



SecureWave
Safeguarding Tomorrow



Power User vs. Local Administrator



Table of Contents

1	About this document.....	3
1.1	Context	3
1.2	Purpose.....	3
1.3	Scope.....	3
1.4	Definitions & Acronyms	3
1.5	Document history	4
2	The “Power Users” group – Summary	5
3	Comparison between the “Local Users” group and the “Local Administrators” group	6
3.1	Windows 2000/XP User Rights	6
3.2	Security Options	7



1 About this document

1.1 Context

Although it is clear that from a security perspective, giving local administrative rights to users is generally not advisable, administrators often do give users local administrative rights to their computers, only to allow those users to change certain settings as time, date, etc.

However, since Windows 2000 availability, Microsoft introduced a new local group, called "Power Users". The "Power Users" group allows system administrators to restrict the user rights of users on their workstation without them losing the right to perform simple administrative tasks.

1.2 Purpose

This document highlights why SecureWave recommends all its clients to use the "power users" group instead of the "local administrators" group, as this reduces considerably the risk related to the fact to give administrator rights to a large community that might not have the right skills and may misuse those rights, be it on purpose or not.

1.3 Scope

You will find hereafter an overview of the differences and similarities between the "Local Administrators" group and the "Power Users" group.

1.4 Definitions & Acronyms

Terms	Definitions
Local Group	A security group that can be granted rights and permissions on only resources on the computer on which the group is created. Local groups can have any user accounts that are local to the computer as members, as well as users, groups, and computers from a domain to which the computer belongs as well as the local groups that you create. The default local groups are automatically created when you install a stand-alone server
Stand-alone Server	A server that runs Windows 2000 or Windows Server 2003, but does not participate in a domain. A stand-alone server has only its own database of users, and it processes logon requests by itself. A stand-alone server does not share account information with other computers and cannot provide access to domain accounts, but it can participate in a workgroup.
Member Server	A server that is joined to a domain but is not a domain controller. Member servers typically function as file servers, application servers, database servers, Web servers, certificate servers, firewalls, or remote access servers running Windows Server 2000/2003.
Local Computer	The computer that you are currently logged on to as a user. More generally, a local computer is a computer that you can access directly without using a communications line or a communications device, such as a network adapter or a modem.
Domain	In Active Directory, a collection of computer, user, and group objects defined by the administrator. These objects share a common directory database, security policies, and security relationships with other domains.
Process	The virtual address space and the control information necessary for the execution of a program
Named Pipes	A portion of memory that can be used by one process to pass information to another process,



	so that the output of one is the input of the other. The second process can be local (on the same computer as the first) or remote (on a networked computer).
Auditing	The process that tracks the activities of users by recording selected types of events in the security log of a server or a workstation
Acronyms	Descriptions
API	Application Programming Interface – A set of routines that an application uses to request and carry out lower-level services performed by a computer's operating system. These routines usually carry out maintenance tasks such as managing files and displaying information
RPC	Remote Procedure Call – A message-passing facility that allows a distributed application to call services that are available on various computers on a network. Used during remote administration of computers.

1.5 Document history

Version	Date	Description	Author	Reviewer
1.0	15/12/2003	Document Creation	Bruno van Branden	
1.1	19/12/2003	QA and Document Standardization	Bertrand Manhe	



2 The “Power Users” group - Summary

The “Power Users” group in Windows 2000 and Windows XP is a built-in group. By default, the group has no members. This group does not exist on domain controllers.

The Power User class can perform any task except for those reserved for Administrators. They are allowed to carry out functions that will not directly affect the operating system or risk security.

Power Users for example can:

- > Create local user accounts
- > Modify user accounts which they have created
- > Change user permissions on users, power users, and guests
- > Install and run applications that do not affect the operating system
- > Customize settings and resources on the Control Panel, such as Printers, Date/Time, and Power Options
- > Do anything a User can

Power Users cannot:

- > Access other users' data without permission
- > Delete or modify user accounts they did not create.
- > Uninstall System Drivers, making this of great interest for Sanctuary® Device Control and/or Sanctuary® administrators.

A detailed list of all the differences and similarities between the “Power Users” group and the “Local Administrators” group can be found hereafter.



3 Comparison between the “Local Users” group and the “Local Administrators” group

3.1 Windows 2000/XP User Rights

The following table lists the DEFAULT settings for all user rights by default attributed to Local Administrators and/or Power Users. As all these User Rights are configurable via GPO's, one can adapt the settings as acquired.

<i>User Rights</i>	<i>Power Users</i>	<i>Local Administrators</i>
Access this computer from the network ⁱ	✓	✓
Adjust memory quotas for a process ⁱⁱ	✗	✓
Allow log on locally ⁱⁱⁱ	✓	✓
Allow log on through Terminal Services ^{iv}	✗	✓
Back up files and directories ^v	✗	✓
Bypass traverse checking ^{vi}	✓	✓
Change the system time ^{vii}	✓	✓
Create a pagefile ^{viii}	✗	✓
Create global objects ^{ix}	✗	✓
Debug programs ^x	✗	✓
Force shutdown from a remote system ^{xi}	✗	✓
Impersonate a client after authentication ^{xii}	✗	✓
Increase scheduling priority ^{xiii}	✗	✓
Load and unload device drivers ^{xiv}	✗	✓
Manage auditing and security log ^{xv}	✗	✓
Perform volume maintenance tasks ^{xvi}	✗	✓
Profile single process ^{xvii}	✓	✓
Profile system performance ^{xviii}	✗	✓
Remove computer from docking station ^{xix}	✓	✓
Restore files and directories ^{xx}	✗	✓
Shut down the system ^{xxi}	✓	✓
Take ownership of files or other objects ^{xxii}	✗	✓



3.2 Security Options

The following table lists the DEFAULT settings for all Security Options by default attributed to Local Administrators and/or Power Users. As all these Security Options are configurable via GPO's, one can adapt the settings as acquired.

<i>Security Option</i>	<i>Power Users</i>	<i>Local Administrators</i>
Allowed to format and eject removable media ^{xxiii}	✓	✓
Do not require CTRL+ALT+DEL ^{xxiv}	✓	✓
Force logoff when logon hours expire ^{xxv}	✓	✓

ⁱ This user right determines which users and groups are allowed to connect to the computer over the network. Terminal Services are not affected by this user right.

ⁱⁱ This privilege determines who can change the maximum memory that can be consumed by a process

ⁱⁱⁱ This logon right determines which users can interactively log on to this computer. Logons initiated by pressing CTRL+ALT+DEL sequence on the attached keyboard requires the user to have this logon right. Additionally this logon right may be required by some service or administrative applications that can log on users.

^{iv} This security setting determines which users or groups have permission to log on as a Terminal Services client.

^v This user right determines which users can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system.

^{vi} This user right determines which users can traverse directory trees even though the user may not have permissions on the traversed directory. This privilege does not allow the user to list the contents of a directory, only to traverse directories.

^{vii} This user right determines which users and groups can change the time and date on the internal clock of the computer. Users that are assigned this user right can affect the appearance of event logs. If the system time is changed, events that are logged will reflect this new time, not the actual time that the events occurred.

^{viii} This user right determines which users and groups can call an internal application programming interface (API) to create a page file. This user right is used internally by the operating system and usually does not need to be assigned to any users.

^{ix} This user right is required for a user account to create global objects during Terminal Services sessions. Users can still create session-specific objects without being assigned this user right.

^x This user right determines which users can attach a debugger to any process or to the kernel.

^{xi} This security setting determines which users are allowed to shut down a computer from a remote location on the network.

^{xii} Assigning this privilege to a user allows programs running on behalf of that user to impersonate a client. Requiring this user right for this kind of impersonation prevents an unauthorized user from convincing a client to connect (for example, by remote procedure call (RPC) or named pipes) to a service that they have created and then impersonating that client, which can elevate the unauthorized user's permissions to administrative or system levels.



-
- ^{xiii} This security setting determines which accounts can use a process with Write Property access to another process to increase the execution priority assigned to the other process. A user with this privilege can change the scheduling priority of a process through the Task Manager user interface.
 - ^{xiv} This user right determines which users can dynamically load and unload device drivers or other code in to kernel mode. This user right does not apply to Plug and Pray device drivers. It is recommended that you do not assign this privilege to other users.
 - ^{xv} This security setting determines which users can specify object access auditing options for individual resources, such as files, Active Directory objects, and registry keys.
 - ^{xvi} This security setting determines which users and groups can run maintenance tasks on a volume, such as remote defragmentation. Use caution when assigning this user right. Users with this user right can explore disks and extend files in to memory that contains other data. When the extended files are opened, the user might be able to read and modify the acquired data.
 - ^{xvii} This security setting determines which users can use performance monitoring tools to monitor the performance of non-system processes.
 - ^{xviii} This security setting determines which users can use performance monitoring tools to monitor the performance of system processes.
 - ^{xix} Allows the user of a portable computer to undock the computer by clicking Eject PC on the Start menu.
 - ^{xx} This security setting determines which users can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories, and determines which users can set any valid security principal as the owner of an object.
 - ^{xxi} This security setting determines which users who are logged on locally to the computer can shut down the operating system using the Shut Down command.
 - ^{xxii} This security setting determines which users can take ownership of any securable object in the system, including Active Directory objects, files and folders, printers, registry keys, processes, and threads.
 - ^{xxiii} This user right determines which users and groups are allowed to connect to the computer over the network. Terminal Services are not affected by this user right.
 - ^{xxiv} This security setting determines whether pressing CTRL+ALT+DEL is required before a user can log on. This security setting is by default disabled on workstations and servers that are joined to a domain, but is enabled on stand-alone workstations.
 - ^{xxv} This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component.



SecureWave

Safeguarding Tomorrow

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America

+1 (703) 713-3960 Phone
+1 (703) 793-7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom

+44 (0) 1908 357897 Phone
+44 (0) 1908 357600 Fax

Continental Europe

Atrium Business Park
23-ZA Bourmicht
L-8070 Bertrange
Grand Duchy of Luxembourg

+352 265 364-11 Phone
+352 265 364-12 Fax

www.securewave.com
info@securewave.com