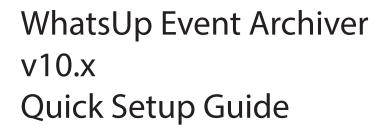


ІРЅWITCH



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 Recommendations	23

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 2003[®], Microsoft Windows Vista[®], Microsoft Windows Server 2008[®], Microsoft Windows 7, Microsoft Windows Vista[®], Microsoft Windows Server 2008[®], Microsoft Windows ^P, Microsoft

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.

mm

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.

vent Archive	er Properties	?
Member Of Remote co	Dial-in Environment	Sessions s Profile
-	s Account Profile Telephones Archiver	0 rganization
First name:	Initials:	
Last na 🐙	Event Archiver	
Display name:	Event Archiver	
Description	Event Archiver Domain Admin Accou	nt
Office:	[
Telephone number		Other
E-mail:		
Web page:		Other
Figure 1	OK Cancel	Apply

Description	trol I Terminal Services	0.0.
Remote con		
General Address		Organization
Member Of	Dial-in Environment	Sessions
Member of:		
Name	Active Directory Folder	
Administrators	MYDOMAIN.com/Builtin	
Domain Admins	MYDOMAIN.com/Users	
Domain Users	MYDOMAIN.com/Users	
	Ls.	
	R	
	L3	
Add	Remove	
	Remove	
Primary group:	Remove Domain Users	y group unless
	Remove Domain Users P There is no need to change Primar you have Macintosh clients of POS	
Primary group:	Remove Domain Users	
Primary group:	Remove Domain Users P There is no need to change Primar you have Macintosh clients of POS	

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).

tion Current Status
Database Idle
matted name of your
moved name or your
Cancel

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.

the statement of the st	chiver Enter	and provide the second s	.11 - i	6 a 6	_ 🗆 🗙
			<u>~10 01 ?</u>	Domain: BUBB	A 💌
	with Event Archiver:		F	1	
Computer	Log	Schedule	Clear	Collection	Current Status
W2K-SERVE		Daily (Every Day)	Yes	ODBC Database	Idle
W2K-SER'	Select the Pr	imary Doma	ain or Workç	jroup :	and the second se
W2K-SER ⁴		lowing fields correct			
W2K-SER ¹	I am managing (a):	C Domain(s)	Workgroup[s]		
STATES W2K-SER					
		MYWORKGROU			
	Enter the NetBIOS press 'OK.' Press 'F	(e.g. MYWORKGR(1' for additional help	DUP) formatte();name o.	e of your primary work	kgroup, and
				<u>Q</u> K	Gancel
-					
Figure 4					
6 registered log(s)	Þ		Event Archiv	er Service is running	

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.

Remote cont	rol	Te	erminal Services	s Profile
General Address	Account	Profile	Telephones	Organization
Member Of	Dial-in	Envi	ronment	Sessions
Member of:				
Name	Active Directo	ory Folder		
Administrators	MYDOMAIN.			
Domain Admins Domain Users	MYDOMAIN.			
			N	
			ß	
			ß	
Add	Remove		Å	
Add	Remove		ß	
Add	Remove		ß	
	Remove Domain Users		ß	
	Domain Users		ß	
	Domain Users		change Prima	
Primary group:	Domain Users	Macintos	change Prima h clients or POS	
Primary group:	Domain Users	Macintos		

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).

	faults Staging Area Defaults Data Conversion Default
inal Destination Defaults Perfo	ormance Tuning Configuration General Configuration
Date <u>F</u> ormat Used in EVT and T	XT Filenames:
Month/Day/Year C Day	/Month/Year
Date Format Used in TXT and 0	IDBC Conversion Routines:
Begional System Settings	⊂ U.S. Format (mm/dd/yy)
ODBC Connection String Securi	hr
	g 🕝 Omit from event log reporting
Error Notifications:	
	occur. 🔽 Send email when <u>unrecoverable errors occur</u> .
Send email when recoverable	le errors occur.
Email <u>S</u> erver Name/IP (for SMT)	P relay): mail.mydomain.com Email
Email Address of Administrator:	joeuser@mydomain.com
Default Domain \Workgroup:	le .
MYDOMAIN	

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.

Event Archiver Preferences
Computer, Log, & Schedule Defaults Staging Area Defaults Data Conversion Defaults
Processor Utilization: Lower CPU Utilization Greater Accuracy to Schedule
Unavailable Machine Persistence:
Less Persistent More Persistent
Log Fullness Definition: Archive log when only 64 Always Archive When Eult
Regardless of individual log settings, always archive by size when logs are almost full.
Archiving Time Grace Window: SQLQLEDB Database Provider: Use SQLOLEDB instead of ODBC to transmit data to the SQL Server.
ICMP (Ping) Testing: Vge ICMP testing when monitoring server logs Iimeout in milliseconds: 750
Figure 7 OK Cancel

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.

	ging Area Data Conversion Einal Destination
Computer Name:	
W2K-SERVER	DNS Server
Archive this log	
C Hourly	
Daily - Every Day	
C Daily - Selected Days	N 10 10 10 11
⊂ <u>W</u> eekly	At 2:00:00 AM
C Monthly	
C When log is <u>full</u>	
Clear log after archiving	
€Yes C No	
Log Registration Or	otions
omputer, Log, & Schedule	Dtions prog Area Data Conversion Einal Destination R to temporarily save EVT files in:
	ging Area Data Conversion Einal Destination
Computer, Log, & Schedule Star Staging directory on W2K-SERVE C Winnt	ging Area Data Conversion Einal Destination
Computer, Log, & Schedule Star Staging directory on W2K-SERVE C Winnt	ging Area] Data Conversion Einal Destination R to temporarily save EVT files in:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE Ic Winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE (c. winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE Ic Winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE (c. winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE (c. winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE (c. winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE (c. winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:
Computer, Log, & Schedule Star Staging directory on W2K-SERVE Ic Winnt Share folder used by Event Archir	ging Area. Data Conversion Einal Destination R to temporarily save EVT files in: ver to grab EVT files saved in the staging area:

Computer, Log, 8							
	Schedule	Staging Are	a <u>D</u> ata	Conversion	Einal Dest	ination	
Store the log da			-				
C Event Viewe		hat		ıma-delimit			
C An Access o	latabase		⊙ An <u>O</u> l	08C datab	ase (e.g. MS	SQL. Oracle)
Database locati ODBC server co							
Provider=MSDA			ties="DSN	=SQLSER	VER2;Descri	ption=S	
Iable name:							
DNS Server							•
Compress the FTP server.	e EVT and/o	or comma-de	limited text	files befor	e moving ther	n to a file or	
						1	_
gure 10 Log Regi				[<u>O</u> K		:el
igure 10 Log Regis Computer, Log. 8 After archiving: C Leave file(s)	Schedule	<u>S</u> taging Are g area	sa Data		=		;el
igure 10 Log Regis Computer, Log, 8 After archiving: C Leave file(s) C Move file(s)	Schedule	<u>Staging</u> Are g area le server or l	sa Data FTP serve	r ⁱ	=		lec T
igure 10 Log Regis Computer, Log. 8 After archiving: C Leave file(s)	Schedule	<u>Staging</u> Are g area le server or l	sa Data FTP serve	r ⁱ	=		24
igure 10 Log Regis Computer, Log, 8 After archiving: C Leave file(s) C Move file(s)	Schedule	<u>Staging</u> Are g area le server or l	sa Data FTP serve	r ⁱ	=	insten	
igure 10 Log Regis Computer, Log, 8 After archiving: C Leave file(s) C Move file(s) C UNC Share	Schedule	Staging Are g area le server or l ERVER\Eve	sa Data FTP serve	r ⁱ	Enel Dent	insten	

Image: Server Log (2000) Image: S	Setup Archiving	for Multiple	Comput	ers at On	ce (Step 1)
event log names you wish to include. Available domains: BUEBA IF Application Log DIVES Server Log (2000) IF System Log Divectory Service Log (2000) IF Seguity Log Elle Replication Service Log (2000) IF Sectup Archiving for Multiple Computers at Once (Step 2 Step 2 - Select Computers Choose the computers that you wish to gather event logs from, by moving them from the left hand list. Included Computers	Step	1 - Choose a Do	imain and B	EventLogs	
Image: Second Log Image: Dispectation Log (2000) Image: Second Log Image: Dispectation Service Log (2000) Image: D			n to register ev	vent logs from, ar	id then check the
Image: System Log □ Directory Service Log (2000) Image: Segurity Log □ Ele Replication Service Log (2000) Image: Segurity Log □ Ele Replication Service Log (2000) Image: Segurity Log □ Ele Replication Service Log (2000) Image: Segurity Log □ Ele Replication Service Log (2000) Image: Segurity Log □ Ele Replication Service Log (2000) Image: Segurity Log □ Ele Replication Service Log (2000) Image: Segurity Log □ Ele Replication Service Log (2000) Setup Archiving for Multiple Computers at Once (Step 2 Step 2 - Select Computers Choose the computers that you wish to gather event logs from, by moving them from the left hand left. Excluded Computers □ Included Computers Image: W2K-SERVER □ APPSISERVER Image: W2K-SERVER □ W0RKSTATION1 Image: W2K-SERVER □ W0RKSTATION2 Image: W2K-SERVER □ W0RKSTATION3 Image: Second to the optime of the second to the second to the optime of the second to the seco	Available gomains:	BBA			
✓ Seguity Log ☐ Ele Replication Service Log (2000) Figure 12 Help Cancel < Beck	P Application Log			IS Server Log (2	000)
Figure 12 Help Cancel < Beck	🔽 System Log		🗂 Djr	ectary Service L	og (2000)
Figure 12 Help Cencel < Book			Ele	Replication Ser	vice Log (2000)
Help Cancel Eack Next> Setup Archiving for Multiple Computers at Once (Step 2 Step 2 - Select Computers Choose the computers that you wish to gather event logs from, by moving them from the left hand list to the right hand list. Excluded Computers Included Computers W2K-SERVER APPS1SERVER W2K-SERVER WORKSTATION1 W0RKSTATION2 WORKSTATION2 W0RKSTATION3 Step 13	13				
Help Cancel Eack Next> Setup Archiving for Multiple Computers at Once (Step 2 Step 2 - Select Computers Choose the computers that you wish to gather event logs from, by moving them from the left hand list to the right hand list. Excluded Computers Included Computers W2K-SERVER APPS1SERVER W2K-SERVER WORKSTATION1 W0RKSTATION2 WORKSTATION2 W0RKSTATION3 Step 13					
Setup Archiving for Multiple Computers at Once (Step 2 Step 2 - Select Computers Choose the computers that you wish to gather event logs from, by moving them from the left hand list. Excluded Computers Included Computers W2K-SERVER APPS1SERVER W0RKSTATION1 W0RKSTATION2 W0RKSTATION3 Included Tomp (Station of the second of the se	Figure 12				
Step 2 - Select Computers Choose the computers that you wish to gather event logs from, by moving them from the left hand list. Excluded Computers Included Computers W2K-SERVER APPS1SERVER SQL1SERVER SQL1SERVER W0RKSTATION1 W0RKSTATION2 W0RKSTATION3 W0RKSTATION3	Help	Gancel		< <u>B</u> ack	<u>N</u> ext >
Choose the computers that you wish to gather event logs from, by moving them from the left hand list to the right hand list. Excluded Computers W2K-SERVER SQL1SERVER SQL1SERVER W0RKSTATION1 W0RKSTATION2 W0RKSTATION3 Figure 13	Setup Archiving	for Multiple	Comput	ers at On	re (Step 2)
Excluded Computers Included Computers W2K-SERVER APPS1SERVER SQL1SERVER SQL1SERVER W0RKSTATION1 W0RKSTATION2 W0RKSTATION3 W0RKSTATION3		Step 2 - Sele	ct Compute	rs	
W W2K-SERVER APPSISERVER PRINTERISERVER SQLISERVER SQLISERVER WORKSTATIONI WORKSTATION2 WORKSTATION3			went logs from	, by moving then	n from the left
Figure 13	Excluded Computers		Inclu	ded Computers	
SQLISERVER WORKSTATION1 WORKSTATION2 WORKSTATION3	Server W2K-SERVER				
Figure 13					R
Figure 13					
Figure 13		6	2 🚨 W	ORKSTATION2	
Figure 13			. 🔍 W	ORKSTATION3	
		2	8		
Help Cappel / Reck Marks	Figure 13				
Toh Zarrei Zarrei Zarrei	Help	Cancel		< <u>B</u> ack	Next> N

5	Step 3 - Choose Archiving Frequency
Determine whether you w log file comes close to its	vant to archive the logs hourly, daily, weekly, monthly, or simply whe size limit.
Backup and clear these	e log=
Hourly, every	1 Hour starting at 1:00:00 PM
Daily, every day at	2:00:00 AM
C Daily, gelected days	: ☐ Su ☐ M ☐ Tu 21 [1:00:00 PM □ W ☐ Th ☐ F ☐ So
○ Weekly, starting at	1:00:00 PM gn Sunday
C Monthly, starting at	1.00.00 PM gn Day 1
C When the log file is a	almost full (occurs automatically)
etup Archiving	g for Multiple Computers at Once (Step
	oose Staging Area and Central File/FTP Server where the loos will first be saved, a shared folder access point to that
lick a staging directory w	Dose Staging Area and Central File/FTP Server where the logs will first be saved, a shared folder access point to that optional shared folder or FTP server for centralized storage.
Pick a staging directory w taging directory, and an	where the logs will first be saved, a shared folder access point to tha optional shared folder or FTP server for centralized storage.
Pick a staging directory w	where the logs will first be saved, a shared folder access point to the optional shared folder or FTP server for centralized storage. this staging directory: [c:\winnt]
lick a staging directory w taging directory, and an first, save the EVT file in <u>w</u> hich is accessed via th	where the logs will first be saved, a shared folder access point to the optional shared folder or FTP server for centralized storage. this staging directory: [c:\winnt]
Pick a staging directory with taging directory, and an girst, save the EVT file in <u>which is accessed via the After archiving, move log</u> <u>Yes</u> <u>No</u>	where the logs will first be saved, a shared folder access point to the optional shared folder or FTP server for centralized storage. this staging directory: c:/winnt is shared folder: ADMIN\$
Pick a staging directory with taging directory, and an girst, save the EVT file in <u>which is accessed via the After archiving, move log</u> <u>Yes</u> <u>No</u>	where the logs will first be saved, a shared folder access point to the optional shared folder or FTP server for centralized storage. I this staging directory: [c.twinnt is shared folder: [ADMIN\$] Ing file(s) from the staging area to a central file or FTP server.
Pick a staging directory with staging directory, and an Erst, save the EVT file in Which is accessed via the After archiving, move log C Yes C No C UNC Share: WW2 C ETP Serve:	where the logs will first be saved, a shared folder access point to the optional shared folder or FTP server for centralized storage. this staging directory: a winnit is shared folder: ADMIN\$ g file(s) from the staging area to a central file or FTP server. X-SERVER\EventLogArchive
Pick a staging directory witaging directory, and an e- gret, save the EVT file in which is accessed via the After archiving, move to Sector C No Sector No. ETP Servet: Ugem Initial	where the logs will first be saved, a shared folder access point to the optional shared folder or FTP server for centralized storage. It is staging directory: is shared folder: ADMIN\$ g file(s) from the staging area to a central file or FTP server. 2K-SERVER\EventLogArchive
Pick a staging directory witaging directory, and an extra staging directory directory and an extra staging directory direc	where the logs will first be saved, a shared folder access point to the optional shared folder or FTP server for centralized storage. It is staging directory: is shared folder: ADMIN\$ g file(s) from the staging area to a central file or FTP server. 2K-SERVER\EventLogArchive

	Step 5 - Choose Data	Conversion Op	tions	
rver (as defined in	nt logs are stored in EVT form n step 4]. However, you can se, or SQL database. Compre	also store the log e	ntries in a comma	file/FT -delimi
want to store my	event log entries in			
EVT Files (def	auk)	C Comma d	delimited text files	
C an Access da	tabase table	(€ an <u>O</u> DB(C database table	
DBC Info:	Provider=MSDASQL.1;Exter	nded Properties="D	SN-SQLSERVER	τ.
Auto-create a	table per computer			
	table per log type			
	in this single table:			1
<u>_</u>	· · · · · · · · · · · · · · · · · · ·			- 1
I don't need the	EVT files. Bemove them aft	er converting and s	toring the log ent	ries.
- Compress the E	VT and/or comma-delimited	ext files before mov	ring them to a file	or FTF
server.				
<u></u>	1=-			
Help	Cancel FIG	ure 16 👘 🐰	Back N	ext > ,
				-
etup Archi	ving for Multiple	Computers	at Once (S	step
	ving for Multiple Step 6 - Complete ing 18 logs with Event Archiv	Log Registratio		itep
andbyRegiste	Step 6 - Complete	Log Registratio		itep
andbyRegiste	Step 6 - Complete ing 18 logs with Event Archiv	Log Registratio		itep
andby Registe <u>R</u> egistration Res.	Step 6 - Complete ing 18 logs with Event Archiv its (double click for detail)	Log Registratio er		itep
andby Registe Begistration Res. Result	Step 6 - Complete ing 18 logs with Event Archiv its: (double click for detail) Computer	Log Registratio er		itep
andby Registe Begistration Resu Result Success	Step 6 - Complete ing 18 logs with Event Archiv its (double click for detail) Computer APPS1SERVER	Log Registratio er Log Application		itep
andby Registe Begistration Resu Result Success Success	Step 6 - Complete ing 18 logs with Event Archiv its: (double click for detail) Computer APPS 1SERVER APPS 1SERVER	Log Registratio er Log Application System		itep
andby Register Begistration Resu Result Success Success Success	Step 6 - Complete ing 18 logs with Event Archiv its: (double click for detail) Computer APPS1SERVER APPS1SERVER APPS1SERVER	Log Registratio er Log Application System Security		itep
andby Register Begistration Resu Result Success Success Success Success	Step 6 - Complete ing 18 logs with Event Archiv Ars: (double click for detail) Computer APPS1SERVER APPS1SERVER APPS1SERVER PRINTER1SERVER	Log Registratio er Log Application System Security Application		itep
andby Register <u>Registration Result</u> Success Success Success Success Success Success Success	Step 6 - Complete ing 18 logs with Event Archiv Ars: (double click for detail) Computer APPS1SERVER APPS1SERVER APPS1SERVER PRINTER1SERVER PRINTER1SERVER	Log Registratio er Application System Security Application System		itep
andby Registe Result Success Success Success Success Success Success Success Success Success Success	Step 6 - Complete ing 18 logs with Event Archiv Its: (double click for detail) Computer APPS1SERVER APPS1SERVER PRINTER1SERVER PRINTER1SERVER PRINTER1SERVER PRINTER1SERVER	Log Registratio er Application System Security Application System Security		itep
andby Registe Registration Resu Success Success Success Success Success Success Success Success Success Success Success	Step 6 - Complete ing 18 logs with Event Archiv Its: (double click for detail) Computer APPS1SERVER APPS1SERVER PRINTER1SERVER PRINTER1SERVER PRINTER1SERVER SQL1SERVER	Log Registratio er Application System Security Application System Security Application		itep
andby Register Result Success Success Success Success Success Success Success Success Success Success Success Success Success	Step 6 - Complete ing 18 logs with Event Archiv Arc (double click for detail) Computer APPS1SERVER APPS1SERVER PRINTER1SERVER PRINTER1SERVER PRINTER1SERVER SQL1SERVER	Log Registratio er Application System Security Application System Security Application System		itep

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 is 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 exeception 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.

mm.

L

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

🍿 Windows Firewall Settings 🛛 🛛 🔀			
General Exceptions Advanced			
Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.			
Windows Firewall is currently using settings for the domain network location. What are the risks of unblocking a program?			
To enable an exception, select its check box:			
Program or port			
File and Printer Sharing			
Key Management Service			
Network Discovery Devformence Logg and Alerte			
Performance Logs and Alerts Remote Administration			
Remote Event Log Management			
Remote Scheduled Tasks Management			
Remote Service Management			
Remote Volume Management			
Routing and Remote Access			
Add program Add port Properties Delete			
☑ Notify me when Windows Firewall blocks a new program			
OK Cancel Apply			

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.

🚡 Local Security I	Policy		
File Action View	w Help		
🗢 🔿 🔀 📊	🗟 🛛 🖬		
🚡 Security Settings	5		
🛨 📴 Account Poli	cies		
🕀 📑 Local Policies	;		
🖃 🧮 Windows Fire	ewall with Advance	ed S	ecurity
🖃 💣 Windows	s Firewall with Adv	anc	ed Security - Local Group Policy Object
🔣 Int	New Rule		
🌆 Co	Filter by Profile	•	
🕀 🚞 Public Key	Filter by State	•	
🕀 🚞 Software F	Filter by Group	•	
🕀 🛃 IP Security –			ter
	View	<u> </u>	
	Refresh		
	Export List		
	Help		
_			

🍻 New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:		
 Rule Type 	What type of rule would you like to create?	
Predefined Rules		
 Action 	 Program Rule that controls connections for a program. 	
	O Port	
	Rule that controls connections for a TCP or UDP port.	
	Predefined:	
	Remote Event Log Management	
	Rule that controls connections for a Windows experience.	
	C <u>C</u> ustom	
	Custom rule.	

Rule Type	Which rules would you like to create?	
Predefined Rules	The following rules define network connectivity requirer	
Action	Rules that are checked will be created. If a rule already exists and is che the existing rule will be overwritten.	
	-	
	Rules:	
	Name	Rule Exists
	Remote Event Log Management (RPC-EPMAP)	No
	Remote Event Log Management (NP-In)	No
	Remote Event Log Management (RPC)	No
	Remote Event Log Management (RPC-EPMAP)	No
	Remote Event Log Management (NP-In)	No
	En riende Even bog hangement (n in)	

💣 New Inbound Rule Wizard

Action

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

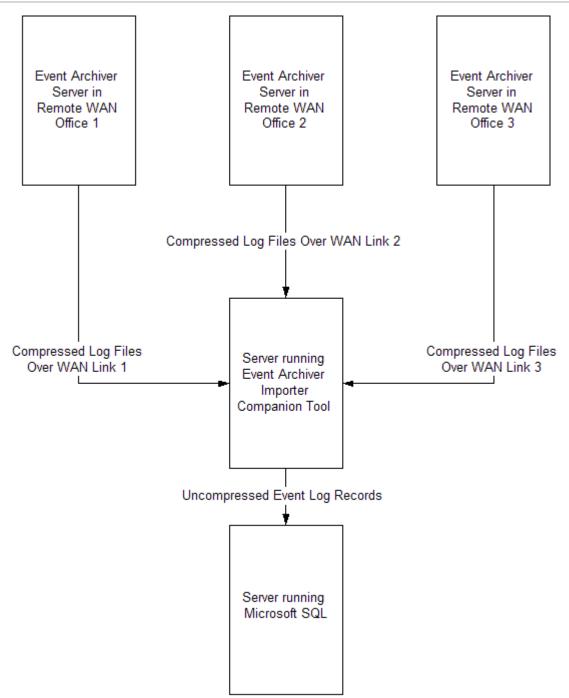
Steps:		
Rule Type	What action should be taken when a connection matches the specified conditions?	
Predefined Rules		
Action	Illow the connection	
	Allow connections that have been protected with IPsec as well as those that have not.	
	C Allow the connection if it is secure	
	Allow only connections 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.	
	Bequire the connections to be encypted	
	Require privacy in addition to integrity and authentication.	
	Override block rules	
	Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.	
	O Block the connection	

19

Network and Bandwidth Considerations

WhatsUp Event Archiver works best in a well-connected LAN environment (e.g. 10 Mbit/100 Mbit/100 Mbit/100 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 lpswitch 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.

Event Archiver Preferences
Einal Destination Defaults Performance Tuning Configuration General Configuration Computer, Log, & Schedule Defaults Staging Area Defaults Data Conversion Defaults Microsoft Vista and Server 2008 Log Settings File Hashing (MD5) Bandwidth Optimizer EVTX Log Record Fetching Limit Fetch 40 log records at a time when converting EVTX event logs. Working Directory Settings Working Directory Settings Staging Area Defaults Data Conversion Defaults
To minimize bandwidth use, move EVT/EVTX files bigger than 256 MBs temporarily into a local working directory before processing (e.g. zipping, converting). Local working directory: C:\Program Files\Event Archiver\Working\
OK Cancel

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. 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.