Windows Security Log Events

 www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx

Windows	512	Windows NT is starting up
Windows	513	Windows is shutting down
Windows	514	An authentication package has been loaded by the Local Security Authority
Windows	515	A trusted logon process has registered with the Local Security Authority
Windows	516	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits
Windows	517	The audit log was cleared
Windows	518	A notification package has been loaded by the Security Account Manager
Windows	519	A process is using an invalid local procedure call (LPC) port
Windows	520	The system time was changed
Windows	521	Unable to log events to security log
Windows	528	Successful Logon
Windows	529	Logon Failure - Unknown user name or bad password
Windows	530	Logon Failure - Account logon time restriction violation
Windows	531	Logon Failure - Account currently disabled
Windows	532	Logon Failure - The specified user account has expired
Windows	533	Logon Failure - User not allowed to logon at this computer
Windows	534	Logon Failure - The user has not been granted the requested logon type at this machine
Windows	535	Logon Failure - The specified account's password has expired
Windows	536	Logon Failure - The NetLogon component is not active
Windows	537	Logon failure - The logon attempt failed for other reasons.
Windows	538	User Logoff
Windows	539	Logon Failure - Account locked out
Windows	540	Successful Network Logon
Windows	551	User initiated logoff
Windows	552	Logon attempt using explicit credentials
Windows	560	Object Open

Windows	561	Handle Allocated
Windows	562	Handle Closed
Windows	563	Object Open for Delete
Windows	564	Object Deleted
Windows	565	Object Open (Active Directory)
Windows	566	Object Operation (W3 Active Directory)
Windows	567	Object Access Attempt
Windows	576	Special privileges assigned to new logon
Windows	577	Privileged Service Called
Windows	578	Privileged object operation
Windows	592	A new process has been created
Windows	593	A process has exited
Windows	594	A handle to an object has been duplicated
Windows	595	Indirect access to an object has been obtained
Windows	596	Backup of data protection master key
Windows	600	A process was assigned a primary token
Windows	601	Attempt to install service
Windows	602	Scheduled Task created
Windows	608	User Right Assigned
Windows	609	User Right Removed
Windows	610	New Trusted Domain
Windows	611	Removing Trusted Domain
Windows	612	Audit Policy Change
Windows	613	IPSec policy agent started
Windows	614	IPSec policy agent disabled
Windows	615	IPSEC PolicyAgent Service
Windows	616	IPSec policy agent encountered a potentially serious failure.
Windows	617	Kerberos Policy Changed
Windows	618	Encrypted Data Recovery Policy Changed
Windows	619	Quality of Service Policy Changed

Windows	620	Trusted Domain Information Modified
Windows	621	System Security Access Granted
Windows	622	System Security Access Removed
Windows	623	Per User Audit Policy was refreshed
Windows	624	User Account Created
Windows	625	User Account Type Changed
Windows	626	User Account Enabled
Windows	627	Change Password Attempt
Windows	628	User Account password set
Windows	629	User Account Disabled
Windows	630	User Account Deleted
Windows	631	Security Enabled Global Group Created
Windows	632	Security Enabled Global Group Member Added
Windows	633	Security Enabled Global Group Member Removed
Windows	634	Security Enabled Global Group Deleted
Windows	635	Security Enabled Local Group Created
Windows	636	Security Enabled Local Group Member Added
Windows	637	Security Enabled Local Group Member Removed
Windows	638	Security Enabled Local Group Deleted
Windows	639	Security Enabled Local Group Changed
Windows	640	General Account Database Change
Windows	641	Security Enabled Global Group Changed
Windows	642	User Account Changed
Windows	643	Domain Policy Changed
Windows	644	User Account Locked Out
Windows	645	Computer Account Created
Windows	646	Computer Account Changed
Windows	647	Computer Account Deleted
Windows	648	Security Disabled Local Group Created
Windows	649	Security Disabled Local Group Changed

Windows	650	Security Disabled Local Group Member Added
Windows	651	Security Disabled Local Group Member Removed
Windows	652	Security Disabled Local Group Deleted
Windows	653	Security Disabled Global Group Created
Windows	654	Security Disabled Global Group Changed
Windows	655	Security Disabled Global Group Member Added
Windows	656	Security Disabled Global Group Member Removed
Windows	657	Security Disabled Global Group Deleted
Windows	658	Security Enabled Universal Group Created
Windows	659	Security Enabled Universal Group Changed
Windows	660	Security Enabled Universal Group Member Added
Windows	661	Security Enabled Universal Group Member Removed
Windows	662	Security Enabled Universal Group Deleted
Windows	663	Security Disabled Universal Group Created
Windows	664	Security Disabled Universal Group Changed
Windows	665	Security Disabled Universal Group Member Added
Windows	666	Security Disabled Universal Group Member Removed
Windows	667	Security Disabled Universal Group Deleted
Windows	668	Group Type Changed
Windows	669	Add SID History
Windows	670	Add SID History
Windows	671	User Account Unlocked
Windows	672	Authentication Ticket Granted
Windows	673	Service Ticket Granted
Windows	674	Ticket Granted Renewed
Windows	675	Pre-authentication failed
Windows	676	Authentication Ticket Request Failed
Windows	677	Service Ticket Request Failed
Windows	678	Account Mapped for Logon by
Windows	679	The name: %2 could not be mapped for logon by: %1

Windows	680	Account Used for Logon by
Windows	681	The logon to account: %2 by: %1 from workstation: %3 failed.
Windows	682	Session reconnected to winstation
Windows	683	Session disconnected from winstation
Windows	684	Set ACLs of members in administrators groups
Windows	685	Account Name Changed
Windows	686	Password of the following user accessed
Windows	687	Basic Application Group Created
Windows	688	Basic Application Group Changed
Windows	689	Basic Application Group Member Added
Windows	690	Basic Application Group Member Removed
Windows	691	Basic Application Group Non-Member Added
Windows	692	Basic Application Group Non-Member Removed
Windows	693	Basic Application Group Deleted
Windows	694	LDAP Query Group Created
Windows	695	LDAP Query Group Changed
Windows	696	LDAP Query Group Deleted
Windows	697	Password Policy Checking API is called
Windows	806	Per User Audit Policy was refreshed
Windows	807	Per user auditing policy set for user
Windows	808	A security event source has attempted to register
Windows	809	A security event source has attempted to unregister
Windows	848	The following policy was active when the Windows Firewall started
Windows	849	An application was listed as an exception when the Windows Firewall started
Windows	850	A port was listed as an exception when the Windows Firewall started
Windows	851	A change has been made to the Windows Firewall application exception list
Windows	852	A change has been made to the Windows Firewall port exception list
Windows	853	The Windows Firewall operational mode has changed
Windows	854	The Windows Firewall logging settings have changed
Windows	855	A Windows Firewall ICMP setting has changed

Windows	856	The Windows Firewall setting to allow unicast responses to multicast/broadcast traffic has changed
Windows	857	The Windows Firewall setting to allow remote administration, allowing port TCP 135 and DCOM/RPC, has changed
Windows	858	Windows Firewall group policy settings have been applied
Windows	859	The Windows Firewall group policy settings have been removed
Windows	860	The Windows Firewall has switched the active policy profile
Windows	861	The Windows Firewall has detected an application listening for incoming traffic
Windows	1100	The event logging service has shut down
Windows	1101	Audit events have been dropped by the transport.
Windows	1102	The audit log was cleared
Windows	1104	The security Log is now full
Windows	1105	Event log automatic backup
Windows	1108	The event logging service encountered an error
Windows	4608	Windows is starting up
Windows	4609	Windows is shutting down
Windows	4610	An authentication package has been loaded by the Local Security Authority
Windows	4611	A trusted logon process has been registered with the Local Security Authority
Windows	4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
Windows	4614	A notification package has been loaded by the Security Account Manager.
Windows	4615	Invalid use of LPC port
Windows	4616	The system time was changed.
Windows	4618	A monitored security event pattern has occurred
Windows	4621	Administrator recovered system from CrashOnAuditFail
Windows	4622	A security package has been loaded by the Local Security Authority.
Windows	4624	An account was successfully logged on
Windows	4625	An account failed to log on
Windows	4626	User/Device claims information
Windows	4627	Group membership information.
Windows	4634	An account was logged off
Windows	4646	IKE DoS-prevention mode started

Windows	4647	User initiated logoff
Windows	4648	A logon was attempted using explicit credentials
Windows	4649	A replay attack was detected
Windows	4650	An IPsec Main Mode security association was established
Windows	4651	An IPsec Main Mode security association was established
Windows	4652	An IPsec Main Mode negotiation failed
Windows	4653	An IPsec Main Mode negotiation failed
Windows	4654	An IPsec Quick Mode negotiation failed
Windows	4655	An IPsec Main Mode security association ended
Windows	4656	A handle to an object was requested
Windows	4657	A registry value was modified
Windows	4658	The handle to an object was closed
Windows	4659	A handle to an object was requested with intent to delete
Windows	4660	An object was deleted
Windows	4661	A handle to an object was requested
Windows	4662	An operation was performed on an object
Windows	4663	An attempt was made to access an object
Windows	4664	An attempt was made to create a hard link
Windows	4665	An attempt was made to create an application client context.
Windows	4666	An application attempted an operation
Windows	4667	An application client context was deleted
Windows	4668	An application was initialized
Windows	4670	Permissions on an object were changed
Windows	4671	An application attempted to access a blocked ordinal through the TBS
Windows	4672	Special privileges assigned to new logon
Windows	4673	A privileged service was called
Windows	4674	An operation was attempted on a privileged object
Windows	4675	SIDs were filtered
Windows	4688	A new process has been created
Windows	4689	A process has exited

Windows	4690	An attempt was made to duplicate a handle to an object
Windows	4691	Indirect access to an object was requested
Windows	4692	Backup of data protection master key was attempted
Windows	4693	Recovery of data protection master key was attempted
Windows	4694	Protection of auditable protected data was attempted
Windows	4695	Unprotection of auditable protected data was attempted
Windows	4696	A primary token was assigned to process
Windows	4697	A service was installed in the system
Windows	4698	A scheduled task was created
Windows	4699	A scheduled task was deleted
Windows	4700	A scheduled task was enabled
Windows	4701	A scheduled task was disabled
Windows	4702	A scheduled task was updated
Windows	4704	A user right was assigned
Windows	4705	A user right was removed
Windows	4706	A new trust was created to a domain
Windows	4707	A trust to a domain was removed
Windows	4709	IPsec Services was started
Windows	4710	IPsec Services was disabled
Windows	4711	PAStore Engine (1%)
Windows	4712	IPsec Services encountered a potentially serious failure
Windows	4713	Kerberos policy was changed
Windows	4714	Encrypted data recovery policy was changed
Windows	4715	The audit policy (SACL) on an object was changed
Windows	4716	Trusted domain information was modified
Windows	4717	System security access was granted to an account
Windows	4718	System security access was removed from an account
Windows	4719	System audit policy was changed
Windows	4720	A user account was created
Windows	4722	A user account was enabled

Windows	4723	An attempt was made to change an account's password
Windows	4724	An attempt was made to reset an accounts password
Windows	4725	A user account was disabled
Windows	4726	A user account was deleted
Windows	4727	A security-enabled global group was created
Windows	4728	A member was added to a security-enabled global group
Windows	4729	A member was removed from a security-enabled global group
Windows	4730	A security-enabled global group was deleted
Windows	4731	A security-enabled local group was created
Windows	4732	A member was added to a security-enabled local group
Windows	4733	A member was removed from a security-enabled local group
Windows	4734	A security-enabled local group was deleted
Windows	4735	A security-enabled local group was changed
Windows	4737	A security-enabled global group was changed
Windows	4738	A user account was changed
Windows	4739	Domain Policy was changed
Windows	4740	A user account was locked out
Windows	4741	A computer account was created
Windows	4742	A computer account was changed
Windows	4743	A computer account was deleted
Windows	4744	A security-disabled local group was created
Windows	4745	A security-disabled local group was changed
Windows	4746	A member was added to a security-disabled local group
Windows	4747	A member was removed from a security-disabled local group
Windows	4748	A security-disabled local group was deleted
Windows	4749	A security-disabled global group was created
Windows	4750	A security-disabled global group was changed
Windows	4751	A member was added to a security-disabled global group
Windows	4752	A member was removed from a security-disabled global group
Windows	4753	A security-disabled global group was deleted

Windows	4754	A security-enabled universal group was created
Windows	4755	A security-enabled universal group was changed
Windows	4756	A member was added to a security-enabled universal group
Windows	4757	A member was removed from a security-enabled universal group
Windows	4758	A security-enabled universal group was deleted
Windows	4759	A security-disabled universal group was created
Windows	4760	A security-disabled universal group was changed
Windows	4761	A member was added to a security-disabled universal group
Windows	4762	A member was removed from a security-disabled universal group
Windows	4763	A security-disabled universal group was deleted
Windows	4764	A groups type was changed
Windows	4765	SID History was added to an account
Windows	4766	An attempt to add SID History to an account failed
Windows	4767	A user account was unlocked
Windows	4768	A Kerberos authentication ticket (TGT) was requested
Windows	4769	A Kerberos service ticket was requested
Windows	4770	A Kerberos service ticket was renewed
Windows	4771	Kerberos pre-authentication failed
Windows	4772	A Kerberos authentication ticket request failed
Windows	4773	A Kerberos service ticket request failed
Windows	4774	An account was mapped for logon
Windows	4775	An account could not be mapped for logon
Windows	4776	The domain controller attempted to validate the credentials for an account
Windows	4777	The domain controller failed to validate the credentials for an account
Windows	4778	A session was reconnected to a Window Station
Windows	4779	A session was disconnected from a Window Station
Windows	4780	The ACL was set on accounts which are members of administrators groups
Windows	4781	The name of an account was changed
Windows	4782	The password hash an account was accessed
Windows	4783	A basic application group was created

Windows	4784	A basic application group was changed
Windows	4785	A member was added to a basic application group
Windows	4786	A member was removed from a basic application group
Windows	4787	A non-member was added to a basic application group
Windows	4788	A non-member was removed from a basic application group..
Windows	4789	A basic application group was deleted
Windows	4790	An LDAP query group was created
Windows	4791	A basic application group was changed
Windows	4792	An LDAP query group was deleted
Windows	4793	The Password Policy Checking API was called
Windows	4794	An attempt was made to set the Directory Services Restore Mode administrator password
Windows	4797	An attempt was made to query the existence of a blank password for an account
Windows	4798	A user's local group membership was enumerated.
Windows	4799	A security-enabled local group membership was enumerated
Windows	4800	The workstation was locked
Windows	4801	The workstation was unlocked
Windows	4802	The screen saver was invoked
Windows	4803	The screen saver was dismissed
Windows	4816	RPC detected an integrity violation while decrypting an incoming message
Windows	4817	Auditing settings on object were changed.
Windows	4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy
Windows	4819	Central Access Policies on the machine have been changed
Windows	4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions
Windows	4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions
Windows	4822	NTLM authentication failed because the account was a member of the Protected User group
Windows	4823	NTLM authentication failed because access control restrictions are required
Windows	4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group
Windows	4864	A namespace collision was detected

Windows	4865	A trusted forest information entry was added
Windows	4866	A trusted forest information entry was removed
Windows	4867	A trusted forest information entry was modified
Windows	4868	The certificate manager denied a pending certificate request
Windows	4869	Certificate Services received a resubmitted certificate request
Windows	4870	Certificate Services revoked a certificate
Windows	4871	Certificate Services received a request to publish the certificate revocation list (CRL)
Windows	4872	Certificate Services published the certificate revocation list (CRL)
Windows	4873	A certificate request extension changed
Windows	4874	One or more certificate request attributes changed.
Windows	4875	Certificate Services received a request to shut down
Windows	4876	Certificate Services backup started
Windows	4877	Certificate Services backup completed
Windows	4878	Certificate Services restore started
Windows	4879	Certificate Services restore completed
Windows	4880	Certificate Services started
Windows	4881	Certificate Services stopped
Windows	4882	The security permissions for Certificate Services changed
Windows	4883	Certificate Services retrieved an archived key
Windows	4884	Certificate Services imported a certificate into its database
Windows	4885	The audit filter for Certificate Services changed
Windows	4886	Certificate Services received a certificate request
Windows	4887	Certificate Services approved a certificate request and issued a certificate
Windows	4888	Certificate Services denied a certificate request
Windows	4889	Certificate Services set the status of a certificate request to pending
Windows	4890	The certificate manager settings for Certificate Services changed.
Windows	4891	A configuration entry changed in Certificate Services
Windows	4892	A property of Certificate Services changed
Windows	4893	Certificate Services archived a key
Windows	4894	Certificate Services imported and archived a key

Windows	4895	Certificate Services published the CA certificate to Active Directory Domain Services
Windows	4896	One or more rows have been deleted from the certificate database
Windows	4897	Role separation enabled
Windows	4898	Certificate Services loaded a template
Windows	4899	A Certificate Services template was updated
Windows	4900	Certificate Services template security was updated
Windows	4902	The Per-user audit policy table was created
Windows	4904	An attempt was made to register a security event source
Windows	4905	An attempt was made to unregister a security event source
Windows	4906	The CrashOnAuditFail value has changed
Windows	4907	Auditing settings on object were changed
Windows	4908	Special Groups Logon table modified
Windows	4909	The local policy settings for the TBS were changed
Windows	4910	The group policy settings for the TBS were changed
Windows	4911	Resource attributes of the object were changed
Windows	4912	Per User Audit Policy was changed
Windows	4913	Central Access Policy on the object was changed
Windows	4928	An Active Directory replica source naming context was established
Windows	4929	An Active Directory replica source naming context was removed
Windows	4930	An Active Directory replica source naming context was modified
Windows	4931	An Active Directory replica destination naming context was modified
Windows	4932	Synchronization of a replica of an Active Directory naming context has begun
Windows	4933	Synchronization of a replica of an Active Directory naming context has ended
Windows	4934	Attributes of an Active Directory object were replicated
Windows	4935	Replication failure begins
Windows	4936	Replication failure ends
Windows	4937	A lingering object was removed from a replica
Windows	4944	The following policy was active when the Windows Firewall started
Windows	4945	A rule was listed when the Windows Firewall started
Windows	4946	A change has been made to Windows Firewall exception list. A rule was added

Windows	4947	A change has been made to Windows Firewall exception list. A rule was modified
Windows	4948	A change has been made to Windows Firewall exception list. A rule was deleted
Windows	4949	Windows Firewall settings were restored to the default values
Windows	4950	A Windows Firewall setting has changed
Windows	4951	A rule has been ignored because its major version number was not recognized by Windows Firewall
Windows	4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall
Windows	4953	A rule has been ignored by Windows Firewall because it could not parse the rule
Windows	4954	Windows Firewall Group Policy settings has changed. The new settings have been applied
Windows	4956	Windows Firewall has changed the active profile
Windows	4957	Windows Firewall did not apply the following rule
Windows	4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer
Windows	4960	IPsec dropped an inbound packet that failed an integrity check
Windows	4961	IPsec dropped an inbound packet that failed a replay check
Windows	4962	IPsec dropped an inbound packet that failed a replay check
Windows	4963	IPsec dropped an inbound clear text packet that should have been secured
Windows	4964	Special groups have been assigned to a new logon
Windows	4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI).
Windows	4976	During Main Mode negotiation, IPsec received an invalid negotiation packet.
Windows	4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet.
Windows	4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet.
Windows	4979	IPsec Main Mode and Extended Mode security associations were established.
Windows	4980	IPsec Main Mode and Extended Mode security associations were established
Windows	4981	IPsec Main Mode and Extended Mode security associations were established
Windows	4982	IPsec Main Mode and Extended Mode security associations were established
Windows	4983	An IPsec Extended Mode negotiation failed
Windows	4984	An IPsec Extended Mode negotiation failed
Windows	5024	The Windows Firewall Service has started successfully

Windows	5025	The Windows Firewall Service has been stopped
Windows	5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage
Windows	5028	The Windows Firewall Service was unable to parse the new security policy.
Windows	5029	The Windows Firewall Service failed to initialize the driver
Windows	5030	The Windows Firewall Service failed to start
Windows	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
Windows	5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network
Windows	5033	The Windows Firewall Driver has started successfully
Windows	5034	The Windows Firewall Driver has been stopped
Windows	5035	The Windows Firewall Driver failed to start
Windows	5037	The Windows Firewall Driver detected critical runtime error. Terminating
Windows	5038	Code integrity determined that the image hash of a file is not valid
Windows	5039	A registry key was virtualized.
Windows	5040	A change has been made to IPsec settings. An Authentication Set was added.
Windows	5041	A change has been made to IPsec settings. An Authentication Set was modified
Windows	5042	A change has been made to IPsec settings. An Authentication Set was deleted
Windows	5043	A change has been made to IPsec settings. A Connection Security Rule was added
Windows	5044	A change has been made to IPsec settings. A Connection Security Rule was modified
Windows	5045	A change has been made to IPsec settings. A Connection Security Rule was deleted
Windows	5046	A change has been made to IPsec settings. A Crypto Set was added
Windows	5047	A change has been made to IPsec settings. A Crypto Set was modified
Windows	5048	A change has been made to IPsec settings. A Crypto Set was deleted
Windows	5049	An IPsec Security Association was deleted
Windows	5050	An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled(FALSE
Windows	5051	A file was virtualized
Windows	5056	A cryptographic self test was performed
Windows	5057	A cryptographic primitive operation failed
Windows	5058	Key file operation
Windows	5059	Key migration operation

Windows	5060	Verification operation failed
Windows	5061	Cryptographic operation
Windows	5062	A kernel-mode cryptographic self test was performed
Windows	5063	A cryptographic provider operation was attempted
Windows	5064	A cryptographic context operation was attempted
Windows	5065	A cryptographic context modification was attempted
Windows	5066	A cryptographic function operation was attempted
Windows	5067	A cryptographic function modification was attempted
Windows	5068	A cryptographic function provider operation was attempted
Windows	5069	A cryptographic function property operation was attempted
Windows	5070	A cryptographic function property operation was attempted
Windows	5071	Key access denied by Microsoft key distribution service
Windows	5120	OCSP Responder Service Started
Windows	5121	OCSP Responder Service Stopped
Windows	5122	A Configuration entry changed in the OCSP Responder Service
Windows	5123	A configuration entry changed in the OCSP Responder Service
Windows	5124	A security setting was updated on OCSP Responder Service
Windows	5125	A request was submitted to OCSP Responder Service
Windows	5126	Signing Certificate was automatically updated by the OCSP Responder Service
Windows	5127	The OCSP Revocation Provider successfully updated the revocation information
Windows	5136	A directory service object was modified
Windows	5137	A directory service object was created
Windows	5138	A directory service object was undeleted
Windows	5139	A directory service object was moved
Windows	5140	A network share object was accessed
Windows	5141	A directory service object was deleted
Windows	5142	A network share object was added.
Windows	5143	A network share object was modified
Windows	5144	A network share object was deleted.
Windows	5145	A network share object was checked to see whether client can be granted desired access

Windows	5146	The Windows Filtering Platform has blocked a packet
Windows	5147	A more restrictive Windows Filtering Platform filter has blocked a packet
Windows	5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
Windows	5149	The DoS attack has subsided and normal processing is being resumed.
Windows	5150	The Windows Filtering Platform has blocked a packet.
Windows	5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
Windows	5152	The Windows Filtering Platform blocked a packet
Windows	5153	A more restrictive Windows Filtering Platform filter has blocked a packet
Windows	5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections
Windows	5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections
Windows	5156	The Windows Filtering Platform has allowed a connection
Windows	5157	The Windows Filtering Platform has blocked a connection
Windows	5158	The Windows Filtering Platform has permitted a bind to a local port
Windows	5159	The Windows Filtering Platform has blocked a bind to a local port
Windows	5168	Spn check for SMB/SMB2 fails.
Windows	5376	Credential Manager credentials were backed up
Windows	5377	Credential Manager credentials were restored from a backup
Windows	5378	The requested credentials delegation was disallowed by policy
Windows	5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started
Windows	5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started
Windows	5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started
Windows	5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started
Windows	5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started
Windows	5446	A Windows Filtering Platform callout has been changed
Windows	5447	A Windows Filtering Platform filter has been changed
Windows	5448	A Windows Filtering Platform provider has been changed

Windows	5449	A Windows Filtering Platform provider context has been changed
Windows	5450	A Windows Filtering Platform sub-layer has been changed
Windows	5451	An IPsec Quick Mode security association was established
Windows	5452	An IPsec Quick Mode security association ended
Windows	5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started
Windows	5456	PAStore Engine applied Active Directory storage IPsec policy on the computer
Windows	5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer
Windows	5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer
Windows	5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer
Windows	5460	PAStore Engine applied local registry storage IPsec policy on the computer
Windows	5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer
Windows	5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer
Windows	5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes
Windows	5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services
Windows	5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully
Windows	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
Windows	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
Windows	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
Windows	5471	PAStore Engine loaded local storage IPsec policy on the computer
Windows	5472	PAStore Engine failed to load local storage IPsec policy on the computer
Windows	5473	PAStore Engine loaded directory storage IPsec policy on the computer
Windows	5474	PAStore Engine failed to load directory storage IPsec policy on the computer
Windows	5477	PAStore Engine failed to add quick mode filter
Windows	5478	IPsec Services has started successfully
Windows	5479	IPsec Services has been shut down successfully
Windows	5480	IPsec Services failed to get the complete list of network interfaces on the computer

Windows	5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started
Windows	5484	IPsec Services has experienced a critical failure and has been shut down
Windows	5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces
Windows	5632	A request was made to authenticate to a wireless network
Windows	5633	A request was made to authenticate to a wired network
Windows	5712	A Remote Procedure Call (RPC) was attempted
Windows	5888	An object in the COM+ Catalog was modified
Windows	5889	An object was deleted from the COM+ Catalog
Windows	5890	An object was added to the COM+ Catalog
Windows	6144	Security policy in the group policy objects has been applied successfully
Windows	6145	One or more errors occured while processing security policy in the group policy objects
Windows	6272	Network Policy Server granted access to a user
Windows	6273	Network Policy Server denied access to a user
Windows	6274	Network Policy Server discarded the request for a user
Windows	6275	Network Policy Server discarded the accounting request for a user
Windows	6276	Network Policy Server quarantined a user
Windows	6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy
Windows	6278	Network Policy Server granted full access to a user because the host met the defined health policy
Windows	6279	Network Policy Server locked the user account due to repeated failed authentication attempts
Windows	6280	Network Policy Server unlocked the user account
Windows	6281	Code Integrity determined that the page hashes of an image file are not valid...
Windows	6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.
Windows	6401	BranchCache: Received invalid data from a peer. Data discarded.
Windows	6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.
Windows	6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client's message to offer it data.
Windows	6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
Windows	6405	BranchCache: %2 instance(s) of event id %1 occurred.
Windows	6406	%1 registered to Windows Firewall to control filtering for the following:

Windows	6407	%1
Windows	6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2.
Windows	6409	BranchCache: A service connection point object could not be parsed
Windows	6416	A new external device was recognized by the system.