AceHash

Archived: 2026-04-05 18:01:46 UTC

1 Microsoft-Windows-Sysmon/Operational 1 Process Create (rule: ProcessCreate) Process Create.

- LogonGuid/LogonId: ID of the logon session
- ParentProcessGuid/ParentProcessId: Process ID of the parent process
- ParentImage: Executable file of the parent process
- CurrentDirectory: Work directory (directory of the tool)
- CommandLine: Command line of the execution command ([Executable File Name of Tool] -l)
- IntegrityLevel: Privilege level
- ParentCommandLine: Command line of the parent process
- UtcTime: Process execution date and time (UTC)
- ProcessGuid/ProcessId: Process ID
- User: Execute as user
- Hashes: Hash value of the executable file
- Image: Path to the executable file (path to the tool)

Security 4688 Process Create A new process has been created.

- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Log Date and Time: Process execution date and time (local time)
- Process Information > New Process Name: Path to the executable file (path to the tool)
- Process Information > Token Escalation Type: Presence of privilege escalation (2)
- Process Information > New Process ID: Process ID (hexadecimal)
- Process Information > Source Process ID: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7
- Subject > Logon ID: Session ID of the user who executed the process

2 Microsoft-Windows-Sysmon/Operational 10 Process accessed (rule: ProcessAccess) Process accessed.

- SourceProcessGUID/SourceProcessId/SourceThreadId: Process of the access source process/Thread ID
- TargetProcessGUID/TargetProcessId: Process ID of the access destination process
- GrantedAccess: Details of the granted access (0x1FFFFF)
- SourceImage: Path to the access source process (path to the tool)
- TargetImage: Path to the access destination process (C:\Windows\system32\lsass.exe)

Microsoft-Windows-Sysmon/Operational 8 CreateRemoteThread detected (rule: CreateRemoteThread) CreateRemoteThread detected.

- NewThreadId: Thread ID of the new thread

- TargetProcessGuid/TargetProcessId: Process ID of the destination process
- TargetImage: Path to the destination process (C:\Windows\system32\lsass.exe)
- UtcTime: Execution date and time (UTC)
- SourceImage: Path to the source process (path to the tool)
- SourceProcessGuid/SourceProcessId: Process ID of the source process

3 Microsoft-Windows-Sysmon/Operational 5 Process terminated (rule: ProcessTerminate) Process terminated.

- UtcTime: Process terminated date and time (UTC)
- ProcessGuid/ProcessId: Process ID
- Image: Path to the executable file (path to the tool)

Security 4689 Process Termination A process has exited.

- Process Information > Process ID: Process ID (hexadecimal)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Process Information > Exit Status: Process return value (0x1)
- Log Date and Time: Process terminated date and time (local time)
- Process Information > Process Name: Path to the executable file (path to the tool)
- Subject > Logon ID: Session ID of the user who executed the process

4 Microsoft-Windows-Sysmon/Operational 11 File created (rule: FileCreate) File created.

- Image: Path to the executable file (C:\Windows\System32\svchost.exe)
- ProcessGuid/ProcessId: Process ID
- TargetFilename: Created file (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf)
- CreationUtcTime: File creation date and time (UTC)

Security 4656 File System/Other Object Access Events A handle to an object was requested.

- Process Information > Process ID: Process ID (hexadecimal)
- Access Request Information > Access/Reason for Access/Access Mask: Requested privileges (WriteData or AddFile, AppendData)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Object > Object Name: Target file name (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf)
- Process Information > Process Name: Name of the process that closed the handle (C:\Windows\System32\svchost.exe)
- Object > Object Type: Type of the file (File)
- Subject > Logon ID: Session ID of the user who executed the process
- Object > Handle ID: ID of the relevant handle

Security 4663 File System An attempt was made to access an object.

- Process Information > Process ID: Process ID (hexadecimal)
- Access Request Information > Access/Reason for Access/Access Mask: Requested privileges (WriteData or AddFile, AppendData)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Object > Object Name: Target file name (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf)
- Audit Success: Success or failure (access successful)
- Process Information > Process Name: Name of the process that closed the handle (C:\Windows\System32\svchost.exe)
- Object > Object Type: Category of the target (File)
- Subject > Logon ID: Session ID of the user who executed the process
- Object > Handle ID: ID of the relevant handle (handle obtained with Event ID 4656)

Security 4658 File System The handle to an object was closed.

- Process Information > Process ID: Process ID (hexadecimal)
- Process Information > Process Name: Name of the process that requested the object (C:\Windows\System32\svchost.exe)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Subject > Logon ID: Session ID of the user who executed the process
- Object > Handle ID: ID of the relevant handle (handle obtained with Event ID 4656)

5 Microsoft-Windows-Sysmon/Operational 1 Process Create (rule: ProcessCreate) Process Create.

- LogonGuid/LogonId: ID of the logon session
- ParentProcessGuid/ParentProcessId: Process ID of the parent process
- ParentImage: Executable file of the parent process
- CurrentDirectory: Work directory
- CommandLine: Command line of the execution command ([Executable File Name] -s [User Name]:[Domain Name]:[Hash] "[Execution Command]")
- IntegrityLevel: Privilege level (High)
- ParentCommandLine: Command line of the parent process
- UtcTime: Process execution date and time (UTC)
- ProcessGuid/ProcessId: Process ID
- User: Execute as user
- Hashes: Hash value of the executable file
- Image: Path to the executable file (path to the executable file)

Security 4688 Process Create A new process has been created.

- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool

- Log Date and Time: Process execution date and time (local time)
- Process Information > New Process Name: Path to the executable file (path to the tool)
- Process Information > Token Escalation Type: Presence of privilege escalation (2)
- Process Information > New Process ID: Process ID (hexadecimal)
- Process Information > Source Process ID: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7
- Subject > Logon ID: Session ID of the user who executed the process

6 Microsoft-Windows-Sysmon/Operational 1 Process Create (rule: ProcessCreate) Process Create.

- LogonGuid/LogonId: ID of the logon session
- ParentProcessGuid/ParentProcessId: Process ID of the parent process
- ParentImage: Executable file of the parent process (path to the tool)
- CurrentDirectory: Work directory (C:\Windows\system32\)
- CommandLine: Command line of the execution command (cmd.exe)
- IntegrityLevel: Privilege level (High)
- ParentCommandLine: Command line of the parent process ([Executable File Name of Tool] -s [User Name]:[Password]:[Hash] "[Execution Command]")
- UtcTime: Process execution date and time (UTC)
- ProcessGuid/ProcessId: Process ID
- User: Execute as user
- Hashes: Hash value of the executable file
- Image: Path to the executable file (C:\Windows\System32\cmd.exe)

Security 4688 Process Create A new process has been created.

- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Log Date and Time: Process execution date and time (local time)
- Process Information > New Process Name: Path to the executable file (C:\Windows\System32\cmd.exe)
- Process Information > Token Escalation Type: Presence of privilege escalation (1)
- Process Information > New Process ID: Process ID (hexadecimal)
- Process Information > Source Process ID: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7
- Subject > Logon ID: Session ID of the user who executed the process

7 Microsoft-Windows-Sysmon/Operational 10 Process accessed (rule: ProcessAccess) Process accessed.

- SourceProcessGUID/SourceProcessId/SourceThreadId: Process of the access source process/Thread ID
- TargetProcessGUID/TargetProcessId: Process ID of the access destination process
- GrantedAccess: Details of the granted access (0x1FFFFF)
- SourceImage: Path to the access source process (path to the executable file)
- TargetImage: Path to the access destination process (C:\Windows\system32\lsass.exe)

Microsoft-Windows-Sysmon/Operational 8 CreateRemoteThread detected (rule: CreateRemoteThread) CreateRemoteThread detected.

- NewThreadId: Thread ID of the new thread
- TargetProcessGuid/TargetProcessId: Process ID of the destination process
- TargetImage: Path to the destination process (C:\Windows\system32\lsass.exe)
- UtcTime: Execution date and time (UTC)
- SourceImage: Path to the source process (path to the executable file)
- SourceProcessGuid/SourceProcessId: Process ID of the source process

8 Microsoft-Windows-Sysmon/Operational 3 Network connection detected (rule: NetworkConnect) Network connection detected.

- Protocol: Protocol (tcp)
- DestinationIp: Destination IP address (Domain Controller IP address)
- Image: Path to the executable file (System)
- DestinationHostname: Destination host name (Domain Controller host name)
- ProcessGuid/ProcessId: Process ID (4)
- User: Execute as user (NT AUTHORITY\SYSTEM)
- DestinationPort: Destination port number (445)
- SourcePort: Source port number (high port)
- SourceHostname: Source host name (source host)
- SourceIp: Source IP address (source host IP address)

Security 5156 Filtering Platform Connection The Windows Filtering Platform has allowed a connection.

- Network Information > Destination Port: Destination port number (445)
- Network Information > Source Port: Source port number (high port)
- Network Information > Destination Address: Destination IP address (Domain Controller)
- Network Information > Protocol: Protocol used (6=TCP)
- Application Information > Application Name: Execution process (System)
- Network Information > Direction: Communication direction (outbound)
- Network Information > Source Address: Source IP address (source host)
- Application Information > Process ID: Process ID (4)

9 Microsoft-Windows-Sysmon/Operational 5 Process terminated (rule: ProcessTerminate) Process terminated.

- UtcTime: Process terminated date and time (UTC)
- ProcessGuid/ProcessId: Process ID
- Image: Path to the executable file (C:\Windows\System32\cmd.exe)

Security 4689 Process Termination A process has exited.

- Process Information > Process ID: Process ID (hexadecimal)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool

- Process Information > Exit Status: Process return value (0x0)
- Log Date and Time: Process terminated date and time (local time)
- Process Information > Process Name: Path to the executable file (C:\Windows\System32\cmd.exe)
- Subject > Logon ID: Session ID of the user who executed the process

10 Microsoft-Windows-Sysmon/Operational 5 Process terminated (rule: ProcessTerminate) Process terminated.

- UtcTime: Process terminated date and time (UTC)
- ProcessGuid/ProcessId: Process ID
- Image: Path to the executable file (execution path to the tool)

Security 4689 Process Termination A process has exited.

- Process Information > Process ID: Process ID (hexadecimal)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Process Information > Exit Status: Process return value (0xFFFFFFFF)
- Log Date and Time: Process terminated date and time (local time)
- Process Information > Process Name: Path to the executable file (execution path to the tool)
- Subject > Logon ID: Session ID of the user who executed the process

11 Security 4656 File System/Other Object Access Events A handle to an object was requested.

- Process Information > Process ID: Process ID (hexadecimal)
- Access Request Information > Access/Reason for Access/Access Mask: Requested privileges (WriteData or AddFile, AppendData)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Object > Object Name: Target file name (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf)
- Process Information > Process Name: Name of the process that closed the handle (C:\Windows\System32\svchost.exe)
- Object > Object Type: Type of the file (File)
- Subject > Logon ID: Session ID of the user who executed the process
- Object > Handle ID: ID of the relevant handle

Security 4663 File System An attempt was made to access an object.

- Process Information > Process ID: Process ID (hexadecimal)
- Access Request Information > Access/Reason for Access/Access Mask: Requested privileges (WriteData or AddFile, AppendData)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Object > Object Name: Target file name (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf)

- Audit Success: Success or failure (access successful)
- Process Information > Process Name: Name of the process that closed the handle (C:\Windows\System32\svchost.exe)
- Object > Object Type: Category of the target (File)
- Subject > Logon ID: Session ID of the user who executed the process
- Object > Handle ID: ID of the relevant handle (handle obtained with Event ID 4656)

Security 4658 File System The handle to an object was closed.

- Process Information > Process ID: Process ID (hexadecimal)
- Process Information > Process Name: Name of the process that requested the object (C:\Windows\System32\svchost.exe)
- Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the tool
- Subject > Logon ID: Session ID of the user who executed the process
- Object > Handle ID: ID of the relevant handle (handle obtained with Event ID 4656)
