Starting and Quitting Event Viewer

To start Event Viewer

- Click **Start,** point to **Programs,** then point to **Administrative Tools,** and click **Event Viewer**.

To quit Event Viewer

- On the **Log** menu, click **Exit**.

Viewing Event Logs

To select another computer for viewing

1 On the **Log** menu, click **Select Computer**.

2 Enter the name of a computer in **Computer**.

3 If your computer is connected to the selected computer by a low-speed device, such as a modem, select the **Low Speed Connection** check box.

To select another log for viewing

1 On the **Log** menu, click System, Security, or Application.

2 Select the log you want to see.

3 If you want to view specific event records in that log, you can do one of the following.

- To sort events chronologically, click **Oldest First** or **Newest First** on the **View** menu.
- To view only events with specific characteristics, click **Filter Events** on the **View** menu.
- To search for events based on specific characteristics or event descriptions, click **Find** on the **View** menu.
- To see descriptions and additional details that the event source might, click **Detail** on the **View** menu.

Changing the Font

To change the font used in event lists

1 On the **Options** menu, click **Font**.

2 In **Font**, click the font you want to use.

3 In **Font Style**, click a style, such as **Bold** or **Italic**.

4 In **Size**, enter a number for point size.

Filter

Use the **Filter** dialog box to define the date range, type of events, source, and category of events displayed for the current log.

Your choices for filtering are used throughout the current Event Viewer session. When filtering is on, a check mark appears by **Filter** on the **View** menu and "(Filtered)" appears in the title bar.

Click the following buttons for specific information about this dialog box:

- View From
- View Through
- Information
- Warning
- Error
- Success Audit
- Failure Audit
- Source
- Category
- User
- Computer
- Event

See Also

Filtering Events

Find

Use the **Find** dialog box to search the current log for specific events by type, source, or category. For example, you can search for all Warning events related to a specific application.

Click the following buttons for specific information about this dialog box:

- Information
- Warning
- Error
- Success Audit
- Failure Audit
- Source
- Category
- Event
- Computer
- User
- Description
- Direction

See Also

Searching for Events

Event Detail

Use the **Event Detail** dialog box to see more information about a selected event .

The information displayed at the top of this dialog box is the same information that is presented in the Event Viewer main window.

All event information is saved if you archive a log in log file format (*.EVT). The event data is discarded if you archive the file in any text format (*.TXT).

Click the following buttons for specific information about this dialog box:

- Description
- Data
- Previous and Next

See Also

Viewing Event Details

Event Viewer Main Window.

Event Log Settings

Use the **Event Log Settings** dialog box to define the maximum log size and what Windows NT should do when the event log is full.

Click the following buttons for specific information about this dialog box:

- Change Settings
- Maximum Log Size
- Overwrite Events as Needed
- Overwrite Events Older Than [ ] Days
- Do Not Overwrite Events
- Default

See Also

Setting Options for Logging Events

Open

Use the **Open** command to open an archived log file.

When you click **Open** after specifying options in the **Open** dialog box, the **Open File Type** dialog box appears. You can then specify whether the event log you want is a System, Security, or Application

log.

Click the following buttons for specific information about this dialog box:

- File name
- Files of type
- Look in

See Also

Viewing a Log Archived in Log File Format

Open File Type

This dialog box appears when you click **OK** in the **Open** dialog box.

Use the **Open File Type** dialog box to specify the type of log saved in the archived file that you want to open.

Open File Type

Click System, Security, or Application to specify the type of log in the archived file that you want to open.

If you do not specify the correct log type, the Description displayed for the archived log in the **Event Detail** dialog box will be incorrect.

See Also

Viewing a Log Archived in Log File Format

Archiving Event Logs

Save As

Use the **Save As** dialog box to archive events in log file format or in text file format.

This dialog box appears when you click **Save As** on the **Log** menu. It also appears when you click **Clear All Events** on the **Log** menu, and then click **Yes** to save the events before clearing the log.

- File name
- Save as type
- Save in

See Also

Archiving Event Logs

Clear All Events

Select Computer

Use the **Select Computer** dialog box when you want to view events for another computer.

To specify the computer whose events you want to view

- Type the computer name in **Select Computer**, beginning with "\\" characters, for example, **\\mypc1**.

Or, click a computer name in **Select Computer**.

To specify a low-speed connection

- If your computer is connected to the selected computer by a low-speed device, such as a modem, select this check box.

Note

- **Select Computer** on the **Log** menu is not available unless you are logged on as an Administrator.

Saving a Log Before Clearing

To save a log before clearing

In the **Clear Event Log** dialog box, click one of the following.

- Click **Yes** if you want to create an archive of the records now listed in your event log.
- Click **No** if you want to permanently discard all current event records and start recording new events in your log.
- Click **Cancel** if you want the log to remain as is.

See Also

Save As Dialog Box

Clearing All Events

To clear all events before saving

1. In the **Clear Event Log** dialog box, click one of the following.
   - Click **Yes** if you want to create an archive of the records now listed in your event log.
   - Click **No** if you want to permanently discard all current event records and start recording new events in your log.
   - Click **Cancel** if you want the log to remain as is.

Resetting to the Default Settings

To reset your default settings

1. In the **Event Log Settings** dialog box, click **Yes** if you want to discard all the current setting and revert to the default values.

   Or, click **No** if you want to keep any or all of the current settings.

Reducing Log Size

1 In the **Event Log Settings** dialog box, enter a number for **Maximum Log Size**.

2 On the **Log** menu, click **Clear All Events**, to put the new maximum size setting in effect.

Tip

- You can archive the records in the current log by clicking **Save As** on the **Log** menu.

System

- On the **Log** menu, click **System** to display the System log for the selected computer.

You can now view, sort, filter, and search for details about events.

See Also

Viewing Event Details

Sorting Events

Filtering Events

Searching for Events

Security

- On the **Log** menu, click **Security** to display the Security log for the selected computer.

You can now view, sort, filter, and search for details about events.

See Also

Viewing Event Details

Sorting Events

Filtering Events

Searching for Events

Application

- On the **Log** menu, click **Application** to display the Application log for the selected computer.

You can now view, sort, filter, and search for details about events.

See Also

Viewing Event Details

Sorting Events

Filtering Events

Searching for Events

Exit

Quits Event Viewer.

Clear All Events

To clear a log

1 Switch to the log you want to clear.

2 On the **Log** menu, click **Clear All Events**.

A message asks if you want to archive the currently logged events.

- If you answer **Yes**, the **Save As** dialog box appears. Enter the filename and folder path where you want the archived log to be stored.
- After you answer **Yes** or **No**, Event Viewer empties the current log. Only new events will appear in the log.

Notes

- If you check **Do Not Overwrite Events (Clear Log Manually)** in the **Event Settings** dialog box, you must periodically clear the log, either when the log reaches a certain size or when a message notifies you that the log is full.
- You cannot clear archived logs; instead, delete the archived log file.

All Events

- On the **View** menu, click **All Events** to display all events for the current log.

Note

- When a check mark appears by **All Events**, **Filter** is automatically unchecked.

Newest First

- On the **View** menu, click **Newest First** to display the most recent events at the top of the Event Viewer window.

A check mark appears by **Newest First** when it is selected.

Note

- If a check mark appears by **Save Settings On Exit** on the **Options** menu when you quit, this newest-first sort order is used the next time you start Event Viewer.

See Also

Sorting Events

Save Settings On Exit

Oldest First

- On the **View** menu, click **Oldest First** to display the oldest events at the top of the Event Viewer window.

A check mark appears by **Oldest First** when it is selected

Note

- If **Save Settings On Exit** on the **Options** menu is checked when you quit Event Viewer, this oldest-first sort order remains in effect when you restart Event Viewer.

See Also

Sorting Events

Save Settings On Exit

Refreshing a log

- On the **View** menu, click **Refresh** to update the events currently shown in Event Viewer.

Notes

- **Refresh** is not available for archived logs because those files are never updated.
- When you first open a log, Event Viewer displays the current information for that log. That information is not updated while you view the list unless you refresh it. The log is automatically updated only when it is no longer the current log displayed in Event Viewer.

Low Speed Connection

Use the **Low Speed Connection** setting if you are connected to the network by a low-speed device, such as a modem.

If **Save Settings On Exit** on the **Options** menu is checked when you quit Event Viewer, your **Low Speed Connection** setting remains in effect when you restart Event Viewer.

See Also

Save Settings On Exit

Save Settings On Exit

Save Settings On Exit ensures that any changes made during the current session are saved. This includes:

- Current size and position settings for the Event Viewer window.
- Filtering options and sort order for logs.
- Settings for **Find**.
- Type of log displayed.

However, if an archived log is displayed when you quit, the System log (the default) are displayed the next time you start Event Viewer.

Understanding Event Viewer

Event Viewer is the tool you can use to monitor events in your system. You can use Event Viewer to view and manage System, Security, and Application event logs. You can also archive event logs.

The event-logging service starts automatically when you run Windows NT. You can stop event logging with the Services tool in Control Panel.

Click the following buttons for specific information about the contents of the Event Viewer window:

- Source
- User
- Category
- Computer
- Event
- Type

Setting Options for Logging Events

To set event-logging options (for Administrators only)

1 On the **Log** menu, click **Log Settings**.

2 In the **Event Settings** dialog box, select the type of log to which the settings will apply under **Change Settings For**.

3 In Maximum Log Size, specify the log size, in kilobytes.

4 Under **Event Log Wrapping**, select an option that defines how the events are retained for the selected log.

5 If you want to restore all default settings, click Default.

Note

- Click to see information about the **Event Log Wrapping**
- Overwrite Events As Needed
- Overwrite Events Older Than [ ] Days
- Do Not Overwrite Events

Sorting Events

To specify sort order

- On the **View** menu, click **Newest First** or **Oldest First**.

If **Save Settings On Exit** on the **Options** menu is checked when you quit, the current sort order is used the next time you start Event Viewer.

Notes:

- When a log is archived, the sort order affects files that you save in text format or comma-delimited text format. The sort order does not affect event records you save in log-file format.
- The default is from newest to oldest.

See Also

Save Settings On Exit

Filtering Events

To filter events

1 On the **View** menu, click **Filter Events**.

2 In the **Filter** dialog box, specify the characteristics for displayed events.

3 To return to the default criteria, click **Clear**.

Tip

To turn off event filtering, click **All Events** on the **View** menu.

Searching for Events

To search for specific kinds of events in a log

1 On the **View** menu, click **Find**.

2 In the **Find** dialog box, click the Types of events you want to find.

3 Specify any other Source, Category, Event, Computer, and User events you want to find.

4 In **Description**, you can type any text that matches a portion of an event record description.

5 To specify the direction of the search, click **Up** or **Down**.

6 Click **Find Next** to begin the search.

7 To restore the default search criteria, click **Clear** before clicking **Find Next**.

Tips

- After you define the search criteria, you can press F3 to find the next matching event without displaying the **Find** dialog box.
- Your search choices remain in the **Find** dialog box throughout the current session. The default settings are restored the next time you start Event Viewer.

Viewing Event Details

To view more details about an event

1 Click the event you want to see; then click **Detail** on the **View** menu.

2 In the **Event Detail** dialog box, use the scroll box to browse the information in **Description** and **Data**.

3 To see details about other events, click **Next** or **Previous**.

Tips

- Click **Bytes** to view binary data as characters. Click **Words** to see binary data as DWORDS.
- Not all events generate binary data. This information can be interpreted by an experienced programmer or a support technician familiar with the source application.
- Archived logs and logs saved in log-file format retain the event description, also called binary data. Saving your files in text format or comma-delimited text format discards the binary data.

Archiving Event Logs

To archive an event log

1 On the **Log** menu, click **Save As**.

2 In **Save as type**, click a file format.

3 In **File Name**, enter a filename for the archived log file.

Event Viewer adds the .EVT filename extension for log files, or the .TXT extension for either kind of text-file format.

Note

When you archive a log file, the entire log is saved, regardless of filtering options. Logs saved as text files or comma-delimited text files retain the current sort-order but not the binary data for each event record.

See Also

Viewing a Log Archived in Log File Format

Viewing a Log Archived in Log File Format

To display an archived log in Event Viewer

1 On the **Log** menu, click **Open**.

2 In the **Open** dialog box, enter the filename in **File Name**, and click **OK**.

3 The **Open File Type** dialog box appears.

4 Click System, Security, or Application, to match the type of log you want to see.

Notes

- If you do not specify the correct log type, the Description displayed log in the **Event Detail** dialog box is incorrect.
- You can view an archived file in Event Viewer only if the log is saved in log file format. You cannot click **Refresh** or **Clear All Events** to update the display or to clear an archived log. To remove an archived log file, you must delete the file in Windows NT Explorer.

See Also

Archiving Event Logs

Recovering After Windows NT Halts Because it Cannot Generate an Audit-Event Record

To recover when Windows NT halts because it cannot generate an audit-event record

1 Restart the computer and log on using an account in the Administrators group.

2 Use Event Viewer to clear all events from the Security log, archiving the currently logged events.

3 Use Registry Editor to delete and replace the CrashOnAuditFail value in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa key Use data type REG_DWORD and a value of 1.

4 Exit, and restart the computer.

See Also

Clear All Events

Event

Shows an event number to identify the specific event.

The **Event** helps product-support representatives track events in the system.

View From

- Click **Events On** to see events that occur after a specific date and time.

  The default value is the date of the first event in the log file.

View Through

- Click **Events On** to see events that occur up to and including a specific date and time.

  The default value is the date of the most recent event in the log file.

Information

Select this check box to see events logged by successful operations of major server services, such as when a database program loads successfully.

Warning

 Select this check box to see events that are not necessarily significant but that may cause future problems, such as when disk space is low.

Error

Select this check box to see events logged by significant problems, such as a loss of data or loss of functions.

Success Audit

 Select this check box to see audited security-access attempts that were successful, such as a user successfully logging onto the system.

Failure Audit

Select this check box to see audited security access attempts that failed, such as a user failing to access a network drive.

Source

The software that logged the event, which can be either an application or a component of the system, such as a driver.

User

Specific text that exactly matches text in the **User** name field. This field is not case sensitive.

Category

A classification of the event, as defined by the source.

For example, the categories for Security event logs are Logon and Logoff, Policy Change, Privilege Use, System Event, Object Access, Detailed Tracking, and Account Management.

Computer

The exact name of the computer where the logged event occurred. This field is not case sensitive.

Type

A classification of the event by the Windows NT operating system, such as Error, Warning, Information, Success Audit, or Failure Audit.

Description

Text you enter that matches any portion of an event-record description (the text string that appears in the **Event Detail** dialog box).

Note

You can search for any portion of an event record description.

The complete text is not required.

Direction

Specifies the direction of the search, either **Up** or **Down**.

Note

The search direction is independent of the sort-order checked on the **View** menu.

Description

A text description of the event, created by the event source of the event.

You can click **Find** to search for specific events, using any portion of this description. The description is also saved in all archived logs.

Data

Determines the format in which binary data is displayed. Click **Bytes** to see the information in hexadecimal format

Click **Words** to see DWORDS for the same data.

Note

Not all events generate binary data. This information can be interpreted by an experienced programmer or a support technician familiar with the source application.

Previous or Next

Used to browse details about other events in the current log.

Click **Previous** or **Next** to see details about the adjacent events in the sort-order sequence.

Change Settings

Used to select the type of log for which you want to specify settings: System Event, Security Event, or Application Event.

Maximum Log Size

Used to specify the maximum log-file size. The default maximum size is 512K.

To change the maximum size, click the up arrow or down arrow.

Overwrite Events as Needed

When selected, ensures that all new events are written to the log, even when the log is full. Each new event then replaces the oldest event.

Tip

This option is the best choice for ease of maintenance and is the default.

Overwrite Events Older than [ ] Days

When selected, retains a log for a specific number of days before overwriting it. You can set the number of days before a log can be overwritten, using numbers from 1 to 365.

Tip

The default setting for this option is 7 days. This is the best choice if you want to archive log files weekly.

Do Not Overwrite Events

When selected, retains all existing events when the log is full.

This option requires that you manually clear the log. Click this option only if you must retain all events

Default

Restores all default settings for the selected log.

What to Do When an Event Log Is Full

- To free a log when it is full (no more events can be logged), click **Clear All Events** from the **Log** menu.

  You can also free a log by decreasing the retention period in the **Event Settings** dialog box.

Note

- You cannot reinstate logging by increasing the maximum log size. To increase the log size, first clear the log, and then increase the maximum size in the **Event Settings** dialog box. Then restart the system.

File name

Specifies the filename for the archived log file.

Files of type

Specifies the type of file you want to open.

- Click **Event Log File** (*.EVT) to see all files in the current folder that were saved with an .EVT extension.
- Click **All Files (*.*)** to see all files in the current folder.

Look in

Lists the available folders and files. To see how the current folder fits in the hierarchy on your computer, click the arrow. To open a folder, click it.

Look in shows the folders and files in the selected location. You can double-click one of these folders or files to open it. If you want to see the folder one level higher, click the up folder button on the toolbar.

Save in

Lists the available folders and files. To see how the current folder fits in the hierarchy on your computer, click the down arrow. To open a folder, click it.

The folders and files in the selected location appear below **Save in**. You can double-click one of these folders or files to open them. If you want to see the folder one level higher, click the up folder button on the toolbar.

Save as type

Specifies the file format for saving the log information. Your can select any of the following.

- If you want to be able to open the archived log in Event Viewer later, click **Event Log File (*.EVT)** to save event records in log-file format.
- If you want to use the information in another application such as a word processor, click **Text Files (*.TXT)** to save the log in text-file format.
- If you want to use the information in another application such as a spreadsheet or a flat-file database, click **Comma Delim. Text (*.TXT)** to save the log in comma-delimited text file format.

Event

In the Windows NT operating system, an event is any significant occurrence in the system or in an application that requires users to be notified. For critical events such as a full server or an interrupted power supply, you may see a message on screen. For many other events that do not require immediate attention, the Windows NT operating system adds information to an event-log file to provide information without disturbing your usual work. This event logging service starts automatically each time you start you computer running Windows NT.

System Log

The System log records events logged by the Windows NT system components. For example, the failure of a driver or other system component to load during startup is recorded in the System log.

Security Log

The Security log records security events. This helps track changes to the security system and identify any possible breaches to security. For example, attempts to log on the system may be recorded in the Security log, depending on the Audit settings in User Manager.

You can view the Security log only if you are an Administrator for a computer.

Application Log

The Application log records events logged by applications. For example, a database application might record a file error in the Application log.

Event Log Size

Appears if you specify a maximum-log size that is not a multiple of 64K.

You can make the following changes.

- Click **O** to increase the size of the log to the next higher multiple of 64K.

  For example, if you enter 500K, the log size is set to 512K.
- To leave the log size as it was before you started, click **Cancel** both here and again in the **Event Log Settings** dialog box.
- To enter a different log size, click **Cancel**; then, in the **Event Log Settings** dialog box, enter a new log size, using a multiple of 64K.

Contents

Starts Help and displays the topics in Event Viewer Help.

Search for Help on

Opens the **Index** tab for Event Viewer Help. You can use keywords on this tab to look up Help information.

How to Use Help

Describes how to use Help.

About Event Viewer

Displays version, mode, and copyright information about Windows NT.

Click **Help Topics** for a list of Help topics