IPSWITCH

WhatsUp Log Management v10 and v10.1 Getting Started Guide

Welcome to WhatsUp Log Management

Log files contain a wealth of information you can leverage to reduce an organization's exposure to intruders, malware, damage, loss and legal liabilities. Log data needs to be collected, stored, analyzed and monitored to meet and report on regulatory compliance standards like Sarbanes Oxley, Basel II, HIPAA, GLB, FISMA, PCI DSS and NISPOM. Yet, monitoring log files is impossible without the right tools, because log files come from many different sources, in different formats, and in massive volumes.

With WhatsUp Log Management Suite, you can automatically collect, archive, monitor, analyze and report on Syslog messages, Windows computer event logs, or W3C logs generated by Web Application Servers, Load Balancers, Firewalls, Proxy Servers or Content Security appliances. This Getting Started Guide provides an overview for installing WhatsUp Log Management Suite to get your software up and running quickly.

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 guideline to deploy the WhatsUp Log Management Suite to begin managing your log data.

Before You Begin

Before beginning the WhatsUp Log Management Suite installation process, 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.

Step 1: Setup Your Database

When installing and setting up your database, first determine the size of database your environment requires. To size your database, leverage the Auditing Volume Analyzer, which is available in the Program menu and from the WhatsUp Log Management Resource Tools subfolder.

After determining the requirements for your database size, install Microsoft SQL. Two 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 website.
- Microsoft SQL Server 2005 and 2008 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 the WhatsUp Event Archiver module. 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.

Step 3: Install Event Analyst

The third step in the installation process is the installation of 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.

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.

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, detailing the process for using the WhatsUp Log Management Integration Tool, making WhatsUp Log Management data visible from within the WhatsUp Gold management console.

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
- WhatsUp Log Management Product Documentation
- Support Knowledgebase
- WUGspace Log Management Forum and Log Management Evaluators Forum