# How to prevent domain Group Policies from applying to certain user or computer accounts

https://support.microsoft.com/en-us/kb/816100


**SUMMARY**

This article describes how to keep domain group policies from also applying to administrator accounts, selected users, or both. Windows Server 2003 and Windows Server 2008 use group policies to control operating system behavior and security settings for users and computers in a Windows network. Group policies can be applied either to users or to computers, or to both. Group policies can be applied at the site, domain, or organizational unit level.


## Prevent Group Policies from applying to Administrator accounts

Typically, if you want Group Policy to apply only to specific accounts (either user accounts, computer accounts, or both), you can put the accounts in an organizational unit, and then apply Group Policy at that organizational unit level. However, there may be situations where you want to apply Group Policy to a whole domain, although you may not want those policy settings to also apply to administrator accounts or to other specific users or groups. The following procedures can prevent Group Policy from applying to administrative accounts (or any other group or user account that you specify) by editing the Discretionary Access Control List (DACL) for the policy.

### Use Active Directory Users and Computers

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree on the left, right-click the name of the domain in which the policy is applied. Then, click **Properties**.
3. Click the **Group Policy** tab.
4. Click the Group Policy object that you do not want to apply to administrators. By default, the only policy that is listed in the window is the Default Domain Policy.
5. Click **Properties**, and then click the **Security** tab.

   Note If the group or user who you do not want policies to apply does not appear in the list, follow these steps:
   1. Click **Add**.
   2. Click the domain in which the account resides.
   3. Locate the account, and then click it in the list.
   4. Click **OK**.
6. Click the administrators group (or other group or user) that you do not want the policy to apply to.
7. In the Permissions window, click to select the **Deny** check box for the **Apply Group Policy** permission.

   Note This action prevents the Group Policy object from being accessed and applied to the selected group or user account.

### Use Group Policy Management Console

1. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. In the console tree on the left, expand **Forest**.
3. Expand **Domains**.
4. Expand **Domain Name**.
5. Expand **Group Policy Objects**.
6. Click the Group Policy object that you do not want to apply to administrators.

7. In the display pane on the right, click the **Delegation** tab.
8. Click the **Advanced** button in the lower-right corner of the display pane.
9. Click **Add**, and then type the account name that you do not want the Group Policy object to apply to.
10. Click **OK**.

    Note Group Policy objects contain settings that apply to computer objects and to user objects. If you want only to restrict user settings from applying, add only the user account that you do not want the policy settings to apply to. If you want only to restrict computer settings from applying, add only the computer account that you do not want the policy settings to apply to. To add computer accounts, you have to click the **Object Types** button, and then click to select the **Computers** check box.
11. Make sure that the newly-added account is selected in the **Group or user names** window. Then, scroll down in the **Permissions** window, and click to select the **Deny** check box for the **Apply group policy permission**.
12. Click **OK**.
13. Click **Yes** at the Windows Security prompt.