IPSWITCH

# WhatsUp Auditing Volume Analyzer Tool v10.x User Guide

# Using the WhatsUp Auditing Volume Analyzer Tool

The WhatsUp Auditing Volume Analyzer report is designed to show how much event log data is being generated on servers and workstations in various Microsoft Windows domains and workgroups, as well as the storage requirements to maintain that log data over time. Various federal acts, such as HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley, require the preservation and analysis of this data over certain time frames. Therefore, it is important to understand how different auditing policies affect the growth of Windows event log files.

The WhatsUp Auditing Volume Analyzer tool allows you, the administrator, to choose which domain controllers, servers, and workstations you wish to include in the report from various domains.

If analyzing logs in your domain, full domain Administrator rights are required when running the software. If analyzing logs in a workgroup, local Administrative rights across all machines are required. If analyzing logs only on the local machine, local Administrative rights are required.

### To analyze and report on event log data:

**1** Designate the domain name and computer types you would like to analyze.

a) In the **Domain Name** field, type the domain of the servers and workstations with log activity you want to analyze. The domain can be in either NetBIOS or DNS-style formats (if a Windows 2000 or Windows 2003 domain).

b) Click to select the categories of computers you want to report on (e.g. domain controllers, member servers, and workstations).

c) Click **Fetch Computers** to retrieve all computers in your domain in the selected categories.

**Note**: If you are only analyzing the local computer's event logs, or if you are analyzing computers with unified administrative accounts and passwords in a workgroup, skip step 1 and add the computers manually.

**Note**: To manually retrieve computers correctly, NetBIOS over TCP/IP must be enabled, and, if your domain spans multiple TCP/IP subnets, a WINS system should be in place. If some computers remain missing after clicking the Fetch Computers button, type their names or IP addresses manually in Step 2.

2. Adjust the machine names as desired to control which computer logs are used to generate the report. Unchecked computers are not used in the report; alternatively, you can remove them from the list by using the **Remove** buttons. Click the **Add** buttons to add machine names or IP addresses manually to the lists.
3. Select the types of information to include in your report. Only checked items are reported on.

   a) Click to select the information to be analyzed.

   b) Click **Analyze and Report** to prepare your report. A progress indicator displays as the report is prepared, and once finished, the Auditing Volume Analyzer launches your report in your default web browser. All reports are saved in HTML format in the directory where you installed the Auditing Volume Analyzer.