User Rights Assignment

Microsoft defines user rights in two types of categories: Logon Rights and Privileges. These are defined as follows:

- **Logon Right**: A user right that is assigned to a user and that specifies the ways in which a user can log onto a system. An example of a logon right is the right to log on to a system remotely.
- **Privilege**: A user right that is assigned to a user and that specifies allowable actions on the system. An example of a privilege is the right to shut down a system.
- Although they can apply to individual user accounts, user rights are best administered on a group account basis. This ensures that a user logging on as a member of a group automatically inherits the rights associated with that group. By assigning rights to groups rather than individual users, user account administration can be simplified. When users in a group all require the same user rights, they can be assigned the set of rights once to the group, rather than repeatedly assigning the same set to each individual user account.
- User rights that are assigned to a group are applied to all members of the group while they remain members. If a user is a member of multiple groups, the user's rights are cumulative, which means that the user has more than one set of rights and privileges. The only time that rights assigned to one group might conflict with those assigned to another is in the case of certain logon rights. For example a member of multiple groups who is given the "Deny Access to This Computer from the Network" logon right would not be able to log on despite the logon rights granted to the user by other groups. The user would be logged on locally with cached credentials, but when attempting to access the domain resources would receive the following message:

- ❑ User rights govern the methods by which a user can log on to a system.
- ❑ User rights are applied at the local computer level, or at the domain level.
- ❑ User rights are managed in Group Policy under the **User Rights Assignment** item.

User rights can be configured through Group Policy

- **Computer Configuration**
- **Policies**
- **Windows Settings**
- **Security Settings**
- **Local Policies**

- **User Rights Assignment**

or on the local computer by using the **Local Group Policy Editor (gpedit.msc**

List of User Rights Policy settings

Group Policy Setting	Constant Name
Access Credential Manager as a trusted caller	SeTrustedCredManAccessPrivilege
Access this computer from the network	SeNetworkLogonRight
Act as part of the operating system	SeTcbPrivilege
Add workstations to domain	SeMachineAccountPrivilege
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege
Allow log on locally	SeInteractiveLogonRight
Allow log on through Remote Desktop Services	SeRemoteInteractiveLogonRight
Back up files and directories	SeBackupPrivilege
Bypass traverse checking	SeChangeNotifyPrivilege
Change the system time	SeSystemtimePrivilege
Change the time zone	SeTimeZonePrivilege
Create a pagefile	SeCreatePagefilePrivilege
Create a token object	SeCreateTokenPrivilege
Create global objects	SeCreateGlobalPrivilege
Create permanent shared objects	SeCreatePermanentPrivilege
Create symbolic links	SeCreateSymbolicLinkPrivilege
Debug programs	SeDebugPrivilege
Deny access to this computer from the network	SeDenyNetworkLogonRight
Deny log on as a batch job	SeDenyBatchLogonRight
Deny log on as a service	SeDenyServiceLogonRight
Deny log on locally	SeDenyInteractiveLogonRight
Deny log on through Remote Desktop Services	SeDenyRemoteInteractiveLogonRight
Enable computer and user accounts to be trusted for delegation	SeEnableDelegationPrivilege
Force shutdown from a remote system	SeRemoteShutdownPrivilege
Generate security audits	SeAuditPrivilege
Impersonate a client after authentication	SeImpersonatePrivilege
Increase a process working set	SeIncreaseWorkingSetPrivilege
Increase scheduling priority	SeIncreaseBasePriorityPrivilege
Load and unload device drivers	SeLoadDriverPrivilege

Lock pages in memory	SeLockMemoryPrivilege
Log on as a batch job	SeBatchLogonRight
Log on as a service	SeServiceLogonRight
Manage auditing and security log	SeSecurityPrivilege
Modify an object label	SeRelabelPrivilege
Modify firmware environment values	SeSystemEnvironmentPrivilege
Perform volume maintenance tasks	SeManageVolumePrivilege
Profile single process	SeProfileSingleProcessPrivilege
Profile system performance	SeSystemProfilePrivilege
Remove computer from docking station	SeUndockPrivilege
Replace a process level token	SeAssignPrimaryTokenPrivilege
Restore files and directories	SeRestorePrivilege
Shut down the system	SeShutdownPrivilege
Synchronize directory service data	SeSyncAgentPrivilege
Take ownership of files or other objects	SeTakeOwnershipPrivilege