WhatsUp Event Analyst v10.x Quick Setup Guide

WhatsUp Event Analyst Quick Setup Guide

WhatsUp Event Analyst Quick Setup Guide

In This Guide

WhatsUp Event Analyst Quick Setup Guide

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

Click on any of the topics below to review them in depth.

Installation Requirements (on page 3)

Before You Begin (on page 4)

Vista, Windows 2008, and Windows 7 Requirements and Recommendations (on page 6)

Other Recommendations (on page 6)

Legal Information Including Patent and Trademark Notices

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.

Phone: 800-793-4825 / 781-676-5700 Fax: 781-676-5715

WWW: http://www.whatsupgold.com

Installation Requirements

The following platforms are supported:

- 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 Analyst can convert event logs into Microsoft Access database tables, so you need Microsoft Access installed if you wish to view these tables directly. However, WhatsUp Event Analyst can still read and operate on event logs stored in Microsoft Access database tables within its own interface.

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

WhatsUp Event Analyst can view, report, and filter event log information from certain ODBC server database tables (Microsoft SQL Server). Microsoft SQL Server is the recommended database server platform for LANs generating a great deal of event log activity. It is best to install WhatsUp Event Analyst to a *different* machine than the ODBC database server.

Before You Begin

1 Determine which domain(s) you want WhatsUp Event Analyst to analyze event logs from. If you want to analyze logs from more than one domain, you must choose a primary domain that is trusted by other domains. WhatsUp Event Analyst refers to this primary domain as the default domain. When prompted, enter the default domain you have chosen.

Note: If you are installing WhatsUp Event Analyst to a server or workstation not participating in a domain, please enter its workgroup instead.

Note: If you only plan to analyze event log entries stored in text files, Microsoft Access database table(s), or ODBC database table(s), enter the domain or workgroup name of your workstation

2 Make sure you are logged in with local administrator rights on the machine where you are installing the product. In addition, if the product is used to work with active or saved EVT/EVTX files in a domain, make sure you have domain administrator or organizational unit admin rights as well. Fundamentally, your domain account (or primary domain group) needs to be in the local Administrators group of all machines whose logs you will access. Otherwise, you may not be able to work with and convert all types of event log files (e.g. security logs). If you only plan to work with event log entries from Access database tables or ODBC database tables, install the software with local administrator rights, and make sure you have read and indexing rights on the database tables being viewed/reported against.

3 If you do not have an established user account with domain admin or OU admin rights that services can run under in your organization, and you plan to schedule reports against active or saved EVT/EVTX files, create a user account with Active Directory Users and Computers and place it into the Domain Admins or an OU Admins group. Also, make sure that this account has administrator rights (either by itself or via group membership) on the local machine you installed WhatsUp Event Analyst on. To prevent scheduled report interruption, make sure this account's password does not expire. The WhatsUp Event Analyst Service will run under this account, in order to have full rights across the domain when it creates reports against EVT/EVTX log files.

Note: If your domain is Windows 2000 or later, you should enter the domain name in a NetBIOS style format as opposed to a DNS-style format. If the primary domain controller or Active Directory server name cannot be resolved correctly for your domain, WhatsUp Event Analyst will ask you to enter in the name or IP address of the domain controller.

Note: If you are installing WhatsUp Event Analyst to a server or workstation not participating in a domain, or if you will only be running reports against Microsoft Access or ODBC database tables, please enter a local user account that is an Administrator of your workstation (e.g. SERVERNAME\Administrator or Domain\UserWithLocalAdmin).

4 Depending on your network structure, choose the most appropriate computer retrieval option when prompted with the Computer Name Retrieval Dialog.

> **Note**: If you are in a large, flat domain with many computer accounts, it may be best to choose either The browse list option or The following OU option to prevent lengthy timeouts associated with enumerating all computer accounts in the domain

5 If you want WhatsUp Event Analyst to email reports to interested parties after the reports are created by the WhatsUp Event Analyst Service, locate an available SMTP server on your network (we recommend the Microsoft SMTP Service that ships free with Microsoft's Internet Information Server), and adjust its security settings so that the machine(s) running WhatsUp Event Analyst may relay mail through it. Then, from the **Options** menu > **WhatsUp Event Analyst Preferences > Report Emailing** tab, enter the fully-qualified domain name or IP address of this server in the SMTP Server field. When scheduling reports, enter the email addresses of the persons wanting copies of the report in the Email Recipients field, separating each email address with a comma.

If you are installing WhatsUp Event Analyst on Windows XP or older

1 Open the **Component Services Tool** from **Administrative Tools** (or **Control Panel > Administrative Tools**). On Windows Vista or later, start it directly by locating and opening **windows\System32\comexp.msc**.

2 Expand **Component Services > Computers > My Computer**.

3 Right-click **My Computer**, and then select **Properties**. Click the **Default COM Security** tab.

4 Under **Access Permissions**, explicitly add the **Authenticated Users** identity.

5 Click **Add** to browse for this identity, select it, verify that **Allow** is checked for this user, and then click **OK** to close the dialog.

> **Note**: The security identity Authenticated Users is defined by Microsoft as follows: Includes all users and computers whose identities have been authenticated. Authenticated Users does not include Guest even if the Guest account has a password.
>
> **Note**: You are free to tighten COM security as you see fit. However, test your settings thoroughly to make sure that the WhatsUp Event Analyst Service can create scheduled reports when no user is logged on, and also verify that other interactive programs function properly after adjusting these access permissions.

6 Under **Launch Permissions**, explicitly add the user account that the WhatsUp Event Analyst Service runs/will run under. Click **Add** to browse for the account, select it, verify that **Allow** is checked for this user, and then click **OK** to close the dialog.

7 Click **OK** to close the **My Computer Properties** dialog, and then close the Component Services tool. The WhatsUp Event Analyst Service should now be able to generate scheduled reports, even when no interactive user is logged on.

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

In Microsoft 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 Analyst version 6, the software was redesigned with these considerations in mind, using only the bare minimum of network access techniques to read and manage log files from Microsoft Vista systems. 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 Analyst version 9, we have added special technology that now allows the software to open and report on 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 need to add a few additional exceptions to the Windows Firewall in order for EVTX logs to be processed successfully when WhatsUp Event Analyst is installed on a legacy operating system. You 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 Analyst.

If you install WhatsUp Event Analyst on a Windows Vista or later operating system, and will be working with EVTX log files, you will need to allow the Remote Event Log Management exception in the Windows Firewall in order for WhatsUp Event Analyst to successfully read and work with logs from Microsoft Vista or later 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 Analyst on a legacy pre-Vista Windows operating system, and will be working with EVTX log files, you 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 Analyst to successfully read and work with EVTX logs from Microsoft Vista or later machines. You also 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 Analyst over the network. Please review the aforementioned paragraph for guidance on how to do this.

Other Recommendations

WhatsUp Event Analyst works best in a well-connected LAN environment (e.g. 10 Mbit or 100 Mbit Ethernet). If you plan to convert event logs into text, Access databases, or ODBC databases, it is best to locate your WhatsUp Event Analyst server near your Primary Domain

Controller / Active Directory Server for the purpose of account lookups. Likewise, if you plan to read and/or filter active computer event logs and event log files, the reading time will be reduced if the software has adequate amounts of bandwidth to the remote server and the PDC. If you plan to use WhatsUp Event Analyst in a WAN environment, it is beneficial to install a copy of WhatsUp Event Analyst locally at each local point to speed up conversion, reading, filtering, and reporting. Use of remote desktop type software (Microsoft Terminal Services, VNC, etc) is useful in such a scenario. Optionally, you can instruct WhatsUp Event Analyst to make a copy of a live log when it is opened and transfer it to the system where WhatsUp Event Analyst is running to minimize total WAN traffic.

Another way to optimize reading, conversion, filtering, and reporting operations inside WhatsUp Event Analyst is to work with event log formats other than active computer and saved EVT/EVTX log files. Event log information stored inside EVT/EVTX files is not completely self-contained. In order to display full record information, message files and account information must be looked up across the network. Therefore, to speed up the reading process, make sure that the WhatsUp Event Analyst workstation is well connected to the primary domain controller (Active Directory Server) for account name lookups, and the actual machine where the EVT/EVTX file came from. If you do not need to perform account lookups, you can turnoff SID to account name resolutions under **Options > WhatsUp Event Analyst Preferences**. In addition, you can change the number of record WhatsUp Event Analyst reads at a time by changing the **Record Window** setting under **Options > WhatsUp Event Analyst Preferences**. Analysis using database tables is always quicker than EVT files, and Ipswitch's WhatsUp Event Archiver automatically collects your event log information into database tables that WhatsUp Event Analyst can read from.

If you plan to run scheduled reports on event logs from many different event log sources, it is beneficial to space out their report schedules. Having WhatsUp Event Analyst attempt to report on 20 different event log sources at the same time can be a severe drain on server resources. Therefore, it is best to space out reporting times and dates. All scheduled reports log a success or failure event in the Application log where WhatsUp Event Analyst is installed. Use the Application Log to check for errors if reports are not being generated properly. If scheduled reports are not running, and no errors are being logged by the WhatsUp Event Analyst Service, make sure that a.) the WhatsUp Event Analyst Service is running, and b.) your COM security settings are set correctly (see the aforementioned section on COM).

You should use filters and indexes to your advantage when working with large database tables full of event log information (inside Access or ODBC). If there are over 50,000 log records in a database table, you should use the Filter button to attach a filter to the data source before opening it. This reduces the number of records in the result set, and also reduces the time it takes to open the table. The same rule of thumb applies when scheduling a report: filters can also greatly reduce the amount of data the report module must work with. To create new filters with limiting criteria (e.g. a computer name, date range), select **Define Basic Filter** or **Define Advanced Filter** from the **Edit** menu. Indexes can also help return records more quickly. When setting up a data source in the Database Table Links Manager dialog, use the **Index Table** button when available to create a default set of indexes on your database table. These indexes help WhatsUp Event Analyst retrieve data more quickly, especially if you are limiting the data to recent dates.