Question

Article Number: 00070
Last Review Date: Friday February 18, 2004
Question:
Which Microsoft Windows Event Viewer Log Event IDs does Net Report Treat?

Answer

Net Report Solution
The Net Report WMI Kit for Windows Logs for Version 3.11 treats the following Microsoft Windows Event Viewer Log Event IDs:

ID	Source	Category	Log File	Description
512	Security	Security	4	Windows is starting up.
513	Security	Security	4	Windows is shutting down.
514	Security	Security	4	An authentication package has been loaded by the local Security Authority.
515	Security	Security	4	A trusted logon process has registered with the Local Security Authority.
516	Security	Security	4	Internal resources allocated for the queuing of audit messages have been exhausted, \nleading to the loss of some audits.
517	Security	Security	4	The audit log was cleared.
518	Security	Security	4	A notification package has been loaded by the Security Account Manager.
519	Security	Security	4	Invalid use of LPC port.
520	Security	Security	1	The system time was changed.
521	Security	Security		Unable to log events to security log.
522	Security	Security		The audit collection system has encountered an error.
523	Security	Security		The security log is now %1 percent full.
524	Security	Security		"Event log auto-backup%n\ n%tLog:%t%1%n\ n%tFile:%t%2%n\n%tStatus:%t%3%n"""
528	Security	Security	4	Successful Logon
529	Security	Security	5	Logon Failure: Reason: Unknown user name or bad password.
530	Security	Security	5	Logon Failure: Account Logon time restriction violation.
531	Security	Security	5	Logon Failure: Reason: Account currently disabled.
532	Security	Security	5	Logon Failure: Reason: The specified user account has expired.
533	Security	Security	5	Logon Failure: Reason: User not allowed to logon at this computer.

534	Security	Security	5	Logon Failure: Reason: The user has not been granted the requested.
535	Security	Security	5	Logon Failure: Reason: The specified account's password has expired.
536	Security	Security	5	Logon Failure: Reason: The NetLogon component is not active.
537	Security	Security	5	Logon Failure: Reason the NetLogon component is not active.
538	Security	Security	4	User Logoff.
539	Security	Security	4	Logon Failure: Reason: Account locked out.
540	Security	Security	4	Successful Network Logon.
541	Security	Security		IKE security association established.
542	Security	Security		IKE security association ended. Mode: Data Protection (Quick mode).
543	Security	Security		Security 543 Security IKE security association ended. Mode: Key Exchange (Main mode).
544	Security	Security		Security 544 Security IKE security association establishment failed because peer could not authenticate.
545	Security	Security		Security 545 Security IKE peer authentication failed.
546	Security	Security		IKE security association establishment failed because peer sent invalid proposal.
547	Security	Security		IKE security association negotiation failed.
548	Security	Security		Logon Failure: Reason: Domain sid inconsistent.
549	Security	Security		Logon Failure: Reason: All sids were filtered out.
550	Security	Security		"""%1%n"""
551	Security	Security		User initiated logoff.
552	Security	Security		Logon attempt using explicit credentials
553	Security	Security		Logon failure. This event is generated when an authentication package detects a replay attack.
560	Security	Security	4	Object Open.
562	Security	Security	4	Handle Closed.
563	Security	Security	4	Object Open for Delete.
564	Security	Security	4	Object Deleted.
565	Security	Security	4	Object Open.
566	Security	Security	4	Object Operation.
567	Security	Security		Object Access Attempt.
568	Security	Security		Hard link creation attempt.
569	Security	Security		Application client context creation attempt.

570	Security	Security		Application operation attempt.
571	Security	Security		Application client context deletion.
572	Security	Security		Application Initialized.
573	Security	Security		Application-specific security event.
576	Security	Security	4	Special privileges assigned to new logon.
577	Security	Security	4	Privileged Service Called.
578	Security	Security	4	Privileged object operation.
592	Security	Security	4	A new process has been created.
593	Security	Security	4	A process has exited.
594	Security	Security		A handle to an object has been duplicated.
595	Security	Security		Indirect access to an object has been obtained.
596	Security	Security	5	Backup of data protection master key.
597	Security	Security		Recovery of data protection master key.
598	Security	Security		Protection of auditable protected data.
599	Security	Security		Unprotection of auditable protected data.
600	Security	Security	4	A process was assigned a primary token.
601	Security	Security		Attempt to install service.
602	Security	Security		Scheduled Task created.
608	Security	Security		User Right Assigned.
609	Security	Security		User Right Removed.
610	Security	Security		New Trusted Domain.
611	Security	Security		Trusted Domain Removed.
612	Security	Security	4	Audit Policy Change.
613	Security	Security		IPSec Services started.
614	Security	Security		IPSec Services disabled.
615	Security	Security		IPSec Services.
616	Security	Security		IPSec Services encountered a potentially serious failure.
617	Security	Security		Kerberos Policy Changed.
618	Security	Security		Encrypted Data Recovery Policy Changed.
620	Security	Security		Trusted Domain Information Modified.
621	Security	Security	4	System Security Access Granted.
622	Security	Security	4	System Security Access Removed.
624	Security	Security	4	User Account Created.
626	Security	Security	4	User Account Enabled.
627	Security	Security	5	Change Password Attempt.
628	Security	Security	4	User Account password set.
629	Security	Security	4	User Account Disabled.
630	Security	Security	4	User Account Deleted.
631	Security	Security	4	Security Enabled Global Group Created.
632	Security	Security		Security Enabled Global Group Member Added.

633	Security	Security	4	Security Enabled Global Group Member Removed.
634	Security	Security	4	Security Enabled Global Group Deleted.
635	Security	Security	4	Security Enabled Local Group Created.
636	Security	Security	4	Security Enabled Local Group Member Added.
637	Security	Security	4	Security Enabled Local Group Member Removed.
638	Security	Security	4	Security Enabled Local Group Deleted.
639	Security	Security	4	Security Enabled Local Group Changed.
640	Security	Security	4	General Account Database Change.
641	Security	Security	4	Security Enabled Global Group Changed.
642	Security	Security	4	User Account Changed.
643	Security	Security	4	Domain Policy Changed.
644	Security	Security	4	User Account Locked Out.
645	Security	Security	4	Computer Account Created.
646	Security	Security	4	Computer Account Changed.
647	Security	Security		Computer Account Deleted.
648	Security	Security		Security Disabled Local Group Created.
649	Security	Security		Security Disabled Local Group Changed.
650	Security	Security		Security Security Disabled Local Group Member Added.
651	Security	Security		Security Disabled Local Group Member Removed.
652	Security	Security		Security Disabled Local Group Deleted.
653	Security	Security		Security Disabled Global Group Created.
654	Security	Security		Security Disabled Global Group Changed.
655	Security	Security		Security Disabled Global Group Member Added.
656	Security	Security		Security Disabled Global Group Member Removed.
657	Security	Security		Security Disabled Global Group Deleted.
658	Security	Security		Security Enabled Universal Group Created.
659	Security	Security		Security Enabled Universal Group Changed.
660	Security	Security		Security Enabled Universal Group Member Added.
661	Security	Security		Security Enabled Universal Group Member Removed.
662	Security	Security		Security Security Enabled Universal Group Deleted.
663	Security	Security		Security Disabled Universal Group Created.
664	Security	Security		Security Disabled Universal Group Changed.

665	Security	Security		Security Disabled Universal Group Member Added.
666	Security	Security		Security Disabled Universal Group Member Removed.
667	Security	Security		Security Disabled Universal Group Deleted.
668	Security	Security		Group Type Changed.
669	Security	Security		Add SID History.
670	Security	Security		Add SID History.
671	Security	Security		User Account Unlocked.
672	Security	Security		Authentication Ticket Request.
673	Security	Security		Service Ticket Request.
674	Security	Security		Service Ticket Renewed.
675	Security	Security		Pre-authentication failed.
676	Security	Security		Authentication Ticket Request Failed.
677	Security	Security		Service Ticket Request Failed.
678	Security	Security		Account Mapped for Logon.
679	Security	Security		A name could not be mapped for logon.
680	Security	Security		Logon attempt by user.
681	Security	Security	4	The logon to account failed.
682	Security	Security		Session reconnected to winstation.
683	Security	Security		Session disconnected from winstation.
684	Security	Security		Set ACLs of members in administrators groups.
685	Security	Security		Account Name Changed.
686	Security	Security		Password of the following user accessed.
687	Security	Security		Basic Application Group Created.
688	Security	Security		Basic Application Group Changed.
689	Security	Security		Basic Application Group Member Added.
690	Security	Security		Security Basic Application Group Member Removed.
691	Security	Security		Security Basic Application Group Non-Member Added.
692	Security	Security		Security Basic Application Group Non-Member Removed.
693	Security	Security		Basic Application Group Deleted.
694	Security	Security		LDAP Query Group Created.
695	Security	Security		LDAP Query Group Changed.
696	Security	Security		LDAP Query Group Deleted.
697	Security	Security		Password Policy Checking API is called.
698	Security	Security		An attempt to set the Directory Services Restore Mode.
768	Security	Security		Namespace collision detected.
769	Security	Security		Trusted Forest Information Entry Added.

770	Security	Security		Trusted Forest Information Entry Removed.
771	Security	Security		Trusted Forest Information Entry Modified.
772	Security	Security		The certificate manager denied a pending certificate request.
773	Security	Security		Certificate Services received a resubmitted certificate request.
774	Security	Security		Certificate Services revoked a certificate.
775	Security	Security		Certificate Services received a request to publish the certificate revocation list (CRL).
776	Security	Security		Certificate Services published the certificate revocation list (CRL).
777	Security	Security		A certificate request extension changed.
778	Security	Security		One or more certificate request attributes changed.
779	Security	Security		Certificate Services received a request to shut down.
780	Security	Security		Certificate Services backup started.
781	Security	Security		Certificate Services backup completed.
782	Security	Security		Certificate Services restore started.
783	Security	Security		Certificate Services restore completed.
784	Security	Security		Certificate Services started.
785	Security	Security		Certificate Services stopped.
786	Security	Security		The security permissions for Certificate Services changed.
787	Security	Security		Certificate Services retrieved an archived key.
788	Security	Security		Certificate Services imported a certificate into its database.
789	Security	Security		The audit filter for Certificate Services changed.
790	Security	Security		Certificate Services received a certificate request.
791	Security	Security		Security Certificate Services approved a certificate request and issued a certificate.
792	Security	Security		Security Certificate Services denied a certificate request.
793	Security	Security		Security Certificate Services set the status of a certificate request to pending.
794	Security	Security		The certificate manager settings for Certificate Services changed.
795	Security	Security		A configuration entry changed in Certificate Services.
796	Security	Security		A property of Certificate Services changed.
797	Security	Security		Certificate Services archived a key.

798	Security	Security		Certificate Services imported and archived a key.
799	Security	Security		Certificate Services published the CA certificate to Active Directory.
800	Security	Security		One or more rows have been deleted from the certificate database.
801	Security	Security		Role separation enabled.
805	Security	Security		Configuration of security log for this session.
806	Security	Security		Per User Audit Policy was refreshed.
807	Security	Security		Per user auditing policy set for user.
808	Security	Security		A security event source has attempted to register.
809	Security	Security		A security event source has attempted to unregister.
832	Security	Security		Destination DRA.
833	Security	Security		Destination DRA.
834	Security	Security		Destination DRA.
835	Security	Security		Destination DRA.
836	Security	Security		Destination DRA.
837	Security	Security		Destination DRA.
838	Security	Security		Session Change.
839	Security	Security		Replication Event.
840	Security	Security		Replication Event.
841	Security	Security		Destination DRA.

Further Information

For further information, please
Visit our web site at: http://www.net-report.us
Use our Knowledge Base: http://82.127.62.167/us/support/sup_knowledgebase.asp