

 Filter by title

- Event Logging
- ▾ About Event Logging
- About Event Logging
- Event Types
- Logging Guidelines
- ▾ Event Logging Elements
- Event Logging Elements
- Eventlog Key**
- Event Sources
- Event Categories
- Event Identifiers
- Message Files
- Event Log Records
- Event Data
- Event Logging Operations
- Event Logging Model
- Event Logging Security
- Using Event Logging
- Event Logging Reference

⋮ / [Diagnostics](#) / [Windows Events](#) / [Event Logging](#) /

⊕ ✎ ⋮

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.
System	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:

 Copy

```
HKEY_LOCAL_MACHINE
  SYSTEM
    CurrentControlSet
      Services
        Eventlog
          Application
          Security
          System
          CustomLog
```

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_SZ. The format used is Security Descriptor Definition Language (SDDL) . Clear (0x0004) Read (0x0001) Write (0x0002) To be a syntactically valid SDDL, the CustomSD value must specify an owner and a DACL. For more information, see Event Logging Security . Windows Server 2003: SACLs are supported.

 [Download PDF](#)

	Windows XP/2000: This value is not supported.
DisplayNameFile	This value is not used. Windows Server 2003 and Windows XP/2000: Name of the file that contains the event log.
DisplayNameID	This value is not used. Windows Server 2003 and Windows XP/2000: Message identifier.
File	Fully qualified path to the file where each event log is stored. This enables Event Viewer to find the log file. If a specific file is set, make sure that the event log service has full permissions on the file. This value needs to be a valid file name for a file that is located on a local directory. Do not use environment variables, in the path to the file, that cannot be expanded. Windows Server 2003 and Windows XP/2000: This value defaults to %SystemRoot%\System32\eventlog\%SourceName%.log.
MaxSize	Maximum size, in bytes, of the log file. This value is of type REG_DWORD. The value must be greater than 0.
PrimaryModule	This value is not used.Windows Server 2003 and Windows XP/2000: This value is the name of the module that generated the event.
Retention	This value is of type REG_DWORD. The default value is 0. If this value is 0, the record is deleted when the log file is full. If this value is non-zero, the record is retained for the specified number of days.
Sources	This value is not used. Windows Server 2003 and Windows XP/2000: Names of the event sources that are associated with the log.
AutoBackupLogFiles	This value is of type REG_DWORD, and is used by the event log service to determine whether to backup the log file when it is full.
RestrictGuestAccess	This value is not used. Windows XP/2000: This value is of type REG_DWORD, and is used to restrict guest access to the log.
Isolation	<div>Defines the default access permissions for the log. This value is of type REG_SZ. You can specify one of the following values:</div> <ul style="list-style-type: none">ApplicationSystemCustom <div>The default isolation is Application. The default permissions for Application are (shown using SDDL):</div> <div><div>L"O:BAG:SYD:"</div><div>L"(A;;;0xf0007;;;SY)"</div></div> <div>The default permissions for System are (shown using SDDL):</div> <div><div>L"O:BAG:SYD:"</div><div>L"(A;;;0xf0007;;;SY)"</div></div> <div>The default permissions for Custom isolation is the same as Application.</div> <div>Windows Server 2003 and Windows XP/2000: This value is not available.</div>

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](#)

Additional resources

Training

Module
[Manage and monitor Windows Server event logs - Training](#)

Learn how Event Viewer provides a convenient and accessible location for you to observe events that occur. Access event information quickly and conveniently. Learn how to interpret the data in the event log.

Events

Nov 20, 12 AM - Nov 22, 12 AM

Gain the competitive edge you need with powerful AI and Cloud solutions by attending Microsoft Ignite online.
[Register now](#)