**Administrators** The Administrators group has full permissions and privileges. Its

members can grant themselves any permissions they do not have by default to manage

all the objects on the computer. (Objects include the filesystem, printers, and account

management.) By default, the Administrator account, which is disabled by default, and the

Initial User account are members of the Administrators local group.

Members of the Administrators group can perform the following tasks:

■ Install the operating system.

■ Install and configure hardware device drivers.

■ Install system services.

■ Install service packs, hot fixes, and Windows updates.

■ Upgrade the operating system.

■ Repair the operating system.

■ Install applications that modify the Windows system files.

■ Configure password policies.

■ Configure audit policies.

■ Manage security logs.

■ Create administrative shares.

■ Create administrative accounts.

■ Modify groups and accounts that have been created by other users.

■ Remotely access the Registry.

■ Stop or start any service.

■ Configure services.

■ Increase and manage disk quotas.

■ Increase and manage execution priorities.

■ Remotely shut down the system.

■ Assign and manage user rights.

■ Reenable locked-out and disabled accounts.

■ Manage disk properties, including formatting hard drives.

■ Modify systemwide environment variables.

■■ Access any data on the computer.

■■ Back up and restore all data.

**Backup Operators** Members of the Backup Operators group have permissions to back up

and restore the filesystem, even if the filesystem is NTFS and they have not been assigned

permissions to access the filesystem. However, the members of Backup Operators can

access the filesystem only through the Backup utility. To access the filesystem directly,

Backup Operators must have explicit permissions assigned. There are no default members

of the Backup Operators local group.

**Cryptographic Operators** The Cryptographic Operators group has access to perform

cryptographic operations on the computer. There are no default members of the

Cryptographic Operators local group.

**Distributed COM Users** The Distributed COM Users group has the ability to launch

and run Distributed COM objects on the computer. There are no default members of the

Distributed COM Users local group.

**Event Log Readers** The Event Log Readers group has access to read the event log on the

local computer. There are no default members of the Event Log Readers local group.

**Guests** The Guests group has limited access to the computer. This group is provided so

that you can allow people who are not regular users to access specific network resources.

As a general rule, most administrators do not allow Guest access because it poses a potential

security risk. By default, the Guest user account is a member of the Guests local group.

**IIS\_IUSRS** The IIS\_IUSRS group is used by Internet Information Services (IIS). The NT

AUTHORITY\IUSR user account (premade for IIS) is a member of the IIS\_IUSRS group by

default.

**Network Configuration Operators** Members of the Network Configuration Operators

group have some administrative rights to manage the computer’s network configuration, for

example, editing the computer’s TCP/IP settings.

**Performance Log Users** The Performance Log Users group has the ability to access and

schedule logging of performance counters and can create and manage trace counters on the

computer. There are no default members of this group.

**Performance Monitor Users** The Performance Monitor Users group has the ability to

access and view performance counter information on the computer. Users who are members

of this group can access performance counters both locally and remotely. There are no

default members of this group.

**Power Users** The Power Users group is included in Windows 10 for backward compatibility

to ensure that computers upgraded from Windows XP function as before with regard

to folders that allow access to members of the group. Otherwise, the Power Users group has

limited administrative rights. There are no default members of this group.

**Remote Desktop Users** The Remote Desktop Users group allows members of the group to

log on remotely for the purpose of using the Remote Desktop service. There are no default

members of this group.

**Replicator** The Replicator group is intended to support directory replication, which is a

feature used by domain servers. Only domain users who will start the replication service

should be assigned to this group. The Replicator local group has no default members.

**Users** The Users group is intended for end users who should have very limited system access. If

you have installed a fresh copy of Windows 10, the default settings for the Users group prohibit

its members from compromising the operating system or program files. By default, all users who

have been created on the computer, except Guest, are members of the Users local group.

**Special Groups**

Special groups are premade groups that can be used by the system or by administrators.

Membership in special groups is automatic if certain criteria are met. You cannot manage

special groups through the Local Users and Groups utility, but an administrator can

add special groups to resources. The following text describes the special groups that are

built into Windows 10.

**Anonymous Logon** This group includes users who access the computer through anonymous

logons. When users gain access through special accounts created for anonymous

access to Windows 10 services, they become members of the Anonymous Logon group.

**Authenticated Users** This group includes users who access the Windows 10 operating

system through a valid username and password. Users who can log on belong to the

Authenticated Users group.

**Batch** This group includes users who log on as a user account that is used only to run a

batch job.

**Creator Owner** This is the account that created or took ownership of an object. This is

typically a user account. Each object (files, folders, printers, and print jobs) has an owner.

Members of the Creator Owner group have special permissions to resources. For example,

if you are a regular user who has submitted 12 print jobs to a printer, you can manipulate

your print jobs as Creator Owner, but you can’t manage any print jobs submitted by other

users.

**Dialup** This group includes users who log on to the network from a dial-up connection.

**Everyone** This group includes anyone who could possibly access the computer—all users

who have been defined on the computer (including Guest), plus (if your computer is a part

of a domain) all users within the domain. If the domain has trust relationships with other

domains, all users in the trusted domains are part of the Everyone group as well. The

exception to automatic group membership with the Everyone group is that members of the

Anonymous Logon group are not included as a part of the Everyone group.

**Interactive** This group includes all users who use the computer’s resources locally.

**Network** This group includes users who access the computer’s resources over a network

connection.

**Service** This group includes users who log on as a user account that is used only to

run a service. You can configure the use of user accounts for logon through the Services

program.

**System** There are times when the Windows 10 operating system will access functions within the

system. When the operating system accesses these functions, it does it as a system user. When the

system accesses specific functions as a user, that process becomes a member of the System group.

**Terminal Server User** This group includes users who log on through Terminal Services.