IPSWITCH

WhatsUp Log Management Installation and Migration Guide, including Getting Started Information

(Applies to v10.1.5 and later)

Getting Started with WhatsUp Log Management

Installing WhatsUp Log Management

CHAPTER 1

Getting Started with WhatsUp Log Management

In This Chapter

Before You Begin

Before beginning the WhatsUp Log Management Suite installation process, it is recommended that you turn on appropriate levels of auditing on your Windows systems. This is accomplished via the Group Policy option within Active Directory. In addition, confirm that Syslog devices are configured to send data to the server running the WhatsUp Log Management Suite.

Note that additional installation and upgrade information is available within the *WhatsUp Log Management Suite v10 Release Notes* (*http://www.whatsupgold.com/ELM10relnotes*).

Operating in FIPS Mode

This topic provides information about considerations if you plan to operate WhatsUp Log Management in FIPS mode, as well as link to instructions for enabling FIPS mode and background information provided by the United States Department of Commerce.

If you are installing WhatsUp Log Management on an operating system that is currently running in FIPS140-2 mode, WhatsUp Log Management detects the FIPS compliant operating system and automatically places WhatsUp Log Management in FIPS 140-2 mode upon initial installation and start-up. However, if you plan to install WhatsUp Log Management on an operating system that is not running in FIPS mode, you must enable FIPS mode before installing the product suite.

For information about enabling FIPS mode, see the *System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting effects in Windows XP and in later versions of Windows http://support.microsoft.com/kb/811833* on the Microsoft Support site.

For more information about the FIPS 140-2 specification, see the *U.S. Department of Commerce documentation* (*http://www.whatsupgold.com/wug_USDOC_FIPS*).

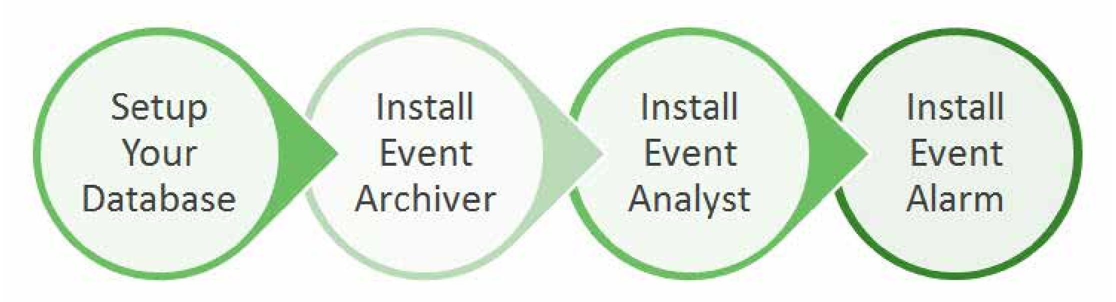
To enable or disable FIPS 140-2 mode:

Depending on your operating system, exact instructions for enabling FIPS mode may be slightly different; the instructions below are based on a Microsoft Windows 7 operating system.

1 Access **Program Options (Start)** menu **> Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options**.
2 If not already enabled, enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** option.

Deploying WhatsUp Log Management Suite

WhatsUp Log Management Suite enables you to quickly begin collecting, archiving, monitoring, analyzing and reporting on your critical log information. Use the following guidelines to deploy the WhatsUp Log Management Suite to begin managing your log data.



Additional Resources

The following resources are available for additional information on installation, setup and administration of the WhatsUp Log Management Suite:

§ WhatsUp Log Management "How-To" *Videos* (*http://www.youtube.com/playlist?list=pl4d1d3d1b5a89300c&feature=plcp*)

§ WhatsUp Log Management *Product Documentation* (*http://www.whatsupgold.com/support/guides.aspx*)

§

Support Knowledgebase (*http://whatsupgold.force.com/kb/*)

- WUGspace Log Management *Forum* (*http://community.whatsupgold.com/forums/logmanagement*) and Log Management *Evaluators Forum* (*http://community.whatsupgold.com/forums/lms-evaluators*)

Integration with WhatsUp Gold

When running WhatsUp Gold, version 15.0 or higher offers integration with the WhatsUp Log Management central database, allowing you to view data collected by Log Management within the WhatsUp Gold console. Setup instructions are available within the *Using ELM Reports in WhatsUp Gold Guide* (*http://www.whatsupgold.com/usingelmreportswug15*), detailing the process for using the WhatsUp Log Management Integration Tool, making WhatsUp Log Management data visible from within the WhatsUp Gold management console.

Step 1: Setup Your Database

You have options for installing and setting up your database. One option is to setup and install your database during the installation of WhatsUp Log Management. During the WhatsUp Log Management installation, follow the prompts to install Microsoft SQL Server 2008 Express and setup the database.

If you already have a database you want to point to, you can skip installing a database during the installation process.

If you install and setup your database after installing WhatsUp Log Management, determine the database size your environment requires. To size your database, leverage the Auditing Volume Analyzer, which is available from the Programs menu and from the WhatsUp Log Management Resource Tools subfolder.

After determining your database size requirements, install Microsoft SQL. The following options are available, depending on your storage requirements:

- Microsoft SQL Server Express 2008 R2 supports up to 10GB of storage per database and is available for free from the Microsoft web site.
- Microsoft SQL Server 2008 and 2012 provide unlimited storage options for large reporting periods. We recommend you license the Workgroup edition or higher.

Complete the database installation according to Microsoft's setup and installation procedures. Additional information for configuring SQL Server is available in the User Guide for Creating a WhatsUp Event Log Database on Microsoft SQL Server for ELM v10.x.

Step 2: Install WhatsUp Event Archiver

The next step is to install WhatsUp Event Archiver. After the installation completes, start Event Archiver from the Program menu, and follow the step-by-step wizards to establish your log collection strategy.

Based on customer experience, we have found that the best practice is to collect individual log files compressed in their native format while also importing the data into SQL Server at the time of collection. When coupled with Event Archiver's cryptographic hashing features, this provides you with the best of both worlds, as you can maintain logs in their native format for forensic purposes and create centralized reports that track similar sets of data across all of your collected systems.

Additional setup instructions are available in the *WhatsUp Event Archiver v10.x Quick Setup Guide* (*http://www.whatsupgold.com/elm10wuearqsg*).

Step 3: Install Event Analyst

The third step in the installation process is the installation of WhatsUp Event Analyst. After the installation completes, start Event Analyst from the Program menu. During the setup process, point Event Analyst to the same SQL Server used for Event Archiver by choosing the **Manage Database Table Links** option from the **File** menu. Event Analyst recognizes that they are Archiver database tables, automatically indexes them, and makes them available for reporting.

After the indexing completes, schedule recurring reports for your compliance needs by visiting the Reports menu. You can limit the data contained in the reports by first defining Basic or Advanced Filters from the Edit menu, and then selecting those filters when scheduling your reports.

Additional setup instructions are available in the *WhatsUp Event Analyst v10 Quick Setup Guide* (*http://www.whatsupgold.com/elm10wueanqsg*).

Step 4: Install Event Alarm

The final step is to install Event Alarm. After the installation completes, start Event Alarm from the Program menu. Wizards, such as the Rapid Configuration Setup or Add Multiple Syslog Devices by Subnet, available from the Tools menu, guide you through the process of establishing a log monitoring profile. The wizards help you setup new alarms, identify what logs are being monitored, for what purpose, and identify how you want to be notified about the events when they happen.

Additional setup instructions are available in the *WhatsUp Event Alarm v10 Quick Setup Guide* (*http://www.whatsupgold.com/elm10wueaqsg*).

CHAPTER 2

Installing WhatsUp Log Management

In This Chapter

Installing WhatsUp Log Management

The instructions below are for installing WhatsUp Log Management as a "fresh", first time installation.

Before beginning the installation, we recommend viewing the WhatsUp Log Management release notes, available from a link on the Welcome screen.

> **Important**: If you want to install WhatsUp Log Management 10.1.5 or later on a **Windows Server 2012** operating system and using **Microsoft SQL Server 2012**, make sure SQL Server 2012 is installed before you install WhatsUp Log Management v10.1.5 or later. If you are installing WhatsUp Log Management v10.1.5 or later and are currently using a previous version of WhatsUp Log Management, be sure to back-up your existing database and copy that database after the WhatsUp Log Management installation completes. Windows Server 2012 and SQL Server 2012 are not compatible with previous versions of WhatsUp Log Management.

1 Access Microsoft Windows using:

   § a full Domain Admin account if managing servers/workstations across a domain.

   § a local administrator account if installing to a workgroup or to a standalone machine only managing its own logs. This account should be the same as the account you will later assign to the WhatsUp Event Archiver service, WhatsUp Event Alarm service, and/orWhatsUp Event Analyst service.

2 Navigate to the directory where you downloaded the electronic version of the WhatsUp Log Management Suite and double-click the file.

3 After reading the information, click **Next** on the Welcome to the InstallShield Wizard for WhatsUp Log Management Suite screen.

4 On the License Agreement screen, select **I accept the terms of the license agreement**, and then click **Next**.

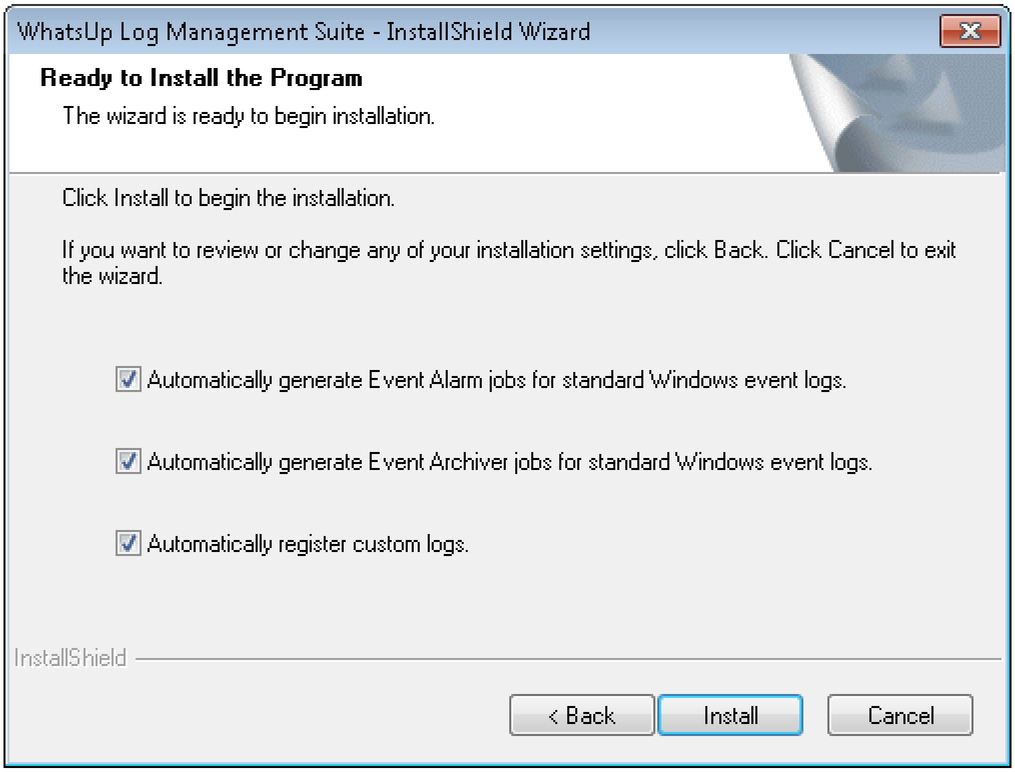
5 On the Setup Type screen:

- select **Complete** to install the full WhatsUp Log Management Suite (recommended).
- select **Custom** to install specific applications within the WhatsUp Log Management Suite.

Note: If you select and complete a Custom installation and at a later date decide to install another application within the suite or install the entire suite, reinitiate the installation process and select the appropriate installation type.

6 Depending on what suite applications you are installing, the Ready to Install the Program screen displays up to three checkboxes.

- If your installation includes Event Alarm, indicate whether you want to automatically generate Event Alarm jobs for standard Windows event logs.
- If your installation includes Event Archiver, indicate whether you want to automatically generate Event Archiver jobs for standard Windows event logs.
- Indicate whether you want to automatically register custom logs.



WhatsUp Log Management Suite - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

☑ Automatically generate Event Alarm jobs for standard Windows event logs.

☑ Automatically generate Event Archiver jobs for standard Windows event logs.

☑ Automatically register custom logs.

7 Click **Install**. The installation process begins and provides you with information until the installation completes.

8 Click **Finish** to exit the installation.

> **Tip**: Any log management title you do not install can be installed later. To access any uninstalled product, rerun your installation and select **Custom** installation. Select the products you wish to install and continue with the installation process documented in this help topic.

9 Run each installed program. As prompted, supply the service account information and default domain/workgroup information requested by each program.

> **Tip**: By default, the Syslog Listener Service is set to use the Syslog Listener Service routinely, change its startup type to Automatic in the Services MMC tool.

Important information needed before you begin an upgrade

Before you begin an upgrade to any v10.x installation of WhatsUp Log Management, it is recommended that you backup registry keys and files.

Below is a complete list of the information you need to backup.

- **Registry Keys**
- **HKEY_LOCAL_MACHINE\Software\DorianSoft** (the whole key)

> **Important**: The registry values contain paths (i.e. C:\Program Files (x86)\Ipswitch\WhatsUp Event Alarm…). As a result, WULM has to be installed in same path on the new box and/or the values in the registry must be adjusted. Also, if you are moving from 10.1.3 or 10.1.4 with Event Archiver and installed a database, that database needs to be in the same state (i.e. remote\local\none) as there is a key "WizardDatabaseTarget" that points Event Archiver in the right direction.

- **Files**
- WhatsUp Event Alarm
  - config.mdb
  - configupdate01.dat
  - easl.dat
  - easl6.dat
  - easlex.dat
  - easlex6.dat
  - rapidconfigbasic.dat
  - Listener Console\ealisten.ini

- WhatsUp Event Archiver
    - config.mdb
    - easl.dat
    - easl6.dat
    - easlex.dat
    - easlex6.dat
    - EventDrop.ini
    - friendly_eids.dat
- WhatsUp Event Analyst
    - config.mdb
    - configupdate01.dat
    - configupdate02.dat
    - configupdate03.dat
    - schedule.mdb
    - friendly_eids.dat
- WhatsUp Event Rover
    - friendly_eids.dat
    - Incidents.ini
    - RecentFiles.ini
    - RecentFilters.ini
    - SavedGroups.ini
    - SavedQuickFilters.ini
- Database information
    - If WhatsUp Event Archiver is pointed to a local database, you need to move the database to the new server. If you used a remote database, and it is still remote, no changes are needed.
    - By default, the database is named "WhatsUpLogManagementData," and you can backup/restore the database using Management Studio or a similar tool.

Upgrading the WhatsUp Log Managment Suite

To upgrade the WhatsUp Log Management Suite if you are currently using version 8 or earlier of various titles (e.g. Event Archiver, Event Analyst, Event Alarm)

Currently, there is no automated mechanism for upgrading older versions of the software. You must first manually upgrade the software to version 9 of the WhatsUp Log Management Suite, then proceed with the automated procedure below. For manual upgrade instructions, and the version 9 installation package, visit http://www.myipswitch.com and log on to your account.

To upgrade the WhatsUp Log Management Suite if you are currently using version 9 or later

1 Access Microsoft Windows using:

- a full Domain Admin account if managing servers/workstations across a domain.
- a local administrator account if installing to a workgroup or to a standalone machine only managing its own logs. This account should be the same as the account you will later assign to the WhatsUp Event Archiver service, WhatsUp Event Alarm service, and/or WhatsUp Event Analyst service.

2 Make a note of the current accounts you have assigned to the WhatsUp Event Archiver Service, WhatsUp Event Analyst Service, and WhatsUp Event Alarm Services. You need to resupply this information after the upgrade process completes.

Navigate to the directory where you downloaded the electronic version of the WhatsUp Log Management Suite (WUELM.exe), and double-click the file.

3 The WhatsUp Log Management Upgrade Validation tool appears. If not already present, type your name, your company name, email address, and service number, and then select **Validate Online**. If you do not have a connection to the Internet, choose **Validate Offline**, and write down the information you need to enter at the https://www.myipswitch.com/licensing/ Web page.

4 After submitting your upgrade request via the Web, type the validation code displayed on the website in the Enter Your Upgrade Validation Code form, and click **OK**.

5 Indicate whether you accept or do not accept the terms of the license agreement. If you accept the terms of the license agreement, click **Next**.

6 You are offered the options of a Complete installation or a Custom installation. To install the entire WhatsUp Log Management Suite, select **Complete**, and then click **Next**. To install specific products within the suite, select **Custom**, and then click **Next**.

7 Click **Install** on the Ready to Install the Program screen. The installation process begins and provides you with information until the installation completes.

8 Click **Finish** to exit the installation.

9 Run each installed program. As prompted, supply the service account information and default domain/workgroup information requested by each program.

Tip: By default, the Syslog Listener Service is set to use the Syslog Listener Service routinely, change its startup type to Automatic in the Services MMC tool.

Note: WhatsUp Log Management Suite v9 customers who upgrade in place to WhatsUp Log Management Suite v10 or later may notice that there are no default basic Syslog filters defined in the software after the upgrade. To remedy this, click the **Edit** menu, then choose **Define Basic Filters**. Click **Add Syslog** to create a new filter. After the filter properties are assigned, click **Save**, then on the next screen, file your filter under the **Syslog OS Type** and type a new Category name, depending on how you want to categorize your filter.

Note: When upgrading 10.1.5, you need to run the Database Update Tool, see the last item in the *New in WhatsUp Log Management Suite v10.1 release notes* (*http://www.whatsupgold.com/ELM10relnotes*) for more information. The Database Update Tool is NOT required for 10.1.6 and later releases.

Activating the WhatsUp Log Management Suite

Activation of the WhatsUp Log Management Suite is done manually on a product by product basis. To start this process, please enter your information, including the service number provided by Ipswitch customer service after your purchase, in the Licensing Dialog. Here's how to access the licensing dialog in each product:

WhatsUp Event Archiver. From the Help menu, select Register WhatsUp Event Archiver.

WhatsUp Event Analyst. From the Help menu, select Register WhatsUp Event Analyst.

WhatsUp Event Alarm. From the Help menu, select Register WhatsUp Event Alarm.

WhatsUp Event Rover. From the Help menu, select Register WhatsUp Event Rover.

To later add licenses to any installed instance of one or more of the above products, visit the Help menu, and this time, select Upgrade WhatsUp [Product Name] Licenses.

For complete help on how to use the Licensing Dialog, press **F1** when this dialog is actively displayed.

For more information and updates

The following are information resources for the WhatsUp Log Management Suite.

§ **Context-sensitive Help**. From within each log management title. Press **F1** from within WhatsUp Event Archiver, WhatsUp Event Analyst, WhatsUp Event Alarm, or WhatsUp Event Rover to displays that product's help system.

§ **User Guide**. Each log management title ships with its own comprehensive User Guide. These can be found under the Program group for each log management title in the Start Menu.

§ **Quick Setup Guide**. Each log management title also ships with a Quick Setup Guide that helps users quickly configure each program and other network/security settings for optimal performance. These can be found under the Program group for each log management title in the Start Menu.

§ **Creating a Microsoft SQL Server Database**. For log management titles that can utilize a database server, this guide explains how to create, configure, and initially size a Microsoft SQL Server database for use with WhatsUp Event Archiver, WhatsUp Event Analyst, or WhatsUp Event Alarm. These can be found under the Program group for each log management title in the Start Menu.

§ **Technical Support**. Use the WhatsUp Gold Support Site for a variety of WhatsUp Gold product help resources. From here you can view product documentation, search Knowledge Base articles, access the community site for help from other users, and get other Technical Support information. The Support Site is available on the WhatsUp Gold web site.