1.2.1.1

1.2.1

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx (LINK)

KB299475 – Windows 2000 Security Event Descriptions (Part 1 of 2) (LINK)
KB301677 – Windows 2000 Security Event Descriptions (Part 2 of 2) (LINK)
Windows 2003 Security Guide, Chapter 4, Audit Policy (LINK)

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

1.2.2

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx (LINK)

http://www.microsoft.com/download/en/details.aspx?id=17871 (LINK)

http://www.microsoft.com/download/en/details.aspx?id=21561 (LINK)

http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Event-IDs-Windows-Server-2008-Vista-Revealed.html (LINK)

KB947226 – Description of security events in Windows Vista and in Windows Server 2008 (LINK)

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	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	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	4985	The state of a transaction has changed
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

1.2.3

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

https://technet.microsoft.com/

SharePoint	11	Site collection audit policy changed
SharePoint	12	Audit policy changed
SharePoint	13	Document checked in
SharePoint	14	Document checked out
SharePoint	15	Child object deleted
SharePoint	16	Child object moved
SharePoint	17	Object copied
SharePoint	18	Custom event
SharePoint	19	Object deleted
SharePoint	20	SharePoint audit logs deleted
SharePoint	21	Object moved
SharePoint	22	Object profile changed
SharePoint	23	SharePoint object structure changed
SharePoint	24	Search performed
SharePoint	25	SharePoint group created
SharePoint	26	SharePoint group deleted
SharePoint	27	SharePoint group member added
SharePoint	28	SharePoint group member removed
SharePoint	29	Unique permissions created
SharePoint	30	Unique permissions removed
SharePoint	31	Permissions updated
SharePoint	32	Permissions removed

SharePoint	33	Unique permission levels created
SharePoint	34	Permission level created
SharePoint	35	Permission level deleted
SharePoint	36	Permission level modified
SharePoint	37	SharePoint site collection administrator added
SharePoint	38	SharePoint site collection administrator removed
SharePoint	39	Object restored
SharePoint	40	Site collection updated
SharePoint	41	Web updated
SharePoint	42	Document library updated
SharePoint	43	Document updated
SharePoint	44	List updated
SharePoint	45	List item updated
SharePoint	46	Folder updated
SharePoint	47	Document viewed
SharePoint	48	Document library viewed
SharePoint	49	List viewed
SharePoint	50	Object viewed
SharePoint	51	Workflow accessed
SharePoint	52	Information management policy created
SharePoint	53	Information management policy changed
SharePoint	54	Site collection information management policy created
SharePoint	55	Site collection information management policy changed
SharePoint	56	Export of objects started
SharePoint	57	Export of objects completed
SharePoint	58	Import of objects started
SharePoint	59	Import of objects completed
SharePoint	60	Possible tampering warning

SharePoint	61	Retention policy processed
SharePoint	62	Document fragment updated
SharePoint	63	Content type imported

1.2.4

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

https://technet.microsoft.com/en-us/library/cc645603(v=sql.105).aspx

SQL Server	24000	SQL audit event
SQL Server	24001	Login succeeded
SQL Server	24002	Logout succeeded
SQL Server	24003	Login failed
SQL Server	24004	Change own password succeeded
SQL Server	24005	Change own password failed
SQL Server	24006	Change password succeeded
SQL Server	24007	Change password failed
SQL Server	24008	Reset own password succeeded
SQL Server	24009	Reset own password failed
SQL Server	24010	Reset password succeeded
SQL Server	24011	Reset password failed
SQL Server	24012	Must change password
SQL Server	24013	Account unlocked
SQL Server	24014	Change application role password succeeded
SQL Server	24015	Change application role password failed
SQL Server	24016	Add member to server role succeeded
SQL Server	24017	Add member to server role failed
SQL Server	24018	Remove member from server role succeeded
SQL Server	24019	Remove member from server role failed
SQL Server	24020	Add member to database role succeeded

SQL Server 24021 Add member to database role failed

SQL Server 24022 Remove member from database role succeeded

SQL Server 24023 Remove member from database role failed

SQL Server 24024 Issued database backup command

SQL Server 24025 Issued transaction log backup command

SQL Server 24026 Issued database restore command

SQL Server 24027 Issued transaction log restore command

SQL Server 24028 Issued database console command

SQL Server 24029 Issued a bulk administration command

SQL Server 24030 Issued an alter connection command

SQL Server 24031 Issued an alter resources command

SQL Server 24032 Issued an alter server state command

SQL Server 24033 Issued an alter server settings command

SQL Server 24034 Issued a view server state command

SQL Server 24035 Issued an external access assembly command

SQL Server 24036 Issued an unsafe assembly command

SQL Server 24037 Issued an alter resource governor command

SQL Server 24038 Issued a database authenticate command

SQL Server 24039 Issued a database checkpoint command

SQL Server 24040 Issued a database show plan command

SQL Server 24041 Issued a subscribe to query information command

SQL Server 24042 Issued a view database state command

SQL Server 24043 Issued a change server audit command

SQL Server 24044 Issued a change server audit specification command

SQL Server 24045 Issued a change database audit specification command

SQL Server 24046 Issued a create server audit command

SQL Server 24047 Issued a create server audit specification command

SQL Server 24048 Issued a create database audit specification command

SQL Server	24049	Issued a delete server audit command
SQL Server	24050	Issued a delete server audit specification command
SQL Server	24051	Issued a delete database audit specification command
SQL Server	24052	Audit failure
SQL Server	24053	Audit session changed
SQL Server	24054	Started SQL server
SQL Server	24055	Paused SQL server
SQL Server	24056	Resumed SQL server
SQL Server	24057	Stopped SQL server
SQL Server	24058	Issued a create server object command
SQL Server	24059	Issued a change server object command
SQL Server	24060	Issued a delete server object command
SQL Server	24061	Issued a create server setting command
SQL Server	24062	Issued a change server setting command
SQL Server	24063	Issued a delete server setting command
SQL Server	24064	Issued a create server cryptographic provider command
SQL Server	24065	Issued a delete server cryptographic provider command
SQL Server	24066	Issued a change server cryptographic provider command
SQL Server	24067	Issued a create server credential command
SQL Server	24068	Issued a delete server credential command
SQL Server	24069	Issued a change server credential command
SQL Server	24070	Issued a change server master key command
SQL Server	24071	Issued a back up server master key command
SQL Server	24072	Issued a restore server master key command
SQL Server	24073	Issued a map server credential to login command
SQL Server	24074	Issued a remove map between server credential and login command
SQL Server	24075	Issued a create server principal command
SQL Server	24076	Issued a delete server principal command

SQL Server	24077	Issued a change server principal credentials command
SQL Server	24078	Issued a disable server principal command
SQL Server	24079	Issued a change server principal default database command
SQL Server	24080	Issued an enable server principal command
SQL Server	24081	Issued a change server principal default language command
SQL Server	24082	Issued a change server principal password expiration command
SQL Server	24083	Issued a change server principal password policy command
SQL Server	24084	Issued a change server principal name command
SQL Server	24085	Issued a create database command
SQL Server	24086	Issued a change database command
SQL Server	24087	Issued a delete database command
SQL Server	24088	Issued a create certificate command
SQL Server	24089	Issued a change certificate command
SQL Server	24090	Issued a delete certificate command
SQL Server	24091	Issued a back up certificate command
SQL Server	24092	Issued an access certificate command
SQL Server	24093	Issued a create asymmetric key command
SQL Server	24094	Issued a change asymmetric key command
SQL Server	24095	Issued a delete asymmetric key command
SQL Server	24096	Issued an access asymmetric key command
SQL Server	24097	Issued a create database master key command
SQL Server	24098	Issued a change database master key command
SQL Server	24099	Issued a delete database master key command
SQL Server	24100	Issued a back up database master key command
SQL Server	24101	Issued a restore database master key command
SQL Server	24102	Issued an open database master key command
SQL Server	24103	Issued a create database symmetric key command
SQL Server	24104	Issued a change database symmetric key command

SQL Server	24105	Issued a delete database symmetric key command
SQL Server	24106	Issued a back up database symmetric key command
SQL Server	24107	Issued an open database symmetric key command
SQL Server	24108	Issued a create database object command
SQL Server	24109	Issued a change database object command
SQL Server	24110	Issued a delete database object command
SQL Server	24111	Issued an access database object command
SQL Server	24112	Issued a create assembly command
SQL Server	24113	Issued a change assembly command
SQL Server	24114	Issued a delete assembly command
SQL Server	24115	Issued a create schema command
SQL Server	24116	Issued a change schema command
SQL Server	24117	Issued a delete schema command
SQL Server	24118	Issued a create database encryption key command
SQL Server	24119	Issued a change database encryption key command
SQL Server	24120	Issued a delete database encryption key command
SQL Server	24121	Issued a create database user command
SQL Server	24122	Issued a change database user command
SQL Server	24123	Issued a delete database user command
SQL Server	24124	Issued a create database role command
SQL Server	24125	Issued a change database role command
SQL Server	24126	Issued a delete database role command
SQL Server	24127	Issued a create application role command
SQL Server	24128	Issued a change application role command
SQL Server	24129	Issued a delete application role command
SQL Server	24130	Issued a change database user login command
SQL Server	24131	Issued an auto-change database user login command
SQL Server	24132	Issued a create schema object command

SQL Server	24133	Issued a change schema object command
SQL Server	24134	Issued a delete schema object command
SQL Server	24135	Issued a transfer schema object command
SQL Server	24136	Issued a create schema type command
SQL Server	24137	Issued a change schema type command
SQL Server	24138	Issued a delete schema type command
SQL Server	24139	Issued a transfer schema type command
SQL Server	24140	Issued a create XML schema collection command
SQL Server	24141	Issued a change XML schema collection command
SQL Server	24142	Issued a delete XML schema collection command
SQL Server	24143	Issued a transfer XML schema collection command
SQL Server	24144	Issued an impersonate within server scope command
SQL Server	24145	Issued an impersonate within database scope command
SQL Server	24146	Issued a change server object owner command
SQL Server	24147	Issued a change database owner command
SQL Server	24148	Issued a change schema owner command
SQL Server	24150	Issued a change role owner command
SQL Server	24151	Issued a change database object owner command
SQL Server	24152	Issued a change symmetric key owner command
SQL Server	24153	Issued a change certificate owner command
SQL Server	24154	Issued a change asymmetric key owner command
SQL Server	24155	Issued a change schema object owner command
SQL Server	24156	Issued a change schema type owner command
SQL Server	24157	Issued a change XML schema collection owner command
SQL Server	24158	Grant server permissions succeeded
SQL Server	24159	Grant server permissions failed
SQL Server	24160	Grant server permissions with grant succeeded
SQL Server	24161	Grant server permissions with grant failed

SQL Server	24162	Deny server permissions succeeded
SQL Server	24163	Deny server permissions failed
SQL Server	24164	Deny server permissions with cascade succeeded
SQL Server	24165	Deny server permissions with cascade failed
SQL Server	24166	Revoke server permissions succeeded
SQL Server	24167	Revoke server permissions failed
SQL Server	24168	Revoke server permissions with grant succeeded
SQL Server	24169	Revoke server permissions with grant failed
SQL Server	24170	Revoke server permissions with cascade succeeded
SQL Server	24171	Revoke server permissions with cascade failed
SQL Server	24172	Issued grant server object permissions command
SQL Server	24173	Issued grant server object permissions with grant command
SQL Server	24174	Issued deny server object permissions command
SQL Server	24175	Issued deny server object permissions with cascade command
SQL Server	24176	Issued revoke server object permissions command
SQL Server	24177	Issued revoke server object permissions with grant command
SQL Server	24178	Issued revoke server object permissions with cascade command
SQL Server	24179	Grant database permissions succeeded
SQL Server	24180	Grant database permissions failed
SQL Server	24181	Grant database permissions with grant succeeded
SQL Server	24182	Grant database permissions with grant failed
SQL Server	24183	Deny database permissions succeeded
SQL Server	24184	Deny database permissions failed
SQL Server	24185	Deny database permissions with cascade succeeded
SQL Server	24186	Deny database permissions with cascade failed
SQL Server	24187	Revoke database permissions succeeded
SQL Server	24188	Revoke database permissions failed
SQL Server	24189	Revoke database permissions with grant succeeded

SQL Server	24190	Revoke database permissions with grant failed
SQL Server	24191	Revoke database permissions with cascade succeeded
SQL Server	24192	Revoke database permissions with cascade failed
SQL Server	24193	Issued grant database object permissions command
SQL Server	24194	Issued grant database object permissions with grant command
SQL Server	24195	Issued deny database object permissions command
SQL Server	24196	Issued deny database object permissions with cascade command
SQL Server	24197	Issued revoke database object permissions command
SQL Server	24198	Issued revoke database object permissions with grant command
SQL Server	24199	Issued revoke database object permissions with cascade command
SQL Server	24200	Issued grant schema permissions command
SQL Server	24201	Issued grant schema permissions with grant command
SQL Server	24202	Issued deny schema permissions command
SQL Server	24203	Issued deny schema permissions with cascade command
SQL Server	24204	Issued revoke schema permissions command
SQL Server	24205	Issued revoke schema permissions with grant command
SQL Server	24206	Issued revoke schema permissions with cascade command
SQL Server	24207	Issued grant assembly permissions command
SQL Server	24208	Issued grant assembly permissions with grant command
SQL Server	24209	Issued deny assembly permissions command
SQL Server	24210	Issued deny assembly permissions with cascade command
SQL Server	24211	Issued revoke assembly permissions command
SQL Server	24212	Issued revoke assembly permissions with grant command
SQL Server	24213	Issued revoke assembly permissions with cascade command
SQL Server	24214	Issued grant database role permissions command
SQL Server	24215	Issued grant database role permissions with grant command
SQL Server	24216	Issued deny database role permissions command
SQL Server	24217	Issued deny database role permissions with cascade command

SQL Server	24218	Issued revoke database role permissions command
SQL Server	24219	Issued revoke database role permissions with grant command
SQL Server	24220	Issued revoke database role permissions with cascade command
SQL Server	24221	Issued grant application role permissions command
SQL Server	24222	Issued grant application role permissions with grant command
SQL Server	24223	Issued deny application role permissions command
SQL Server	24224	Issued deny application role permissions with cascade command
SQL Server	24225	Issued revoke application role permissions command
SQL Server	24226	Issued revoke application role permissions with grant command
SQL Server	24227	Issued revoke application role permissions with cascade command
SQL Server	24228	Issued grant symmetric key permissions command
SQL Server	24229	Issued grant symmetric key permissions with grant command
SQL Server	24230	Issued deny symmetric key permissions command
SQL Server	24231	Issued deny symmetric key permissions with cascade command
SQL Server	24232	Issued revoke symmetric key permissions command
SQL Server	24233	Issued revoke symmetric key permissions with grant command
SQL Server	24234	Issued revoke symmetric key permissions with cascade command
SQL Server	24235	Issued grant certificate permissions command
SQL Server	24236	Issued grant certificate permissions with grant command
SQL Server	24237	Issued deny certificate permissions command
SQL Server	24238	Issued deny certificate permissions with cascade command
SQL Server	24239	Issued revoke certificate permissions command
SQL Server	24240	Issued revoke certificate permissions with grant command
SQL Server	24241	Issued revoke certificate permissions with cascade command
SQL Server	24242	Issued grant asymmetric key permissions command
SQL Server	24243	Issued grant asymmetric key permissions with grant command
SQL Server	24244	Issued deny asymmetric key permissions command
SQL Server	24245	Issued deny asymmetric key permissions with cascade command

SQL Server	24246	Issued revoke asymmetric key permissions command
SQL Server	24247	Issued revoke asymmetric key permissions with grant command
SQL Server	24248	Issued revoke asymmetric key permissions with cascade command
SQL Server	24249	Issued grant schema object permissions command
SQL Server	24250	Issued grant schema object permissions with grant command
SQL Server	24251	Issued deny schema object permissions command
SQL Server	24252	Issued deny schema object permissions with cascade command
SQL Server	24253	Issued revoke schema object permissions command
SQL Server	24254	Issued revoke schema object permissions with grant command
SQL Server	24255	Issued revoke schema object permissions with cascade command
SQL Server	24256	Issued grant schema type permissions command
SQL Server	24257	Issued grant schema type permissions with grant command
SQL Server	24258	Issued deny schema type permissions command
SQL Server	24259	Issued deny schema type permissions with cascade command
SQL Server	24260	Issued revoke schema type permissions command
SQL Server	24261	Issued revoke schema type permissions with grant command
SQL Server	24262	Issued revoke schema type permissions with cascade command
SQL Server	24263	Issued grant XML schema collection permissions command
SQL Server	24264	Issued grant XML schema collection permissions with grant command
SQL Server	24265	Issued deny XML schema collection permissions command
SQL Server	24266	Issued deny XML schema collection permissions with cascade command
SQL Server	24267	Issued revoke XML schema collection permissions command
SQL Server	24268	Issued revoke XML schema collection permissions with grant command
SQL Server	24269	Issued revoke XML schema collection permissions with cascade command
SQL Server	24270	Issued reference database object permissions command
SQL Server	24271	Issued send service request command
SQL Server	24272	Issued check permissions with schema command
SQL Server	24273	Issued use service broker transport security command

SQL Server	24274	Issued use database mirroring transport security command
SQL Server	24275	Issued alter trace command
SQL Server	24276	Issued start trace command
SQL Server	24277	Issued stop trace command
SQL Server	24278	Issued enable trace C2 audit mode command
SQL Server	24279	Issued disable trace C2 audit mode command
SQL Server	24280	Issued server full-text command
SQL Server	24281	Issued select command
SQL Server	24282	Issued update command
SQL Server	24283	Issued insert command
SQL Server	24284	Issued delete command
SQL Server	24285	Issued execute command
SQL Server	24286	Issued receive command
SQL Server	24287	Issued check references command
SQL Server	24288	Issued a create user-defined server role command
SQL Server	24289	Issued a change user-defined server role command
SQL Server	24290	Issued a delete user-defined server role command
SQL Server	24291	Issued grant user-defined server role permissions command
SQL Server	24292	Issued grant user-defined server role permissions with grant command
SQL Server	24293	Issued deny user-defined server role permissions command
SQL Server	24294	Issued deny user-defined server role permissions with cascade command
SQL Server	24295	Issued revoke user-defined server role permissions command
SQL Server	24296	Issued revoke user-defined server role permissions with grant command
SQL Server	24297	Issued revoke user-defined server role permissions with cascade command
SQL Server	24298	Database login succeeded
SQL Server	24299	Database login failed
SQL Server	24300	Database logout successful
SQL Server	24301	Change password succeeded

SQL Server 24302 Change password failed

SQL Server 24303 Change own password succeeded

SQL Server 24304 Change own password failed

SQL Server 24305 Reset own password succeeded

SQL Server 24306 Reset own password failed

SQL Server 24307 Reset password succeeded

SQL Server 24308 Reset password failed

SQL Server 24309 Copy password

SQL Server 24310 User-defined SQL audit event

SQL Server 24349 Issued a change assembly owner command