

**Report title:**        **Audit policy changes**

**Description:**        The report is based on the 612 event - local audit policy changed and the 643 event - domain audit policy changed. The events identify any change to audit policy. Correlate these events with changes that authorized personnel make to audit policy.

**Generated on:**        13-Sep-2006 16:29

**Generated by:**        Calin

**Date filter:**         9/7/2006 12:00:00AM to 9/13/2006 11:59:59PM

**Event logs:**         Security

**Other filters:**        event ID= 612 from Security log  
and event ID= 643 from Security log

**Reviewed by:** \_\_\_\_\_

**Reviewed date:** \_\_\_\_\_

**Signature:** \_\_\_\_\_



The following report may contain information about the privileges assigned to an account. Below you have a legend which explains the meaning of each privilege.

Privilege value	Short description
SeTcbPrivilege	Act as part of the operating system
SeMachineAccountPrivilege	Add workstation to domain
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process
SeBackupPrivilege	Backup files and directories
SeSystemtimePrivilege	Change the system time
SeCreatePagefilePrivilege	Create a page file
SeCreateTokenPrivilege	Create a token object
SeCreateGlobalPrivilege	Create global objects
SeCreatePermanentPrivilege	Create permanent shared objects
SeDebugPrivilege	Debug programs
SeRemoteShutdownPrivilege	Shutdown the system remotely
SeImpersonatePrivilege	Impersonate a client after authentication
SeLoadDriverPrivilege	Load and unload device drivers
SeSecurityPrivilege	Manage audit logs
SeSystemEnvironmentPrivilege	Modify environmental variables
SeManageVolumePrivilege	Perform volume maintenance tasks
SeSystemProfilePrivilege	Profile system performance
SeRestorePrivilege	Restore files or folders
SeSyncAgentPrivilege	Synchronize directory service data
SeTakeOwnershipPrivilege	Take ownership of files and folders
SeNetworkLogonRight	Access this computer from the network
SeBatchLogonRight	Logon as batch job
SeServiceLogonRight	Logon as service
SeInteractiveLogonRight	Logon locally

User Name	By User	Event Description	Privilege	Time	Date
NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER\$	Local audit policy changed	N/A	11:54:14AM	9/8/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	2:24:58PM	9/8/2006
NT AUTHORITY\SYSTEM	WORKGROUP\FSERVER\$	Local audit policy changed	N/A	3:02:05PM	9/8/2006
NT AUTHORITY\SYSTEM	WORKGROUP\FSERVER\$	Local audit policy changed	N/A	3:02:05PM	9/8/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	3:09:24PM	9/8/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	3:14:33PM	9/8/2006
GFITEMASOFT\Administrator	N/A	Domain audit policy changed	N/A	3:17:56PM	9/8/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	4:39:35PM	9/8/2006
NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER\$	Local audit policy changed	N/A	11:54:14AM	9/12/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	2:24:58PM	9/12/2006
NT AUTHORITY\SYSTEM	WORKGROUP\FSERVER\$	Local audit policy changed	N/A	3:02:05PM	9/12/2006
NT AUTHORITY\SYSTEM	WORKGROUP\FSERVER\$	Local audit policy changed	N/A	3:02:05PM	9/12/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	3:09:24PM	9/12/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	3:14:33PM	9/12/2006
GFITEMASOFT\Administrator	N/A	Domain audit policy changed	N/A	3:17:56PM	9/12/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	4:39:35PM	9/12/2006
NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER\$	Local audit policy changed	N/A	11:54:14AM	9/13/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	2:24:58PM	9/13/2006
NT AUTHORITY\SYSTEM	WORKGROUP\FSERVER\$	Local audit policy changed	N/A	3:02:05PM	9/13/2006
NT AUTHORITY\SYSTEM	WORKGROUP\FSERVER\$	Local audit policy changed	N/A	3:02:05PM	9/13/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	3:09:24PM	9/13/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	3:14:33PM	9/13/2006
GFITEMASOFT\Administrator	N/A	Domain audit policy changed	N/A	3:17:56PM	9/13/2006
NT AUTHORITY\SYSTEM	N/A	Domain audit policy changed	N/A	4:39:35PM	9/13/2006

User Name	By User	Event Description	Privilege	Time	Date
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	8:07:08PM	9/8/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	10:58:21PM	9/8/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	10:59:28PM	9/8/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	8:07:08PM	9/12/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	10:58:21PM	9/12/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	10:59:28PM	9/12/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	8:07:08PM	9/13/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	10:58:21PM	9/13/2006
NT AUTHORITY\SYSTEM	\\MACHINENAME\$	Local audit policy changed	N/A	10:59:28PM	9/13/2006