Windows 2000/XP and Windows Server 2003

According to the version of Windows installed on the system under investigation, the number and types of events will differ, so the events logged by a Windows XP machine may be incompatible with an event log analysis tool designed for Windows 8.

For example, Event ID 551 on a Windows XP machine refers to a logoff event; the Windows 7 equivalent is Event ID 4647.

- **512** - Windows NT is starting up
- **513** - Windows is shutting down
- **514** - An authentication package has been loaded by the Local Security Authority
- **515** - A trusted logon process has registered with the Local Security Authority
- **516** - Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits
- **517** - The audit log was cleared
- **518** - A notification package has been loaded by the Security Account Manager
- **519** - A process is using an invalid local procedure call (LPC) port
- **520** - The system time was changed
- **521** - Unable to log events to security log
- **528** - Successful Logon
- **529** - Logon Failure - Unknown user name or bad password
- **530** - Logon Failure - Account logon time restriction violation
- **531** - Logon Failure - Account currently disabled
- **532** - Logon Failure - The specified user account has expired
- **533** - Logon Failure - User not allowed to logon at this computer
- **534** - Logon Failure - The user has not been granted the requested logon type at this machine
- **535** - Logon Failure - The specified account's password has expired
- **536** - Logon Failure - The NetLogon component is not active
- **537** - Logon failure - The logon attempt failed for other reasons.
- **538** - User Logoff
- **539** - Logon Failure - Account locked out
- **540** - Successful Network Logon
- **551** - User initiated logoff
- **552** - Logon attempt using explicit credentials
- **560** - Object Open
- **561** - Handle Allocated
- **562** - Handle Closed
- **563** - Object Open for Delete
- **564** - Object Deleted
- **565** - Object Open (Active Directory)
- **566** - Object Operation (Active Directory)
- **567** - Object Access Attempt
- **576** - Special privileges assigned to new logon
- **577** - Privileged Service Called
- **578** - Privileged object operation
- **592** - A new process has been created
- **593** - A process has exited
- **594** - A handle to an object has been duplicated
- **595** - Indirect access to an object has been obtained
- **596** - Backup of data protection master key
- **600** - A process was assigned a primary token
- **601** - Attempt to install service
- **602** - Scheduled Task created
- **608** - User Right Assigned
- **609** - User Right Removed
- **610** - New Trusted Domain
- **611** - Removing Trusted Domain
- **612** - Audit Policy Change
- **613** - IPSec policy agent started
- **614** - IPSec policy agent disabled
- **615** - IPSEC PolicyAgent Service
- **616** - IPSec policy agent encountered a potentially serious failure.
- **617** - Kerberos Policy Changed
- **618** - Encrypted Data Recovery Policy Changed
- **619** - Quality of Service Policy Changed
- **620** - Trusted Domain Information Modified
- **621** - System Security Access Granted
- **622** - System Security Access Removed
- **623** - Per User Audit Policy was refreshed
- **624** - User Account Created
- **625** - User Account Type Changed
- **626** - User Account Enabled
- **627** - Change Password Attempt
- **628** - User Account password set
- **629** - User Account Disabled
- **630** - User Account Deleted
- **631** - Security Enabled Global Group Created
- **632** - Security Enabled Global Group Member Added
- **633** - Security Enabled Global Group Member Removed
- **634** - Security Enabled Global Group Deleted
- **635** - Security Enabled Local Group Created
- **636** - Security Enabled Local Group Member Added
- **637** - Security Enabled Local Group Member Removed

- 638 - Security Enabled Local Group Deleted
- 639 - Security Enabled Local Group Changed
- 640 - General Account Database Change
- 641 - Security Enabled Global Group Changed
- 642 - User Account Changed
- 643 - Domain Policy Changed
- 644 - User Account Locked Out
- 645 - Computer Account Created
- 646 - Computer Account Changed
- 647 - Computer Account Deleted
- 648 - Security Disabled Local Group Created
- 649 - Security Disabled Local Group Changed
- 650 - Security Disabled Local Group Member Added
- 651 - Security Disabled Local Group Member Removed
- 652 - Security Disabled Local Group Deleted
- 653 - Security Disabled Global Group Created
- 654 - Security Disabled Global Group Changed
- 655 - Security Disabled Global Group Member Added
- 656 - Security Disabled Global Group Member Removed
- 657 - Security Disabled Global Group Deleted
- 658 - Security Enabled Universal Group Created
- 659 - Security Enabled Universal Group Changed
- 660 - Security Enabled Universal Group Member Added
- 661 - Security Enabled Universal Group Member Removed
- 662 - Security Enabled Universal Group Deleted
- 663 - Security Disabled Universal Group Created
- 664 - Security Disabled Universal Group Changed
- 665 - Security Disabled Universal Group Member Added
- 666 - Security Disabled Universal Group Member Removed
- 667 - Security Disabled Universal Group Deleted
- 668 - Group Type Changed
- 669 - Add SID History
- 670 - Add SID History
- 671 - User Account Unlocked
- 672 - Authentication Ticket Granted
- 673 - Service Ticket Granted
- 674 - Ticket Granted Renewed
- 675 - Pre-authentication failed
- 676 - Authentication Ticket Request Failed
- 677 - Service Ticket Request Failed
- 678 - Account Mapped for Logon by
- 679 - The name: %2 could not be mapped for logon by: %1
- 680 - Account Used for Logon by
- 681 - The logon to account: %2 by: %1 from workstation: %3 failed.
- 682 - Session reconnected to winstation
- 683 - Session disconnected from winstation
- 684 - Set ACLs of members in administrators groups
- 685 - Account Name Changed
- 686 - Password of the following user accessed
- 687 - Basic Application Group Created
- 688 - Basic Application Group Changed
- 689 - Basic Application Group Member Added
- 690 - Basic Application Group Member Removed
- 691 - Basic Application Group Non-Member Added
- 692 - Basic Application Group Non-Member Removed
- 693 - Basic Application Group Deleted
- 694 - LDAP Query Group Created
- 695 - LDAP Query Group Changed
- 696 - LDAP Query Group Deleted
- 697 - Password Policy Checking API is called
- 806 - Per User Audit Policy was refreshed
- 807 - Per user auditing policy set for user
- 808 - A security event source has attempted to register
- 809 - A security event source has attempted to unregister
- 848 - The following policy was active when the Windows Firewall started
- 849 - An application was listed as an exception when the Windows Firewall started
- 850 - A port was listed as an exception when the Windows Firewall started
- 851 - A change has been made to the Windows Firewall application exception list
- 852 - A change has been made to the Windows Firewall port exception list
- 853 - The Windows Firewall operational mode has changed
- 854 - The Windows Firewall logging settings have changed
- 855 - A Windows Firewall ICMP setting has changed
- 856 - The Windows Firewall setting to allow unicast responses to multicast/broadcast traffic has changed
- 857 - The Windows Firewall setting to allow remote administration, allowing port TCP 135 and DCOM/RPC, has changed
- 858 - Windows Firewall group policy settings have been applied
- 859 - The Windows Firewall group policy settings have been removed
- 860 - The Windows Firewall has switched the active policy profile
- 861 - The Windows Firewall has detected an application listening for incoming traffic

Windows 7/Vista/8/10

Windows Server 2008/2012R2/2016/2019

- 1100 - The event logging service has shut down
- 1101 - Audit events have been dropped by the transport.
- 1102 - The audit log was cleared
- 1104 - The security Log is now full
- 1105 - Event log automatic backup
- 1108 - The event logging service encountered an error
- 4608 - Windows is starting up
- 4609 - Windows is shutting down
- 4610 - An authentication package has been loaded by the Local Security Authority
- 4611 - A trusted logon process has been registered with the Local Security Authority
- 4612 - Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
- 4614 - A notification package has been loaded by the Security Account Manager.
- 4615 - Invalid use of LPC port
- 4616 - The system time was changed.
- 4618 - A monitored security event pattern has occurred
- 4621 - Administrator recovered system from CrashOnAuditFail
- 4622 - A security package has been loaded by the Local Security Authority.
- 4624 - An account was successfully logged on
- 4625 - An account failed to log on
- 4626 - User/Device claims information
- 4627 - Group membership information.
- 4634 - An account was logged off
- 4646 - IKE DoS-prevention mode started
- 4647 - User initiated logoff
- 4648 - A logon was attempted using explicit credentials
- 4649 - A replay attack was detected
- 4650 - An IPsec Main Mode security association was established
- 4651 - An IPsec Main Mode security association was established
- 4652 - An IPsec Main Mode negotiation failed
- 4653 - An IPsec Main Mode negotiation failed
- 4654 - An IPsec Quick Mode negotiation failed
- 4655 - An IPsec Main Mode security association ended
- 4656 - A handle to an object was requested
- 4657 - A registry value was modified
- 4658 - The handle to an object was closed
- 4659 - A handle to an object was requested with intent to delete
- 4660 - An object was deleted
- 4661 - A handle to an object was requested
- 4662 - An operation was performed on an object
- 4663 - An attempt was made to access an object
- 4664 - An attempt was made to create a hard link
- 4665 - An attempt was made to create an application client context.
- 4666 - An application attempted an operation
- 4667 - An application client context was deleted
- 4668 - An application was initialized
- 4670 - Permissions on an object were changed
- 4671 - An application attempted to access a blocked ordinal through the TBS
- 4672 - Special privileges assigned to new logon
- 4673 - A privileged service was called
- 4674 - An operation was attempted on a privileged object
- 4675 - SIDs were filtered
- 4688 - A new process has been created
- 4689 - A process has exited
- 4690 - An attempt was made to duplicate a handle to an object
- 4691 - Indirect access to an object was requested
- 4692 - Backup of data protection master key was attempted
- 4693 - Recovery of data protection master key was attempted
- 4694 - Protection of auditable protected data was attempted
- 4695 - Unprotection of auditable protected data was attempted
- 4696 - A primary token was assigned to process
- 4697 - A service was installed in the system
- 4698 - A scheduled task was created
- 4699 - A scheduled task was deleted
- 4700 - A scheduled task was enabled
- 4701 - A scheduled task was disabled
- 4702 - A scheduled task was updated
- 4703 - A token right was adjusted
- 4704 - A user right was assigned
- 4705 - A user right was removed
- 4706 - A new trust was created to a domain
- 4707 - A trust to a domain was removed

- 4709 - IPsec Services was started
- 4710 - IPsec Services was disabled
- 4711 - PAStore Engine (1%)
- 4712 - IPsec Services encountered a potentially serious failure
- 4713 - Kerberos policy was changed
- 4714 - Encrypted data recovery policy was changed
- 4715 - The audit policy (SACL) on an object was changed
- 4716 - Trusted domain information was modified
- 4717 - System security access was granted to an account
- 4718 - System security access was removed from an account
- 4719 - System audit policy was changed
- 4720 - A user account was created
- 4722 - A user account was enabled
- 4723 - An attempt was made to change an account's password
- 4724 - An attempt was made to reset an accounts password
- 4725 - A user account was disabled
- 4726 - A user account was deleted
- 4727 - A security-enabled global group was created
- 4728 - A member was added to a security-enabled global group
- 4729 - A member was removed from a security-enabled global group
- 4730 - A security-enabled global group was deleted
- 4731 - A security-enabled local group was created
- 4732 - A member was added to a security-enabled local group
- 4733 - A member was removed from a security-enabled local group
- 4734 - A security-enabled local group was deleted
- 4735 - A security-enabled local group was changed
- 4737 - A security-enabled global group was changed
- 4738 - A user account was changed
- 4739 - Domain Policy was changed
- 4740 - A user account was locked out
- 4741 - A computer account was created
- 4742 - A computer account was changed
- 4743 - A computer account was deleted
- 4744 - A security-disabled local group was created
- 4745 - A security-disabled local group was changed
- 4746 - A member was added to a security-disabled local group
- 4747 - A member was removed from a security-disabled local group
- 4748 - A security-disabled local group was deleted
- 4749 - A security-disabled global group was created
- 4750 - A security-disabled global group was changed
- 4751 - A member was added to a security-disabled global group
- 4752 - A member was removed from a security-disabled global group
- 4753 - A security-disabled global group was deleted
- 4754 - A security-enabled universal group was created
- 4755 - A security-enabled universal group was changed
- 4756 - A member was added to a security-enabled universal group
- 4757 - A member was removed from a security-enabled universal group
- 4758 - A security-enabled universal group was deleted
- 4759 - A security-disabled universal group was created
- 4760 - A security-disabled universal group was changed
- 4761 - A member was added to a security-disabled universal group
- 4762 - A member was removed from a security-disabled universal group
- 4763 - A security-disabled universal group was deleted
- 4764 - A groups type was changed
- 4765 - SID History was added to an account
- 4766 - An attempt to add SID History to an account failed
- 4767 - A user account was unlocked
- 4768 - A Kerberos authentication ticket (TGT) was requested
- 4769 - A Kerberos service ticket was requested
- 4770 - A Kerberos service ticket was renewed
- 4771 - Kerberos pre-authentication failed
- 4772 - A Kerberos authentication ticket request failed
- 4773 - A Kerberos service ticket request failed
- 4774 - An account was mapped for logon
- 4775 - An account could not be mapped for logon
- 4776 - The domain controller attempted to validate the credentials for an account
- 4777 - The domain controller failed to validate the credentials for an account
- 4778 - A session was reconnected to a Window Station
- 4779 - A session was disconnected from a Window Station
- 4780 - The ACL was set on accounts which are members of administrators groups
- 4781 - The name of an account was changed
- 4782 - The password hash an account was accessed
- 4783 - A basic application group was created
- 4784 - A basic application group was changed
- 4785 - A member was added to a basic application group
- 4786 - A member was removed from a basic application group
- 4787 - A non-member was added to a basic application group
- 4788 - A non-member was removed from a basic application group..
- 4789 - A basic application group was deleted
- 4790 - An LDAP query group was created
- 4791 - A basic application group was changed
- 4792 - An LDAP query group was deleted
- 4793 - The Password Policy Checking API was called
- 4794 - An attempt was made to set the Directory Services Restore Mode administrator password
- 4797 - An attempt was made to query the existence of a blank password for an account
- 4798 - A user's local group membership was enumerated.
- 4799 - A security-enabled local group membership was enumerated
- 4800 - The workstation was locked
- 4801 - The workstation was unlocked
- 4802 - The screen saver was invoked

- 4803 - The screen saver was dismissed
- 4816 - RPC detected an integrity violation while decrypting an incoming message
- 4817 - Auditing settings on object were changed.
- 4818 - Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy
- 4819 - Central Access Policies on the machine have been changed
- 4820 - A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions
- 4821 - A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions
- 4822 - NTLM authentication failed because the account was a member of the Protected User group
- 4823 - NTLM authentication failed because access control restrictions are required
- 4824 - Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group
- 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
- 4826 - Boot Configuration Data loaded
- 4830 - SID History was removed from an account
- 4864 - A namespace collision was detected
- 4865 - A trusted forest information entry was added
- 4866 - A trusted forest information entry was removed
- 4867 - A trusted forest information entry was modified
- 4868 - The certificate manager denied a pending certificate request
- 4869 - Certificate Services received a resubmitted certificate request
- 4870 - Certificate Services revoked a certificate
- 4871 - Certificate Services received a request to publish the certificate revocation list (CRL)
- 4872 - Certificate Services published the certificate revocation list (CRL)
- 4873 - A certificate request extension changed
- 4874 - One or more certificate request attributes changed.
- 4875 - Certificate Services received a request to shut down
- 4876 - Certificate Services backup started
- 4877 - Certificate Services backup completed
- 4878 - Certificate Services restore started
- 4879 - Certificate Services restore completed
- 4880 - Certificate Services started
- 4881 - Certificate Services stopped
- 4882 - The security permissions for Certificate Services changed
- 4883 - Certificate Services retrieved an archived key
- 4884 - Certificate Services imported a certificate into its database
- 4885 - The audit filter for Certificate Services changed
- 4886 - Certificate Services received a certificate request
- 4887 - Certificate Services approved a certificate request and issued a certificate
- 4888 - Certificate Services denied a certificate request
- 4889 - Certificate Services set the status of a certificate request to pending
- 4890 - The certificate manager settings for Certificate Services changed.
- 4891 - A configuration entry changed in Certificate Services
- 4892 - A property of Certificate Services changed
- 4893 - Certificate Services archived a key
- 4894 - Certificate Services imported and archived a key
- 4895 - Certificate Services published the CA certificate to Active Directory Domain Services
- 4896 - One or more rows have been deleted from the certificate database
- 4897 - Role separation enabled
- 4898 - Certificate Services loaded a template
- 4899 - A Certificate Services template was updated
- 4900 - Certificate Services template security was updated
- 4902 - The Per-user audit policy table was created
- 4904 - An attempt was made to register a security event source
- 4905 - An attempt was made to unregister a security event source
- 4906 - The CrashOnAuditFail value has changed
- 4907 - Auditing settings on object were changed
- 4908 - Special Groups Logon table modified
- 4909 - The local policy settings for the TBS were changed
- 4910 - The group policy settings for the TBS were changed
- 4911 - Resource attributes of the object were changed
- 4912 - Per User Audit Policy was changed
- 4913 - Central Access Policy on the object was changed
- 4928 - An Active Directory replica source naming context was established
- 4929 - An Active Directory replica source naming context was removed
- 4930 - An Active Directory replica source naming context was modified
- 4931 - An Active Directory replica destination naming context was modified
- 4932 - Synchronization of a replica of an Active Directory naming context has begun
- 4933 - Synchronization of a replica of an Active Directory naming context has ended
- 4934 - Attributes of an Active Directory object were replicated
- 4935 - Replication failure begins
- 4936 - Replication failure ends
- 4937 - A lingering object was removed from a replica
- 4944 - The following policy was active when the Windows Firewall started
- 4945 - A rule was listed when the Windows Firewall started
- 4946 - A change has been made to Windows Firewall exception list. A rule was added
- 4947 - A change has been made to Windows Firewall exception list. A rule was modified
- 4948 - A change has been made to Windows Firewall exception list. A rule was deleted
- 4949 - Windows Firewall settings were restored to the default values
- 4950 - A Windows Firewall setting has changed
- 4951 - A rule has been ignored because its major version number was not recognized by Windows Firewall

- 4952 - Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall
- 4953 - A rule has been ignored by Windows Firewall because it could not parse the rule
- 4954 - Windows Firewall Group Policy settings has changed. The new settings have been applied
- 4956 - Windows Firewall has changed the active profile
- 4957 - Windows Firewall did not apply the following rule
- 4958 - Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer
- 4960 - IPsec dropped an inbound packet that failed an integrity check
- 4961 - IPsec dropped an inbound packet that failed a replay check
- 4962 - IPsec dropped an inbound packet that failed a replay check
- 4963 - IPsec dropped an inbound clear text packet that should have been secured
- 4964 - Special groups have been assigned to a new logon
- 4965 - IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI).
- 4976 - During Main Mode negotiation, IPsec received an invalid negotiation packet.
- 4977 - During Quick Mode negotiation, IPsec received an invalid negotiation packet.
- 4978 - During Extended Mode negotiation, IPsec received an invalid negotiation packet.
- 4979 - IPsec Main Mode and Extended Mode security associations were established.
- 4980 - IPsec Main Mode and Extended Mode security associations were established
- 4981 - IPsec Main Mode and Extended Mode security associations were established
- 4982 - IPsec Main Mode and Extended Mode security associations were established
- 4983 - An IPsec Extended Mode negotiation failed
- 4984 - An IPsec Extended Mode negotiation failed
- 4985 - The state of a transaction has changed
- 5024 - The Windows Firewall Service has started successfully
- 5025 - The Windows Firewall Service has been stopped
- 5027 - The Windows Firewall Service was unable to retrieve the security policy from the local storage
- 5028 - The Windows Firewall Service was unable to parse the new security policy.
- 5029 - The Windows Firewall Service failed to initialize the driver
- 5030 - The Windows Firewall Service failed to start
- 5031 - The Windows Firewall Service blocked an application from accepting incoming connections on the network.
- 5032 - Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network
- 5033 - The Windows Firewall Driver has started successfully
- 5034 - The Windows Firewall Driver has been stopped
- 5035 - The Windows Firewall Driver failed to start
- 5037 - The Windows Firewall Driver detected critical runtime error. Terminating
- 5038 - Code integrity determined that the image hash of a file is not valid
- 5039 - A registry key was virtualized.
- 5040 - A change has been made to IPsec settings. An Authentication Set was added.
- 5041 - A change has been made to IPsec settings. An Authentication Set was modified
- 5042 - A change has been made to IPsec settings. An Authentication Set was deleted
- 5043 - A change has been made to IPsec settings. A Connection Security Rule was added
- 5044 - A change has been made to IPsec settings. A Connection Security Rule was modified
- 5045 - A change has been made to IPsec settings. A Connection Security Rule was deleted
- 5046 - A change has been made to IPsec settings. A Crypto Set was added
- 5047 - A change has been made to IPsec settings. A Crypto Set was modified
- 5048 - A change has been made to IPsec settings. A Crypto Set was deleted
- 5049 - An IPsec Security Association was deleted
- 5050 - An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled(FALSE
- 5051 - A file was virtualized
- 5056 - A cryptographic self test was performed
- 5057 - A cryptographic primitive operation failed
- 5058 - Key file operation
- 5059 - Key migration operation
- 5060 - Verification operation failed
- 5061 - Cryptographic operation
- 5062 - A kernel-mode cryptographic self test was performed
- 5063 - A cryptographic provider operation was attempted
- 5064 - A cryptographic context operation was attempted
- 5065 - A cryptographic context modification was attempted
- 5066 - A cryptographic function operation was attempted
- 5067 - A cryptographic function modification was attempted
- 5068 - A cryptographic function provider operation was attempted
- 5069 - A cryptographic function property operation was attempted
- 5070 - A cryptographic function property operation was attempted
- 5071 - Key access denied by Microsoft key distribution service
- 5120 - OCSP Responder Service Started
- 5121 - OCSP Responder Service Stopped
- 5122 - A Configuration entry changed in the OCSP Responder Service
- 5123 - A configuration entry changed in the OCSP Responder Service
- 5124 - A security setting was updated on OCSP Responder Service
- 5125 - A request was submitted to OCSP Responder Service
- 5126 - Signing Certificate was automatically updated by the OCSP Responder Service
- 5127 - The OCSP Revocation Provider successfully updated the revocation information
- 5136 - A directory service object was modified
- 5137 - A directory service object was created
- 5138 - A directory service object was undeleted
- 5139 - A directory service object was moved
- 5140 - A network share object was accessed
- 5141 - A directory service object was deleted
- 5142 - A network share object was added.
- 5143 - A network share object was modified

- 5144 - A network share object was deleted.
- 5145 - A network share object was checked to see whether client can be granted desired access
- 5146 - The Windows Filtering Platform has blocked a packet
- 5147 - A more restrictive Windows Filtering Platform filter has blocked a packet
- 5148 - The Windows Filtering Platform has detected a DoS attack and entered a defensive mode
- 5149 - The DoS attack has subsided and normal processing is being resumed.
- 5150 - The Windows Filtering Platform has blocked a packet.
- 5151 - A more restrictive Windows Filtering Platform filter has blocked a packet.
- 5152 - The Windows Filtering Platform blocked a packet
- 5153 - A more restrictive Windows Filtering Platform filter has blocked a packet
- 5154 - The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections
- 5155 - The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections
- 5156 - The Windows Filtering Platform has allowed a connection
- 5157 - The Windows Filtering Platform has blocked a connection
- 5158 - The Windows Filtering Platform has permitted a bind to a local port
- 5159 - The Windows Filtering Platform has blocked a bind to a local port
- 5168 - Spn check for SMB/SMB2 fails.
- 5169 - A directory service object was modified
- 5170 - A directory service object was modified during a background cleanup task
- 5376 - Credential Manager credentials were backed up
- 5377 - Credential Manager credentials were restored from a backup
- 5378 - The requested credentials delegation was disallowed by policy
- 5379 - Credential Manager credentials were read
- 5380 - Vault Find Credential
- 5381 - Vault credentials were read
- 5382 - Vault credentials were read
- 5440 - The following callout was present when the Windows Filtering Platform Base Filtering Engine started
- 5441 - The following filter was present when the Windows Filtering Platform Base Filtering Engine started
- 5442 - The following provider was present when the Windows Filtering Platform Base Filtering Engine started
- 5443 - The following provider context was present when the Windows Filtering Platform Base Filtering Engine started
- 5444 - The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started
- 5446 - A Windows Filtering Platform callout has been changed
- 5447 - A Windows Filtering Platform filter has been changed
- 5448 - A Windows Filtering Platform provider has been changed
- 5449 - A Windows Filtering Platform provider context has been changed
- 5450 - A Windows Filtering Platform sub-layer has been changed
- 5451 - An IPsec Quick Mode security association was established
- 5452 - An IPsec Quick Mode security association ended
- 5453 - An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started
- 5456 - PAStore Engine applied Active Directory storage IPsec policy on the computer
- 5457 - PAStore Engine failed to apply Active Directory storage IPsec policy on the computer
- 5458 - PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer
- 5459 - PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer
- 5460 - PAStore Engine applied local registry storage IPsec policy on the computer
- 5461 - PAStore Engine failed to apply local registry storage IPsec policy on the computer
- 5462 - PAStore Engine failed to apply some rules of the active IPsec policy on the computer
- 5463 - PAStore Engine polled for changes to the active IPsec policy and detected no changes
- 5464 - PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services
- 5465 - PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully
- 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
- 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
- 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
- 5471 - PAStore Engine loaded local storage IPsec policy on the computer
- 5472 - PAStore Engine failed to load local storage IPsec policy on the computer
- 5473 - PAStore Engine loaded directory storage IPsec policy on the computer
- 5474 - PAStore Engine failed to load directory storage IPsec policy on the computer
- 5477 - PAStore Engine failed to add quick mode filter
- 5478 - IPsec Services has started successfully
- 5479 - IPsec Services has been shut down successfully
- 5480 - IPsec Services failed to get the complete list of network interfaces on the computer
- 5483 - IPsec Services failed to initialize RPC server. IPsec Services could not be started
- 5484 - IPsec Services has experienced a critical failure and has been shut down
- 5485 - IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces
- 5632 - A request was made to authenticate to a wireless network
- 5633 - A request was made to authenticate to a wired network

- 5712 - A Remote Procedure Call (RPC) was attempted
- 5888 - An object in the COM+ Catalog was modified
- 5889 - An object was deleted from the COM+ Catalog
- 5890 - An object was added to the COM+ Catalog
- 6144 - Security policy in the group policy objects has been applied successfully
- 6145 - One or more errors occured while processing security policy in the group policy objects
- 6272 - Network Policy Server granted access to a user
- 6273 - Network Policy Server denied access to a user
- 6274 - Network Policy Server discarded the request for a user
- 6275 - Network Policy Server discarded the accounting request for a user
- 6276 - Network Policy Server quarantined a user
- 6277 - Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy
- 6278 - Network Policy Server granted full access to a user because the host met the defined health policy
- 6279 - Network Policy Server locked the user account due to repeated failed authentication attempts
- 6280 - Network Policy Server unlocked the user account
- 6281 - Code Integrity determined that the page hashes of an image file are not valid...
- 6400 - BranchCache: Received an incorrectly formatted response while discovering availability of content.
- 6401 - BranchCache: Received invalid data from a peer. Data discarded.
- 6402 - BranchCache: The message to the hosted cache offering it data is incorrectly formatted.
- 6403 - BranchCache: The hosted cache sent an incorrectly formatted response to the client's message to offer it data.
- 6404 - BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
- 6405 - BranchCache: %2 instance(s) of event id %1 occurred.
- 6406 - %1 registered to Windows Firewall to control filtering for the following:
- 6407 - %1
- 6408 - Registered product %1 failed and Windows Firewall is now controlling the filtering for %2.
- 6409 - BranchCache: A service connection point object could not be parsed
- 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
- 6416 - A new external device was recognized by the system.
- 6417 - The FIPS mode crypto selftests succeeded
- 6418 - The FIPS mode crypto selftests failed
- 6419 - A request was made to disable a device
- 6420 - A device was disabled
- 6421 - A request was made to enable a device
- 6422 - A device was enabled
- 6423 - The installation of this device is forbidden by system policy
- 6424 - The installation of this device was allowed, after having previously been forbidden by policy
- 8191 - Highest System-Defined Audit Message Value