Category	Subcategory	Event ID	Message Summary
System	Security State Change	4608	Windows is starting up.
System	Security State Change	4609	Windows is shutting down.
System	Security System Extension	4610	An authentication package has been loaded by the Local Security Authority.
System	Security System Extension	4611	A trusted logon process has been registered with the Local Security Authority.
System	System Integrity	4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
System	Security System Extension	4614	A notification package has been loaded by the Security Account Manager.
System	System Integrity	4615	Invalid use of LPC port.
System	Security State Change	4616	The system time was changed.
System	System Integrity	4618	A monitored security event pattern has occurred.
System	Security State Change	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.
System	Security System Extension	4622	A security package has been loaded by the Local Security Authority.
Logon/Logoff	Logon	4624	An account was successfully logged on.
Logon/Logoff	Logon	4625	An account failed to log on.
Logon/Logoff	Logon	4626	User/Device claims information.
Logon/Logoff	Group Membership	4627	Group membership information.
Logon/Logoff	Logoff	4634	An account was logged off.
Logon/Logoff	IPsec Main Mode	4646	%1
Logon/Logoff	Logoff	4647	User initiated logoff.
Logon/Logoff	Logon	4648	A logon was attempted using explicit credentials.
Logon/Logoff	Other Logon/Logoff Events	4649	A replay attack was detected.
Logon/Logoff	IPsec Main Mode	4650	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
Logon/Logoff	IPsec Main Mode	4651	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
Logon/Logoff	IPsec Main Mode	4652	An IPsec Main Mode negotiation failed.
Logon/Logoff	IPsec Main Mode	4653	An IPsec Main Mode negotiation failed.
Logon/Logoff	IPsec Quick Mode	4654	An IPsec Quick Mode negotiation failed.
Logon/Logoff	IPsec Main Mode	4655	An IPsec Main Mode security association ended.
Object Access	Handle Manipulation	4656	A handle to an object was requested.
Object Access	Registry	4657	A registry value was modified.
Object Access	Handle Manipulation	4658	The handle to an object was closed.
Object Access	SAM	4659	A handle to an object was requested with intent to delete.
Object Access	Kernel	4659	A handle to an object was requested with intent to delete.
Object Access	SAM	4660	An object was deleted.
Object Access	Kernel	4660	An object was deleted.
Object Access	SAM	4661	A handle to an object was requested.
Object Access	Kernel	4661	A handle to an object was requested.
DS Access	Directory Service Access	4662	An operation was performed on an object.
Object Access	SAM	4663	An attempt was made to access an object.
Object Access	Kernel	4663	An attempt was made to access an object.
Object Access	File System	4664	An attempt was made to create a hard link.
Object Access	Application Generated	4665	An attempt was made to create an application client context.
Object Access	Application Generated	4666	An application attempted an operation:
Object Access	Application Generated	4667	An application client context was deleted.

Object Access	Application Generated	4668	An application was initialized.
Policy Change	Subcategory (special)	4670	Permissions on an object were changed.
Object Access	Other Object Access Events	4671	An application attempted to access a blocked ordinal through the TBS.
Privilege Use	Sensitive Privilege Use / Non Sensitive Privilege Use	4672	Special privileges assigned to new logon.
Privilege Use	Sensitive Privilege Use / Non Sensitive Privilege Use	4673	A privileged service was called.
Privilege Use	Sensitive Privilege Use / Non Sensitive Privilege Use	4674	An operation was attempted on a privileged object.
Logon/Logoff	Logon	4675	SIDs were filtered.
Detailed Tracking	Process Creation	4688	A new process has been created.
Detailed Tracking	Process Termination	4689	A process has exited.
Object Access	Handle Manipulation	4690	An attempt was made to duplicate a handle to an object.
Object Access	Other Object Access Events	4691	Indirect access to an object was requested.
Detailed Tracking	DPAPI Activity	4692	Backup of data protection master key was attempted.
Detailed Tracking	DPAPI Activity	4693	Recovery of data protection master key was attempted.
Detailed Tracking	DPAPI Activity	4694	Protection of auditable protected data was attempted.
Detailed Tracking	DPAPI Activity	4695	Unprotection of auditable protected data was attempted.
Detailed Tracking	Process Creation	4696	A primary token was assigned to process.
System	Security System Extension	4697	A service was installed in the system.
Object Access	Other Object Access Events	4698	A scheduled task was created.
Object Access	Other Object Access Events	4699	A scheduled task was deleted.
Object Access	Other Object Access Events	4700	A scheduled task was enabled.
Object Access	Other Object Access Events	4701	A scheduled task was disabled.
Object Access	Other Object Access Events	4702	A scheduled task was updated.
Policy Change	Authorization Policy Change	4703	A user right was adjusted.
Policy Change	Authorization Policy Change	4704	A user right was assigned.
Policy Change	Authorization Policy Change	4705	A user right was removed.
Policy Change	Authorization Policy Change	4706	A new trust was created to a domain.
Policy Change	Authorization Policy Change	4707	A trust to a domain was removed.
Policy Change	Filtering Platform Policy Change	4709	IPsec Services was started.
Policy Change	Filtering Platform Policy Change	4710	IPsec Services was disabled.
Policy Change	Filtering Platform Policy Change	4711	May contain any one of the following: PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine applied Active Directory storage IPsec policy on the computer. PAStore Engine applied local registry storage IPsec policy on the computer. PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply local registry storage IPsec policy on the computer. PAStore Engine failed to apply some rules of the active IPsec policy on the computer. PAStore Engine failed to load directory storage IPsec policy on the computer. PAStore Engine loaded directory storage IPsec policy on the computer. PAStore Engine failed to load local storage IPsec policy on the computer. PAStore Engine loaded local storage IPsec policy on the computer. PAStore Engine polled for changes to the active IPsec policy and detected no changes.
Policy Change	Filtering Platform Policy Change	4712	IPsec Services encountered a potentially serious failure.

Policy Change	Authentication Policy Change	4713	Kerberos policy was changed.
Policy Change	Authorization Policy Change	4714	Encrypted data recovery policy was changed.
Policy Change	Audit Policy Change	4715	The audit policy (SACL) on an object was changed.
Policy Change	Authentication Policy Change	4716	Trusted domain information was modified.
Policy Change	Authentication Policy Change	4717	System security access was granted to an account.
Policy Change	Authentication Policy Change	4718	System security access was removed from an account.
Policy Change	Audit Policy Change	4719	System audit policy was changed.
Account Management	User Account Management	4720	A user account was created.
Account Management	User Account Management	4722	A user account was enabled.
Account Management	User Account Management	4723	An attempt was made to change an account's password.
Account Management	User Account Management	4724	An attempt was made to reset an account's password.
Account Management	User Account Management	4725	A user account was disabled.
Account Management	User Account Management	4726	A user account was deleted.
Account Management	Security Group Management	4727	A security-enabled global group was created.
Account Management	Security Group Management	4728	A member was added to a security-enabled global group.
Account Management	Security Group Management	4729	A member was removed from a security-enabled global group.
Account Management	Security Group Management	4730	A security-enabled global group was deleted.
Account Management	Security Group Management	4731	A security-enabled local group was created.
Account Management	Security Group Management	4732	A member was added to a security-enabled local group.
Account Management	Security Group Management	4733	A member was removed from a security-enabled local group.
Account Management	Security Group Management	4734	A security-enabled local group was deleted.
Account Management	Security Group Management	4735	A security-enabled local group was changed.
Account Management	Security Group Management	4737	A security-enabled global group was changed.
Account Management	User Account Management	4738	A user account was changed.
Policy Change	Authentication Policy Change	4739	Domain Policy was changed.
Account Management	User Account Management	4740	A user account was locked out.
Account Management	Computer Account Management	4742	A computer account was changed.
Account Management	Computer Account Management	4743	A computer account was deleted.
Account Management	Distribution Group Management	4744	A security-disabled local group was created.
Account Management	Distribution Group Management	4745	A security-disabled local group was changed.
Account Management	Distribution Group Management	4746	A member was added to a security-disabled local group.
Account Management	Distribution Group Management	4747	A member was removed from a security-disabled local group.
Account Management	Distribution Group Management	4748	A security-disabled local group was deleted.
Account Management	Distribution Group Management	4749	A security-disabled global group was created.
Account Management	Distribution Group Management	4750	A security-disabled global group was changed.
Account Management	Distribution Group Management	4751	A member was added to a security-disabled global group.
Account Management	Distribution Group Management	4752	A member was removed from a security-disabled global group.
Account Management	Distribution Group Management	4753	A security-disabled global group was deleted.
Account Management	Security Group Management	4754	A security-enabled universal group was created.
Account Management	Security Group Management	4755	A security-enabled universal group was changed.
Account Management	Security Group Management	4756	A member was added to a security-enabled universal group.
Account Management	Security Group Management	4757	A member was removed from a security-enabled universal group.
Account Management	Security Group Management	4758	A security-enabled universal group was deleted.
Account Management	Distribution Group Management	4759	A security-disabled universal group was created.
Account Management	Distribution Group Management	4760	A security-disabled universal group was changed.
Account Management	Distribution Group Management	4761	A member was added to a security-disabled universal group.

Account Management	Distribution Group Management	4762	A member was removed from a security-disabled universal group.
Account Management	Security Group Management	4764	A group's type was changed.
Account Management	User Account Management	4765	SID History was added to an account.
Account Management	User Account Management	4766	An attempt to add SID History to an account failed.
Account Management	User Account Management	4767	A user account was unlocked.
Account Logon	Kerberos Authentication Service	4768	A Kerberos authentication ticket (TGT) was requested.
Account Logon	Kerberos Service Ticket Operations	4769	A Kerberos service ticket was requested.
Account Logon	Kerberos Service Ticket Operations	4770	A Kerberos service ticket was renewed.
Account Logon	Kerberos Authentication Service	4771	Kerberos pre-authentication failed.
Account Logon	Kerberos Authentication Service	4772	A Kerberos authentication ticket request failed.
Account Logon	Kerberos Authentication Service	4773	A Kerberos service ticket request failed.
Account Logon	Credential Validation	4774	An account was mapped for logon.
Account Logon	Credential Validation	4775	An account could not be mapped for logon.
Account Logon	Credential Validation	4776	The domain controller attempted to validate the credentials for an account.
Account Logon	Credential Validation	4777	The domain controller failed to validate the credentials for an account.
Logon/Logoff	Other Logon/Logoff Events	4778	A session was reconnected to a Window Station.
Logon/Logoff	Other Logon/Logoff Events	4779	A session was disconnected from a Window Station.
Account Management	User Account Management	4780	The ACL was set on accounts which are members of administrators groups.
Account Management	User Account Management	4781	The name of an account was changed:
Account Management	Other Account Management Events	4782	The password hash an account was accessed.
Account Management	Application Group Management	4783	A basic application group was created.
Account Management	Application Group Management	4784	A basic application group was changed.
Account Management	Application Group Management	4785	A member was added to a basic application group.
Account Management	Application Group Management	4786	A member was removed from a basic application group.
Account Management	Application Group Management	4787	A non-member was added to a basic application group.
Account Management	Application Group Management	4788	A non-member was removed from a basic application group.
Account Management	Application Group Management	4789	A basic application group was deleted.
Account Management	Application Group Management	4790	An LDAP query group was created.
Account Management	Application Group Management	4791	A basic application group was changed.
Account Management	Application Group Management	4792	An LDAP query group was deleted.
Account Management	Other Account Management Events	4793	The Password Policy Checking API was called.
Account Management	User Account Management	4794	An attempt was made to set the Directory Services Restore Mode.
Account Management	User Account Management	4797	An attempt was made to query the existence of a blank password for an account.
Account Management	User Account Management	4798	A user's local group membership was enumerated.
Account Management	Security Group Management	4799	A security-enabled local group membership was enumerated.
Logon/Logoff	Other Logon/Logoff Events	4800	The workstation was locked.
Logon/Logoff	Other Logon/Logoff Events	4801	The workstation was unlocked.
Logon/Logoff	Other Logon/Logoff Events	4802	The screen saver was invoked.
Logon/Logoff	Other Logon/Logoff Events	4803	The screen saver was dismissed.
System	System Integrity	4816	RPC detected an integrity violation while decrypting an incoming message.
Policy Change	Audit Policy Change	4817	Auditing settings on an object were changed.
Object Access	Central Access Policy Staging	4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy
Policy Change	Other Policy Change Events	4819	Central Access Policies on the machine have been changed.
Account Logon	Kerberos Authentication Service	4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.
Account Logon	Kerberos Service Ticket Operations	4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.
Account Logon	Credential Validation	4822	NTLM authentication failed because the account was a member of the Protected User group.

Account Logon	Credential Validation	4823	NTLM authentication failed because access control restrictions are required.
Account Logon	Kerberos Authentication Service	4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.
Logon/Logoff	Other Logon/Logoff Events	4825	A user was denied the access to Remote Desktop.
Policy Change	Other Policy Change Events	4826	Boot Configuration Data loaded.
Policy Change	Authentication Policy Change	4864	A namespace collision was detected.
Policy Change	Authentication Policy Change	4865	A trusted forest information entry was added.
Policy Change	Authentication Policy Change	4866	A trusted forest information entry was removed.
Policy Change	Authentication Policy Change	4867	A trusted forest information entry was modified.
Object Access	Certification Services	4868	The certificate manager denied a pending certificate request.
Object Access	Certification Services	4869	Certificate Services received a resubmitted certificate request.
Object Access	Certification Services	4870	Certificate Services revoked a certificate.
Object Access	Certification Services	4871	Certificate Services received a request to publish the certificate revocation list (CRL).
Object Access	Certification Services	4872	Certificate Services published the certificate revocation list (CRL).
Object Access	Certification Services	4873	A certificate request extension changed.
Object Access	Certification Services	4874	One or more certificate request attributes changed.
Object Access	Certification Services	4875	Certificate Services received a request to shut down.
Object Access	Certification Services	4876	Certificate Services backup started.
Object Access	Certification Services	4877	Certificate Services backup completed.
Object Access	Certification Services	4878	Certificate Services restore started.
Object Access	Certification Services	4879	Certificate Services restore completed.
Object Access	Certification Services	4880	Certificate Services started.
Object Access	Certification Services	4881	Certificate Services stopped.
Object Access	Certification Services	4882	The security permissions for Certificate Services changed.
Object Access	Certification Services	4883	Certificate Services retrieved an archived key.
Object Access	Certification Services	4884	Certificate Services imported a certificate into its database.
Object Access	Certification Services	4885	The audit filter for Certificate Services changed.
Object Access	Certification Services	4886	Certificate Services received a certificate request.
Object Access	Certification Services	4887	Certificate Services approved a certificate request and issued a certificate.
Object Access	Certification Services	4888	Certificate Services denied a certificate request.
Object Access	Certification Services	4889	Certificate Services set the status of a certificate request to pending.
Object Access	Certification Services	4890	The certificate manager settings for Certificate Services changed.
Object Access	Certification Services	4891	A configuration entry changed in Certificate Services.
Object Access	Certification Services	4892	A property of Certificate Services changed.
Object Access	Certification Services	4893	Certificate Services archived a key.
Object Access	Certification Services	4894	Certificate Services imported and archived a key.
Object Access	Certification Services	4895	Certificate Services published the CA certificate to Active Directory Domain Services.
Object Access	Certification Services	4896	One or more rows have been deleted from the certificate database.
Object Access	Certification Services	4897	Role separation enabled:
Object Access	Certification Services	4898	Certificate Services loaded a template.
Object Access	Certification Services	4899	A Certificate Services template was updated.
Object Access	Certification Services	4900	Certificate Services template security was updated.
Policy Change	Audit Policy Change	4902	The Per-user audit policy table was created.
Policy Change	Audit Policy Change	4904	An attempt was made to register a security event source.
Policy Change	Audit Policy Change	4905	An attempt was made to unregister a security event source.
Policy Change	Audit Policy Change	4906	The CrashOnAuditFail value has changed.
Policy Change	Audit Policy Change	4907	Auditing settings on object were changed.

Policy Change	Audit Policy Change	4908	Special Groups Logon table modified.
Policy Change	Other Policy Change Events	4909	The local policy settings for the TBS were changed.
Policy Change	Other Policy Change Events	4910	The group policy settings for the TBS were changed.
Policy Change	Authorization Policy Change	4911	Resource attributes of the object were changed.
Policy Change	Audit Policy Change	4912	Per User Audit Policy was changed.
Policy Change	Authorization Policy Change	4913	Central Access Policy on the object was changed.
DS Access	Detailed Directory Service Replication	4928	An Active Directory replica source naming context was established.
DS Access	Detailed Directory Service Replication	4929	An Active Directory replica source naming context was removed.
DS Access	Detailed Directory Service Replication	4930	An Active Directory replica source naming context was modified.
DS Access	Detailed Directory Service Replication	4931	An Active Directory replica destination naming context was modified.
DS Access	Directory Service Replication	4932	Synchronization of a replica of an Active Directory naming context has begun.
DS Access	Directory Service Replication	4933	Synchronization of a replica of an Active Directory naming context has ended.
DS Access	Detailed Directory Service Replication	4934	Attributes of an Active Directory object were replicated.
DS Access	Detailed Directory Service Replication	4935	Replication failure begins.
DS Access	Detailed Directory Service Replication	4936	Replication failure ends.
DS Access	Detailed Directory Service Replication	4937	A lingering object was removed from a replica.
Policy Change	MPSSVC Rule-Level Policy Change	4944	The following policy was active when the Windows Firewall started.
Policy Change	MPSSVC Rule-Level Policy Change	4945	A rule was listed when the Windows Firewall started.
Policy Change	MPSSVC Rule-Level Policy Change	4946	A change has been made to Windows Firewall exception list. A rule was added.
Policy Change	MPSSVC Rule-Level Policy Change	4947	A change has been made to Windows Firewall exception list. A rule was modified.
Policy Change	MPSSVC Rule-Level Policy Change	4948	A change has been made to Windows Firewall exception list. A rule was deleted.
Policy Change	MPSSVC Rule-Level Policy Change	4949	Windows Firewall settings were restored to the default values.
Policy Change	MPSSVC Rule-Level Policy Change	4950	A Windows Firewall setting has changed.
Policy Change	MPSSVC Rule-Level Policy Change	4951	A rule has been ignored because its major version number was not recognized by Windows Firewall.
Policy Change	MPSSVC Rule-Level Policy Change	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.
Policy Change	MPSSVC Rule-Level Policy Change	4953	A rule has been ignored by Windows Firewall because it could not parse the rule.
Policy Change	MPSSVC Rule-Level Policy Change	4954	Windows Firewall Group Policy settings have changed. The new settings have been applied.
Policy Change	MPSSVC Rule-Level Policy Change	4956	Windows Firewall has changed the active profile.
Policy Change	MPSSVC Rule-Level Policy Change	4957	Windows Firewall did not apply the following rule:
Policy Change	MPSSVC Rule-Level Policy Change	4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:
System	IPsec Driver	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.
System	IPsec Driver	4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
System	IPsec Driver	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.
System	IPsec Driver	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.
Logon/Logoff	Special Logon	4964	Special groups have been assigned to a new logon.
System	IPsec Driver	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.

Logon/Logoff	IPsec Main Mode	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.
Logon/Logoff	IPsec Quick Mode	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.
Logon/Logoff	IPsec Extended Mode	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.
Logon/Logoff	IPsec Extended Mode	4979	IPsec Main Mode and Extended Mode security associations were established.
Logon/Logoff	IPsec Extended Mode	4980	IPsec Main Mode and Extended Mode security associations were established.
Logon/Logoff	IPsec Extended Mode	4981	IPsec Main Mode and Extended Mode security associations were established.
Logon/Logoff	IPsec Extended Mode	4982	IPsec Main Mode and Extended Mode security associations were established.
Logon/Logoff	IPsec Extended Mode	4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
Logon/Logoff	IPsec Extended Mode	4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
Object Access	File System	4985	The state of a transaction has changed.
System	Other System Events	5024	The Windows Firewall Service has started successfully.
System	Other System Events	5025	The Windows Firewall Service has been stopped.
System	Other System Events	5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
System	Other System Events	5028	The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
System	Other System Events	5029	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
System	Other System Events	5030	The Windows Firewall Service failed to start.
Object Access	Filtering Platform Connection	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
System	Other System Events	5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
System	Other System Events	5033	The Windows Firewall Driver has started successfully.
System	Other System Events	5034	The Windows Firewall Driver has been stopped.
System	Other System Events	5035	The Windows Firewall Driver failed to start.
System	Other System Events	5037	The Windows Firewall Driver detected critical runtime error. Terminating.
System	System Integrity	5038	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.
Object Access	Registry	5039	A registry key was virtualized.
Policy Change	Filtering Platform Policy Change	5040	A change has been made to IPsec settings. An Authentication Set was added.
Policy Change	Filtering Platform Policy Change	5041	A change has been made to IPsec settings. An Authentication Set was modified.
Policy Change	Filtering Platform Policy Change	5042	A change has been made to IPsec settings. An Authentication Set was deleted.
Policy Change	Filtering Platform Policy Change	5043	A change has been made to IPsec settings. A Connection Security Rule was added.
Policy Change	Filtering Platform Policy Change	5044	A change has been made to IPsec settings. A Connection Security Rule was modified.
Policy Change	Filtering Platform Policy Change	5045	A change has been made to IPsec settings. A Connection Security Rule was deleted.
Policy Change	Filtering Platform Policy Change	5046	A change has been made to IPsec settings. A Crypto Set was added.
Policy Change	Filtering Platform Policy Change	5047	A change has been made to IPsec settings. A Crypto Set was modified.
Policy Change	Filtering Platform Policy Change	5048	A change has been made to IPsec settings. A Crypto Set was deleted.
Logon/Logoff	IPsec Main Mode	5049	An IPsec Security Association was deleted.
System	Other System Events	5050	An attempt to programmatically disable the Windows Firewall was rejected because this API is not supported on Windows Vista.
Object Access	File System	5051	A file was virtualized.
System	System Integrity	5056	A cryptographic self test was performed.
System	System Integrity	5057	A cryptographic primitive operation failed.
System	Other System Events	5058	Key file operation.

System	Other System Events	5059	Key migration operation.
System	System Integrity	5060	Verification operation failed.
System	System Integrity	5061	Cryptographic operation.
System	System Integrity	5062	A kernel-mode cryptographic self test was performed.
Policy Change	Other Policy Change Events	5063	A cryptographic provider operation was attempted.
Policy Change	Other Policy Change Events	5064	A cryptographic context operation was attempted.
Policy Change	Other Policy Change Events	5065	A cryptographic context modification was attempted.
Policy Change	Other Policy Change Events	5066	A cryptographic function operation was attempted.
Policy Change	Other Policy Change Events	5067	A cryptographic function modification was attempted.
Policy Change	Other Policy Change Events	5068	A cryptographic function provider operation was attempted.
Policy Change	Other Policy Change Events	5069	A cryptographic function property operation was attempted.
Policy Change	Other Policy Change Events	5070	A cryptographic function property modification was attempted.
System	Other System Events	5071	Key access denied by Microsoft key distribution service.
Object Access	Certification Services	5120	OCSP Responder Service Started.
Object Access	Certification Services	5121	OCSP Responder Service Stopped.
Object Access	Certification Services	5122	A Configuration entry changed in the OCSP Responder Service.
Object Access	Certification Services	5123	A configuration entry changed in the OCSP Responder Service.
Object Access	Certification Services	5124	A security setting was updated on OCSP Responder Service.
Object Access	Certification Services	5125	A request was submitted to OCSP Responder Service.
Object Access	Certification Services	5126	Signing Certificate was automatically updated by the OCSP Responder Service.
Object Access	Certification Services	5127	The OCSP Revocation Provider successfully updated the revocation information.
DS Access	Directory Service Changes	5136	A directory service object was modified.
DS Access	Directory Service Changes	5137	A directory service object was created.
DS Access	Directory Service Changes	5138	A directory service object was undeleted.
DS Access	Directory Service Changes	5139	A directory service object was moved.
Object Access	File Share	5140	A network share object was accessed.
DS Access	Directory Service Changes	5141	A directory service object was deleted.
Object Access	File Share	5142	A network share object was added.
Object Access	File Share	5143	A network share object was modified.
Object Access	File Share	5144	A network share object was deleted.
Object Access	Detailed File Share	5145	A network share object was checked to see whether the client can be granted desired access.
Object Access	Filtering Platform Packet Drop	5146	The Windows Filtering Platform has blocked a packet.
Object Access	Filtering Platform Packet Drop	5147	A more restrictive Windows Filtering Platform filter has blocked a packet.
Object Access	Other Object Access Events	5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
Object Access	Other Object Access Events	5149	The DoS attack has subsided and normal processing is being resumed.
Object Access	Filtering Platform Connection	5150	The Windows Filtering Platform has blocked a packet.
Object Access	Filtering Platform Connection	5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
Object Access	Filtering Platform Packet Drop	5152	The Windows Filtering Platform blocked a packet.
Object Access	Filtering Platform Packet Drop	5153	A more restrictive Windows Filtering Platform filter has blocked a packet.
Object Access	Filtering Platform Connection	5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
Object Access	Filtering Platform Connection	5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
Object Access	Filtering Platform Connection	5156	The Windows Filtering Platform has allowed a connection.
Object Access	Filtering Platform Connection	5157	The Windows Filtering Platform has blocked a connection.
Object Access	Filtering Platform Connection	5158	The Windows Filtering Platform has permitted a bind to a local port.
Object Access	Filtering Platform Connection	5159	The Windows Filtering Platform has blocked a bind to a local port.

Object Access	File Share	5168	Spn check for SMB/SMB2 failed.
DS Access	Directory Service Access	5169	A directory service object was modified.
Account Management	User Account Management	5376	Credential Manager credentials were backed up.
Account Management	User Account Management	5377	Credential Manager credentials were restored from a backup.
Logon/Logoff	Other Logon/Logoff Events	5378	The requested credentials delegation was disallowed by policy.
Policy Change	Filtering Platform Policy Change	5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
Policy Change	Filtering Platform Policy Change	5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
Policy Change	Filtering Platform Policy Change	5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
Policy Change	Filtering Platform Policy Change	5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
Policy Change	Filtering Platform Policy Change	5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.
Policy Change	Filtering Platform Policy Change	5446	A Windows Filtering Platform callout has been changed.
Policy Change	Other Policy Change Events	5447	A Windows Filtering Platform filter has been changed.
Policy Change	Filtering Platform Policy Change	5448	A Windows Filtering Platform provider has been changed.
Policy Change	Filtering Platform Policy Change	5449	A Windows Filtering Platform provider context has been changed.
Policy Change	Filtering Platform Policy Change	5450	A Windows Filtering Platform sub-layer has been changed.
Logon/Logoff	IPsec Quick Mode	5451	An IPsec Quick Mode security association was established.
Logon/Logoff	IPsec Quick Mode	5452	An IPsec Quick Mode security association ended.
Logon/Logoff	IPsec Main Mode	5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.
Policy Change	Filtering Platform Policy Change	5456	PAStore Engine applied Active Directory storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5460	PAStore Engine applied local registry storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	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 Change	Filtering Platform Policy Change	5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes.
Policy Change	Filtering Platform Policy Change	5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.
Policy Change	Filtering Platform Policy Change	5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.
Policy Change	Filtering Platform Policy Change	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.
Policy Change	Filtering Platform Policy Change	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.
Policy Change	Filtering Platform Policy Change	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.
Policy Change	Filtering Platform Policy Change	5471	PAStore Engine loaded local storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5472	PAStore Engine failed to load local storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5473	PAStore Engine loaded directory storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5474	PAStore Engine failed to load directory storage IPsec policy on the computer.
Policy Change	Filtering Platform Policy Change	5477	PAStore Engine failed to add quick mode filter.
System	IPsec Driver	5478	IPsec Services has started successfully.
System	IPsec Driver	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.

System	IPsec Driver	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.
System	IPsec Driver	5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started.
System	IPsec Driver	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.
System	IPsec Driver	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.
Logon/Logoff	Other Logon/Logoff Events	5632	A request was made to authenticate to a wireless network.
Logon/Logoff	Other Logon/Logoff Events	5633	A request was made to authenticate to a wired network.
Detailed Tracking	RPC Events	5712	A Remote Procedure Call (RPC) was attempted.
Object Access	Other Object Access Events	5888	An object in the COM+ Catalog was modified.
Object Access	Other Object Access Events	5889	An object was deleted from the COM+ Catalog.
Object Access	Other Object Access Events	5890	An object was added to the COM+ Catalog.
Policy Change	Other Policy Change Events	6144	Security policy in the group policy objects has been applied successfully.
Policy Change	Other Policy Change Events	6145	One or more errors occurred while processing security policy in the group policy objects.
Logon/Logoff	Network Policy Server	6272	Network Policy Server granted access to a user.
Logon/Logoff	Network Policy Server	6273	Network Policy Server denied access to a user.
Logon/Logoff	Network Policy Server	6274	Network Policy Server discarded the request for a user.
Logon/Logoff	Network Policy Server	6275	Network Policy Server discarded the accounting request for a user.
Logon/Logoff	Network Policy Server	6276	Network Policy Server quarantined a user.
Logon/Logoff	Network Policy Server	6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
Logon/Logoff	Network Policy Server	6278	Network Policy Server granted full access to a user because the host met the defined health policy.
Logon/Logoff	Network Policy Server	6279	Network Policy Server locked the user account due to repeated failed authentication attempts.
Logon/Logoff	Network Policy Server	6280	Network Policy Server unlocked the user account.
System	System Integrity	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
System	Other System Events	6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.
System	Other System Events	6401	BranchCache: Received invalid data from a peer. Data discarded.
System	Other System Events	6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.
System	Other System Events	6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client.
System	Other System Events	6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
System	Other System Events	6405	BranchCache: %2 instance(s) of event id %1 occurred.
System	Other System Events	6406	%1 registered to Windows Firewall to control filtering for the following: %2
System	Other System Events	6407	1%
System	Other System Events	6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2
System	Other System Events	6409	BranchCache: A service connection point object could not be parsed.
System	System Integrity	6410	Code integrity determined that a file does not meet the security requirements to load into a process.
System	Plug and Play Events	6416	A new external device was recognized by the System
System	System Integrity	6417	The FIPS mode crypto selftests succeeded.
System	System Integrity	6418	The FIPS mode crypto selftests failed.
System	Plug and Play Events	6419	A request was made to disable a device
System	Plug and Play Events	6420	A device was disabled.
System	Plug and Play Events	6421	A request was made to enable a device.
System	Plug and Play Events	6422	A device was enabled.

System	Plug and Play Events	6423	The installation of this device is forbidden by system policy
System	Plug and Play Events	6424	The installation of this device was allowed, after having previously been forbidden by policy.