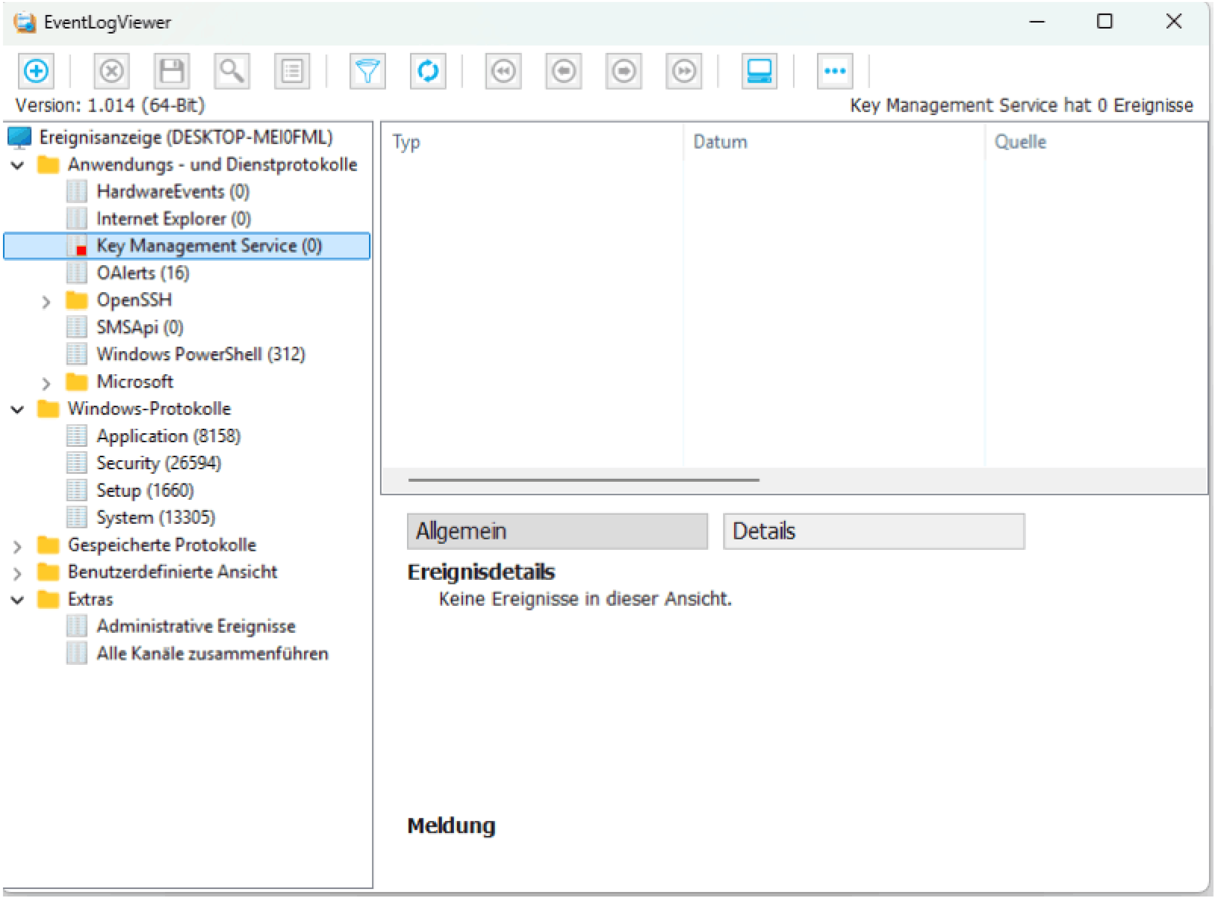

Key Management Service hat 0 Ereignisse

Keine Ereignisse in dieser Ansicht.

EventLogViewer - Help file

Use the EventLogViewer to filter and find details about each log

To assist in troubleshooting, EventLogViewer displays event logs with system and application messages that contain errors, warnings, and information about specific events that administrators can analyze to take necessary actions.

EventLogViewer Structure

The EventLogViewer consists of **five different sections**:
1) Application and Service Logs - This section contains many options such as Hardware Events, Key Management Service, OpenSSH and Windows PowerShell...
2) Windows Logs - contains Application, Security, Setup and System subsections.
3) Saved Logs - used to open saved logs.
4) Custom View - used to create custom views with different filters
5) Tools - View Administrative Events and Merge All Channels

EventLogViewer Levels and Definitions

There are **four main levels** that the Event Viewer displays at different times: Critical Error, Error, Warning and Information.

Use the EventLogViewer to filter and find details about any log

Find all possible details of all logged items. Specify the type of information to be recorded in the event logs. The information can include: Event Types, Event Types, Category, Event ID, User, Computer, Events for different times/dates, Text in Description, Text in XML View...

Finding Events
Search for events with a **super fast search algorithm**. Search **supports case sensitive, whole string match, wilcard and regex**!
Windows Event Logs tell you the order and type of events that led to a particular condition or situation.
Windows Event Logs include:
System Event Log
Security Event Log
Application Event Log
Directory Service
File Replication Service

Instructions:

Changing Event Viewer Settings
Adjust Event Viewer settings by right-clicking the log and clicking Properties.
The following Event Log settings can be adjusted:
Maximum log size
Overwrite events as needed
Overwrite events older than x days
Never overwrite events (manually clear log)
Using a low-speed connection (Windows)
To change Event Viewer settings
Right-click the appropriate log file (Application, Security, System, Directory Service, or File Replication Service).
Click Properties.

Exporting Event Logs
Event logs can be saved for future reference or for historical data. Event log files can be saved as event files (*.evt), text files (*.txt), or comma-delimited text files (*.txt).
To save event logs
Right-click the appropriate log file (Application, Security, System, Directory Service, or File Replication Service).
Click Export log file as.
Enter a name for the file and click Save.

Clearing Event Logs
Clear event logs by selecting Clear All Events from the Action menu after selecting the appropriate log file. You have the option to save the event log before clearing it.
To clear event logs
Select the appropriate log file (Application, Security, System, Directory Service, or File Replication Service).
Right-click the appropriate log file.
Click Clear Log

Selecting Computers

Select any computer on your network to view its event logs in Event Viewer.
To select computers in Event Viewer
Click the Computer Selection icon
Select Connect to another computer.
Enter the computer name on which you want to view event logs, and click OK.

Filtering Events
Specify the type of information you want to record in the event logs. The information can include:
Events for different times/dates
Event types
Event source
Category
Event ID
Text in description
Text in XML view
User
Computer
To filter events
Right-click the appropriate log file (Application, Security, System, Directory Service, or File Replication Service).
Click Filter the log file.
Enter the appropriate information you want to filter, then click Apply.

Finding events
The search supports **case sensitivity, whole string matching, Wilcard and RegEx** support!
In the search mask, specify which event type to find:
Event type
Source
Category
Event ID
Computer
User
Description
To find events
Select the appropriate log file (Application, Security, System, Directory Service, or File Replication Service).
Right-click the appropriate log file.
Click Find.
Click Cancel when you are finished.

Supported RegEx operators for searching
. Period, matches any single character except a newline.
^ Caret, matches the beginning of the line or string the regular expression is searching.
$ Dollar, matches the end of the line or string the regular expression is searching.
* Asterisk, matches zero or more + Plus, matches one or more
? Question, matches zero or any of the preceding characters.
{n} Matches the preceding expression exactly n times.
{n,} Matches n or more times
{n,m} Matches the preceding expression at least n times and at most m times.

[abc] Matches any of a, b, and c.
[^abc] A caret ^ at the beginning of the square bracket means "not," in which case it matches anything except a, b, or c.
[a-zA-Z] Character ranges, the character set of the ranges { a-z | A-Z }
\s Matches a space, \t \f \r \n \v and spaces
\S Matches a non-space character.
\w Matches an alphanumeric character., [a-zA-Z0-9_]
\W Matches a non-alphanumeric character.
\d Matches a digit [0-9].
\D Matches a non-digit.
| OR operator (|): For example, the regular expression four|4 accepts the strings "four" or "4".