating an MD5 hash of the file, converting it to another format (e.g. text file or database table), and/or zip compressing it, WhatsUp Event Archiver will consume substantially less bandwidth if the EVT/EVTX file is first transferred to the WhatsUp Event Archiver server before such processing. You can control how large a file must be before WhatsUp Event Archiver transfers it to the "Working Directory" by selecting *WhatsUp Event Archiver Preferences* (on page 81) from the **Options** menu, and then selecting the Bandwith Optimizer tab. All files larger than the size limit are moved into the Working Directory with log processing performed locally, and all files smaller than the size limit are not moved, with log processing taking place across the network. You can experiment with the size of files that should be copied across the WAN link before processing.

If reliable log archiving cannot be accomplished by using the Working Directory, consider setting up one WhatsUp Event Archiver system at each end of the WAN link. This reduces traffic flowing across the often bandwidth-limited WAN link. If data needs to flow from the remote WAN site to the central network, instruct WhatsUp Event Archiver to push the data upstream using TCP/IP-based ODBC connections, or have WhatsUp Event Archiver compress flat files (EVT/EVTX or Text) into ZIP files and then transport them using traditional Microsoft File and Print Sharing or via an FTP server. Only the finished product of log processing will then be sent over the WAN link.

For database collection in extremely bandwidth-limited WANs, or if auditing requirements produce log file sizes in excess of what WAN link bandwidth can support, contact Ipswitch Support (<http://www.whatsupgold.com/support> (<http://www.whatsupgold.com/support/library/index.aspx>)) regarding the WhatsUp Event Archiver Importer utility, which is designed to process compressed EVT/EVTX and TXT files into a centralized database automatically when these files arrive at a local fileshare.

Collection Strategies

Different organizations have different requirements for preserving log information over time. The following section outlines a few more common collection practices, and how to implement them with WhatsUp Event Archiver.

Long-term Preservation of EVT/EVTX Files, No Analysis Needed

Use this scenario if your organization only requires the preservation of log data in EVT/EVTX formats over time, and seldom, if ever, needs to analyze log entries. In this scenario, WhatsUp

Event Archiver should be configured to save and compress the event log entries into zipped EVT/EVTX files, and then directed to store these compressed flat files on a central file server or FTP server.

Long-term Preservation of EVT/EVTX Files, Periodic Ad-Hoc Analysis Needed

Use this scenario if your organization requires the preservation of log data in EVT/EVTX formats over time, but sometimes needs to do ad-hoc analysis on certain server data within a very narrow timeframe (such as during an audit). In this scenario, configure WhatsUp Event Archiver to save and compress the event log entries into zipped EVT/EVTX AND comma-delimited text files, and then directed to store these compressed flat files on a central file server or FTP server. Duplicating the data into text format is an important feature of this strategy, as it makes import/analysis of the data easier than working with the data in the native EVT/EVTX format.

Long-term Preservation of EVT/EVTX Files, Routine Analysis Needed

Use this scenario if your organization requires the preservation of log data in EVT/EVTX formats over time, yet also must do rigorous, routine analysis on server data on a recurring basis. In this scenario, configure WhatsUp Event Archiver to save and compress the event log entries into zipped EVT/EVTX file for long term storage, extract data out of the EVT/EVTX files for inclusion in a database (Access or ODBC), and then directed to store the compressed EVT/EVTX files on a central file server or FTP server.

Duplicating the data into a database allows the administrator to routinely harness the power of the database platform to perform queries and build reports on the collected data. Such queries and reports can be produced with *lpswitch's WhatsUp Event Analyst product* (<http://www.whatsupgold.com/support/library/index.aspx>), or can be developed in house. Finally, administrators may wish to routinely purge old data (e.g. older than 120 days) from the database server in order to save space. By having the data preserved in EVT/EVTX files as well, the older data can be re-imported at a later date should a need arise.

It should be noted that if more than 10 servers' logs are being imported into a database, an ODBC database server like Microsoft SQL Server should be used instead of Microsoft Access.

No Preservation of EVT/EVTX Files Needed, Routine Analysis Required

Use this scenario if your organization only wants to run reports and build queries against relatively recent sets of event log data. In this scenario, configure WhatsUp Event Archiver to extract the data out of the EVT/EVTX files for inclusion in a database (Access or ODBC), and then directed to delete the backed-up event log files after they are successfully imported.

Administrators may wish to routinely purge old data (e.g. older than 120 days) from the database server (or archive it to tape) in order to save space.

It should be noted that if more than 10 servers' logs are being imported into a database, an ODBC database server like Microsoft SQL Server should be used instead of Microsoft Access.

Initial Setup

The links below will open up topics in the WhatsUp Event Archiver Quick Setup Help Guide.

Installation Requirements (on page 5)

Manually Creating Firewall Exceptions (on page 6)

Before You Begin (on page 6)

Microsoft Vista Requirements and Recommendations (on page 15)

Network and Bandwidth Considerations

Other Recommendations (on page 20)

Syslog Configuration (on page 21)

Configuring the WhatsUp Event Archiver Service Account (on page 89)

Installation Requirements

- § Microsoft Windows XP Professional SP2
- § Microsoft Windows 2003 Server SP2
- § Microsoft Windows Server 2008 / Windows Server 2008 R2
- § Windows Server 2012 and 2012 R2
- § Microsoft Windows 7

Installation is supported on both 32-bit and 64-bit versions of the above operating systems.

Recommended Hardware Requirements:

Dual-core 2GHz or faster processor

2 GB RAM

4 GB Available Hard Disk space minimum for database storage, if detected events are stored in a database. Size depends on the volume of log data stored in a database.

Microsoft Access (optional)

WhatsUp Event Archiver can convert event logs into Microsoft Access database tables, so you will need to have Microsoft Access installed if you wish to view these tables directly. Alternatively you can download WhatsUp Event Analyst to view, filter, and report on data stored in Microsoft Access and Microsoft SQL Server database tables.

Microsoft SQL Server 2005/2008/2012 (Workgroup Edition or Later) OR Microsoft SQL Server Express 2008 (optional)

WhatsUp Event Archiver can also convert event logs into ODBC server database tables. Microsoft SQL Server is the recommended database server for LANs generating a great deal of event log activity.

Manually Creating Firewall Exceptions

During the installation process, WhatsUp Event Archiver creates firewall exceptions for all critical ports. However, if the Windows firewall is turned off at the time of installation, WhatsUp Event Archiver does not create a firewall exception for the Windows firewall. If you decide to turn on the Windows firewall after you install WhatsUp Event Archiver, you must manually create a Windows firewall exception for WhatsUp Event Archiver to work properly.



Note: The steps below may vary slightly based on your operating system

To manually create a Windows firewall exception

- 1 From the Windows Start menu, click **Control Panel**, then select **System and Security**.



Note: Depending on your operating system, your selection may vary. For example, from the Control Panel, you may see an option for Windows Firewall, in which case you would select Windows Firewall.

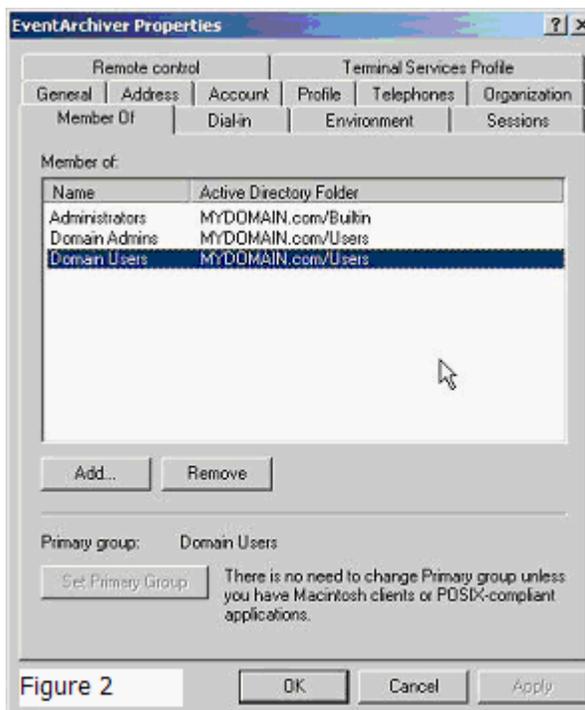
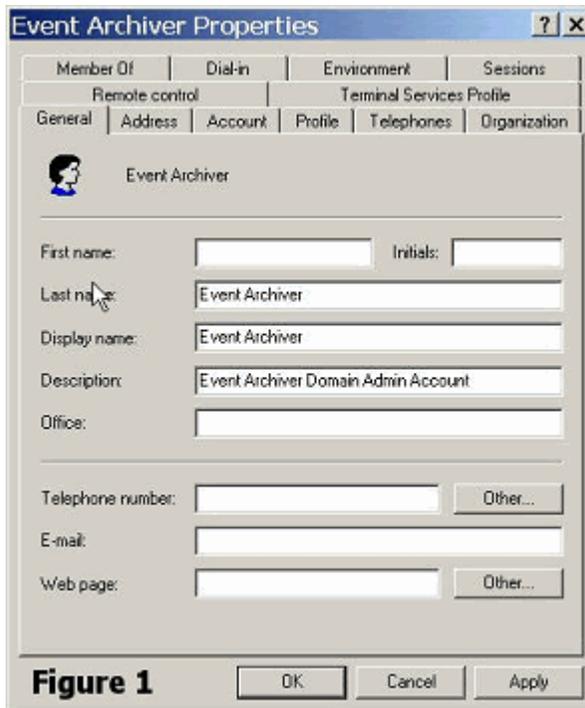
- 2 Click **Windows Firewall**, then select **Allow programs to communicate through Windows Firewall**.
- 3 Click the **Allow Another Program** button.
- 4 Browse to **Program Files(X86) > Common Files > Ipswitch > Syslog Listener**.
- 5 Select the **Service Host** check box, then click **Add**.
- 6 Check the **Domain** check box associated with Service Host.

Before You Begin

1.) Make sure you are logged in with local administrator rights on the machine where you are installing the product. In addition, if the product will be used to collect logs in a domain, make sure you have domain admin rights or OU (organizational unit) admin rights as well. Check these settings in the Active Directory or via the Computer Management snap-in (figure 1 & 2). Otherwise, you will not be able to properly setup the software.



Note: If you do not have access to a full domain admin account in your domain, the software still can be configured by using an account with local Admin rights on all member servers and workstations, such as one created to administer the computers in a specific OU. Consult this KB article for more details, and/or consult with Ipswitch Support if needed.



WhatsUp Event Archiver User Guide

2.) Determine which domain(s) you want WhatsUp Event Archiver to collect event logs from. If you want to collect logs from more than one domain, you must choose a primary domain that is trusted by other domains. WhatsUp Event Archiver refers to this primary domain as the "default domain." When prompted during the first run of the software, enter the default domain you have chosen. (Figure 3).

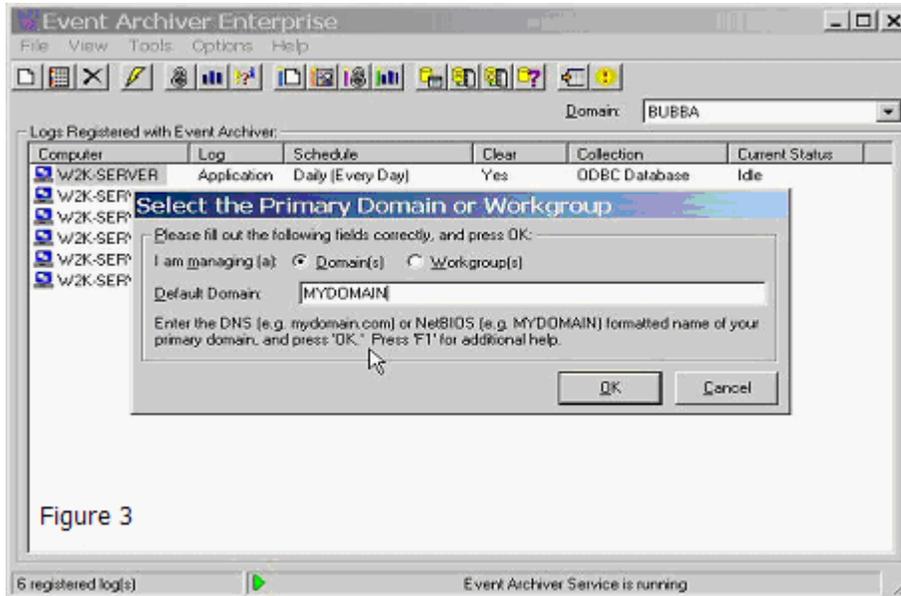


Figure 3



Note: If you are installing WhatsUp Event Archiver to a server or workstation not participating in a domain, please enter its workgroup instead (figure 4). For complicated networks that include WANs and/or demilitarized zones, please read the "Other Recommendations" section listed below, as well as the Deployment Scenarios section of the WhatsUp Event Archiver User's Guide.

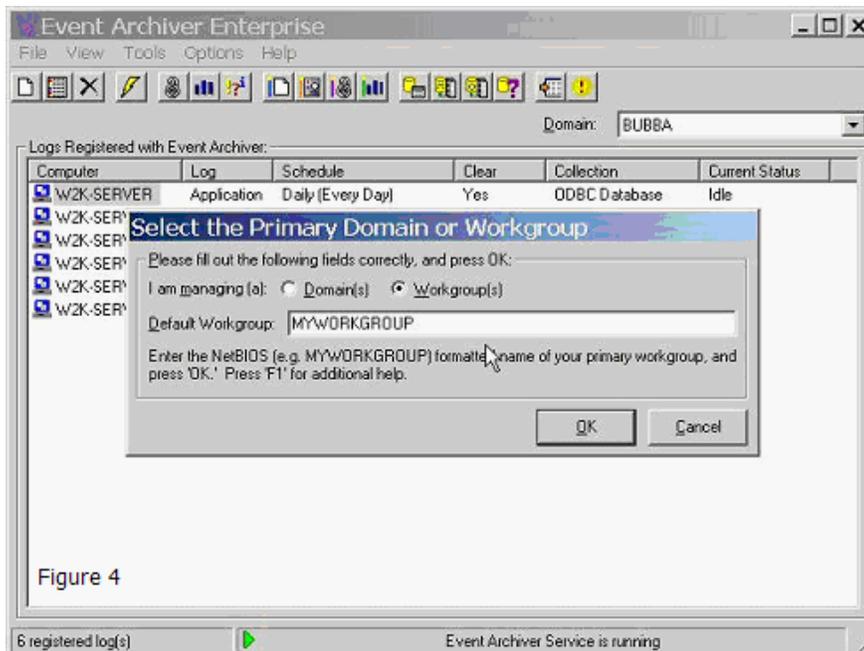


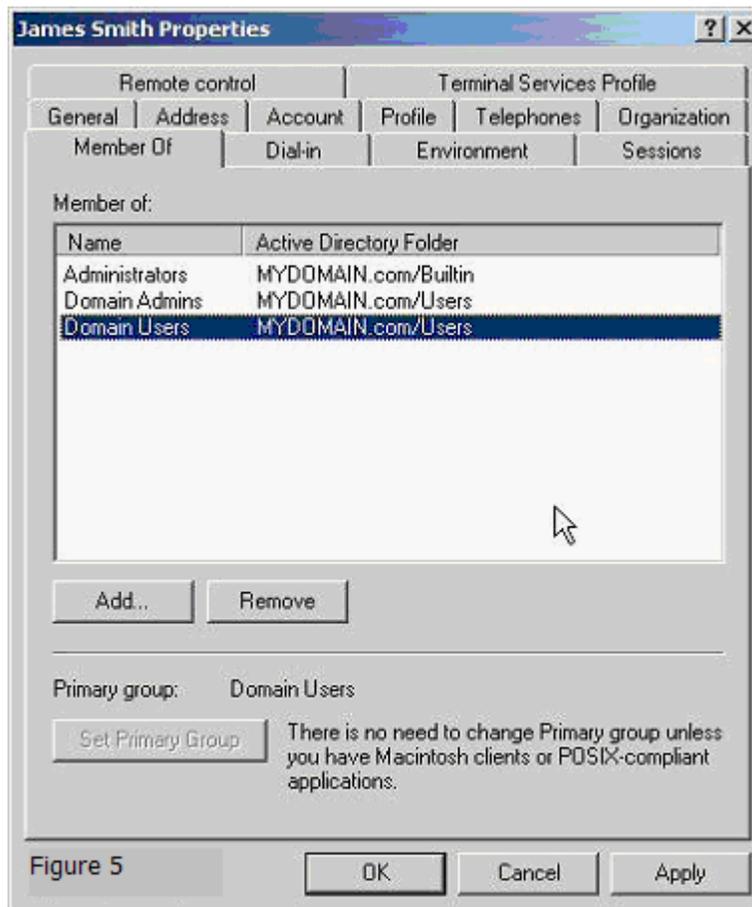
Figure 4

3.) If you do not already have an established user account with domain admin/OU admin rights that services can run under in your organization, create one with User Manager or Active Directory Users and Computers and place it into the Domain Admins/OU Admins group (figure 1 & 2). Also, make sure that it has administrator rights (either by itself or via group membership) on the local machine you installed WhatsUp Event Archiver on.



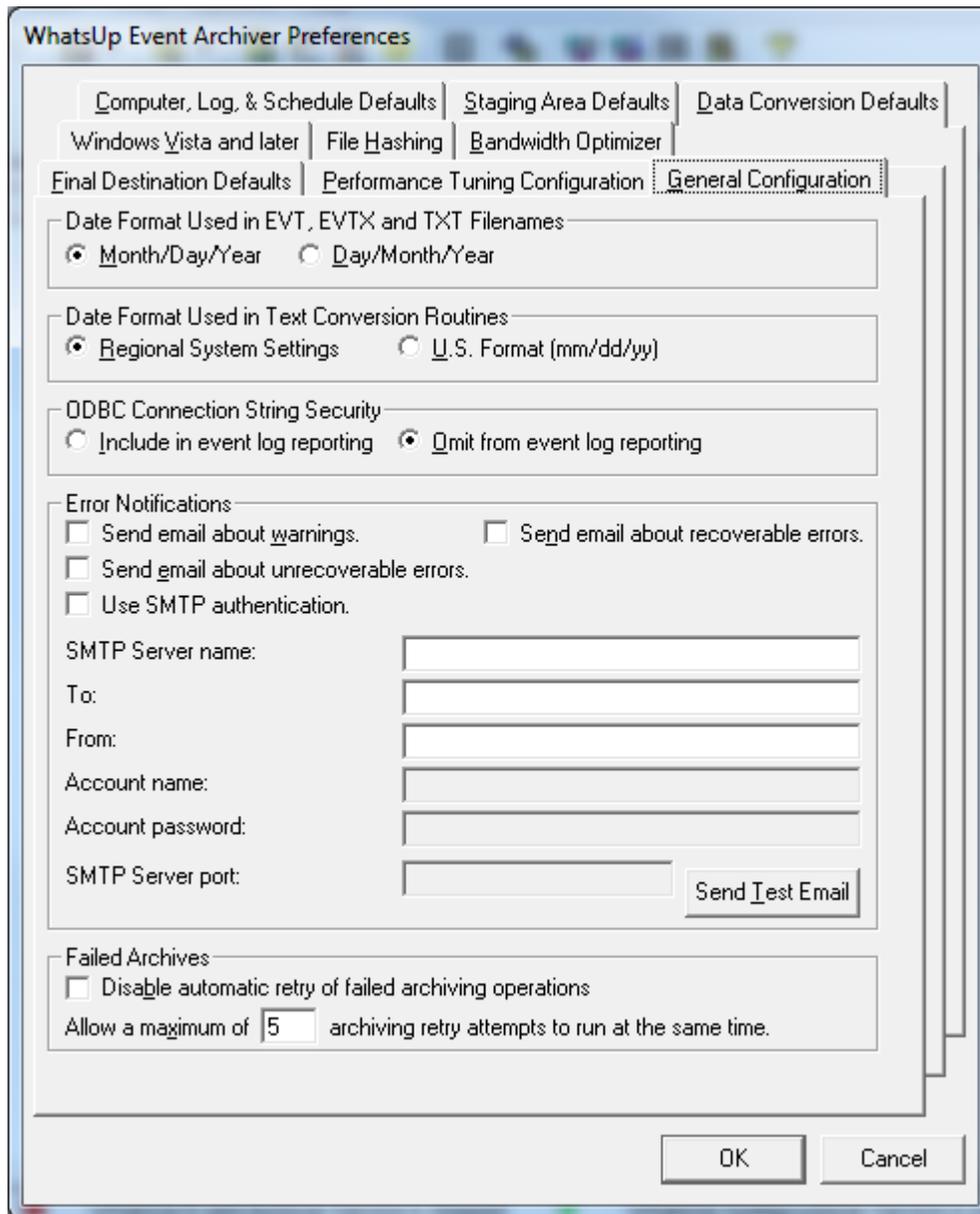
Note: If you are installing WhatsUp Event Archiver to a server or workstation not participating in a domain, please enter a local user who is an Administrator (e.g. SERVERNAME\Administrator).

4.) Make sure you yourself have domain administrator or OU admin rights in the domains/OUs you manage with WhatsUp Event Archiver (figure 5). The WhatsUp Event Archiver Control Panel does do some security intensive tasks, such as changing access control lists, so domain admin/OU admin rights are required to operate it. In the case of a workgroup, you should run the software with a local Administrator account common to all servers and workstations in the workgroup.



5.) If you would like to be notified about archiving errors and warnings, locate an available SMTP server on your network (we recommend the Microsoft Virtual SMTP Server that ships free with Microsoft's Internet Information Server), and adjust its security settings so that the WhatsUp Event Archiver server may relay mail through it. Then, in the **Options** menu > **WhatsUp Event Archiver Preferences** > **General Configuration** tab, check the types of

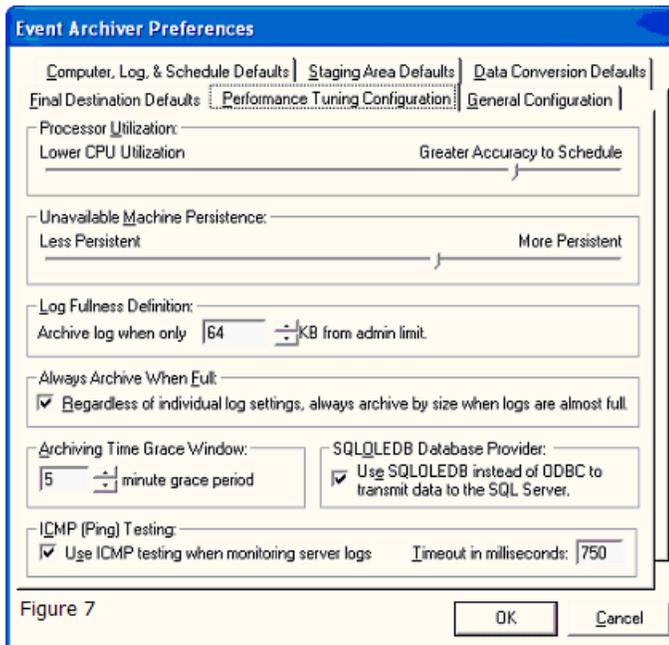
events you want to be notified about, and enter the SMTP server name or IP to relay through as well as a recipient email address that will receive notifications (figure 6).



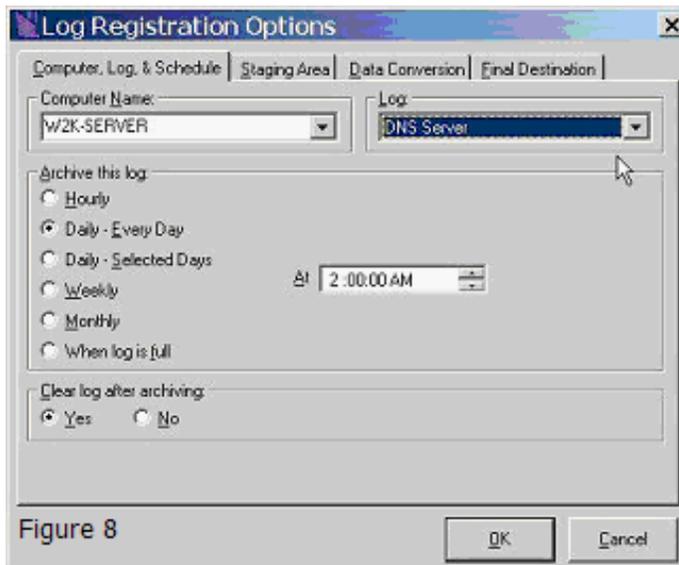
6.) By default, WhatsUp Event Archiver will attempt to periodically ping servers it connects to for log file size monitoring. If you have disabled ICMP on your network, or if you do not use TCP/IP as your primary network protocol, this may interfere with archiving based on file size. If that is the case, you can disable ICMP (Ping) testing in the WhatsUp Event Archiver Preferences Dialog, under the Performance Tuning Configuration Tab (figure 7).



Note: By default, Microsoft Vista workstations have ICMP disabled via the Windows Firewall. If you plan on archiving logs from Vista workstations with WhatsUp Event Archiver based on their file size, you must either a.) disable ICMP (Ping) testing in WhatsUp Event Archiver, or b.) allow ICMP responses from your Vista workstations using Group Policy to control this Windows Firewall setting.



8.) Begin scheduling logs for archiving by either using the **File** menu > **Add a New Log** option (figure 8 thru 11), or the **Tools** menu > **Step-By-Step Wizards** > **Setup Archiving for Multiple Computers at Once** option (figure 12 thru 17). The Setup Archiving for Multiple Computers at Once Wizard allows you to add multiple logs from multiple servers all at once to the WhatsUp Event Archiver server.



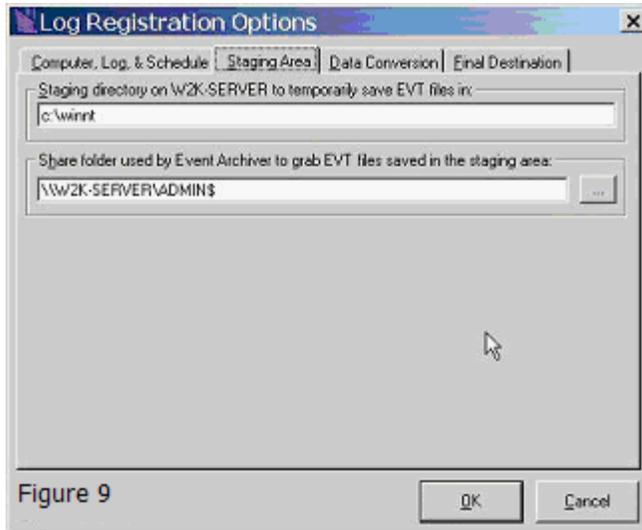


Figure 9

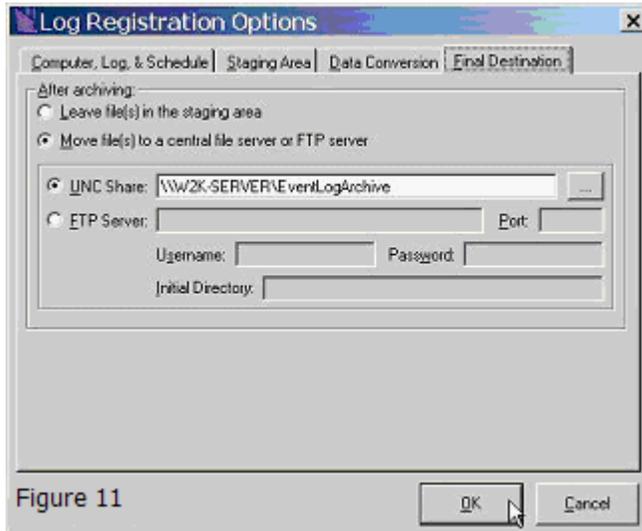
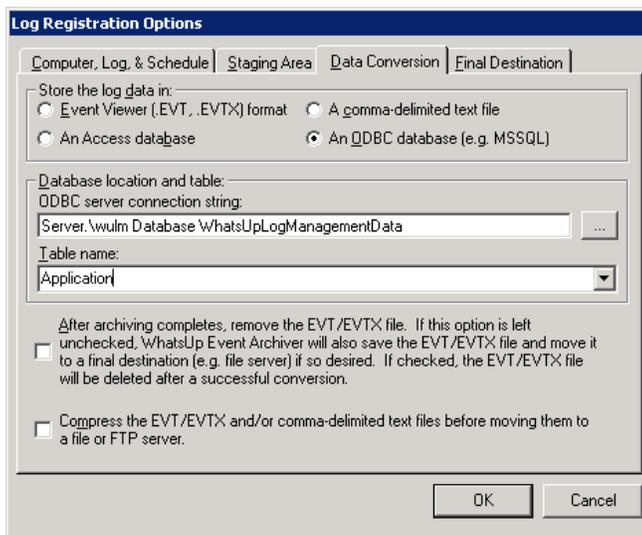


Figure 11

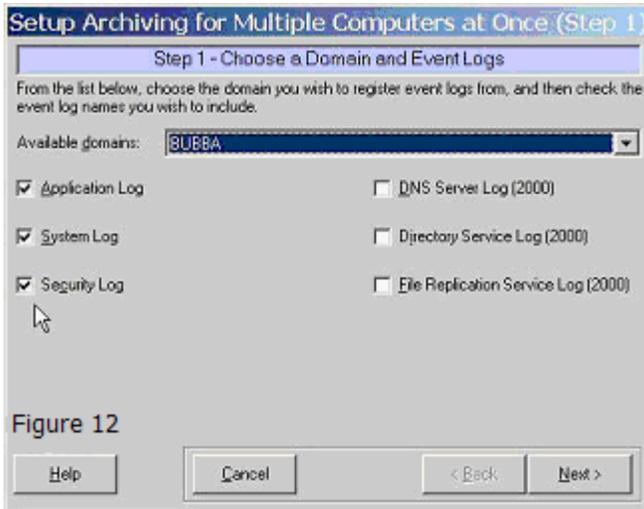


Figure 12



Figure 13

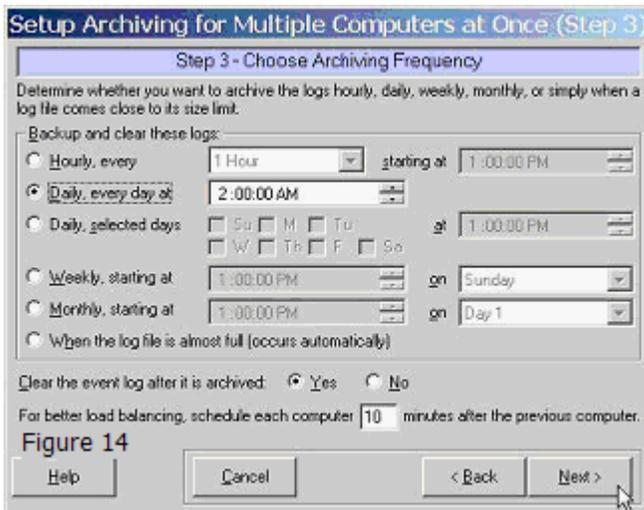


Figure 14



Figure 15

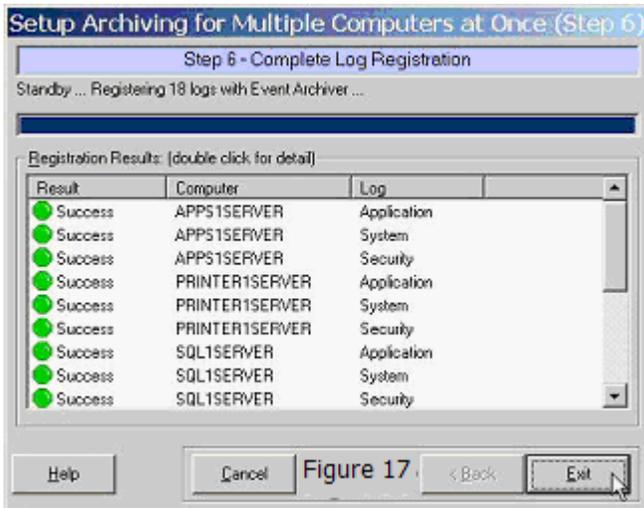
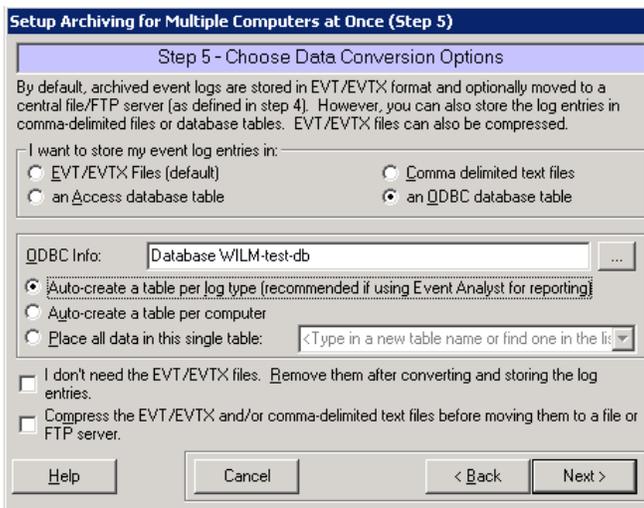


Figure 17

Microsoft Vista Requirements and Recommendations

In Microsoft Windows Vista and later operating systems, the default security settings are much stronger than in previous Microsoft operating systems. This is in keeping with Microsoft's focus on reducing the potential surface area for attacks over the network.

In WhatsUp Event Archiver, we redesigned the software with these considerations in mind, using only the bare minimum of network access techniques to collect and convert the logs. 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.

In WhatsUp Event Archiver version 8 and later, we have added special technology that now allows the software to archive and process EVTX log files from Vista and later operating systems, ***even when installed on a legacy operating system like Windows XP or Windows 2003.*** In that scenario, you will need to add a few additional exceptions to the Windows Firewall in order for EVTX logs to be processed successfully when WhatsUp Event Archiver is installed on a legacy operating system. You will also need to establish a Group Policy to make sure that the Remote Registry Service is running on all of your servers/workstations targeted by WhatsUp Event Archiver.

If you install WhatsUp Event Archiver on a Windows Vista or later operating system, and will be collecting EVTX log files, you will need to allow the **Remote Event Log Management** exception in the Windows Firewall in order for WhatsUp Event Archiver to successfully collect and convert logs from Microsoft Vista machines. The easiest way to do this in a Domain is to use a Group Policy Object that governs all Vista workstations. 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 **seccedit** command line tool.

If you install WhatsUp Event Archiver on a legacy pre-Vista Windows operating system, and will be collecting EVTX log files, you will need to allow the **Remote Event Log Management Exception**, the **File and Printer Sharing Exception**, the **Remote Administration Exception**, and the **Remote Service Management** exception in the Windows Firewall in order for WhatsUp Event Archiver to successfully collect and convert EVTX logs from Microsoft Vista machines. Please review the aforementioned paragraph and screenshots below for guidance on how to do this.

Also, if you want WhatsUp Event Archiver to automatically archive the event logs on Windows Vista machines when the logs are close to becoming full, you will either need to a.) disable ICMP (Ping) testing in the WhatsUp Event Archiver Preferences dialog or b.) create an exception in your Group Policy or Local Security Policy in the Windows Firewall with Advanced Security area to allow ICMP traffic between your WhatsUp Event Archiver server(s) and the Windows Vista systems being managed.

Finally, you will need to establish a Group Policy that makes sure that the Remote Registry Service starts automatically and continues to run on all servers and workstations targeted by WhatsUp Event Archiver over the network.

Figure 1 - Setting the exception manually on each machine with the Exceptions tab

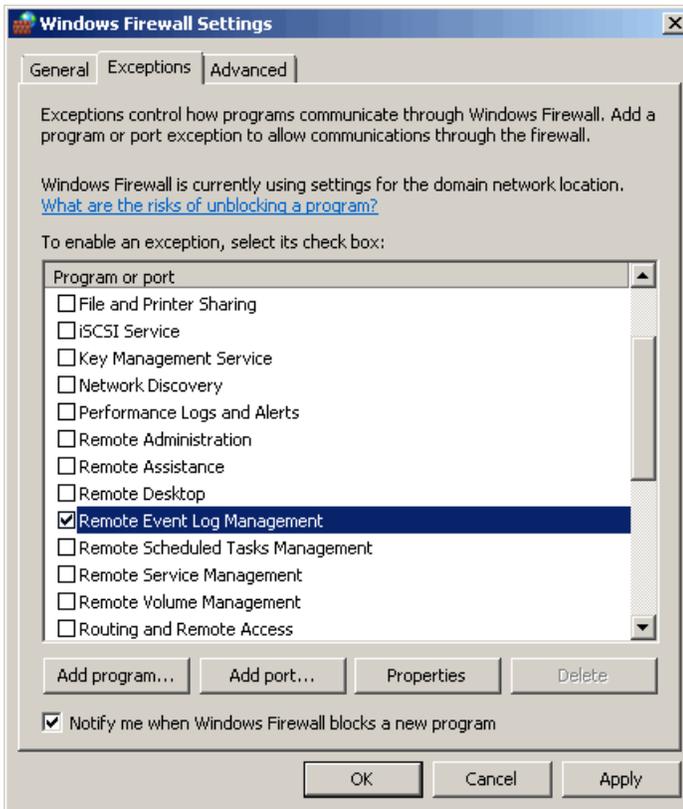
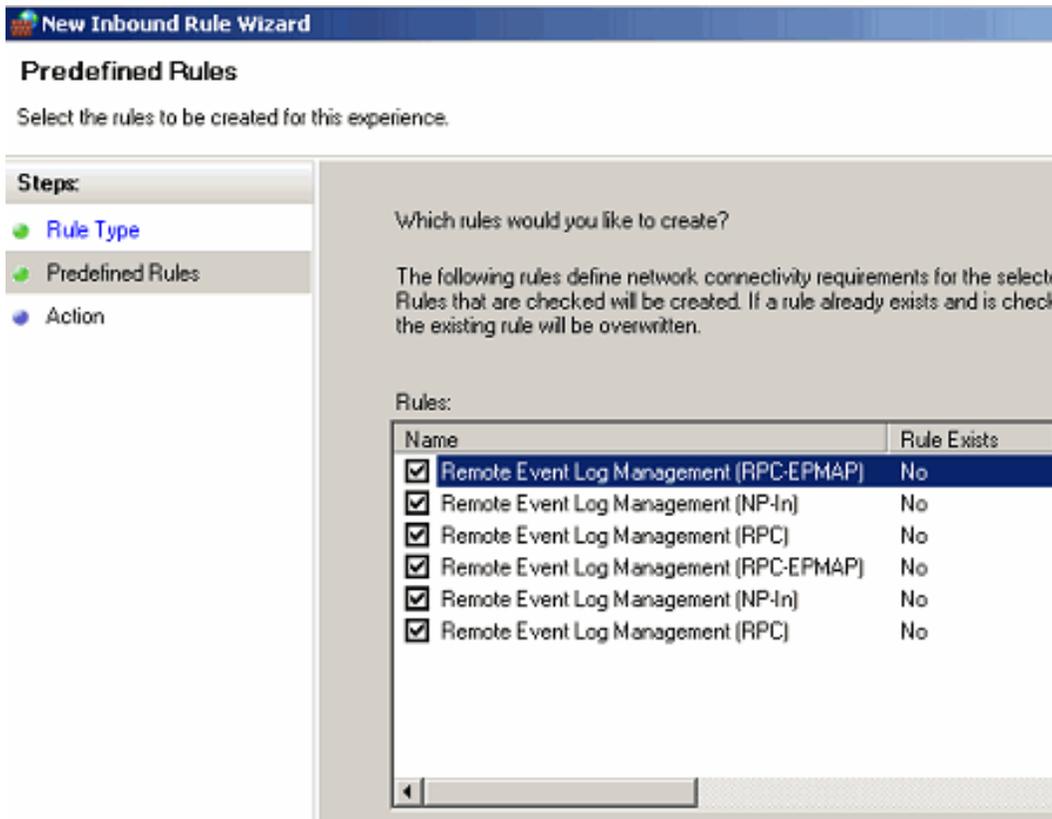
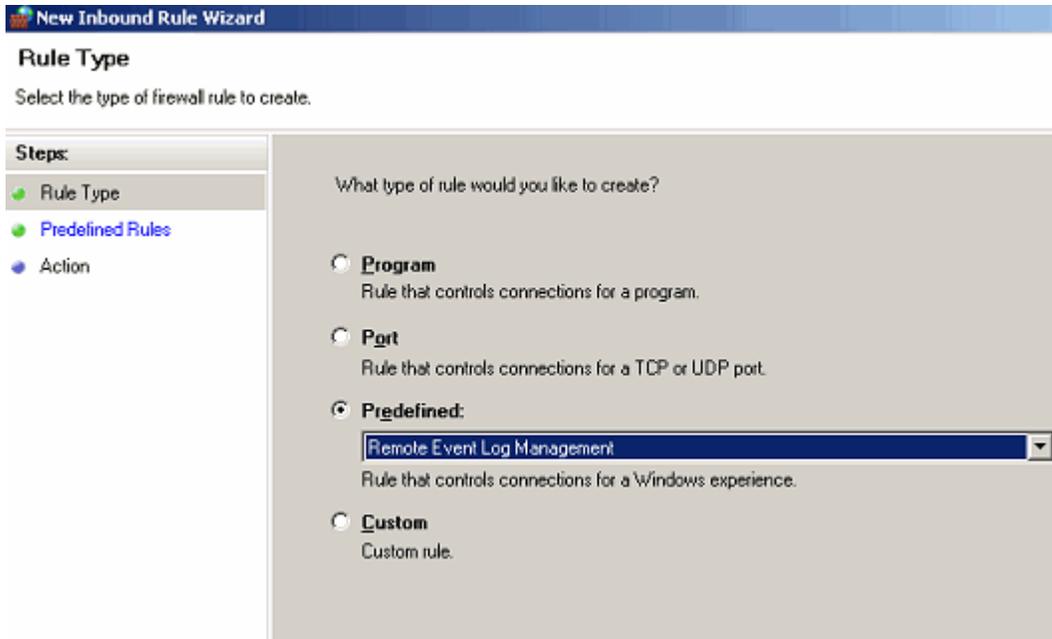
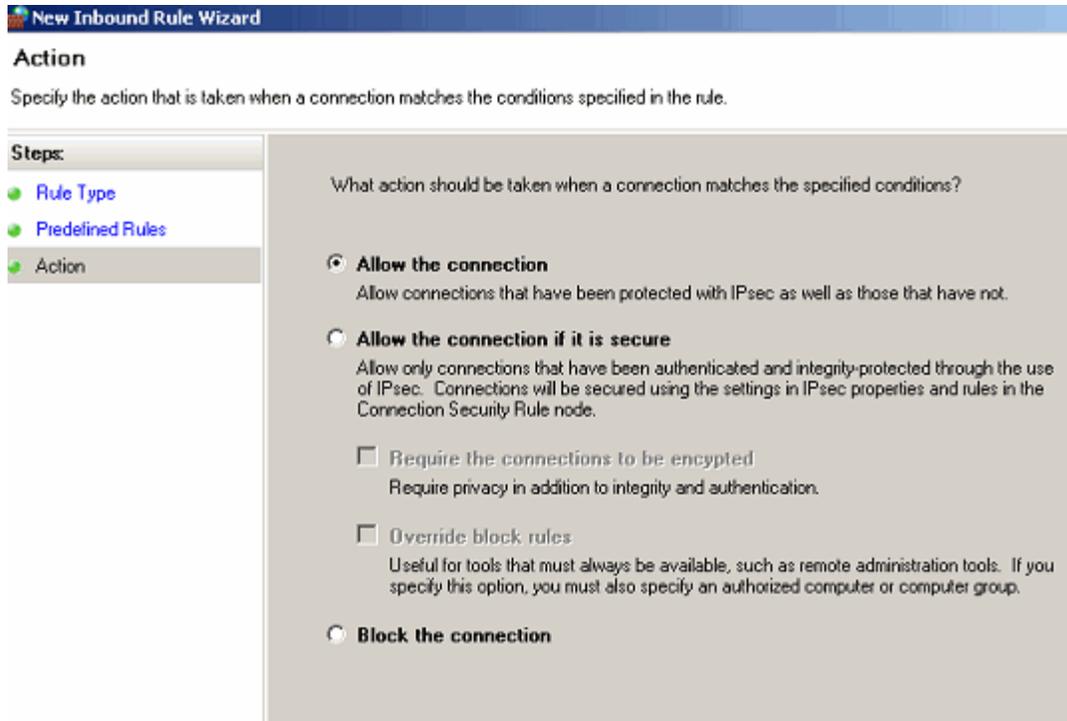


Figure 2a,2b,2c,2d - Setting the exception via a Policy object (local Policy or Group Policy)

 **Note:** Ipswitch recommends creating both an inbound and outbound rule allowing Remote Event Log Management and other exceptions as needed.



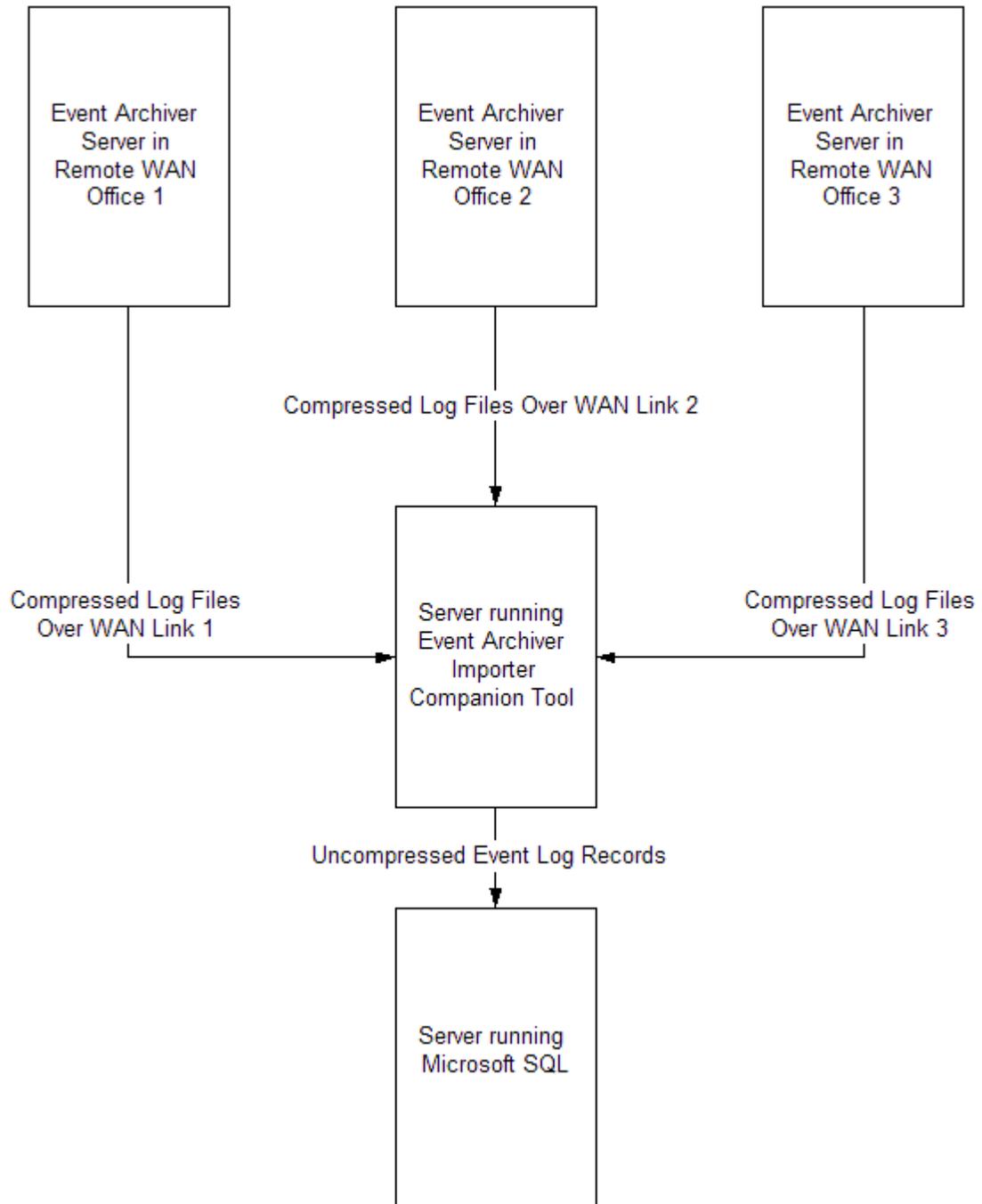




Network and Bandwidth Considerations

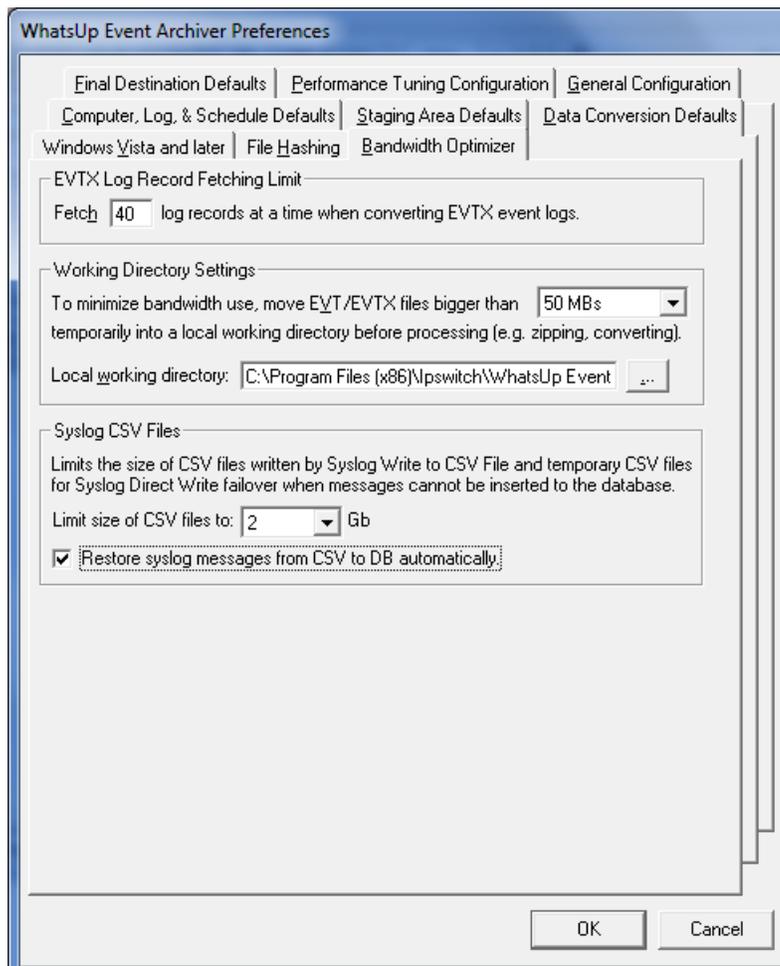
WhatsUp Event Archiver works best in a well-connected LAN environment (e.g. 10 Mbit/100 Mbit/1000 Mbit Ethernet). If you plan on converting event logs into text, Access databases, or ODBC databases, it is best to locate your WhatsUp Event Archiver server "near" your Primary Domain Controller / Active Directory Server for the purpose of account lookups. If you plan to use WhatsUp Event Archiver in a WAN environment, it is beneficial to install an WhatsUp Event Archiver Server locally at each remote end to speed up collection. Moving EVT files over WAN links can prove slow and unreliable.

In many networks, the available bandwidth is such that you can transmit event log records directly to a central database or database server immediately after archiving with WhatsUp Event Archiver. However, if you have a very limited amount of bandwidth from your central office to remote sites containing logs you must archive, yet you still need to bring your event log records into a central database for analysis, contact Ipswitch Support to request a copy of the WhatsUp Event Archiver Importer companion tool. The WhatsUp Event Archiver Importer tool can be installed on a server at your central office and then be instructed to monitor a local folder or share where compressed copies of your event logs are arriving from your remote sites. When the compressed logs arrive in the folder, the WhatsUp Event Archiver Importer tool will automatically uncompress them and read their contents directly into a Microsoft SQL database server. The following diagram illustrates this process:



Starting in Version 7 of WhatsUp Event Archiver, you can utilize a "Working Directory" that is local to the machine where WhatsUp Event Archiver is installed. If you plan on doing lots of processing to a log after it is archived, such as creating an MD5 hash of the file, converting it to another format (e.g. text file or database table), and/or zip compressing it, WhatsUp Event Archiver will consume substantially less bandwidth if the EVT/EVTX file is transferred first to the WhatsUp Event Archiver server before such processing. You can control how large a file must be before WhatsUp Event Archiver will transfer it to this "Working Directory" by selecting WhatsUp Event Archiver Preferences from the Options Menu, and then selecting the Bandwidth Optimizer Tab. All files larger than the limit will be moved into the Working

Directory with log processing performed locally, and all files smaller than the limit will not be moved, with log processing taking place across the network.



Other Recommendations

If you are an administrator of several different workgroups, or of multiple OUs in a larger Active Directory, but possess a common domain or local account with Administrator rights on the various workgroups or servers, you can create a **custom domain** to keep track of all of the managed computers in a logical group. Likewise, if you are a domain administrator who wants to separate different servers (e.g. by role) into different logical groups, a custom domain affords this flexibility. Computer to custom domain mappings can be established under the Options Menu with the Manage Custom Domain to Computer Mappings option. Once computer names have been mapped to custom domains, you can work within a custom domain by selecting in the upper right hand corner of the WhatsUp Event Archiver Control Panel.

Automatic database maintenance of Microsoft Access MDB files and Microsoft SQL Server database tables can be controlled by choosing the Setup/Adjust Automatic Database Maintenance item under the Tools menu. Event Archiver can be instructed to automatically prune older data out of MS SQL database tables, as well as automatically archive MDB files nearing their file size limit, all on a scheduled basis.

If you plan to collect event logs from many different servers (e.g., over 50), it is beneficial to space out their collection schedules. Having WhatsUp Event Archiver attempt to collect 20 different event logs at the same time can be a severe drain on server resources. Therefore, it is best to space out collection times and dates. In fact, we recommend the "When the log is full" scheduling option, because server event logs often reach their maximum sizes at different times from one another.

Syslog Configuration

Use this tab to set Port numbers for each syslog mode. To disable a specific mode, type "0" in the corresponding field.

IP Version 4 - UDP. If you are using Internet protocol version 4 and user datagram protocol for syslog messaging, type the associated port number.

IP Version 6 - UDP. If you are using Internet protocol version 6 and user datagram protocol for syslog messaging, type the associated port number.

IP Version 4 - TCP. If you are using Internet protocol version 4 and transmission control protocol for syslog messaging, type the associated port number.

IP Version 6 - TCP. If you are using Internet protocol version 6 and transmission control protocol for syslog messaging, type the associated port number.

Tips and Tricks

- 1 Install WhatsUp Event Archiver on more than one server.** By installing the program on more than one server, you can make different servers manage different sets of computers on your network. For example, you could have 7 archiving servers, each managing 100 computers to better optimize your network traffic according to topology: where you have switches as opposed to hubs on the LAN. Plus, this reduces the processor and memory load on each WhatsUp Event Archiver server.
- 2 Avoid scheduling archiving times too close to one another.** If you elect to collect your logs daily, weekly, or monthly, ensure you space out the collection times. Even a few minutes in between logs can make a noticeable difference. You can also schedule logs to archive when they approach their size limits. Because logs on different computers grow at different rates, this guarantees that the archiving process is spread out across a wide range of times.
- 3 Collect the logs as EVT/EVTX files as opposed to converting them to text files, Access, or ODBC databases.** It takes extra processor overhead to convert saved log files into other formats, such as Access or ODBC databases. Collecting them in their native EVT/EVTX format reduces work for the WhatsUp Event Archiver Service. However, if you spread out the collection times well enough as mentioned in Tip 2, converting into different data formats should present no problems.
- 4 Match platforms.** If you plan on converting event log entries into text files, Access databases, or ODBC databases, install WhatsUp Event Archiver on the platform (e.g., Windows 2003) that matches the majority of your servers and workstations. If you match platforms, WhatsUp Event Archiver can take advantage of caching which can increase data conversion speed and reduce network bandwidth.

- 5 **Compress data.** If you are collecting logs in EVT or text formats, you may want to compress the files after each archive. Compressing log files can shrink them down to 5% of their original size and will greatly reduce the amount of storage needed on the final destination file server.
- 6 **Use the Working Directory.** WhatsUp Event Archiver allows you to first transport archived EVT/EVTX files to a temporary working directory local to the machine running WhatsUp Event Archiver. This greatly speeds up the time needed for log processing, such as MD5 hash calculation, zipping, and conversion into other formats, and also saves bandwidth. You can control the size of files transported to this directory, as well as the location of the directory here.

Did you know that you can consolidate event log entries from untrusting domains into a single database? If you have a Microsoft SQL Server on a TCP/IP based LAN, you can set the SQL Server up so that it uses standard authentication (as opposed to Windows authentication). After defining a username and password for the SQL server, you can make WhatsUp Event Archiver servers from different domains send all of their log entries to that central server. Read more about how to work with ODBC databases in the Log Registration Options dialog section of this help file.

Visit the *Ipswitch Support* (<http://www.whatsupgold.com/support/library/index.aspx>) website to find additional information and upgrades for this product.

WhatsUp Event Archiver's Feature Areas

WhatsUp Event Archiver's Main Interface (The Control Panel)

In order to make the administration of the WhatsUp Event Archiver system as simple as possible, WhatsUp Event Archiver ships with a GUI console called the WhatsUp Event Archiver Control Panel. From the control panel, you can schedule new logs for archiving, edit the archiving properties of existing logs, and delete logs from the system. In addition, the WhatsUp Event Archiver Control Panel comes with step-by-step wizards that can help you to register logs from multiple computers at the same time, *unify the audit policies* (on page 70) across Windows machines in your domains, and *unify the event log settings* (on page 72) (such as log size and retention intervals) across multiple machines. Here are the 5 components of the WhatsUp Event Archiver Control Panel:

WhatsUp Event Archiver Control Panel Menu

Each of the five Control Panel menus has a different set of commands to help you manage your event logs. In order to find out more about each menu, click on each menu name below:

- § *File* (on page 41)
- § *Syslog* (on page 42)
- § *View* (on page 43)
- § *Tools* (on page 44)
- § *Options* (on page 43)
- § *Help* (on page 45)



Note: By right-mouse clicking on any scheduled computer log in the Logs Collected Listing, you can pull up a context menu that mimics the commands of the file menu.

Toolbar

The toolbar serves as a quick access mechanism to many of the commands present in the 5 Control Panel menus. If you hover over any toolbar button, descriptive text will appear indicating what menu option the button controls.

Domain Chooser

The domain chooser appears as a pull-down list in the upper right hand corner of the control panel. The list contains the primary domain you chose when you installed the software, as well as any other domains that trust the primary domain and custom domain sets of computers that you personally define. Selecting a new domain causes the Logs Collected Listing to refresh itself, listing only the computers and logs associated with that domain.

Logs Collected Listing

The Logs Collected Listing shows you at a glance the logs (and their corresponding computers) that the WhatsUp Event Archiver Service is currently managing. You can sort this list by heading by clicking on any of the column headers. The following icons displayed by the computer names have special meanings:

Icon Legend:



- The computer is idle, no archiving operation is being carried out



- An error occurred when the last archiving operation was attempted. This can occur when 1.) you have specified an incorrect directory on a remote server where EVT/EVTX files are saved initially (e.g. D:\Winnt instead of C:\Winnt), 2.) the particular log does not exist on a given machine (e.g. Windows NT 4 machines don't have DNS Server or Directory Service logs), or 3.) the machine was not present on the network at its scheduled time. Launch the *Log Registration Options* (on page 46) dialog to double check the local path and/or log type you have selected.



- An archiving operation is currently underway. You cannot edit or delete a log during an archiving operation.

Status Bar

This bar at the bottom of the Control Panel always indicates two things: the number of logs managed in a given domain, and the status of the WhatsUp Event Archiver Service.

Performing Test Archives

If you would like to perform a test archive operation to verify that the archiving settings you have chosen work properly, highlight a log in the WhatsUp Event Archiver Control Panel, and select the **Archive Now!** option from the **File** menu. You can only select one log on one server to test at a time.

After WhatsUp Event Archiver indicates that the archiving operation has initiated, select **View WhatsUp Event Archiver Log Entries** from the **Tools** menu, and check for information, warning, and error events logged in the local Application log from the WhatsUp Event Archiver Service. A series of all information events (blue icons) indicates that all archiving operations (staging area backup, compression, data conversion, and/or relocation) were successful. If warning events (yellow icons) are present, it may mean that the WhatsUp Event Archiver Service detected a non-critical problem. If error events are present (red icons), one or more of the archiving operations failed for a particular log. Click an event to determine what may be the root cause of the error, which displays detailed information in the Description field.

If test archives perform correctly but scheduled archives fail, you may be experiencing a permissions issue with the WhatsUp Event Archiver Service. Test archives run under the context of your logged-on (interactive) user account. Scheduled archives run under the context of the WhatsUp Event Archiver Service account. Double-check the WhatsUp Event Archiver Service account to verify that it is a member of the Domain Admins and/or local Administrators group. More troubleshooting tips can be found *here* (<http://whatsupgold.force.com/kb>).

Setting Up Databases and Making Connections

To prepare a new ODBC-compliant database to receive logs from WhatsUp Event Archiver, simply create (or have your Database Administrator create) a new database (or schema/tablespace) on your database server with default settings. Ipswitch recommends Microsoft SQL Server 2005/2008 or later as your database server back end, as these platforms have been tested and work well with WhatsUp Event Archiver.

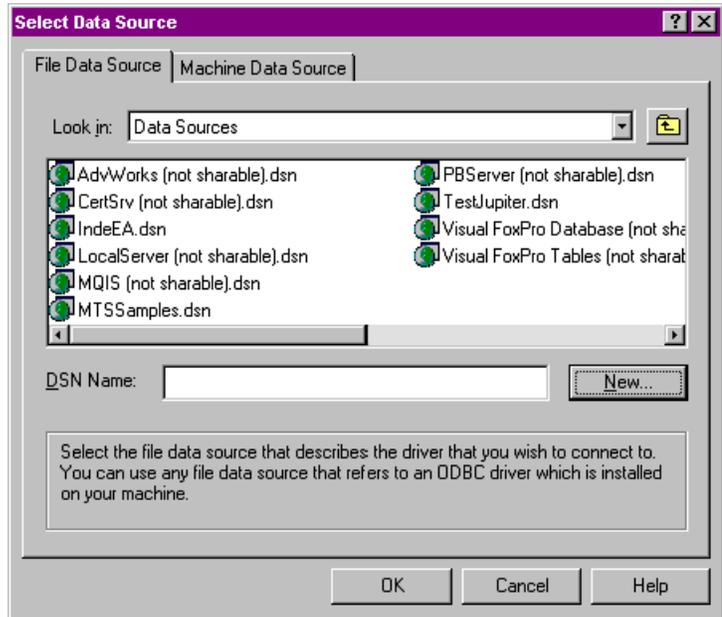
Then, if necessary, create a new database login that has full read and write permissions to this database. In Microsoft SQL Server, this username and password should be a standard security login as opposed to an Windows-account integrated login. If you do opt to use integrated Windows security, make sure that the WhatsUp Event Archiver Service account has full read and write permissions to the database.

Once the database and login has been created, use the ODBC connection manager that can be opened from several WhatsUp Event Archiver dialogs to create a connection string to that database. The most important thing to remember is that this connection should be set up as a File DSN, as opposed to a System DSN.

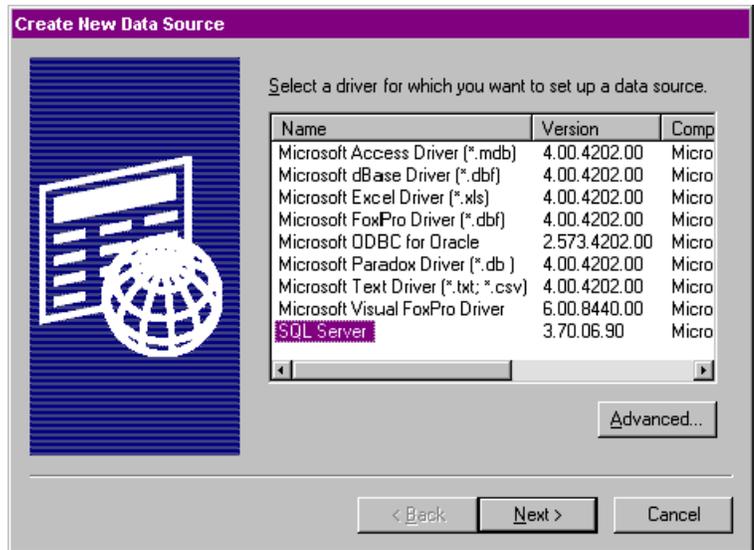
Once the File DSN is created, you do not have to change these ODBC settings again, unless your database server or login is modified. Simply choose your previously-created File DSN by name whenever WhatsUp Event Archiver raises the ODBC connection manager dialog.

Here are sample screen shot walkthroughs of how to set up a File DSN for a Microsoft SQL Server:

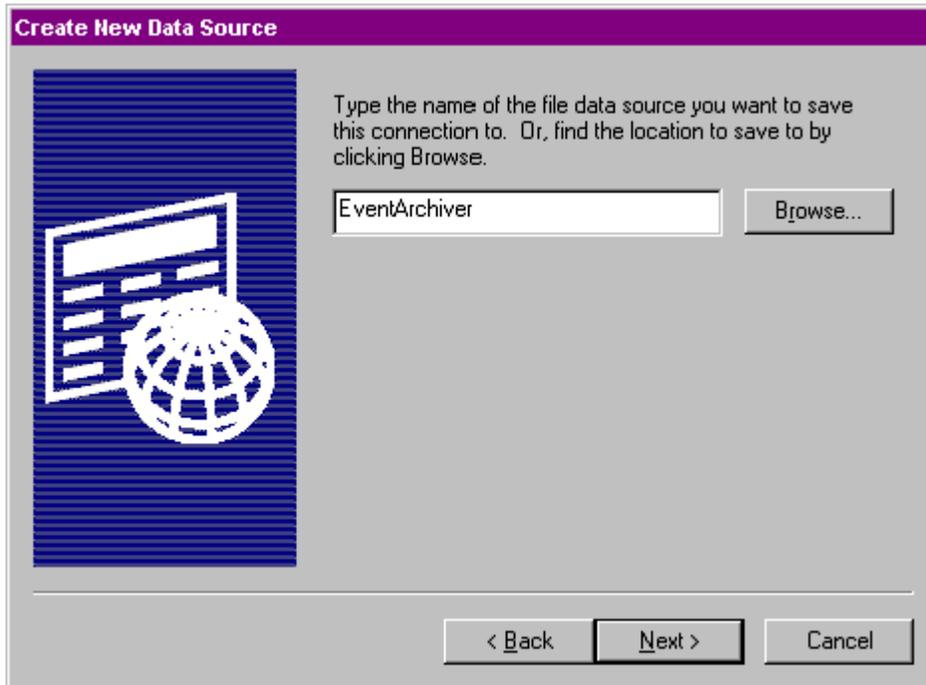
CREATING AN ODBC FILE DATA SOURCE FOR MICROSOFT SQL SERVER



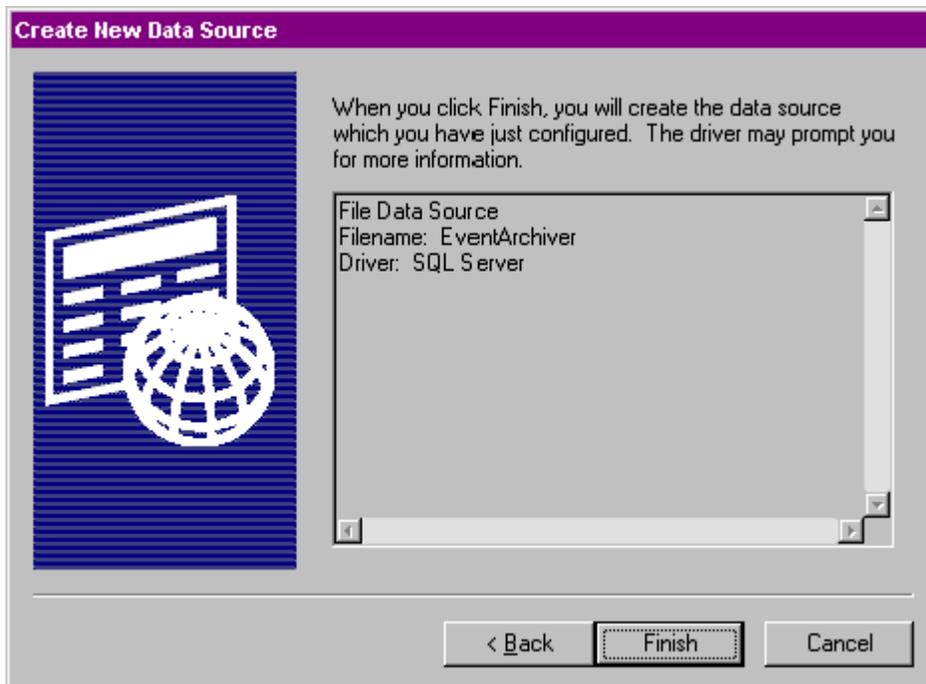
Open the Data Sources (ODBC) Applet under the **Control Panel** or **Administrative Tools**, select the **File Data Source** tab, and then click the **New** button.



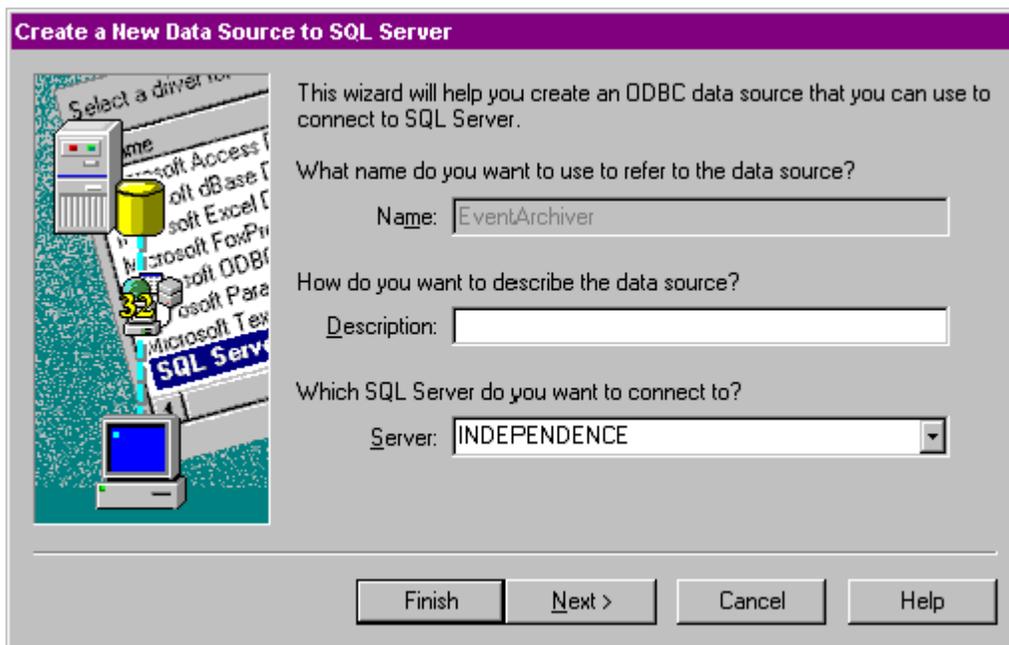
Select the **SQL Server** driver.



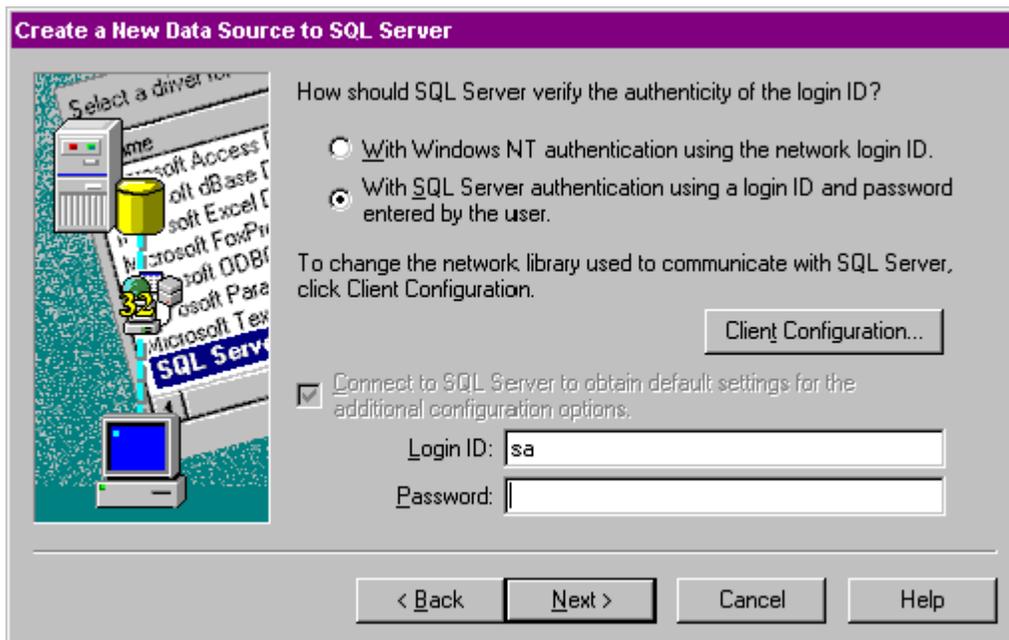
Type a name for the Data Source you are creating.



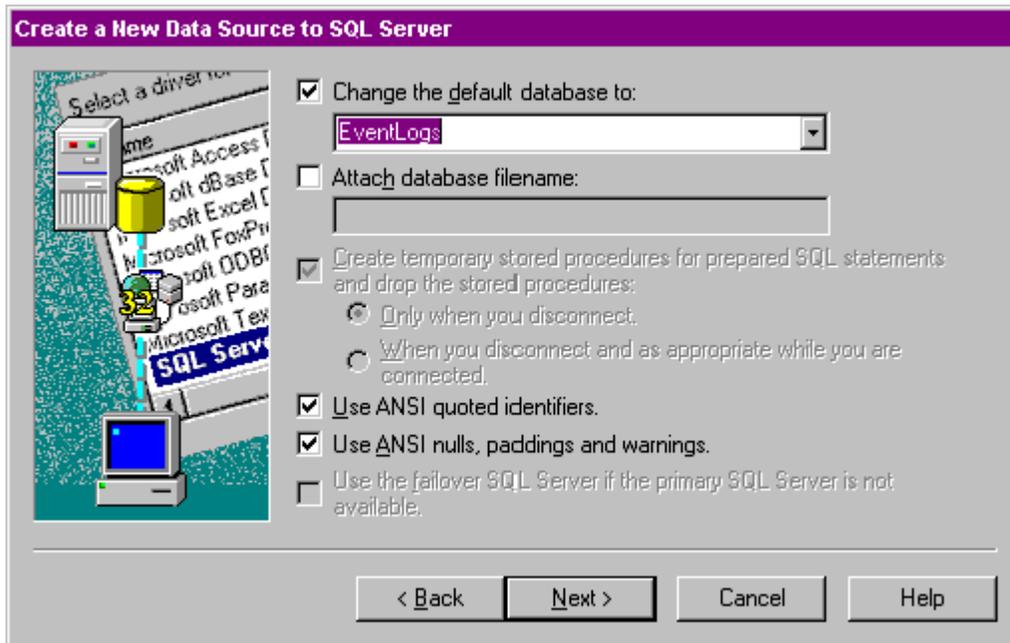
Click **Finish**.



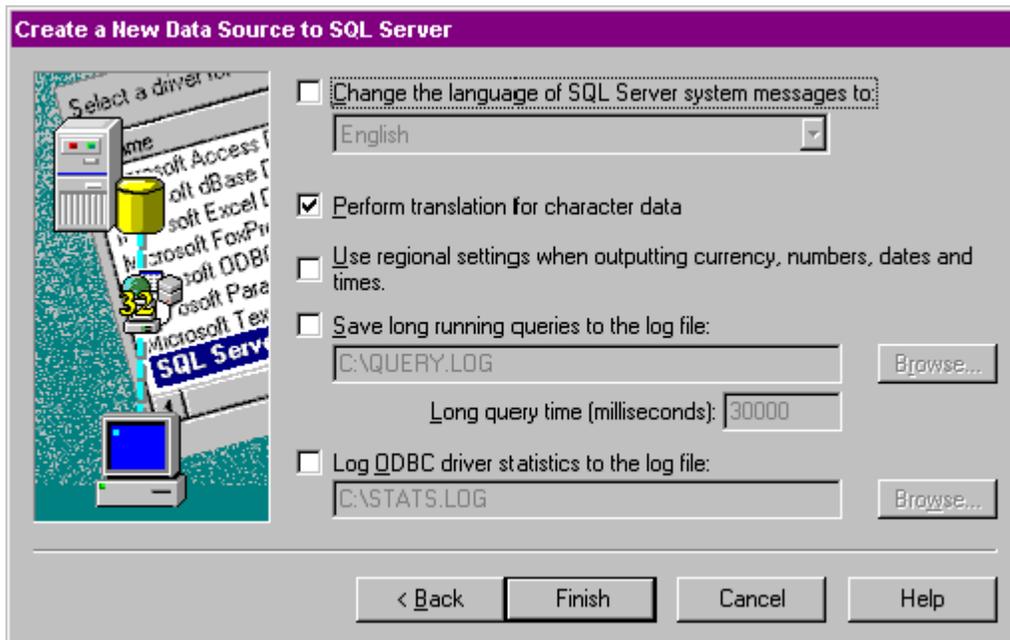
Select the SQL Server you want to connect to, or type in the IP address of the server.



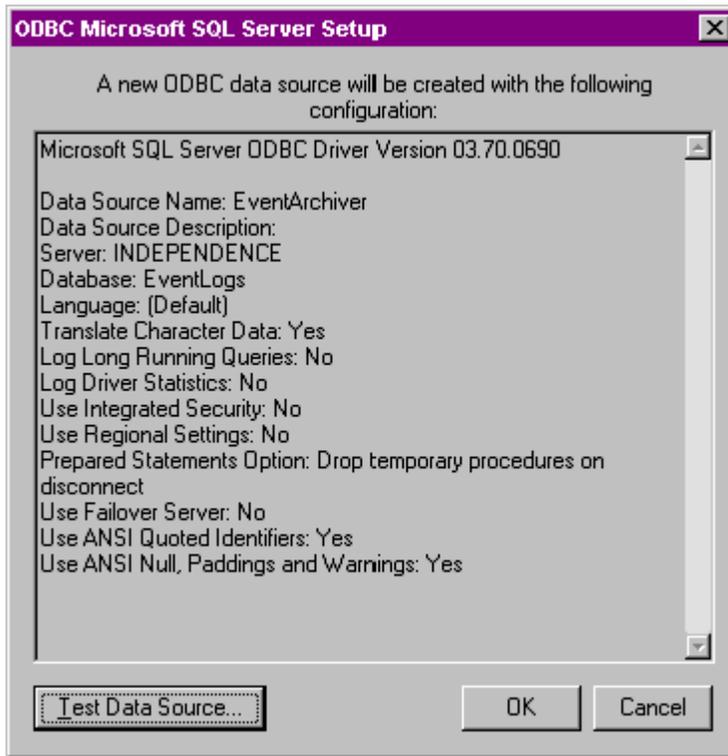
Choose an authentication method. SQL Server authentication is recommended.



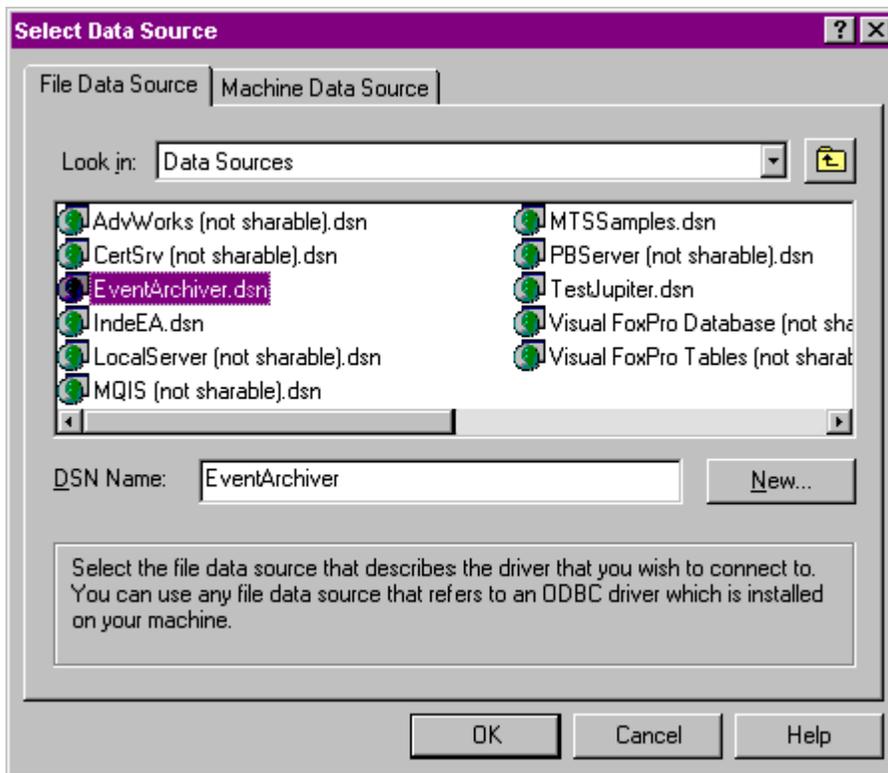
Change the default database to the database your DBA created to store your event logs.



Leave these settings on their defaults.



Test the data source, and then click **OK** if the test succeeds.



Now, whenever specifying an ODBC data source inside WhatsUp Event Archiver, select the File data source you created in these series of steps.

Managing Your WhatsUp Event Archiver Licenses

When you install WhatsUp Event Archiver, it automatically runs in 30-day evaluation mode, and it allows you to archive event logs from up to 50 different computers. To registering WhatsUp Event Archiver, complete the following steps every time you need to purchase licenses.

Before your purchase and how to purchase:

When you are evaluating WhatsUp Event Archiver for the first 30 days, you can use it to archive logs on 50 different computers. Registering and purchasing licenses is simple, and is handled by the License Manager dialog found under the *Help* (on page 45) menu. Whenever you need to add more licenses, you generate an encrypted key that you send to Ipswitch or an authorized reseller. After receiving payment (credit card or PO) for the licenses, we'll issue you a license upgrade key. If you would also like to use WhatsUp Event Archiver to collect logs from Windows NT, Windows 2000 Professional, Windows XP, Windows Vista, or Windows 7, we have special discounted license rates for workstations.

Call us at **781-676-5700** or visit the *Ipswitch Support Site* (<http://www.whatsupgold.com/support/index.aspx>) to make a purchase with credit card, purchase order, or to find resellers in your area.



Note: WhatsUp Event Archiver licensing is determined by the total number of computers you collect logs from, not by the computers actually doing the collecting.

After your purchase, but before your registration:

Shortly after processing your order, you will receive an email with instructions on how to activate your software over the Internet. This email message will contain your service number. Enter this service number, along with your name, organization, and email address, in the **User Information** section of the License Manager. If you have multiple monitoring stations to configure (see below), repeat this step at each station.

Determine how many archiving stations (i.e. separate WhatsUp Event Archiver installations) you want to set up. An archiving station is simply a spare (but reliable) XP/2003/Vista/2008/Windows 7 workstation or server where WhatsUp Event Archiver is installed. If you have a well-connected domain (10 MBit or greater LAN), we recommend only managing a maximum of 100 servers per archiving station. The actual number may vary depending on how much audit data your servers produce. We recommend setting up collection stations in evaluation mode first to check load balancing before you register the software. If you have standalone servers in a demilitarized zone or other isolated network, you can install WhatsUp Event Archiver to each standalone machine, configuring it to only archive itself. If you have WAN network links, it's best to set up a WhatsUp Event Archiver archiving station at each of the remote ends, as to minimize traffic WAN traffic during archiving and log conversion.

After all archiving stations are configured appropriately, you can license each archiving station independently by going to the **Help > Register WhatsUp Event Archiver** menu item, and preparing an Internet registration at that station.

In general, it is best to configure the stations first (since WhatsUp Event Archiver is fully functional during the first 30 days), and then register after the configuration.

Here's a hypothetical example of how your registration might look after configuring your collection stations:

Collection Station 1: 25 servers in domain / LAN

Collection Station 2: 1 server in a DMZ / Firewalled LAN

Collection Station 3: 1 server in a DMZ / Firewalled LAN

Collection Station 4: 5 servers in a domain / WAN remote end

In this scenario, logs are being collected on 32 servers, spread out over 4 archiving stations. This means that you would submit a separate registration, one for each archiving station, specifying the number of servers you will manage at that station (e.g. 25 at Station 1, 1 at Station 2, 1 at Station 3, and 5 at Station 4).

The Ipswitch's Fulfillment Team will respond within 24 hours with an unlocking code for each archiving station once they receive your request.

After Station Configuration:

Indicate how many servers and workstations whose logs you want to archive in the **Request Licenses** section of the License Manager.

If you are directly connected to the Internet, click the **Send request via the Web** button. Your license request is transmitted directly to Ipswitch, Inc. via the Web.

If you are not directly connected to the Internet, click the **Export this request to an HTML file** button. An HTML file is generated at the location on disk you specify. Transport this HTML file via your network, or via removable media, to a machine with Internet access. Open the HTML file on your Internet-connected machine, and follow the instructions to request licenses via the web.

After you receive an activation email, paste your response key into the **Response Key** field. After entering the key, click the **Unlock/Add Licenses** button. If the key is validated successfully, WhatsUp Event Archiver registers with the number of licenses you requested.

Restart the WhatsUp Event Archiver Control Panel.

Repeat these steps for each archiving station needing licenses.

If you need to add licenses as a later date:

If, after registering WhatsUp Event Archiver, you discover you need more licenses, you can repeat the steps above to get a license upgrade response key, and increase the number of licensed computers.



Note: Only enter the number of licenses you want to add to the existing total to create a new license limit. The response you receive from Ipswitch will increase your number of licenses to the desired total.

- § **Registration Status.** Displays whether WhatsUp Event Archiver is running in evaluation mode or has been registered.
- § **Licensed Computer Total.** Displays the number of computers you can archive event logs from this station.
- § **User Information.** Enter end user information associated with your purchase of WhatsUp Event Archiver. Make sure the email address used here is the same email address that should receive the unlocking codes.
- § **Send Request Via the Web.** Click to submit your registration request directly to Ipswitch's registration system via our website. This requires an active Internet connection.
- § **Export This Request to a HTML File.** Click to build an HTML file that you can transport to a machine connected to the Internet. Then, once the HTML file is transferred there, you can open it in any web browser and submit your information to the registration system on our website.
- § **Unlock/Add Licenses.** After entering your unlocking code (response key) into the Response Key field, click this button to activate the software. Likewise, if you have requested more licenses for a copy of WhatsUp Event Archiver that is already registered and activated, click the button to add those additional licenses using the response code you receive.
- § **Reset Request.** Aborts the current license request, allowing you to modify your initial request.



Note: If you reset your request, you must send in a new request to Ipswitch. As a general rule, do not reset your request unless told to do so by a member of the Ipswitch fulfillment team.

- § **Close.** Closes the dialog.

Troubleshooting / Contacting Technical Support

If for any reason logs are not being archived, or are not being archived according to the settings specified in the WhatsUp Event Archiver Control Panel, always check the Application Event Log on the machine or machines running the WhatsUp Event Archiver program.

The easiest way to review these log entries is to use the built-in *WhatsUp Event Archiver Log Entries* (on page 67) dialog, available from the **Tools** menu. When launched, the WhatsUp Event Archiver Log Entries dialog loads all of the WhatsUp Event Archiver Service events from the Windows event log. You can filter out certain types of activity by unchecking **Show Error Events**, **Show Warning Events**, and **Show Information Events**.

To copy the highlighted event to the Windows clipboard, click **Copy to Clipboard**.

To refresh all WhatsUp Event Archiver Service log entries from the local Application event log, click **Refresh Log Entries**.

To export all displayed log entries to an HTML file for further review or to send to Ipswitch Support, click **Export to HTML**.

Note: Only WhatsUp Event Archiver Service events currently present in the active Application Event Log are displayed. Older events may already be archived into saved EVT/EVTX files, and if so, you must load those older files in the Microsoft Event Viewer to view their contents.

If you find an error or other issue among the log entries, have this information ready when you visit the Ipswitch Knowledge Base or *Ipswitch Support Site* (<http://www.whatsupgold.com/support/index.aspx>) to research your problem further.

Common Causes Of Archiving Failure

There are numerous issues that can cause problems with an archiving operation, but the issues listed below are the most common:

Is the WhatsUp Event Archiver Service Running With Full Admin Rights?

Archiving event logs is a highly privileged operation, so the WhatsUp Event Archiver Service should be running under the context of a Domain Admin (if working with logs in a domain), an OU Admin account (if working with logs in an Organizational Unit), or a local Administrator account (if only archiving local logs on the machine where it is installed, or logs on computers in a workgroup that share a common administrator account).

Have you verified all share and NTFS access control lists (ACLs)?

The WhatsUp Event Archiver Service always attempts to add itself to the Access Control List of any share it must use to access event logs (e.g. the Staging Area share) or move event logs into (e.g. the Destination Share), but restrictive NTFS settings on the underlying file system of a server or Deny entries in a share ACL may prevent the archiving operation from working properly. Make sure to verify all relevant ACLs if you receive file access errors.

Is there any backup or anti-virus software that runs when WhatsUp Event Archiver is running that could be breaking open file handles and interrupting archive operations?

Anti-virus and backup software sometimes forcibly breaks open file handles. This can prevent the WhatsUp Event Archiver Service from working properly. If possible, scheduling archiving at times that are different from network backups or anti-virus scans.

Are you attempting to collect logs across WAN or VLAN links?

WANs, and in some cases VLANs, can break the file handles WhatsUp Event Archiver must keep open when archiving event logs. If you experience extreme time delays when collecting logs, or if you experience numerous failures and retries, the underlying network link may be to blame. If that is the case, consider either a.) changing your Working Directory settings in the *WhatsUp Event Archiver Preferences* (on page 81) dialog so that smaller logs are copied to a local folder for processing first or B.) installing a presence of WhatsUp Event Archiver at each remote WAN/VLAN end to collect the logs over LAN network links, and then transmit the logs

and or SQL data over the WAN. For more information, see the *Deployment Scenarios* (on page 2) section of this help guide.

Are you running the software on a virtual machine?

In many cases, if the networking subsystem in a Virtual Machine Environment is not configured properly, performance of WhatsUp Event Archiver can be severely degraded. WhatsUp Event Archiver depends on reliable and speedy access to the Windows network subsystem to perform log collection correctly. If performance problems persist, consider locating WhatsUp Event Archiver onto a non-VM environment.

Are the hidden shares (C\$, D\$, Admin\$, etc) enabled and functioning on all your servers?

These shares must be open and enabled for WhatsUp Event Archiver to archive logs remotely. If these must be locked down, you will need to install WhatsUp Event Archiver on each machine and let each computer manage its own event logs autonomously.

Is the Remote Registry Service enabled on each remote machine?

This service must be running in order for WhatsUp Event Archiver to archive many of the event logs successfully on various Microsoft Windows operating systems. And if you are performing any conversion of log entries into a different format (e.g. Access/ODBC), the remote registry service must be enabled to facilitate the conversion of any type of log from these computers.



Note: On Microsoft Windows Vista and Microsoft Windows Server 2008, the remote registry service does not have to be enabled for WhatsUp Event Archiver to work properly. However, the Remote Event Log Management exception must be enabled in the Windows Firewall. Also, in order to enumerate custom event logs on Windows Vista and later operating systems, the Remote Registry Service must be enabled.

Does the WhatsUp Event Archiver Service account have Full Control access to the HKLM\System section of the registry on each non-Microsoft Vista remote computer?

By default, Domain Admins have Full Control to this section of the registry on all machines in a domain. However, if you have hardened your servers, you may have restricted the Access Control Lists in this section of the registry. Verify that the WhatsUp Event Archiver Service account has full control by using the regedt32.exe utility.



Note: On Microsoft Windows Vista and Microsoft Windows Server 2008, no access to the remote registry is required for the software to work properly. However, the Remote Event Log Management exception must be enabled in the Windows Firewall. Also, in order to enumerate custom event logs on Windows Vista and later operating systems, the Remote Registry Service must be enabled.

Is the "Remote Event Log Management" exception enabled in the Windows Firewall on Microsoft Vista and Microsoft Windows Server 2008 computers?

In order to properly archive and convert event logs from Microsoft Vista and Microsoft Windows Server 2008 computers, this exception must be enabled in the Windows Firewall. You can also enable this exception for all computers in your domain by creating a Windows Firewall exception via Group Policy.

Is the Windows Event Collector Service running on Microsoft Windows Vista and Microsoft Windows Server 2008 computers?

WhatsUp Event Archiver does not archive logs if this service is running on Microsoft Windows Vista and/or Microsoft Windows Server 2008 computers. Please disable and/or stop the service on computers whose logs are collected by WhatsUp Event Archiver.

Visiting the Ipswitch Knowledge Base

If you are encountering an error or problem with WhatsUp Event Archiver that is not addressed in this User's Guide, please first visit our *Knowledge Base* (<http://whatsupgold.force.com/kb>).

Enter in any applicable error numbers or messages in the Search field, or simply leave the Search field blank to browse all articles applicable to WhatsUp Event Archiver.

Contacting Ipswitch Support

If you cannot find a resolution to your issue in our Knowledge Base, please open a support ticket at our Support Web Site, available at <http://www.whatsupgold.com/support> (<http://whatsupgold.force.com/kb>).

Ipswitch prides itself on providing quality pre-sales and post-sales support to all users of our solutions.

Legal Information and License Agreement

Legal Information Including Patent and Trademark Notices

WhatsUp Event Archiver is Copyright © 1997-2010 Ipswitch, Inc. All Rights Reserved.

WhatsUp Event Archiver is protected by U.S. Patent # 7,155,514. Other patents pending.

WhatsUp Event Archiver, WhatsUp Event Analyst, WhatsUp Event Alarm, WhatsUp Event Rover, and the WhatsUp word mark are trademarks or registered trademarks of Ipswitch, Inc.

Microsoft Windows NT®, Microsoft Windows 2000®, Microsoft Windows XP®, Microsoft Windows Server 2003®, Microsoft Windows Vista®, Microsoft Windows Server 2008®, Microsoft Windows 7®, Microsoft Access®, and Microsoft SQL Server® are all registered trademarks of Microsoft Corp. Microsoft Windows NT®, Microsoft Windows 2000®, Microsoft Windows XP®, Microsoft Windows 2003®, Microsoft Vista®, Microsoft Windows Server 2008®, Microsoft Windows 7®, Microsoft Access®, Microsoft Exchange® and Microsoft SQL Server® will hereafter be referred to as NT, 2000, XP, 2003, Vista, 2008, Windows 7, Windows, Access, Exchange, and SQL Server respectively. All other products or technologies not specifically mentioned here are the registered trademarks of their respective companies, and are used by permission.

WhatsUp Event Archiver License Agreement

Ipswitch License Agreement

READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE LOADING, AND/OR OTHERWISE USING THE SOFTWARE. THE TERMS OF USE OF THE SOFTWARE ARE DESCRIBED IN THE IPSWITCH LICENSE AGREEMENT OR LICENSE AND MAINTENANCE AGREEMENT FOR THE SOFTWARE WHICH MUST BE EXECUTED BETWEEN YOU (OR YOUR COMPANY OR INSTITUTION) AND IPSWITCH, INC. IF NO SUCH AGREEMENT HAS BEEN EXECUTED, THEN THIS AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND IPSWITCH, AND IT SUPERSEDES ANY PRIOR PROPOSAL OR UNDERSTANDING BETWEEN YOU AND IPSWITCH. BY DOWNLOADING OR INSTALLING THE SOFTWARE, AND/OR USING THE SOFTWARE, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS AGREEMENT, AND ARE THEREBY CREATING A CONTRACTUAL AGREEMENT BETWEEN YOU AND IPSWITCH. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU SHOULD NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND PROMPTLY RETURN THE SOFTWARE AND ASSOCIATED DOCUMENTATION.

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.

83 Hartwell Ave.

Lexington, MA 02421

(781) 676-5700

Fax: (781) 240-5813

International Issues and Log File Conversion

When WhatsUp Event Archiver attempts to convert log files from their native EVT/EVTX format into other formats, such as comma-delimited text or ODBC databases, it must use a date standard that is appropriate for the international locale where it is operating. For example, when exporting log records to text, WhatsUp Event Archiver can export them using either the U.S. date/time format (mm/dd/yy), or other country date/time formats, such as (dd/mm/yy). You can choose date/time options by accessing the *Preferences* (on page 81) dialog and selecting the **General** tab.

The format you choose has very important repercussions. If you export your log entries to text in a U.S. format, and then try to import them into a database using a European locale, the days and months may be reversed. Likewise, if you export log entries directly into a database, you should make sure that the server running WhatsUp Event Archiver has the same locale defined as the database server. Alternatively, you can override these locale considerations by

making all exported entries adhere to a U.S. date format. Regardless, it is important to give this topic consideration as you plan your archiving strategy.

Note: Whenever possible, WhatsUp Event Archiver uses a format-neutral method of importing log entries into ODBC database tables to minimize potential conflicts.

WhatsUp Event Archiver Menu and Menu Option Descriptions

In This Chapter

Using the File Menu.....	41
Using the Syslog Menu.....	42
Using the IIS/W3C Logs Menu.....	42
Using the View Menu.....	43
Using the Options Menu	43
Using the Tools Menu.....	44
Using the Help Menu	45

Using the File Menu

The File menu allows you to:

- 1 Schedule event logs on computers for collection
- 2 Change collection settings on individual logs
- 3 Stop the collection of logs on certain computers
- 4 Set audit policies on individual servers
Set log retention settings on individual logs
Raise the Microsoft Event Viewer to view the event log entries on that computer.

File menu option descriptions:

- § **Add a New Log.** Raises the *Log Registration* (on page 46) dialog so you can add a new log to the WhatsUp Event Archiver database.
- § **Edit the Selected Log.** Raises the *Log Registration* (on page 46) dialog so you can reconfigure the archiving settings on the existing log highlighted in the Listing of Registered Logs.
- § **Delete the Selected Log(s).** Removes all selected logs in the Registered Log Listing from the WhatsUp Event Archiver database, so that they are no longer collected by the WhatsUp Event Archiver Service.
- § **Archive Now!** Attempts to manually start the archiving process on the currently selected computer. You can only start a manual archive on one computer log at a time to prevent load-balancing problems. Also, the manual archiving operation runs under the context of your interactive user account, so if you are not an administrator on the target machine, an archiving process started manually may fail.

- § **Audit Policy.** Choosing this option raises the *Audit Policy* (on page 51) dialog, which you can use to change the individual audit policies on the selected computer.
- § **Log Settings.** Raises the *Log Settings* (on page 52) dialog, which you can use to change items like the event log size and method of retention for the selected computer and log.
- § **Event Viewer.** Launches the Microsoft Event Viewer, and sets the focus to the selected computer if able.

Using the Syslog Menu

Use the Syslog menu to add, edit or delete syslog device messages for archiving.

Syslog menu option descriptions

- § **Add a new Syslog Device.** Opens the Add New Syslog Device dialog where you can add a device for which you want to archive syslog messages.
- § **Edit a Syslog Device.** Opens the Edit Syslog Device dialog where you can edit the device for which you want to archive syslog messages.
- § **Delete Syslog Device(s).** After you select the syslog device you want to delete, displays a confirmation message asking if you are sure you want to delete the selected syslog device messages.
- § **Syslog Direct Write Settings.** Opens the configuration dialog where you can enable archiving to a specific SQL Server database.
- § **Syslog Write to CSV File Settings.** Opens the configuration dialog where you can enable archiving to directly to .csv files.
- § **Syslog Archiving Settings.** Opens the configuration dialog where you can set the actions associated with and the frequency for archiving a specific log.
- § **Add Multiple Syslog Devices by Subnet.** Launches a wizard in which you can specify IP and/or subnet addresses to scan for the purposes of adding found devices to the database in bulk.

Using the IIS/W3C Logs Menu

Use the IIS/W3C Logs menu to manage your logs in IIS/W3C format, generated by IIS servers running FTP, WWW, ISA, and SMTP services. WhatsUp Event Archiver supports collection, compression, and storage of IIS/W3C log files into database tables.

IIS/W3C Log menu option descriptions:

Add New Directory. Opens the Directory Settings dialog, allowing you to set how you want to manage the new directory, including archive scheduling, log data storage, database table and location information, managing files after archiving.

Edit Directory. To edit information for a directory, select the directory you want to edit, and then select **Edit Directory**.

Delete Directory. To delete a directory, select the directory you want to delete, and then select **Delete Directory**.

Archive Now. To archive information associated with a directory, select the directory, and then select **Archive Now!**.

Using the View Menu

Use the View menu to manually refresh the Registered Log Listing. F5 is the keyboard shortcut for this refresh operation.

Using the Options Menu

Use the Options menu to configure WhatsUp Event Archiver's default operating behaviors and settings. It also allows you to manage the account used by the WhatsUp Event Archiver Service. Furthermore, you can build custom domains of computer names should your network structure require it. You can centrally control which specific Event IDs get imported into your database tables during log collection.

Options menu option descriptions:

- § *WhatsUpEvent Archiver Preferences* (on page 81). Opens a dialog you can use to customize WhatsUp Event Archiver's default settings for new log registrations, and also optimize the behavior of the WhatsUp Event Archiver Service, such as CPU utilization.
- § *Set Service Account* (on page 89). Allows you to change the user account the WhatsUp Event Archiver Service runs under.
- § **Start the WhatsUp Event Archiver Service.** If the WhatsUp Event Archiver Service is stopped, attempts to restart it.
- § **Stop the WhatsUp Event Archiver Service.** If the WhatsUp Event Archiver Service is running, attempts to stop it.
- § *Set Default Domain* (on page 90). Changes the default domain which the WhatsUp Event Archiver Control Panel initially works in. If other domains trust this domain, they also display in the domain listing located in the upper right-hand corner of the WhatsUp Event Archiver Control Panel.
- § *Manage Custom Domain to Computer Mappings* (on page 91). If your network structure requires it, you can create custom domains in WhatsUp Event Archiver and map computer names to the custom domains you create. For example, you may need to manage a set of different computers spread out across multiple organizational units, or you may have computers located in different workgroups that share a common administrator account. In both scenarios, you can create a custom domain to bind together unrelated computers into a logical group and then use WhatsUp Event Archiver's wizards to manage them.

- § *Retrieve Computer Names From* (on page 92). Opens a dialog that allows you to control how WhatsUp Event Archiver retrieves computer lists throughout the application. For example, you can have WhatsUp Event Archiver display all computer accounts in a specific domain or just computer accounts from a particular organizational unit (OU) in Active Directory.
- § *Manage Custom Logs* (on page 92). Opens the Manage Custom Logs dialog, where you can add any additional Windows Custom Event Logs that may exist on your workstations or servers beyond the standard six.
- § *Set Global Import Filters* (on page 93). Opens a dialog you can use to create import filters that WhatsUp Event Archiver uses when processing event log data out of EVT/EVTX files into database tables. Filters control which events are placed in the database and which events are dropped altogether.

Using the Tools Menu

The Tools menu contains several items designed to help you automate the process of collecting event logs from your servers. Additionally, you can use this menu to create WhatsUp Event Archiver compatible tables in Access, Microsoft SQL Server, or ODBC databases. The Tools menu also provides access to other useful dialogs you can use to manage failed archives, import older EVT/EVTX files, set up automatic database maintenance, and view events logged by the WhatsUp Event Archiver Service.

Step-By-Step Wizards. Use the step-by-step wizards to automate the process of scheduling the collection of logs with WhatsUp Event Archiver, unify your audit policies, or unify your log settings across a domain.

- § *Setup Archiving for Multiple Computers at Once.* Opens a series of dialogs used to schedule event logs for collection from many different servers at once. You can select a certain number of computers, and then apply a uniform archiving and collection strategy to all of them.
- § *Adjust Settings for Currently Managed Logs* (on page 59). Opens a series of dialogs used to adjust the archiving settings on computer logs currently managed by WhatsUp Event Archiver.
- § *Unify Audit Policies* (on page 70). Sometimes it is difficult to set audit policy by hand for all of the assorted workstations and servers in your LAN. Use this wizard to apply a uniform set of audit policies to multiple computers at once, if you are not already using a Group Policy Object for this purpose.
- § *Unify Log Settings* (on page 72). Instead of using the Microsoft Event Viewer to set event log settings (such as log size and retention) on each computer individually, you can use this wizard to automatically unify these settings on multiple computers at once if you are not already using a Group Policy Object for this purpose.
- § **Database Helpers.** WhatsUp Event Archiver has a built-in table schema designed for storing event log entries. You can use the following menu items to create WhatsUp Event Archiver tables automatically in the databases you specify.
- § *Create Access Table(s)* (on page 74). Opens a dialog that can create WhatsUp Event Archiver tables in Microsoft Access databases.

- § *Create Microsoft SQL Server Table(s)* (on page 74). Like above, this dialog creates WhatsUp Event Archiver tables on Microsoft SQL Server.
- § *Creating Tables on Other ODBC Servers* (on page 75). Opens a help topic that shows you how to create WhatsUp Event Archiver tables in other ODBC databases.
- § **Setup/Adjust Automatic Database Maintenance.** If desired, you can instruct WhatsUp Event Archiver to perform automatic maintenance, such as the removal of older log entries from Microsoft Access and Microsoft SQL Server databases. This menu item opens the *Database Manager Settings* (on page 64) dialog where you can adjust the maintenance schedule and other properties.
- § **Import Orphaned or Older EVT/EVTX Files.** Occasionally, you may need to import older EVT or EVTX files into a database for more meaningful analysis. This menu item opens the *Import Older EVT/EVTX Files* (on page 66) dialog where you can select multiple EVT and/or EVTX files and push them into a central Access or ODBC database table.
- § **View WhatsUp Event Archiver Log Entries.** The WhatsUp Event Archiver Service logs all of the actions it takes when collecting event logs in the local Application Event Log on the computer where it is running. Use this menu item to open the *WhatsUp Event Archiver Log Entries* (on page 67) dialog which displays all WhatsUp Event Archiver Service entries present in the local Application Log. You can filter entries by type (e.g. error, warning, information) as well as export them to an HTML file.
- § **Manage Failed Archives.** WhatsUp Event Archiver automatically keeps track of and retries failed archives. However, there may be an occasional need to examine these failed archives and/or to delete them from the WhatsUp Event Archiver Service's internal database. Use this menu item to open the *Failed Archives* (on page 68) dialog, where you can perform additional management tasks, such as viewing, deleting or manually retrying failed archives.

Using the Help Menu

The Help menu contains links to the Ipswitch website, this help file, and allows you to register/activate WhatsUp Event Archiver and/or upgrade your total number of computer licenses.

Help menu option descriptions:

- § **Visit Ipswitch Network Management Online.** Attempts to connect to the Ipswitch Network Management home page, using your default browser.
- § **Register WhatsUp Event Archiver / Upgrade WhatsUp Event Archiver Licenses.** Displays the License Manager dialog, which you can use to initially register and activate WhatsUp Event Archiver, and later, add more licenses to the product.
- § **How Many Licenses Am I Using?.** Displays the number of computers WhatsUp Event Archiver is currently collecting logs from. Use this menu item to determine how close you are to reaching your license limit.
- § **WhatsUp WhatsUp Event Archiver Help File.** Displays the help file you are viewing.
- § **About WhatsUp Event Archiver.** Displays the current WhatsUp Event Archiver version and splash screen.

CHAPTER 3

Scheduling and Managing Logs for Collection

In This Chapter

Adding or Editing Log	46
Deleting Scheduled Logs.....	50
Using the Archive Now! Option	50
Managing Audit Policies.....	51
Managing Log Settings.....	52
Launching Event Viewer.....	53

Adding or Editing Log

While working in the WhatsUp Event Archiver Control Panel, use the Log Registration Options dialog to either schedule new logs for collection (e.g. you register them with the WhatsUp Event Archiver Service), or change archiving/collection properties on a log you have already registered.

To add a new log:

- 1 Click the **File** menu, and then select **Add a New Log**. The Log Registration Options dialog appears.
- 2 Set the options for the log you want to add by completing the boxes in the Log Registration Options dialog.
- 3 Click OK. Your newly defined log is added to WhatsUp Event Archiver.

To edit an existing log:

- 1 From the WhatsUp Event Archiver Control Panel, select the log you want to edit.
- 2 Click the **File** menu, and then select **Edit the Selected Log**. The Log Registration Options dialog appears.
- 3 Edit the options for the selected log, and then click **OK**. Your changes are saved.

Log Registration Options dialog tab and box descriptions:

Computer, Log, & Schedule tab. This tab houses all of the properties that determine what log and computer to archive, when to archive it, and whether to clear the active event log file on the server when archiving takes place.

- § **Computer name.** Choose a computer from the list. You can only select computers from the currently active domain in the list box. This box is disabled when you are editing an existing log.
- § **Log.** Choose Application, System, Security, etc to determine which event log you want to archive. This box is disabled when you are editing an existing log.
- § **Archive this log.** Determine how often you want the event log archived. Choose the **Hourly** option if you need to continuously archive event logs, as often as once every hour. WhatsUp Event Archiver then attempt archives every 1, 2, 4, 6, or 12 hours from the starting time, depending on the interval you choose.
- § If you choose **Daily - Every Day**, provide a time, and WhatsUp Event Archiver attempts the archive operation each day at that time. Alternatively, you can choose to archive **Daily - Selected Days** to archive at the same time on certain days in the week.
- § If you choose **Weekly** or **Monthly**, pick a day of the week or month, and a time, when you want WhatsUp Event Archiver to attempt this archive.
- § The default setting is **When log is full**. If you choose this option, WhatsUp Event Archiver monitors the server 24/7 to see if the log is approaching its file size limit. When the log is within a certain size (the default setting is 64K) of its administrator-defined limit, WhatsUp Event Archiver automatically archives the log. If you choose this option, the **Clear log after archiving** option must always be set to **Yes**. For network administrators sensitive to bandwidth issues, the impact of monitoring each log around the clock is minimal, as it only requires a few hundred bytes of data transfer each query.
- § **Clear log after archiving.** If you select Yes, which is the default, WhatsUp Event Archiver clears the log after saving it to the staging area on the originating server.

Staging Area Tab. Before a log is transported to a file server, or converted into a different data format, it must first be saved to a staging area on the originating server. This tab allows you to define the staging folder on the originating server, and the share folder that WhatsUp Event Archiver uses to access data files placed in the staging folder.

- § **Staging directory on COMPUTER to temporarily save EVT/EVTX files in.** Every time WhatsUp Event Archiver archives a log, it must first save that file to an area on the remote machine's hard disk. The default recommended value for this location is C:\WINNT. However, you must make sure that this path does correspond to a local drive and folder on the remote machine, or the archiving process will fail. If you specify a directory that does not exist on the remote machine, WhatsUp Event Archiver attempts to auto create the folder for you, provided you have the administrator rights to do so.
- § If you leave the default value of C:\WINNT here, WhatsUp Event Archiver can archive the log properly, even if the remote computer's system root folder is C:\WINDOWS. WhatsUp Event Archiver will try C:\WINDOWS if C:\WINNT does not exist.
- § **Share folder used by WhatsUp Event Archiver to grab EVT/EVTX files saved in the staging area.** In order to consolidate log files to a central location or database, WhatsUp Event Archiver needs to access them over the network. This required box is a fully qualified UNC share name (e.g. \\SERVERNAME\ShareName) that corresponds to the staging directory on the target machine where the logs are saved. The default recommended setting is \\SERVERNAME\ADMIN\$. You can click on the (...) button to use the Share Folder dialog to select a UNC share.

- § Notes about share folders: If you enter a share name that does not exist on the remote machine, WhatsUp Event Archiver attempts to create the share automatically, and give the service account permission to access it. Ensure that if you select a share that is already created on the remote machine, that it corresponds correctly to the staging directory. If it does not, WhatsUp Event Archiver cannot consolidate log entries to a central location. Also, this share **MUST BE** a top-level share; it cannot contain a subfolder underneath the main share folder. For example, "\\SERVERNAME\ShareName" is a correct setting, while "SERVERNAME\ShareName\SubfolderName" is not.

Data Conversion Tab. The properties contained under this tab allow you to specify the format you want to convert your EVT files into, should you wish to convert them.

- § **Store the log data in.** Where you define how you want WhatsUp Event Archiver to format your event log entries after they are archived. **Event Viewer (.EVT, .EVTX) format** is the default option, which means that WhatsUp Event Archiver leaves the log files in their default format after archiving. You can use the Microsoft Event Viewer or Ipswitch's WhatsUp Event Analyst or Event Rover solutions to read these file formats. **A comma-delimited text file** causes WhatsUp Event Archiver to convert the .EVT or .EVTX file into comma-delimited records, with each new line in the file representing a new log record. If you choose **an Access database**, WhatsUp Event Archiver converts the event log records directly into a Microsoft Access database table. Likewise, if you choose an **ODBC database**, WhatsUp Event Archiver attempts to place the log records into an ODBC database server.



Tip: If you are archiving logs from many different servers (100 or more) and do not need to perform regular analysis of log entries, you may want to archive and collect the logs in EVT/EVTX format only. It is a relatively CPU-expensive (and to a lesser degree, network expensive) process to import event log entries into other formats. WhatsUp Event Archiver does have a multiprocess architecture to minimize such performance issues, but if you have a large LAN with many computers, you should evenly distribute archiving times so that all logs are not operated on at once.

- § **Database location and table.** If you elect to import the log entries into an Access or ODBC database, you have to let WhatsUp Event Archiver know where the database is and the table name receiving the log entries.
- § **Path to Access .MDB file.** If you are importing event records into Access, enter the full file name of the Access database receiving the records. You can use the (...) button to browse for (or create) an Access .MDB file. This file must reside on the same computer as WhatsUp Event Archiver.
- § **ODBC Server Connection String.** If you are importing event records into an ODBC database, you need to create an ODBC connection string via the ODBC connection manager. Click the (...) button to launch the ODBC Manager. Choose an existing data source name from the File Data Source area, or create a new one by clicking on the **New...** button. After you have selected/created a data source, highlight it, click **OK** and the ODBC connection manager automatically places the connection string into this box. You may want to consult with your local database administrator to find out more about ODBC connection strings and the database servers available on your network. For more information, view the *Setting Up Databases and Making Connections* (on page 24) section of the help file.



Tip: It's recommended that you use standard (non-trusting) authentication if you are importing event log entries into a Microsoft SQL server. If you elect to use a Trusted Connection to the database, you must make sure that the database is configured so that the service account that WhatsUp Event Archiver runs under has read and write permission to all associated databases and tables.

- § **Table Name.** After you select a database, you need to tell WhatsUp Event Archiver which table to send the event log entries to. After you connect to a database, WhatsUp Event Archiver automatically populates this list with all of the tables in the database. You can choose an existing table, or by typing in a new name, have WhatsUp Event Archiver automatically create one for you.



Note: If you choose an existing table, you must make sure that it is a WhatsUp Event Archiver compatible table with the correct boxes and datatypes. In order to create WhatsUp Event Archiver compatible tables, go to the **Database Tables** section under the **Tools** menu.

- § **Remove EVT/EVTX file after archiving.** If you are choosing to import the event log data into a format besides the native EVT or EVTX formats, you can make WhatsUp Event Archiver delete the EVT/EVTX file that was created when the archiving first took place. However, you can also keep the EVT/EVTX file so that you have two different copies of the data in different formats. If this option remains unchecked, WhatsUp Event Archiver moves your EVT/EVTX file to a central file server if you specify one in the Final Destination tab.
- § **Compress the EVT/EVTX and/or comma-delimited text files before moving them.** On average, zipping EVT/EVTX or text files yields an average 95% compression ratio. For example, compressing a 100MB EVT/EVTX file produces a ZIP output file approximately 5MB in size. Compression is a nice feature for two reasons:
 - § If you need to maintain a very long archive of audit data (e.g. 2 years or more), compression allows you to store about 20 times more data on file servers.
 - § If you need to minimize traffic across WAN segments, have WhatsUp Event Archiver compress the files on a remote WAN end before transmitting them over a WAN link.

Final Destination tab. The final destination tab allows the administrator to specify the location where flat files (e.g. EVT/EVTX and/or Text files) should be moved. Destination options include a file server on the local area network, or a FTP server on any network.

- § **After archiving.** Regardless of the data format you choose, you can have WhatsUp Event Archiver move the initial .EVT/.EVTX file that was saved (and/or the comma-delimited .TXT file) off of the remote machine to a central network share or even to an FTP server for storage. This frees up space on the local machine, and lets you keep an extra copy of the .EVT/.EVTX file even after the data is imported into a database. If you elect to **Remove EVT file after archiving**, the file is deleted and cannot be deposited in this share or FTP Server.
- § **UNC Share.** You can click the (...) button to use the Share Folder dialog to select a UNC share.



Note: This share must already exist on a remote machine. WhatsUp Event Archiver automatically adds the service account to the share's access control list so that it can move the files. The share folder you enter must be in fully qualified UNC format (e.g. \\SERVERNAME\ShareName). Also, this share must be a top-level share. That is, it cannot contain a subfolder underneath the main share folder. For example, "\\SERVERNAME\ShareName" is a correct setting, while "SERVERNAME\ShareName\SubfolderName" is not.

- § **FTP Server.** If firewall settings prohibit you from reaching a file server using standard File and Print Sharing, you can directly FTP the files to an FTP server. Enter the fully-qualified Internet domain name or IP address of the FTP server in this box.
- § **Port.** The standard port for FTP transfers is 21, but you can specify a non-standard port for additional security. Ensure the FTP Server is configured to receive files on this port.
- § **Username.** Enter the username needed to log on to the FTP server.
- § **Password.** Enter the password needed to log on to the FTP server.
- § **Initial Directory.** If needed, you can specify an initial directory where your log files should be stored. If this box is used, WhatsUp Event Archiver attempts a change directory (CD) command on the FTP server after connecting. Leave this box blank if you want files placed in the root directory.
- § **OK.** When you click OK, WhatsUp Event Archiver double checks all your settings for validity, and either add the new log to the log registration database, or update it in the log registration database.
- § **Cancel.** Abandons the current attempt to add a new log or change its settings.

Deleting Scheduled Logs

You can delete scheduled logs that are no longer needed.

To remove logs scheduled for collection from WhatsUp Event Archiver:

- 1 From the WhatsUp Event Archiver Control Panel, select the logs you want to delete.
- 2 Click the **File** menu, and then select **Delete the Selected Log(s)**.

Using the Archive Now! Option

You can quickly archive existing logs by using the Archive Now! Option.

To quickly archive and existing log:

- 1 From the WhatsUp Event Archiver Control Panel, select the log you want to archive.
- 2 Click the **File** menu, and then select **Archive Now!**. A message confirming that the manual archiving function has been initiated displays.
- 3 Click **OK**.

Managing Audit Policies

WhatsUp Event Archiver allows the administrator to adjust audit policies on individual machines, and also provides the administrator with the ability to unify the audit policies of many workstations and servers at once by using a wizard. This is useful when organizations do not use Group Policy to control audit settings or are instead managing computers in one or more workgroups.

- 1 To manage audit policies, click the **File** menu, and then click **Audit Policy on X** where X equals the machine name. The Event Audit Policy dialog opens.
- 2 When you are finished managing the audit policy, click **OK**. Your changes are saved.

The Audit Policy dialog allows you to change security events you want to audit on an individual machine (such as a standalone workstation or server), or across an entire domain (in the case of a Primary Domain Controller or Active Directory Server). Note that if you choose to display audit policies on a domain controller, the focus automatically shifts to the domain that domain controller manages.



Note: If you are running a Microsoft Windows 2000, 2003 or 2008 domain and have Group Policies enabled, you should use the Group Policy editor to manage your audit policy settings for related groups of computers.

The Audit Policy dialog field definitions:

Audit (Security Event Logging) on \\ComputerName is. Set this option to **Enabled** to turn on security event logging on the specified Windows computer or domain. Switching to **Disabled** turns off all auditing, regardless of the way each audit category is configured.

Audit Categories

For each audit category, you can choose to record successful events (by checking success), failed events (by checking failure), both (by checking both), or neither (by checking none).

- § **System Events.** Audit attempts to shutdown or restart the computer. Also, audit events that affect system security or the security log.
- § **Logon Events.** Audit attempts to log on to or log off from the system. Also, attempts to make a network connection.
- § **Object Access.** Audit attempts to access securable objects, such as files.
- § **Privilege Use.** Audit attempts to use Windows NT privileges.
- § **Process Tracking.** Audit events such as program activation, some forms of handle duplication, indirect access to an object, and process exit.
- § **Policy Change.** Audit attempts to change policy object rules.
- § **Account Management.** Audit attempts to create, delete, or change user or group accounts. Also, audit password changes.
- § **Directory Service Access (Windows 2000/XP/2003/Vista/2008 only).** Audit attempts to access the directory service.

- § **Account Logons (Windows 2000/XP/2003/Vista/2008 only).** Audit logon attempts by domain accounts that log on to the domain controller. These audit events are generated when the Kerberos Key Distribution Center logs on to the domain controller and by MSV1_0 for Windows NT 4.0 - style logons.

Managing Log Settings

WhatsUp Event Archiver allows the administrator to adjust log retention and log size settings on individual machines, and also provides the administrator with the ability to unify the log retention settings and log sizes of many workstations and servers at once by using a wizard. This can be useful when organizations do not use Group Policy to control log retention and size settings, or are managing computers in one or more workgroups instead.



Note: If you are running a Microsoft Windows 2000, 2003 or 2008 domain and have Group Policies enabled, use the Group Policy Editor to manage your log size and retention settings for related groups of computers.



Note: Adjusting log settings on Microsoft Vista or later computers is not yet supported. In the interim, use the Local Security Policy tool and/or Group Policy Editor to adjust these settings on Microsoft Vista computers.

To manage log settings:

- 1 Click the **File** menu, and then select **Log Settings on X**, where X equals the machine name. The Log Settings dialog opens.
- 2 When you are finished managing the log settings, click **OK**. Your changes are saved.

Use the Log Settings dialog to set individual event log file sizes and retention properties.

Log Settings dialog field descriptions:

- § **Log Type.** Use this list to choose an individual event log from the computer to modify settings on.
- § **File Size.** Type a new size into the text box, or use the up/down arrows to adjust the file size. Due to the architecture of the Microsoft Event Log subsystem, your size entry is rounded to the nearest 64 kilobyte increment.
- § **Event Log Retention.** When an event log becomes full, there are three actions a Microsoft Windows operating system can take. One is to start overwriting all events, beginning with the oldest and working forward. This is a relatively low security setting, since once events are overwritten, they cannot be recovered. A slightly more secure setting is to only allow events to be overwritten if they are a certain number of days old or older. The optimal setting from a security standpoint is to prevent the event log system from overwriting any events. WhatsUp Event Archiver empowers you to choose this last option, since it can automatically archive the logs when they are nearing their maximum size.

Launching Event Viewer

Event viewer allows you to view events that have occurred on your computer. After Event Viewer is launched, follow the instructions in the Overview area.

To launch Event Viewer, click the **File** menu, and then select **Event Viewer**. The Event Viewer window opens.

Scheduling Logs for Multiple Computers

In This Chapter

Setting-up Archiving for Multiple Computers at Once (Step 1).....	54
Setting-up Archiving for Multiple Computers at Once (Step 2).....	54
Setting-up Archiving for Multiple Computers at Once (Step 3).....	55
Setting-up Archiving for Multiple Computers at Once (Step 4).....	56
Setting-up Archiving for Multiple Computers at Once (Step 5).....	56
Setting-up Archiving for Multiple Computers at Once (Step 6).....	58

Setting-up Archiving for Multiple Computers at Once (Step 1)

While working in the WhatsUp Event Archiver Control Panel, you can use the Setup Monitoring for Multiple Computers at Once Wizard to schedule logs for archiving from many different servers with similar settings. To open the wizard, click the **Tools** menu, and then select the **Setup Monitoring for Multiple Computers at Once Wizard** option in the **Step-By-Step Wizards** submenu. Below are instructions for Step 1 of this wizard.

Before you begin deploying an event log collection strategy to multiple servers, you must first choose the domain from which you want to computers, and also select the types of logs you want to collect from those computers. The DNS Server, Directory Service, and File Replication Service logs are only available for collection on certain Windows 2000, Windows 2003, and Windows 2008 servers. If you select them in addition to the Application, System, and Security logs, make sure that you limit your computer selection to only Windows 2000, Windows 2003, and Windows 2008 servers in Step 2. Once you are finished choosing the domain and log files for collection, click **Next** to continue.

Setting-up Archiving for Multiple Computers at Once (Step 2)

In Step 2, select the servers and workstations whose logs you want WhatsUp Event Archiver to collect. The event logs from each computer chosen is scheduled for collection, and WhatsUp Event Archiver begins archiving their logs according to your schedule. You can group select multiple computers by holding down CTRL or SHIFT while selecting them with your mouse. Using the >> button to move them to the right side includes them in the

registration process. Using the << button to move them to the left side excludes them from the registration process. When you are satisfied with your selections, click **Next** to continue.

Setting-up Archiving for Multiple Computers at Once (Step 3)

In Step 3, you choose how often you want the event logs collected. WhatsUp Event Archiver has six scheduling options, five that are dependent on the date and time, and the remaining one dependent on an event log's actual file size.

- § **Hourly.** All logs on the computers you selected in Step 2 are archived at hourly or semi-hourly intervals from a given starting time.
- § **Daily, every day.** All of the logs on the computers you selected in Step 2 are archived at a specific time each day.
- § **Daily, selected days.** All of the logs on the computers you selected in Step 2 are archived at a specific time only on days of the week that you specify.
- § **Weekly.** Initiates the archiving process at a given time on a specific weekday.
- § **Monthly.** Initiates the archiving process at a given time on a specific day of the month (1 through 28).
- § **When the log file is almost full.** Makes the WhatsUp Event Archiver Service poll each computer event log registered with it on an around-the-clock basis. As soon as the log file grows close (within 64KB by default) to its administrator-defined limit (e.g. what you define in the *Log Settings* (on page 52) dialog), WhatsUp Event Archiver initiates the archiving and collection process.



Note: Using this technique has a lot of advantages. First, if you are collecting event logs from a lot of different machines, this reduces network stress because you are not moving a lot of files or data across the network at a specific time. In addition, if a computer is down for maintenance and you archive computer logs at a daily or weekly time, that computer may not get archived. With this setting, as long as the computer is on the network, its log size is being monitored. Even at its most aggressive settings, the WhatsUp Event Archiver Service does not exceed 1 KB per second of data transfer when it polls log sizes in this manner.

- § **Clear the log after it is archived.** Use this option to select whether you would like WhatsUp Event Archiver to clear the active event log when it is archived. In most situations, it is desirable to clear the log during the archiving process.
- § **For better load balancing.** If you have chosen a date and time-based archiving schedule, enter the number of minutes that WhatsUp Event Archiver should use to disperse archiving between different computers. For example, if you choose 15 minutes, and want to collect logs daily at 12:00 AM, WhatsUp Event Archiver schedules the first computer's logs at 12:00 AM, the next computer's logs at 12:15 AM, and so on. As a general rule, if you archive a lot of computers with WhatsUp Event Archiver (e.g. 50+), or you have slow network links to certain computers, it is better to use a greater number of minutes in this field.

Setting-up Archiving for Multiple Computers at Once (Step 4)

Now its time to determine where on each remote machine's disk drive to store the archived EVT/EVTX file. In addition to specifying the staging folder where this file is saved on each server, you need to indicate a shared folder used to access the staging area remotely over the network. Or in other words, the share folder that WhatsUp Event Archiver uses to access the EVT/EVTX file for further processing. If your choice of shared folder is not a built in share (e.g. ADMIN\$, C\$), WhatsUp Event Archiver automatically creates the share for you on each computer. Likewise, if the staging folder (e.g. C:\EventLogs) does not exist on a machine, this wizard attempts to create it. Finally, WhatsUp Event Archiver automatically adds its service account to the access control list of the file share so it can access the files within.

Note about the default C:\WINNT path: If you leave the default value of C:\WINNT here, WhatsUp Event Archiver can archive the log properly, even if the remote computer's system root folder is C:\WINDOWS. WhatsUp Event Archiver tries C:\WINDOWS if C:\WINNT does not exist.

Lastly, if you want to have WhatsUp Event Archiver move EVT, EVTX, or TXT files to a file server or FTP server, choose the appropriate server for your needs and enter the necessary connection information (e.g. the UNC path to the file server on your LAN, or the network address, port, username, password, and initial directory of an FTP server). If you choose a UNC share, you may use the (...) button to browse to a file server and share on your domain. The WhatsUp Event Archiver Service account is added to the access control list of this destination file share as well if the UNC Share option is chosen.

Here is an example of entries for this step:

First, save the EVT/EVTX file to C:\WINNT

Which is accessed via the ADMIN\$ share.

When archiving is finished, I want to move the log to a central share:

Yes \\FILESERVER\EventLogs



Note: The central share for collection must be a top-level share. That is, it cannot contain a subfolder underneath the main share folder. For example, "\\SERVERNAME\ShareName" is a correct setting, while "SERVERNAME\ShareName\SubfolderName" is not.

Setting-up Archiving for Multiple Computers at Once (Step 5)

In step 5, you choose how you want to consolidate the event log entries from all of the computers whose logs will be archived. Event Viewer (.EVT, .EVTX) format means that

WhatsUp Event Archiver leaves the log files in their native format after archiving. You can use the Microsoft Event Viewer to read this file format. A comma-delimited text file causes WhatsUp Event Archiver to convert the .EVT/.EVTX file into comma-delimited records, with each new line in the file representing a new log record. If you choose an Access database, WhatsUp Event Archiver converts the event log records out of their native format directly into a Microsoft Access database table. Likewise, if you choose an ODBC database, WhatsUp Event Archiver converts the log records into an ODBC database table.

If you choose the Access Database or ODBC database option, you need to provide WhatsUp Event Archiver with some additional information about the database(s) and table(s).

Access Databases

Database Path. Enter the full filename of the Access .MDB file you want to store the data in, or use the (...) button to browse for or create an Access database. This database file must reside on the same computer as WhatsUp Event Archiver.

ODBC Databases

- § **ODBC Info.** Use the (...) button to launch the ODBC Connection Manager, and then choose an existing or create a new ODBC File Data Source. For more information, view the *Setting Up Databases and Making Connections* (on page 24) section of this help file.
- § **Auto-create a table per log type (recommended if using WhatsUp Event Analyst for reporting).** If you want to create a new table for each log type being collected, choose this option. WhatsUp Event Archiver auto-creates all the tables necessary in the database, using each log type you selected in Step 2. The tables are named Application, System, Security, DNS Server, Directory Service, and File Replication Service, according to the log types you select.



Note: This is the recommended option if you are using Ipswitch's WhatsUp Event Analyst product to produce consolidated reports on activity across multiple servers. WhatsUp Event Analyst reporting has been optimized when reporting against single tables of related activity.



Note: WhatsUp Event Archiver can only auto-create tables on Microsoft Access or Microsoft SQL Server databases.

- § **Auto-create a table per computer.** If you want to create a new table for each computer you are collecting logs from, choose this option. WhatsUp Event Archiver auto-creates all the tables necessary in the database, using each computer name you selected in Step 2.
- § **Place all data in this single table.** Alternatively, you can store all log entries from different computers in a single database table. Choose a predefined table name from this list, or type in a new name to automatically create it.
- § **I don't need the EVT/EVTX files.** If you do not want to hang on to the EVT/EVTX files after the logs are archived and stored in a different format, check this box. Otherwise, leave it unchecked. If you choose any other format besides EVT/EVTX for collection, and leave this option unchecked, WhatsUp Event Archiver first saves and then moves the archived EVT/EVTX files to the final location you specify.

- § **Compress the EVT/EVTX and/or comma-delimited text files.** Checking this option makes WhatsUp Event Archiver compress all EVT/EVTX and text files into ZIP files before moving the files to and storing the files on a final destination server. This can be beneficial, as the typical compression ratio is 95%, resulting in reduced bandwidth (if sending files over a WAN link) and reduced long-term storage requirements.

Setting-up Archiving for Multiple Computers at Once (Step 6)

In Step 6, WhatsUp Event Archiver attempts to schedule the event logs on all of the computers you selected in Step 2 for collection by the WhatsUp Event Archiver Service. When finished, WhatsUp Event Archiver displays the successes and failures encountered during scheduling, ordered by individual computer. Double click a computer name for more details about what caused a success or failure.



Note: There is a good chance that some failures are recorded, because computers are often not present on the network, and this wizard needs to access computers in order to create file shares and set access permissions.

When you are finished previewing the results, click the **Exit** button to return to the WhatsUp Event Archiver Control Panel.

The icon legend in the Results pane is as follows:

-  - Indicates an error occurred.
-  - Indicates a warning condition; the registration operation may only be partially complete.
-  - Indicates the operation was successful.

Editing Settings on Multiple Computers

In This Chapter

Adjusting Settings for Currently Managed Logs (Step 1).....	59
Adjusting Settings for Currently Managed Logs (Step 2).....	60
Adjusting Settings for Currently Managed Logs (Step 3).....	60
Adjusting Settings for Currently Managed Logs (Step 4).....	61
Adjusting Settings for Currently Managed Logs (Step 5).....	62
Adjusting Settings for Currently Managed Logs (Step 6).....	63
Setting Up/Adjusting Automatic Database Maintenance.....	64
Importing Older EVT/EVTX Files.....	66
Viewing WhatsUp Event Archiver Log Entries.....	67
Managing Failed Archives.....	68

Adjusting Settings for Currently Managed Logs (Step 1)

If you need to adjust the archiving properties of multiple computers at the same time, you can use the Adjust Settings for Currently Managed Logs Wizard. To access this wizard, click the **Tools Menu**, and then select **Step-By-Step Wizards**; from the submenu, select **Adjust Settings for Currently Managed Logs Wizard**.

Below is information on Step 1 of this wizard.

Before you begin adjusting your event log collection strategy on multiple servers, you must first select the types of logs whose archiving settings you will modify on those computers. Note that the DNS Server, Directory Service, and File Replication Service logs are only available for collection on certain Windows 2000, Windows 2003, and Windows 2008 servers. If you select them in addition to the Application, System, and Security logs, make sure that you limit your computer selection to only Windows 2000, Windows 2003, and Windows 2008 servers in Step 2. After you finish choosing the domain and log files for collection, click **Next** to continue.

Adjusting Settings for Currently Managed Logs (Step 2)

In Step 2, select the servers and workstations whose log archiving settings you would like to modify. The event logs from each computer chosen is modified in the log registration database, and WhatsUp Event Archiver will begin to archive their logs according to the new archiving properties you set in this wizard. You can group select computers by holding down CTRL or SHIFT while selecting items with your mouse. Using the >> button to move them to the right side includes them in the registration process. Using the << button to move them to the left side excludes them from the registration process. When you are satisfied with your selections, click **Next** to continue.

Adjusting Settings for Currently Managed Logs (Step 3)

In Step 3, you decide the frequency in which the event logs are archived and collected. WhatsUp Event Archiver has six scheduling options, five dependent on the date and time, and the other dependent on an event log's actual file size.

- § **Hourly.** If you choose this option, all logs on the computers you selected in Step 2 are archived at semi-hourly intervals from a given starting time.
- § **Daily, every day.** If you choose this option, all logs on the computers you selected in Step 2 are archived at a specific time each day.
- § **Daily, selected days.** If you choose this option, all logs on the computers you selected in Step 2 are archived at a specific time only on days of the week you specify.
- § **Weekly.** This option initiates the archiving process at a given time on a specific weekday.
- § **Monthly.** This option initiates the archiving process at a given time on a specific day of the month (1 through 28).
- § **When the log file is almost full.** This option requires the WhatsUp Event Archiver Service to poll each computer event log registered with it on an around-the-clock basis. As soon as the log file is close (within 64KB by default) to its administrator-defined limit (e.g. what you define in the *Log Settings* (on page 46) dialog), WhatsUp Event Archiver initiates the archiving and collection process.



Note: Using this technique has many advantages. First, if you are collecting event logs from several different machines, this reduces network stress because you are not moving a lot of files or data across the network at a specific time. In addition, if a computer is down for maintenance and you archive computer logs at a daily or weekly time, that computer may not get archived. With this setting, as long as the computer is on the network, its log size is being monitored. Even at its most aggressive settings, the WhatsUp Event Archiver Service does not exceed 1000 bytes per second of data transfer when it is polling their sizes in this manner.

- § **Clear the log after it is archived.** Use this option to select whether you want WhatsUp Event Archiver to clear the active event log when it is archived. In most situations, it is desirable to clear the log during the archiving process.
- § **For better load balancing.** If you have chosen a date and time-based archiving schedule, enter the number of minutes that WhatsUp Event Archiver should use to space out archiving between different computers. For example, if you choose 15 minutes, and want to collect logs daily at 12:00 AM, WhatsUp Event Archiver schedules the first computer's logs at 12:00 AM, the next computer's logs at 12:15 AM, and so on. As a general rule, if you archive a lot of logs with WhatsUp Event Archiver (e.g. 20+), or you have slow network links to certain computers, it is better to use a greater number of minutes in this box.

Adjusting Settings for Currently Managed Logs (Step 4)

Step for is about determining where on each remote machine's disk drive to store the backup EVT file. In addition to specifying where to save the file on the originating server (e.g. the staging folder), you need to indicate a shared folder that used to access the staging area remotely over the network. In other words, this is the share folder that WhatsUp Event Archiver uses to "reach in" and grab the EVT file for additional data conversion and data transfer. If your choice of shared folder is not a built in share (e.g. ADMIN\$, C\$), WhatsUp *Event Archiver automatically creates the share for you on each computer.* Likewise, if the staging folder (e.g. C:\EventLogs) does not currently exist on a machine, the wizard attempts to create it. In addition, WhatsUp Event Archiver automatically adds its service account to the access control list of the file share so it can access and move the files inside.

Note about the default C:\WINNT path. If you leave the default value of C:\WINNT here, WhatsUp Event Archiver archives the log properly, even if the remote computer's system root folder is C:\WINDOWS. WhatsUp Event Archiver tries C:\WINDOWS if C:\WINNT does not exist.

If you want WhatsUp Event Archiver to move the .EVT file or .TXT (the comma-delimited format available in Step 3) to a file server or FTP server, choose the appropriate server for your needs, and enter the necessary connection information (e.g. the UNC path to the file server on your LAN, or the network address, port, username, password, and initial directory of an FTP server). If you choose a UNC share, you may use the (...) button to browse to a file server and share on your domain. *The WhatsUp Event Archiver Service account is added to the access control list of this destination file share as well if the UNC Share option is chosen.*

Here is an example of entries for this step:

First, save the .EVT file to: **C:\WINNT**

Which is accessed via this share: **ADMIN\$**

When archiving finishes, I want to move the log to a central share:

Yes \\FILESERVER\EventLogs



Note: The central share for collection must be a "top-level" share. That is, it cannot contain a subfolder underneath the main share folder. For example, "\\SERVERNAME\ShareName" is a correct setting, while "SERVERNAME\ShareName\SubfolderName" is not.

Adjusting Settings for Currently Managed Logs (Step 5)

In step 5, you determine how you want to consolidate the event log entries from all of the computers whose logs you want archived. **Event Viewer (EVT/EVTX) format** indicates that WhatsUp Event Archiver leaves the log files in their native format after archiving. You can use the Microsoft Event Viewer to read this file format. **A comma-delimited text file** causes WhatsUp Event Archiver to convert the EVT/EVTX file into comma-delimited records, with each new line in the file representing a new log record. If you choose **an Access database**, WhatsUp Event Archiver pushes the event log records directly into a Microsoft Access database table. Likewise, if you choose an **ODBC database**, WhatsUp Event Archiver places the log records into an ODBC database server.

If you choose the access database or ODBC database option, you must provide WhatsUp Event Archiver with some additional information about the databases and tables.

If you choose to collect the logs into text files, Access database tables, or ODBC database tables, you can still retain the data in EVT/EVTX format as well. Leave the **I don't need the EVT files** option unchecked, and WhatsUp Event Archiver retains and optionally moves the archived EVT files to a file server.

Access Databases

Database Path. Enter the full filename of the Access .MDB file you want to store the data in, or use the (...) button to browse for or create an Access database. This database file must reside on the same computer as WhatsUp Event Archiver.

ODBC Databases

- § **ODBC Info.** Use the (...) button to launch the ODBC connection manager, and choose or create a new ODBC data source. For more information, view *Setting Up Databases and Making Connections* (on page 24).
- § **Auto-create a table per log type (recommended if using WhatsUp Event Analyst for reporting).** If you want to create a new table for each log type being collected, choose this option. WhatsUp Event Archiver auto-creates all the tables necessary in the database, using each log type you selected in Step 2. The tables are named Application, System, Security, DNS Server, Directory Service, and File Replication Service according to the log types you select.



Note: This is the recommended option if you are using Ipswitch's WhatsUp Event Analyst product to produce consolidated reports on activity across multiple servers. WhatsUp Event Analyst reporting has been optimized when reporting against single tables of related activity.



Note: WhatsUp Event Archiver can only auto-create tables on Microsoft Access or Microsoft SQL Server databases.

- § **Auto-create a table per computer.** If you want to create a new table for each computer you are collecting logs from, choose this option. WhatsUp Event Archiver auto-creates all the tables necessary in the database, using each computer name you selected in Step 2.



Note: WhatsUp Event Archiver can only auto-create tables on Microsoft Access or Microsoft SQL Server databases.

- § **Place all data in this single table.** You can store all log entries from different computers in a single database table. Choose a predefined table name from this list, or type in a new name to automatically create it.
- § **I don't need the EVT files.** If you do not want to keep the EVT files after the logs are archived and stored in a different format, check this box. Otherwise, leave it unchecked. If you choose any other format besides EVT for collection, and leave this option unchecked, WhatsUp Event Archiver saves and then moves the archived EVT files to the final location you specify.
- § **Compress the EVT and/or comma-delimited text files.** Checking this option makes WhatsUp Event Archiver compress all EVT and text files into ZIP files before moving the files to and storing the files on a final destination server. This is beneficial, as the typical compression ratio is 95%, resulting in reduced bandwidth (if sending files over a WAN link) and reduced storage requirements.

Adjusting Settings for Currently Managed Logs (Step 6)

In Step 6, WhatsUp Event Archiver attempts to adjust the archiving settings on the event logs from the computers you selected in Step 2. When finished, WhatsUp Event Archiver displays the successes and failures, ordered by individual computer. Double click a computer name to view details about what caused a success or failure.



Note: It is not uncommon to see some failures, because computers are often not present on the network, and this wizard needs to access computers in order to create file shares and set access permissions.

When you are finished previewing the results, click the **Exit** button to return to the WhatsUp Event Archiver Control Panel.

The icon legend in the Results panel:

 - Indicates an error occurred.

-  - Indicates a warning condition; the registration operation may only be partially complete.
-  - Indicates the operation was successful.

Setting Up/Adjusting Automatic Database Maintenance

One of the challenges of collecting log data is working with the large volume of information stored in databases. WhatsUp Event Archiver provides a database maintenance module that can:

- § Run on a daily basis at a user-definable time.
- § Automatically archive Microsoft Access databases (e.g. MDB files) that are a certain percentage from their maximum size of 2147483648 bytes.
- § Automatically remove log records older than a certain number of days from the current date from Microsoft SQL Server databases.



Note: Any data deletion or alteration techniques used by WhatsUp Event Archiver's database maintenance module are irreversible, and Ipswitch, Inc highly recommends backing up your database files/structures before enabling this portion of the software. In addition, should you wish to design a more complex database maintenance and backup program, you are free to do so and you can leave this portion of the software disabled.



Note: All successful or failed database maintenance actions are logged in the local Windows Application Event Log by the WhatsUp Event Archiver Service. To review the success or failure of daily maintenance tasks, consult the *WhatsUp Event Archiver Log Entries dialog* (on page 67), available from the Tools Menu (View WhatsUp Event Archiver Log Entries).

Microsoft Access Database Maintenance Program

After you have defined the percentage of the MDB file size you consider to be full, the WhatsUp Event Archiver database maintenance module checks the file sizes of all Microsoft Access databases receiving log data at the scheduled time. If any of the MDB files are over the file size limit, WhatsUp Event Archiver:

- § Renames the existing MDB file as: <ORIGINAL FILE NAME>_FROM_<Oldest Date in File>_TO_<Newest Date in File>.mdb
- § Creates a new MDB file with the original file name and transfers the existing table structure from the old file into new file name, so that log collection operations can resume at the next scheduled time.

All of the above operations occur in the directory where the respective MDB files are located.

It is important to schedule the WhatsUp Event Archiver database maintenance module to run at a time when log collection is not taking place, as database maintenance cannot occur if MDB files are in use.

Microsoft SQL Server Maintenance Program

To periodically remove records from your Microsoft SQL Database, you can specify a number of days older than the current date, representing the oldest log data allowable in your database tables. In most cases, the purpose of bringing data into Microsoft SQL is to obtain consolidated reporting and speedy analysis with Ipswitch's WhatsUp Event Analyst or another database reporting tool. Therefore, keeping records in SQL beyond the immediate reporting window may not be necessary, especially if EVT/EVTX files are being retained for the purpose of forensics and long-term storage.

Each day at the scheduled time, the WhatsUp Event Archiver database maintenance tool connects to all SQL database tables recognized as Ipswitch log data tables and issue statements to delete records older than a certain date.

For optimal results, schedule the daily database maintenance at a time before or after WhatsUp Event Archiver performs log collection.

Configurable Database Maintenance Settings

- § **Allow WhatsUp Event Archiver to automatically delete and/or archive old log data in Microsoft databases.** Checking this option effectively turns on the WhatsUp Event Archiver database maintenance module. If this option remains unchecked, the WhatsUp Event Archiver database maintenance module will not run on a scheduled basis.
- § **Run database tasks daily at XX:XX AM/PM.** Choose the hour and minute you would like the WhatsUp Event Archiver database maintenance module to execute.
- § **Delete all event log records older than XX days from the current date from MS SQL DB tables.** Enter the number of days prior to the current date you want the WhatsUp Event Archiver database maintenance module to consider old data fit for purging. All records older than this date are deleted from WhatsUp Event Archiver database tables when the database maintenance module runs. Valid day ranges are between 1 and 750 days from the current date.
- § **Automatically archive MDB files when they are XX percent full.** Enter a percentage of the maximum Microsoft Access MDB file size (e.g. 2147483648 bytes) that the WhatsUp Event Archiver database maintenance module will consider to be a full Access database. Files beyond this size are automatically renamed and a new MDB file with the same original file name is recreated with the same table structure. Valid percentage ranges are between 1 and 90%.
- § **Run Manager Now.** Administrators can manually execute the WhatsUp Event Archiver database maintenance module at any time by clicking this button. When clicked, WhatsUp Event Archiver confirms that you want to delete and/or alter database log data, save the current settings in the dialog, and then execute the database maintenance module.
- § **Note:** The database maintenance module runs under the context of the logged-on user, so that account must have rights on the WhatsUp Event Archiver database, either via NTFS permissions for Access files or via Microsoft SQL database permissions.
- § **Update Settings.** Updates the operating settings for the database maintenance module after you confirm that you want to schedule the deletion and/or alteration of log data.

- § **Cancel.** Abandons any changes you have made to the database management module settings.

Importing Older EVT/EVTX Files

Periodically, you may find need to manually import several EVT/EVTX files into an Access or ODBC database all at once. The potential reasons for needing to do this are numerous, including:

- § A forensic incident requires you to import old event log files into a database for rigorous analysis.
- § An outside agency performs an audit and demands reports on data stored in event log files from a particular date and time.
- § Network problems prevent archiving from functioning properly over an extended period of time, and, as a result, orphaned event log files are produced.

This dialog allows you to take one or more event log files of the same type (e.g. Security), and import them into an Access database table or ODBC database table for analysis. Below are instructions on how to complete this process inside the dialog.

Step 1

Click the **Add Files for Import...** button to browse for EVT/EVTX files you want included in the import process. You can select multiple event logs in this common dialog by holding down CTRL while selecting various files with your mouse. You can also select zipped EVT/EVTX files, as the import process unzips them as needed to perform the import. When satisfied with your selections, click **OK** to add your files to the import list. You can continue browsing for files on other machines or folders by pressing the browse button several times.

- § **Clear Selected File.** Removes the currently selected EVT/EVTX file from the import list.
- § **Clear All Files.** Removes all of the EVT/EVTX files from the import list.
- § **Files are _____ logs.** Select the type of logs you are importing into the database. When using this dialog, you must always select log files of the same type for an import operation.

Step 2

- § **Database type.** Choose the type of database you want to import the log files into. Valid options include Microsoft Access, and Microsoft SQL Server database servers.
- § **Database path.** Use the (...) button to browse for either a path to a Microsoft Access database (.MDB file) or use the ODBC Manager dialog to select or create an ODBC File Data Source link.
- § **Table name.** Choose an existing WhatsUp Event Archiver compatible database table from the list, or type in a new table name and WhatsUp Event Archiver creates it inside the database.

- § **Use global import filters when importing logs to reduce the database size.** If checked, the Import Older EVT/EVTX Files dialog uses the global import filters you have defined to limit which events are transferred from the selected EVT/EVTX files into the database table. If unchecked, ALL events from the EVT/EVTX files are imported. To learn how to set up Global Import Filters, please view that help topic *here* (on page 93).
- § **Start Import.** Starts importing records from the various EVT/EVTX files into the database and table you have selected.
- § **Cancel.** Aborts the import process. If a log import is cancelled for any reason, and the database platform you are using supports transactions, WhatsUp Event Archiver attempts to automatically rollback the transaction, effectively removing records from the files imported into the database. Only when a file is completely imported into the database is the transaction committed, with the recently imported records retained in the database table.
- § After all logs are imported, WhatsUp Event Archiver displays whether each importing job was successful, and if unsuccessful, displays the error encountered.

Viewing WhatsUp Event Archiver Log Entries

During log collection and database maintenance activity, WhatsUp Event Archiver logs all successful and failed operations to the local Windows Application Event Log. As a convenience to the administrator, WhatsUp Event Archiver provides a viewer for these events, where administrators can filter out certain types of activity (e.g. errors, warnings), as well as export diagnostic information to an HTML file.

When launched, the WhatsUp Event Archiver Log Entries dialog loads all WhatsUp Event Archiver Service events from the Windows event log. You can filter out certain types of activity by unchecking **Show Error Events**, **Show Warning Events**, and **Show Information Events**.

To copy the highlighted event to the Windows clipboard, click **Copy to Clipboard**.

To refresh all WhatsUp Event Archiver Service log entries from the local Application event log, click **Refresh Log Entries**.

To export all displayed log entries to an HTML file for further review or to send to Ipswitch Support, click **Export to HTML**.



Note: Only WhatsUp Event Archiver Service events currently present in the active Application Event Log are displayed. Older events may already be archived into saved EVT/EVTX files, and if so, you must load those older files in the Microsoft Event Viewer to view their contents.

Managing Failed Archives

Sometimes, when WhatsUp Event Archiver is processing an event log after archiving it, problems can occur on your network preventing the successful conversion or moving of the event log data. Often, these problems are due to 1.) an over-worked WhatsUp Event Archiver server, 2.) an over-worked ODBC database server, or 3.) general network issues, such as backup or anti-virus programs that close file handles.

WhatsUp Event Archiver automatically records such problem logs internally, and reattempts the data conversion and file moving operations at regular intervals after the first archive attempt. This adds a great degree of robustness to WhatsUp Event Archiver, allowing it to overcome periodic problems that may develop in your network.

Archiving retries first occur 5 minutes after the first attempt, and will continue to be retried at progressively longer intervals (15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 6 hours, 12 hours, and finally one day after the last attempt). If the final retry fails, WhatsUp Event Archiver notes this in its database, and automatically deletes the failed job 7 days after its originally scheduled date and time. It will not, however, delete any intermediary files (such as EVT/EVTX files) produced during the archiving process, allowing you to manually import or move those files as necessary.

Administrators can use the Failed Archives Dialog (available from the Tools menu) to check on logs that are currently scheduled as retried, as well as logs that will no longer be retried (e.g. that have already been retried 9 times prior), but have not yet been purged from the Failed Archives database. Within this dialog, you can manually retry the archiving operations, immediately purge them from the database, and/or view more details about any of the archiving operations listed.



Note: You can disable automatic retry of failed archives in the *WhatsUp Event Archiver Preferences* (on page 81) dialog, and you can also control how many failed archiving jobs can be retried at the same time.

Failed Archives dialog:

Failed Archives That Will Be Retried Automatically

The archives available in this list are archives WhatsUp Event Archiver Service will retry a few more times before considering them permanently failed.

- § **Refresh List.** Refreshes the list of failed archives from the internal database.
- § **View Details.** Opens the Failed Archive Details dialog you can use to examine all of the details about a particular recently failed archive job.
- § **Force Retry.** Manually forces a retry of one or more selected archiving operations. You can only force a retry 9 times; afterward, the WhatsUp Event Archiver Service considers it permanently failed and no longer attempts to automatically retry the job.
- § **Purge.** Deletes a failed archive from WhatsUp Event Archiver's internal database. Any related EVT/EVTX files, etc, remain in staging or working areas.

Permanently Failed Archives That Will Be Removed By the WhatsUp Event Archiver Service

The archives available in this list are archives that the WhatsUp Event Archiver Service has permanently failed, after 9 successive unsuccessful retry operations.

- § **Refresh List.** Refreshes the list of permanently failed archives from the internal database.
- § **View Details.** Raises the Failed Archive Details Dialog that you can use to examine all of the details about a particular archive job that has recently become permanently failed.
- § **Force Retry.** Manually forces a retry of the selected archiving operation. This can be useful since no jobs in this list will ever be automatically retried by the WhatsUp Event Archiver Service.
- § **Purge.** Deletes one or more permanently failed archives from WhatsUp Event Archiver's internal database. Any related EVT/EVTX files, etc, will remain in staging areas even if the job is deleted.
- § **Close.** Closes this dialog.

Adjusting Audit Policies Across Multiple Machines

In This Chapter

Unifying Audit Policies (Step 1).....	70
Unifying Audit Policies (Step 2).....	70
Unifying Audit Policies (Step 3).....	71

Unifying Audit Policies (Step 1)

In order to implement a more consistent security strategy across computers in your domain(s), administrators should unify the types of events they wish to audit in the security logs of their workstations and servers. WhatsUp Event Archiver allows administrators to push a similar audit policy to member servers and workstations in a domain in one operation. To unify audit policies on your member servers and workstations, invoke the Unify Audit Policies Wizard, located in the Tools menu under Step-By-Step Wizards.

In Step 1, select the member servers and workstations you would like to unify audit policies on. You can group select computers by holding down CTRL or SHIFT while selecting items with your mouse. Using the >> button to move them to the right side includes them in the unification process. Using the << button to move them to the left side excludes them from the unification process. When you are satisfied with your selections, click **Next** to continue.



Note: Domain controlling servers are intentionally not displayed in this list. If you want to adjust audit policies for an entire domain, choose the Primary Domain Controller in the WhatsUp Event Archiver Control Panel, and click the Audit Policy menu option listed from the File Menu.



Note: If you are running a Microsoft Windows 2000, 2003 or 2008 domain and have Group Policies enabled, you should use the Group Policy Editor to manage your audit policy settings for related groups of computers.

Unifying Audit Policies (Step 2)

In Step 2, choose whether you want enable auditing on the machines you selected in Step 1, and if enabled, which categories you wish to audit. For more information about each category, please view the *Audit Policy* (on page 51) dialog help topic.

Unifying Audit Policies (Step 3)

In Step 3, WhatsUp Event Archiver attempts to unify the audit policies on all of the computers you selected in Step 1. When finished, WhatsUp Event Archiver displays the successes and failures, ordered by individual computer. Double click a computer name for more details about what caused a success or failure. Click **Exit** when you are ready to return to the WhatsUp Event Archiver Control Panel.

The icon legend in the Results pane is as follows:

 - Indicates an error occurred.

 - Indicates the operation was successful.

Adjusting Log Retention/Size Across Multiple Machines

In This Chapter

Unifying Log Settings (Step 1)	72
Unifying Log Settings (Step 2)	73
Unifying Log Settings (Step 3)	73
Unifying Log Settings (Step 4)	73

Unifying Log Settings (Step 1)

It is important to choose appropriate log retention and size settings for different types of servers. Log retention settings, which determine when events can be overwritten in an event log, if ever, play an important role in security. If your retention policy is too liberal, critical log entries may be overwritten by the Event Log service, never to be seen again. Also, you must choose a log size that is big enough to accommodate the levels of auditing happening on a machine, but that is not so big as to make periodic analysis too time consuming.

In order to streamline the chore of standardizing log file sizes and retention settings, WhatsUp Event Archiver allows administrators to push similar retention settings and log sizes to member servers and workstations in a domain in one operation. To unify these settings on your member servers and workstations, invoke the Unify Log Settings Wizard, located in the Tools menu under Step-By-Step Wizards.

Choose a domain and one or more event log types that will receive the same log settings, such as a uniform file size and retention policy. The DNS Server, Directory Service, and File Replication Service logs are only available on certain Windows 2000, Windows 2003, and Windows 2008 servers. If you select them in addition to the Application, System, and Security logs, ensure that you limit your computer selection to only Windows 2000, Windows 2003, and Windows 2008 servers in Step 2. At the completion of this wizard, WhatsUp Event Archiver applies the log settings you chose to the logs on the computers you select in Step 2. When you are finished, click **Next** to continue.



Note: If you are running a Microsoft Windows 2000, 2003 or 2008 domain and have Group Policies enabled, you should use the Group Policy Editor to manage your log size and retention settings for related groups of computers.



Note: Adjusting log settings on Microsoft Vista or later computers is not yet supported. In the interim, use the Local Security Policy tool and/or Group Policy Editor to adjust these settings on Microsoft Vista computers.

Unifying Log Settings (Step 2)

In Step 2, you choose whether you want enable auditing on the machines you selected in Step 1, and if enabled, which categories you wish to audit. For more information about each category, view the *Audit Policy* (on page 51) dialog help topic.

Unifying Log Settings (Step 3)

After you have selected the computers and event logs you want to unify log settings on, use this step to define the settings that you want to apply to all of them. For more information about these settings, refer to the *Log Settings* (on page 46) dialog help topic.

Unifying Log Settings (Step 4)

In Step 4, WhatsUp Event Archiver attempts to unify the log settings on all of the logs and computers you selected in Steps 1 and 2. When finished, WhatsUp Event Archiver displays successes and failures, ordered by individual computer. Double click a computer name to find out more detail about what caused a success or failure. Click **Finished** when you are ready to return to the WhatsUp Event Archiver Control Panel.

The icon legend in the Results pane is as follows:



- Indicates an error occurred.



- Indicates the operation was successful.

Creating Database Tables

In This Chapter

Creating Access Tables.....	74
Creating Microsoft SQL Server Tables.....	74
Creating Tables on ODBC Servers.....	75

Creating Access Tables

WhatsUp Event Archiver allows you to create WhatsUp Event Archiver-compatible database tables in a variety of different ways. For example, when you use the *Log Registration Options* (on page 46) dialog or *Setup Archiving for Multiple Computers at Once* (on page 54) wizard to set up logs for archiving, WhatsUp Event Archiver can auto-create one or more tables after you connect to a data source (e.g., Microsoft Access or Microsoft SQL Server). Furthermore, you can use the Create Table dialog, available from the *Tools menu* (on page 44) in the Database Helpers section to create WhatsUp Event Archiver compatible tables in Microsoft Access or Microsoft SQL Server databases. After creating the tables, you can instruct WhatsUp Event Archiver to import event log entries into these tables when you schedule new logs for collection with the WhatsUp Event Archiver Control Panel.

Create Table dialog field descriptions:

- § **Browse and choose your database.** Click the (...) button to either find/create an Access .MDB database, or find/create a File DSN link to an ODBC data source.
- § **Tables.** After you connect to a database, WhatsUp Event Archiver automatically populates this list with all of the tables in that database. To create a new table, type in the table name below the list and click "Add."
- § **Table Name.** The name of the table you wish to create.
- § **Close.** Closes this dialog.

Creating Microsoft SQL Server Tables

WhatsUp Event Archiver allows you to create WhatsUp Event Archiver-compatible database tables in a variety of different ways. For example, when you use the *Log Registration Options* (on page 46) Dialog or *Setup Archiving for Multiple Computers at Once* (on page 54) wizard to set up logs for archiving, WhatsUp Event Archiver can auto-create one or more tables after you connect to a data source (e.g. Microsoft Access or Microsoft SQL Server). Furthermore, you can use the Create Table Dialog, available from the *Tools menu* (on page 44) in the Database Helpers section to create WhatsUp Event Archiver compatible tables in Microsoft Access or Microsoft SQL Server databases. After creating the tables, you can instruct WhatsUp

Event Archiver to import event log entries into these tables when you schedule new logs for collection with the WhatsUp Event Archiver Control Panel.

Create Table dialog field descriptions:

- § **Browse and choose your database.** Click the (...) button to either find/create an Access .MDB database, or find/create a File DSN link to an ODBC data source.
- § **Tables.** After you connect to a database, WhatsUp Event Archiver automatically populates this list with all of the tables in that database. To create a new table, type in the table name below the list and click "Add."
- § **Table Name.** The name of the table you wish to create.
- § **Close.** Closes this dialog.

Creating Tables on ODBC Servers

Although WhatsUp Event Archiver is designed to import event log data into Microsoft Access and Microsoft SQL Server database tables, it can import this data into ODBC database tables as well. The key to importing event log data into other databases is using a WhatsUp Event Archiver compatible table format. In order to create a WhatsUp Event Archiver compatible database table, you must adhere to the following field names and field data types. Consider printing this help topic and consult with your database administrator to create the following table structure. If your database server supports SQL CREATE TABLE statements, here is a sample script to generate such a table:

```
CREATE TABLE [NewTest] ([RecordNum] [bigint] IDENTITY (1, 1) NOT NULL , [DateAndTime] [datetime] NOT NULL , [Source] [varchar] (100) NOT NULL , [TypeOfEvent] [varchar] (50) NOT NULL , [Category] [varchar] (100) NOT NULL , [EventID] [int] NOT NULL , [AccountInfo] [varchar] (150) NOT NULL , [Computer] [varchar] (100) NOT NULL , [Description] [text] NOT NULL , [LogType] [int] NOT NULL);
```

Field Name	Field Data Format	Comments
RecordNum	8-byte integer	Optional auto-number/identity field.
DateAndTime	8-byte date/time	Autonumber field
Source	100-character string	
TypeOfEvent	50-character string	
Category	255-character string	
EventID	4-byte integer	
AccountInfo	150-character string	
Computer	100-byte string	
Description	Large text field	Large text (e.g. 2000+ bytes)

WhatsUp Event Archiver User Guide

LogType 4-byte integer See below for explanation

In this table, every field is self-explanatory except for the LogType field. This integer indicates the particular log file the event record came from, and works as follows:

1 Application Log

2 System Log

3 Security Log

4 DNS Server Log

5 Directory Service Log

6 File Replication Service Log

<OTHER> Custom Log files each have their own unique integer generated and assigned when they are scheduled for collection.



Note: In many cases, other database platforms may treat certain character sequences as escape sequences, which can result in missing or altered data during import. If you are using a database format other than Microsoft Access or Microsoft SQL, it is your responsibility to set up appropriate transformations and/or turn-off special character sequence processing.

Setting-up Multiple IIS/W3C Directories at Once

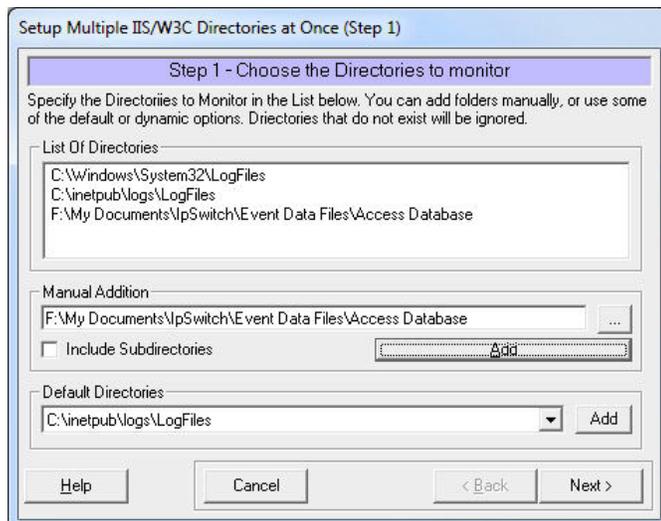
In This Chapter

Setting-up Multiple IIS/W3C Directories at Once (Step 1)	77
Setting-up Multiple IIS/W3C Directories at Once (Step 2)	78
Setting-up Multiple IIS/W3C Directories at Once (Step 3)	78
Setting-up Multiple IIS/W3C Directories at Once (Step 4)	79
Setting-up Multiple IIS/W3C Directories at Once (Step 5)	80
Setting-up Multiple IIS/W3C Directories at Once (Step 6)	80

Setting-up Multiple IIS/W3C Directories at Once (Step 1)

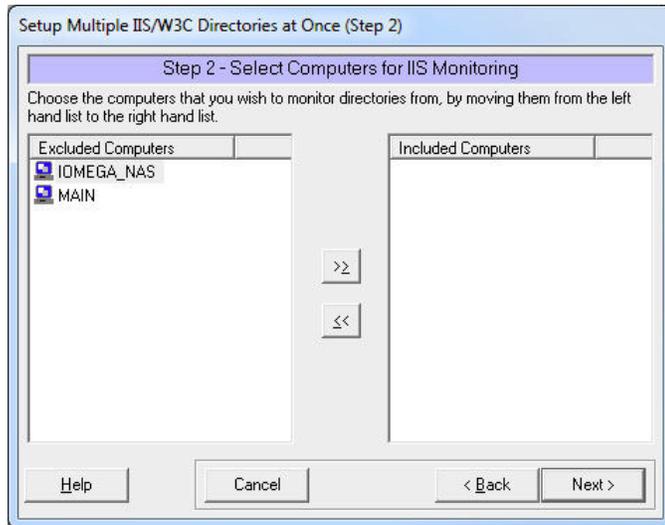
The Setting up Multiple IIS/W3C Directories at Once wizard assists with collecting and working with your IIS/W3C formatted logs generated by IIS servers running FTP, WWW, ISA, and SMTP services. WhatsUp Event Archiver supports the collection, compression, and storage of IIS/W3C log files into database tables.

In Step 1, choose the directories you want to monitor. A list of your directories displays, and you can manually add directories using the Manual Addition field and the Add button. You can also add default directories. When you are satisfied with your settings, click **Next**.



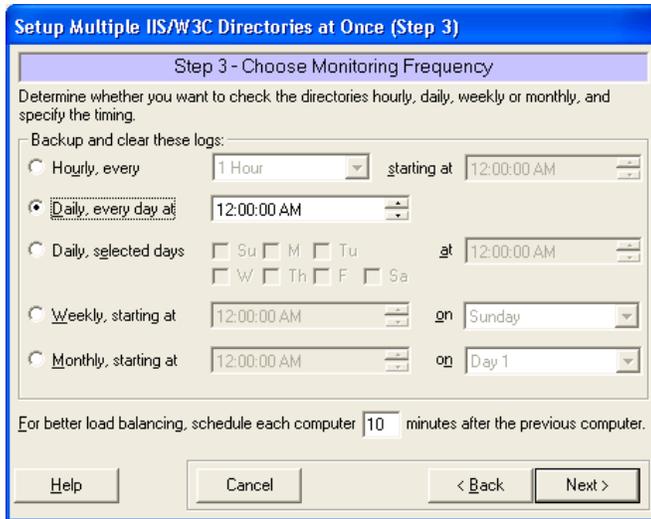
Setting-up Multiple IIS/W3C Directories at Once (Step 2)

In Step 2, select the computers you want to monitor directories from. Computers on the left are excluded from monitoring; computers on the right are included. To move computers from one side to the other, select the computer you want to move, then click the appropriate arrow to move the computer. When you are satisfied with your selections, click **Next**.



Setting-up Multiple IIS/W3C Directories at Once (Step 3)

In Step 3, choose a monitoring frequency. From this step, you can set whether you want to monitor your directories hourly, daily, weekly, or monthly. You can also specify the time and day on which you want monitoring to occur. Finally, for better load balancing, you can schedule out the collection of IIS/W3C logs by several minutes per computer. Valid ranges are between 1 and 150 minutes. When you are satisfied with your settings, click the **Next** button.

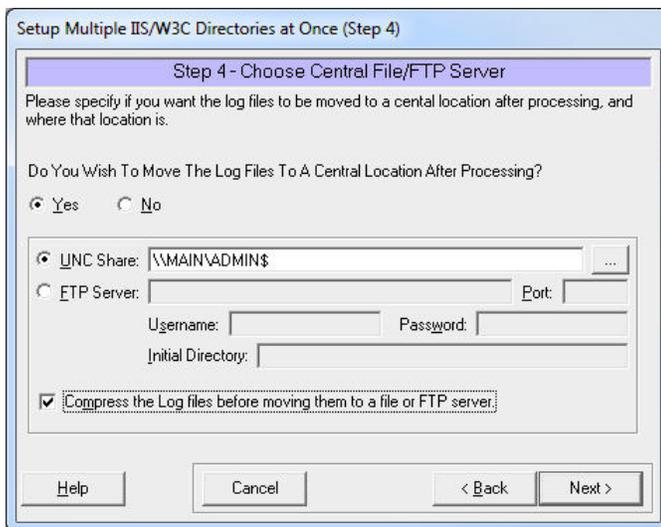


Setting-up Multiple IIS/W3C Directories at Once (Step 4)

In Step 4, specify whether you want log files moved to a central location after processing. In addition, specify the location to which you want processed log files stored. When you are satisfied with your settings, click the **Next** button.

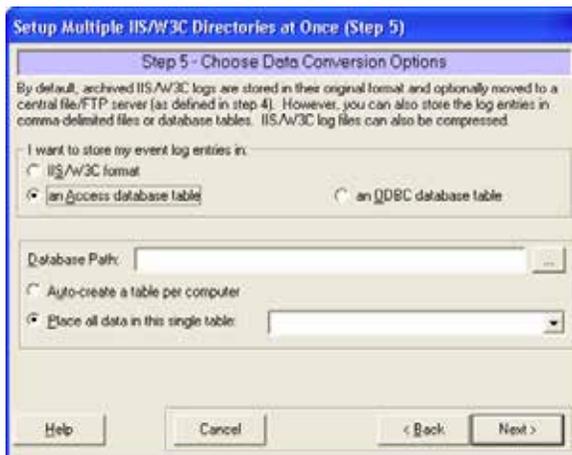


Note: In Step 5, you have the option to choose whether you want to store log entries in IIS/W3C format, as an Access database table, or an ODBC database table. If you want to store the entries in IIS/W3C format, you must choose a destination directory in Step 4.



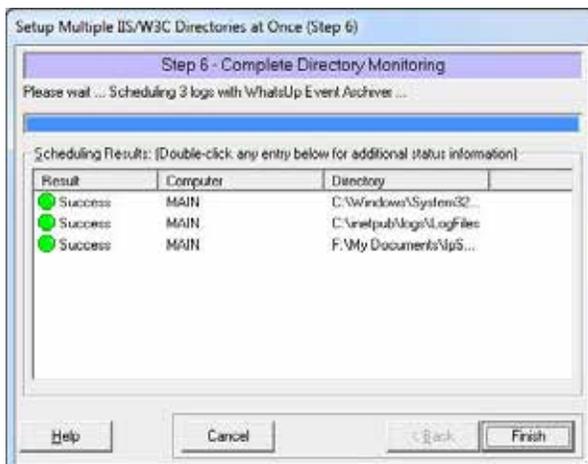
Setting-up Multiple IIS/W3C Directories at Once (Step 5)

In Step 5, you can choose data conversion options. By default, archived event logs are stored in EVT/EVTX format, and optionally, moved to a central file/FTP server. However, you can also store the log entries in IIS/W3C format, comma-delimited files, or database tables. If you want store event log entries in IIS/W3C format, you must choose a destination directory for the logs in Step 4. If you want event log entries stored in an Access database table or an ODBC database table, select the appropriate option, indicate the database path, and indicate table settings. When you are satisfied with your settings, click the **Next** button.



Setting-up Multiple IIS/W3C Directories at Once (Step 6)

In Step 6, your scheduling results designated using the wizard display. Double-click any entry for additional status information. If you are satisfied with your results, click the **Finish** button to complete setting up your IIS/W3C directories.



Configuring WhatsUp Event Archiver and Setting Defaults

In This Chapter

Setting Up Archiver Preferences.....	81
Configuring the WhatsUp Event Archiver Service Account.....	89
Setting the Default Domain or Workgroup	90
Managing Custom Domain to Computer Mappings	91
Global Settings - Retrieving Computer Names.....	92
Managing Custom Logs.....	92
Setting Global Import Filters.....	93

Setting Up Archiver Preferences

The WhatsUp Event Archiver Preferences page, available from the Options menu, controls how the WhatsUp Event Archiver Service works, and also governs the settings used by WhatsUp Event Archiver whenever an administrator attempts to schedule a new log for archiving. The tabs governing archiving behaviors do not globally reconfigure all existing log archiving settings. Rather, they are used whenever an administrator attempts to schedule new logs for collection, individually or in a group. You can think of them as a time saving feature that aids you as you start to collect logs from more computers.

Below is an explanation of all the tabs and fields in the WhatsUp Event Archiver Preferences page.

Log tab

Use this tab to set which event log is the default when adding new logs to WhatsUp Event Archiver.

Log. Use the list box to select which of the following event log types you want to set as default when adding new logs to WhatsUp Event Archiver.

- § Application
- § Archived Syslog Messages (custom)
- § Directory Service
- § DNS Server
- § File Replication Service

§ Security

§ Syslog

§ System

When finished, click **Submit**.

Schedule tab

Set Schedule. Set how often you want event logs archived. Choose the **Hourly** option if you need to continuously archive event logs every few hours. WhatsUp Event Archiver then attempts archives every 1, 2, 4, 6, or 12 hours from the starting time, depending on your selected interval.

If you choose **Daily - Everyday**, provide a time, and WhatsUp Event Archiver attempts the archive operation each day at that time. Alternatively, you can choose to archive **Daily - Selected Days** to archive at the same time on certain days in the week. If you choose **Weekly** or **Monthly**, pick a day of the week or month and a time when WhatsUp Event Archiver attempts this archive.

The default schedule setting is **When log is full**. If you choose this option, WhatsUp Event Archiver monitors the server 24/7 to see if the log is approaching its file size limit. When the log is within a certain size (the default setting is 64K) of its administrator-defined limit, WhatsUp Event Archiver automatically archives the log. If you choose this option, the **Clear log after archiving** option must always be set to **Yes**. For network administrators sensitive to bandwidth issues, the impact of monitoring each log 24/7 is minimal, as it only requires a few hundred bytes of data transfer for each query.

§ **Clear log after archiving.** Selecting **Yes** instructs WhatsUp Event Archiver to clear the log after saving it to the server's disk. Choosing **No** instructs WhatsUp Event Archiver to perform a backup of the log without clearing the current log entries.

Staging Area tab.

Before a log can be transported to a file server, or converted into a different data format, it must first be saved to a staging area on the originating server. This tab allows you to define the staging folder on the originating server, and the share folder that WhatsUp Event Archiver uses to access data files placed in the staging folder.

§ **Staging directory on remote machine to temporarily save EVT/EVTX files in.** Every time WhatsUp Event Archiver archives a log, it must first save that file to an area on the remote machine's local hard disk. The recommended/default value for this location is C:\WINNT. However, you must make sure that this path does correspond to a local drive and folder on the remote machine, or the archiving process will fail. When adding new logs, some machines may have a different drive letter (e.g. D:) assigned to the system drive.

Note about the default C:\WINNT path. If you leave the default value of C:\WINNT here, WhatsUp Event Archiver archives the log properly, even if the remote computer's system root folder is C:\WINDOWS. WhatsUp Event Archiver tries C:\WINDOWS if C:\WINNT does not exist.

§ **Share folder used by Event Archiver to grab EVT/EVTX files saved in the staging area.** To consolidate log files to a central location or database, WhatsUp Event Archiver needs to access them over the network. The recommended/default setting is ADMIN\$. When you register a new log, WhatsUp Event Archiver automatically appends the server name to the share name to make a fully qualified UNC share. Always double check that this share folder corresponds to the directory on the remote machine where the EVT/EVTX files are initially saved.

Data Conversion tab.

This tab allows you to specify the formats and locations for event log consolidation.

Store the log data in. From here, define how you want WhatsUp Event Archiver to format your event log entries after they are archived. Select **Event Viewer (EVTX) format** if you want WhatsUp Event Archiver to leave the log files in their native format after archiving. You can use the Microsoft Event Viewer to read this file format. **A comma-delimited text file** causes WhatsUp Event Archiver to convert the EVT/EVTX file into comma-delimited records, with each new line in the file representing a new log record. If you choose **an OLE DB connection**, WhatsUp Event Archiver attempts to place the log records into a SQL Server database.



Note: If you are archiving logs from many different servers (100 or more) and do not want to convert the entries into a central database, you may want to archive and collect the logs in EVT/EVTX format only. It is a relatively CPU-expensive (and to a lesser degree, network expensive) process to import event log entries into other formats. WhatsUp Event Archiver does have a multiprocess architecture to minimize such performance impacts; however, if you have a large LAN, you should evenly distribute archiving times so that all logs are not operated on at once.



Note: Even if you choose a format other than EVT/EVTX, you can still keep your original EVT/EVTX files that are archived, optionally compressing them and storing them in a central location. If you want WhatsUp Event Archiver to keep the original archived EVT/EVTX file, simply leave the **Delete the EVT/EVTX file after successful conversion** option unchecked below, and choose an appropriate location where the files should be moved to in the Final Destination tab.

§ **Database Connections.** If you elect to import log entries into an Access or SQL Server database, you have to let WhatsUp Event Archiver know where the database is to insert the log entries into.



Tip: Its recommended that you use standard (non-trusting) authentication if you are importing event log entries into a Microsoft SQL Server database. If you do elect to use a Trusted Connection to the database, you must make sure that the database is configured so that the service account that WhatsUp Event Archiver runs under has read and write permission to all associated databases and tables. Also, if you use Standard Authentication, you can consolidate log entries from many different non-trusting domains/workgroups into a single database, if desired.

- § **Table Name.** After you select a database, you need to tell WhatsUp Event Archiver what table you want to place the event log entries into. After you connect to a database, WhatsUp Event Archiver automatically populates this list with all of the tables in the database. You can choose an existing table, or by typing in a new name, have WhatsUp Event Archiver automatically create one for you.



Note: If you choose an existing table, you must make sure that it is a WhatsUp Event Archiver compatible table with the correct fields and datatypes. To create WhatsUp Event Archiver compatible tables, open the Database Helper located in **Organization > Common Settings**.

- § **Delete the EVT/EVTX file after successful conversion.** If you choose to import the event log data into a format other than the native .EVT/.EVTX format, you can make WhatsUp Event Archiver delete the EVT/EVTX file created when the archiving first took place. However, you can also keep the EVT/EVTX file so you have two different copies of the data in different formats. If this option remains unchecked, WhatsUp Event Archiver moves your EVT/EVTX file to a central file server if you specify one in the Final Destination tab.
- § **Compress the EVT/EVTX and/or comma-delimited text files before moving them to a file or FTP server.** On average, zipping an EVT/EVTX or text file yields an average 95% compression ratio. For example, compressing a 100MB EVT file produces a ZIP output file approximately 5 to 7 MBs in size. Compression is a nice feature for two reasons:
 - § If you need to maintain a very long archive of audit data (e.g. 2 years or more), compression allows you to store 20 times more data on file servers.
 - § If you need to minimize traffic across WAN segments, you can have WhatsUp Event Archiver compress the files on a remote WAN end before transmitting them over a WAN link provided you have multiple installations of WhatsUp Event Archiver.

Final Destination tab.

This tab allows the administrator to specify the location where flat files (e.g. EVT/EVTX and/or text files) should be moved. Destination options include a file server on the local area network, or a FTP server.

- § **After archiving.** Regardless of the data format you choose, you can have WhatsUp Event Archiver move the initial EVT/EVTX file that was saved (and/or the comma-delimited text file) off of the remote machine to a central network share or an FTP server for storage. This frees up space on the local machine, and lets you keep an extra copy of the EVT/EVTX file even after the data is imported into a database.
- § **UNC Share.** You can click the (...) button to select a UNC share.



Note: This share must already exist on a remote machine - WhatsUp Event Archiver automatically adds the service account to the share's access control list so that it can move the files. The share folder you enter must be in fully qualified UNC format (e.g. \\SERVERNAME\ShareName). Also, this share must be a top-level share. That is, it cannot contain a subfolder underneath the main share folder. For example, "\\SERVERNAME\ShareName" is a correct setting, while "SERVERNAME\ShareName\SubfolderName" is not correct.

- § **FTP Server.** If firewall settings prohibit you from reaching a file server via standard Microsoft Networking, you can FTP the files to an FTP Server. Enter the fully-qualified Internet domain name or IP address of the FTP server in this field.
- § **Port.** The standard port for FTP transfers is 21, but you can specify a non-standard port for additional security. Make sure the FTP Server is configured to receive files on this port.
- § **User name.** Enter the user name needed to log on to the FTP server.
- § **Password.** Click the link to set or reset your password.
- § **Initial Directory.** If needed, you can specify an initial directory where your log files should be stored. If this field is used, WhatsUp Event Archiver attempts a change directory (CD) command on the FTP server after connecting. Leave this field blank if you want files placed in the root directory.

Performance Tuning tab.

Each additional log you register with WhatsUp Event Archiver puts an added burden on the WhatsUp Event Archiver Service. However, by optimizing the following tuning categories, you can somewhat offset that burden.

- § **Processor Utilization.** If you have registered a lot of servers for archiving (40+), you may want to move this slider closer to the **Lower CPU Utilization** side. In general, this slider controls how much of a rest period the service takes between checking on the next log in its database. The only downside to choosing a larger rest period is that it may result in logs not getting archived if the service rests too long in a large database of logs. However, you can virtually eliminate this possibility by properly setting the **Archiving Time Grace Window** option.
- § **Unavailable Machine Persistence.** When archiving logs based on file size, WhatsUp Event Archiver checks the file size of the log at a regular interval to see if it is ready for archival. When machines are not on the network, the attempt to check the log's file size causes a small timeout. By changing this number, you can determine how persistent WhatsUp Event Archiver is at checking the file sizes of logs whose machines were previously not on the network. Greater machine persistence increases network timeouts when machines are not available.
- § **Log Fullness Definition.** If you elect to have WhatsUp Event Archiver clear your event logs when the log is full, you can use this setting to adjust when a log is full. For example, if the file size limit for a log is 1024KB, and the Log Fullness Definition is 192KB, then WhatsUp Event Archiver attempts to archive the log when it reaches a size of 832KB. The default and recommended setting for the log fullness definition is 64KB.
- § **Always Archive When Full.** This option is a global setting that affects all logs registered with the WhatsUp Event Archiver Service. If checked, WhatsUp Event Archiver always archives any log that comes close to meeting its file size limit, regardless of its normal scheduled archiving time. For example, if you schedule a log for archival every Friday at 11:00PM, but the log fills up at 4:00AM Thursday, the WhatsUp Event Archiver Service automatically archives the log as to prevent any events from being overwritten.



Note: This option creates more overhead for the WhatsUp Event Archiver Service and slightly increases the bandwidth load on your network, so only use it if necessary.

- § **Archiving Time Grace Window.** If you register a large number of logs with the WhatsUp Event Archiver Service, the service may not reach logs that are scheduled for daily or weekly collection at the exact minute in the time you have specified. This option determines how many grace minutes can elapse before the service no longer checks to see if the log needs archiving. For example, if you set the grace minute interval to 5 minutes, and a log is scheduled to be archived at 2:00 AM, even if the service does not reach that log until 2:04 AM in the archiving sequence, the log is still archived.
- § **ICMP (Ping) Testing.** This option enables WhatsUp Event Archiver to perform a ping test operation on servers before it attempts to monitor the size of their log files. While this option can greatly improve performance, you may want to disable it if you are not using the TCP/IP protocol on your network, or if ICMP is disabled on your network. You can also control the timeout in milliseconds that WhatsUp Event Archiver waits for an ICMP response. Valid ranges are between 5 ms and 2000ms. The more latency on your network, the longer the timeout period recommended.

General tab.

This tab governs other settings controlling WhatsUp Event Archiver operation.

- § **Date Format Used in EVT and TXT filenames.** When saving event logs to disk in either the native EVT format or comma-delimited text files, WhatsUp Event Archiver uses a special file naming convention to help you keep track of when the logs were saved. In the Month/Day/Year format, log files have this convention:

COMPUTERNAME + LOGTYPE + Day-Month-Year + "@" + Hour-Minute-Second

(e.g. MARSapp3-4-1999@10-3-56.evt)

Using the **Day/Month/Year** format, the convention looks like this:

COMPUTERNAME + LOGTYPE + Month-Day-Year + "@" + Hour-Minute-Second

(e.g. MARSapp4-3-1999@10-3-56.evt)

- § **Date Format Used in Text Conversion Routines.** This option controls how WhatsUp Event Archiver constructs dates before inserting log records into either a text file or an ODBC database. The default setting is for WhatsUp Event Archiver to use the Regional System Settings, which are specified in the Regional Settings section of the Control Panel. For example, U.S. dates are formatted mm/dd/yy, but European dates are often formatted dd/mm/yy. Alternatively, you can set WhatsUp Event Archiver to use the U.S. format when performing these conversions. The settings you choose affect how dates are output to files and input into ODBC databases.
- § **Connection String Security.** Occasionally, the WhatsUp Event Archiver Service logs diagnostic information to the Application event log where it is running. If the connection string used for your database contains sensitive (e.g. password) information, you can set this option to omit the connection string from any event log entries.

- § **Error Notifications.** You can have WhatsUp Event Archiver notify you by email every time an error or warning occurs in an archiving operation. Check the items you wish to be notified about (e.g. recoverable errors, unrecoverable errors, and/or warnings), enter the email address you want these message sent to, an SMTP server to relay the messages through, and a valid sender address (e.g. account@yourdomain.com).



Note: In order to relay messages successfully, the SMTP server must be set up to accept messages from the machine running WhatsUp Event Archiver. This typically requires configuring IP relaying restrictions on the SMTP server. We recommend using the Microsoft SMTP Service that is a part of Internet Information Server (IIS) for this purpose.



Note: Check **Send email about unrecoverable errors** by itself if you only want to be emailed when an archiving job has permanently failed (e.g. it could not be completed after 2 days of retries.)

- § **Failed Archives.** In some circumstances, you may wish to disable WhatsUp Event Archiver's automatic retry mechanism for failed archives. If you check this option, failed archiving operations are permanently failed, but you can always reattempt them manually.
- § **Allow a maximum of X archiving retry attempts to run at the same time.** Here is where you control how many failed archives WhatsUp Event Archiver attempts to process at the same time; the default value is 5. While setting the value higher may reduce the amount of time WhatsUp Event Archiver needs to catch up on its archiving after a network or database server failure, a higher value may also place a great stress on the network and database server. Adjust this setting carefully.

Vista and Newer tab.

Use this tab to govern how WhatsUp Event Archiver converts Microsoft Vista and Microsoft Windows Server 2008 logs out of EVTX format into new formats.

- § **Vista & Newer: For security logs into new data formats, change Information event to Success Audits and Failure Audits as appropriate.** When checked, WhatsUp Event Archiver converts the Level field in a security EVTX file from Information to Success Audit or Failure Audit in the text file or database table, depending on the nature of the event. This feature is useful if you are analyzing Microsoft Vista and/or Microsoft Windows Server 2008 security events alongside events from older operating systems in a central database.
- § **Vista & Newer: For security logs into new data formats, place User information from the Description field into the User field as appropriate.** Microsoft Vista does not record information about the user performing the action or *affected by the action* in the User field or the Security log. This option makes WhatsUp Event Archiver extract the most appropriate user from the Description field of each EVTX record and place it in the User field in the converted text file or database table.
- § **Vista & Newer: For events that log keywords and opcodes, append those fields to the Category field (e.g. Category:Keyword:Opcode).** To maintain a common number of fields between EVT and EVTX files that are output into text files and database tables, WhatsUp Event Archiver appends the Keyword and Opcode fields to the Task/Category field in an EVTX record when converting it into a new format. The consolidated Task/Category field also contains the Keyword and Opcode fields.

File Hashing tab.

This tab controls whether MD5 cryptographic hashes or AES-256 cryptographic hashes are generated when flat files are created during the archiving process.

Automatically generate a hash for all flat files (e.g. EVT, EVTX, TXT) archived by WhatsUp Event Archiver, and log this hash in the local Windows Application Event Log alongside other program operations. Check the check box so that the selected hash is placed in the Windows Application event log on the machine where WhatsUp Event Archiver is installed, alongside the description of the archiving action taken by the WhatsUp Event Archiver Service. If selected, WhatsUp Event Archiver checks to determine whether the operating system is in FIPS mode. If not, an error displays. At the time of the SHA-256 checksum hashing during log archiving, if an appropriate cryptographic provider that is FIPS 140-2 validated cannot load, a warning message is immediately generated following the archiving action in the Windows Event log from the WhatsUp Event Archiver service.



Note: Hashing against large EVT/EVTX files should not be attempted over the network. For this reason, if you enable this option, please also set an appropriate size for the Working Directory in the Bandwidth Optimizer tab (see below).

Bandwidth tab.

Use this tab to control how WhatsUp Event Archiver fetches log records from Microsoft Vista EVTX files, as well as whether it uses a local working directory when processing EVT and EVTX files.

- § **EVTX Log Record Fetching Limit.** The value entered here determines how many records WhatsUp Event Archiver fetches at the same time for processing into a new format (e.g. a text file or database table). The default value is 40, but this limit can be lowered or raised depending on your network's topology and available bandwidth.
- § **Move EVT/EVTX Files Bigger Than _____.** Use this list box to select a log file size that prompts WhatsUp Event Archiver to copy the EVT/EVTX file from the staging area on the remote machine to the Working Directory on the WhatsUp Event Archiver computer. Any log archived that is larger than this size is automatically transported to the Working Directory for further processing.
- § **Local Working Directory.** Click the ellipsis button (...) to change the directory used by WhatsUp Event Archiver as the local working directory. This directory should be on a local (non-network) drive, and should have enough space to handle many multiples of the largest file size being archived, especially if multiple logs may be archiving at the same time.
- § **Syslog CSV File Limit.** The value entered determines the maximum size of the .csv files written by Syslog Write to CSV File and temporary .csv files for Syslog Direct Write's failover feature when messages cannot be written to the database.
- § **Restore Syslog Messages from CSV to DB automatically.** Indicate if you want messages in temporary .csv files written by Syslog Direct Write's failover feature automatically inserted into the database when the database connection is restored.

Configuring the WhatsUp Event Archiver Service Account

The Service Account dialog configures the WhatsUp Event Archiver Service to run under a specific user account. If WhatsUp Event Archiver is installed on a computer participating in a domain, this account should have domain admin rights, or at minimum, a domain user account with local administrative rights on all member servers and workstations being archived (e.g. an Organizational Unit admin account), because it is responsible for saving and reading event logs on domain computers over the network. If you are running WhatsUp Event Archiver on a computer not participating in a domain, or are monitoring several machines in a workgroup with a common administrative account and password, select a local account on that same machine, which is a member of the local Administrators group.

Setting Up the WhatsUp Event Archiver Service with the Service Account dialog field descriptions:

- § **I want to choose a domain account from a domain.** WhatsUp Event Archiver populates the Account Name listing with all of the user accounts present in your primary domain.
- § **I want to choose a local account from this computer.** WhatsUp Event Archiver populate the Account Name listing with all of the user accounts present on the local computer where WhatsUp Event Archiver is installed.
- § **Account Name.** Choose the name of the user account you want the WhatsUp Event Archiver service to run under. If for any reason WhatsUp Event Archiver cannot automatically populate this list with account names, you can type in an account name yourself. Ensure that the account name is in a fully-qualified format (e.g. DOMAINNAME\AccountName). For example, if you create an account named EAService in the DORIAN domain, you would type in DORIAN\EAService.
- § Again, Ensure that this user account is in the local Administrators group on each member server/workstation in the domain, if monitoring multiple computers in a domain(s). The easiest way to do that is to ensure it is a member of the Domain Admins group, or an OU Admins group created for a specific OU.
- § Alternatively, if you are only planning to archive logs from the local computer, or are planning to archive logs from other workgroup machines that have a common administrator account, designate the service account a local administrator. The WhatsUp Event Archiver service does not run properly under a LocalSystem context.
- § Finally, select an account that is not subject to routine password expiration. If the WhatsUp Event Archiver Service account password expires, the service stops working and archiving jobs are not completed.
- § **Password.** Type in the password of the account you listed in the Account Name field.
- § **Confirm Password.** Retype the password for verification.
- § **OK.** WhatsUp Event Archiver reconfigures the WhatsUp Event Archiver Service to run under the account you have specified. In addition, it attempts add the Log on as a service and Act as part of the operating system user rights to the account to ensure proper operation. If for any reason it cannot add these user rights (e.g. this happens typically when your currently logged-on account is not an admin), it displays a warning message with instructions on how to add these rights manually.

- § **Cancel.** Aborts the account reconfiguration process and leaves the current WhatsUp Event Archiver Service account unchanged.

Setting Up the WhatsUp Event Archiver Service Account Manually:

If for any reason you cannot set the WhatsUp Event Archiver Service account from within the Service Account dialog, you can perform this process manually by visiting the **Control Panel > Services Applet** (on NT 4.0 systems) or **Control Panel > Administrative Tools > Services** (on 2000/XP/2003/Vista/2008/Windows 7 systems).

Before assigning your service account to the WhatsUp Event Archiver Service, verify the following:

- § That the service account is a local administrator (e.g. in the local Administrators group) on every member server and workstation you plan to archive. The easiest way to accomplish this is to make it a member of the Domain Admins group, or an OU Admin group for a given organizational unit. If you plan to archive domain controllers, only Domain Admins can perform this action.
- § That the service account holds the following user rights (either explicitly or through group membership). You may need to adjust domain-wide or ou-wide group policies to accomplish this.
 - § Log on as a service
 - § Act as part of the operating system
 - § Manage auditing and security log
- § That the service account's password will not expire due to account policies in your domain.

Once you have verified these aspects of your service account, assign it to the WhatsUp Event Archiver Service in the Services listing on the local machine. Also, set the WhatsUp Event Archiver Service startup type to Automatic, so it loads when the machine first starts up.

Setting the Default Domain or Workgroup

The primary domain governs what Windows domain WhatsUp Log Management uses to display computer accounts, user accounts, and other domain objects. Alternatively, this can specify a workgroup, if WhatsUp Log Management is not installed on a computer participating in a domain.

To set the default domain or workgroup:

- 1 Click **Organization > settings > Global Settings** and then select the **Domain/Workgroup** tab.
- 2 Indicate whether you are managing a domain or a workgroup by selecting the appropriate radio button.
- 3 In the Default Domain/Workgroup field, enter either your Domain name or Workgroup name.

Managing Custom Domain to Computer Mappings

As networks grow and merge, domain and workgroup structures expand in size and complexity. In many cases, event logs must be collected from multiple computers that reside in different domains, workgroups, or organizational units. WhatsUp Event Archiver helps resolve this potential problem by allowing network administrators to create custom domains.

For example, delegation of administration may require you to manage specific servers in three different organizational units of a larger domain. Or, in another scenario, you may have to collect logs from servers and workstations that reside in different workgroups. Using WhatsUp Event Archiver, you can map these individual computer names to a custom domain. Then, you can easily reference that custom domain to adjust log collection settings on all of the computers at once using WhatsUp Event Archiver's built-in wizards.

To manage custom domain to computer mappings:

From the WhatsUp Event Archiver control panel, click the **Options** menu, and then select the **Manage Custom Domain to Computer Mappings** option. The Manage Custom Domains dialog opens.

Complete the fields in the open dialog, and then click **OK**.

Examples of Computer to Custom Domain Mappings:

Computer Name	Custom Domain Name
COMPUTER1	MYDOMAIN1
COMPUTER2	MYDOMAIN1
COMPUTER3	MYDOMAIN2
COMPUTER4	MYDOMAIN2

If the following computer and custom domain mappings are created as above, WhatsUp Event Archiver displays two additional domains in its domain list in the upper right hand corner of the WhatsUp Event Archiver Control Panel, specifically CUSTOM: MYDOMAIN1 and CUSTOM: MYDOMAIN2. When you change focus to one of the custom domains, WhatsUp Event Archiver displays all computer logs scheduled for collection in that custom domain. Furthermore, when you manually scheduled a computer log for collection, or when you run a wizard to schedule collection on many computers' logs at the same time, WhatsUp Event Archiver displays all of the computer names associated with the custom domain that is currently in focus.



Note: In order to collect all types of logs successfully from computers, the WhatsUp Event Archiver Service must run under an account whose user name and password is a.) common to all machines in the custom domain whose logs are collected, and b.) an account that has administrative rights on those systems.

Adding Computer Names or IP Addresses of Computers To a Custom Domain

- § **Computer / IP Address.** Enter the name of the computer or its IP address.
- § **Custom Domain Name.** Enter the name of the custom domain you want associated with this computer or IP address.
- § **Create Mapping.** When you click this button, the computer name entered above is associated with the custom domain, and appears in the list below.
- § Removing Computer Names or IP Addresses of Computers From a Custom Domain
- § **Remove Computer(s).** Removes all the selected computers in the list above, effectively disassociating them from the custom domain.
- § **OK.** Saves computer to custom domain mappings.
- § **Cancel.** Cancels the operation without saving the changes.

Global Settings - Retrieving Computer Names

To retrieve computer names:

- 1 Click **Organization > settings > Global Settings**, and then click the **Retrieval** tab.
- 2 Complete the fields, and then click **Submit**.

Retrieval Options

- § **The Browser List.** Choose this option if you are using WhatsUp Log Management for logs in a workgroup, not a domain. WhatsUp Log Management uses the master browser in the workgroup to list active computers currently online in the workgroup.
- § **The AD Server / Domain Controller.** Choose this option if you are using WhatsUp Log Management for logs from a domain or multiple domains. When selected, WhatsUp Log Management always enumerates all computer accounts directly from the domain controller / active directory server; this can take some time on very large domains.
- § **The Following OU in Active Directory.** If you are only working with logs on servers in a particular organizational unit in your Active Directory, select this option. Once selected, enter the Organizational Unit from which you want to retrieve computer accounts.
- § **Computer Retrieval Credential.** Credentials for the computer being accessed.

Managing Custom Logs

Typically, 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 creating their own custom Windows event logs for error tracking and reporting. WhatsUp Event Archiver provides you with the option to define custom event logs and display them alongside the Microsoft Windows logs.

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

- 1 From the WhatsUp Event Archiver Control Panel, click the **Options** menu, and then select the **Manage Custom Logs** option. You can browse to various computers to view the custom Windows event logs present on any given system.
- 2 If you wish to make a custom event log available for collection by WhatsUp Event Archiver, select it from the list, and then click the **Add Custom Log** button *or* if you no longer wish to see a particular custom event log as available for collection throughout WhatsUp Event Archiver's Control Panel, select it from the **Custom Event Logs Defined** list and click the **Remove Custom Log** button.

In some cases, you may be unable 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; determine the internal name by finding that logs subkey under the HKLM\System\CurrentControlSet\Services\EventLog section of that computer's registry.

Setting Global Import Filters

One of the challenges of retaining a large central repository of events is controlling database size. WhatsUp Event Archiver allows you to explicitly control which events get imported from EVT/EVTX files into an Access or ODBC database through the use of Global Import Filters.

There are two approaches you can use to restrict the number of events that are imported into your database.

To set global import filters:

- 1 From that WhatsUp Event Archiver control panel, click the **Options** menu, and then click **Set Global Import Filters**. The Global Import Filters dialog appears.
- 2 Set global import filters using the Global Import Filters dialog.
- 3 After setting global import filters, click **OK**.

Import Only the Events Listed Below Into the Database

With this option enabled, only specific events you define are imported into your database. All other events are dropped. This setting is useful if you are only planning on reporting and/or tracking a discrete range of activity (e.g. Logon Failures and Account Management events).

Exclude All the Events Listed Below From Import Into the Database

This option allows you to choose a few events that you want WhatsUp Event Archiver to drop during database import operations. All other events not in the list are imported. This setting is useful if you have isolated events that are not needed for analysis, but are over-represented in the collected data.

- § **Quick Add.** Opens the Global Import Filter Selector dialog, allowing you to quickly select many common Windows events for use as filters.
- § **Add.** Adds a new event definition to the import filters listing.
- § **Edit.** Allows you to edit an existing event definition.
- § **Delete.** Deletes the selected event definition.
- § **Save.** Saves the filter you are adding or editing.
- § **Cancel.** Abandons changes to the filter you are adding or editing.
- § **Log Type.** Select the log type (e.g. Application, System) where this event is found.
- § **Event Source.** Enter in the Source field of the event, exactly as it appears in the Event Viewer.
- § **Event ID.** Enter in the Event ID numeric code of the event, exactly as it appears in the Event Viewer; you can create a filter that looks for all events from a specific source by entering in -1 in the Event ID field.
- § **Type.** Select the event types you want the filter to look for. To make the filter match all event types, select **All Event Types**. To target specific event types, choose **Specific Event Types**, and then place a check mark by the event types matching the filter.
- § **Close.** Closes the dialog and saves any changes you have made to your global import filters.
- § Once global import filters are defined, every time an archive operation takes place that inserts data into a database table, these filters control the log records placed in the database. Information on the number of events dropped for any given import operation is placed in the Application Event log as an event from the WhatsUp Event Archiver Service.

Managing Syslog Messages

In This Chapter

Syslog Messages in WhatsUp Event Archiver	95
About Syslog Direct Write and Syslog Write to CSV File.....	96
Selecting Syslog Direct Write and Syslog Write to CSV File preferences	96
Setting up Syslog Direct Write.....	96
Configuring Syslog Direct Write database settings.....	98
Setting up Syslog Write to CSV File	101
Configuring Syslog Archiving Settings.....	102

Syslog Messages in WhatsUp Event Archiver

From the WhatsUp Event Archiver control panel, you can configure how you want to receive and archive Syslog messages. WhatsUp Event Archiver offers three options for archiving Syslog messages which work independently, but can be used concurrently:

- § **Syslog Archiving** writes Syslog messages to the Archived Syslog Messages custom event log. Event Archiver can then operate on the Archived Syslog Messages event log much as it does with Windows and other custom event logs. It supports the same tools for managing the log files and options for storing messages in .csv files, Access databases, or ODBC databases, compressing the log files, moving the files to a UNC share or FTP server, and cryptographic hash generation.
- § **Syslog Direct Write** supports high volume writing of Syslog messages directly to a SQL Server database. With Syslog Direct Write, Event Archiver does not first write the messages to a custom event log file, so it does not support the log file management and data archiving options of Syslog Archiving. However, Syslog Direct Write is much more efficient at archiving messages directly to a SQL Server database and able to reliably handle high message throughput rates. Event Archiver's Automatic Database Maintenance tool allows for the management of the Syslog Direct Write SQL Server database table.
- § **Syslog Write to CSV File** supports high volume writing of Syslog messages directly to .csv files. Syslog Write to CSV File also does not support the log file management and data archiving options of Syslog Archiving, including the compression, moving, and purging of its .csv files. You must implement or integrate with your own processes outside of Event Archiver for moving and purging its .csv files. Syslog Write to CSV File supports very high message throughput rates generating .csv files you can incorporate into your own long term storage processes.

About Syslog Direct Write and Syslog Write to CSV File

Syslog Direct Write and Syslog Write to CSV File are optional, more efficient methods of adding Syslog messages directly to a SQL Server database or to a .csv file, respectively. They avoid first writing messages to an EVT file, like Syslog Archiving does, and can support much higher message throughput rates. They do not support the file moving, compression or purging of Syslog Archiving. While Syslog Direct Write, Syslog Write to CSV File, and Syslog Archiving work independently of one another, they may be used simultaneously.

Selecting Syslog Direct Write and Syslog Write to CSV File preferences

WhatsUp Event Archiver allows you to customize the size of both the temporary recovery .csv files for Syslog Direct Write's failover feature when messages cannot be inserted to the database and the storage .csv files from Syslog Write to CSV File.

To configure Syslog Direct Write preferences:

- 1 Launch WhatsUp Event Archiver.
- 2 Click **Options > WhatsUp Event Archiver Preferences**.
- 3 Select the Bandwidth Optimizer tab.
- 4 Specify the Syslog CSV Files settings.
 - § Select the maximum size for Syslog Write to CSV File's storage .csv files and Syslog Direct Write's temporary recovery .csv files.
 - § Indicate if Syslog messages should be written to the database automatically once Syslog Direct Write's primary connection is restored.



Note: If you do not choose to automatically restore the Syslog messages, you need to manually import them or use WhatsUp Event Analyst and make sure to purge files.

- 5 Click **OK**.

Setting up Syslog Direct Write

Syslog Direct Write allows for very efficient insertion of syslog messages into a SQL Server database. When the database is unavailable due to a broken connection, Syslog Direct Write handler saves syslog messages in temporary recovery .csv files. Once the connection is restored, Syslog Direct Write handler moves those messages from their recovery .csv files to the database.



Important: The process of generating recovery .csv files is intended to help prevent Syslog message loss due to temporary database problems. This workflow is independent of the Syslog Write to CSV File process in which storage .csv files are created.

When using Syslog Direct Write, keep in mind the following:

- § Syslog Direct Write does not support storing, compressing or moving of data files.
- § The database can be maintained with Event Archiver's Automatic Database Maintenance.
- § Both failed and successful database connections as well as information on any message drops are logged in Windows Application Event Log and viewable in WhatsUp Event Archiver Log Entries.
- § Restored recovery .csv files are deleted after an automatic import is completed. If you choose not to automatically import the recovered messages, you should delete the files after your recovery process.
- § Automatic importing of Syslog messages from .csv files can be disabled in the Archiver Preferences. Recovery .csv files can be opened and its messages exported to the SQL Server database using WhatsUp Event Analyst.

To begin setting up Syslog Direct Write:

- 1 Launch WhatsUp Event Archiver.



Note: Syslog Direct Write uses the credentials of the Event Archiver Service Account to connect the SQL Server database.

- 2 Click **Syslog > Add a new Syslog Device**.
- 3 Enter the device name and IP address information, then click **OK**.



Note: Configure the target device to stream Syslog messages to the IP address for your system.

- 4 Click **Syslog > Syslog Direct Write Settings**.
- 5 Click **Enable archiving to SQL Server** to edit the dialog.

Syslog Direct Write Settings

Enable archiving to SQL Server

Database location and table:

SQL server connection string:
Data Source SQAELMDEMO\WULM Initial Catalog \WULM-test-db ...

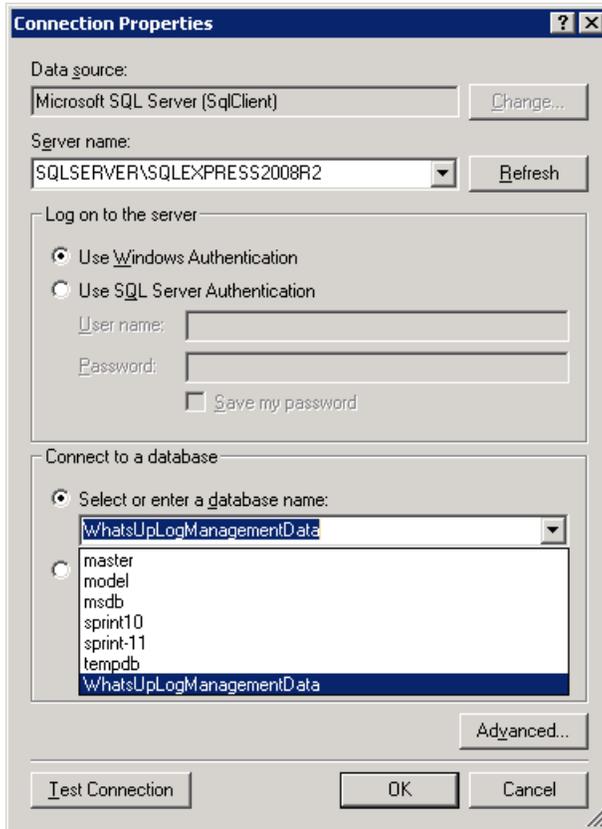
Syslog tables:
syslog1

Copy DB config Ok Cancel



Note: Syslog Direct Write Handler can also be enabled using the WhatsUp Log Management Suite Service Manager.

- 6 Select an existing SQL Server data source or add a new one making sure to specify the SQL Server name, authentication type and database name.



- 7 Select the target table where Syslog messages should be written.
- 8 Click **OK**. The database connection and permissions are validated.
- 9 Verify Syslog Direct Write is functional by checking the status of the Syslog Direct Write Archiver handler in WhatsUp Log Management Service Manager. You can also check for problems in the Event Archiver Application Log.



Note: The Archiver Service Account must have the sysadmin role or specific permissions to create, open, and insert into the specified table. For Windows Authentication, WhatsUp Event Archiver's Service Account is used to connect to the SQL Server database.

Configuring Syslog Direct Write database settings

To configure Syslog Direct Write settings using existing Syslog Archiving database settings:

- 1 Launch WhatsUp Event Archiver.

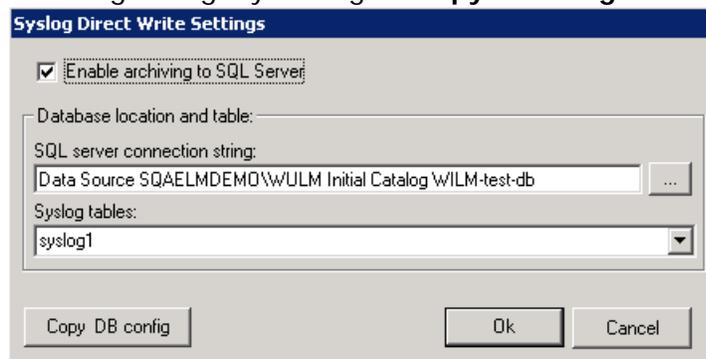
2 Select **Syslog > Syslog Direct Write Settings**.

- a) During the initial configuration of Direct Write handler, click **OK** when asked if you would like to migrate the database connection string from the Syslog Archiving settings.



This launches a populated Syslog Direct Write Settings dialog.

- b) After initial configuration, the Syslog Direct Write Settings dialog launches immediately. You can always migrate the database connection string from the Syslog Archiving settings by clicking the **Copy DB config** button



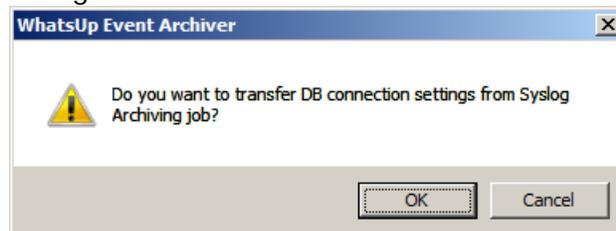
- 3 Ensure the correct database information is shown in the dialog.
4 When prompted, click **OK** to disable Syslog Archiving after the database settings have been successfully configured.

To configure a data source manually

1 Launch WhatsUp Event Archiver.

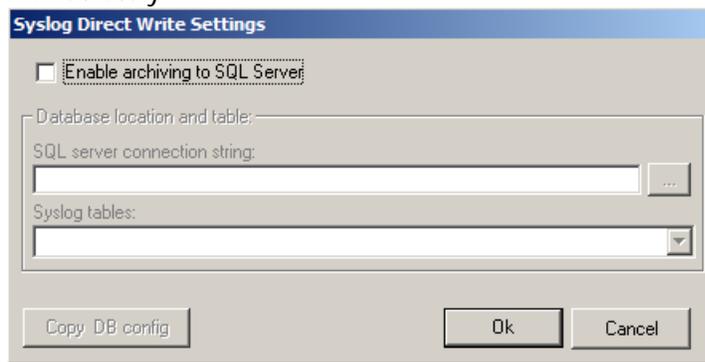
2 Select **Syslog > Syslog Direct Write Settings**.

- a) During the initial configuration of Direct Write handler, click **Cancel** when asked if you would like to migrate the database connection string from the Syslog Archiving settings.

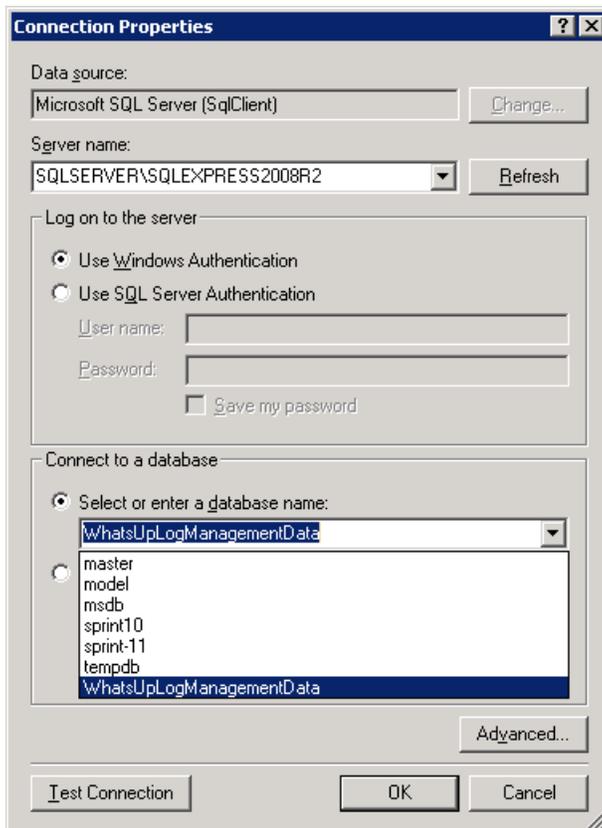


This launches an empty Syslog Direct Write Settings dialog.

- b) After initial configuration, the Syslog Direct Write Settings dialog launches immediately.



- 3 Click **Enable archiving to SQL Server** to edit the dialog.
- 4 Select an existing SQL Server data source or add a new one making sure to specify the SQL Server name, authentication type and database name.



- 5 Select the target table where Syslog messages should be written.
- 6 Click **Ok**. The database connection and permissions are validated.



Note: The Archiver Service Account must have the sysadmin role or specific permissions to create, open, and insert the specified table. For Windows Authentication, Event Archiver's Service Account is used to connect to the SQL Server database.

Setting up Syslog Write to CSV File

Syslog Write to CSV File allows you to write syslog messages to storage .csv files, which you can then work into your own long term archiving processes. Syslog Archiving's file compression and moving to a central file server or FTP server functionality are not supported on Syslog Write to CSV File .csv files. Syslog Write to CSV File writes storage .csv files only.



Caution: The Syslog Write to CSV File workflow allows you to export Syslog messages to storage .csv files very quickly. It does not currently support moving files to a final destination or automatic purging functionality. Syslog Archiving does support these procedures.

To begin setting up Syslog Direct Write:

- 1 Launch WhatsUp Event Archiver.
- 2 Click **Syslog > Add a new Syslog Device**.
- 3 Enter the device name and IP address information, then click **OK**.



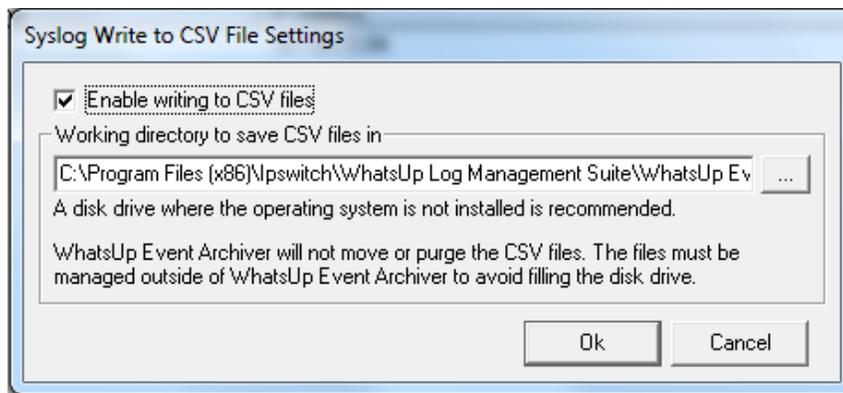
Note: Configure the target device to stream Syslog messages to the IP address for your system.

- 4 Click **Syslog > Syslog Write to CSV File Settings**.
- 5 Click **Enable writing to CSV files** to edit the dialog.



Note: Syslog Write to CSV File handler can also be enabled using the WhatsUp Log Management Suite Service Manager.

- 6 Input a file directory where Storage .csv files will be stored.



- 7 Click **OK**.
- 8 Verify Syslog Write to CSV File is functional by checking the status of the Syslog Write to CSV File handler in WhatsUp Log Management Service Manager. You can also check for problems in the Event Archiver Application Log.



Note: When choosing a file directory for writing storage .csv files, Ipswitch recommends using a disk drive separate from the drive where the operating system is installed.

Configuring Syslog Archiving Settings

You can use the Event Archiver control panel to configure or customize the archiving characteristics for Syslogs.

To configure Syslog archiving settings:

- 1 From the WhatsUp Event Archiver control panel, click **Options > Syslog Archiving Settings**. The Log Registration Options dialog opens.
- 2 Select the Computer, Log, & Schedule tab.
- 3 Configure the following:
 - a) Computer, Log, & Schedule tab
 - § **Computer Name**. Select the appropriate computer from the list.
 - § **Log**. Select the appropriate message type from the list.
 - § **Archive this log**. Set how often you want to archive the selected log.
 - § **Clear log after archiving**. Specify if you want to clear the log after it is archived.
 - b) Staging Area tab
 - § **Staging directory on <device name> to temporarily save**. Displays the location of the temporary staging directory.
 - § **Share folder used by Event Archiver to grab files saved in the staging area**. Displays the folder Event Archiver accesses to files from in the staging area. Use the browse button (...) to select a different share folder.
 - c) Data Conversion tab
 - § **Store the log data in**. Select the format in which you want to store log data.
 - § **After archiving completes, remove the EVT/EVTX file....** Follow the on screen instructions for this control.
 - § **Compress the EVT/EVTX and/or comma-delimited text files before moving them to a file or FTP server**. Enable this option to compress text files before moving them to a file or FTP server.
 - d) Final Destination tab
 - § **After archiving**. Select whether you want to leave files in the staging area or move them to a central file or FTP server after they are archived.
- 4 Click **OK** to save changes.