Advanced Event Viewer
Manual

Download Advanced Event Viewer at: http://www.AdvancedEventViewer.com

Document version: 2.2944.01
Introduction

Advanced Event Viewer is an award winning application to centrally view and manage all Windows event logs and disk capacity. Advanced Event Viewer doesn’t require any modifications to your network and is doesn’t require agents to be installed. Advanced Event Viewer retrieves events remotely and is fully multithreaded. The program is easy to install and easy to use.

Starting in version 2 you are able to select an internal database for small and medium sized organizations and any Microsoft SQL Server for medium to large organizations.

Download Advanced Event Viewer

Advanced Event Viewer can be downloaded from:

Evaluate Advanced Event Viewer

Advanced Event Viewer can be evaluated for 30 days. The evaluation version is fully functional and doesn’t expire (e.g. it doesn’t stop working after 30 days), however if you want to use Advanced Event Viewer after 30 days, the appropriate license is required.

Purchase Advanced Event Viewer

To calculate the number of licenses you need, count the number of systems you have added in Advanced Event Viewer and each machine you run Advanced Event Viewer on (e.g. your management workstation)

For more information and to order Advanced Event Viewer, please visit our order site at:
http://www.AdvancedEventViewer.com/Order
# Table of Content

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Download Advanced Event Viewer</td>
<td>2</td>
</tr>
<tr>
<td>Evaluate Advanced Event Viewer</td>
<td>2</td>
</tr>
<tr>
<td>Purchase Advanced Event Viewer</td>
<td>2</td>
</tr>
<tr>
<td>Installation</td>
<td>5</td>
</tr>
<tr>
<td>Installation using the build in database</td>
<td>5</td>
</tr>
<tr>
<td>Installation using a Microsoft SQL Server database</td>
<td>5</td>
</tr>
<tr>
<td>Windows Firewall configuration</td>
<td>5</td>
</tr>
<tr>
<td>Using Advanced Event Viewer</td>
<td>6</td>
</tr>
<tr>
<td>Advanced Event Viewer tips</td>
<td>6</td>
</tr>
<tr>
<td>Shortcuts</td>
<td>6</td>
</tr>
<tr>
<td>Toolbars</td>
<td>6</td>
</tr>
<tr>
<td>Themes</td>
<td>6</td>
</tr>
<tr>
<td>Modify Advanced Event Viewer settings</td>
<td>7</td>
</tr>
<tr>
<td>Preferences panel</td>
<td>7</td>
</tr>
<tr>
<td>Retrieving Options Settings</td>
<td>7</td>
</tr>
<tr>
<td>Events Age</td>
<td>8</td>
</tr>
<tr>
<td>Events Types</td>
<td>8</td>
</tr>
<tr>
<td>Other Options</td>
<td>8</td>
</tr>
<tr>
<td>Displaying Options Settings</td>
<td>9</td>
</tr>
<tr>
<td>Mail Connection Settings</td>
<td>10</td>
</tr>
<tr>
<td>Scheduler Settings</td>
<td>11</td>
</tr>
<tr>
<td>Miscellaneous Settings</td>
<td>12</td>
</tr>
<tr>
<td>Disk Capacity Settings</td>
<td>13</td>
</tr>
<tr>
<td>Database Engine Settings</td>
<td>14</td>
</tr>
<tr>
<td>Adding Servers to Advanced Event Viewer</td>
<td>14</td>
</tr>
<tr>
<td>Add computers by name</td>
<td>15</td>
</tr>
<tr>
<td>Add computers using the Activate Directory Browser</td>
<td>15</td>
</tr>
<tr>
<td>Analyze server connection</td>
<td>16</td>
</tr>
<tr>
<td>Removing servers from Advanced Event Viewer</td>
<td>16</td>
</tr>
<tr>
<td>View server information from Advanced Event Viewer</td>
<td>17</td>
</tr>
<tr>
<td>Retrieving Windows events logs</td>
<td>17</td>
</tr>
</tbody>
</table>
Manually retrieving events .......................................................... 17
Automatic retrieving events ......................................................... 18
Scheduled event retrieval ............................................................ 18
Viewing Event Log records .......................................................... 18
Navigating Event Log records ....................................................... 19
Direct link to the Microsoft Knowledge base ................................. 20
Direct link to Google .................................................................... 20
Direct link to the Event ID database ............................................. 20
Open Remote Desktop ................................................................. 20
Open Event Viewer ....................................................................... 20
Add to filter .................................................................................. 21
Modifying the view ....................................................................... 21
Quick Filters ................................................................................. 22
Event Log Types (application, security, etc) ................................. 22
  Monitoring disk capacity ............................................................. 23
  Email Current Page .................................................................... 23
  Export Log option ..................................................................... 24
  Folder Tree Size Scanner .......................................................... 24
  Filtering event records ............................................................... 26
  Mark as Reviewed ..................................................................... 26
Creating reports ........................................................................... 27
Reports Management .................................................................... 29
Server and Credential Manager .................................................. 30
**Installation**

To install Advanced Event Viewer, simply double-click the setup MSI file available from:


Advanced Event Viewer doesn’t require any agents to be installed and uses the same interface as the build in event viewer from Microsoft to retrieve events.

To install Advanced Event Viewer, you must be a local administrator on the machine where the program is installed and you need permissions to read the event logs of the servers that you want to monitor using Advanced Event Viewer.

The supported operating systems are Windows 2000, XP, 2003, Vista, 2008, 2008 R2 and Windows 7, both x86 and x64.

**Installation using the build in database**

Advanced Event Viewer includes a build in database for easy installation. The build in database is based on the popular SQLite database engine ([http://www.sqlite.org](http://www.sqlite.org)). This database is optimized for small to medium networks (75+ servers). Advanced Event Viewer also includes support for Microsoft SQL Server based databases (all versions of Microsoft SQL Server and Microsoft SQL Server Express).

During the installation of Advanced Event Viewer, you are able to select the database you want to use. After installation you can always modify the database type and location using the Preferences dialog.

**Installation using a Microsoft SQL Server database**

Advanced Event Viewer allows you to use all versions of Microsoft SQL Server and Microsoft SQL Server Express.

During installation you are able to select the database of your choice. If you select Microsoft SQL Server, Advanced Event Viewer will contact the SQL Server and check if an Advanced Event Viewer database is already present (named: AEVDB). If AEVDB is not already available on the selected SQL Server, Advanced Event Viewer will offer you to create the database automatically.

Please note that Microsoft SQL Express default configuration doesn’t allow remote connections. To modify this and allow remote connections, use the “SQL Server Surface Area Configuration for Services and Connections” available in:

"%programfiles%\Microsoft SQL Server\90\Shared\SqlSAC.exe"

Then go to: SQLEXPRESS -> Database Engine -> Remote Connections -> Local and remote connections (using TCP/IP). Restart the “SQL Server (SQLEXPRESS)” service to effectuate the change.

**Windows Firewall configuration**

If your Windows Servers are using the build in Windows Firewall, please ensure “Remote Administration” (Windows 2008) or “Remote Event Log Management” (Windows 2008 R2) is enabled in the Firewall Exceptions list.

You can test the (Event log) connection to your server by right clicking on the selected server in the “Managed Servers” tab, and then selecting “Analyze Server Connection”.

---

Page 5
Using Advanced Event Viewer

This chapter describes the functionality of Advanced Event Viewer. It will show you how easy it is to add all your servers and configure Advanced Event Viewer to suite your needs.

Advanced Event Viewer tips

Shortcuts

Advanced Event Viewer allows the users to use shortcuts for different actions. Below you can find a table with some of the important shortcuts:

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL + P</td>
<td>Opens the Preferences panel</td>
</tr>
<tr>
<td>ALT + X</td>
<td>Closes the Advanced Event Viewer application</td>
</tr>
<tr>
<td>F5</td>
<td>Refresh the event list</td>
</tr>
<tr>
<td>F12</td>
<td>Get Events</td>
</tr>
<tr>
<td>CTRL + Enter</td>
<td>Open the selected event in detail view</td>
</tr>
<tr>
<td>Del</td>
<td>Remove selected server/event</td>
</tr>
<tr>
<td>ALT + R</td>
<td>Open Remove Desktop</td>
</tr>
<tr>
<td>ALT + E</td>
<td>Open Event Viewer</td>
</tr>
</tbody>
</table>

Toolbars

Advanced Event Viewer’s toolbars (Standard, Filters, Reports and Search toolbars) can be disabled or enabled. Also, you can arrange them as you want, just moving them with the mouse.

Themes

You can change Advanced Event Viewer theme at any time, selecting the theme from the “View” menu, using “User Interface Style” option. You can choose from the following themes: AEV Theme Silver, AEV Theme Luna, AEV Theme Obsidian, AEV Theme Blue, AEV Theme Silver Old, AEV Theme Olive, AEV Theme Classic, AEV Theme XP and AEV Theme Whidbey.
Modify Advanced Event Viewer settings

Advance Event Viewer settings can be change anytime. To do that, go to File and select the “Preferences” option:

Preferences panel

This is the “Preferences” panel. All settings, with their details, will be described below.

General Settings

In the general settings tab, you can modify the “Database path”, the “HTML templates location”, the “Temporary Path” and the “Default HTML template”. The “Database path”, “HTML templates location” and “Temporary Path” can be set to any location on your hard-drive. The “Default HTML Template” can be chosen from 4 different HTML templates.

Retrieving Options Settings

In this tab you can change how Advanced Event Viewer is retrieving the events.
**Events Age**
Using this option, you can select if you want to retrieve all events or only the events from the last day. Also, you can choose to retrieve all events using “Load all events” option or select maximum events to be retrieved using “Load the most recent” option.

**Events Types**
You can choose what kind of events to be retrieved from the server: “Information”, “Critical”, “Warning”, “Error”, “Audit Success” and “Audit Failure”. By default, the “Information” and “Audit Success” event types are not retrieved.

**Other Options**
Here you can select if you want to “Update Events on Consolidated Mode”, “Remember last Update / Get Only New”, “Show retrieving detail dialog” and “Clear info on finish” or “Clear Event log on the server side, after the events are retrieved”.

![Image of Preferences window showing options for retrieving events, event types, and other options.](image-url)
Displaying Options Settings
In this tab you can select how to display the events. You can choose from “Show Events in Consolidated Mode”, what event types to be displayed and select from the following filters: “Last Hour Events”, “Last 4 Hours”, “Current Day”, “Last Day Events”, “Last Week Events”, “Last Month Events” or “View All Events”.

![Preferences window]

- Show Events in Consolidated Mode
- Event Types: Information, Warning, Critical, Error, Audit Success, Audit Failure
- Filters: Last Day Events
Mail Connection Settings
In this tab you have setup your STMP server and how do you want the report to be sent. The “Mail From Information” can be setup using the “From E-mail” and “To E-mail” options. Also, you can choose the “Report Format” as PDF, HTM, TXT or CSV, to be sent as a plain text or attached. For the “HTM” option, you can select a default template for the email.
Scheduler Settings
Advanced Event Viewer allows you to retrieve events automatically when the program is running. Select the Preferences dialog, click Scheduler and check the “Enable automatic retrieval” checkbox. You can also click the “Automatic Retrieval...” label in the Status Bar (on the bottom of the Advanced Event Viewer screen). You can also Manage the saved reports or create a new report.
**Miscellaneous Settings**
In this section you can select the thread priority and the maximum number of threads, how to run the database maintenance and what kind of Event logs you want to display. You can create a list of events that you don’t want to retrieve from the server (Add, Remove or Clear List).
Disk Capacity Settings
Using this option, you can enable or disable the “Disk Capacity Check”. You can also setup when to display a warning or an error.
**Database Engine Settings**

Advanced Event Viewer allows you to “Use Advanced Event Viewer integrated database” which is a SQLite database automatically created by Advanced Event Viewer or to “Use Microsoft SQL Server”. If you want to use Microsoft SQL Server, you have to insert your server name, authentication type and the user and password. After setting up the SQL Server, you will be asked to migrate the existing data from SQLite to your SQL Server.

![Database Engine Settings](image)

**Adding Servers to Advanced Event Viewer**

When Advanced Event Viewer is started for the first time, it will show you the following dialog:

![Adding Servers to Advanced Event Viewer](image)
These options are also available via the menu bar.

**Add computers by name**

When you click the “Add computers by name” option, you will be presented with the following dialog:

![Add Server Dialog](image)

You can enter the name or IP address of any server in your network. Optionally you can specify to what Server Group you would like to add the servers. Advanced Event Viewer uses the logged on credentials by default, but also allows you to enter alternate credentials. When you click the “Add Server” button, Advanced Event Viewer will contact the server and check if you have the correct permissions and if the server is available. You can enter as many servers as required. When you click the “Close” button, Advanced Event Viewer will ask you if you want to retrieve events immediately, from the servers you added.

Tip: to add the machine where Advanced Event Viewer is installed, simply enter the value “.” and click the “Add Server” button.

**Add computers using the Activate Directory Browser**

When you click the “Add computers from Active Directory”, Advanced Event Viewer will present you with a dialog of all Organizational Units (OU) of your domain contain computer accounts. You can simply select a complete OU, or individual servers to be added to Advanced Event Viewer.
**Analyze server connection**

If a server is offline, or it is listed with an exclamation point, you can always analyze the server connection, using the “Analyze Server Connection” option via the “Servers” menu. This option is checking the server’s host, ping reply, RPC, NetBIOS and sharing, remote desktop service ports, resource and registry access permission and WMI connection.

![Server Connection Analyzer](image)

**Removing servers from Advanced Event Viewer**

To remove servers from Advanced Event Viewer, select the “Managed Servers” tab, right click a server and click the “Remove selected server...” option. All events logs of the removed server will deleted from the Advanced Event Viewer database.
View server information from Advanced Event Viewer

Advanced Event Viewer allows you to verify your servers’ information (e.g. Computer Name, IP Address, Domain, OS Name, OS Version, OS Language, System Type, Processor, Username, TimeZone, Memory, Update and many others). You can do that using the “Server Information” found in the Managed Servers tab or in the “Servers” menu.

Retrieving Windows events logs

Advanced Event Viewer automatically detects the event log books of your servers. By default, Windows machines contain the Application, System and Security event log books. But of for example Domain controllers the “Directory Service” and “DNS Server” event log books are also available. Advanced Event Viewer will automatically show all event log books that are available. Also event log books created by third party programs (for example the “File Replication Service” or “DPM Alerts” event log books).

Manually retrieving events

After you have added at least one machine to Advanced Event Viewer, you can click the “Get Events” button on the “Event Log Books” tab. You can also press F12 to retrieve events.
**Automatic retrieving events**
Advanced Event Viewer also allows you to retrieve events automatically when the program is running. Select the Preferences dialog, click Scheduler and check the “Enable automatic retrieval” checkbox. You can also click the “Automatic Retrieval...” label in the Status Bar (on the bottom of the Advanced Event Viewer screen).

![Preferences dialog for Advanced Event Viewer](image)

**Scheduled event retrieval**
Advanced Event Viewer allows you to schedule event retrieval and reporting. To setup, go to Preferences and select the Scheduler tab. Click the “New” button in the “Saved Reports” frame.

**Viewing Event Log records**
Advanced Event Viewer supports several ways to view the event logs of your servers. By default, a single view is presented of all your servers, grouped by event log book (e.g. Application, System, Security).
Navigating Event Log records

All retrieved events are presented in a grid list, grouped per event log. You can navigate the different event log books via the “Event Log Books” dialog.

To view an individual event log, click the event record on the right side of the screen;

You can also double click on an event record to view the event details dialog;
Use the arrow buttons on the top right of the dialog to navigate events. You can also use the up and down keys on the keyboard.

**Direct link to the Microsoft Knowledge base**
If you require more information regarding a selected event, click the “Look in Microsoft Knowledge Base” for more information. Advanced Event Viewer will automatically open your web browser and start a search in the Microsoft Knowledge Base.

**Direct link to Google**
Advanced Event Viewer can also automatically start a search regarding the selected event using Google by clicking on the “Search on Google” link.

**Direct link to the Event ID database**
To view the information regarding a selected event using the Event ID database, click the “Look in Event ID Database” link.

**Open Remote Desktop**
To connect to the desktop of the selected machine via RDP, click the “Open Remote Desktop” link.

**Open Event Viewer**
A direct link to Microsoft’s build in simplistic event viewer is available via the “Open Event Viewer” link.
Add to filter
Advanced Event Viewer retrieves all events of your servers. By default, only Warning, Error, Audit Failure and Critical events are retrieved and displayed. To filter out any event you do not want to see anymore, click the “Add to filter” link.

To modify the filter, click the “Manage Filters” link in the menu bar.

Wildcards are supported. E.g. Event Source: \*exchange\* Will filter out all events with Exchange in the event source). Event filters are not case sensitive.

Modifying the view
Using the View filter, Advanced Event Viewer allows you to view the events of the selected period;

By default, Advanced Event Viewer will consolidate repeated events. To modify this behavior, uncheck the “Consolidate View” checkbox.

Events that occur repeatedly will be shown once in Advanced Event Viewer by default. The “Occured” column will show you how many times the event occurred.
Consolidation of events is per server. The Event Type, Source, Category, Event ID, etc are used to consolidate events. To also include the Event Description, check the “Include event description” checkbox.

**Quick Filters**

The Quick Filters option allows you to set quick filters on the events list.

Example showing events from user “LOCAL SERVICE”;

**Event Log Types (application, security, etc)**

Advanced Event Viewer automatically detects all event log books available on your servers. To navigate the events, click an event log book on the left side of the screen;
Monitoring disk capacity
Advanced Event Viewer also monitors the disk capacity of your servers. Click on “Server Disk Capacity” to view the available disk capacity of all servers added to Advanced Event Viewer.

You will be presented with the following overview of the available disk capacity of your servers when you double-click on a record, Windows Explorer will be opened to the selected disk.

Email Current Page
This option allows sending an email with the logs that are in current view.
**Export Log option**
Advanced Event Viewer allows you to export the logs for the events in current view or for all events. There are multiple ways to export the logs (PDF Report, HTML Report, TXT Report or CSV Report). You can also choose to “Open report after creation”.

![Export Log Window]

**Folder Tree Size Scanner**
Advanced Event Viewer also includes a build in Tree Size scanner allowing you to see what directories or files are using up disk space on the selected server. To open, click the “Folder Tree Size Scan” button in the menu bar;

![Folder Tree Size Scan]

To scan the selected disk, click the “Scan” button
Using the frame on the right, you will be able to perform actions like deleting the selected file or folder.
Filtering event records
Advanced Event Viewer allows you to filter records. To filter a record, select it and click the “Add to Filter” button.

Mark as Reviewed
You can Mark an event as Reviewed via the “Mark Items as Reviewed” option
Creating reports
Advanced Event Viewer includes a built-in Reports Manager to create and schedule reports of your servers. Use the “Create a New Report” button to start the Report Wizard;

Follow all steps in the wizard. The “Report Format” page, select the output type (PDS, HTML, TXT or CSV) and specify a target for the report (a directory or email address)
The last page of the wizard allows you to schedule the report, or run it now;
Reports Management
After creating a new report, you can always run the report by opening Reports Manager in the “Reports” menu. Select the report you want to run and click the “Run Now” button.
Server and Credential Manager
Advanced Event Viewer includes a “Server and Credential Manager” that allows you to create Server groups and specify the account used to retrieve events;

Alternate credentials can be specified per Server List. This allows you to retrieve events on servers in different domains and workgroups.

Please note that the account used to run Advanced Event Viewer must have the appropriate permission on the local domain to retrieve events. Alternate credentials can be specified for domains and workgroups the current computer is not a member of.