

Events Every Security Administrator Should Monitor

Event Log Event IDs or Categories	Recommended Monitoring
Account logon failures 529-537	<ul style="list-style-type: none"> • Immediate Notification Alert for any administrator account logon failure • Immediate Notification Alert for any logon failure during non-business hours • Daily Filter Viewing
Profile Changes 624-630	<ul style="list-style-type: none"> • Immediate Notification Alert • Daily Filter Viewing
Password Changes 627,628	<ul style="list-style-type: none"> • Notification alert for any administrator password change • Notification alert for password change during non-business hours • Daily Filter Viewing
All error events	<ul style="list-style-type: none"> • Daily Filter Viewing
User or Group Changes	<ul style="list-style-type: none"> • Immediate Notification Alert • Daily Filter Viewing
Policy Changes	<ul style="list-style-type: none"> • Immediate Notification Alert • Daily Filter Viewing
Handle Duplication/Handle Closed	<ul style="list-style-type: none"> • Daily Filter Viewing of critical files
System Events	<ul style="list-style-type: none"> • Daily Filter Viewing

Listed below are some of the more important security events. While security monitoring needs vary between different organizations, this list will provide a baseline level of monitoring for general security purposes.

Event ID	Type	Description
512	Success Audit	NT starts
513	Success Audit	NT is shut down
514	Success Audit	Authentication Package is loaded by the LSA (Local Security Authority)
515	Success Audit	A trusted logon process has registered with the LSA
516	Success Audit	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits
517	Success Audit	Security log is cleared
518	Success Audit	SAM has loaded a notification package
528	Success Audit	Successful logon
529	Failure Audit	Logon failure: unknown username or password
530	Failure Audit	Logon failure: account logon time restriction violation
531	Failure Audit	Logon failure: account currently disabled
532	Failure Audit	Logon failure: the specified user account has expired
533	Failure Audit	Logon failure: user not allowed to logon at this computer
534	Failure Audit	Logon failure: the user has not been granted the requested logon type at this

		machine
535	Failure Audit	Logon failure: the specified account's password has expired
536	Failure Audit	Logon failure: the Netlogon component is not active
537	Failure Audit	Logon failure: An unexpected error occurred during logon
538	Success Audit	User logoff
539	Failure Audit	Logon failure: Account locked out
540	Success Audit	Successful network logon
560	Success Audit	Object access success audit event
561	Success Audit	Handle allocated
562	Success Audit	Handle closed
563	Success Audit	Object opened for delete
564	Success Audit	Object deleted
576	Success Audit	Special privileges assigned to new logon
577	Success Audit	Privilege service called
578	Success Audit	Privilege object operation
592	Success Audit	A new process has been created
593	Success Audit	A process has been exited
594	Success Audit	A handle to an object has been obtained
595	Success Audit	Indirect access to an object has been obtained
608	Success Audit	User right assigned. The event message lists the assigned rights
609	Success Audit	User right removed. The event message lists the removed rights
610	Success Audit	New domain trust created
611	Success Audit	Trust relationship removed
612	Success Audit	The audit policy has been changed. The event message describes the new policy
624	Success Audit	New user account created. The event message lists the new account name and SID
625	Success Audit	User account changed. The event message lists the affected user account
626	Success Audit	User account enabled (from disabled state). The event message lists the affected user account
627	Success Audit	Attempt to change password. The event message lists the affected user
628	Success Audit	User account password set. The event message lists the affected user
629	Success Audit	Account disabled. The event message lists the affected user
630	Success Audit	Account deleted. The event message lists the affected user
631	Success Audit	Global group created. The event message lists the group
632	Success Audit	New member added to global group. The event message lists the affected group, as well as the name of the added account
633	Success Audit	Member removed from global group. The event message lists the affected group, as well as the name of the removed account
634	Success Audit	Global group deleted. The event message lists the affected group
635	Success Audit	Local group created. The event message lists the affected group
636	Success Audit	New member added to local group. The event message lists the affected group, as well as the name of the added account
637	Success Audit	Member removed from local group. The event message lists the affected group, as well as the name of the removed account
638	Success Audit	Local group deleted. The event message lists the affected group
639	Success Audit	Local group changed. The event lists the affected group
640	Success Audit	General account database change. The event lists the change that was made
641	Success Audit	Global group changed. The event message lists the affected group
642	Success Audit	User account changed. The event lists the affected account
643	Success Audit	Domain policy changed. The event lists the affected domain
644	Success Audit	User account locked out. This event is logged when an account is locked out due to repeated logon failures.