WINDOWS SECURITY LOG REFERENCE

USER ACCOUNT CHANGES

EVENT ID	DESCRIPTION
4720	Created
4722	Enabled
4723	User changed own password
4724	Privileged User changed this user's password
4725	Disabled
4726	Deleted
4738	Changed
4740	Locked out
4767	Unlocked
4781	Name change

DOMAIN CONTROLLER AUTHENTICATION EVENTS

EVENT ID	DESCRIPTION
4768	A Kerberos authentication ticket (TGT) was requested
4771	Kerberos pre-authentication failed
4820	A Kerberos TGT was denied because the device does not meet the access control restrictions

LOGON SESSION EVENTS (CORRELATE BY LOGON ID)

EVENT ID	DESCRIPTION
4624	Successful logon
4647	User initiated logoff
4625	Logon failure {See Logon Failure Codes)
4778	Remote desktop session reconnected
4779	Remote desktop session disconnected
4800	Workstation locked
4801	Workstation unlocked
4802	Screen saver invoked
4803	Screen saver dismissed

LOGON TYPES

TYPE ID	DESCRIPTION
2	Interactive
3	Network (i.e. mapped drive)
4	Batch
5	Service (service startup)
7	Unlock
8	Network Cleartext
10	Remote Desktop
11	Logon with cached credentials

SECURITY GROUP CHANGES

ACTION	LOCAL	GLOBAL	UNIVERSAL
Created	4731	4727	4754
Changed	4735	4737	4755
Deleted	4734	4730	4758
Member Added	4732	4728	4756
Member Removed	4733	4729	4757

SECURITY GROUP CHANGES

ACTION	LOCAL	GLOBAL	UNIVERSAL
Created	4744	4749	4759
Changed	4745	4750	4760
Deleted	4748	4753	4763
Member Added	4746	4751	4761
Member Removed	4747	4752	4762