

## Ch05 Key Terms

access token	Created when a user logs on, this value identifies the user and all of the user's group memberships. Like a club membership card, it verifies a user's permissions when the user attempts to access a local or network resource.
Anonymous Logon	Special identity that refers to users who have not supplied a username and password.
authenticate	To gain access to the network, prospective network users must identify themselves to a network using specific user accounts.
authentication	Process of confirming a user's identity using a known value such as a password, pin number on a smart card, or the user's fingerprint or handprint in the case of biometric authentication.
authorization	Process of confirming that an authenticated user has the correct permissions to access one or more network resources.
batch file	Files, typically configured with either a .bat extension or a .cmd extension, that can be used to automate many routine or repetitive tasks.
built-in user accounts	Accounts automatically created when Microsoft Windows Server 2008 is installed. By default, two built-in user accounts are created on a Windows Server 2008 computer: the Administrator account and the Guest account.
CSVDE	(Comma-Separated Value Directory Exchange) Command-line utility used to import or export Active Directory information from a comma-separated value (.csv) file.
CSV	(Comma-Separated Values) Format that contains a comma between each value. The CSV format can be used to import and export information from other third-party applications.
distribution group	Non-security-related groups created for the distribution of information to one or more persons.
domain account	Accounts used to access Active Directory or network-based resources, such as shared folders or printers.
domain local group	Group used to assign permissions to resources that reside only in the same domain as the domain local group. They can contain user accounts, computer accounts, global groups, and universal groups from any domain, in addition to other domain local groups from the same domain.
dsadd	Command-line tool used to create, delete, view, and modify Active Directory objects including users, groups, and organizational units.
Everyone	Special identity group that contains all authenticated users and domain guests.
global group	Group used to grant or deny permissions to any resource located in any domain in the forest. Global groups can contain user accounts, computer accounts, and/or other global groups only from within the same domain as the global group.
group	Collection of user or computer accounts that is used to simplify the assignment of permissions to network resources.
group nesting	Process of configuring one or more groups as members of another group.
group scope	Group characteristic that defines the extent of the group in the domain tree or forest.
group type	Group characteristic that defines how a group is to be used within Active Directory.
header record	First line of the imported or exported text file that uses proper attribute names.
LDIF	(LDAP Data Interchange Format) Format for the data file containing the object records to be created.
LDIFDE	(LDAP Data Interchange Format Directory Exchange) Command-line utility used to import or export Active Directory information and create, modify, and delete Active Directory objects.

local account	Account used to access the local computer only. They are stored in the local Security Account Manager (SAM) database on the computer where they reside. Local accounts are never replicated to other computers, nor do these accounts have domain access.
local group	Collection of user accounts that are local to one specific workstation or member server. Local groups are created in the security database of a local computer and are not replicated to Active Directory or any other computers on the network.
nested	Object placed inside another object of the same type.
nested membership	When a group is placed in a second group, the members of the first group become members of the second group.
SAM account name	Each user's login name—the portion to the left of the "@" within a User Principal Name. The SAM account name must be unique across a domain.
SAM	(Security Account Manager) Database containing user accounts and security information that is located on a server.
security group	Security-related group created for purposes of granting resource access permissions to multiple users.
special identity group	Group used to define permission assignments. Administrators cannot manually modify the group membership of special identity groups, nor can they view their membership lists.
WSH	(Windows Script Host) Allows scripts to be run from a Windows desktop or a command prompt. The runtime programs provided to do this are WScript.exe and CScript.exe, respectively.