Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
512	Windows NT is starting up	System		Success	4608							0	Unknown
513	Windows is shutting down	System		Success	4609							0	Unknown
514	An authentication package has been loade	System		Success	4610							2	Unknown
515	A trusted logon process has registered with	System		Success	4611							2	Unknown
516	Internal resources allocated for the queuin	System		Success	4612							3	Unknown
517	The audit log was cleared	System		Success	1102							4	Unknown
518	A notification package has been loaded by	System		Success	4614							2	Unknown
519	A process is using an invalid local procedur	System		Success Fai	4615							3	Unknown
520	The system time was changed	System		Success	4616							1	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	2			Interactive logon at keyboard and screen of		1	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	3			Network i.e. connection to shared folder or		2	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	4			Batch i.e. scheduled task		1	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	5			Service Service startup		1	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	7			Unlock i.e. unnattended workstation with p		1	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	8			NetworkCleartext Logon with credentials se		4	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	9			NewCredentials		1	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	10			RemoteInteractive Terminal Services Remot		2	Unknown
528	Successful Logon	Logon/Logoff		Success	4624	Logon Type	11			CachedInteractive logon with cached doma		1	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	2			Interactive logon at keyboard and screen of		2	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	3			Network i.e. connection to shared folder or		2	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	4			Batch i.e. scheduled task		1	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	5			Service Service startup		1	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	7			Unlock i.e. unnattended workstation with p		1	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	8			NetworkCleartext Logon with credentials se		4	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	9			NewCredentials		1	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	10			RemoteInteractive Terminal Services Remot		2	Unknown
529	Logon Failure - Unknown user name or bad	Logon/Logoff		Failure	4625	Logon Type	11			CachedInteractive logon with cached doma		1	Unknown
530	Logon Failure - Account logon time restricti	Logon/Logoff		Failure	4625							4	Unknown
531	Logon Failure - Account currently disabled	Logon/Logoff		Failure	4625							3	Unknown
532	Logon Failure - The specified user account l	Logon/Logoff		Failure	4625							4	Unknown
533	Logon Failure - User not allowed to logon a	Logon/Logoff		Failure	4625							4	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
534	Logon Failure - The user has not been grant	Logon/Logoff		Failure	4625							3	Unknown
535	Logon Failure - The specified account's pass	Logon/Logoff		Failure	4625							1	Unknown
536	Logon Failure - The NetLogon component is	Logon/Logoff		Failure	4625							2	Unknown
537	Logon failure - The logon attempt failed for	Logon/Logoff		Failure	4625							4	Unknown
538	User Logoff	Logon/Logoff		Success	4634							1	Unknown
539	Logon Failure - Account locked out	Logon/Logoff		Failure	4625							3	Unknown
540	Successful Network Logon	Logon/Logoff		Success	4624							1	Unknown
551	User initiated logoff	Logon/Logoff		Success	4647							1	Unknown
552	Logon attempt using explicit credentials	Logon/Logoff		Success	4648							2	Unknown
560	Object Open	Object Access		Success Fai	4656							0	Unknown
561	Handle Allocated	Object Access		Success								0	Unknown
562	Handle Closed	Object Access		Success	4658							0	Unknown
563	Object Open for Delete	Object Access		Success	4659							0	Unknown
564	Object Deleted	Object Access		Success	4660							1	Unknown
565	Object Open (Active Directory)	Directory Service		Success Fai	4661							0	Unknown
566	Object Operation (W3 Active Directory)	Directory Service		Success Fai	4662							0	Unknown
567	Object Access Attempt	Object Access		Success Fai	4657							0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeTcbPrivilege			Act as part of the operating system		2	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeMachineAccountPrivilege			Add workstations to domain		2	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeIncreaseQuotaPrivilege			Adjust memory quotas for a process		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeBackupPrivilege			Back up files and directories		1	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeChangeNotifyPrivilege			Bypass traverse checking		2	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeSystemtimePrivilege			Change the system time		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeCreatePagefilePrivilege			Create a pagefile		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeCreateTokenPrivilege			Create a token object		1	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeCreatePermanentPrivilege			Create permanent shared objects		2	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeDebugPrivilege			Debug programs		1	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeEnableDelegationPrivilege			Enable computer and user accounts to be t		3	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeRemoteShutdownPrivilege			Force shutdown from a remote system		2	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeAuditPrivilege			Generate security audits		3	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeIncreaseBasePriorityPrivilege			Increase scheduling priority		0	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeLoadDriverPrivilege			Load and unload device drivers		1	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeLockMemoryPrivilege			Lock pages in memory		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeSecurityPrivilege			Manage auditing and security log		3	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeSystemEnvironmentPrivilege			Modify firmware environment values		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeManageVolumePrivilege			Perform volume maintenance tasks		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeProfileSingleProcessPrivilege			Profile single process		1	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeSystemProfilePrivilege			Profile system performance		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeUndockPrivilege			Remove computer from docking station		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeAssignPrimaryTokenPrivilege			Replace a process level token		1	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeRestorePrivilege			Restore files and directories		1	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeShutdownPrivilege			Shut down the system		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeSyncAgentPrivilege			Synchronize directory service data		0	Unknown
576	Special privileges assigned to new logon	Privilege Use		Success Fai	4672	User Right	SeTakeOwnershipPrivilege			Take ownership of files or other objects		3	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeTcbPrivilege			Act as part of the operating system		2	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeMachineAccountPrivilege			Add workstations to domain		2	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeIncreaseQuotaPrivilege			Adjust memory quotas for a process		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeBackupPrivilege			Back up files and directories		1	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeChangeNotifyPrivilege			Bypass traverse checking		2	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeSystemtimePrivilege			Change the system time		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeCreatePagefilePrivilege			Create a pagefile		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeCreateTokenPrivilege			Create a token object		1	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeCreatePermanentPrivilege			Create permanent shared objects		2	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeDebugPrivilege			Debug programs		1	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeEnableDelegationPrivilege			Enable computer and user accounts to be t		3	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeRemoteShutdownPrivilege			Force shutdown from a remote system		2	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeAuditPrivilege			Generate security audits		3	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeIncreaseBasePriorityPrivilege			Increase scheduling priority		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeLoadDriverPrivilege			Load and unload device drivers		1	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeLockMemoryPrivilege			Lock pages in memory		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeSecurityPrivilege			Manage auditing and security log		3	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeSystemEnvironmentPrivilege			Modify firmware environment values		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeManageVolumePrivilege			Perform volume maintenance tasks		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeProfileSingleProcessPrivilege			Profile single process		1	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeSystemProfilePrivilege			Profile system performance		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeUndockPrivilege			Remove computer from docking station		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeAssignPrimaryTokenPrivilege			Replace a process level token		1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeRestorePrivilege			Restore files and directories		1	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeShutdownPrivilege			Shut down the system		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeSyncAgentPrivilege			Synchronize directory service data		0	Unknown
577	Privileged Service Called	Privilege Use		Success Fai	4673	User Right	SeTakeOwnershipPrivilege			Take ownership of files or other objects		3	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeTcbPrivilege			Act as part of the operating system		2	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeMachineAccountPrivilege			Add workstations to domain		2	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeIncreaseQuotaPrivilege			Adjust memory quotas for a process		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeBackupPrivilege			Back up files and directories		1	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeChangeNotifyPrivilege			Bypass traverse checking		2	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeSystemtimePrivilege			Change the system time		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeCreatePagefilePrivilege			Create a pagefile		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeCreateTokenPrivilege			Create a token object		1	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeCreatePermanentPrivilege			Create permanent shared objects		2	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeDebugPrivilege			Debug programs		1	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeEnableDelegationPrivilege			Enable computer and user accounts to be t		3	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeRemoteShutdownPrivilege			Force shutdown from a remote system		2	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeAuditPrivilege			Generate security audits		3	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeIncreaseBasePriorityPrivilege			Increase scheduling priority		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeLoadDriverPrivilege			Load and unload device drivers		1	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeLockMemoryPrivilege			Lock pages in memory		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeSecurityPrivilege			Manage auditing and security log		3	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeSystemEnvironmentPrivilege			Modify firmware environment values		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeManageVolumePrivilege			Perform volume maintenance tasks		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeProfileSingleProcessPrivilege			Profile single process		1	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeSystemProfilePrivilege			Profile system performance		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeUndockPrivilege			Remove computer from docking station		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeAssignPrimaryTokenPrivilege			Replace a process level token		1	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeRestorePrivilege			Restore files and directories		1	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeShutdownPrivilege			Shut down the system		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeSyncAgentPrivilege			Synchronize directory service data		0	Unknown
578	Privileged object operation	Privilege Use		Success Fai	4674	User Right	SeTakeOwnershipPrivilege			Take ownership of files or other objects		3	Unknown
592	A new process has been created	Process Tracking		Success	4688							3	Unknown
593	A process has exited	Process Tracking		Success	4689							0	Unknown
594	A handle to an object has been duplicated	Process Tracking		Success	4690							0	Unknown
595	Indirect access to an object has been obtai	Process Tracking		Success								3	Unknown
600	A process was assigned a primary token	Process Tracking		Success Fai	4696							0	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
601	Attempt to install service	Process Tracking		Success Fai	4697							3	Unknown
602	Scheduled Task created	Process Tracking		Success	4698							2	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeTcbPrivilege			Act as part of the operating system		2	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeMachineAccountPrivilege			Add workstations to domain		2	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeIncreaseQuotaPrivilege			Adjust memory quotas for a process		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeBackupPrivilege			Back up files and directories		1	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeChangeNotifyPrivilege			Bypass traverse checking		2	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeSystemtimePrivilege			Change the system time		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeCreatePagefilePrivilege			Create a pagefile		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeCreateTokenPrivilege			Create a token object		1	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeCreatePermanentPrivilege			Create permanent shared objects		2	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeDebugPrivilege			Debug programs		1	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeEnableDelegationPrivilege			Enable computer and user accounts to be t		3	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeRemoteShutdownPrivilege			Force shutdown from a remote system		2	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeAuditPrivilege			Generate security audits		3	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeIncreaseBasePriorityPrivilege			Increase scheduling priority		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeLoadDriverPrivilege			Load and unload device drivers		1	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeLockMemoryPrivilege			Lock pages in memory		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeSecurityPrivilege			Manage auditing and security log		3	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeSystemEnvironmentPrivilege			Modify firmware environment values		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeManageVolumePrivilege			Perform volume maintenance tasks		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeProfileSingleProcessPrivilege			Profile single process		1	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeSystemProfilePrivilege			Profile system performance		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeUndockPrivilege			Remove computer from docking station		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeAssignPrimaryTokenPrivilege			Replace a process level token		1	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeRestorePrivilege			Restore files and directories		1	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeShutdownPrivilege			Shut down the system		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeSyncAgentPrivilege			Synchronize directory service data		0	Unknown
608	User Right Assigned	Policy Change		Success	4704	User Right	SeTakeOwnershipPrivilege			Take ownership of files or other objects		3	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeTcbPrivilege			Act as part of the operating system		2	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeMachineAccountPrivilege			Add workstations to domain		2	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeIncreaseQuotaPrivilege			Adjust memory quotas for a process		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeBackupPrivilege			Back up files and directories		1	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeChangeNotifyPrivilege			Bypass traverse checking		2	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeSystemtimePrivilege			Change the system time		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeCreatePagefilePrivilege			Create a pagefile		0	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
609	User Right Removed	Policy Change		Success	4705	User Right	SeCreateTokenPrivilege			Create a token object		1	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeCreatePermanentPrivilege			Create permanent shared objects		2	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeDebugPrivilege			Debug programs		1	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeEnableDelegationPrivilege			Enable computer and user accounts to be t		3	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeRemoteShutdownPrivilege			Force shutdown from a remote system		2	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeAuditPrivilege			Generate security audits		3	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeIncreaseBasePriorityPrivilege			Increase scheduling priority		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeLoadDriverPrivilege			Load and unload device drivers		1	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeLockMemoryPrivilege			Lock pages in memory		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeSecurityPrivilege			Manage auditing and security log		3	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeSystemEnvironmentPrivilege			Modify firmware environment values		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeManageVolumePrivilege			Perform volume maintenance tasks		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeProfileSingleProcessPrivilege			Profile single process		1	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeSystemProfilePrivilege			Profile system performance		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeUndockPrivilege			Remove computer from docking station		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeAssignPrimaryTokenPrivilege			Replace a process level token		1	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeRestorePrivilege			Restore files and directories		1	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeShutdownPrivilege			Shut down the system		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeSyncAgentPrivilege			Synchronize directory service data		0	Unknown
609	User Right Removed	Policy Change		Success	4705	User Right	SeTakeOwnershipPrivilege			Take ownership of files or other objects		3	Unknown
610	New Trusted Domain	Policy Change		Success	4706							4	Unknown
611	Removing Trusted Domain	Policy Change		Success	4707							4	Unknown
612	Audit Policy Change	Policy Change		Success	4719							3	Unknown
613	IPSec policy agent started	Policy Change		Success Failure								2	Unknown
614	IPSec policy agent disabled	Policy Change		Success Failure								2	Unknown
615	IPSEC PolicyAgent Service	Policy Change		Success Failure								2	Unknown
616	IPSec policy agent encountered a potentiall	Policy Change		Success Failure								3	Unknown
617	Kerberos Policy Changed	Policy Change		Success	4713							4	Unknown
618	Encrypted Data Recovery Policy Changed	Policy Change		Success	4714							3	Unknown
619	Quality of Service Policy Changed	Policy Change		Success Failure								1	Unknown
620	Trusted Domain Information Modified	Policy Change		Success	4716							4	Unknown
621	System Security Access Granted	Policy Change		Success	4717							2	Unknown
622	System Security Access Removed	Policy Change		Success	4718							2	Unknown
623	Per User Audit Policy was refreshed	Policy Change		Success								2	Unknown
624	User Account Created	Account Management		Success	4720							2	Unknown
625	User Account Type Changed	Policy Change		Success								2	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
626	User Account Enabled	Account Management		Success	4722							1	Unknown
627	Change Password Attempt	Account Management		Success Fai	4723							3	Unknown
628	User Account password set	Account Management		Success Fai	4724							1	Unknown
629	User Account Disabled	Account Management		Success	4725							3	Unknown
630	User Account Deleted	Account Management		Success	4726							2	Unknown
631	Security Enabled Global Group Created	Account Management		Success	4727							3	Unknown
632	Security Enabled Global Group Member Ad	Account Management		Success	4728							3	Unknown
633	Security Enabled Global Group Member Re	Account Management		Success	4729							2	Unknown
634	Security Enabled Global Group Deleted	Account Management		Success	4730							2	Unknown
635	Security Enabled Local Group Created	Account Management		Success	4731							2	Unknown
636	Security Enabled Local Group Member Add	Account Management		Success	4732							3	Unknown
637	Security Enabled Local Group Member Rem	Account Management		Success	4733							2	Unknown
638	Security Enabled Local Group Deleted	Account Management		Success	4734							2	Unknown
639	Security Enabled Local Group Changed	Account Management		Success	4735							2	Unknown
640	General Account Database Change	Account Management		Success Failure								3	Unknown
641	Security Enabled Global Group Changed	Account Management		Success	4737							2	Unknown
642	User Account Changed	Account Management		Success	4738							2	Unknown
643	Domain Policy Changed	Account Management		Success	4739							2	Unknown
644	User Account Locked Out	Account Management		Success Fai	4740							4	Unknown
645	Computer Account Created	Account Management		Success	4741							2	Unknown
646	Computer Account Changed	Account Management		Success	4742							2	Unknown
647	Computer Account Deleted	Account Management		Success	4743							1	Unknown
648	Security Disabled Local Group Created	Account Management		Success	4744							2	Unknown
649	Security Disabled Local Group Changed	Account Management		Success	4745							1	Unknown
650	Security Disabled Local Group Member Adc	Account Management		Success	4746							1	Unknown
651	Security Disabled Local Group Member Rer	Account Management		Success	4747							1	Unknown
652	Security Disabled Local Group Deleted	Account Management		Success	4748							1	Unknown
653	Security Disabled Global Group Created	Account Management		Success	4749							2	Unknown
654	Security Disabled Global Group Changed	Account Management		Success	4750							1	Unknown
655	Security Disabled Global Group Member Ac	Account Management		Success	4751							1	Unknown
656	Security Disabled Global Group Member Re	Account Management		Success	4752							1	Unknown
657	Security Disabled Global Group Deleted	Account Management		Success	4753							1	Unknown
658	Security Enabled Universal Group Created	Account Management		Success	4754							3	Unknown
659	Security Enabled Universal Group Changed	Account Management		Success	4755							2	Unknown
660	Security Enabled Universal Group Member	Account Management		Success	4756							2	Unknown
661	Security Enabled Universal Group Member	Account Management		Success	4757							2	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
662	Security Enabled Universal Group Deleted	Account Management		Success	4758							2	Unknown
663	Security Disabled Universal Group Created	Account Management		Success	4759							2	Unknown
664	Security Disabled Universal Group Changed	Account Management		Success	4760							1	Unknown
665	Security Disabled Universal Group Member	Account Management		Success								1	Unknown
666	Security Disabled Universal Group Member	Account Management		Success	4762							1	Unknown
667	Security Disabled Universal Group Deleted	Account Management		Success	4763							1	Unknown
668	Group Type Changed	Account Management		Success	4764							3	Unknown
669	Add SID History	Account Management		Success Failure								4	Unknown
670	Add SID History	Account Management		Success Failure								4	Unknown
671	User Account Unlocked	Account Management		Success	4767							2	Unknown
672	Authentication Ticket Granted	Account Logon		Success Fai	4768	Result Code	0	0x0	KDC_ERR_NONE	No error		0	
672	Authentication Ticket Granted			Success Failure			1	0x1	KDC_ERR_NAME_EXP	Client's entry in KDC database has expired		1	Low
672	Authentication Ticket Granted			Success Failure			2	0x2	KDC_ERR_SERVICE_EXP	Server's entry in KDC database has expired		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	3	0x3	KDC_ERR_BAD_PVNO	Requested Kerberos version number not su		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	4	0x4	KDC_ERR_C_OLD_MAST_K	Client's key encrypted in old master key		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	5	0x5	KDC_ERR_S_OLD_MAST_K	Server's key encrypted in old master key		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	6	0x6	KDC_ERR_C_PRINCIPAL_UI	Client not found in Kerberos database		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	7	0x7	KDC_ERR_S_PRINCIPAL_UI	Server not found in Kerberos database		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	8	0x8	KDC_ERR_PRINCIPAL_NOT	Multiple principal entries in KDC database		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	9	0x9	KDC_ERR_NULL_KEY	The client or server has a null key (master k		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	10	0xA	KDC_ERR_CANNOT_POSTD	Ticket (TGT) not eligible for postdating		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	11	0xB	KDC_ERR_NEVER_VALID	Requested start time is later than end time		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	12	0xC	KDC_ERR_POLICY	Requested start time is later than end time		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	13	0xD	KDC_ERR_BADOPTION	KDC cannot accommodate requested optio		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	14	0xE	KDC_ERR_ETYPE_NOTSUPI	KDC has no support for encryption type		1	High
672	Authentication Ticket Granted			Success Fai	4768	Result Code	15	0xF	KDC_ERR_SUMTYPE_NOSU	KDC has no support for checksum type		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	16	0x10	KDC_ERR_PADATA_TYPE_N	KDC has no support for PADATA type (pre-a		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	17	0x11	KDC_ERR_TRTYPE_NO_SU	KDC has no support for transited type		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	18	0x12	KDC_ERR_CLIENT_REVOKE	Client’s credentials have been revoked		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	19	0x13	KDC_ERR_SERVICE_REVOK	Credentials for server have been revoked		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	20	0x14	KDC_ERR_TGT_REVOKED	TGT has been revoked		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	21	0x15	KDC_ERR_CLIENT_NOTYET	Client not yet valid—try again later		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	22	0x16	KDC_ERR_SERVICE_NOTYE	Server not yet valid—try again later		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	23	0x17	KDC_ERR_KEY_EXPIRED	Password has expired—change password to		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	24	0x18	KDC_ERR_PREAUTH_FAILE	Pre-authentication information was invalid		1	High
672	Authentication Ticket Granted			Success Fai	4768	Result Code	25	0x19	KDC_ERR_PREAUTH_REQU	Additional preauthentication required		2	Low

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
672	Authentication Ticket Granted			Success Fai	4768	Result Code	26	0x1A	KDC_ERR_SERVER_NOMAT	KDC does not know about the requested se		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	27	0x1B	KDC_ERR_SVC_UNAVAILAE	KDC is unavailable		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	31	0x1F	KRB_AP_ERR_BAD_INTEGF	Integrity check on decrypted field failed		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	32	0x20	KRB_AP_ERR_TKT_EXPIREI	The ticket has expired		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	33	0x21	KRB_AP_ERR_TKT_NYV	The ticket is not yet valid		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	34	0x22	KRB_AP_ERR_REPEAT	The request is a replay		4	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	35	0x23	KRB_AP_ERR_NOT_US	The ticket is not for us		4	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	36	0x24	KRB_AP_ERR_BADMATCH	The ticket and authenticator do not match		4	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	37	0x25	KRB_AP_ERR_SKEW	The clock skew is too great		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	38	0x26	KRB_AP_ERR_BADADDR	Network address in network layer header d		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	39	0x27	KRB_AP_ERR_BADVERSION	Protocol version numbers don't match (PVN		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	40	0x28	KRB_AP_ERR_MSG_TYPE	Message type is unsupported		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	41	0x29	KRB_AP_ERR_MODIFIED	Message stream modified and checksum di		4	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	42	0x2A	KRB_AP_ERR_BADORDER	Message out of order (possible tampering)		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	44	0x2C	KRB_AP_ERR_BADKEYVER	Specified version of key is not available		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	45	0x2D	KRB_AP_ERR_NOKEY	Service key not available		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	46	0x2E	KRB_AP_ERR_MUT_FAIL	Mutual authentication failed		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	47	0x2F	KRB_AP_ERR_BADDIRECTI	Incorrect message direction		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	48	0x30	KRB_AP_ERR_METHOD	Alternative authentication method require		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	49	0x31	KRB_AP_ERR_BADSEQ	Incorrect sequence number in message		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	50	0x32	KRB_AP_ERR_INAPP_CKSU	Inappropriate type of checksum in message		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	51	0x33	KRB_AP_PATH_NOT_ACCE	Desired path is unreachable		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	52	0x34	KRB_ERR_RESPONSE_TOO	Too much data		1	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	60	0x3C	KRB_ERR_GENERIC	Generic error; the description is in the e-da		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	61	0x3D	KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	62	0x3E	KDC_ERR_CLIENT_NOT_TR	The client trust failed or is not implemente		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	63	0x3F	KDC_ERR_KDC_NOT_TRUS	The KDC server trust failed or could not be		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	64	0x40	KDC_ERR_INVALID_SIG	The signature is invalid		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	65	0x41	KDC_ERR_KEY_TOO_WEAI	A higher encryption level is needed		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	66	0x42	KRB_AP_ERR_USER_TO_U	User-to-user authorization is required		2	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	67	0x43	KRB_AP_ERR_NO_TGT	No TGT was presented or available		3	Low
672	Authentication Ticket Granted			Success Fai	4768	Result Code	68	0x44	KDC_ERR_WRONG_REALM	Incorrect domain or principal		3	Low
673	Service Ticket Granted	Account Logon		Success	4769							1	Unknown
674	Ticket Granted Renewed	Account Logon		Success	4770							1	Unknown
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	0	0x0	KDC_ERR_NONE	No error		0	
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	1	0x1	KDC_ERR_NAME_EXP	Client's entry in KDC database has expired		1	Low

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	2	0x2	KDC_ERR_SERVICE_EXP	Server's entry in KDC database has expired		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	3	0x3	KDC_ERR_BAD_PVNO	Requested Kerberos version number not su		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	4	0x4	KDC_ERR_C_OLD_MAST_K	Client's key encrypted in old master key		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	5	0x5	KDC_ERR_S_OLD_MAST_K	Server's key encrypted in old master key		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	6	0x6	KDC_ERR_C_PRINCIPAL_UI	Client not found in Kerberos database		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	7	0x7	KDC_ERR_S_PRINCIPAL_UI	Server not found in Kerberos database		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	8	0x8	KDC_ERR_PRINCIPAL_NOT	Multiple principal entries in KDC database		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	9	0x9	KDC_ERR_NULL_KEY	The client or server has a null key (master k		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	10	0xA	KDC_ERR_CANNOT_POSTD	Ticket (TGT) not eligible for postdating		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	11	0xB	KDC_ERR_NEVER_VALID	Requested start time is later than end time		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	12	0xC	KDC_ERR_POLICY	Requested start time is later than end time		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	13	0xD	KDC_ERR_BADOPTION	KDC cannot accommodate requested optio		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	14	0xE	KDC_ERR_ETYPE_NOTSUPI	KDC has no support for encryption type		1	High
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	15	0xF	KDC_ERR_SUMTYPE_NOSU	KDC has no support for checksum type		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	16	0x10	KDC_ERR_PADATA_TYPE_N	KDC has no support for PADATA type (pre-a		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	17	0x11	KDC_ERR_TRTYPE_NO_SU	KDC has no support for transited type		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	18	0x12	KDC_ERR_CLIENT_REVOKE	Client’s credentials have been revoked		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	19	0x13	KDC_ERR_SERVICE_REVOK	Credentials for server have been revoked		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	20	0x14	KDC_ERR_TGT_REVOKED	TGT has been revoked		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	21	0x15	KDC_ERR_CLIENT_NOTYET	Client not yet valid—try again later		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	22	0x16	KDC_ERR_SERVICE_NOTYE	Server not yet valid—try again later		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	23	0x17	KDC_ERR_KEY_EXPIRED	Password has expired—change password to		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	24	0x18	KDC_ERR_PREAUTH_FAILE	Pre-authentication information was invalid		1	High
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	25	0x19	KDC_ERR_PREAUTH_REQU	Additional preauthentication required		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	26	0x1A	KDC_ERR_SERVER_NOMAT	KDC does not know about the requested se		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	27	0x1B	KDC_ERR_SVC_UNAVAILAB	KDC is unavailable		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	31	0x1F	KRB_AP_ERR_BAD_INTEGI	Integrity check on decrypted field failed		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	32	0x20	KRB_AP_ERR_TKT_EXPIRE	The ticket has expired		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	33	0x21	KRB_AP_ERR_TKT_NYV	The ticket is not yet valid		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	34	0x22	KRB_AP_ERR_REPEAT	The request is a replay		4	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	35	0x23	KRB_AP_ERR_NOT_US	The ticket is not for us		4	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	36	0x24	KRB_AP_ERR_BADMATCH	The ticket and authenticator do not match		4	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	37	0x25	KRB_AP_ERR_SKEW	The clock skew is too great		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	38	0x26	KRB_AP_ERR_BADADDR	Network address in network layer header d		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	39	0x27	KRB_AP_ERR_BADVERSION	Protocol version numbers don't match (PVN		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	40	0x28	KRB_AP_ERR_MSG_TYPE	Message type is unsupported		3	Low

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	41	0x29	KRB_AP_ERR_MODIFIED	Message stream modified and checksum di		4	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	42	0x2A	KRB_AP_ERR_BADORDER	Message out of order (possible tampering)		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	44	0x2C	KRB_AP_ERR_BADKEYVER	Specified version of key is not available		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	45	0x2D	KRB_AP_ERR_NOKEY	Service key not available		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	46	0x2E	KRB_AP_ERR_MUT_FAIL	Mutual authentication failed		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	47	0x2F	KRB_AP_ERR_BADDIRECTI	Incorrect message direction		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	48	0x30	KRB_AP_ERR_METHOD	Alternative authentication method require		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	49	0x31	KRB_AP_ERR_BADSEQ	Incorrect sequence number in message		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	50	0x32	KRB_AP_ERR_INAPP_CKSU	Inappropriate type of checksum in message		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	51	0x33	KRB_AP_PATH_NOT_ACCE	Desired path is unreachable		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	52	0x34	KRB_ERR_RESPONSE_TOO	Too much data		1	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	60	0x3C	KRB_ERR_GENERIC	Generic error; the description is in the e-da		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	61	0x3D	KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	62	0x3E	KDC_ERR_CLIENT_NOT_TR	The client trust failed or is not implemente		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	63	0x3F	KDC_ERR_KDC_NOT_TRUS	The KDC server trust failed or could not be		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	64	0x40	KDC_ERR_INVALID_SIG	The signature is invalid		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	65	0x41	KDC_ERR_KEY_TOO_WEAK	A higher encryption level is needed		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	66	0x42	KRB_AP_ERR_USER_TO_U	User-to-user authorization is required		2	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	67	0x43	KRB_AP_ERR_NO_TGT	No TGT was presented or available		3	Low
675	Pre-authentication failed	Account Logon		Failure	4771	Result Code	68	0x44	KDC_ERR_WRONG_REALM	Incorrect domain or principal		3	Low
676	Authentication Ticket Request Failed	Account Logon		Failure	4768							3	Unknown
677	Service Ticket Request Failed	Account Logon		Failure								3	Unknown
678	Account Mapped for Logon by	Account Logon		Success	4774							1	Unknown
679	The name: %2 could not be mapped for log	Account Logon		Failure	4775							1	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000064		user name does not exist		3	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC000006A		user name is correct but the password is w		3	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000234		user is currently locked out		3	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000072		account is currently disabled		3	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC000006F		user tried to logon outside his day of week		4	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000070		workstation restriction		3	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000193		account expiration		2	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000071		expired password		2	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000224		user is required to change password at nex		2	Unknown
680	Account Used for Logon by	Account Logon		Success Fai	4776	Error Code	322122	0xC0000225		evidently a bug in Windows and not a risk		2	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000064		user name does not exist		3	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC000006A		user name is correct but the password is w		3	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000234		user is currently locked out		3	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000072		account is currently disabled		3	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC000006F		user tried to logon outside his day of week		4	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000070		workstation restriction		3	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000193		account expiration		2	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000071		expired password		2	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000224		user is required to change password at nex		2	Unknown
681	The logon to account	Account Logon		Failure	4776	Error Code	322122	0xC0000225		evidently a bug in Windows and not a risk		2	Unknown
682	Session reconnected to winstation	Logon/Logoff		Success	4778							3	Unknown
683	Session disconnected from winstation	Logon/Logoff		Success	4779							2	Unknown
684	Set ACLs of members in administrators grou	Account Management		Success	4780							3	Unknown
685	Account Name Changed	Account Management		Success	4781							1	Unknown
686	Password of the following user accessed	Account Management		Failure								3	Unknown
687	Basic Application Group Created	Account Management		Success Failure								1	Unknown
688	Basic Application Group Changed	Account Management		Success								1	Unknown
689	Basic Application Group Member Added	Account Management		Success	4785							1	Unknown
690	Basic Application Group Member Removed	Account Management		Success	4786							1	Unknown
691	Basic Application Group Non-Member Add	Account Management		Success	4787							1	Unknown
692	Basic Application Group Non-Member Rem	Account Management		Success Fai	4788							1	Unknown
693	Basic Application Group Deleted	Account Management		Success	4789							1	Unknown
694	LDAP Query Group Created	Account Management		Success	4790							1	Unknown
695	LDAP Query Group Changed	Account Management		Success	4791							1	Unknown
696	LDAP Query Group Deleted	Account Management		Success	4792							1	Unknown
697	Password Policy Checking API is called	Account Management		Success								1	Unknown
806	Per User Audit Policy was refreshed	Policy Change		Success								1	Unknown
807	Per user auditing policy set for user	Policy Change		Success	4912							2	Unknown
808	A security event source has attempted to re	Policy Change		Success	4904							3	Unknown
809	A security event source has attempted to u	Policy Change		Success	4905							3	Unknown
848	The following policy was active when the W	Policy Change		Success	4944							1	Unknown
849	An application was listed as an exception w	Policy Change		Success	4945							3	Unknown
850	A port was listed as an exception when the	Policy Change		Success	4945							3	Unknown
852	A change has been made to the Windows F	Policy Change		Success	4946							3	Unknown
861	The Windows Firewall has detected an app	Process Tracking		Success	5154							2	Unknown
1100	The event logging service has shut down	Non Audit (Even	Service s	Success								3	Unknown
1101	Audit events have been dropped by the tra	Non Audit (Even	Event pr	Success								3	Unknown
1102	The audit log was cleared	Non Audit (Even	Log clea	Success	517							3	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
1104	The security Log is now full	Non Audit (Even	Event pr	Success								3	Unknown
1105	Event log automatic backup	Non Audit (Even	Log autc	Success								2	Unknown
1108	The event logging service encountered an e	Non Audit (Even	Event pr	Failure								2	Unknown
4608	Windows is starting up	System	Security	Success	512							1	Unknown
4609	Windows is shutting down	System	Security	Success	513							1	Unknown
4610	An authentication package has been loaded	System	Security	Success	514							3	Unknown
4611	A trusted logon process has been registere	System	Security	Success	515							2	Unknown
4612	Internal resources allocated for the queuin	Non Audit (Even	Event pr	Success	516							3	Unknown
4614	A notification package has been loaded by	System	Security	Success	518							2	Unknown
4615	Invalid use of LPC port	System	Other Sy	Success	519							2	Unknown
4616	The system time was changed.	System	Security	Success	520							2	Unknown
4618	A monitored security event pattern has occ	Uncategorized	Subcate	Success								3	Unknown
4621	Administrator recovered system from Crash	Uncategorized	Subcate	Success								3	Unknown
4622	A security package has been loaded by the	System	Security	Success								2	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	2			Interactive logon at keyboard and screen of		1	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	3			Network logon		3	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	4			Batch i.e. scheduled task		2	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	5			Service startup		2	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	6			Proxy		1	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	7			Unlock i.e. unnattended workstation with p		1	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	8			NetworkCleartext Logon with credentials se		3	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	9			NewCredentials such as with RunAs or map		3	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	10			RemoteInteractive Terminal Services Remot		3	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	11			CachedInteractive logon with cached doma		2	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	12			CachedRemoteInteractive		2	Unknown
4624	An account was successfully logged on	Logon/Logoff	Logon	Success	528	Logon Type	13			CachedUnlock		2	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	2			Interactive logon at keyboard and screen of		1	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	3			Network logon		3	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	4			Batch i.e. scheduled task		2	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	5			Service startup		2	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	6			Proxy		1	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	7			Unlock i.e. unnattended workstation with p		1	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	8			NetworkCleartext Logon with credentials se		3	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	9			NewCredentials such as with RunAs or map		3	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	10			RemoteInteractive Terminal Services Remot		3	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	11			CachedInteractive logon with cached doma		2	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	12			CachedRemoteInteractive		2	Unknown
4625	An account was successfully logged on	Logon/Logoff	Logon	Success	529	Logon Type	13			CachedUnlock		2	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC000006A		user name is correct but the password is w		2	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000234		user is currently locked out		3	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000072		account is currently disabled		2	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC000006F		user tried to logon outside his day of week		3	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000070		workstation restriction		3	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000193		account expiration		3	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000071		expired password		2	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000133		clocks between DC and other computer toc		2	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000224		user is required to change password at nex		2	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xC0000225		evidently a bug in Windows and not a risk		2	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Status and Sub Status C		0xc000015b		The user has not been granted the requeste		3	Unknown
4625	An account failed to log on	Logon/Logoff	Logon	Failure	529	Logon Type	3			Network logon (fail	PTH	3	Unknown
4634	An account was logged off	Logon/Logoff	Logoff	Success	538							1	Unknown
4646	IKE DoS-prevention mode started	Uncategorized	Subcate	Success								2	Unknown
4647	User initiated logoff	Logon/Logoff	Logoff	Success	551							1	Unknown
4648	A logon was attempted using explicit crede	Logon/Logoff	Logon	Success	552							2	Unknown
4649	A replay attack was detected	Uncategorized	Subcate	Success								4	Low
4650	An IPsec Main Mode security association w	Logon/Logoff	IPsec Ma	Success								1	Unknown
4651	An IPsec Main Mode security association w	Logon/Logoff	IPsec Ma	Success								1	Unknown
4652	An IPsec Main Mode negotiation failed	Logon/Logoff	IPsec Ma	Failure								2	Unknown
4653	An IPsec Main Mode negotiation failed	Logon/Logoff	IPsec Ma	Failure								2	Unknown
4654	An IPsec Quick Mode negotiation failed	Logon/Logoff	IPsec Qu	Failure								2	Unknown
4655	An IPsec Main Mode security association en	Logon/Logoff	IPsec Ma	Success								1	Unknown
4656	A handle to an object was requested	Object Access	File Syst	Success Fai	560							1	Unknown
4657	A registry value was modified	Object Access	Registry	Success	567							1	Unknown
4658	The handle to an object was closed	Object Access	File Syst	Success	562							1	Unknown
4659	A handle to an object was requested with i	Object Access	Other O	Success	563							1	Unknown
4660	An object was deleted	Object Access	File Syst	Success	564							1	Unknown
4661	A handle to an object was requested	Object Access	SAM	Success	565							2	Unknown
4662	An operation was performed on an object	Directory Service	Director	Success	566							1	Unknown
4663	An attempt was made to access an object	Object Access	File Syst	Success	567							1	Unknown
4664	An attempt was made to create a hard link	Object Access	Other O	Success								2	Unknown
4665	An attempt was made to create an applicat	Object Access	Applicat	Success								1	Unknown
4666	An application attempted an operation	Object Access	Applicat	Success	i got the raw event for this. Please update the same in the event details.							1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4667	An application client context was deleted	Object Access	Applicat	Success	i got the raw event for this. Please update this in the event details							1	Unknown
4668	An application was initialized	Object Access	Applicat	Success								1	Unknown
4670	Permissions on an object were changed	Object Access	File Syst	Success								2	Unknown
4671	An application attempted to access a block	Object Access	Other O	Success								2	Unknown
4672	Special privileges assigned to new logon	Logon/Logoff	Special L	Success	576						Very noisy - includes re	2	Unknown
4673	A privileged service was called	Privilege Use	Sensitive	Success	577							3	Unknown
4674	An operation was attempted on a privilege	Privilege Use	Sensitive	Success	578							2	Unknown
4675	SIDs were filtered	Uncategorized	Subcate	Success								2	Unknown
4685	The state of a transaction has changed	Object Access	File Syst	Success								1	Unknown
4688	A new process has been created	Process Tracking	Process	Success	592						[1]	3	Unknown
4689	A process has exited	Process Tracking	Process	Success	593							1	Unknown
4690	An attempt was made to duplicate a handle	Object Access	Handle M	Success	594							1	Unknown
4691	Indirect access to an object was requested	Object Access	Other O	Success								1	Unknown
4692	Backup of data protection master key was a	Process Tracking	DPAPI Ac	Success								3	Unknown
4693	Recovery of data protection master key wa	Process Tracking	DPAPI Ac	Success								3	Unknown
4694	Protection of auditable protected data was	Process Tracking	DPAPI Ac	Success								3	Unknown
4695	Unprotection of auditable protected data w	Process Tracking	DPAPI Ac	Failure								3	Unknown
4696	A primary token was assigned to process	Process Tracking	Process	Success	600							2	Unknown
4697	A service was installed in the system	System	Security	Success	601							3	Unknown
4698	A scheduled task was created	Object Access	Other O	Success	602							3	Unknown
4699	A scheduled task was deleted	Object Access	Other O	Success	602							3	Unknown
4700	A scheduled task was enabled	Object Access	Other O	Success	602							2	Unknown
4701	A scheduled task was disabled	Object Access	Other O	Success	602							2	Unknown
4702	A scheduled task was updated	Object Access	Other O	Success	602							2	Unknown
4704	A user right was assigned	Policy Change	Authoriz	Success	608							2	Unknown
4705	A user right was removed	Policy Change	Authoriz	Success	609							2	Unknown
4706	A new trust was created to a domain	Policy Change	Authent	Success	610							4	Unknown
4707	A trust to a domain was removed	Policy Change	Authent	Success	611							3	Unknown
4709	IPsec Services was started	Policy Change	Filtering	Success								2	Unknown
4710	IPsec Services was disabled	Policy Change	Filtering	Success								1	Unknown
4711	PAStore Engine	Policy Change	Filtering	Success								1	Unknown
4712	IPsec Services encountered a potentially se	Policy Change	Filtering	Failure								2	Unknown
4713	Kerberos policy was changed	Policy Change	Authent	Success	617							3	Unknown
4714	Encrypted data recovery policy was change	Policy Change	Authoriz	Success	618							3	Unknown
4715	The audit policy (SACL) on an object was ch	Policy Change	Audit Po	Success								2	Unknown
4716	Trusted domain information was modified	Policy Change	Authent	Success	620							2	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4717	System security access was granted to an a	Policy Change	Authent	Success	621							2	Unknown
4718	System security access was removed from a	Policy Change	Authent	Success	622							2	Unknown
4719	System audit policy was changed	Policy Change	Audit Po	Success	612							3	Unknown
4720	A user account was created	Account Manage	User Acc	Success	624							3	Unknown
4722	A user account was enabled	Account Manage	User Acc	Success	626							2	Unknown
4723	An attempt was made to change an accoun	Account Manage	User Acc	Success	627							2	Unknown
4724	An attempt was made to reset an accounts	Account Manage	User Acc	Success	628							2	Unknown
4725	A user account was disabled	Account Manage	User Acc	Success	629							2	Unknown
4726	A user account was deleted	Account Manage	User Acc	Success	630							2	Unknown
4727	A security-enabled global group was create	Account Manage	Security	Success	631							2	Unknown
4728	A member was added to a security-enablec	Account Manage	Security	Success	632							3	Unknown
4729	A member was removed from a security-en	Account Manage	Security	Success	633							1	Unknown
4730	A security-enabled global group was delete	Account Manage	Security	Success	634							1	Unknown
4731	A security-enabled local group was created	Account Manage	Security	Success	635							2	Unknown
4732	A member was added to a security-enablec	Account Manage	Security	Success	636							3	Unknown
4733	A member was removed from a security-en	Account Manage	Security	Success	637							1	Unknown
4734	A security-enabled local group was deleted	Account Manage	Security	Success	638							1	Unknown
4735	A security-enabled local group was changec	Account Manage	Security	Success	639							2	Unknown
4737	A security-enabled global group was chang	Account Manage	Security	Success	641							2	Unknown
4738	A user account was changed	Account Manage	User Acc	Success	642							2	Unknown
4739	Domain Policy was changed	Account Manage	Other Ac	Success	643							2	Unknown
4740	A user account was locked out	Account Manage	User Acc	Success	644							3	Unknown
4741	A computer account was created	Account Manage	Comput	Success	645							2	Unknown
4742	A computer account was changed	Account Manage	Comput	Success	646							2	Unknown
4743	A computer account was deleted	Account Manage	Comput	Success	647							1	Unknown
4744	A security-disabled local group was created	Account Manage	Distribut	Success	648							2	Unknown
4745	A security-disabled local group was change	Account Manage	Distribut	Success	649							1	Unknown
4746	A member was added to a security-disablec	Account Manage	Distribut	Success	650							1	Unknown
4747	A member was removed from a security-di	Account Manage	Distribut	Success	651							1	Unknown
4748	A security-disabled local group was deleted	Account Manage	Distribut	Success	652							1	Unknown
4749	A security-disabled global group was create	Account Manage	Distribut	Success	653							1	Unknown
4750	A security-disabled global group was chang	Account Manage	Distribut	Success	654							1	Unknown
4751	A member was added to a security-disablec	Account Manage	Distribut	Success	655							1	Unknown
4752	A member was removed from a security-di	Account Manage	Distribut	Success	656							1	Unknown
4753	A security-disabled global group was delete	Account Manage	Distribut	Success	657							1	Unknown
4754	A security-enabled universal group was cre	Account Manage	Security	Success	658							2	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4755	A security-enabled universal group was cha	Account Manage	Security	Success	659							2	Unknown
4756	A member was added to a security-enablec	Account Manage	Security	Success	660							3	Unknown
4757	A member was removed from a security-en	Account Manage	Security	Success	661							1	Unknown
4758	A security-enabled universal group was del	Account Manage	Security	Success	662							1	Unknown
4759	A security-disabled universal group was cre	Account Manage	Distribut	Success	663							2	Unknown
4760	A security-disabled universal group was cha	Account Manage	Distribut	Success	664							2	Unknown
4761	A member was added to a security-disablec	Account Manage	Distribut	Success	655							2	Unknown
4762	A member was removed from a security-dis	Account Manage	Distribut	Success	666							1	Unknown
4763	A security-disabled universal group was del	Account Manage	Distribut	Success	667							1	Unknown
4764	A groups type was changed	Account Manage	Security	Success	668							2	Unknown
4765	SID History was added to an account	Account Manage	User Acc	Success								3	Unknown
4766	An attempt to add SID History to an accoun	Account Manage	User Acc	Failure								4	Unknown
4767	A user account was unlocked	Account Manage	User Acc	Success	671							1	Unknown
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	0	0x0	KDC_ERR_NONE	No error		0	
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	1	0x1	KDC_ERR_NAME_EXP	Client's entry in KDC database has expired		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	2	0x2	KDC_ERR_SERVICE_EXP	Server's entry in KDC database has expired		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	3	0x3	KDC_ERR_BAD_PVNO	Requested Kerberos version number not su		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	4	0x4	KDC_ERR_C_OLD_MAST_K	Client's key encrypted in old master key		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	5	0x5	KDC_ERR_S_OLD_MAST_K	Server's key encrypted in old master key		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	6	0x6	KDC_ERR_C_PRINCIPAL_UI	Client not found in Kerberos database		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	7	0x7	KDC_ERR_S_PRINCIPAL_UI	Server not found in Kerberos database		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	8	0x8	KDC_ERR_PRINCIPAL_NOT	Multiple principal entries in KDC database		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	9	0x9	KDC_ERR_NULL_KEY	The client or server has a null key (master k		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	10	0xA	KDC_ERR_CANNOT_POSTD	Ticket (TGT) not eligible for postdating		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	11	0xB	KDC_ERR_NEVER_VALID	Requested start time is later than end time		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	12	0xC	KDC_ERR_POLICY	Requested start time is later than end time		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	13	0xD	KDC_ERR_BADOPTION	KDC cannot accommodate requested optio		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	14	0xE	KDC_ERR_ETYPE_NOTSUPI	KDC has no support for encryption type		1	High
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	15	0xF	KDC_ERR_SUMTYPE_NOSU	KDC has no support for checksum type		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	16	0x10	KDC_ERR_PADATA_TYPE_N	KDC has no support for PADATA type (pre-a		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	17	0x11	KDC_ERR_TRTYPE_NO_SU	KDC has no support for transited type		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	18	0x12	KDC_ERR_CLIENT_REVOKE	Client’s credentials have been revoked		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	19	0x13	KDC_ERR_SERVICE_REVOK	Credentials for server have been revoked		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	20	0x14	KDC_ERR_TGT_REVOKED	TGT has been revoked		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	21	0x15	KDC_ERR_CLIENT_NOTYET	Client not yet valid—try again later		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	22	0x16	KDC_ERR_SERVICE_NOTYE	Server not yet valid—try again later		1	Low

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	23	0x17	KDC_ERR_KEY_EXPIRED	Password has expired—change password to		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	24	0x18	KDC_ERR_PREAUTH_FAILE	Pre-authentication information was invalid		1	High
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	25	0x19	KDC_ERR_PREAUTH_REQU	Additional preauthentication required		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	26	0x1A	KDC_ERR_SERVER_NOMAT	KDC does not know about the requested se		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	27	0x1B	KDC_ERR_SVC_UNAVAILAE	KDC is unavailable		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	31	0x1F	KRB_AP_ERR_BAD_INTEGI	Integrity check on decrypted field failed		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	32	0x20	KRB_AP_ERR_TKT_EXPIRE	The ticket has expired		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	33	0x21	KRB_AP_ERR_TKT_NYV	The ticket is not yet valid		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	34	0x22	KRB_AP_ERR_REPEAT	The request is a replay		4	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	35	0x23	KRB_AP_ERR_NOT_US	The ticket is not for us		4	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	36	0x24	KRB_AP_ERR_BADMATCH	The ticket and authenticator do not match		4	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	37	0x25	KRB_AP_ERR_SKEW	The clock skew is too great		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	38	0x26	KRB_AP_ERR_BADADDR	Network address in network layer header d		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	39	0x27	KRB_AP_ERR_BADVERSION	Protocol version numbers don't match (PVN		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	40	0x28	KRB_AP_ERR_MSG_TYPE	Message type is unsupported		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	41	0x29	KRB_AP_ERR_MODIFIED	Message stream modified and checksum di		4	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	42	0x2A	KRB_AP_ERR_BADORDER	Message out of order (possible tampering)		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	44	0x2C	KRB_AP_ERR_BADKEYVER	Specified version of key is not available		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	45	0x2D	KRB_AP_ERR_NOKEY	Service key not available		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	46	0x2E	KRB_AP_ERR_MUT_FAIL	Mutual authentication failed		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	47	0x2F	KRB_AP_ERR_BADDIRECTI	Incorrect message direction		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	48	0x30	KRB_AP_ERR_METHOD	Alternative authentication method required		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	49	0x31	KRB_AP_ERR_BADSEQ	Incorrect sequence number in message		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	50	0x32	KRB_AP_ERR_INAPP_CKSU	Inappropriate type of checksum in message		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	51	0x33	KRB_AP_PATH_NOT_ACCE	Desired path is unreachable		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	52	0x34	KRB_ERR_RESPONSE_TOO	Too much data		1	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	60	0x3C	KRB_ERR_GENERIC	Generic error; the description is in the e-da		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	61	0x3D	KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	62	0x3E	KDC_ERR_CLIENT_NOT_TR	The client trust failed or is not implemente		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	63	0x3F	KDC_ERR_KDC_NOT_TRUS	The KDC server trust failed or could not be		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	64	0x40	KDC_ERR_INVALID_SIG	The signature is invalid		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	65	0x41	KDC_ERR_KEY_TOO_WEAK	A higher encryption level is needed		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	66	0x42	KRB_AP_ERR_USER_TO_U	User-to-user authorization is required		2	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	67	0x43	KRB_AP_ERR_NO_TGT	No TGT was presented or available		3	Low
4768	A Kerberos authentication ticket (TGT) was	Account Logon	Kerberos	Success Fai	672	Failure Code	68	0x44	KDC_ERR_WRONG_REALM	Incorrect domain or principal		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	0	0x0	KDC_ERR_NONE	No error		0	

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	1	0x1	KDC_ERR_NAME_EXP	Client's entry in KDC database has expired		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	2	0x2	KDC_ERR_SERVICE_EXP	Server's entry in KDC database has expired		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	3	0x3	KDC_ERR_BAD_PVNO	Requested Kerberos version number not su		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	4	0x4	KDC_ERR_C_OLD_MAST_K	Client's key encrypted in old master key		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	5	0x5	KDC_ERR_S_OLD_MAST_K	Server's key encrypted in old master key		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	6	0x6	KDC_ERR_C_PRINCIPAL_UI	Client not found in Kerberos database		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	7	0x7	KDC_ERR_S_PRINCIPAL_UI	Server not found in Kerberos database		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	8	0x8	KDC_ERR_PRINCIPAL_NOT	Multiple principal entries in KDC database		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	9	0x9	KDC_ERR_NULL_KEY	The client or server has a null key (master k		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	10	0xA	KDC_ERR_CANNOT_POSTD	Ticket (TGT) not eligible for postdating		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	11	0xB	KDC_ERR_NEVER_VALID	Requested start time is later than end time		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	12	0xC	KDC_ERR_POLICY	Requested start time is later than end time		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	13	0xD	KDC_ERR_BADOPTION	KDC cannot accommodate requested optio		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	14	0xE	KDC_ERR_ETYPE_NOTSUPI	KDC has no support for encryption type		1	High
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	15	0xF	KDC_ERR_SUMTYPE_NOSU	KDC has no support for checksum type		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	16	0x10	KDC_ERR_PADATA_TYPE_N	KDC has no support for PADATA type (pre-a		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	17	0x11	KDC_ERR_TRTYPE_NO_SU	KDC has no support for transited type		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	18	0x12	KDC_ERR_CLIENT_REVOKE	Client’s credentials have been revoked		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	19	0x13	KDC_ERR_SERVICE_REVOK	Credentials for server have been revoked		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	20	0x14	KDC_ERR_TGT_REVOKED	TGT has been revoked		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	21	0x15	KDC_ERR_CLIENT_NOTYET	Client not yet valid—try again later		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	22	0x16	KDC_ERR_SERVICE_NOTYE	Server not yet valid—try again later		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	23	0x17	KDC_ERR_KEY_EXPIRED	Password has expired—change password to		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	24	0x18	KDC_ERR_PREAUTH_FAILE	Pre-authentication information was invalid		1	High
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	25	0x19	KDC_ERR_PREAUTH_REQU	Additional preauthentication required		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	26	0x1A	KDC_ERR_SERVER_NOMAT	KDC does not know about the requested se		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	27	0x1B	KDC_ERR_SVC_UNAVAILAB	KDC is unavailable		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	31	0x1F	KRB_AP_ERR_BAD_INTEGR	Integrity check on decrypted field failed		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	32	0x20	KRB_AP_ERR_TKT_EXPIRE	The ticket has expired		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	33	0x21	KRB_AP_ERR_TKT_NYV	The ticket is not yet valid		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	34	0x22	KRB_AP_ERR_REPEAT	The request is a replay		4	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	35	0x23	KRB_AP_ERR_NOT_US	The ticket is not for us		4	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	36	0x24	KRB_AP_ERR_BADMATCH	The ticket and authenticator do not match		4	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	37	0x25	KRB_AP_ERR_SKEW	The clock skew is too great		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	38	0x26	KRB_AP_ERR_BADADDR	Network address in network layer header d		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	39	0x27	KRB_AP_ERR_BADVERSION	Protocol version numbers don't match (PVN		3	Low

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	40	0x28	KRB_AP_ERR_MSG_TYPE	Message type is unsupported		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	41	0x29	KRB_AP_ERR_MODIFIED	Message stream modified and checksum di		4	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	42	0x2A	KRB_AP_ERR_BADORDER	Message out of order (possible tampering)		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	44	0x2C	KRB_AP_ERR_BADKEYVER	Specified version of key is not available		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	45	0x2D	KRB_AP_ERR_NOKEY	Service key not available		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	46	0x2E	KRB_AP_ERR_MUT_FAIL	Mutual authentication failed		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	47	0x2F	KRB_AP_ERR_BADDIRECTI	Incorrect message direction		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	48	0x30	KRB_AP_ERR_METHOD	Alternative authentication method require		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	49	0x31	KRB_AP_ERR_BADSEQ	Incorrect sequence number in message		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	50	0x32	KRB_AP_ERR_INAPP_CKSU	Inappropriate type of checksum in message		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	51	0x33	KRB_AP_PATH_NOT_ACCE	Desired path is unreachable		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	52	0x34	KRB_ERR_RESPONSE_TOO	Too much data		1	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	60	0x3C	KRB_ERR_GENERIC	Generic error; the description is in the e-da		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	61	0x3D	KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	62	0x3E	KDC_ERR_CLIENT_NOT_TR	The client trust failed or is not implemente		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	63	0x3F	KDC_ERR_KDC_NOT_TRUS	The KDC server trust failed or could not be		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	64	0x40	KDC_ERR_INVALID_SIG	The signature is invalid		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	65	0x41	KDC_ERR_KEY_TOO_WEAK	A higher encryption level is needed		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	66	0x42	KRB_AP_ERR_USER_TO_U	User-to-user authorization is required		2	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	67	0x43	KRB_AP_ERR_NO_TGT	No TGT was presented or available		3	Low
4769	A Kerberos service ticket was requested	Account Logon	Kerberos	Success Fai	673	Failure Code	68	0x44	KDC_ERR_WRONG_REALM	Incorrect domain or principal		3	Low
4770	A Kerberos service ticket was renewed	Account Logon	Kerberos	Success	674							1	Unknown
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	0	0x0	KDC_ERR_NONE	No error		0	
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	1	0x1	KDC_ERR_NAME_EXP	Client's entry in KDC database has expired		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	2	0x2	KDC_ERR_SERVICE_EXP	Server's entry in KDC database has expired		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	3	0x3	KDC_ERR_BAD_PVNO	Requested Kerberos version number not su		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	4	0x4	KDC_ERR_C_OLD_MAST_K	Client's key encrypted in old master key		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	5	0x5	KDC_ERR_S_OLD_MAST_K	Server's key encrypted in old master key		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	6	0x6	KDC_ERR_C_PRINCIPAL_UI	Client not found in Kerberos database		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	7	0x7	KDC_ERR_S_PRINCIPAL_UI	Server not found in Kerberos database		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	8	0x8	KDC_ERR_PRINCIPAL_NOT	Multiple principal entries in KDC database		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	9	0x9	KDC_ERR_NULL_KEY	The client or server has a null key (master k		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	10	0xA	KDC_ERR_CANNOT_POSTD	Ticket (TGT) not eligible for postdating		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	11	0xB	KDC_ERR_NEVER_VALID	Requested start time is later than end time		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	12	0xC	KDC_ERR_POLICY	Requested start time is later than end time		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	13	0xD	KDC_ERR_BADOPTION	KDC cannot accommodate requested optio		2	Low

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	14	0xE	KDC_ERR_ETYPE_NOTSUPI	KDC has no support for encryption type		1	High
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	15	0xF	KDC_ERR_SUMTYPE_NOSU	KDC has no support for checksum type		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	16	0x10	KDC_ERR_PADATA_TYPE_N	KDC has no support for PADATA type (pre-a		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	17	0x11	KDC_ERR_TRTYPE_NO_SU	KDC has no support for transited type		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	18	0x12	KDC_ERR_CLIENT_REVOKE	Client’s credentials have been revoked		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	19	0x13	KDC_ERR_SERVICE_REVOK	Credentials for server have been revoked		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	20	0x14	KDC_ERR_TGT_REVOKED	TGT has been revoked		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	21	0x15	KDC_ERR_CLIENT_NOTYET	Client not yet valid—try again later		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	22	0x16	KDC_ERR_SERVICE_NOTYE	Server not yet valid—try again later		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	23	0x17	KDC_ERR_KEY_EXPIRED	Password has expired—change password to		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	24	0x18	KDC_ERR_PREAUTH_FAILE	Pre-authentication information was invalid		1	High
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	25	0x19	KDC_ERR_PREAUTH_REQU	Additional preauthentication required		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	26	0x1A	KDC_ERR_SERVER_NOMAT	KDC does not know about the requested se		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	27	0x1B	KDC_ERR_SVC_UNAVAILAE	KDC is unavailable		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	31	0x1F	KRB_AP_ERR_BAD_INTEGI	Integrity check on decrypted field failed		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	32	0x20	KRB_AP_ERR_TKT_EXPIRE	The ticket has expired		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	33	0x21	KRB_AP_ERR_TKT_NYV	The ticket is not yet valid		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	34	0x22	KRB_AP_ERR_REPEAT	The request is a replay		4	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	35	0x23	KRB_AP_ERR_NOT_US	The ticket is not for us		4	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	36	0x24	KRB_AP_ERR_BADMATCH	The ticket and authenticator do not match		4	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	37	0x25	KRB_AP_ERR_SKEW	The clock skew is too great		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	38	0x26	KRB_AP_ERR_BADADDR	Network address in network layer header d		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	39	0x27	KRB_AP_ERR_BADVERSION	Protocol version numbers don't match (PVN		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	40	0x28	KRB_AP_ERR_MSG_TYPE	Message type is unsupported		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	41	0x29	KRB_AP_ERR_MODIFIED	Message stream modified and checksum di		4	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	42	0x2A	KRB_AP_ERR_BADORDER	Message out of order (possible tampering)		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	44	0x2C	KRB_AP_ERR_BADKEYVER	Specified version of key is not available		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	45	0x2D	KRB_AP_ERR_NOKEY	Service key not available		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	46	0x2E	KRB_AP_ERR_MUT_FAIL	Mutual authentication failed		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	47	0x2F	KRB_AP_ERR_BADDIRECTI	Incorrect message direction		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	48	0x30	KRB_AP_ERR_METHOD	Alternative authentication method required		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	49	0x31	KRB_AP_ERR_BADSEQ	Incorrect sequence number in message		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	50	0x32	KRB_AP_ERR_INAPP_CKSU	Inappropriate type of checksum in message		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	51	0x33	KRB_AP_PATH_NOT_ACCE	Desired path is unreachable		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	52	0x34	KRB_ERR_RESPONSE_TOO	Too much data		1	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	60	0x3C	KRB_ERR_GENERIC	Generic error; the description is in the e-da		2	Low

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	61	0x3D	KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	62	0x3E	KDC_ERR_CLIENT_NOT_TR	The client trust failed or is not implemente		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	63	0x3F	KDC_ERR_KDC_NOT_TRUS	The KDC server trust failed or could not be		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	64	0x40	KDC_ERR_INVALID_SIG	The signature is invalid		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	65	0x41	KDC_ERR_KEY_TOO_WEAK	A higher encryption level is needed		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	66	0x42	KRB_AP_ERR_USER_TO_U	User-to-user authorization is required		2	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	67	0x43	KRB_AP_ERR_NO_TGT	No TGT was presented or available		3	Low
4771	Kerberos pre-authentication failed	Account Logon	Kerberos	Success Fai	675	Failure Code	68	0x44	KDC_ERR_WRONG_REALM	Incorrect domain or principal		3	Low
4772	A Kerberos authentication ticket request fa	Account Logon	Kerberos	Failure	672							2	Unknown
4773	A Kerberos service ticket request failed	Account Logon	Kerberos	Failure	673							2	Unknown
4774	An account was mapped for logon	Account Logon	Other Ac	Success	678							1	Unknown
4775	An account could not be mapped for logon	Account Logon	Credenti	Failure	679							2	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Success	680							2	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC0000064		user name does not exist		2	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC000006A		user name is correct but the password is w		2	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC0000234		user is currently locked out		3	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC0000072		account is currently disabled		3	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC000006F		user tried to logon outside his day of week		3	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC0000070		workstation restriction		3	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC0000193		account expiration		3	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC0000071		expired password		2	Unknown
4776	The domain controller attempted to validat	Account Logon	Credenti	Failure	681			0xC0000224		user is required to change password at next		2	Unknown
4776	The domain controller attempted to validate the credentials for an ac			Failure	681			0xC0000225		evidently a bug in Windows and not a risk		2	Unknown
4777	The domain controller failed to validate the	Account Logon	Credenti	Failure								2	Unknown
4778	A session was reconnected to a Window St	Logon/Logoff	Other Lo	Success	682							1	Unknown
4779	A session was disconnected from a Windov	Logon/Logoff	Other Lo	Success	683							1	Unknown
4780	The ACL was set on accounts which are me	Account Manage	User Acc	Success	684							2	Unknown
4781	The name of an account was changed	Account Manage	User Acc	Success	685							2	Unknown
4782	The password hash an account was accesse	Account Manage	Other Ac	Success								3	Unknown
4783	A basic application group was created	Account Manage	Applicat	Success	667							1	Unknown
4784	A basic application group was changed	Account Manage	Applicat	Success								1	Unknown
4785	A member was added to a basic applicatior	Account Manage	Applicat	Success	689							1	Unknown
4786	A member was removed from a basic appli	Account Manage	Applicat	Success	690							1	Unknown
4787	A non-member was added to a basic applic	Account Manage	Applicat	Success	691							1	Unknown
4788	A non-member was removed from a basic a	Account Manage	Applicat	Success	692							1	Unknown
4789	A basic application group was deleted	Account Manage	Applicat	Success	693							1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4790	An LDAP query group was created	Account Manage	Applicat	Success	694							1	Unknown
4791	A basic application group was changed	Account Manage	Applicat	Success	695							1	Unknown
4792	An LDAP query group was deleted	Account Manage	Applicat	Success	696							1	Unknown
4793	The Password Policy Checking API was calle	Account Manage	Other Ac	Success								2	Unknown
4794	An attempt was made to set the Directory S	Account Manage	User Acc	Success								2	Unknown
4800	The workstation was locked	Logon/Logoff	Other Lo	Success								1	Unknown
4801	The workstation was unlocked	Logon/Logoff	Other Lo	Success								1	Unknown
4802	The screen saver was invoked	Logon/Logoff	Other Lo	Success								1	Unknown
4803	The screen saver was dismissed	Logon/Logoff	Other Lo	Success								1	Unknown
4816	RPC detected an integrity violation while de	Process Tracking	RPC Eve	Success								3	Unknown
4817	Auditing settings on object were changed.	Policy Change	Audit Po	Success								2	Unknown
4864	A namespace collision was detected	Uncategorized	Subcate	Success								1	Unknown
4865	A trusted forest information entry was add	Policy Change	Authent	Success								3	Unknown
4866	A trusted forest information entry was rem	Policy Change	Authent	Success								2	Unknown
4867	A trusted forest information entry was moc	Policy Change	Authent	Success								3	Unknown
4868	The certificate manager denied a pending c	Object Access	Certifica	Success								2	Unknown
4869	Certificate Services received a resubmitted	Object Access	Certifica	Success								2	Unknown
4870	Certificate Services revoked a certificate	Object Access	Certifica	Success								2	Unknown
4871	Certificate Services received a request to pu	Object Access	Certifica	Success								2	Unknown
4872	Certificate Services published the certificat	Object Access	Certifica	Success								1	Unknown
4873	A certificate request extension changed	Object Access	Certifica	Success								1	Unknown
4874	One or more certificate request attributes c	Object Access	Certifica	Success								1	Unknown
4875	Certificate Services received a request to sh	Object Access	Certifica	Success								1	Unknown
4876	Certificate Services backup started	Object Access	Certifica	Success								1	Unknown
4877	Certificate Services backup completed	Object Access	Certifica	Success								1	Unknown
4878	Certificate Services restore started	Object Access	Certifica	Success								3	Unknown
4879	Certificate Services restore completed	Object Access	Certifica	Success								3	Unknown
4880	Certificate Services started	Object Access	Certifica	Success								1	Unknown
4881	Certificate Services stopped	Object Access	Certifica	Success								1	Unknown
4882	The security permissions for Certificate Ser	Object Access	Certifica	Success								2	Unknown
4883	Certificate Services retrieved an archived ke	Object Access	Certifica	Success								2	Unknown
4884	Certificate Services imported a certificate in	Object Access	Certifica	Success								1	Unknown
4885	The audit filter for Certificate Services chan	Object Access	Certifica	Success								3	Unknown
4886	Certificate Services received a certificate re	Object Access	Certifica	Success								1	Unknown
4887	Certificate Services approved a certificate r	Object Access	Certifica	Success								1	Unknown
4888	Certificate Services denied a certificate req	Object Access	Certifica	Failure								1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4889	Certificate Services set the status of a certif	Object Access	Certifica	Success								1	Unknown
4890	The certificate manager settings for Certific	Object Access	Certifica	Success								1	Unknown
4891	A configuration entry changed in Certificate	Object Access	Certifica	Success								2	Unknown
4892	A property of Certificate Services changed	Object Access	Certifica	Success								2	Unknown
4893	Certificate Services archived a key	Object Access	Certifica	Success								1	Unknown
4894	Certificate Services imported and archived	Object Access	Certifica	Success								2	Unknown
4895	Certificate Services published the CA certifi	Object Access	Certifica	Success								1	Unknown
4896	One or more rows have been deleted from	Object Access	Certifica	Success								2	Unknown
4897	Role separation enabled	Object Access	Certifica	Success								1	Unknown
4898	Certificate Services loaded a template	Object Access	Certifica	Success								1	Unknown
4899	A Certificate Services template was update	Object Access	Certifica	Success								1	Unknown
4900	Certificate Services template security was u	Object Access	Certifica	Success								1	Unknown
4902	The Per-user audit policy table was created	Policy Change	Audit Po	Success								1	Unknown
4904	An attempt was made to register a security	Policy Change	Audit Po	Success	808							2	Unknown
4905	An attempt was made to unregister a secur	Policy Change	Audit Po	Success	809							1	Unknown
4906	The CrashOnAuditFail value has changed	Policy Change	Audit Po	Success								3	Unknown
4907	Auditing settings on object were changed	Policy Change	Audit Po	Success							reference for security d https://technet.microsc	2	Unknown
4908	Special Groups Logon table modified	Policy Change	Audit Po	Success								2	Unknown
4909	The local policy settings for the TBS were ch	Uncategorized	Subcate	Success								2	Unknown
4910	The group policy settings for the TBS were	Uncategorized	Subcate	Success								2	Unknown
4912	Per User Audit Policy was changed	Policy Change	Audit Po	Success	807							2	Unknown
4928	An Active Directory replica source naming c	Directory Service	Director	Success								2	Unknown
4929	An Active Directory replica source naming c	Directory Service	Detailed	Success								2	Unknown
4930	An Active Directory replica source naming c	Directory Service	Detailed	Success								2	Unknown
4931	An Active Directory replica destination nam	Directory Service	Detailed	Success								2	Unknown
4932	Synchronization of a replica of an Active Dir	Directory Service	Director	Success								1	Unknown
4933	Synchronization of a replica of an Active Dir	Directory Service	Director	Success								1	Unknown
4934	Attributes of an Active Directory object wer	Directory Service	Detailed	Success								1	Unknown
4935	Replication failure begins	Directory Service	Detailed	Success								2	Unknown
4936	Replication failure ends	Directory Service	Director	Success								2	Unknown
4937	A lingering object was removed from a repl	Directory Service	Director	Success								2	Unknown
4944	The following policy was active when the W	Policy Change	MPSSVC	Success	848							1	Unknown
4945	A rule was listed when the Windows Firewa	Policy Change	MPSSVC	Success	849							2	Unknown
4946	A change has been made to Windows Firev	Policy Change	MPSSVC	Success	852							3	Unknown
4947	A change has been made to Windows Firev	Policy Change	MPSSVC	Success	852							1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
4948	A change has been made to Windows Firev	Policy Change	MPSSVC	Success	852							1	Unknown
4949	Windows Firewall settings were restored to	Policy Change	MPSSVC	Success								2	Unknown
4950	A Windows Firewall setting has changed	Policy Change	MPSSVC	Success								2	Unknown
4951	A rule has been ignored because its major v	Policy Change	MPSSVC	Success								1	Unknown
4952	Parts of a rule have been ignored because i	Policy Change	MPSSVC	Success								1	Unknown
4953	A rule has been ignored by Windows Firewa	Uncategorized	Subcate	Success								1	Unknown
4954	Windows Firewall Group Policy settings has	Policy Change	MPSSVC	Success								2	Unknown
4956	Windows Firewall has changed the active p	Policy Change	MPSSVC	Success								2	Unknown
4957	Windows Firewall did not apply the followi	Policy Change	MPSSVC	Failure								2	Unknown
4958	Windows Firewall did not apply the followi	Policy Change	MPSSVC	Success								2	Unknown
4960	IPsec dropped an inbound packet that faile	Uncategorized	Subcate	Success								2	Unknown
4961	IPsec dropped an inbound packet that faile	Uncategorized	Subcate	Success								2	Unknown
4962	IPsec dropped an inbound packet that faile	Uncategorized	Subcate	Success								2	Unknown
4963	IPsec dropped an inbound clear text packet	Uncategorized	Subcate	Success	Event ID 4963						list of SIDs https://support.microsc	3	Unknown
4964	Special groups have been assigned to a nev	Logon/Logoff	Special L	Success								2	Unknown
4965	IPsec received a packet from a remote com	Uncategorized	Subcate	Success								3	Unknown
4976	During Main Mode negotiation, IPsec recei	Logon/Logoff	IPsec Ma	Success								3	Unknown
4977	During Quick Mode negotiation, IPsec recei	Logon/Logoff	IPsec Qu	Success								3	Unknown
4978	During Extended Mode negotiation, IPsec r	Logon/Logoff	IPsec Ext	Success								3	Unknown
4979	IPsec Main Mode and Extended Mode secu	Logon/Logoff	IPsec Ma	Success								1	Unknown
4980	IPsec Main Mode and Extended Mode secu	Logon/Logoff	IPsec Ma	Success								1	Unknown
4981	IPsec Main Mode and Extended Mode secu	Logon/Logoff	IPsec Ma	Success								1	Unknown
4982	IPsec Main Mode and Extended Mode secu	Logon/Logoff	IPsec Ma	Success								1	Unknown
4983	An IPsec Extended Mode negotiation failed	Logon/Logoff	IPsec Ma	Success								2	Unknown
4984	An IPsec Extended Mode negotiation failed	Logon/Logoff	IPsec Ma	Success								2	Unknown
4985	The state of a transaction has changed	Object Access	File Syst	Success								1	Unknown
5024	The Windows Firewall Service has started s	System	Other Sy	Success								1	Unknown
5025	The Windows Firewall Service has been sto	System	Other Sy	Success								2	Unknown
5027	The Windows Firewall Service was unable t	System	Other Sy	Success								2	Unknown
5028	The Windows Firewall Service was unable t	System	Other Sy	Success								2	Unknown
5029	The Windows Firewall Service failed to initi	System	Other Sy	Success								2	Unknown
5030	The Windows Firewall Service failed to star	System	Other Sy	Success								2	Unknown
5031	The Windows Firewall Service blocked an a	Object Access	Filtering	Failure								2	Unknown
5032	Windows Firewall was unable to notify the	System	Other Sy	Failure								2	Unknown
5033	The Windows Firewall Driver has started su	System	Other Sy	Success								1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
5034	The Windows Firewall Driver has been stop	System	Other Sy	Success								1	Unknown
5035	The Windows Firewall Driver failed to start	System	Other Sy	Failure								2	Unknown
5037	The Windows Firewall Driver detected criti	System	Other Sy	Failure								2	Unknown
5038	Code integrity determined that the image h	System	System I	Failure								4	Unknown
5039	A registry key was virtualized.	Uncategorized	Subcate	Success								2	Unknown
5040	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5041	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5042	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5043	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5044	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5045	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5046	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5047	A change has been made to IPsec settings.	Uncategorized	Subcate	Success								2	Unknown
5048	A change has been made to IPsec settings.	Uncategorized	Subcate	Success	Sample Log for EVID 5048							2	Unknown
5049	An IPsec Security Association was deleted	Uncategorized	Subcate	Success								2	Unknown
5050	An attempt to programmatically disable the	Uncategorized	Subcate	Failure								3	Unknown
5051	A file was virtualized	Uncategorized	Subcate	Success								2	Unknown
5056	A cryptographic self test was performed	System	System I	Success								2	Unknown
5057	A cryptographic primitive operation failed	Uncategorized	Subcate	Failure								2	Unknown
5058	Key file operation	System	Other Sy	Success								2	Unknown
5059	Key migration operation	System	Other Sy	Success								2	Unknown
5060	Verification operation failed	Uncategorized	Subcate	Failure								2	Unknown
5061	Cryptographic operation	System	System I	Success								2	Unknown
5062	A kernel-mode cryptographic self test was	Uncategorized	Subcate	Success								2	Unknown
5063	A cryptographic provider operation was att	Policy Change	Other Po	Success								2	Unknown
5064	A cryptographic context operation was atte	Policy Change	Other Po	Success								2	Unknown
5065	A cryptographic context modification was a	Policy Change	Other Po	Success								2	Unknown
5066	A cryptographic function operation was att	Policy Change	Other Po	Success								2	Unknown
5067	A cryptographic function modification was	Policy Change	Other Po	Success								2	Unknown
5068	A cryptographic function provider operatio	Policy Change	Other Po	Success								2	Unknown
5069	A cryptographic function property operatio	Policy Change	Other Po	Success								2	Unknown
5070	A cryptographic function property operatio	Policy Change	Other Po	Success								2	Unknown
5120	OCSP Responder Service Started	Object Access	Certifica	Success								1	Unknown
5121	OCSP Responder Service Stopped	Uncategorized	Subcate	Success								1	Unknown
5122	A Configuration entry changed in the OCSP	Uncategorized	Subcate	Success								1	Unknown
5123	A configuration entry changed in the OCSP	Uncategorized	Subcate	Success								1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
5124	A security setting was updated on OCSP Re	Uncategorized	Subcate	Success								1	Unknown
5125	A request was submitted to OCSP Respond	Uncategorized	Subcate	Success								1	Unknown
5126	Signing Certificate was automatically updat	Uncategorized	Subcate	Success								2	Unknown
5127	The OCSP Revocation Provider successfully	Uncategorized	Subcate	Success								1	Unknown
5136	A directory service object was modified	Directory Service	Director	Success	566							1	Unknown
5137	A directory service object was created	Directory Service	Director	Success	566							2	Unknown
5138	A directory service object was undeleted	Directory Service	Director	Success								2	Unknown
5139	A directory service object was moved	Directory Service	Director	Success								1	Unknown
5140	A network share object was accessed	Object Access	File Shar	Success								1	Unknown
5141	A directory service object was deleted	Directory Service	Director	Failure								2	Unknown
5142	A network share object was added.	Object Access	File Shar	Success								2	Unknown
5143	A network share object was modified	Object Access	File Shar	Success								1	Unknown
5144	A network share object was deleted.	Object Access	File Shar	Success								1	Unknown
5145	A network share object was checked to see	Object Access	Detailed	Success Failure								2	Unknown
5148	The Windows Filtering Platform has detecte	Object Access	Other O	Success Failure								3	Unknown
5149	The DoS attack has subsided and normal pr	Object Access	Other O	Success Failure								2	Unknown
5150	The Windows Filtering Platform has blocke	Object Access	Filtering	Success								2	Unknown
5151	A more restrictive Windows Filtering Platfo	Object Access	Filtering	Success Failure								2	Unknown
5152	The Windows Filtering Platform blocked a p	Object Access	Filtering	Failure								2	Unknown
5153	A more restrictive Windows Filtering Platfo	Object Access	Filtering	Success								2	Unknown
5154	The Windows Filtering Platform has permit	Object Access	Filtering	Success	861							1	Unknown
5155	The Windows Filtering Platform has blocke	Object Access	Filtering	Success	861							2	Unknown
5156	The Windows Filtering Platform has allowe	Object Access	Filtering	Success								1	Unknown
5157	The Windows Filtering Platform has blocke	Object Access	Filtering	Failure								2	Unknown
5158	The Windows Filtering Platform has permit	Object Access	Filtering	Success								1	Unknown
5159	The Windows Filtering Platform has blocke	Object Access	Filtering	Failure								2	Unknown
5168	Spn check for SMB/SMB2 fails.	Object Access	File Shar	Success Failure								2	Unknown
5376	Credential Manager credentials were backe	Account Manage	User Acc	Success								1	Unknown
5377	Credential Manager credentials were resto	Account Manage	User Acc	Success								3	Unknown
5378	The requested credentials delegation was d	Uncategorized	Subcate	Failure								3	Unknown
5440	The following callout was present when the	Policy Change	Filtering	Success								1	Unknown
5441	The following filter was present when the V	Policy Change	Filtering	Success								1	Unknown
5442	The following provider was present when t	Policy Change	Filtering	Success								1	Unknown
5443	The following provider context was present	Policy Change	Filtering	Success								1	Unknown
5444	The following sub-layer was present when t	Policy Change	Filtering	Success								1	Unknown
5446	A Windows Filtering Platform callout has be	Policy Change	Filtering	Success								1	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
5447	A Windows Filtering Platform filter has bee	Policy Change	Other Pc	Success								1	Unknown
5448	A Windows Filtering Platform provider has	Policy Change	Filtering	Success								1	Unknown
5449	A Windows Filtering Platform provider cont	Policy Change	Filtering	Success								1	Unknown
5450	A Windows Filtering Platform sub-layer has	Policy Change	Filtering	Success								1	Unknown
5451	An IPsec Quick Mode security association w	Logon/Logoff	IPsec Qu	Success								1	Unknown
5452	An IPsec Quick Mode security association e	Logon/Logoff	IPsec Qu	Success								1	Unknown
5453	An IPsec negotiation with a remote comput	Logon/Logoff	IPsec Ma	Success								1	Unknown
5456	PAStore Engine applied Active Directory sto	Policy Change	Filtering	Success								2	Unknown
5457	PAStore Engine failed to apply Active Direct	Policy Change	Filtering	Success								2	Unknown
5458	PAStore Engine applied locally cached copy	Policy Change	Filtering	Success								2	Unknown
5459	PAStore Engine failed to apply locally cache	Policy Change	Filtering	Failure								2	Unknown
5460	PAStore Engine applied local registry storag	Policy Change	Filtering	Success								2	Unknown
5461	PAStore Engine failed to apply local registry	Policy Change	Filtering	Failure	534							2	Unknown
5462	PAStore Engine failed to apply some rules o	Policy Change	Filtering	Failure								2	Unknown
5463	PAStore Engine polled for changes to the ac	Policy Change	Filtering	Success								2	Unknown
5464	PAStore Engine polled for changes to the ac	Policy Change	Filtering	Success								2	Unknown
5465	PAStore Engine received a control for force	Policy Change	Filtering	Success								2	Unknown
5466	PAStore Engine polled for changes to the Ac	Policy Change	Filtering	Failure								2	Unknown
5467	PAStore Engine polled for changes to the Ac	Policy Change	Filtering	Failure								2	Unknown
5468	PAStore Engine polled for changes to the Ac	Policy Change	Filtering	Success								2	Unknown
5471	PAStore Engine loaded local storage IPsec p	Policy Change	Filtering	Success								2	Unknown
5472	PAStore Engine failed to load local storage I	Policy Change	Filtering	Failure								2	Unknown
5473	PAStore Engine loaded directory storage IPs	Policy Change	Filtering	Success								2	Unknown
5474	PAStore Engine failed to load directory stor	Policy Change	Filtering	Failure								2	Unknown
5477	PAStore Engine failed to add quick mode fil	Policy Change	Filtering	Failure								2	Unknown
5478	IPsec Services has started successfully	System	IPsec Dr	Success								1	Unknown
5479	IPsec Services has been shut down successf	System	IPsec Dr	Success								1	Unknown
5480	IPsec Services failed to get the complete lis	System	IPsec Dr	Failure								2	Unknown
5483	IPsec Services failed to initialize RPC server.	System	IPsec Dr	Failure								2	Unknown
5484	IPsec Services has experienced a critical fail	System	IPsec Dr	Failure								2	Unknown
5485	IPsec Services failed to process some IPsec	System	IPsec Dr	Failure								2	Unknown
6144	Security policy in the group policy objects h	Policy Change	Other Pc	Success								1	Unknown
6145	One or more errors occured while processi	Policy Change	Other Pc	Failure								2	Unknown
6272	Network Policy Server granted access to a u	Logon/Logoff	Network	Success								2	Unknown
6273	Network Policy Server denied access to a us	Logon/Logoff	Network	Success								2	Unknown
6274	Network Policy Server discarded the reques	Logon/Logoff	Network	Success								2	Unknown

Security Eventlog

ID	Description	Category	Sub-category	Type	Corresponding	Element	Val	Val Hex	Condition	Description	Comment	Relevancy	Volume
6275	Network Policy Server discarded the accou	Logon/Logoff	Network	Success								2	Unknown
6276	Network Policy Server quarantined a user	Logon/Logoff	Network	Success								3	Unknown
6277	Network Policy Server granted access to a u	Logon/Logoff	Network	Success								2	Unknown
6278	Network Policy Server granted full access to	Logon/Logoff	Network	Success								2	Unknown
6279	Network Policy Server locked the user acco	Logon/Logoff	Network	Success								3	Unknown
6280	Network Policy Server unlocked the user ac	Logon/Logoff	Network	Success								2	Unknown
6281	Code Integrity determined that the page ha	System	System I	Success Failure								4	Unknown
7045	A service was installed in the system	System		Information								4	Unknown
6400	BranchCache: Received an incorrectly form	System	Audit Ot	Success Failure								2	Unknown
6401	BranchCache: Received invalid data from a	System	Audit Ot	Success Failure								2	Unknown
6402	BranchCache: The message to the hosted c	System	Audit Ot	Success Failure								2	Unknown
6403	BranchCache: The hosted cache sent an inc	System	Audit Ot	Success Failure								2	Unknown
6404	BranchCache: Hosted cache could not be au	System	Audit Ot	Success Failure								2	Unknown
6405	BranchCache: %2 instance(s) of event id %1	System	Audit Ot	Success Failure								2	Unknown
6406	%1 registered to Windows Firewall to contr	System	Audit Ot	Success Failure								2	Unknown
6407	1% (no more info in MSDN)	System	Audit Ot	Success Failure								2	Unknown
6408	Registered product %1 failed and Windows	System	Audit Ot	Success Failure								2	Unknown
6410	Code integrity determined that a file does not meet the security requ			Failure								4	Low

[1] I put more weight on this for workstations than non workstations. Servers are more protected, and I expect this to happen regularly. I don't expect a user to run whois, ipconfig and netstat on a regularl basis.
-Andrew Alaniz