Contents for Event Viewer Help

Expand

You can use Event Viewer to monitor events in your system.

How To...

- View Event Logs
- Use and Manage Event Logs
- Archive Event Logs

Commands

- Log Menu Commands
- View Menu Commands
- Option Menu Commands

Contents for Event Viewer Help

Collapse

You can use Event Viewer to monitor events in your system.

How To...

Commands

Contents for Event Viewer Help

You can use Event Viewer to monitor events in your system.

How To...

Commands

Contents for Event Viewer Help

You can use Event Viewer to monitor events in your system.

How To...

Commands

Contents for Event Viewer Help

You can use Event Viewer to monitor events in your system.

How To...

Commands

Contents for Event Viewer Help

You can use Event Viewer to monitor events in your system.

How To...

Commands

Contents for Event Viewer Help

You can use Event Viewer to monitor events in your system.

How To...

Commands

Contents for Event Viewer Help

You can use Event Viewer to monitor events in your system.

How To...

Commands

Viewing Event Logs

You determine the log and computer selected for viewing in Event Viewer.

To select another computer for viewing

1. From the Log menu, choose Select Computer.
2. Select a computer from the Select Computer list, or enter a computer name in the Computer box.
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.
4. Choose the OK button.

To select another log for viewing

- From the Log menu, choose System, Security, and Application.

After you select a log to view in Event Viewer, you can take several actions to view specific event records in that log, such as:

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

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 the Filter command on the View menu and (Filtered) appears in the title bar.

Choose one of the following buttons for information about this dialog box:

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

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.

Choose one of the following buttons for information about this dialog box:

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

See Also

Searching for Events

Event Detail

Use the Event Detail dialog box to view additional information about a selected event . This dialog box appears when you select an event in the Event Viewer window and then choose the Detail command from the View menu.

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).

Choose one of the following buttons for 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. This dialog box appears when you choose Log Settings from the Log menu.

Choose one of the following buttons for 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. This dialog box appears when you choose Open from the Log menu.

When you choose the OK button after specifying options in this dialog box, the Open File Type dialog box appears so that you can specify whether the log you want is a System, Security, or Application event log.

Choose one of the following buttons for information about this dialog box:

- File Name
- List Files Of Type
- Drives
- Directories
- Networks

See Also

Viewing a Log Archived in Log File Format

Open File Type

Use the Open File Type dialog box to specify what type of log was saved in the archived file you are opening. This dialog box appears when you choose the OK button in the Open dialog box.

Open File Type

- To specify the type of log saved in the archived file that you want to open, select the System, Security, or Application option button.

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 choose the Save As command from the Log menu. It also appears when you choose the Clear All Events command, and then choose Yes when the message asks if you want to save the events before clearing the log.

- File Name
- Save Files As Type
- Drives
- Directories
- Networks

See Also

Archiving Event Logs

Clear All Events

Select Computer

Use the Select Computer dialog box to view events for another computer. You can either type a computer name or select from the list.

This dialog box appears when you choose Select Computer from the Log menu. This command is not available unless you are logged on as an Administrator.

Computer

- To specify the computer whose events you want to view, type a computer name in this box.

Select Computer

- To specify the computer whose events you want to view, select a computer name in this list.

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.

Save a Log Before Clearing

You have chosen to clear all events in the current log, but Windows NT first gives you the opportunity to save the current records in an archive file.

If you choose Yes in the message box, the Save As dialog box appears so that you can specify a filename for the log. Then the current records in the event log are cleared.

If you choose No to proceed, all current events are discarded. New events are recorded in the log. Old records are not archived.

If you want to keep the events in the current log, choose Cancel.

See Also

Save As Dialog Box

Clearing All Events

You have chosen to clear all events in the current log.

If you choose Yes to proceed, all event records in the current log are discarded. New events are recorded in the log.

If you want to keep the events in the current log, choose No.

After you close this message, you can archive the events in the current log by choosing the Save As command from the Log menu.

Reset to Default Settings

You have chosen to reset all the values in the Event Log Settings dialog box to their default values.

If you want to proceed and discard all the current settings, choose the Yes button.

If you want to keep any current settings, choose the No button.

Reducing Log Size

You have chosen to reduce the maximum size of the log file for the current event log. For the reduced size to take effect, you must first clear this log by choosing the Clear All Events command from the Log menu.

Before you clear the log, you can archive the records in the current log by choosing the Save As command from the Log menu.

System

Choose the System command from the Log menu to display the System log for the selected computer.

After you select a log for display in Event Viewer, you can view, sort, filter, and search for details about events.

See Also

Viewing Event Details

Sorting Events

Filtering Events

Searching for Events

Security

Choose the Security command from the Log menu to display the Security log for the selected computer.

After you select a log for display in Event Viewer, you can view, sort, filter, and search for details about events.

See Also

Viewing Event Details

Sorting Events

Filtering Events

Searching for Events

Application

Choose the Application command from the Log menu to display the Application log for the selected computer.

After you select a log for display in Event Viewer, you can 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

Choose the Clear All Events command to clear all events in the current log.

If you specify that events cannot be overwritten in a log in the Event Settings dialog box, you will need to clear the log periodically--either when the log reaches a certain size or when a message notifies you that the log is full. Archived logs cannot be cleared.

To clear a log

1. Switch to the log whose events you want to clear.
2. From the Log menu, choose 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 directory path where you want the archived log to be stored.

   After you answer Yes or No, Event Viewer empties the current log. All new events will be recorded in the log.

All Events

Choose the All Events command from the View menu to display all events for the current log in the Event Viewer window.

Choosing this command turns off the Filter command.

Newest First

Choose the Newest First command to display the most recent events at the top of the Event Viewer window.

When this command is currently in effect, its command name is checked on the View menu.

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

See Also

Sorting Events

Save Settings On Exit

Oldest First

Choose the Oldest First command to display the oldest events at the top of the Event Viewer window.

When this command is currently in effect, its command name is checked on the View menu.

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

See Also

Sorting Events

Save Settings On Exit

Refresh

Choose the Refresh command to update the events currently shown in Event Viewer.

When you first open a log, Event Viewer displays the current information for that log. Unless you choose the Refresh command, this information is not updated automatically while you are viewing the list: new events are not added, and overwritten entries are not removed from the list. The event listing is updated automatically only when you select a different log for viewing or when you start Event Viewer again.

If you are viewing an archived log, the Refresh command is not available because archived files are never updated.

Low Speed Connection

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

If the Save Setttings On Exit command is checked on the Options menu, the setting of the Low Speed Connection command is retained from one Event Viewer session to the next.

See Also

Save Settings On Exit

Save Settings On Exit

Choose the Save Settings On Exit command to ensure 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 the Find command.
- 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.

Font

Enables you to change the font used for the list of events in the Event Viewer main window.

What Is 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 by choosing the Services tool in Control Panel.

To control the types of security events to be audited, choose Audit from the Policies menu in User Manager. To control the auditing of file and directory access, choose Auditing from the Security menu in File Manager.

Choose one of the following buttons for information about the contents of the Event Viewer window:

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

Setting Options for Logging Events

You can define the maximum log size for each type of log, and also specify whether the events are overwritten or stored. For the Security log, the administrator can also set auditing policies in User Manager that cause the system to halt when the security log is full.

To set event logging options

1. From the Log menu, choose Log Settings.
2. In the Change Settings For box of the Event Settings dialog box, select the type of log for which you want to specify settings.
3. In the Maximum Log Size box, specify the size of the log in kilobytes.
4. Select an Event Log Wrapping option to define how the events are retained for the selected log. For information about these options, choose one of the following topics:

   - Overwrite Events As Needed
     - Overwrite Events Older Than [ ] Days
     - Do Not Overwrite Events
5. If you want to restore all default settings, choose the Default button.
6. Choose the OK button.

Sorting Events

The events displayed in Event Viewer are listed in sequence by date and time of occurrence. You can specify the order, depending on whether you want to show newest events first or oldest first. The default listing order is from newest to oldest.

When a log is archived, the sort order affects the order in which event records are saved in a text format or comma-delimited text format file. But sort order does not affect the order of event records in a log archived in log file format. If the Save Settings On Exit command from the Options menu is checked when you quit, then the current sort order is used the next time you start Event Viewer.

To specify sort order

- From the View menu, choose Newest First or Oldest First.

The command currently in effect is checked on the View menu.

See Also

Save Settings On Exit

Filtering Events

When you first start Event Viewer, all events recorded in the selected log are displayed. Filtering has no effect on an archived log file, because the unfiltered log is saved.

To filter events

1. From the View menu, choose Filter Events.
2. In the Filter dialog box, specify the characteristics that qualify an event for display in Event Viewer.
3. To return to the default criteria, choose the Clear button.
4. Choose the OK button to view the filtered events.

To turn off event filtering

- Choose All Events from the View menu.

Searching for Events

You can search for specific events that match the type, source, or category that you define. For example, you can search for all Error events related to a specific source.

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.

To search for specific kinds of events in a log

1. From the View menu, choose Find.
2. In the Find dialog box, select any of the Types of events you want to find.
3. Specify any other Source, Category, Event ID, Computer, and User events you want to find.
4. In the Description box, type text that matches any portion of an event record description.
5. To specify the direction of the search, select the Up or Down option.
6. To restore the default search criteria, choose the Clear button.
7. Choose the Find Next button to begin the search.

After you define the search criteria, you can press F3 to find the next matching event without displaying the Find dialog box.

Viewing Event Details

For many events, you can view more information than is displayed in Event Viewer. This information is generated by the application that was the source of the event record. However, not all sources or events generate event details.

The event description is saved in all archived logs. The event binary data is saved if you archive a log in log file format, but is discarded if you archive it in text or comma-delimited text format.

To view more details about an event

1. In Event Viewer, double-click the event for which you want to view details. Or select an event in the list, and then choose Detail from the View menu.
2. In the Description or Data box of the Event Detail dialog box, use the scroll box to browse the information about the event.

   To view binary data in hexadecimal format, select the Bytes option. To view binary data as DWORDS, select the Words option. This information can be interpreted only by a support technician familiar with the source application or by an experienced programmer.
3. To view details about other events in sort-order sequence, choose the Next or Previous button.
4. When you finish viewing details, choose the OK button to return to Event Viewer.

Archiving Event Logs

You can archive an event log in log file format so that you can later reopen it in Event Viewer. Or the log can be saved in text format or comma-delimited text format so that you can use the information in other applications.

When you archive a log file, the entire log is saved, regardless of filtering options. For a log saved in a text or comma-delimited text file, event records are saved in the current sort order, and the binary data for each event record is discarded.

To archive an event log

1. From the Log menu, choose Save As.
2. In the Save File As Type box, select a file format option for saving the log information, and then choose the OK button.
3. In the File Name box, type a filename for the archived log file.
4. Choose the OK button.

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

See Also

Viewing a Log Archived in Log File Format

Viewing a Log Archived in Log File Format

You can view an archived file in Event Viewer only if the log is saved in log file format. You cannot choose the Refresh or Clear All Events commands to update the display or to clear an archived log. To remove an archived log file, you must delete the file in File Manager.

To display an archived log in Event Viewer

1. From the Log menu, choose Open.
2. In the File Name list of the Open dialog box, select the filename of the log you want to view, and then choose the OK button.
3. When the Open File Type dialog box appears, select the type of log you saved originally: System, Security, or Application. Then choose the OK button.

If you do not specify the correct log type, the Description displayed log in the Event Detail dialog box is incorrect.

See Also

Archiving Event Logs

Event ID

Shows a specific event number to identify the event. The Event ID helps product support representatives track events in the system.

View From

- Select the Events On button to view 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

Select the Events On button to view events that occur up to and including a specific date and time. The default value is the date of the last event in the log file.

Information

Select this check box to view events logged by successful operations of major server services. For example, when a database program loads successfully, it may log an Information event.

Warning

Select this check box to view events that are not necessarily significant but that may cause future problems. For example, a Warning event might be logged when disk space is low.

Error

Select this check box to view significant problems, such as a loss of data or loss of functions. For example, an Error event might be logged if a service was not loaded during Windows NT startup.

Success Audit

Select this check box to view audited security access attempts that were successful. For example, a user's successful attempt to log onto the system might be logged as a Success Audit event.

Failure Audit

Select this check box to view audited security access attempts that failed. For example, if a user tries and fails to access a network drive, the attempt might be logged as a Failure Audit event.

Source

The software that logged the event, which can be either an application name or a component of the system or an application, such as a driver name. For example, "Elinkii" indicates the Etherlink II driver.

User

A specific user that matches an actual user name. This field is not case sensitive.

Category

A classification of the event as defined by the source. For example, the Security event categories are Logon and Logoff, Policy Change, Privilege Use, System Event, Object Access, Detailed Tracking, and Account Management.

Computer

A specific computer that matches an actual computer name where the event occurs. This field is not case sensitive.

Type

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

Description

Type text that matches any portion of an event record description (the text string that appears in the Event Detail dialog box).

You can search for any portion of an event record description. The complete text is not required.

Direction

- To specify the direction of the search, select the Up or Down option.

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

Description

A text description of the event that is created by the source of the event.

You can use the Find command to search for specific events based on any portion of this description. The description is also saved in all archived logs.

Data

To view binary data for the selected event in hexadecimal format, select the Bytes option and then scroll to view the data.

To view binary data as DWORDS, select the Words option and then scroll to view the data.

Not all events generate binary data. Unless you are an experienced programmer, this information can only be interpreted by a support technician familiar with the source application.

Previous or Next

To browse details about other events in the current log, choose the Previous button or Next button. Details are presented in sort-order sequence.

Change Settings

To select the type of log for which you want to specify settings, scroll in the Change Settings list to select System Event, Security Event, or Application Event.

Maximum Log Size

To specify the maximum log file size, choose the up arrow or down arrow button to select a number. Or type a number in kilobytes.

The default maximum size is 512 kilobytes.

Overwrite Events as Needed

To ensure that all new events are written to the log when the log is full, select the Overwrite Events As Needed option.

When you select this option, each new event replaces the oldest event if the log is full. This option is the default and the best choice for ease of maintenance.

Overwrite Events Older than [ ] Days

To retain a log for a specific number of days, select Overwrite Events Older than [ ] Days, and then enter the number of days, from 1 to 365, you want to retain events before overwriting.

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

Do Not Overwrite Events

To ensure that all events are retained when the log is full, select the Never Overwrite Events option.

This option requires that you clear the log manually. Select this option only if you must retain all events. For example, select this option for the Security log if security is extremely important at your site.

Default

To restore all default settings for the selected log, choose the Default button.

What to Do When an Event Log Is Full

To free a log when it is full (no more events can be logged), choose Clear All Events from the Log menu. You can also free a log by decreasing the retention period in the Event Settings dialog box.

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

File Name

To specify the filename for this file, type a filename in the text box or select a filename in the list. This box lists files with the extension you select in the Files Of Type box.

List Files Of Type

To specify the type of file you want to open, select an option in the list.

Event Log File (*.EVT) lists all files in the current directory that were saved with an .EVT extension.

All Files (*.*) lists all files in the current directory.

Drives

To specify the drive for where this file is stored, scroll in the list and select a drive.

Directories

- To specify the directory for this file, scroll in the list and select a directory.

Networks

To specify the network drive for this file, choose the Networks button, and then scroll in the list to select a network drive.

Save File As Type

To specify the file format for saving the log information, select an option in the list.

Select the Event Log File (*.EVT) option to save event records in log file format if you want to view the archived log in Event Viewer later.

Select the Text Files (*.TXT) option to save the log in text file format, for using the information in an application such as a word processor.

Select the Comma Delim. Text (*.TXT) option to save the log in comma-delimited text file format, for using the information in an application such as a spreadsheet or a flat-file database.

Event

In Windows NT, 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, Windows NT 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 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 only view the Security log 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

You have specified a maximum log size that is not a multiple of 64 KB.

If you choose the OK button in this dialog box, the size of the log is increased to the next higher multiple of 64 KB. For instance, if you entered 500 KB, the log size is set to 512 KB.

To leave the log size as it was before you started, choose the Cancel button in this dialog box and again in the Event Log Settings dialog box.

To enter a different log size, choose Cancel in this dialog box. In the Event Log Settings dialog box, enter a new log size that is a multiple of 64 KB, and then choose the OK button.

Contents

Starts Help and displays the topics in Event Viewer Help.

Search for Help on

Opens the Search dialog box for Event Viewer Help. You can look up Help information by using keywords in this dialog box.

How to Use Help

Describes how to use Help.

About Event Viewer

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