

**Report title:** User rights changes

**Description:** The report is based on the 608 and 609 events. The event signals the fact that a new privilege was granted / removed to /for a user account. The event log records this action along with the user account Security Identifier (SID), not the user account name. In order to display the information in a more understandable manner, the privileges granted were translated to the associated policy name which was changed. For example, instead of SeTcbPrivilege, the report lists "Act as part of the operating system".

**Generated on:** 13-Sep-2006 17:23

**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= 608 from Security log  
and event ID= 609 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

Assigned to	By User	Event Description	Privilege	Time	Date
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	User right assigned	SeTakeOwnershipPrivilege	1:49:29PM	9/8/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	User right assigned	SeAssignPrimaryTokenPrivilege	2:51:44PM	9/8/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	User right assigned	SeIncreaseQuotaPrivilege	2:51:45PM	9/8/2006
GFITEMASOFT\IIS_WPG	GFITEMASOFT\administrator	User right assigned	SeImpersonatePrivilege	2:51:56PM	9/8/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	User right removed	SeTakeOwnershipPrivilege	11:40:10PM	9/8/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	User right assigned	SeTakeOwnershipPrivilege	1:49:29PM	9/12/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	User right assigned	SeAssignPrimaryTokenPrivilege	2:51:44PM	9/12/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	User right assigned	SeIncreaseQuotaPrivilege	2:51:45PM	9/12/2006
GFITEMASOFT\IIS_WPG	GFITEMASOFT\administrator	User right assigned	SeImpersonatePrivilege	2:51:56PM	9/12/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	User right removed	SeTakeOwnershipPrivilege	11:40:10PM	9/12/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	User right assigned	SeTakeOwnershipPrivilege	1:49:29PM	9/13/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	User right assigned	SeAssignPrimaryTokenPrivilege	2:51:44PM	9/13/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	User right assigned	SeIncreaseQuotaPrivilege	2:51:45PM	9/13/2006
GFITEMASOFT\IIS_WPG	GFITEMASOFT\administrator	User right assigned	SeImpersonatePrivilege	2:51:56PM	9/13/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	User right removed	SeTakeOwnershipPrivilege	11:40:10PM	9/13/2006