Event ID	**Detailed Message**	**Minimum Operating System Requirement**
4608	Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.	Windows Vista, Windows Server 2008
4609	Windows is shutting down. All logon sessions will be terminated by this shutdown.	Windows Vista, Windows Server 2008
4610	An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts. Authentication Package Name: %1	Windows Vista, Windows Server 2008
4611	This logon process will be trusted to submit logon requests. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Process Name: %5	Windows Vista, Windows Server 2008
4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. Number of audit messages discarded: %1 This event is generated when audit queues are filled and events must be discarded. This most commonly occurs when security events are being generated faster than they are being written to disk, or when the auditing system loses connectivity to the event log, such as when the event log service is stopped.	Windows Vista, Windows Server 2008
4614	A notification package has been loaded by the Security Account Manager. This package will be notified of any account or password changes. Notification Package Name: %1	Windows Vista, Windows Server 2008
4615	Invalid use of LPC port. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: PID: %7 Name: %8 Invalid Use: %5 LPC Server Port Name: %6 Windows Local Security Authority (LSA) communicates with the Windows kernel using Local Procedure Call (LPC) ports. If you see this event, an application has inadvertently or intentionally accessed this port which is reserved exclusively for LSA's use. The application (process) should be investigated to ensure that it is not attempting to tamper with this communications channel.	Windows Vista, Windows Server 2008

4616	The system time was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: Process ID: %9 Name: %10 Previous Time: %6 %5 New Time: %8 %7 This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer. Note: Process Information audit data is available only on computers running Windows Server 2008 R2 or Windows 7.	Windows Vista, Windows Server 2008
4616	The system time was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: Process ID: %9 Name: %10 Previous Time: %6 %5 New Time: %8 %7 This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer. Note: Process Information audit data is available only on computers running Windows Server 2008 R2 or Windows 7.	Windows 7, Windows Server 2008 R2
4618	A monitored security event pattern has occurred. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Alert Information: Computer: %2 Event ID: %1 Number of Events: %7 Duration: %8 This event is generated when Windows is configured to generate alerts in accordance with the Common Criteria Security Audit Analysis requirements (FAU_SAA) and an auditable event pattern occurs.	Windows Vista, Windows Server 2008

4621	Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded. Value of CrashOnAuditFail: %1 This event is logged after a system reboots following CrashOnAuditFail.	Windows Vista, Windows Server 2008
4622	A security package has been loaded by the Local Security Authority. Security Package Name: %1	Windows Vista, Windows Server 2008
4624	An account was successfully logged on. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Type: %9 New Logon: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Logon GUID: %13 Process Information: Process ID: %17 Process Name: %18 Network Information: Workstation Name: %12 Source Network Address: %19 Source Port: %20 Detailed Authentication Information: Logon Process: %10 Authentication Package: %11 Transited Services: %14 Package Name (NTLM only): %15 Key Length: %16 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most	Windows Vista, Windows Server 2008

4624	An account was successfully logged on. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Type: %9 Impersonation Level: %21 New Logon: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Logon GUID: %13 Process Information: Process ID: %17 Process Name: %18 Network Information: Workstation Name: %12 Source Network Address: %19 Source Port: %20 Detailed Authentication Information: Logon Process: %10 Authentication Package: %11 Transited Services: %14 Package Name (NTLM only): %15 Key Length: %16 This event is generated when a logon session is created. It is generated on the computer that was accessed.	Windows 8, Windows Server 2012

4624	An account was successfully logged on. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Information: Logon Type: %9 Restricted Admin Mode: %22 Virtual Account: %25 Elevated Token: %27 Impersonation Level: %21 New Logon: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Linked Logon ID: %26 Network Account Name: %23 Network Account Domain: %24 Logon GUID: %13 Process Information: Process ID: %17 Process Name: %18 Network Information: Workstation Name: %12 Source Network Address: %19 Source Port: %20 Detailed Authentication Information: Logon Process: %10 Authentication Package: %11 Transited Services: %14	Windows 10

4625	An account failed to log on. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Type: %11 Account For Which Logon Failed: Security ID: %5 Account Name: %6 Account Domain: %7 Failure Information: Failure Reason: %9 Status: %8 Sub Status: %10 Process Information: Caller Process ID: %18 Caller Process Name: %19 Network Information: Workstation Name: %14 Source Network Address: %20 Source Port: %21 Detailed Authentication Information: Logon Process: %12 Authentication Package: %13 Transited Services: %15 Package Name (NTLM only): %16 Key Length: %17 This event is generated when a logon request fails. It is generated on the computer where access was attempted.	Windows Vista, Windows Server 2008

4626	User / Device claims information Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Type: %9 New Logon: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Event in sequence: %10 of %11 User Claims: %12 Device Claims: %13 The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit User/Device claims subcategory is configured and the user's logon token contains user/device claims information. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.	Windows 8, Windows Server 2012

4627	Group membership information. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Type: %9 New Logon: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Event in sequence: %10 of %11 Group Membership: %12 The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.	Windows 10
4634	An account was logged off. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Type: %5 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.	Windows Vista, Windows Server 2008
4646	%1	Windows Vista, Windows Server 2008
4647	User initiated logoff: Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 This event is generated when a logoff is initiated but the token reference count is not zero and the logon session cannot be destroyed. No further user-initiated activity can occur. This event can be interpreted as a logoff event.	Windows Vista, Windows Server 2008

4648	A logon was attempted using explicit credentials. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon GUID: %5 Account Whose Credentials Were Used: Account Name: %6 Account Domain: %7 Logon GUID: %8 Target Server: Target Server Name: %9 Additional Information: %10 Process Information: Process ID: %11 Process Name: %12 Network Information: Network Address: %13 Port: %14 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.	Windows Vista, Windows Server 2008
4649	A replay attack was detected. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Credentials Which Were Replayed: Account Name: %5 Account Domain: %6 Process Information: Process ID: %12 Process Name: %13 Network Information: Workstation Name: %10 Detailed Authentication Information: Request Type: %7 Logon Process: %8 Authentication Package: %9 Transited Services: %11 This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration.	Windows Vista, Windows Server 2008

4650	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used. Local Endpoint: Principal Name: %1 Network Address: %3 Keying Module Port: %4 Remote Endpoint: Principal Name: %2 Network Address: %5 Keying Module Port: %6 Security Association Information: Lifetime (minutes): %12 Quick Mode Limit: %13 Main Mode SA ID: %17 Cryptographic Information: Cipher Algorithm: %9 Integrity Algorithm: %10 Diffie-Hellman Group: %11 Additional Information: Keying Module Name: %7 Authentication Method: %8 Role: %14 Impersonation State: %15 Main Mode Filter ID: %16	Windows Vista, Windows Server 2008
4651	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication. Local Endpoint: Principal Name: %1 Network Address: %9 Keying Module Port: %10 Local Certificate: SHA Thumbprint: %2 Issuing CA: %3 Root CA: %4 Remote Endpoint: Principal Name: %5 Network Address: %11 Keying Module Port: %12 Remote Certificate: SHA thumbprint: %6 Issuing CA: %7 Root CA: %8 Cryptographic Information: Cipher Algorithm: %15 Integrity Algorithm: %16 Diffie-Hellman Group: %17 Security Association Information: Lifetime (minutes): %18 Quick Mode Limit: %19 Main Mode SA ID: %23 Additional Information: Keying Module Name: %13 Authentication Method: %14 Role: %20 Impersonation State: %21 Main Mode Filter ID: %22	Windows Vista, Windows Server 2008

4652	An IPsec Main Mode negotiation failed. Local Endpoint: Principal Name: %1 Network Address: %9 Keying Module Port: %10 Local Certificate: SHA Thumbprint: %2 Issuing CA: %3 Root CA: %4 Remote Endpoint: Principal Name: %5 Network Address: %11 Keying Module Port: %12 Remote Certificate: SHA thumbprint: %6 Issuing CA: %7 Root CA: %8 Additional Information: Keying Module Name: %13 Authentication Method: %16 Role: %18 Impersonation State: %19 Main Mode Filter ID: %20 Failure Information: Failure Point: %14 Failure Reason: %15 State: %17 Initiator Cookie: %21 Responder Cookie: %22	Windows Vista, Windows Server 2008
4653	An IPsec Main Mode negotiation failed. Local Endpoint: Local Principal Name: %1 Network Address: %3 Keying Module Port: %4 Remote Endpoint: Principal Name: %2 Network Address: %5 Keying Module Port: %6 Additional Information: Keying Module Name: %7 Authentication Method: %10 Role: %12 Impersonation State: %13 Main Mode Filter ID: %14 Failure Information: Failure Point: %8 Failure Reason: %9 State: %11 Initiator Cookie: %15 Responder Cookie: %16	Windows Vista, Windows Server 2008

4654	An IPsec Quick Mode negotiation failed. Local Endpoint: Network Address: %1 Network Address mask: %2 Port: %3 Tunnel Endpoint: %4 Remote Endpoint: Network Address: %5 Address Mask: %6 Port: %7 Tunnel Endpoint: %8 Private Address: %10 Additional Information: Protocol: %9 Keying Module Name: %11 Virtual Interface Tunnel ID: %20 Traffic Selector ID: %21 Mode: %14 Role: %16 Quick Mode Filter ID: %18 Main Mode SA ID: %19 Failure Information: State: %15 Message ID: %17 Failure Point: %12 Failure Reason: %13 Note: Virtual Interface Tunnel ID and Traffic Selector ID data is available only on computers running Windows Server 2008 R2 or Windows 7.	Windows Vista, Windows Server 2008
4654	An IPsec quick mode negotiation failed. Local Endpoint: Network Address: %1 Network Address mask: %2 Port: %3 Tunnel Endpoint: %4 Remote Endpoint: Network Address: %5 Address Mask: %6 Port: %7 Tunnel Endpoint: %8 Private Address: %10 Additional Information: Protocol: %9 Keying Module Name: %11 Virtual Interface Tunnel ID: %20 Traffic Selector ID: %21 Mode: %14 Role: %16 Quick Mode Filter ID: %18 Main Mode SA ID: %19 Failure Information: State: %15 Message ID: %17 Failure Point: %12 Failure Reason: %13	Windows 7, Windows Server 2008 R2

4655	An IPsec Main Mode security association ended. Local Network Address: %1 Remote Network Address: %2 Keying Module Name: %3 Main Mode SA ID: %4	Windows Vista, Windows Server 2008
4656	A handle to an object was requested. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %14 Process Name: %15 Access Request Information: Transaction ID: %9 Accesses: %10 Access Mask: %11 Privileges Used for Access Check: %12 Restricted SID Count: %13	Windows Vista, Windows Server 2008
4656	A handle to an object was requested. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Resource Attributes: %17 Process Information: Process ID: %15 Process Name: %16 Access Request Information: Transaction ID: %9 Accesses: %10 Access Reasons: %11 Access Mask: %12 Privileges Used for Access Check: %13 Restricted SID Count: %14	Windows 7, Windows Server 2008 R2

4657	A registry value was modified. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Name: %5 Object Value Name: %6 Handle ID: %7 Operation Type: %8 Process Information: Process ID: %13 Process Name: %14 Change Information: Old Value Type: %9 Old Value: %10 New Value Type: %11 New Value: %12	Windows Vista, Windows Server 2008
4658	The handle to an object was closed. Subject : Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Handle ID: %6 Process Information: Process ID: %7 Process Name: %8	Windows Vista, Windows Server 2008
4659	A handle to an object was requested with intent to delete. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %13 Access Request Information: Transaction ID: %9 Accesses: %10 Access Mask: %11 Privileges Used for Access Check: %12	Windows Vista, Windows Server 2008

4660	An object was deleted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Handle ID: %6 Process Information: Process ID: %7 Process Name: %8 Transaction ID: %9	Windows Vista, Windows Server 2008
4661	A handle to an object was requested. Subject : Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %15 Process Name: %16 Access Request Information: Transaction ID: %9 Accesses: %10 Access Mask: %11 Privileges Used for Access Check: %12 Properties: %13 Restricted SID Count: %14	Windows Vista, Windows Server 2008

4661	A handle to an object was requested. Subject : Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %16 Process Name: %17 Access Request Information: Transaction ID: %9 Accesses: %10 Access Reasons: %11 Access Mask: %12 Privileges Used for Access Check: %13 Properties: %14 Restricted SID Count: %15	Windows 7, Windows Server 2008 R2
4662	An operation was performed on an object. Subject : Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %9 Operation: Operation Type: %8 Accesses: %10 Access Mask: %11 Properties: %12 Additional Information: Parameter 1: %13 Parameter 2: %14	Windows Vista, Windows Server 2008

4663	An attempt was made to access an object. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %11 Process Name: %12 Access Request Information: Accesses: %9 Access Mask: %10	Windows Vista, Windows Server 2008
4663	An attempt was made to access an object. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Resource Attributes: %13 Process Information: Process ID: %11 Process Name: %12 Access Request Information: Accesses: %9 Access Mask: %10	Windows 8, Windows Server 2012
4664	An attempt was made to create a hard link. Subject: Account Name: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Link Information: File Name: %5 Link Name: %6 Transaction ID: %7	Windows Vista, Windows Server 2008

4665	An attempt was made to create an application client context. Subject: Client Name: %3 Client Domain: %4 Client Context ID: %5 Application Information: Application Name: %1 Application Instance ID: %2 Status: %6	Windows Vista, Windows Server 2008
4666	An application attempted an operation: Subject: Client Name: %5 Client Domain: %6 Client Context ID: %7 Object: Object Name: %3 Scope Names: %4 Application Information: Application Name: %1 Application Instance ID: %2 Access Request Information: Role: %8 Groups: %9 Operation Name: %10 (%11)	Windows Vista, Windows Server 2008
4667	An application client context was deleted. Subject: Client Name: %3 Client Domain: %4 Client Context ID: %5 Application Information: Application Name: %1 Application Instance ID: %2	Windows Vista, Windows Server 2008

4668	A new process has been created. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: New Process ID: %5 New Process Name: %6 Token Elevation Type: %7 Creator Process ID: %8 Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.	Windows Vista, Windows Server 2008

4668	A new process has been created. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: New Process ID: %5 New Process Name: %6 Token Elevation Type: %7 Creator Process ID: %8 Process Command Line: %9 Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.	Windows 8.1, Windows Server 2012 R2

4668	A new process has been created. Creator Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Target Subject: Security ID: %10 Account Name: %11 Account Domain: %12 Logon ID: %13 Process Information: New Process ID: %5 New Process Name: %6!S! Token Elevation Type: %7 Mandatory Label: %15 Creator Process ID: %8 Creator Process Name: %14!S! Process Command Line: %9!S! Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account	Windows 10
4670	Permissions on an object were changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process: Process ID: %11 Process Name: %12 Permissions Change: Original Security Descriptor: %9 New Security Descriptor: %10	Windows Vista, Windows Server 2008
4671	An application attempted to access a blocked ordinal through the TBS. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Ordinal: %5	Windows Vista, Windows Server 2008

4672	Special privileges assigned to new logon. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Privileges: %5	Windows Vista, Windows Server 2008
4673	A privileged service was called. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Service: Server: %5 Service Name: %6 Process: Process ID: %8 Process Name: %9 Service Request Information: Privileges: %7	Windows Vista, Windows Server 2008
4674	An operation was attempted on a privileged object. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Object Handle: %8 Process Information: Process ID: %11 Process Name: %12 Requested Operation: Desired Access: %9 Privileges: %10	Windows Vista, Windows Server 2008
4675	SIDs were filtered. Target Account: Security ID: %1 Account Name: %2 Account Domain: %3 Trust Information: Trust Direction: %4 Trust Attributes: %5 Trust Type: %6 TDO Domain SID: %7 Filtered SIDs: %8	Windows Vista, Windows Server 2008

4688	A new process has been created. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: New Process ID: %5 New Process Name: %6 Token Elevation Type: %7 Creator Process ID: %8 Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.	Windows Vista, Windows Server 2008
4688	A new process has been created. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: New Process ID: %5 New Process Name: %6 Token Elevation Type: %7 Creator Process ID: %8 Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.	Windows 8.1, Windows Server 2012 R2

4688	A new process has been created. Creator Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Target Subject: Security ID: %10 Account Name: %11 Account Domain: %12 Logon ID: %13 Process Information: New Process ID: %5 New Process Name: %6!S! Token Elevation Type: %7 Mandatory Label: %15 Creator Process ID: %8 Creator Process Name: %14!S! Process Command Line: %9!S! Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account	Windows 10
4689	A process has exited. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: Process ID: %6 Process Name: %7 Exit Status: %5	Windows Vista, Windows Server 2008
4690	An attempt was made to duplicate a handle to an object. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Source Handle Information: Source Handle ID: %5 Source Process ID: %6 New Handle Information: Target Handle ID: %7 Target Process ID: %8	Windows Vista, Windows Server 2008

4691	Indirect access to an object was requested. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Type: %5 Object Name: %6 Process Information: Process ID: %9 Access Request Information: Accesses: %7 Access Mask: %8	Windows Vista, Windows Server 2008
4692	Backup of data protection master key was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Key Information: Key Identifier: %5 Recovery Server: %6 Recovery Key ID: %7 Status Information: Status Code: %8	Windows Vista, Windows Server 2008
4693	Recovery of data protection master key was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Key Information: Key Identifier: %5 Recovery Server: %6 Recovery Key ID: %8 Recovery Reason: %7 Status Information: Status Code: %9	Windows Vista, Windows Server 2008
4694	Protection of auditable protected data was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Protected Data: Data Description: %6 Key Identifier: %5 Protected Data Flags: %7 Protection Algorithms: %8 Status Information: Status Code: %9	Windows Vista, Windows Server 2008

4695	Unprotection of auditable protected data was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Protected Data: Data Description: %6 Key Identifier: %5 Protected Data Flags: %7 Protection Algorithms: %8 Status Information: Status Code: %9	Windows Vista, Windows Server 2008
4696	A primary token was assigned to process. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process Information: Process ID: %11 Process Name: %12 Target Process: Target Process ID: %9 Target Process Name: %10 New Token Information: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8	Windows Vista, Windows Server 2008
4697	A service was installed in the system. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Service Information: Service Name: %5 Service File Name: %6 Service Type: %7 Service Start Type: %8 Service Account: %9	Windows Vista, Windows Server 2008
4698	A scheduled task was created. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Task Information: Task Name: %5 Task Content: %6	Windows Vista, Windows Server 2008

4699	A scheduled task was deleted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Task Information: Task Name: %5 Task Content: %6	Windows Vista, Windows Server 2008
4700	A scheduled task was enabled. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Task Information: Task Name: %5 Task Content: %6	Windows Vista, Windows Server 2008
4701	A scheduled task was disabled. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Task Information: Task Name: %5 Task Content: %6	Windows Vista, Windows Server 2008
4702	A scheduled task was updated. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Task Information: Task Name: %5 Task New Content: %6	Windows Vista, Windows Server 2008

4703	A user right was adjusted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Target Account: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Process Information: Process ID: %10 Process Name: %9 Enabled Privileges: %11 Disabled Privileges: %12	Windows 10
4704	A user right was assigned. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Target Account: Account Name: %5 New Right: User Right: %6	Windows Vista, Windows Server 2008
4705	A user right was removed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Target Account: Account Name: %5 Removed Right: User Right: %6	Windows Vista, Windows Server 2008
4706	A new trust was created to a domain. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Trusted Domain: Domain Name: %1 Domain ID: %2 Trust Information: Trust Type: %7 Trust Direction: %8 Trust Attributes: %9 SID Filtering: %10	Windows Vista, Windows Server 2008

4707	A trust to a domain was removed. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Domain Information: Domain Name: %1 Domain ID: %2	Windows Vista, Windows Server 2008
4709	IPsec Services was started. %1 Policy Source: %2 %3	Windows Vista, Windows Server 2008
4710	IPsec Services was disabled. %1 %2	Windows Vista, Windows Server 2008
4711	%1	Windows Vista, Windows Server 2008
4712	IPsec Services encountered a potentially serious failure. %1	Windows Vista, Windows Server 2008
4713	Kerberos policy was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Changes Made: ('--' means no changes, otherwise each change is shown as: (Parameter Name): (new value) (old value)) %5	Windows Vista, Windows Server 2008
4714	Encrypted data recovery policy was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Changes Made: ('--' means no changes, otherwise each change is shown as: (Parameter Name): (new value) (old value)) %5	Windows Vista, Windows Server 2008
4715	The audit policy (SACL) on an object was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Audit Policy Change: Original Security Descriptor: %5 New Security Descriptor: %6	Windows Vista, Windows Server 2008

4716	Trusted domain information was modified. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Trusted Domain: Domain Name: %5 Domain ID: %6 New Trust Information: Trust Type: %7 Trust Direction: %8 Trust Attributes: %9 SID Filtering: %10	Windows Vista, Windows Server 2008
4717	System security access was granted to an account. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Account Modified: Account Name: %5 Access Granted: Access Right: %6	Windows Vista, Windows Server 2008
4718	System security access was removed from an account. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Account Modified: Account Name: %5 Access Removed: Access Right: %6	Windows Vista, Windows Server 2008
4719	System audit policy was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Audit Policy Change: Category: %5 Subcategory: %6 Subcategory GUID: %7 Changes: %8	Windows Vista, Windows Server 2008

4720	A user account was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 New Account: Security ID: %3 Account Name: %1 Account Domain: %2 Attributes: SAM Account Name: %9 Display Name: %10 User Principal Name: %11 Home Directory: %12 Home Drive: %13 Script Path: %14 Profile Path: %15 User Workstations: %16 Password Last Set: %17 Account Expires: %18 Primary Group ID: %19 Allowed To Delegate To: %20 Old UAC Value: %21 New UAC Value: %22 User Account Control: %23 User Parameters: %24 SID History: %25 Logon Hours: %26 Additional Information: Privileges %8	Windows Vista, Windows Server 2008
4722	A user account was enabled. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %3 Account Name: %1 Account Domain: %2	Windows Vista, Windows Server 2008
4723	An attempt was made to change an account's password. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %3 Account Name: %1 Account Domain: %2 Additional Information: Privileges %8	Windows Vista, Windows Server 2008

4724	An attempt was made to reset an account's password. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %3 Account Name: %1 Account Domain: %2	Windows Vista, Windows Server 2008
4725	A user account was disabled. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %3 Account Name: %1 Account Domain: %2	Windows Vista, Windows Server 2008
4726	A user account was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %3 Account Name: %1 Account Domain: %2 Additional Information: Privileges %8	Windows Vista, Windows Server 2008
4727	A security-enabled global group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 New Group: Security ID: %3 Group Name: %1 Group Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4728	A member was added to a security-enabled global group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008
4728	A member was added to a security-enabled global group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10 Expiration time: %11	Windows Vista, Windows Server 2008
4729	A member was removed from a security-enabled global group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008

4730	A security-enabled global group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Deleted Group: Security ID: %3 Group Name: %1 Group Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4731	A security-enabled local group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 New Group: Security ID: %3 Group Name: %1 Group Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4732	A member was added to a security-enabled local group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008

4732	A member was added to a security-enabled local group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10 Expiration time: %11	Windows Vista, Windows Server 2008
4733	A member was removed from a security-enabled local group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008
4734	A security-enabled local group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4735	A security-enabled local group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Changed Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4737	A security-enabled global group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Changed Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4738	A user account was changed. Subject: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Target Account: Security ID: %4 Account Name: %2 Account Domain: %3 Changed Attributes: SAM Account Name: %10 Display Name: %11 User Principal Name: %12 Home Directory: %13 Home Drive: %14 Script Path: %15 Profile Path: %16 User Workstations: %17 Password Last Set: %18 Account Expires: %19 Primary Group ID: %20 AllowedToDelegateTo: %21 Old UAC Value: %22 New UAC Value: %23 User Account Control: %24 User Parameters: %25 SID History: %26 Logon Hours: %27 Additional Information: Privileges: %9	Windows Vista, Windows Server 2008
4739	Domain Policy was changed. Change Type: %1 modified Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Domain: Domain Name: %2 Domain ID: %3 Changed Attributes: Min. Password Age: %9 Max. Password Age: %10 Force Logoff: %11 Lockout Threshold: %12 Lockout Observation Window: %13 Lockout Duration: %14 Password Properties: %15 Min. Password Length: %16 Password History Length: %17 Machine Account Quota: %18 Mixed Domain Mode: %19 Domain Behavior Version: %20 OEM Information: %21 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4740	0x8000000000000000 message: A user account was locked out. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Account That Was Locked Out: Security ID: %3 Account Name: %1 Additional Information: Caller Computer Name: %2	Windows Vista, Windows Server 2008
4741	A computer account was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 New Computer Account: Security ID: %3 Account Name: %1 Account Domain: %2 Attributes: SAM Account Name: %9 Display Name: %10 User Principal Name: %11 Home Directory: %12 Home Drive: %13 Script Path: %14 Profile Path: %15 User Workstations: %16 Password Last Set: %17 Account Expires: %18 Primary Group ID: %19 AllowedToDelegateTo: %20 Old UAC Value: %21 New UAC Value: %22 User Account Control: %23 User Parameters: %24 SID History: %25 Logon Hours: %26 DNS Host Name: %27 Service Principal Names: %28 Additional Information: Privileges %8	Windows Vista, Windows Server 2008

4742	A computer account was changed. Subject: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Computer Account That Was Changed: Security ID: %4 Account Name: %2 Account Domain: %3 Changed Attributes: SAM Account Name: %10 Display Name: %11 User Principal Name: %12 Home Directory: %13 Home Drive: %14 Script Path: %15 Profile Path: %16 User Workstations: %17 Password Last Set: %18 Account Expires: %19 Primary Group ID: %20 AllowedToDelegateTo: %21 Old UAC Value: %22 New UAC Value: %23 User Account Control: %24 User Parameters: %25 SID History: %26 Logon Hours: %27 DNS Host Name: %28 Service Principal Names: %29 Additional Information: Privileges: %9	Windows Vista, Windows Server 2008
4743	A computer account was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Computer: Security ID: %3 Account Name: %1 Account Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4744	A security-disabled local group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 New Group: Security ID: %3 Group Name: %1 Group Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4745	A security-disabled local group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Changed Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4746	A member was added to a security-disabled local group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008

4746	A member was added to a security-disabled local group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10 Expiration time: %11	Windows 10 [Version 1511]
4747	A member was removed from a security-disabled local group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008
4748	A security-disabled local group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4749	A security-disabled global group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4750	A security-disabled global group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Changed Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4751	A member was added to a security-disabled global group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008

4751	A member was added to a security-disabled global group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10 Expiration time: %11	Windows 10 [Version 1511]
4752	A member was removed from a security-disabled global group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008
4753	A security-disabled global group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4754	A security-enabled universal group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4755	A security-enabled universal group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Changed Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4756	A member was added to a security-enabled universal group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Account Name: %3 Account Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008

4756	A member was added to a security-enabled universal group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Account Name: %3 Account Domain: %4 Additional Information: Privileges: %10 Expiration time: %11	Windows 10 [Version 1511]
4757	A member was removed from a security-enabled universal group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008
4758	A security-enabled universal group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4759	A security-disabled universal group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4760	A security-disabled universal group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Changed Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4761	A member was added to a security-disabled universal group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008

4761	A member was added to a security-disabled universal group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10 Expiration time: %11	Windows 10 [Version 1511]
4762	A member was removed from a security-disabled universal group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008
4763	A security-disabled universal group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4764	A group's type was changed. Subject: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Change Type: %1 Group: Security ID: %4 Group Name: %2 Group Domain: %3 Additional Information: Privileges: %9	Windows Vista, Windows Server 2008
4765	SID History was added to an account. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Target Account: Security ID: %5 Account Name: %3 Account Domain: %4 Source Account: Security ID: %2 Account Name: %1 Additional Information: Privileges: %10 SID List: %11	Windows Vista, Windows Server 2008
4766	An attempt to add SID History to an account failed. Subject: Security ID: Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %4 Account Name: %2 Account Domain: %3 Source Account Account Name: %1 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4767	A user account was unlocked. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %3 Account Name: %1 Account Domain: %2	Windows Vista, Windows Server 2008

4768	A Kerberos authentication ticket (TGT) was requested. Account Information: Account Name: %1 Supplied Realm Name: %2 User ID: %3 Service Information: Service Name: %4 Service ID: %5 Network Information: Client Address: %10 Client Port: %11 Additional Information: Ticket Options: %6 Result Code: %7 Ticket Encryption Type: %8 Pre-Authentication Type: %9 Certificate Information: Certificate Issuer Name: %12 Certificate Serial Number: %13 Certificate Thumbprint: %14 Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.	Windows Vista, Windows Server 2008
4769	A Kerberos service ticket was requested. Account Information: Account Name: %1 Account Domain: %2 Logon GUID: %10 Service Information: Service Name: %3 Service ID: %4 Network Information: Client Address: %7 Client Port: %8 Additional Information: Ticket Options: %5 Ticket Encryption Type: %6 Failure Code: %9 Transited Services: %11 This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.	Windows Vista, Windows Server 2008

4770	A Kerberos service ticket was renewed. Account Information: Account Name: %1 Account Domain: %2 Service Information: Service Name: %3 Service ID: %4 Network Information: Client Address: %7 Client Port: %8 Additional Information: Ticket Options: %5 Ticket Encryption Type: %6 Ticket options and encryption types are defined in RFC 4120.	Windows Vista, Windows Server 2008
4771	Kerberos pre-authentication failed. Account Information: Security ID: %2 Account Name: %1 Service Information: Service Name: %3 Network Information: Client Address: %7 Client Port: %8 Additional Information: Ticket Options: %4 Failure Code: %5 Pre-Authentication Type: %6 Certificate Information: Certificate Issuer Name: %9 Certificate Serial Number: %10 Certificate Thumbprint: %11 Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options and failure codes are defined in RFC 4120. If the ticket was malformed or damaged during transit and could not be decrypted, then many fields in this event might not be present.	Windows Vista, Windows Server 2008
4772	A Kerberos authentication ticket request failed. Account Information: Account Name: %1 Supplied Realm Name: %2 Service Information: Service Name: %3 Network Information: Client Address: %6 Client Port: %7 Additional Information: Ticket Options: %4 Failure Code: %5 Ticket options and failure codes are defined in RFC 4120.	Windows Vista, Windows Server 2008

4773	A Kerberos service ticket request failed. Account Information: Account Name: %1 Account Domain: %2 Service Information: Service Name: %3 Network Information: Client Address: %6 Client Port: %7 Additional Information: Ticket Options: %4 Failure Code: %5 Ticket options and failure codes are defined in RFC 4120.	Windows Vista, Windows Server 2008
4774	An account was mapped for logon. Authentication Package: %1 Account UPN: %2 Mapped Name: %3	Windows Vista, Windows Server 2008
4775	An account could not be mapped for logon. Authentication Package: %1 Account Name: %2	Windows Vista, Windows Server 2008
4776	The domain controller attempted to validate the credentials for an account. Authentication Package: %1 Logon Account: %2 Source Workstation: %3 Error Code: %4	Windows Vista, Windows Server 2008
4777	The domain controller failed to validate the credentials for an account. Authentication Package: %1 Logon Account: %2 Source Workstation: %3 Error Code: %4	Windows Vista, Windows Server 2008
4778	A session was reconnected to a Window Station. Subject: Account Name: %1 Account Domain: %2 Logon ID: %3 Session: Session Name: %4 Additional Information: Client Name: %5 Client Address: %6 This event is generated when a user reconnects to an existing Terminal Services session, or when a user switches to an existing desktop using Fast User Switching.	Windows Vista, Windows Server 2008

4779	A session was disconnected from a Window Station. Subject: Account Name: %1 Account Domain: %2 Logon ID: %3 Session: Session Name: %4 Additional Information: Client Name: %5 Client Address: %6 This event is generated when a user disconnects from an existing Terminal Services session, or when a user switches away from an existing desktop using Fast User Switching.	Windows Vista, Windows Server 2008
4780	The ACL was set on accounts which are members of administrators groups. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Target Account: Security ID: %3 Account Name: %1 Account Domain: %2 Additional Information: Privileges: %8 Every hour, the Windows domain controller that holds the primary domain controller (PDC) Flexible Single Master Operation (FSMO) role compares the ACL on all security principal accounts (users, groups, and machine accounts) present for its domain in Active Directory and that are in administrative groups against the ACL on the AdminSDHolder object. If the ACL on the principal account differs from the ACL on the AdminSDHolder object, then the ACL on the principal account is reset to match the ACL on the AdminSDHolder object and this event is generated.	Windows Vista, Windows Server 2008
4781	The name of an account was changed: Subject: Security ID: %5 Account Name: %6 Account Domain: %7 Logon ID: %8 Target Account: Security ID: %4 Account Domain: %3 Old Account Name: %1 New Account Name: %2 Additional Information: Privileges: %9	Windows Vista, Windows Server 2008

4782	The password hash an account was accessed. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Target Account: Account Name: %1 Account Domain: %2	Windows Vista, Windows Server 2008
4783	A basic application group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Account Name: %1 Account Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4784	A basic application group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Account Name: %1 Account Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4785	A member was added to a basic application group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008
4785	A member was added to a basic application group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10 Expiration time: %11	Windows Vista, Windows Server 2008
4786	A member was removed from a basic application group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Group Name: %3 Group Domain: %4 Additional Information: Privileges: %10	Windows Vista, Windows Server 2008

4787	A non-member was added to a basic application group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Account Name: %3 Account Domain: %4 Additional Information: Privileges: %10 A non-member is an account that is explicitly excluded from membership in a basic application group. Even if the account is specified as a member of the application group, either explicitly or through nested group membership, the account will not be treated as a group member if it is listed as a non-member.	Windows Vista, Windows Server 2008
4788	A non-member was removed from a basic application group. Subject: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Member: Security ID: %2 Account Name: %1 Group: Security ID: %5 Account Name: %3 Account Domain: %4 Additional Information: Privileges: %10 A non-member is an account that is explicitly excluded from membership in a basic application group. Even if the account is specified as a member of the application group, either explicitly or through nested group membership, the account will not be treated as a group member if it is listed as a non-member.	Windows Vista, Windows Server 2008
4789	A basic application group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Account Name: %1 Account Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008

4790	An LDAP query group was created. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Account Name: %1 Account Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4791	A basic application group was changed. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Account Name: %1 Account Domain: %2 Attributes: SAM Account Name: %9 SID History: %10 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4792	An LDAP query group was deleted. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Account Name: %1 Account Domain: %2 Additional Information: Privileges: %8	Windows Vista, Windows Server 2008
4793	The Password Policy Checking API was called. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Additional Information: Caller Workstation: %5 Provided Account Name (unauthenticated): %6 Status Code: %7	Windows Vista, Windows Server 2008

4794	An attempt was made to set the Directory Services Restore Mode administrator password. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Additional Information: Caller Workstation: %5 Status Code: %6	Windows Vista, Windows Server 2008
4797	An attempt was made to query the existence of a blank password for an account. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Additional Information: Caller Workstation: %5 Target Account Name: %6 Target Account Domain: %7	Windows 8, Windows Server 2012
4798	A user's local group membership was enumerated. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 User: Security ID: %3 Account Name: %1 Account Domain: %2 Process Information: Process ID: %8 Process Name: %9	Windows 10
4799	A security-enabled local group membership was enumerated. Subject: Security ID: %4 Account Name: %5 Account Domain: %6 Logon ID: %7 Group: Security ID: %3 Group Name: %1 Group Domain: %2 Process Information: Process ID: %8 Process Name: %9	Windows 10
4800	The workstation was locked. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Session ID: %5	Windows Vista, Windows Server 2008

4801	The workstation was unlocked. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Session ID: %5	Windows Vista, Windows Server 2008
4802	The screen saver was invoked. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Session ID: %5	Windows Vista, Windows Server 2008
4803	The screen saver was dismissed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Session ID: %5	Windows Vista, Windows Server 2008
4816	RPC detected an integrity violation while decrypting an incoming message. Peer Name: %1 Protocol Sequence: %2 Security Error: %3	Windows Vista, Windows Server 2008
4816	RPC detected an integrity violation while decrypting an incoming message. Peer Name: %1 Protocol Sequence: %2 Security Error: %3	Windows Vista, Windows Server 2008
4817	A handle to an object was requested. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server:%5 Object Type:%6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %15 Process Name: %16 Access Request Information: Transaction ID: %9 Accesses: %10 Access Reasons: %11 Access Mask: %12 Privileges Used for Access Check: %13 Restricted SID Count: %14	Windows 7, Windows Server 2008 R2

4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %9 Process Name: %10 Current Central Access Policy results: Access Reasons: %11 Proposed Central Access Policy results that differ from the current Central Access Policy results: Access Reasons: %12	Windows 8, Windows Server 2012
4819	Central Access Policies on the machine have been changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 CAPs Added: %7 CAPs Deleted: %8 CAPs Modified: %9 CAPs As-Is: %10	Windows 8, Windows Server 2012

4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions. Account Information: Account Name: %1 Supplied Realm Name: %2 User ID: %3 Authentication Policy Information: Silo Name: %16 Policy Name: %17 TGT Lifetime: %18 Device Information: Device Name: %4 Service Information: Service Name: %5 Service ID: %6 Network Information: Client Address: %11 Client Port: %12 Additional Information: Ticket Options: %7 Result Code: %8 Ticket Encryption Type: %9 Pre-Authentication Type: %10 Certificate Information: Certificate Issuer Name: %13 Certificate Serial Number: %14 Certificate Thumbprint: %15 Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.	Windows 8, Windows Server 2012

4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions. Account Information: Account Name: %1 Account Domain: %2 Logon GUID: %11 Authentication Policy Information: Silo Name: %13 Policy Name: %14 Device Information: Device Name: %3 Service Information: Service Name: %4 Service ID: %5 Network Information: Client Address: %8 Client Port: %9 Additional Information: Ticket Options: %6 Ticket Encryption Type: %7 Failure Code: %10 Transited Services: %12 This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket.	
4822	NTLM authentication failed because the account was a member of the Protected User group. Account Name: %1 Device Name: %2 Error Code: %3	Windows 8.1, Windows Server 2012 R2
4823	NTLM authentication failed because access control restrictions are required. Account Name: %1 Device Name: %2 Error Code: %3 Authentication Policy Information: Silo Name: %4 PolicyName: %5	Windows 8.1, Windows Server 2012 R2

4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group. Account Information: Security ID: %2 Account Name: %1 Service Information: Service Name: %3 Network Information: Client Address: %7 Client Port: %8 Additional Information: Ticket Options: %4 Failure Code: %5 Pre-Authentication Type: %6 Certificate Information: Certificate Issuer Name: %9 Certificate Serial Number: %10 Certificate Thumbprint: %11 Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options and failure codes are defined in RFC 4120. If the ticket was malformed or damaged during transit and could not be decrypted, then many fields in this event might not be present.	Windows 8.1, Windows Server 2012 R2
4825	A user was denied the access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group. Subject: User Name: %1 Domain: %2 Logon ID: %3 Additional Information: Client Address: %4 This event is generated when an authenticated user who is not allowed to log on remotely attempts to connect to this computer through Remote Desktop.	Windows Vista SP2, Windows Server 2008 SP2

4826	Boot Configuration Data loaded. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 General Settings: Load Options: %5 Advanced Options: %6 Configuration Access Policy: %7 System Event Logging: %8 Kernel Debugging: %9 VSM Launch Type: %10 Signature Settings: Test Signing: %11 Flight Signing: %12 Disable Integrity Checks: %13 HyperVisor Settings: HyperVisor Load Options: %14 HyperVisor Launch Type: %15 HyperVisor Debugging: %16	Windows 10
4864	A namespace collision was detected. Target Type: %1 Target Name: %2 Forest Root: %3 Top Level Name: %4 DNS Name: %5 NetBIOS Name: %6 Security ID: %7 New Flags: %8	Windows Vista, Windows Server 2008
4865	A trusted forest information entry was added. Subject: Security ID: %10 Account Name: %11 Account Domain: %12 Logon ID: %13 Trust Information: Forest Root: %1 Forest Root SID: %2 Operation ID: %3 Entry Type: %4 Flags: %5 Top Level Name: %6 DNS Name: %7 NetBIOS Name: %8 Domain SID: %9	Windows Vista, Windows Server 2008

4866	A trusted forest information entry was removed. Subject: Security ID: %10 Account Name: %11 Account Domain: %12 Logon ID: %13 Trust Information: Forest Root: %1 Forest Root SID: %2 Operation ID: %3 Entry Type: %4 Flags: %5 Top Level Name: %6 DNS Name: %7 NetBIOS Name: %8 Domain SID: %9	Windows Vista, Windows Server 2008
4867	A trusted forest information entry was modified. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Trust Information: Forest Root: %5 Forest Root SID: %6 Operation ID: %7 Entry Type: %8 Flags: %9 Top Level Name: %10 DNS Name: %11 NetBIOS Name: %12 Domain SID: %13	Windows Vista, Windows Server 2008
4868	The certificate manager denied a pending certificate request. Request ID: %1	Windows Vista, Windows Server 2008
4869	Certificate Services received a resubmitted certificate request. Request ID: %1	Windows Vista, Windows Server 2008
4870	Certificate Services revoked a certificate. Serial Number: %1 Reason: %2	Windows Vista, Windows Server 2008
4871	Certificate Services received a request to publish the certificate revocation list (CRL). Next Update: %1 Publish Base: %2 Publish Delta: %3	Windows Vista, Windows Server 2008
4872	Certificate Services published the certificate revocation list (CRL). Base CRL: %1 CRL Number: %2 Key Container: %3 Next Publish: %4 Publish URLs: %5	Windows Vista, Windows Server 2008
4873	A certificate request extension changed. Request ID: %1 Name: %2 Type: %3 Flags: %4 Data: %5	Windows Vista, Windows Server 2008

4874	One or more certificate request attributes changed. Request ID: %1 Attributes: %2	Windows Vista, Windows Server 2008
4875	Certificate Services received a request to shut down.	Windows Vista, Windows Server 2008
4876	Certificate Services backup started. Backup Type: %1	Windows Vista, Windows Server 2008
4877	Certificate Services backup completed.	Windows Vista, Windows Server 2008
4878	Certificate Services restore started.	Windows Vista, Windows Server 2008
4879	Certificate Services restore completed.	Windows Vista, Windows Server 2008
4880	Certificate Services started. Certificate Database Hash: %1 Private Key Usage Count: %2 CA Certificate Hash: %3 CA Public Key Hash: %4	Windows Vista, Windows Server 2008
4881	Certificate Services stopped. Certificate Database Hash: %1 Private Key Usage Count: %2 CA Certificate Hash: %3 CA Public Key Hash: %4	Windows Vista, Windows Server 2008
4882	The security permissions for Certificate Services changed. %1	Windows Vista, Windows Server 2008
4883	Certificate Services retrieved an archived key. Request ID: %1	Windows Vista, Windows Server 2008
4884	Certificate Services imported a certificate into its database. Certificate: %1 Request ID: %2	Windows Vista, Windows Server 2008
4885	The audit filter for Certificate Services changed. Filter: %1	Windows Vista, Windows Server 2008
4886	Certificate Services received a certificate request. Request ID: %1 Requester: %2 Attributes: %3	Windows Vista, Windows Server 2008
4887	Certificate Services approved a certificate request and issued a certificate. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Windows Vista, Windows Server 2008
4888	Certificate Services denied a certificate request. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Windows Vista, Windows Server 2008

4889	Certificate Services set the status of a certificate request to pending. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Windows Vista, Windows Server 2008
4890	The certificate manager settings for Certificate Services changed. Enable: %1 %2	Windows Vista, Windows Server 2008
4891	A configuration entry changed in Certificate Services. Node: %1 Entry: %2 Value: %3	Windows Vista, Windows Server 2008
4892	A property of Certificate Services changed. Property: %1 Index: %2 Type: %3 Value: %4	Windows Vista, Windows Server 2008
4893	Certificate Services archived a key. Request ID: %1 Requester: %2 KRA Hashes: %3	Windows Vista, Windows Server 2008
4894	Certificate Services imported and archived a key. Request ID: %1	Windows Vista, Windows Server 2008
4895	Certificate Services published the CA certificate to Active Directory Domain Services. Certificate Hash: %1 Valid From: %2 Valid To: %3	Windows Vista, Windows Server 2008
4896	One or more rows have been deleted from the certificate database. Table ID: %1 Filter: %2 Rows Deleted: %3	Windows Vista, Windows Server 2008
4897	Role separation enabled: %1	Windows Vista, Windows Server 2008
4898	Certificate Services loaded a template. %1 v%2 (Schema V%3) %4 %5 Template Information: Template Content: %7 Security Descriptor: %8 Additional Information: Domain Controller: %6	Windows Vista, Windows Server 2008

4899	A Certificate Services template was updated. %1 v%2 (Schema V%3) %4 %5 Template Change Information: Old Template Content: %8 New Template Content: %7 Additional Information: Domain Controller: %6	Windows Vista, Windows Server 2008
4900	Certificate Services template security was updated. %1 v%2 (Schema V%3) %4 %5 Template Change Information: Old Template Content: %9 New Template Content: %7 Old Security Descriptor: %10 New Security Descriptor: %8 Additional Information: Domain Controller: %6	Windows Vista, Windows Server 2008
4902	The Per-user audit policy table was created. Number of Elements: %1 Policy ID: %2	Windows Vista, Windows Server 2008
4904	An attempt was made to register a security event source. Subject : Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process: Process ID: %7 Process Name: %8 Event Source: Source Name: %5 Event Source ID: %6	Windows Vista, Windows Server 2008
4905	An attempt was made to unregister a security event source. Subject Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Process: Process ID: %7 Process Name: %8 Event Source: Source Name: %5 Event Source ID: %6	Windows Vista, Windows Server 2008
4906	The CrashOnAuditFail value has changed. New Value of CrashOnAuditFail: %1	Windows Vista, Windows Server 2008

4907	Auditing settings on object were changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %11 Process Name: %12 Auditing Settings: Original Security Descriptor: %9 New Security Descriptor: %10	Windows Vista, Windows Server 2008
4908	Special Groups Logon table modified. Special Groups: %1 This event is generated when the list of special groups is updated in the registry or through security policy. The updated list of special groups is indicated in the event.	Windows Vista, Windows Server 2008
4909	The local policy settings for the TBS were changed. Old Blocked Ordinals: %1 New Blocked Ordinals: %2	Windows Vista, Windows Server 2008
4910	The group policy settings for the TBS were changed. Group Policy Setting: Ignore Default Settings Old Value: %1 New Value: %2 Group Policy Setting: Ignore Local Settings Old Value: %3 New Value: %4 Old Blocked Ordinals: %5 New Blocked Ordinals: %6	Windows Vista, Windows Server 2008
4911	Resource attributes of the object were changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %9 Process Name: %10 Resource Attributes: Original Security Descriptor: %11 New Security Descriptor: %12	Windows 8, Windows Server 2012

4912	Per User Audit Policy was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Policy For Account: Security ID: %5 Policy Change Details: Category: %6 Subcategory: %7 Subcategory GUID: %8 Changes: %9	Windows Vista, Windows Server 2008
4913	Central Access Policy on the object was changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 Process Information: Process ID: %11 Process Name: %12 Central Policy ID: Original Security Descriptor: %9 New Security Descriptor: %10	Windows 8, Windows Server 2012
4928	An Active Directory replica source naming context was established. Destination DRA: %1 Source DRA: %2 Source Address: %3 Naming Context: %4 Options: %5 Status Code: %6	Windows Vista, Windows Server 2008
4929	An Active Directory replica source naming context was removed. Destination DRA: %1 Source DRA: %2 Source Address: %3 Naming Context: %4 Options: %5 Status Code: %6	Windows Vista, Windows Server 2008
4930	An Active Directory replica source naming context was modified. Destination DRA: %1 Source DRA: %2 Source Address: %3 Naming Context: %4 Options: %5 Status Code: %6	Windows Vista, Windows Server 2008

4931	An Active Directory replica destination naming context was modified. Destination DRA: %1 Source DRA: %2 Destination Address: %3 Naming Context: %4 Options: %5 Status Code: %6	Windows Vista, Windows Server 2008
4932	Synchronization of a replica of an Active Directory naming context has begun. Destination DRA: %1 Source DRA: %2 Naming Context: %3 Options: %4 Session ID: %5 Start USN: %6	Windows Vista, Windows Server 2008
4933	Synchronization of a replica of an Active Directory naming context has ended. Destination DRA: %1 Source DRA: %2 Naming Context: %3 Options: %4 Session ID: %5 End USN: %6 Status Code: %7	Windows Vista, Windows Server 2008
4934	Attributes of an Active Directory object were replicated. Session ID: %1 Object: %2 Attribute: %3 Type of change: %4 New Value: %5 USN: %6 Status Code: %7	Windows Vista, Windows Server 2008
4935	Replication failure begins. Replication Event: %1 Audit Status Code: %2	Windows Vista, Windows Server 2008
4936	Replication failure ends. Replication Event: %1 Audit Status Code: %2 Replication Status Code: %3	Windows Vista, Windows Server 2008
4937	A lingering object was removed from a replica. Destination DRA: %1 Source DRA: %2 Object: %3 Options: %4 Status Code: %5	Windows Vista, Windows Server 2008
4944	The following policy was active when the Windows Firewall started. Group Policy Applied: %1 Profile Used: %2 Operational mode: %3 Allow Remote Administration: %4 Allow Unicast Responses to Multicast/Broadcast Traffic: %5 Security Logging: Log Dropped Packets: %6 Log Successful Connections: %7	Windows Vista, Windows Server 2008
4945	A rule was listed when the Windows Firewall started. Profile used: %1 Rule: Rule ID: %2 Rule Name: %3	Windows Vista, Windows Server 2008

4946	A change has been made to Windows Firewall exception list. A rule was added. Profile Changed: %1 Added Rule: Rule ID: %2 Rule Name: %3	Windows Vista, Windows Server 2008
4947	A change has been made to Windows Firewall exception list. A rule was modified. Profile Changed: %1 Modified Rule: Rule ID: %2 Rule Name: %3	Windows Vista, Windows Server 2008
4948	A change has been made to Windows Firewall exception list. A rule was deleted. Profile Changed: %1 Deleted Rule: Rule ID: %2 Rule Name: %3	Windows Vista, Windows Server 2008
4949	Windows Firewall settings were restored to the default values.	Windows Vista, Windows Server 2008
4950	A Windows Firewall setting has changed. Profile That Was Changed: %1 New Setting: Type: %2 Value: %3	Windows Vista, Windows Server 2008
4951	A rule has been ignored because its major version number was not recognized by Windows Firewall. Profile: %1 Ignored Rule: ID: %2 Name: %3	Windows Vista, Windows Server 2008
4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced. Profile: %1 Partially Ignored Rule: ID: %2 Name: %3	Windows Vista, Windows Server 2008
4953	A rule has been ignored by Windows Firewall because it could not parse the rule. Profile: %1 Reason for Rejection: %2 Rule: ID: %3 Name: %4	Windows Vista, Windows Server 2008
4954	Windows Firewall Group Policy settings has changed. The new settings have been applied.	Windows Vista, Windows Server 2008
4956	Windows Firewall has changed the active profile. New Active Profile: %1	Windows Vista, Windows Server 2008

4957	Windows Firewall did not apply the following rule: Rule Information: ID: %1 Name: %2 Error Information: Reason: %3 resolved to an empty set.	Windows Vista, Windows Server 2008
4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer: Rule Information: ID: %1 Name: %2 Error Information: Error: %3 Reason: %4	Windows Vista, Windows Server 2008
4960	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations. Remote Network Address: %1 Inbound SA SPI: %2	Windows Vista, Windows Server 2008
4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer. Remote Network Address: %1 Inbound SA SPI: %2	Windows Vista, Windows Server 2008
4962	IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay. Remote Network Address: %1 Inbound SA SPI: %2	Windows Vista, Windows Server 2008
4963	IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt. Remote Network Address: %1 Inbound SA SPI: %2	Windows Vista, Windows Server 2008
4964	Special groups have been assigned to a new logon. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon GUID: %5 New Logon: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Logon GUID: %10 Special Groups Assigned: %11	Windows Vista, Windows Server 2008
4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored. Remote Network Address: %1 Inbound SA SPI: %2	Windows Vista, Windows Server 2008

4976	During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. Local Network Address: %1 Remote Network Address: %2 Keying Module Name: %3	Windows Vista, Windows Server 2008
4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. Local Network Address: %1 Remote Network Address: %2 Keying Module Name: %3	Windows Vista, Windows Server 2008
4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. Local Network Address: %1 Remote Network Address: %2 Keying Module Name: %3	Windows Vista, Windows Server 2008
4979	IPsec Main Mode and Extended Mode security associations were established. Main Mode Local Endpoint: Principal Name: %1 Network Address: %3 Keying Module Port: %4 Main Mode Remote Endpoint: Principal Name: %2 Network Address: %5 Keying Module Port: %6 Main Mode Cryptographic Information: Cipher Algorithm: %8 Integrity Algorithm: %9 Diffie-Hellman Group: %10 Main Mode Security Association: Lifetime (minutes): %11 Quick Mode Limit: %12 Main Mode SA ID: %16 Main Mode Additional Information: Keying Module Name: AuthIP Authentication Method: %7 Role: %13 Impersonation State: %14 Main Mode Filter ID: %15 Extended Mode Information: Local Principal Name: %17 Remote Principal Name: %18 Authentication Method: %19 Impersonation State: %20 Quick Mode Filter ID: %21	Windows Vista, Windows Server 2008

4980	IPsec Main Mode and Extended Mode security associations were established. Main Mode Local Endpoint: Principal Name: %1 Network Address: %3 Keying Module Port: %4 Main Mode Remote Endpoint: Principal Name: %2 Network Address: %5 Keying Module Port: %6 Main Mode Cryptographic Information: Cipher Algorithm: %8 Integrity Algorithm: %9 Diffie-Hellman Group: %10 Main Mode Security Association: Lifetime (minutes): %11 Quick Mode Limit: %12 Main Mode SA ID: %16 Main Mode Additional Information: Keying Module Name: AuthIP Authentication Method: %7 Role: %13 Impersonation State: %14 Main Mode Filter ID: %15 Extended Mode Local Endpoint: Principal Name: %17 Certificate SHA Thumbprint: %18 Certificate Issuing CA: %19 Certificate Root CA: %20 Extended Mode Remote Endpoint: Principal Name: %21 Certificate SHA Thumbprint: %22 Certificate Issuing CA: %23	Windows Vista, Windows Server 2008

4981	IPsec Main Mode and Extended Mode security associations were established. Local Endpoint: Principal Name: %1 Network Address: %9 Keying Module Port: %10 Local Certificate: SHA Thumbprint: %2 Issuing CA: %3 Root CA: %4 Remote Endpoint: Principal Name: %5 Network Address: %11 Keying Module Port: %12 Remote Certificate: SHA Thumbprint: %6 Issuing CA: %7 Root CA: %8 Cryptographic Information: Cipher Algorithm: %13 Integrity Algorithm: %14 Diffie-Hellman Group: %15 Security Association Information: Lifetime (minutes): %16 Quick Mode Limit: %17 Main Mode SA ID: %21 Additional Information: Keying Module Name: AuthIP Authentication Method: SSL Role: %18 Impersonation State: %19 Main Mode Filter ID: %20	Windows Vista, Windows Server 2008

4982	IPsec Main Mode and Extended Mode security associations were established. Local Endpoint: Principal Name: %1 Network Address: Keying Module Port: %9 Local Certificate: SHA Thumbprint: %2 Issuing CA: %3 Root CA: %4 Remote Endpoint: Principal Name: %5 Network Address: %11 Keying Module Port: %12 Remote Certificate: SHA Thumbprint: %6 Issuing CA: %7 Root CA: %8 Cryptographic Information: Cipher Algorithm: %12 Integrity Algorithm: %13 Diffie-Hellman Group: %14 Security Association Information: Lifetime (minutes): %15 Quick Mode Limit: %16 Main Mode SA ID: %20 Additional Information: Keying Module Name: AuthIP Authentication Method: SSL Role: %17 Impersonation State: %18 Main Mode Filter ID: %19	Windows Vista, Windows Server 2008

4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. Local Endpoint: Principal Name: %1 Network Address: %9 Keying Module Port: %10 Local Certificate: SHA Thumbprint: %2 Issuing CA: %3 Root CA: %4 Remote Endpoint: Principal Name: %5 Network Address: %11 Keying Module Port: %12 Remote Certificate: SHA Thumbprint: %6 Issuing CA: %7 Root CA: %8 Additional Information: Keying Module Name: AuthIP Authentication Method: SSL Role: %16 Impersonation State: %17 Quick Mode Filter ID: %18 Failure Information: Failure Point: %13 Failure Reason: %14 State: %15	Windows Vista, Windows Server 2008
4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. Local Endpoint: Principal Name: %1 Network Address: %3 Keying Module Port: %4 Remote Endpoint: Principal Name: %2 Network Address: %5 Keying Module Port: %6 Additional Information: Keying Module Name: AuthIP Authentication Method: %9 Role: %11 Impersonation State: %12 Quick Mode Filter ID: %13 Failure Information: Failure Point: %7 Failure Reason: %8 State: %10	Windows Vista, Windows Server 2008

4985	The state of a transaction has changed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Transaction Information: RM Transaction ID: %5 New State: %6 Resource Manager: %7 Process Information: Process ID: %8 Process Name: %9	Windows Vista, Windows Server 2008
5024	The Windows Firewall Service has started successfully.	Windows Vista, Windows Server 2008
5025	The Windows Firewall Service has been stopped.	Windows Vista, Windows Server 2008
5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy. Error Code: %1	Windows Vista, Windows Server 2008
5028	The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy. Error Code: %1	Windows Vista, Windows Server 2008
5029	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy. Error Code: %1	Windows Vista, Windows Server 2008
5030	The Windows Firewall Service failed to start. Error Code: %1	Windows Vista, Windows Server 2008
5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network. Profiles: %1 Application: %2	Windows Vista, Windows Server 2008
5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network. Error Code: %1	Windows Vista, Windows Server 2008
5033	The Windows Firewall Driver has started successfully.	Windows Vista, Windows Server 2008
5034	The Windows Firewall Driver has been stopped.	Windows Vista, Windows Server 2008
5035	The Windows Firewall Driver failed to start. Error Code: %1	Windows Vista, Windows Server 2008
5037	The Windows Firewall Driver detected critical runtime error. Terminating. Error Code: %1	Windows Vista, Windows Server 2008
5038	0x8000000000000000 message: Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error. File Name: %1	Windows Vista, Windows Server 2008

5039	A registry key was virtualized. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: Key Name: %5 Virtual Key Name: %6 Process Information: Process ID: %7 Process Name: %8	Windows Vista, Windows Server 2008
5040	A change has been made to IPsec settings. An Authentication Set was added. Profile Changed: %1 Added Authentication Set: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5041	A change has been made to IPsec settings. An Authentication Set was modified. Profile Changed: %1 Modified Authentication Set: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5042	A change has been made to IPsec settings. An Authentication Set was deleted. Profile Changed: %1 Deleted Authentication Set: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5043	A change has been made to IPsec settings. A Connection Security Rule was added. Profile Changed: %1 Added Connection Security Rule: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5044	A change has been made to IPsec settings. A Connection Security Rule was modified. Profile Changed: %1 Modified Connection Security Rule: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5045	A change has been made to IPsec settings. A Connection Security Rule was deleted. Profile Changed: %1 Deleted Connection Security Rule: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5046	A change has been made to IPsec settings. A Crypto Set was added. Profile Changed: %1 Added Crypto Set: ID: %2 Name: %3	Windows Vista, Windows Server 2008

5047	A change has been made to IPsec settings. A Crypto Set was modified. Profile Changed: %1 Modified Crypto Set: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5048	A change has been made to IPsec settings. A Crypto Set was deleted. Profile Changed: %1 Deleted Crypto Set: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5049	An IPsec Security Association was deleted. Profile Changed: %1 Deleted SA: ID: %2 Name: %3	Windows Vista, Windows Server 2008
5050	An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled(FALSE) interface was rejected because this API is not supported on Windows Vista. This has most likely occurred due to a program which is incompatible with Windows Vista. Please contact the program's manufacturer to make sure you have a Windows Vista compatible program version. Error Code: E_NOTIMPL Caller Process Name: %1 Process Id: %2 Publisher: %3	Windows Vista, Windows Server 2008
5051	A file was virtualized. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: File Name: %5 Virtual File Name: %6 Process Information: Process ID: %7 Process Name: %8	Windows Vista, Windows Server 2008
5056	A cryptographic self test was performed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Module: %5 Return Code: %6	Windows Vista, Windows Server 2008

5057	A cryptographic primitive operation failed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Cryptographic Parameters: Provider Name: %5 Algorithm Name: %6 Failure Information: Reason: %7 Return Code: %8	Windows Vista, Windows Server 2008
5058	Key file operation. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Cryptographic Parameters: Provider Name: %5 Algorithm Name: %6 Key Name: %7 Key Type: %8 Key File Operation Information: File Path: %9 Operation: %10 Return Code: %11	Windows Vista, Windows Server 2008
5059	Key migration operation. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Cryptographic Parameters: Provider Name: %5 Algorithm Name: %6 Key Name: %7 Key Type: %8 Additional Information: Operation: %9 Return Code: %10	Windows Vista, Windows Server 2008
5060	Verification operation failed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Cryptographic Parameters: Provider Name: %5 Algorithm Name: %6 Key Name: %7 Key Type: %8 Failure Information: Reason: %9 Return Code: %10	Windows Vista, Windows Server 2008

5061	Cryptographic operation. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Cryptographic Parameters: Provider Name: %5 Algorithm Name: %6 Key Name: %7 Key Type: %8 Cryptographic Operation: Operation: %9 Return Code: %10	Windows Vista, Windows Server 2008
5062	A kernel-mode cryptographic self test was performed. Module: %1 Return Code: %2	Windows Vista, Windows Server 2008
5063	A cryptographic provider operation was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Cryptographic Provider: Name: %5 Module: %6 Operation: %7 Return Code: %8	Windows Vista, Windows Server 2008
5064	A cryptographic context operation was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Configuration Parameters: Scope: %5 Context: %6 Operation: %7 Return Code: %8	Windows Vista, Windows Server 2008

5065	A cryptographic context modification was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 %Configuration Parameters: Scope: %5 Context: %6 Change Information: Old Value: %7 New Value: %8 Return Code: %9	Windows Vista, Windows Server 2008
5066	A cryptographic function operation was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Configuration Parameters: Scope: %5 Context: %6 Interface: %7 Function: %8 Position: %9 Operation: %10 Return Code: %11	Windows Vista, Windows Server 2008
5067	A cryptographic function modification was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Configuration Parameters: Scope: %5 Context: %6 Interface: %7 Function: %8 Change Information: Old Value: %9 New Value: %10 Return Code: %11	Windows Vista, Windows Server 2008

5068	A cryptographic function provider operation was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Configuration Parameters: Scope: %5 Context: %6 Interface: %7 Function: %8 Provider: %9 Position: %10 Operation: %11 Return Code: %12	Windows Vista, Windows Server 2008
5069	A cryptographic function property operation was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Configuration Parameters: Scope: %5 Context: %6 Interface: %7 Function: %8 Property: %9 Operation: %10 Value: %11 Return Code: %12	Windows Vista, Windows Server 2008
5070	A cryptographic function property modification was attempted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Configuration Parameters: Scope: %5 Context: %6 Interface: %7 Function: %8 Property: %9 Change Information: Old Value: %10 New Value: %11 Return Code: %12	Windows Vista, Windows Server 2008

5071	Key access denied by Microsoft key distribution service. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Security Descriptor: %5	Windows 8, Windows Server 2012
5120	OCSP Responder Service Started.	Windows Vista, Windows Server 2008
5121	OCSP Responder Service Stopped.	Windows Vista, Windows Server 2008
5122	A Configuration entry changed in the OCSP Responder Service. CA Configuration ID: %1 New Value: %2	Windows Vista, Windows Server 2008
5123	A configuration entry changed in the OCSP Responder Service. Property Name: %1 New Value: %2	Windows Vista, Windows Server 2008
5124	A security setting was updated on OCSP Responder Service. New Value: %1	Windows Vista, Windows Server 2008
5125	A request was submitted to OCSP Responder Service.	Windows Vista, Windows Server 2008
5125	A request was submitted to OCSP Responder Service. Certificate Serial Number: %1 Issuer CA Name: %2 Revocation Status: %3	Windows Vista, Windows Server 2008
5126	Signing Certificate was automatically updated by the OCSP Responder Service. CA Configuration ID: %1 New Signing Certificate Hash: %2	Windows Vista, Windows Server 2008
5127	The OCSP Revocation Provider successfully updated the revocation information. CA Configuration ID: %1 Base CRL Number: %2 Base CRL This Update: %3 Base CRL Hash: %4 Delta CRL Number: %5 Delta CRL Indicator: %6 Delta CRL This Update: %7 Delta CRL Hash: %8	Windows Vista, Windows Server 2008

5136	A directory service object was modified. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Directory Service: Name: %7 Type: %8 Object: DN: %9 GUID: %10 Class: %11 Attribute: LDAP Display Name: %12 Syntax (OID): %13 Value: %14 Operation: Type: %15 Correlation ID: %1 Application Correlation ID: %2	Windows Vista, Windows Server 2008
5137	A directory service object was created. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Directory Service: Name: %7 Type: %8 Object: DN: %9 GUID: %10 Class: %11 Operation: Correlation ID: %1 Application Correlation ID: %2	Windows Vista, Windows Server 2008
5138	A directory service object was undeleted. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Directory Service: Name: %7 Type: %8 Object: Old DN: %9 New DN: %10 GUID: %11 Class: %12 Operation: Correlation ID: %1 Application Correlation ID: %2	Windows Vista, Windows Server 2008

5139	A directory service object was moved. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Directory Service: Name: %7 Type: %8 Object: Old DN: %9 New DN: %10 GUID: %11 Class: %12 Operation: Correlation ID: %1 Application Correlation ID: %2	Windows Vista, Windows Server 2008
5140	A network share object was accessed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Network Information: Source Address: %5 Source Port: %6 Share Name: %7	Windows Vista, Windows Server 2008
5140	A network share object was accessed. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Network Information: Object Type: %5 Source Address: %6 Source Port: %7 Share Information: Share Name: %8 Share Path: %9 Access Request Information: Access Mask: %10 Accesses: %11	Windows Vista, Windows Server 2008

5141	A directory service object was deleted. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Directory Service: Name: %7 Type: %8 Object: DN: %9 GUID: %10 Class: %11 Operation: Tree Delete: %12 Correlation ID: %1 Application Correlation ID: %2	Windows Vista SP1, Windows Server 2008
5142	A network share object was added. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Share Information: Share Name: %5 Share Path: %6	Windows 7, Windows Server 2008 R2
5143	A network share object was modified. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Share Information: Object Type: %5 Share Name: %6 Share Path: %7 Old Remark: %8 New Remark: %9 Old MaxUsers: %10 New Maxusers: %11 Old ShareFlags: %12 New ShareFlags: %13 Old SD: %14 New SD: %15	Windows 7, Windows Server 2008 R2
5144	A network share object was deleted. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Share Information: Share Name: %5 Share Path: %6	Windows 7, Windows Server 2008 R2

5145	A network share object was checked to see whether client can be granted desired access. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Network Information: Object Type: %5 Source Address: %6 Source Port: %7 Share Information: Share Name: %8 Share Path: %9 Relative Target Name: %10 Access Request Information: Access Mask: %11 Accesses: %12 Access Check Results: %13	Windows 7, Windows Server 2008 R2
5146	The Windows Filtering Platform has blocked a packet. Network Information: Direction: %1 Source Address: %2 Destination Address: %3 EtherType: %4 VlanTag: %5 vSwitchId: %6 Source vSwitch Port: %7 Destination vSwitch Port: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows 8, Windows Server 2012
5147	A more restrictive Windows Filtering Platform filter has blocked a packet. Network Information: Direction: %1 Source Address: %2 Destination Address: %3 EtherType: %4 VlanTag: %5 vSwitchId: %6 Source vSwitch Port: %7 Destination vSwitch Port: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows 8, Windows Server 2012
5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded. Network Information: Type: %1	Windows 7, Windows Server 2008 R2
5149	The DoS attack has subsided and normal processing is being resumed. Network Information: Type:%1 Packets Discarded: %2"	Windows 7, Windows Server 2008 R2

5150	The Windows Filtering Platform has blocked a packet. Network Information: Direction: %1 Source Address: %2 Destination Address: %3 EtherType: %4 EncapMethod: %5 SnapControl: %6 SnapOui: %7 VlanTag: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows 7, Windows Server 2008 R2
5151	A more restrictive Windows Filtering Platform filter has blocked a packet. Network Information: Direction: %1 Source Address:%2 Destination Address: %3 EtherType: %4 EncapMethod: %5 SnapControl: %6 SnapOui: %7 VlanTag: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows 7, Windows Server 2008 R2
5152	The Windows Filtering Platform blocked a packet. Application Information: Process ID: %1 Application Name: %2 Network Information: Direction: %3 Source Address: %4 Source Port: %5 Destination Address: %6 Destination Port: %7 Protocol: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows Vista, Windows Server 2008

5153	A more restrictive Windows Filtering Platform filter has blocked a packet. Application Information: Process ID: %1 Application Name: %2 Network Information: Direction: %3 Source Address: %4 Source Port: %5 Destination Address: %6 Destination Port: %7 Protocol: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows Vista, Windows Server 2008
5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections. Application Information: Process ID: %1 Application Name: %2 Network Information: Source Address: %3 Source Port: %4 Protocol: %5 Filter Information: Filter Run-Time ID: %6 Layer Name: %7 Layer Run-Time ID: %8	Windows Vista, Windows Server 2008
5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections. Application Information: Process ID: %1 Application Name: %2 Network Information: Source Address: %3 Source Port: %4 Protocol: %5 Filter Information: Filter Run-Time ID: %6 Layer Name: %7 Layer Run-Time ID: %8	Windows Vista, Windows Server 2008

5156	The Windows Filtering Platform has permitted a connection. Application Information: Process ID: %1 Application Name: %2 Network Information: Direction: %3 Source Address: %4 Source Port: %5 Destination Address: %6 Destination Port: %7 Protocol: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows Vista, Windows Server 2008
5156	The Windows Filtering Platform has permitted a connection. Application Information: Process ID: %1 Application Name: %2 Network Information: Direction: %3 Source Address: %4 Source Port: %5 Destination Address: %6 Destination Port: %7 Protocol: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows 7, Windows Server 2008 R2
5157	The Windows Filtering Platform has blocked a connection. Application Information: Process ID: %1 Application Name: %2 Network Information: Direction: %3 Source Address: %4 Source Port: %5 Destination Address: %6 Destination Port: %7 Protocol: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows Vista, Windows Server 2008

5157	The Windows Filtering Platform has blocked a connection. Application Information: Process ID: %1 Application Name: %2 Network Information: Direction: %3 Source Address: %4 Source Port: %5 Destination Address: %6 Destination Port: %7 Protocol: %8 Filter Information: Filter Run-Time ID: %9 Layer Name: %10 Layer Run-Time ID: %11	Windows 7, Windows Server 2008 R2
5158	The Windows Filtering Platform has permitted a bind to a local port. Application Information: Process ID: %1 Application Name: %2 Network Information: Source Address: %3 Source Port: %4 Protocol: %5 Filter Information: Filter Run-Time ID: %6 Layer Name: %7 Layer Run-Time ID: %8	Windows Vista, Windows Server 2008
5159	The Windows Filtering Platform has blocked a bind to a local port. Application Information: Process ID: %1 Application Name: %2 Network Information: Source Address: %3 Source Port: %4 Protocol: %5 Filter Information: Filter Run-Time ID: %6 Layer Name: %7 Layer Run-Time ID: %8	Windows Vista, Windows Server 2008
5168	SPN check for SMB/SMB2 fails. Subject Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 SPN: SPN Name: %5 Error Code: %6 Server Information: Server Names: %7 Configured Names %8 IP Addresses: %9	Windows 7, Windows Server 2008 R2

5169	A directory service object was modified. Subject: Security ID: %3 Account Name: %4 Account Domain: %5 Logon ID: %6 Directory Service: Name: %7 Type: %8 Object: DN: %9 GUID: %10 Class: %11 Attribute: LDAP Display Name: %12 Syntax (OID): %13 Value: %14 Expiration Time: %15 Operation: Type: %16 Correlation ID: %1 Application Correlation ID: %2	Windows 10
5376	Credential Manager credentials were backed up. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 This event occurs when a user backs up their own Credential Manager credentials. A user (even an Administrator) cannot back up the credentials of an account other than his own.	Windows Vista, Windows Server 2008
5377	Credential Manager credentials were restored from a backup. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 This event occurs when a user restores his Credential Manager credentials from a backup. A user (even an Administrator) cannot restore the credentials of an account other than his own.	Windows Vista, Windows Server 2008
5378	The requested credentials delegation was disallowed by policy. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Credential Delegation Information: Security Package: %5 User's UPN: %6 Target Server: %7 Credential Type: %8	Windows Vista, Windows Server 2008

5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started. Provider Information: ID: %1 Name: %2 Callout Information: ID: %3 Name: %4 Type: %5 Run-Time ID: %6 Layer Information: ID: %7 Name: %8 Run-Time ID: %9	Windows Vista, Windows Server 2008
5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started. Provider Information: ID: %1 Name: %2 Filter Information: ID: %3 Name: %4 Type: %5 Run-Time ID: %6 Layer Information: ID: %7 Name: %8 Run-Time ID: %9 Weight: %10 Additional Information: Conditions: %11 Filter Action: %12 Callout ID: %13 Callout Name: %14	Windows Vista, Windows Server 2008
5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started. Provider ID: %1 Provider Name: %2 Provider Type: %3	Windows Vista, Windows Server 2008
5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started. Provider ID: %1 Provider Name: %2 Provider Context ID: %3 Provider Context Name: %4 Provider Context Type: %5	Windows Vista, Windows Server 2008
5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started. Provider ID: %1 Provider Name: %2 Sub-layer ID: %3 Sub-layer Name: %4 Sub-layer Type: %5 Weight: %6	Windows Vista, Windows Server 2008

5446	A Windows Filtering Platform callout has been changed. Subject: Security ID: %2 Account Name: %3 Process Information: Process ID: %1 Provider Information: ID: %4 Name: %5 Change Information: Change Type: %6 Callout Information: ID: %7 Name: %8 Type: %9 Run-Time ID: %10 Layer Information: ID: %11 Name: %12 Run-Time ID: %13	Windows Vista, Windows Server 2008
5447	A Windows Filtering Platform filter has been changed. Subject: Security ID: %2 Account Name: %3 Process Information: Process ID: %1 Provider Information: ID: %4 Name: %5 Change Information: Change Type: %6 Filter Information: ID: %7 Name: %8 Type: %9 Run-Time ID: %10 Layer Information: ID: %11 Name: %12 Run-Time ID: %13 Callout Information: ID: %17 Name: %18 Additional Information: Weight: %14 Conditions: %15 Filter Action: %16	Windows Vista, Windows Server 2008

5448	A Windows Filtering Platform provider has been changed. Subject: Security ID: %2 Account Name: %3 Process Information: Process ID: %1 Change Information: Change Type: %4 Provider Information: ID: %5 Name: %6 Type: %7	Windows Vista, Windows Server 2008
5449	A Windows Filtering Platform provider context has been changed. Subject: Security ID: %2 Account Name: %3 Process Information: Process ID: %1 Provider Information: Provider ID: %4 Provider Name: %5 Change Information: Change Type: %6 Provider Context: ID: %7 Name: %8 Type: %9	Windows Vista, Windows Server 2008
5450	A Windows Filtering Platform sub-layer has been changed. Subject: Security ID: %2 Account Name: %3 Process Information: Process ID: %1 Provider Information: Provider ID: %4 Provider Name: %5 Change Information: Change Type: %6 Sub-layer Information: Sub-layer ID: %7 Sub-layer Name: %8 Sub-layer Type: %9 Additional Information: Weight: %10	Windows Vista, Windows Server 2008

5451	An IPsec quick mode security association was established. Local Endpoint: Network Address: %1 Network Address mask: %2 Port: %3 Tunnel Endpoint: %4 Remote Endpoint: Network Address: %5 Network Address Mask: %6 Port: %7 Private Address: %8 Tunnel Endpoint: %9 Protocol: %10 Keying Module Name: %11 Cryptographic Information: Integrity Algorithm - AH: %12 Integrity Algorithm - ESP: %13 Encryption Algorithm: %14 Security Association Information: Lifetime - seconds: %15 Lifetime - data: %16 Lifetime - packets: %17 Mode: %18 Role: %19 Quick Mode Filter ID: %20 Main Mode SA ID: %21 Quick Mode SA ID: %22 Additional Information: Inbound SPI: %23 Outbound SPI: %24	Windows Vista, Windows Server 2008

5451	An IPsec quick mode security association was established. Local Endpoint: Network Address: %1 Network Address mask: %2 Port: %3 Tunnel Endpoint: %4 Remote Endpoint: Network Address: %5 Network Address Mask: %6 Port: %7 Private Address: %8 Tunnel Endpoint: %9 Protocol: %10 Keying Module Name: %11 Cryptographic Information: Integrity Algorithm - AH: %12 Integrity Algorithm - ESP: %13 Encryption Algorithm: %14 Security Association Information: Lifetime - seconds: %15 Lifetime - data: %16 Lifetime - packets: %17 Mode: %18 Role: %19 Quick Mode Filter ID: %20 Main Mode SA ID: %21 Quick Mode SA ID: %22 Additional Information: Inbound SPI: %23 Outbound SPI: %24 Virtual Interface Tunnel ID: %25 Traffic Selector ID: %26	Windows Vista, Windows Server 2008
5452	An IPsec quick mode security association ended. Local Endpoint: Network Address: %1 Port: %2 Tunnel Endpoint: %3 Remote Endpoint: Network Address: %4 Port: %5 Tunnel Endpoint: %6 Additional Information: Protocol: %7 Quick Mode SA ID: %8	Windows Vista, Windows Server 2008

5452	An IPsec quick mode security association ended. Local Endpoint: Network Address: %1 Network Address mask: %2 Port: %3 Tunnel Endpoint: %4 Remote Endpoint: Network Address: %5 Network Address mask: %6 Port: %7 Tunnel Endpoint: %8 Additional Information: Protocol: %9 Quick Mode SA ID: %10 Virtual Interface Tunnel ID: %11 Traffic Selector ID: %12	Windows 7, Windows Server 2008 R2
5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.	Windows Vista, Windows Server 2008
5456	PAStore Engine applied Active Directory storage IPsec policy on the computer. Policy: %1	Windows Vista, Windows Server 2008
5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. DN: %1 Error code: %2	Windows Vista, Windows Server 2008
5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. Policy: %1	Windows Vista, Windows Server 2008
5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. Policy: %1 Error Code: %2	Windows Vista, Windows Server 2008
5460	PAStore Engine applied local registry storage IPsec policy on the computer. Policy: %1	Windows Vista, Windows Server 2008
5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer. Policy: %1 Error Code: %2	Windows Vista, Windows Server 2008
5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem. Policy: %1 Error Code: %2	Windows Vista, Windows Server 2008
5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes.	Windows Vista, Windows Server 2008
5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.	Windows Vista, Windows Server 2008
5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.	Windows Vista, Windows Server 2008
5466	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.	Windows Vista, Windows Server 2008
5467	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.	Windows Vista, Windows Server 2008

5468	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.	Windows Vista, Windows Server 2008
5471	PAStore Engine loaded local storage IPsec policy on the computer. Policy: %1	Windows Vista, Windows Server 2008
5472	PAStore Engine failed to load local storage IPsec policy on the computer. Policy: %1 Error Code: %2	Windows Vista, Windows Server 2008
5473	PAStore Engine loaded directory storage IPsec policy on the computer. Policy: %1	Windows Vista, Windows Server 2008
5474	PAStore Engine failed to load directory storage IPsec policy on the computer. Policy: %1 Error Code: %2	Windows Vista, Windows Server 2008
5477	PAStore Engine failed to add quick mode filter. Quick Mode Filter: %1 Error Code: %2	Windows Vista, Windows Server 2008
5478	IPsec Services has started successfully.	Windows Vista, Windows Server 2008
5479	IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.	Windows Vista, Windows Server 2008
5480	IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.	Windows Vista, Windows Server 2008
5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started. Error Code: %1	Windows Vista, Windows Server 2008
5484	IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. Error Code: %1	Windows Vista, Windows Server 2008
5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.	Windows Vista, Windows Server 2008
5632	A request was made to authenticate to a wireless network. Subject: Security ID: %2 Account Name: %3 Account Domain: %4 Logon ID: %5 Network Information: Name (SSID): %1 Interface GUID: %8 Local MAC Address: %7 Peer MAC Address: %6 Additional Information: Reason Code: %10 (%9) Error Code: %11 Note: EAP Reason Code, EAP Root Cause String, and EAP Error Code data is logged only on computers running Windows Server 2008 R2 or Windows 7.	Windows Vista, Windows Server 2008

5632	A request was made to authenticate to a wireless network. Subject: Security ID: %2 Account Name: %3 Account Domain: %4 Logon ID: %5 Network Information: Name (SSID): %1 Interface GUID: %8 Local MAC Address: %7 Peer MAC Address: %6 Additional Information: Reason Code: %10 (%9) Error Code: %11 EAP Reason Code: %12 EAP Root Cause String: %13 EAP Error Code: %14 Note: EAP Reason Code, EAP Root Cause String, and EAP Error Code data is logged only on computers running Windows Server 2008 R2 or Windows 7.	Windows Vista, Windows Server 2008
5633	A request was made to authenticate to a wired network. Subject: Security ID: %2 Account Name: %3 Account Domain: %4 Logon ID: %5 Interface: Name: %1 Additional Information Reason Code: %7 (%6) Error Code: %8	Windows Vista, Windows Server 2008
5712	A Remote Procedure Call (RPC) was attempted. Subject: SID: %1 Name: %2 Account Domain: %3 LogonId: %4 Process Information: PID: %5 Name: %6 Network Information: Remote IP Address: %7 Remote Port: %8 RPC Attributes: Interface UUID: %9 Protocol Sequence: %10 Authentication Service: %11 Authentication Level: %12	Windows Vista, Windows Server 2008

5888	An object in the COM+ Catalog was modified. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: COM+ Catalog Collection: %5 Object Name: %6 Object Properties Modified: %7	Windows Vista, Windows Server 2008
5889	An object was deleted from the COM+ Catalog. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: COM+ Catalog Collection: %5 Object Name: %6 Object Details: %7 This event occurs when an object is deleted from the COM+ catalog.	Windows Vista, Windows Server 2008
5890	An object was added to the COM+ Catalog. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Object: COM+ Catalog Collection: %5 Object Name: %6 Object Details: %7	Windows Vista, Windows Server 2008
6144	Security policy in the group policy objects has been applied successfully. Return Code: %1 GPO List: %2	Windows Vista, Windows Server 2008
6145	One or more errors occured while processing security policy in the group policy objects. Error Code: %1 GPO List: %2	Windows Vista, Windows Server 2008

6272	Network Policy Server granted access to a user. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Proxy Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Quarantine Information: Result: %25 Session Identifier: %26	Windows Vista SP1, Windows Server 2008

6272	Network Policy Server granted access to a user. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Connection Request Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Logging Results: %27 Quarantine Information: Result: %25	Windows 7, Windows Server 2008 R2

6272	Network Policy Server granted access to a user. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 Called Station Identifier: %8 Calling Station Identifier: %9 NAS: NAS IPv4 Address: %10 NAS IPv6 Address: %11 NAS Identifier: %12 NAS Port-Type: %13 NAS Port: %14 RADIUS Client: Client Friendly Name: %15 Client IP Address: %16 Authentication Details: Connection Request Policy Name: %17 Network Policy Name: %18 Authentication Provider: %19 Authentication Server: %20 Authentication Type: %21 EAP Type: %22 Account Session Identifier: %23 Logging Results: %24 Note: Logging Results data is only logged on computers running Windows 7 and Windows Server 2008 R2.	Windows 10

6273	Network Policy Server denied access to a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Proxy Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Reason Code: %25 Reason: %26	Windows Vista SP1, Windows Server 2008

6273	Network Policy Server denied access to a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Connection Request Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Logging Results: %27 Reason Code: %25	Windows 7, Windows Server 2008 R2

6273	Network Policy Server denied access to a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 Called Station Identifier: %8 Calling Station Identifier: %9 NAS: NAS IPv4 Address: %10 NAS IPv6 Address: %11 NAS Identifier: %12 NAS Port-Type: %13 NAS Port: %14 RADIUS Client: Client Friendly Name: %15 Client IP Address: %16 Authentication Details: Connection Request Policy Name: %17 Network Policy Name: %18 Authentication Provider: %19 Authentication Server: %20 Authentication Type: %21 EAP Type: %22 Account Session Identifier: %23 Logging Results: %26 Reason Code: %24 Reason: %25	Windows 10

6274	Network Policy Server discarded the request for a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Connection Request Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Reason Code: %25 Reason: %26	Windows Vista SP1, Windows Server 2008

6274	Network Policy Server discarded the request for a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 Called Station Identifier: %8 Calling Station Identifier: %9 NAS: NAS IPv4 Address: %10 NAS IPv6 Address: %11 NAS Identifier: %12 NAS Port-Type: %13 NAS Port: %14 RADIUS Client: Client Friendly Name: %15 Client IP Address: %16 Authentication Details: Connection Request Policy Name: %17 Network Policy Name: %18 Authentication Provider: %19 Authentication Server: %20 Authentication Type: %21 EAP Type: %22 Account Session Identifier: %23 Reason Code: %24 Reason: %25	Windows 10

6275	Network Policy Server discarded the accounting request for a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Connection Request Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Reason Code: %25 Reason: %26	Windows Vista SP1, Windows Server 2008

6275	Network Policy Server discarded the accounting request for a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 Called Station Identifier: %8 Calling Station Identifier: %9 NAS: NAS IPv4 Address: %10 NAS IPv6 Address: %11 NAS Identifier: %12 NAS Port-Type: %13 NAS Port: %14 RADIUS Client: Client Friendly Name: %15 Client IP Address: %16 Authentication Details: Connection Request Policy Name: %17 Network Policy Name: %18 Authentication Provider: %19 Authentication Server: %20 Authentication Type: %21 EAP Type: %22 Account Session Identifier: %23 Reason Code: %24 Reason: %25	Windows 10

6276	Network Policy Server quarantined a user. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Proxy Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Quarantine Information:	Windows Vista SP1, Windows Server 2008

6277	0x8000000000000000 message: Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy. Contact the Network Policy Server administrator for more information. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Proxy Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24	Windows Vista SP1, Windows Server 2008

6278	Network Policy Server granted full access to a user because the host met the defined health policy. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4 Client Machine: Security ID: %5 Account Name: %6 Fully Qualified Account Name: %7 OS-Version: %8 Called Station Identifier: %9 Calling Station Identifier: %10 NAS: NAS IPv4 Address: %11 NAS IPv6 Address: %12 NAS Identifier: %13 NAS Port-Type: %14 NAS Port: %15 RADIUS Client: Client Friendly Name: %16 Client IP Address: %17 Authentication Details: Proxy Policy Name: %18 Network Policy Name: %19 Authentication Provider: %20 Authentication Server: %21 Authentication Type: %22 EAP Type: %23 Account Session Identifier: %24 Quarantine Information: Result: %25	Windows Vista SP1, Windows Server 2008
6279	Network Policy Server locked the user account due to repeated failed authentication attempts. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4	Windows Vista SP1, Windows Server 2008
6280	Network Policy Server unlocked the user account. User: Security ID: %1 Account Name: %2 Account Domain: %3 Fully Qualified Account Name: %4	Windows Vista SP1, Windows Server 2008
6281	Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error File Name: %1	Windows 7, Windows Server 2008 R2
6400	BranchCache: Received an incorrectly formatted response while discovering availability of content. IP address of the client that sent this response: %1	Windows 7, Windows Server 2008 R2
6401	BranchCache: Received invalid data from a peer. Data discarded. IP address of the client that sent this data: %1	Windows 7, Windows Server 2008 R2

6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted. IP address of the client that sent this data: %1	Windows 7, Windows Server 2008 R2
6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client's message to offer it data. Domain name of the hosted cache: %1	Windows 7, Windows Server 2008 R2
6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate. Domain name of the hosted cache: %1	Windows 7, Windows Server 2008 R2
6405	BranchCache: %2 instance(s) of event id %1 occurred Event ID: %1 Number of instances: %2	Windows 7, Windows Server 2008 R2
6406	%1 registered to Windows Firewall to control filtering for the following: %2. Firewall category: %1	Windows 7, Windows Server 2008 R2
6407	Firewall category unregistered: %1	Windows 7, Windows Server 2008 R2
6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2. Firewall category: %1	Windows 7, Windows Server 2008 R2
6409	BranchCache: A service connection point object could not be parsed. SCP object GUID: %1	Windows 8.1, Windows Server 2012 R2
6410	Code integrity determined that a file does not meet the security requirements to load into a process. This could be due to the use of shared sections or other issues. File Name: %1	Windows 8.1, Windows Server 2012 R2
6416	A new external device was recognized by the system. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Class ID: %5 Vendor IDs: %6 Compatible IDs: %7 Location Information: %8	Windows 10

6416	A new external device was recognized by the system. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Device ID: %5 Device Name: %6 Class ID: %7 Class Name: %8 Vendor IDs: %9 Compatible IDs: %10 Location Information: %11	Windows 10 [Version 1511]
6417	The FIPS mode crypto selftests succeeded. Process ID: %1 Process Name: %2	Windows 10 [Version 1511]
6418	The FIPS mode crypto selftests failed. Process ID: %1 Process Name: %2 Failed test code: %3	Windows 10 [Version 1511]
6419	A request was made to disable a device. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Device ID: %5 Device Name: %6 Class ID: %7 Class Name: %8 Hardware IDs: %9 Compatible IDs: %10 Location Information: %11	Windows 10 [Version 1511]

6420	A device was disabled. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Device ID: %5 Device Name: %6 Class ID: %7 Class Name: %8 Hardware IDs: %9 Compatible IDs: %10 Location Information: %11	Windows 10 [Version 1511]
6421	A request was made to enable a device. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Device ID: %5 Device Name: %6 Class ID: %7 Class Name: %8 Hardware IDs: %9 Compatible IDs: %10 Location Information: %11	Windows 10 [Version 1511]
6422	A device was enabled. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Device ID: %5 Device Name: %6 Class ID: %7 Class Name: %8 Hardware IDs: %9 Compatible IDs: %10 Location Information: %11	Windows 10 [Version 1511]

6423	The installation of this device is forbidden by system policy. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Device ID: %5 Device Name: %6 Class ID: %7 Class Name: %8 Hardware IDs: %9 Compatible IDs: %10 Location Information: %11	Windows 10 [Version 1511]
6424	The installation of this device was allowed, after having previously been forbidden by policy. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Device ID: %5 Device Name: %6 Class ID: %7 Class Name: %8 Hardware IDs: %9 Compatible IDs: %10 Location Information: %11	Windows 10 [Version 1511]
8191	Highest System-Defined Audit Message Value.	N/A