


 Filter by title

Overview
EVT_CHANNEL_CLOCK_TYPE enumeration
EVT_CHANNEL_CONFIG_PROPERTY_ID enumeration
EVT_CHANNEL_ISOLATION_TYPE enumeration
EVT_CHANNEL_REFERENCE_FLAGS enumeration
EVT_CHANNEL_SID_TYPE enumeration
EVT_CHANNEL_TYPE enumeration
EVT_EVENT_METADATA_PROPERTY_ID enumeration
EVT_EVENT_PROPERTY_ID enumeration
EVT_EXPORTLOG_FLAGS enumeration
EVT_FORMAT_MESSAGE_FLAGS enumeration
EVT_LOG_PROPERTY_ID enumeration
EVT_LOGIN_CLASS enumeration
EVT_OPEN_LOG_FLAGS enumeration
EVT_PUBLISHER_METADATA_PROPERTY_ID enumeration
EVT_QUERY_FLAGS enumeration
EVT_QUERY_PROPERTY_ID enumeration
EVT_RENDER_CONTEXT_FLAGS enumeration
EVT_RENDER_FLAGS enumeration
EVT_RPC_LOGIN structure
EVT_RPC_LOGIN_FLAGS enumeration
EVT_SEEK_FLAGS enumeration
EVT_SUBSCRIBE_CALLBACK callback function
EVT_SUBSCRIBE_FLAGS enumeration
EVT_SUBSCRIBE_NOTIFY_ACTION enumeration
EVT_SYSTEM_PROPERTY_ID enumeration
EVT_VARIANT structure
EVT_VARIANT_TYPE enumeration
EvtArchiveExportedLog function
EvtCancel function
EvtClearLog function
 Download PDF

winevt.h header

Article • 01/24/2023

 [Feedback](#)

In this article

- [Functions](#)
- [Callback functions](#)
- [Structures](#)
- [Enumerations](#)

This header is used by Windows Event Log. For more information, see:

- [Windows Event Log](#)

winevt.h contains the following programming interfaces:

Functions


 **Expand table**

EvtArchiveExportedLog
Adds localized strings to the events in the specified log file.
EvtCancel
Cancels all pending operations on a handle.
EvtClearLog
Removes all events from the specified channel and writes them to the target log file.
EvtClose
Closes an open handle.
EvtCreateBookmark
Creates a bookmark that identifies an event in a channel.
EvtCreateRenderContext
Creates a context that specifies the information in the event that you want to render.
EvtExportLog
Copies events from the specified channel or log file and writes them to the target log file.
EvtFormatMessage
Formats a message string. (EvtFormatMessage)
EvtGetChannelConfigProperty
Gets the specified channel configuration property.

EvtGetEventInfo
Gets information that identifies the structured XML query that selected the event and the channel or log file that contained the event.
EvtGetEventMetadataProperty
Gets the specified event metadata property.
EvtGetExtendedStatus
Gets a text message that contains the extended error information for the current error.
EvtGetLogInfo
Gets information about a channel or log file.
EvtGetObjectArrayProperty
Gets a provider metadata property from the specified object in the array.
EvtGetObjectArraySize
Gets the number of elements in the array of objects.
EvtGetPublisherMetadataProperty
Gets the specified provider metadata property.
EvtGetQueryInfo
Gets information about a query that you ran that identifies the list of channels or log files that the query attempted to access. The function also gets a list of return codes that indicates the success or failure of each access.
EvtNext
Gets the next event from the query or subscription results.
EvtNextChannelPath
Gets a channel name from the enumerator.
EvtNextEventMetadata
Gets an event definition from the enumerator.
EvtNextPublisherId
Gets the identifier of a provider from the enumerator.
EvtOpenChannelConfig
Gets a handle that you use to read or modify a channel's configuration property.
EvtOpenChannelEnum
Gets a handle that you use to enumerate the list of channels that are registered on the computer.
EvtOpenEventMetadataEnum
Gets a handle that you use to enumerate the list of events that the provider defines.
EvtOpenLog
Gets a handle to a channel or log file that you can then use to get information about the channel or log file.
EvtOpenPublisherEnum
Gets a handle that you use to enumerate the list of registered providers on the computer.


EvtOpenPublisherMetadata
Gets a handle that you use to read the specified provider's metadata.
EvtOpenSession
Establishes a connection to a remote computer that you can use when calling the other Windows Event Log functions.
EvtQuery
Runs a query to retrieve events from a channel or log file that match the specified query criteria.
EvtRender
Renders an XML fragment based on the rendering context that you specify.
EvtSaveChannelConfig
Saves the changes made to a channel's configuration.
EvtSeek
Seeks to a specific event in a query result set.
EvtSetChannelConfigProperty
Sets the specified configuration property of a channel.
EvtSubscribe
Creates a subscription that will receive current and future events from a channel or log file that match the specified query criteria.
EvtUpdateBookmark
Updates the bookmark with information that identifies the specified event.

Callback functions

 Expand table

EVT_SUBSCRIBE_CALLBACK
Implement this callback if you call the EvtSubscribe function to receive events that match your query.

Structures

 Expand table

EVT_RPC_LOGIN
Contains the information used to connect to a remote computer.
EVT_VARIANT
Contains event data or property values.

Enumerations

 Expand table

EVT_CHANNEL_CLOCK_TYPE
Defines the values that specify the type of time stamp to use when logging events channel.
EVT_CHANNEL_CONFIG_PROPERTY_ID
Defines the identifiers that identify the configuration properties of a channel.
EVT_CHANNEL_ISOLATION_TYPE
Defines the default access permissions to apply to the channel.
EVT_CHANNEL_REFERENCE_FLAGS
Defines the values that specify how a channel is referenced.
EVT_CHANNEL_SID_TYPE
Defines the values that determine whether the event includes the security identifier (SID) of the principal that logged the event.
EVT_CHANNEL_TYPE
Defines the type of a channel.
EVT_EVENT_METADATA_PROPERTY_ID
Defines the identifiers that identify the metadata properties of an event definition.
EVT_EVENT_PROPERTY_ID
Defines the values that determine the query information to retrieve.
EVT_EXPORTLOG_FLAGS
Defines values that indicate whether the events come from a channel or log file.
EVT_FORMAT_MESSAGE_FLAGS
Defines the values that specify the message string from the event to format.
EVT_LOG_PROPERTY_ID
Defines the identifiers that identify the log file metadata properties of a channel or log file.
EVT_LOGIN_CLASS
Defines the types of connection methods you can use to connect to the remote computer.
EVT_OPEN_LOG_FLAGS
Defines the values that specify whether to open a channel or exported log file.
EVT_PUBLISHER_METADATA_PROPERTY_ID
Defines the identifiers that identify the metadata properties of a provider.
EVT_QUERY_FLAGS
Defines the values that specify how to return the query results and whether you are query against a channel or log file.
EVT_QUERY_PROPERTY_ID
Defines the identifiers that identify the query information that you can retrieve.
EVT_RENDER_CONTEXT_FLAGS
Defines the values that specify the type of information to access from the event.

EVT_RENDER_FLAGS
Defines the values that specify what to render.
EVT_RPC_LOGIN_FLAGS
Defines the types of authentication that you can use to authenticate the user when connecting to a remote computer.
EVT_SEEK_FLAGS
Defines the relative position in the result set from which to seek.
EVT_SUBSCRIBE_FLAGS
Defines the possible values that specify when to start subscribing to events.
EVT_SUBSCRIBE_NOTIFY_ACTION
Defines the possible types of data that the subscription service can deliver to your callback.
EVT_SYSTEM_PROPERTY_ID
Defines the identifiers that identify the system-specific properties of an event.
EVT_VARIANT_TYPE
Defines the possible data types of a variant data item.

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](#)