Ch08 Key Terms	
Account Lockout Policies	Subcategory in the Account Policies category that specifies the number of unsuccessful logon attempts that, if made within a contiguous timeframe, might constitute a potential security threat from an intruder. An Account Lockout Policy can be set to lock the account in question after a specified number of invalid attempts. Additionally, the policy specifies how long the account will remain locked.
account logon events	Setting that logs events related to successful user logons to a domain.
account management events	Setting that triggers an event that is written based on changes to account properties and group properties. Log entries written due to this policy setting reflect events related to user or group account creation, deletion, renaming, enabling, or disabling.
Audit Policy	Section of GPO Local Policies that enables administrators to log successful and failed security events such as logon events, account access, and object access.
auditing	Tracking events that take place on the local computer.
disk quotas	Setting that limits the amount of space available on the server for user data.
Enforce Password History	Group Policy setting that indicates the number of passwords that Active Directory should retain in memory before allowing someone to reuse a previously used password.
FGPP	(Fine-Grained Password Policies) Policy that can be applied to one or more users or groups of users, allowing the administrator to specify a more or less stringent password policy for a subset account than the password policy defined for the entire domain.
gpupdate.exe	Command-line tool used to force a manual Group Policy refresh. This tool was introduced in Windows Server 2003, and it is used in Windows Server 2003 and Windows Server 2008 to replace the secedit/refreshpolicy command that was used in Windows 2000.
Kerberos Policies	For domain accounts only, this policy enables administrators to configure settings that govern how Active Directory authentication functions.
KDC	(Key Distribution Center) Used to issue Kerberos tickets to users for domain access.
Local Policies	Policies that enable administrators to set user privileges on the local computer that govern what users can do on the computer and determine whether these actions are tracked within an event log.
logon events	This setting logs events related to successful user logons on a computer.
msDS-Password Settings	New object type in Windows Server 2008 that enables the use of Fine-Grained Password Policies. Also known as a Password Settings Object (PSO).
Offline Files	Separate Group Policy category that allows files to be available to users, even when users are disconnected from the network.
Password Policies	Subcategory in the Account Policies category that enforces password length, password history, and so on. Password Policies can be applied to domain and local user accounts.
PSO	(Password Settings Object) New object type in Windows Server 2008 that enables the use of Fine-Grained Password Policies. Also known as msDS-PasswordSettings.
policy change events	By default, this policy is set to audit successes in the Default Domain Controllers GPO. Policy change audit log entries are triggered by events such as user rights assignment changes, establishment or removal of trust relationships, IPSec policy agent changes, and grants or removals of system access privileges.
precedence	Attribute of the Password Settings Object (PSO) used as a tie-breaker to determine which PSO should apply: a PSO with a precedence of 1 will be applied over a PSO with a precedence of 5.

refresh interval	The available period that each background refresh process can be set to ranges from 0 to 64,800 minutes (45 days).
Restricted Groups	Policy setting that enables an administrator to specify group membership lists.
Security Options	Subcategory of the Local Policies setting area of a Group Policy Object that includes security settings related to interactive logon, digital signing of data, restrictions for access to floppy and CD-ROM drives, unsigned driver installation behavior, and logon dialog box behavior.
system events	Events that trigger a log entry in this category include system startups and shutdowns; system time changes; system event resources exhaustion, such as when an event log is filled and can no longer append entries; security log cleaning; or any event that affects system security or the security log. In the Default Domain Controllers GPO, this setting is set to log successes by default.
System Services	Category used to configure the startup and security settings for services running on a computer.
tattooing	Administrative Template setting that continues to apply until it is reversed by using a policy that overwrites the setting.
User Rights Assignment	Subcategory of the Local Policies setting area of a Group Policy Object that includes settings for items that pertain to rights needed by users to perform system-related tasks.