



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies



Learn

Discover ▾

Product documentation ▾

Development languages ▾

Topics ▾



Sign in



# Eventlog Key

Article • 08/19/2021 • 6 contributors

Feedback

The event log contains the following standard logs as well as custom logs:

Expand table

Log	Description
Application	Contains events logged by applications. For example, a database application might record a file error. The application developer decides which events to record.
Security	Contains events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can start auditing to record events in the security log.

<b>System</b>	Contains events logged by system components, such as the failure of a driver or other system component to load during startup.
<i>CustomLog</i>	Contains events logged by applications that create a custom log. Using a custom log enables an application to control the size of the log or attach ACLs for security purposes without affecting other applications.


The event logging service uses the information stored in the **Eventlog** registry key. The **Eventlog** key contains several subkeys, called *logs*. Each log contains information that the event logging service uses to locate resources when an application writes to and reads from the event log.

The structure of the **Eventlog** key is as follows:



Note that domain controllers record events in the **Directory service** and **File Replication service** logs and DNS servers record events in the **DNS server**.

Each log can contain the following registry values.

 Expand table

Registry value	Description
CustomSD	Restricts access to the event log. This value is of type REG

	<div>Clear (0x0004)</div> <div>Read (0x0001)</div> <div>Write (0x0002)</div> <div>To be a syntactically valid SDDL, the CustomSD value must be a valid SDDL string.</div> <div>For more information, see <a href="#">Event Logging Security</a>.</div> <div><b>Windows Server 2003:</b> SACLs are supported.</div> <div><b>Windows XP/2000:</b> This value is not supported.</div>
DisplayNameFile	This value is not used. <b>Windows Server 2003 and Windows XP/2000:</b> This value is not supported.
DisplayNameID	This value is not used. <b>Windows Server 2003 and Windows XP/2000:</b> This value is not supported.
File	<div>Fully qualified path to the file where each event log is stored.</div> <div>If a specific file is set, make sure that the event log service has write access to the file.</div> <div>This value needs to be a valid file name for a file that is located in the system directory.</div> <div>Do not use environment variables, in the path to the file, to refer to the system directory.</div> <div><b>Windows Server 2003 and Windows XP/2000:</b> This value is not supported.</div>
MaxSize	Maximum size, in bytes, of the log file. This value is of type REG_DWORD.
PrimaryModule	This value is not used. <b>Windows Server 2003 and Windows XP/2000:</b> This value is not supported.
Retention	This value is of type REG_DWORD. The default value is 0.
Sources	This value is not used. <b>Windows Server 2003 and Windows XP/2000:</b> This value is not supported.
AutoBackupLogFiles	This value is of type REG_DWORD, and is used by the event log service to determine whether to backup the log files.
RestrictGuestAccess	This value is not used. <b>Windows XP/2000:</b> This value is not supported.
Isolation	<div>Defines the default access permissions for the log. This value is of type REG_SZ.</div> <div><ul style="list-style-type: none"><li>Application</li><li>System</li><li>Custom</li></ul></div> <div>The default isolation is <b>Application</b>. The default permissions are (shown using SDDL):</div> <div><div>L"O:BAG:SYD:"</div><div>L"(A</div></div> <div>The default permissions for <b>System</b> are (shown using SDDL):</div> <div></div>

L"O:BAG:SYD:"L"(A

The default permissions for **Custom** isolation is the same **Windows Server 2003 and Windows XP/2000**: This valu

Each log also contains event sources. For more information, see [Event Sources](#).

## Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#) | [Get help at Microsoft Q&A](#)