8.1.5 Group Policy Categories

GPOs contain hundreds of configuration settings. The following table describes commonly used policies:

Setting Category	Description
Account Policies	Use account policies to control the following: ▪ Password settings ▪ Account lockout settings ▪ Kerberos settings Account policies are in effect only when configured in a GPO linked to the domain itself. They can't be applied if the GPO is linked to an OU.
Local Policies/Audit Policy	Use audit policy settings to configure auditing for events, such as log on, account management, or privilege use.
Local Policies/User Rights Assignment	Computer policies include a special category of policies called *user rights*. User rights identify system maintenance tasks and the users or groups who can perform them. Examples of user rights include: ▪ Access this computer from the network (the ability to access resources on the computer through a network connection). ▪ Load and unload device drivers. ▪ Back up files and directories (does not include restoring files and directories). ▪ Shut down the system. ▪ Remove a computer from a docking station.
Local Policies/Security Options	Security options allow you to apply or disable rights for all of the users the policy applies to. Examples of Security Options policies include: ▪ Computer shut down when Security event log reaches capacity ▪ Unsigned driver installation
Registry	You can use registry policies to: ▪ Configure specific registry keys and values. ▪ Specify if a user can view and/or change a registry value, view sub-keys, or modify key permissions.
File System	Use File System policies to configure file and folder permissions that apply to multiple computers. For example, you can limit access to specific files that appear on all client computers.
Software Restriction Policies	Use software restrictions policies to define the software permitted to run on any computer in the domain. You can apply these policies to specific users or all users. You can use software restrictions to: ▪ Identify allowed or blocked software. ▪ Allow users to run only specified files on multi-user computers. ▪ Determine who can add trusted publishers. ▪ Apply restrictions to specific users or all users.
Administrative Templates	Administrative templates are registry-based settings that you can configure within a GPO to control the computer and overall user experience, such as: ▪ Use of Windows features such as BitLocker, offline files, and parental controls ▪ Customize the Start menu, taskbar, or desktop environment ▪ Control notifications ▪ Restrict access to Control Panel features ▪ Configure Internet Explorer features and options
Starter Group Policy Objects	Starter Group Policy Objects, or Starter GPOs, allow you to store a collection of administrative template policy settings in a single object. ▪ When you create a new GPO from a starter GPO, the new GPO has all of the Administrative template policy settings and values that were defined in the starter GPO. ▪ You can easily distribute starter GPOs by exporting and then importing them to another environment.

TestOut Corporation All rights reserved.