



Managing Event Logs

This document illustrates how MS Event Logs are a powerful tool for network security. It includes important factors and a breakdown of activities in successful event log management as well as methods to enable effective event logging.

Event Logs

Event logs have been a feature of the MS Operating System (Windows) since the original release of Windows NT in 1993. Designed to provide an audit trail of system use, event logging records the actions that occur within the system, such as users logging in, failure of a component to start, or an attempt to print a document.

Actions are grouped together in event logs so that system usage can be tracked and analyzed. Windows NT defined three categories of logs: System, Application and Security. Additional categories were added as new versions of Windows were released; Windows Vista includes Administrative, Analytic, Debug and Operational log types as well as numerous subcategorized event logs.

Every event that occurs across a network can be recorded in an event log file. The list of events that are recorded by default can be modified to reflect the needs of the organization's system. The most common addition is a type of security auditing, specifically file auditing, which can be set up to record information about access to files and folders. Many other forms of security auditing exist, including printer use, which can enrich event logs.

The amount of data generated is dependent on the number of events that are recorded. It can quickly become very large even in a small organization. Event logs are an important tool in network monitoring; however managing event log data can be very challenging.

Event Log Management

Information stored in event log files is extremely useful to organizations as it provides real-time indications of network incidents as well as an audit trail of user activity. However extracting useful information can be challenging as it is very difficult to manage and filter the vast amount of data generated.

If event log file data is not organized and managed regularly then any network incidents or security breaches may be completely overlooked. When a problem is finally detected, analyzing the data that has been generated since the log files were last reviewed becomes a daunting task. Regularly auditing log file data allows potential incidents to be reported as they occur and may also assist in preventing future occurrences.

Although the MS provided interface (Windows Event Log in Vista) for event logging and tracing has improved dramatically from the original, there are many easier-to-use solutions available that allow event log managing. When examining a solution it is useful to remember that the two most important factors for successful event log management are automation and storage.

Extracting meaningful information from a large amount of data can be very challenging if done manually. Automation of tasks relating to event logs ensures that any information collected is entire and reliable. Data integrity is ensured, and the possibility of overlooking sections of data is removed. An appropriate method of storage and representation of extracted information is also very significant in event log management. An effective analysis of the information provides the necessary details to recognize any security breaches or system incidents.

Event log management can be partitioned into three main activities that together provide an effective use of event logs and a thorough understanding of network activity. The three activities are:

- **Collecting**
Log files need to be collated and maintained in a way that allows the data to be used quickly and not affect its reliability.
- **Reporting**
Data extracted from event log files should be consolidated into a report format that provides easy to access, understandable information.
- **Analyzing**
Data needs to be available in a filtered or enhanced format that provides detailed information, such as specific events or network trends, without including other information.

System Auditing

An organizations' event log management is only as effective as the amount of data they are including from their networks activity. To be able to provide an accurate report on any particular part of the system, data needs to be generated for that part. For example, you cannot compile a report on who accessed a confidential file if you do not set up the file to raise an event (and have the event logged) when the file is accessed.

System auditing helps protect system resources and information by recording access attempts and other related information. This is achieved by setting an event on activities that need to be monitored, and then recording the results in an event log.

As the required level of monitoring depends on the organization and there are many event categories in security auditing, the first step is determining which event categories need to be audited. The following are a list of available categories:

- | | |
|--|---|
| • Account Logon Events
Track users logon and logoff events. | Used to record user access of objects such as files. |
| • Account Management
Tracks attempts to create users or groups, rename users or groups, enable user accounts, disable user accounts or change account passwords. | • Policy Change
Records changes to user rights assignment policies such as Windows Firewall Policy. |
| • Directory Service Access
Used with auditing tasks on domain controllers. | • Privilege Use
Records when users exercise a user privilege. |
| • Logon Events
Records creation and destruction of logon sessions (including remote sessions) | • Process Tracking
Tracks process information such as program activation/exit. |
| • Object Access | • System Events
Records system events such as shutting down a computer. |



Each of these categories contains many subcategories and events which can be used to create a complete audit trail of system activity. It is recommended that only essential events are setup for auditing as generating a large number of events can severely affect system performance. The following information states how to setup file and folder auditing as an example of object access auditing.

File and Folder Auditing

Windows XP introduced the Operation-based auditing feature for files and folders. Prior to this development the only means of auditing files was object-based. Object-based auditing involves generating an event when an object is accessed. This provides information such as user access, however the level of detail is not sufficient to accurately record what occurred.

Operation-based auditing on files provides a means of tracking the history of that file. It allows a distinction to be made between a user who requests write access and then closes the file without making changes, and a user who edited the file. This allows files and folders to be accurately tracked for access, changes and deletion, a crucial element for system security in an organization.

Windows XP

The setup for operation-based file and folder auditing in Windows XP requires administrative privileges and the object-based auditing to be enabled. After auditing is enabled, the files and folders to audit can be specified. If object-based auditing is not enabled an error message will be displayed when attempting to audit files and folders.

After completing the setup for auditing, the Audit log will appear in the Security log which can be viewed using the Event Viewer.

Note: If your computer is part of a domain, then domain-level auditing policies override local security settings.

To enable the Audit log:

1. Click **start**, click **Control Panel**, click **Performance and Maintenance**, and then click **Administrative Tools**
2. Double-click **Local Security Policy** *Note: If the computer is part of a domain then **Domain Security Policy** should be used.*
3. In the left pane, double-click **Security Policies** to expand it
4. In the left pane, click **Audit Policy** to display the individual policy settings
5. Double-click **Audit Object Access**
6. To audit successful access to objects, select the **Success** check box
7. To audit unsuccessful access to objects, select the **Failure** check box
8. Click **OK**

To specify the files and folders to audit:

1. In Windows Explorer, locate the file or folder to audit
2. Right-click the file or folder and then click **Properties**
3. Click the **Security** tab, and then click **Advanced**
4. Click the **Auditing** tab, and then click **Add**
5. In the **Enter the object name to select** box, type the name of the user or group to audit access
*Note: Clicking **Advanced**, and then clicking **Find Now** in the **Select User or Group** dialog box will allow browsing*
6. Click **OK**
7. Click the **Success** or **Failed** check boxes for the action to audit, then click **OK**
8. Click **OK**, then click **OK**

After you set up auditing on a parent folder, new files and subfolders that are created in that folder inherit auditing.

To remove inheriting auditing for a particular file or subfolder:

1. Locate the particular file or subfolder in Windows Explorer
2. Right-click the folder or file and then click **Properties**
3. Click the **Security** tab, then click **Advanced**
4. Click the **Auditing** tab, and clear the **Inherit from parent the auditing entries that apply to child objects** checkbox

To remove inherited auditing for all files and subfolders:

1. Locate the parent folder in Windows Explorer
2. Right-click the parent folder and then click **Properties**
3. Click the **Security** tab, then click **Advanced**
4. Click the **Auditing** tab, and clear the **Inherit from parent the auditing entries that apply to child objects** checkbox

Windows Vista

Operation-based file and folder auditing in Windows Vista is very similar to Windows XP. Administrative privileges are required and object-based auditing needs to be enabled. The Audit Object Access needed to enable the Audit log is located in a slightly different area (see workflow below). The remaining setup is identical (see Windows XP).

To enable the Audit log:

1. Click **start**, click **Control Panel**, click **System and Maintenance**, and then click **Administrative Tools**
2. Double-click **Local Security Policy** *Note: If the computer is part of a domain then **Domain Security Policy | Group Policies** should be used.*
3. In the left pane, double-click **Local Policies** to expand it
4. In the left pane, click **Audit Policy** to display the individual policy settings
5. Double-click **Audit Object Access**
6. To audit successful access to objects, select the **Success** check box
7. To audit unsuccessful access to objects, select the **Failure** check box
8. Click **OK**

WebSpy Vantage

WebSpy offers a software solution, Vantage, which can provide successful event log management specific to an organization.

Vantage provides support for the three essential activities:

- **Collecting**
Log files are stored in an optimized database called a storage, allowing fast data access with complete reliability.
- **Reporting**
Reports collate information from a storage and display useful information that is easy to understand. There are many templates available and reports can be saved in a variety of file formats or emailed
- **Analyzing**
Running an analysis creates a summary based on the data in a storage. A summary can be interactively browsed and filtered to any level.

Vantage also provides filtering, aliasing (to enhance readability of data), automation of tasks, and extensive support.



Vantage Product Information

[WebSpy Vantage](#) is an award-winning software product that provides you with a common reporting window into all the key functions of your network and its usage within your organization. The comprehensive information provided by Vantage can assist in identifying and resolving network problems, reducing security vulnerabilities, as well as maximizing employee productivity by encouraging responsible usage of system resources.

WebSpy [Vantage Ultimate](#) incorporates a Web Module, secure internal website, that enables administrators to securely distribute reports and information throughout an organization. Employees can log into the Web Module to view their reports, and conduct ad-hoc drilldowns into their storages, providing up to date information whenever they need it. Access to information is controlled through customizable permission levels, ensuring employee and company privacy.

Vantage and Event Logs

After file auditing settings have been implemented on the system, it is a simple process to start managing event logs and extracting information using Vantage.

The first step is to import Windows Event Logs into a storage in Vantage. This process can be added to run automatically at appropriate intervals using Tasks. After creating a storage for Windows Event Logs, reports can be generated and analyses run. This will allow useful information to be extracted from Event Log data.

Vantage uses aliases for the creation of more meaningful information, for example, event ID's are translated to an event category to enhance readability of generated reports and analyses. A list of event ID's and their categories has been included in this document for reference purposes.

Importing event logs into a storage:

1. Open Vantage and click the **Storages** tab
2. In the left pane, click **Import Logs** This will start the import dialog wizard
3. Enter a name for the storage in the **Create a new storage** dialog box, then click **Next**
4. Select the **Windows Event Log** radio button, then click **Next**
5. Select the **Microsoft** format (description: Windows Event Log), then click **Next**
6. Click **Add**, enter the name the computer in the **Server** dialog box, click **OK** and then click **Next**
7. Continue through the wizard and select any filter, field or partitioning options to include, then click **OK** The event log data will now be imported into the storage

Generating a Report:

1. Click the **Reports** tab
2. Select the type of Report to generate *Note: Vantage includes many default templates for Windows Event Logs such as Failed Events, Application Errors and Failure Audit Trends.*



3. In the left pane, click **Generate Report** This will launch the Generate Report wizard
4. Select the storage to report on *Note: This should be the storage created previously for Windows Event Logs*
5. Select the document format(s) for the report
6. Enter the report name in the **Document Name** dialog box
7. Continue through the wizard and select any splitting, filtering or email options, then click **OK**
The report will now be generated

Running an Analysis:

1. Click the **Summaries** tab
2. In the left pane, click **New Analysis** This will launch the Create Analysis wizard
3. Enter a name for the analysis in the **Name** dialog box, select the storage, and check that the schema is set to **All Windows Event Schemas**, then click **Next**
4. Select the type of Analysis to run, then click **Next**
5. Continue through the wizard and select any filtering or summaries options, then click **OK** The summary will now be generated

The summary allows interactive drilldowns to any level for data mining and information exploration.

Event ID's and Categories

Account Logon:	680
Logon/Logoff:	529, 534, 537
Installation:	17, 18, 19, 21
Server:	958, 1485, 1486, 3408, 3454, 5084, 8128, 9666, 9688, 9689, 15268, 15457, 17069, 17101, 17103, 17104, 17110, 17111, 17115, 17125, 17126, 17136, 17137, 17147, 17148, 17162, 17164, 17176, 17199, 17403, 17550, 17551, 17656, 17658, 17663, 19030, 19032, 26018, 26048
Setup:	1017, 1019, 1020, 1023, 1025
Policy Change:	612
Web Event:	1309, 1310

Additional Information

Event Log Management

Windows Event Logs - [Microsoft Developer Network](#)

Managing Event Logs in XP – [Microsoft Support](#)

Event Viewer – [Wikipedia](#)

Windows Vista – Event Viewer Improvements – [Computer Performance](#)

Windows XP Event Log – [Windows Help Central](#)

Monitoring Event Logs in Windows Vista – [Mitch Tulloch](#)

System Auditing

Windows Server 2008 Security Guide – [Microsoft Download](#)

Security Auditing in Windows 2000 – [Microsoft Support](#)

Auditing User Access in Windows XP – [Microsoft Support](#)

Information Systems Audit – [Roger Clarke](#)

Windows and Active Directory Auditing – [Derek Melber](#)

Enable Security Auditing in Windows XP Pro – [Tony Bradley](#)

Event ID's

Event ID Search – [EventID](#)

Troubleshooting Windows Event ID – [Chicago Tech](#)

Windows Security Log Encyclopedia – [Randy Smith](#)

WebSpy

For more information about WebSpy please visit <http://www.webspy.com>

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of WebSpy Ltd.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by WebSpy Ltd, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

WebSpy Ltd. reserves the right to change details in this publication without notice.

Other product and company names herein may be the trademarks of their respective owners.



Contact WebSpy Ltd

If you would like more information on managing event logs or any of the products mentioned, please contact your nearest WebSpy Office:

WebSpy North America (Servicing North and South America)

Legacy Southcenter Place 16400 Southcenter Parkway, Suite 201 Seattle, Washington 98188

Toll free: 888-862-4403

Phone: +1 206-575-7763

Fax: +1 206-575-7809

Email: sales@webspy.com

WebSpy Europe (Servicing Europe, Middle East and Africa)

3rd Floor, Unit 19 Angel Gate 326 City Road London, EC1V 2PT

Phone: +44 (0) 207 239 7500

Fax: +44 (0) 207 239 7539

Email: europesales@webspy.com

WebSpy Australia (Servicing Australia, Asia and the Pacific)

Level 3, 9 Colin Street West Perth, Western Australia 6005

Toll Free: 1800 801 121

Phone: +61 8 9321 3322

Fax: +61 8 9321 3377

Email: sales@webspy.com.au

Alternatively contact WebSpy support on our [support page](#)