

IPSWITCH

**WhatsUp Event Archiver
v10 and v10.1
Quick Setup Guide**



IPSWITCH
WhatsUp Event Archiver

WhatsUp Event Archiver Quick Setup Guide

- WhatsUp Event Archiver Quick Setup Guide..... 2
- Installation Requirements..... 3
- Manually Creating Firewall Exceptions..... 4
- Before You Begin 4
- Microsoft Vista Requirements and Recommendations 15
- Network and Bandwidth Considerations.....20
- Other Recommendations23

WhatsUp Event Archiver Quick Setup Guide

In This Guide

WhatsUp Event Archiver Quick Setup Guide.....	2
Installation Requirements	3
Manually Creating Firewall Exceptions.....	4
Before You Begin	4
Microsoft Vista Requirements and Recommendations	15
Network and Bandwidth Considerations.....	19
Other Recommendations	23

WhatsUp Event Archiver Quick Setup Guide

Thank you for choosing to evaluate WhatsUp Event Archiver! Please read the following topics in this help file thoroughly before beginning your installation and configuration.

See any of the topics below to review them in depth.

Installation Requirements (on page 3)

Manually Creating Firewall Exceptions (on page 4)

Before You Begin (on page 4)

Vista Requirements and Recommendations (on page 15)

Network and Bandwidth Considerations (on page 19)

Other Recommendations (on page 23)

Legal Information Including Patent and Trademark Notices

WhatsUp Event Archiver is Copyright © 1997-2011 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 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 Windows 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. Oracle® is a registered trademark of the Oracle Corporation. All other products or technologies not specifically mentioned here are the registered trademarks of their respective companies, and are used by permission.

Ipswitch Contact Information

Ipswitch, Inc.

10 Maguire Road • Lexington, MA 02421

Phone: 781-676-5700 Fax: 781-676-5715

WWW: <http://www.whatsupgold.com>

Installation Requirements

- Microsoft Windows XP Professional SP2
- Microsoft Windows 2003 Server SP2
- Microsoft Windows Vista (Business and Ultimate)
- Microsoft Windows Server 2008 / Windows Server 2008 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/SQL Server 2008 (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.

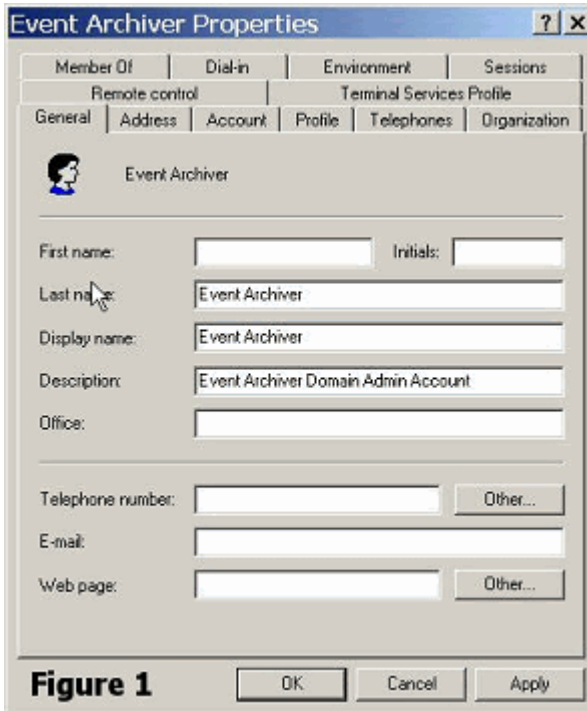
Before You Begin

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.

WhatsUp Event Archiver Quick Setup Guide



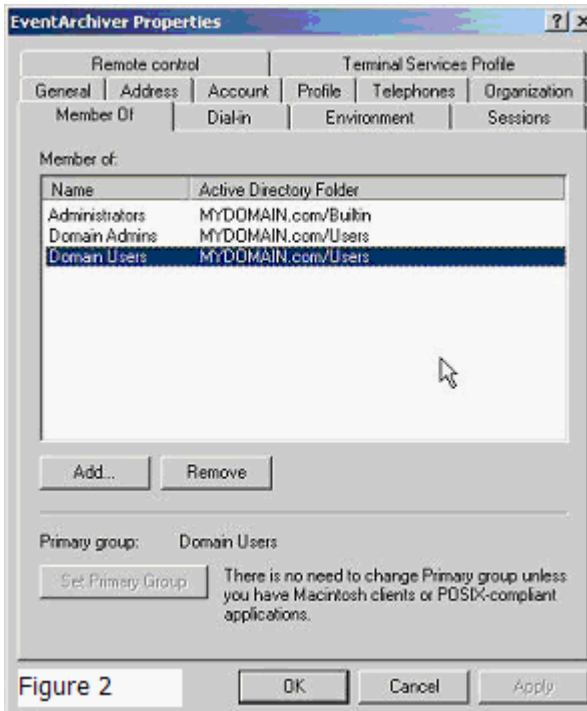
Note: If you do not have access to a full domain admin account in your domain, the software still can be configured by using an account with local Admin rights on all member servers and workstations, such as one created to administer the computers in a specific OU. Consult this KB article for more details,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



The 'Event Archiver Properties' dialog box is shown with the 'General' tab selected. It contains the following fields:

- Member Of: [Empty]
- Dial-in: [Empty]
- Environment: [Empty]
- Sessions: [Empty]
- Remote control: [Empty]
- Terminal Services Profile: [Empty]
- General: [Selected]
- Address: [Empty]
- Account: [Empty]
- Profile: [Empty]
- Telephones: [Empty]
- Organization: [Empty]
- Event Archiver (User icon)
- First name: [Empty] Initials: [Empty]
- Last name: [Event Archiver]
- Display name: [Event Archiver]
- Description: [Event Archiver Domain Admin Account]
- Office: [Empty]
- Telephone number: [Empty] Other... [Button]
- E-mail: [Empty]
- Web page: [Empty] Other... [Button]
- Buttons: OK, Cancel, Apply

Figure 1



The 'Event Archiver Properties' dialog box is shown with the 'Member of' tab selected. It contains the following elements:

- Member of:

Name	Active Directory Folder
Administrators	MYDOMAIN.com/Builtin
Domain Admins	MYDOMAIN.com/Users
Domain Users	MYDOMAIN.com/Users

- Add... [Button]
- Remove [Button]
- Primary group: Domain Users
- Set Primary Group [Button]
- There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
- Buttons: OK, Cancel, Apply

Figure 2

WhatsUp Event Archiver Quick Setup 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).

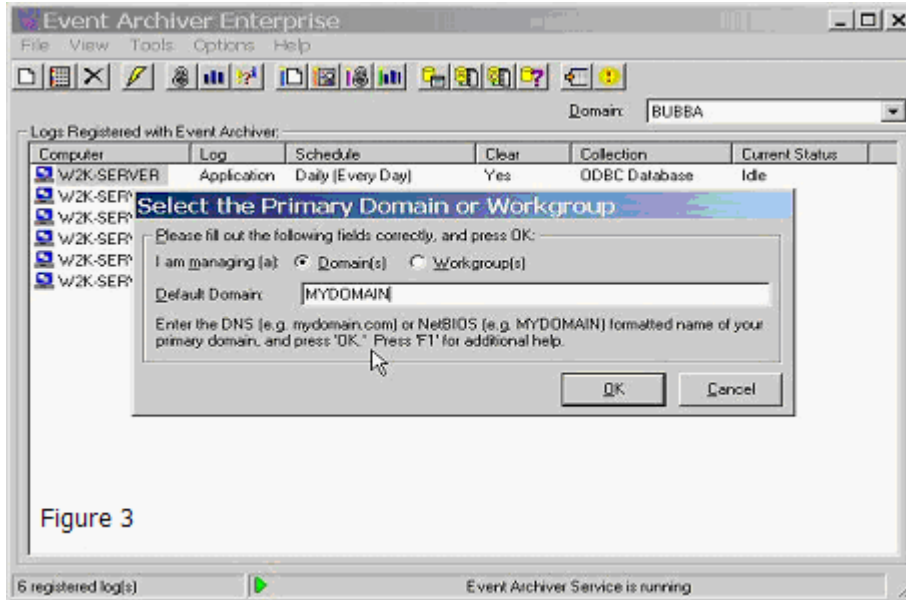
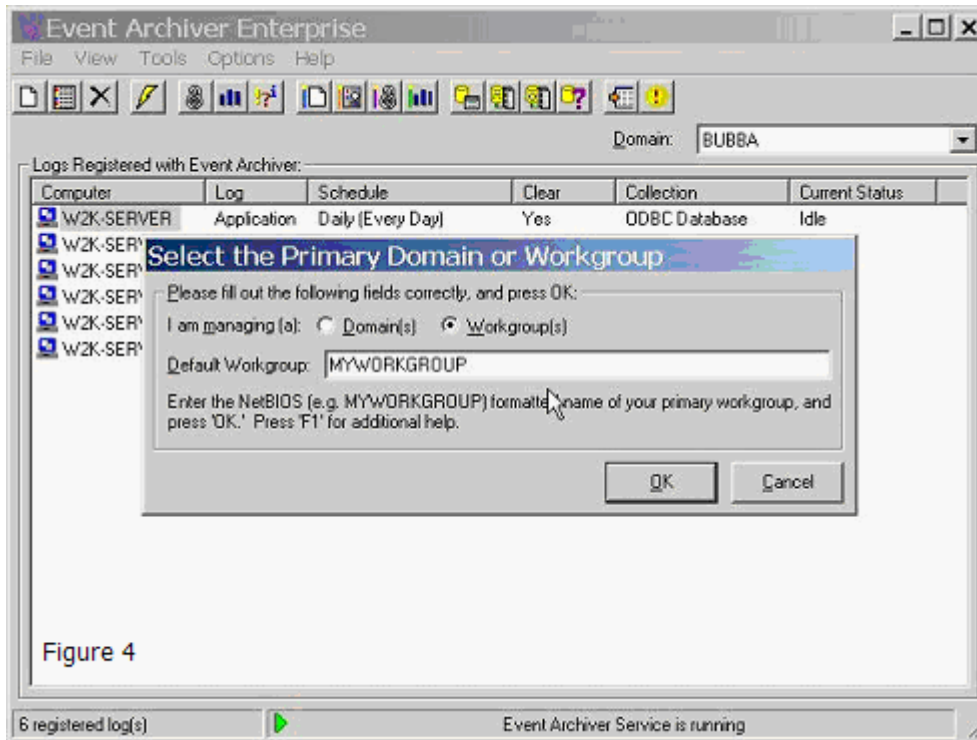


Figure 3



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.

WhatsUp Event Archiver Quick Setup Guide



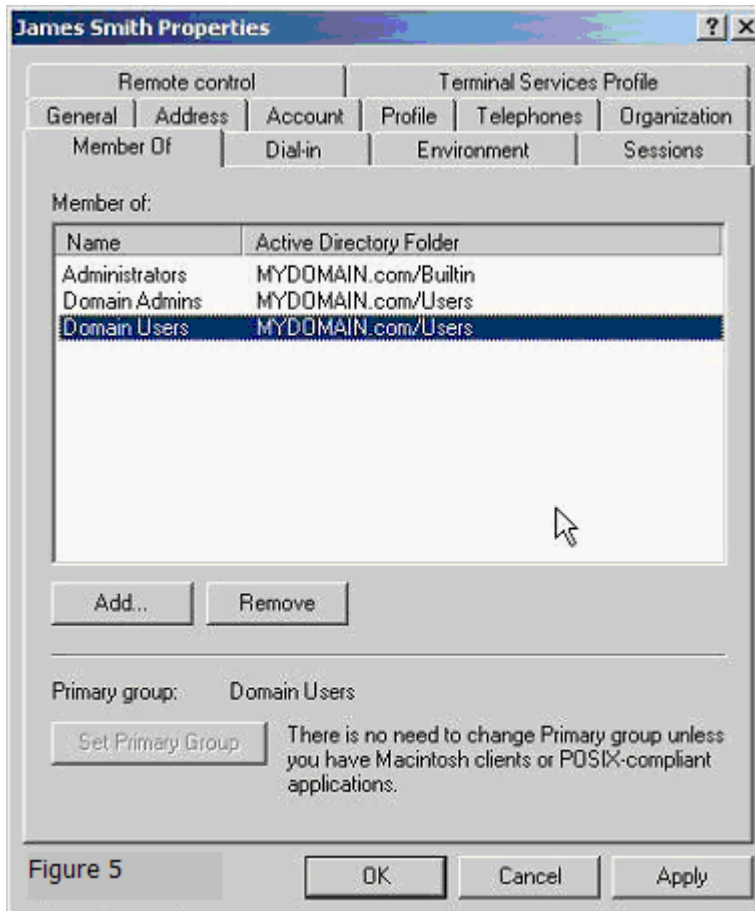
3.) If you do not already have an established user account with domain admin/OU admin rights that services can run under in your organization, create one with User Manager or Active Directory Users and Computers and place it into the Domain Admins/OU Admins group (figure 1 & 2). Also, make sure that 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).

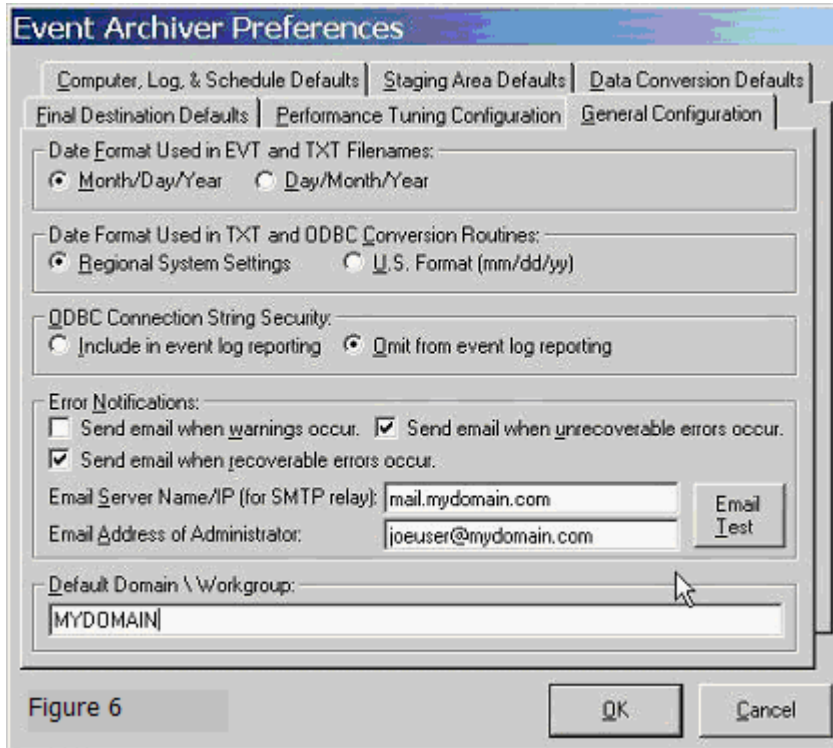
WhatsUp Event Archiver Quick Setup Guide

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.



WhatsUp Event Archiver Quick Setup Guide

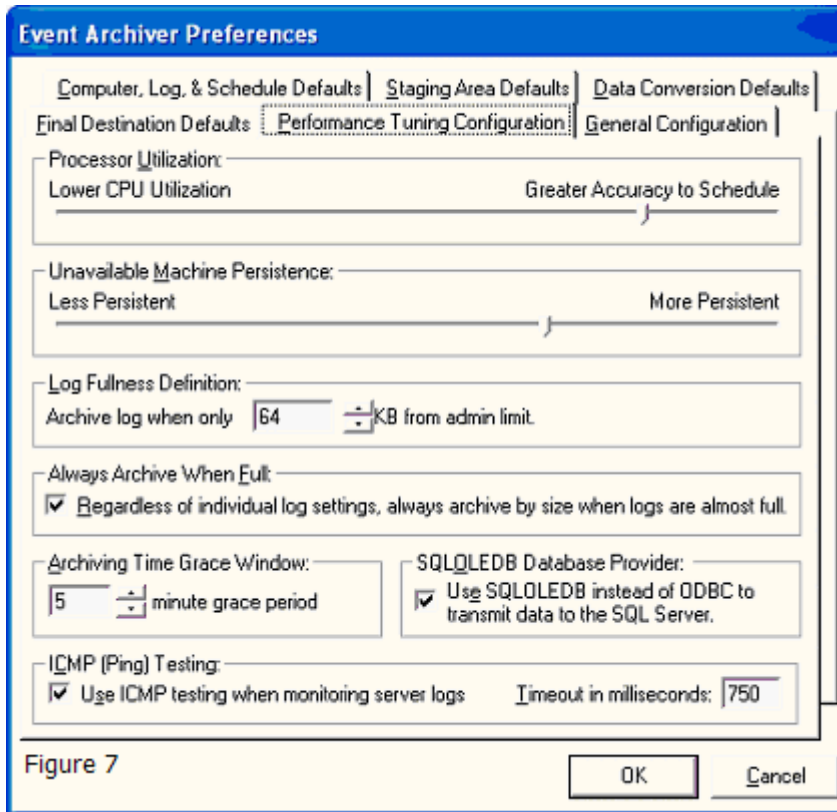
5.) If you would like to be notified about archiving errors and warnings, locate an available SMTP server on your network (we recommend the Microsoft Virtual SMTP Server that ships free with Microsoft's Internet Information Server), and adjust its security settings so that the WhatsUp Event Archiver 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 IMCP 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.



7.) 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.

WhatsUp Event Archiver Quick Setup Guide

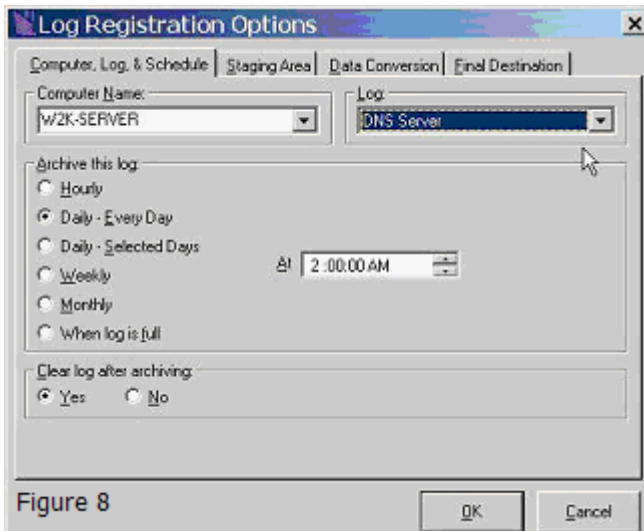


Figure 8

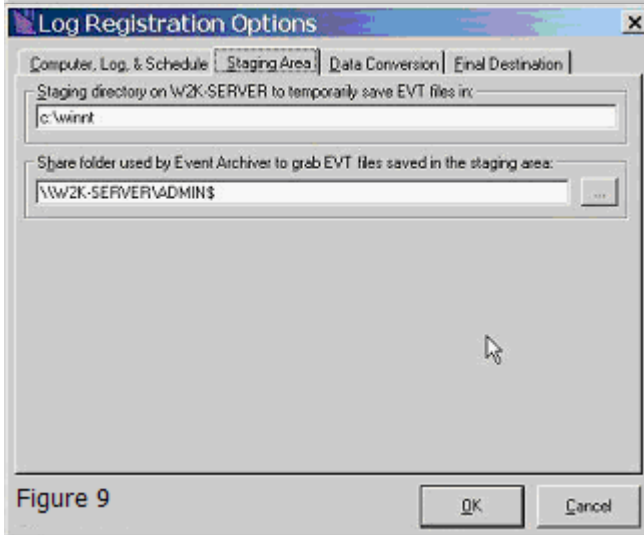
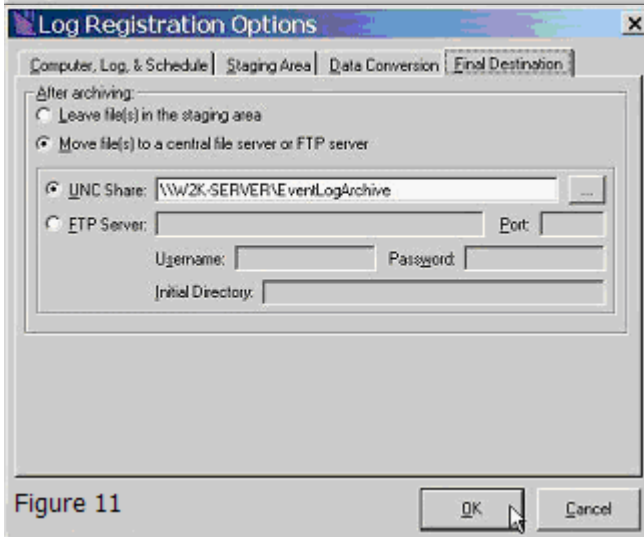
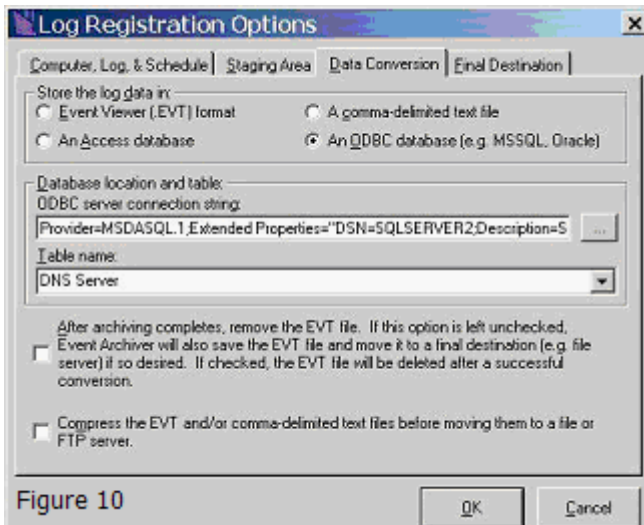


Figure 9

WhatsUp Event Archiver Quick Setup Guide



WhatsUp Event Archiver Quick Setup Guide

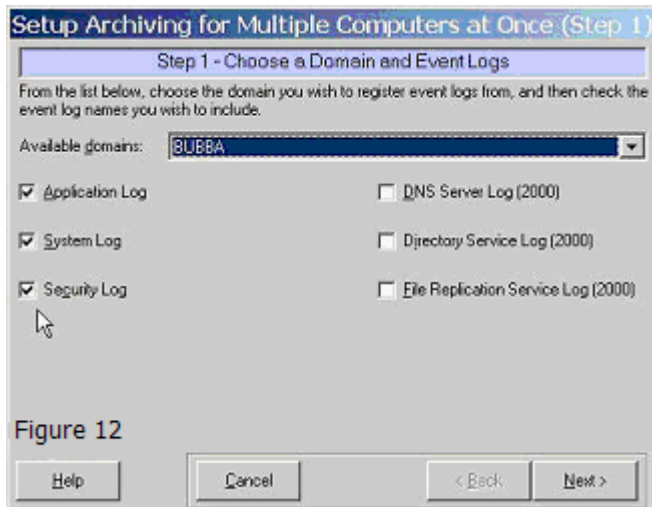


Figure 12

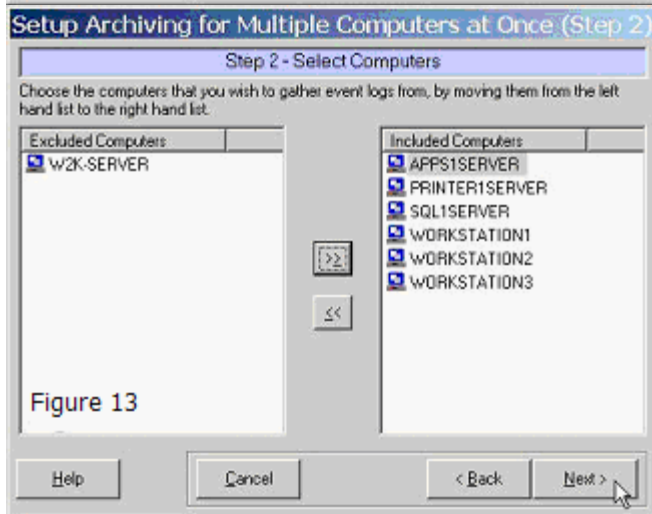


Figure 13

WhatsUp Event Archiver Quick Setup Guide

Setup Archiving for Multiple Computers at Once (Step 3)

Step 3 - Choose Archiving Frequency

Determine whether you want to archive the logs hourly, daily, weekly, monthly, or simply when a log file comes close to its size limit.

Backup and clear these logs:

Hourly, every 1 Hour starting at 1:00:00 PM

Daily, every day at 2:00:00 AM

Daily, selected days: Su M Tu W Th F Sa at 1:00:00 PM

Weekly, starting at 1:00:00 PM on Sunday

Monthly, starting at 1:00:00 PM on Day 1

When the log file is almost full (occurs automatically)

Clear the event log after it is archived: Yes No

For better load balancing, schedule each computer 10 minutes after the previous computer.

Figure 14

Help Cancel < Back Next >

Setup Archiving for Multiple Computers at Once (Step 4)

Step 4 - Choose Staging Area and Central File/FTP Server

Pick a staging directory where the logs will first be saved, a shared folder access point to that staging directory, and an optional shared folder or FTP server for centralized storage.

First, save the EVT file in this staging directory: c:\winnt

Which is accessed via this shared folder: ADMIN\$

After archiving, move log file(s) from the staging area to a central file or FTP server:

Yes No

UNC Share: \\W2K-SERVER\EventLogArchive

FTP Server: _____ Port: _____

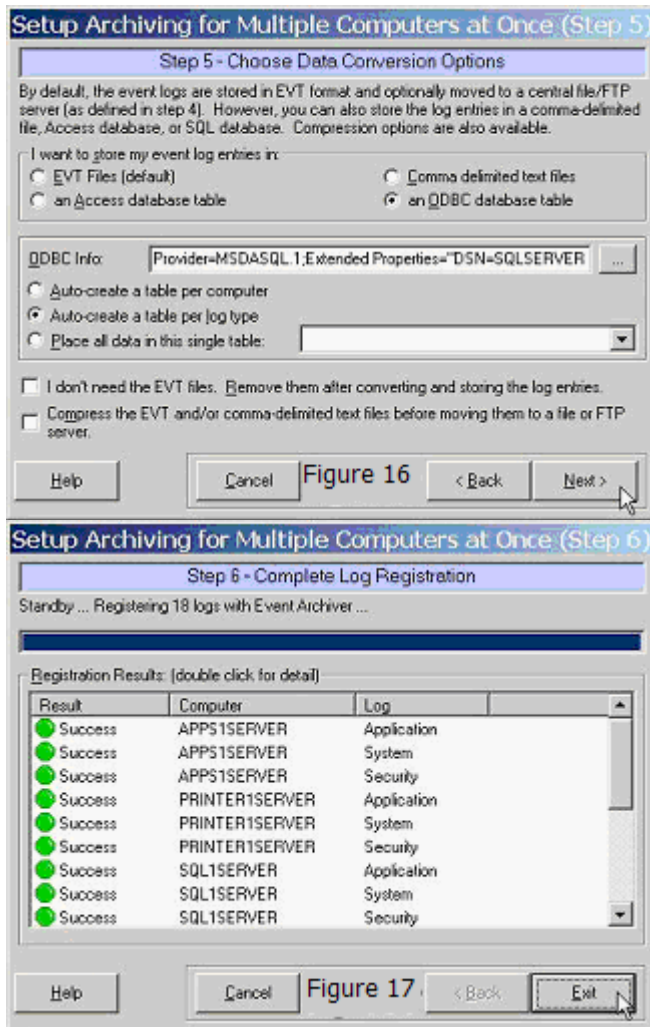
Username: _____ Password: _____

Initial Directory: _____

Figure 15

NOTE: This wizard will automatically create all necessary shared folders (e.g. the staging area shared folder and/or the central UNC share), and will also set the appropriate permissions.

Help Cancel < Back Next >



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

WhatsUp Event Archiver Quick Setup Guide

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 **secedit** 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

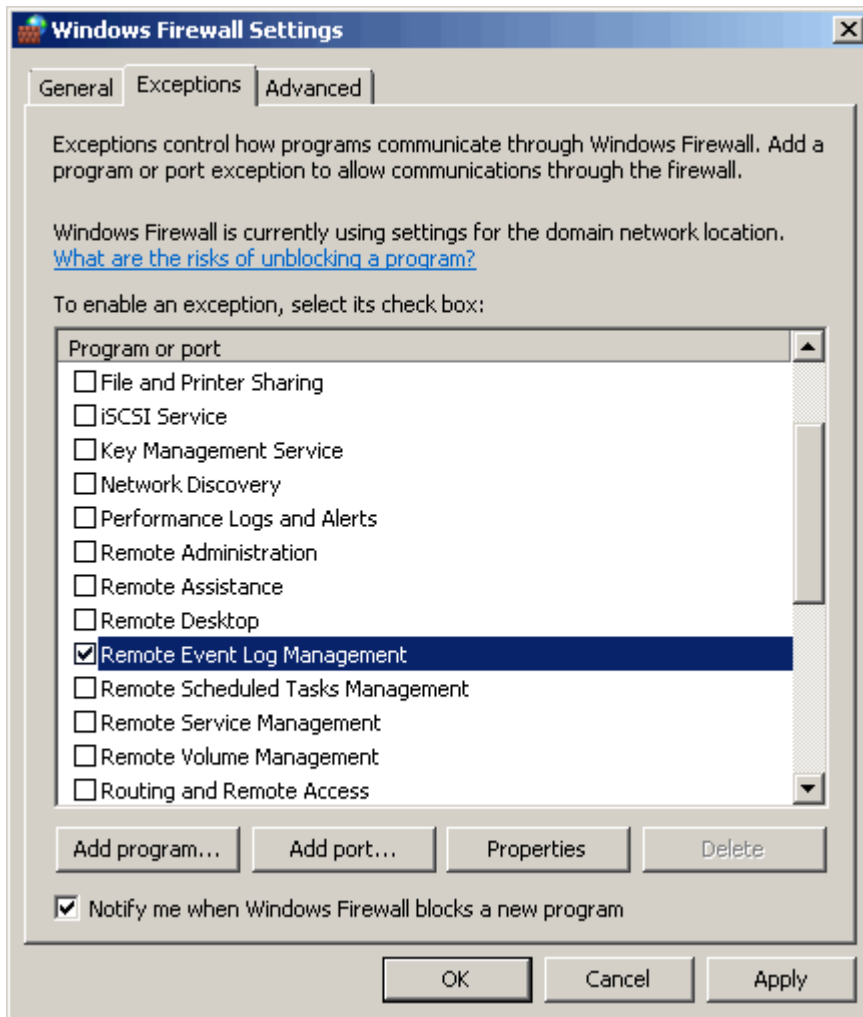
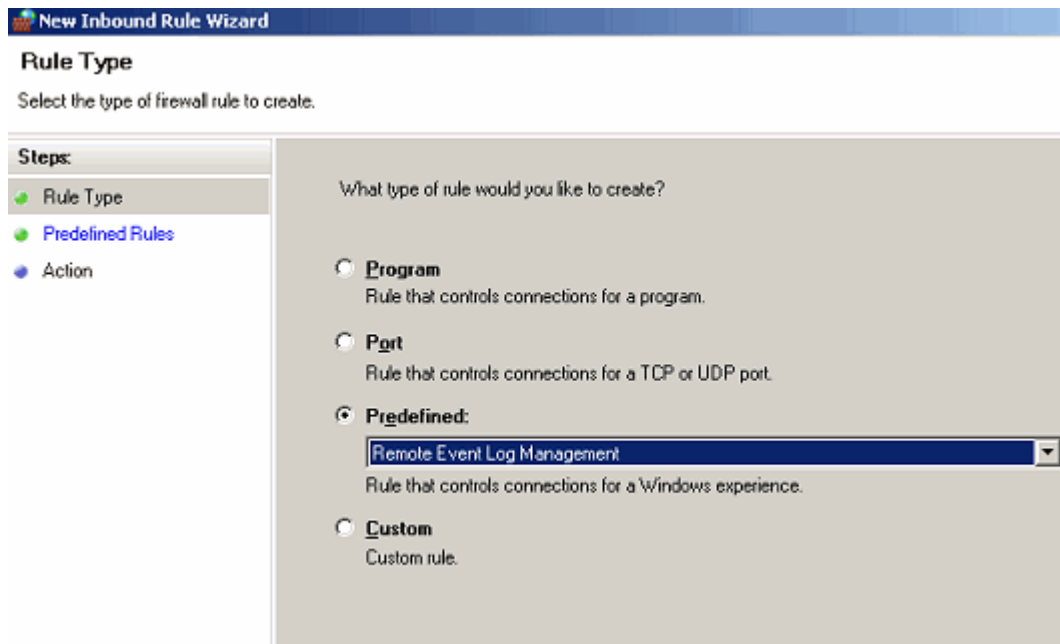
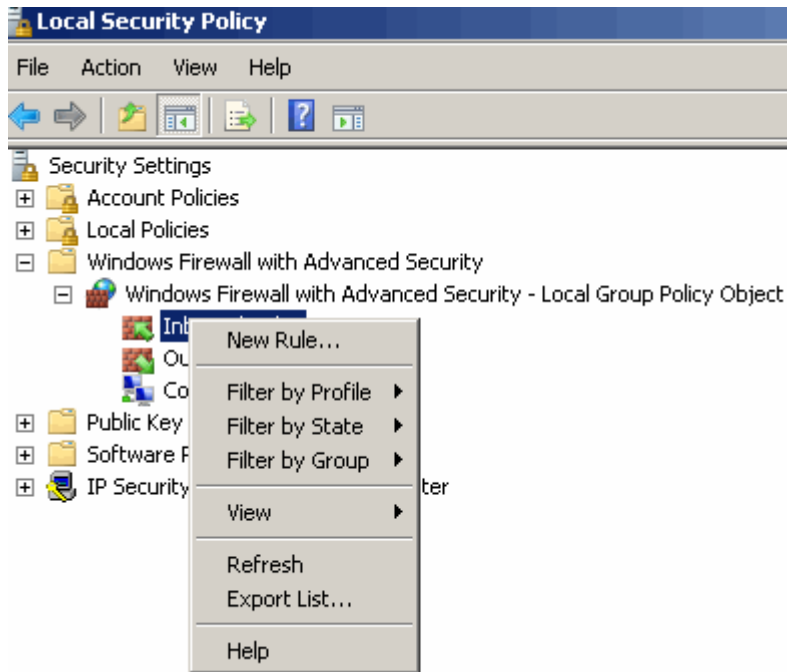


Figure 2a,2b,2c,2d - Setting the exception via a Policy object (local Policy or Group Policy)



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

WhatsUp Event Archiver Quick Setup Guide



WhatsUp Event Archiver Quick Setup Guide

New Inbound Rule Wizard

Predefined Rules

Select the rules to be created for this experience.

Steps:

- Rule Type
- Predefined Rules
- Action

Which rules would you like to create?

The following rules define network connectivity requirements for the selected Rules that are checked will be created. If a rule already exists and is checked, the existing rule will be overwritten.

Rules:

Name	Rule Exists
<input checked="" type="checkbox"/> Remote Event Log Management (RPC-EPMAP)	No
<input checked="" type="checkbox"/> Remote Event Log Management (NP-In)	No
<input checked="" type="checkbox"/> Remote Event Log Management (RPC)	No
<input checked="" type="checkbox"/> Remote Event Log Management (RPC-EPMAP)	No
<input checked="" type="checkbox"/> Remote Event Log Management (NP-In)	No
<input checked="" type="checkbox"/> Remote Event Log Management (RPC)	No

New Inbound Rule Wizard

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Predefined Rules
- Action

What action should be taken when a connection matches the specified conditions?

- Allow the connection**
Allow connections that have been protected with IPsec as well as those that have not.
- Allow the connection if it is secure**
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
 - Require the connections to be encrypted**
Require privacy in addition to integrity and authentication.
 - Override block rules**
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.
- Block the connection**

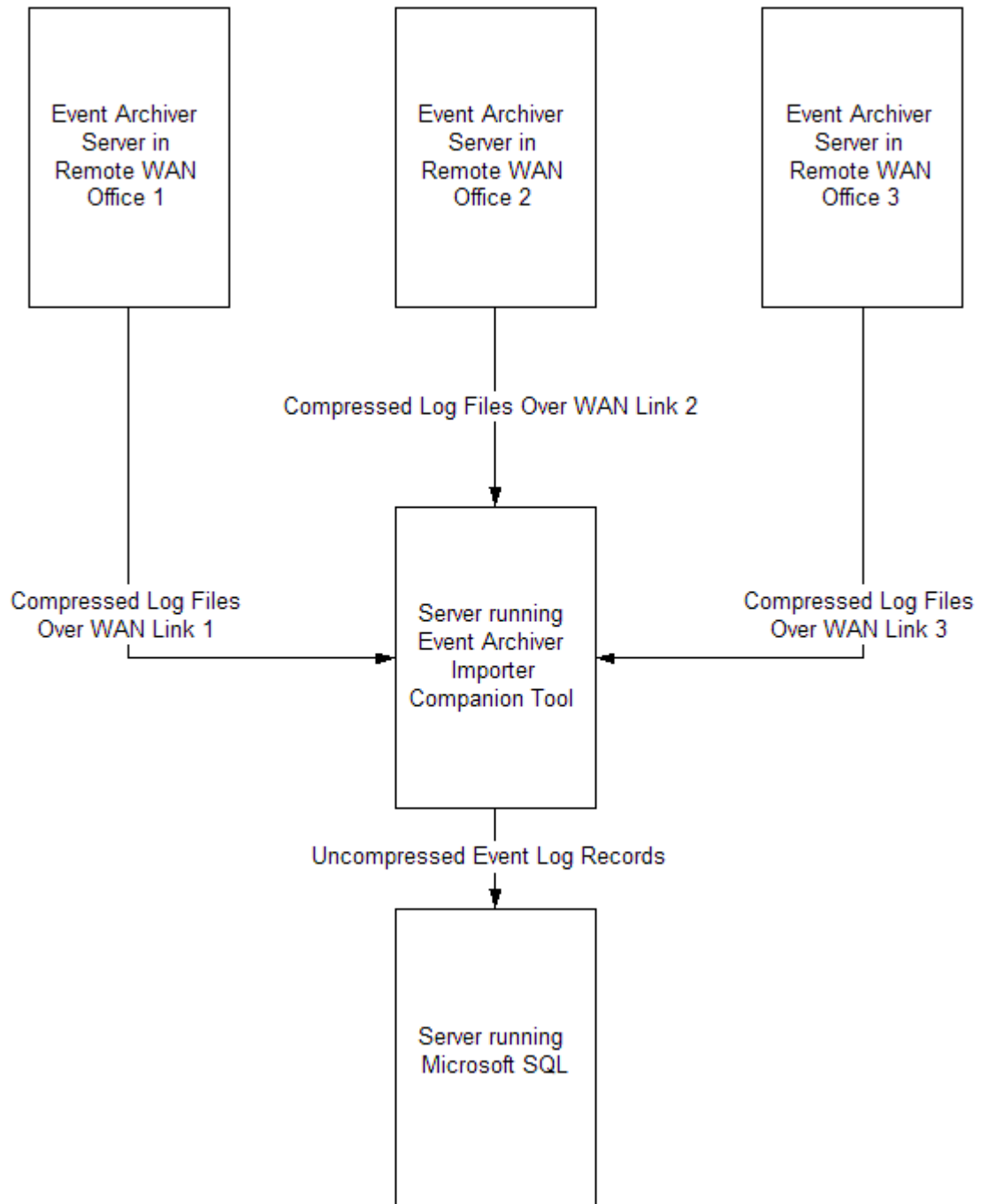
Network and Bandwidth Considerations

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.

WhatsUp Event Archiver Quick Setup Guide

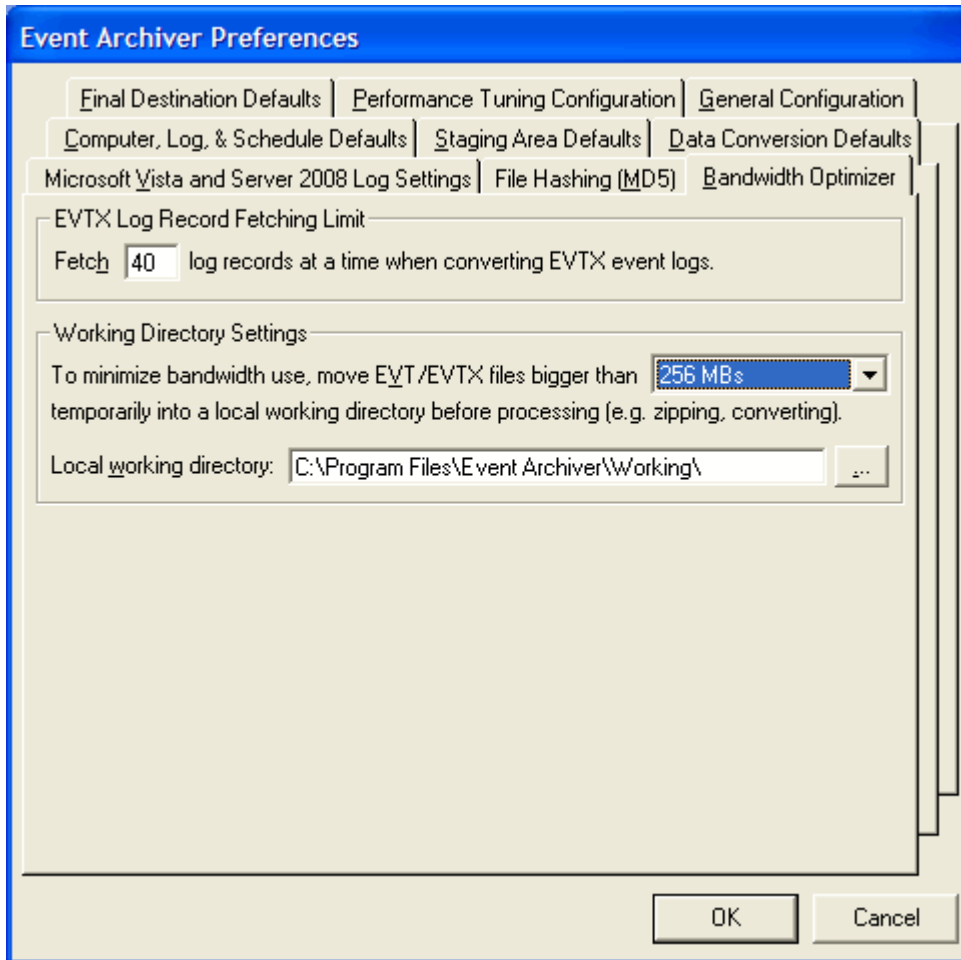
In many networks, the available bandwidth is such that you can transmit event log records directly to a central database or database server immediately after archiving with WhatsUp Event Archiver. However, if you have a very limited amount of bandwidth from your central office to remote sites containing 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:

WhatsUp Event Archiver Quick Setup Guide



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.



We know that every network is different, so if you have additional questions about how to best configure WhatsUp Event Archiver in production, please contact our support team. We'll be happy to assist.

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.

WhatsUp Event Archiver Quick Setup Guide

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.