

Real-World Scenario 5-4: Whitelisting and Blacklisting Applications in a Windows Server Policy

Scenario: You have been employed as a consultant to set up several policies in Windows Server. The first of these is to configure which applications can, and can't, be executed by employees.

Explain in your own words how you would accomplish your goal in Windows Server. If you have access to a Windows Server (for testing purposes), attempt to do this configuration within the operating system. If you don't, consider downloading an evaluation copy of Windows Server and loading it into a virtual machine.

Real-World Scenario 5-4 Solution

Whitelisting means that you give users access to specific applications only; for example, Microsoft Word (winword.exe) or Internet Explorer (iexplore.exe). *Blacklisting* means that you deny users access to specific applications. Both of these are possible within the same group policy object (GPO) in Windows Server. To create this GPO and modify it correctly, it is assumed that you have promoted the Windows Server to a domain controller, and that you have created an organizational unit (OU) to work with. It also assumes that you have an MMC to use as your workspace. The video solution shows how to create the OU. The following shows the basic steps involved in configuring the GPO:

NOTE Different versions of Windows Server can have slightly different steps but conceptually this works in the same manner. The following steps are based on Windows Server 2008.

Step 1. Create a new policy based off the OU and add it to the MMC:

- A. Go to File > Add/Remove Snap-in. This displays the Add/Remove Snap-ins dialog box.
- B. Scroll down to Group Policy Management Editor, highlight it, and click Add. This displays the Select Group Policy Object window.
- C. In the Select Group Policy Object dialog box, click Browse.
- D. Double-click the name of the OU folder (for example, accounting.dpro3.com). Yours might differ in OU name and domain name.
- E. On the upper-right side of the window, click the middle icon, which is called Create New Group Policy Object.
- F. Click the New button. Name the policy (for purposes of this example, use **acct-policy**) and press Enter. Then click OK. This creates a standard policy within the Accounting OU.

- G. Click Finish in the Select Group Policy Object window, and click OK in the Add or Remove Snapins window. This should add the new policy to the MMC.

Step 2. Configure the policy:

- A. Expand the acct-policy.
- B. Navigate to User Configuration > Policies > Administrative Templates > System.
- C. Double-click Don't Run Specified Windows Applications.
- D. Click the Enabled radio button.
- E. Click Show.
- F. Click Add and add an application (for example, winword.exe, the executable for Microsoft Word). Then click OK. Be sure to reset this at the end of the lab if it will affect any computers or users.
- G. Click OK for the policy's Properties window. This brings you back to the MMC. The policy will now be enabled.
- H. Double-click the Run Only Specified Windows Applications policy.
- I. Enable the policy; then click Show.
- J. Add an application by clicking the Add button, typing the name of an application (for example, excel.exe, the executable for Microsoft Excel), and clicking OK.
- K. Click OK for the policy's Properties window. This brings you back to the MMC. The policy will now be enabled.

Step 3. Save your MMC.

Step 4. Test whether your new policy works by logging in to a client computer with one of the user accounts that is part of the OU.

Video Solution: Watch the video solution "5-4: Whitelisting and Blacklisting Applications with a Windows Server Policy."