User Manual


# DeviceLock®

## Management via Group Policy

### SmartLine Inc

# Contents

# Using this Manual

This manual assumes you're familiar with basic functions like click, right-click, and double-click, and that you're familiar with the basics of the operating system you're using. This manual also assumes that you have basic network knowledge as well as the ability to install a Local Area Network (LAN). We strongly recommend reading this manual very carefully and thoroughly.

This manual uses the following conventions:

- *Italics* for file names, paths, buttons, menus, and menu items.
- ***Bold Italics*** for notes and comments.
- Keyboard keys with a plus sign separating keys that you press simultaneously. For example: press Ctrl+Alt+Del to restart your computer.

# 1. General Information

## 1.1 Overview

In addition to the standard way of managing permissions via DeviceLock Manager, DeviceLock also provides you with a more powerful mechanism – permissions and settings can be changed and deployed via Group Policy in an Active Directory domain.

Group Policy enables policy-based administration that uses Active Directory. Group Policy uses directory services and security group membership to provide flexibility and support extensive configuration information. Policy settings are created using the Microsoft Management Console (MMC) snap-in for Group Policy.

System administrators can use system policies to control user and computer configurations from a single location on a network. System policies propagate registry settings to a large number of computers without requiring the administrator to have detailed knowledge of the registry.

Tighter integration into the Active Directory is a very important function of DeviceLock. It makes DeviceLock's permissions management and deployment easier for large networks and more convenient for system administrators.

Integration into the Active Directory eliminates the need to install more third-party applications for centralized management and deployment. DeviceLock does not need to have its own server-based version to control the entire network, instead it uses standard functions provided by the Active Directory.

Via Group Policy it is possible to:

- Install DeviceLock Service on all the computers in a network;
- Change DeviceLock's settings on every computer;
- Control user access to devices and change permissions for an entire domain.

***Please note that to manage DeviceLock via Group Policy, you must have Active Directory properly installed and configured. For more information about installing and configuring Active Directory, please refer to the related Microsoft documentation.***

## 1.2 Applying Group Policy

Policy is applied when the computer starts up. When a user turns on the computer, the system applies DeviceLock's policy.

Policy can be optionally reapplied on a periodic basis. By default, policy is reapplied every 90 minutes. To set the interval at which policy will be reapplied, use the *Group Policy Object Editor*. For more information, please refer to the Microsoft's Knowledge Base:
http://support.microsoft.com/default.aspx?scid=kb;en-us;203607

Policy can also be reapplied on demand. To refresh the current policy settings immediately on Windows XP and later, administrators can call the *gpupdate.exe /force* command-line utility provided by Microsoft. On Windows 2000, administrators can call another command-line utility provided by Microsoft: *secedit /refreshpolicy machine_policy /enforce*.

When applying policy, the system queries the directory service for a list of Group Policy Objects (GPOs) to process. Each GPO is linked to an Active Directory container in which the computer or user belongs. By default, the system processes the GPOs in the following order: local, site, domain, then organizational unit. Therefore, the computer receives the policy settings of the last Active Directory container processed.

When processing the GPO, the system checks the access-control list (ACL) associated with the GPO. If an access-control entry (ACE) denies the computer access to the GPO, the system does not apply the policy settings specified by the GPO. If the ACE allows access to the GPO, the system applies the policy settings specified by the GPO.

***Note that application deployment occurs only during startup, not on a periodic basis. This prevents undesirable results, such as uninstalling or upgrading an application that is in use. However, DeviceLock's policy settings are applied periodically.***

## 1.3 Standard GPO Inheritance Rules

Any unconfigured settings anywhere in a GPO can be ignored since they are not inherited down the tree; only configured settings are inherited. There are three possible scenarios:

- A parent has a value for a setting, and a child does not.
- A parent has a value for a setting, and a child has a nonconflicting value for the same setting.
- A parent has a value for a setting, and a child has a conflicting value for the same setting.

If a GPO has settings that are configured for a parent Organizational Unit, and the same policy settings are unconfigured for a child Organizational Unit, the child inherits the parent's GPO settings. That makes sense.

If a GPO has settings configured for a parent Organizational Unit that do not conflict with a GPO on a child Organizational Unit, the child Organizational Unit inherits the parent GPO settings and applies its own GPOs as well.

If a GPO has settings that are configured for a parent Organizational Unit that conflict with the same settings in another GPO configured for a child Organizational Unit, then the child Organizational Unit does not inherit that specific GPO setting from the parent Organizational Unit. The setting in the GPO child policy takes priority, although there is one case in which this is not true. If the parent disables a setting and the child makes a change to that setting, the child's change is ignored. In other words, the disabling of a setting is always inherited down the hierarchy.

# 2. DeviceLock Service Deployment

This step-by-step instruction describes how to use Group Policy to automatically distribute DeviceLock Service to client computers. DeviceLock Service can be deployed in an Active Directory domain using the Microsoft Software Installer (MSI) package (*DeviceLock Service.msi*).

***NOTE: Microsoft Windows Group Policy automated-program installation requires client computers that are running Windows 2000 or later.***

You can use Group Policy to distribute DeviceLock Service by using the following steps:

- Create a Distribution Point

  To install DeviceLock Service, you must create a distribution point on the server:

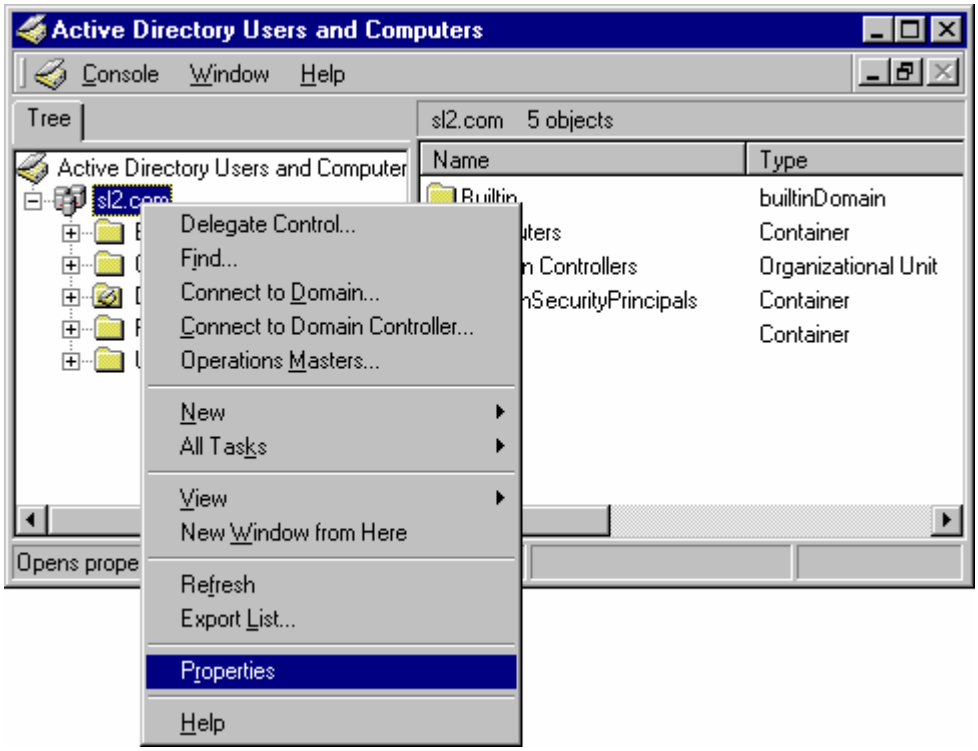
  1. Log on to the server computer as an administrator.
  2. Create a shared network folder in which to place the MSI package.
  3. Set permissions on the share to allow access to the distribution package.
  4. Copy the MSI package (*DeviceLock Service.msi*) to the distribution point.

- Create a Group Policy Object

  To create a Group Policy object (GPO) with which to distribute DeviceLock Service:

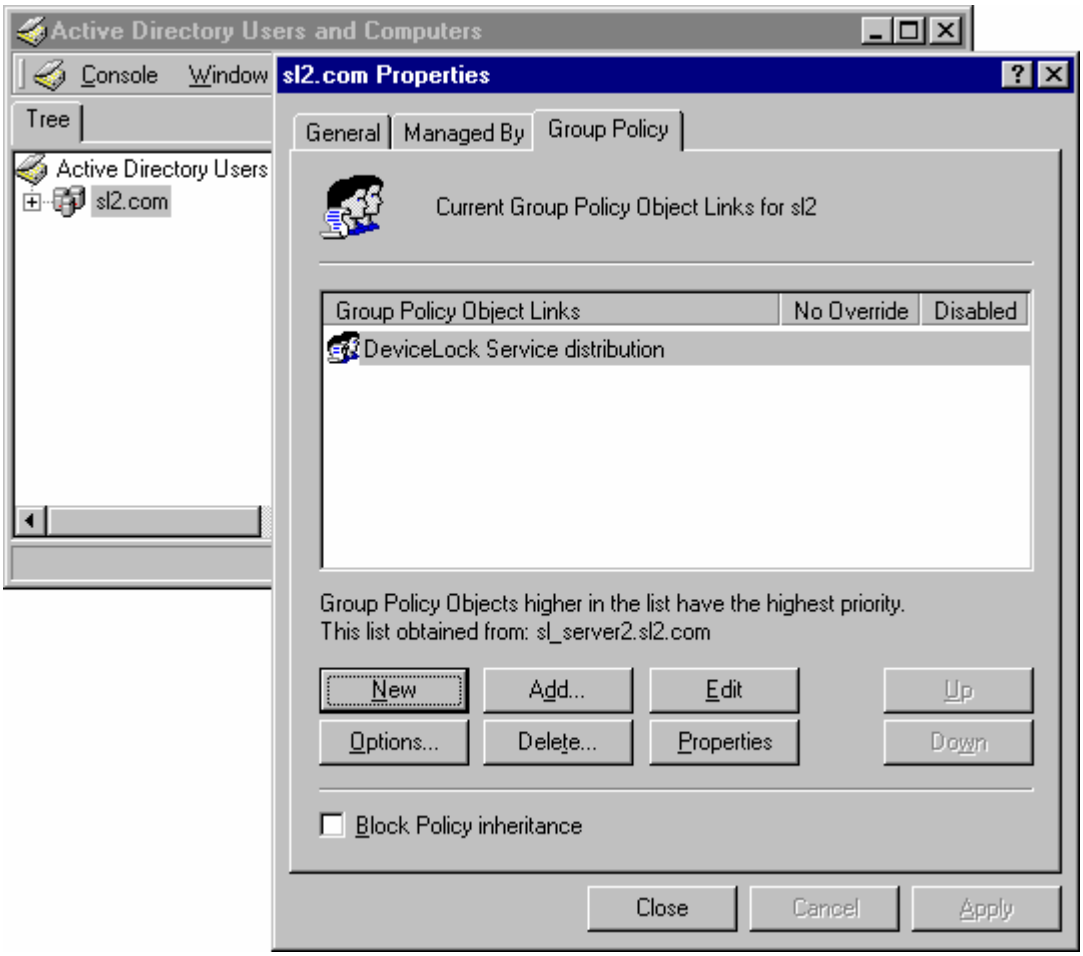
  1. Start the *Active Directory Users and Computers* snap-in.

  2. In the console tree, right-click your domain, and then click *Properties*.



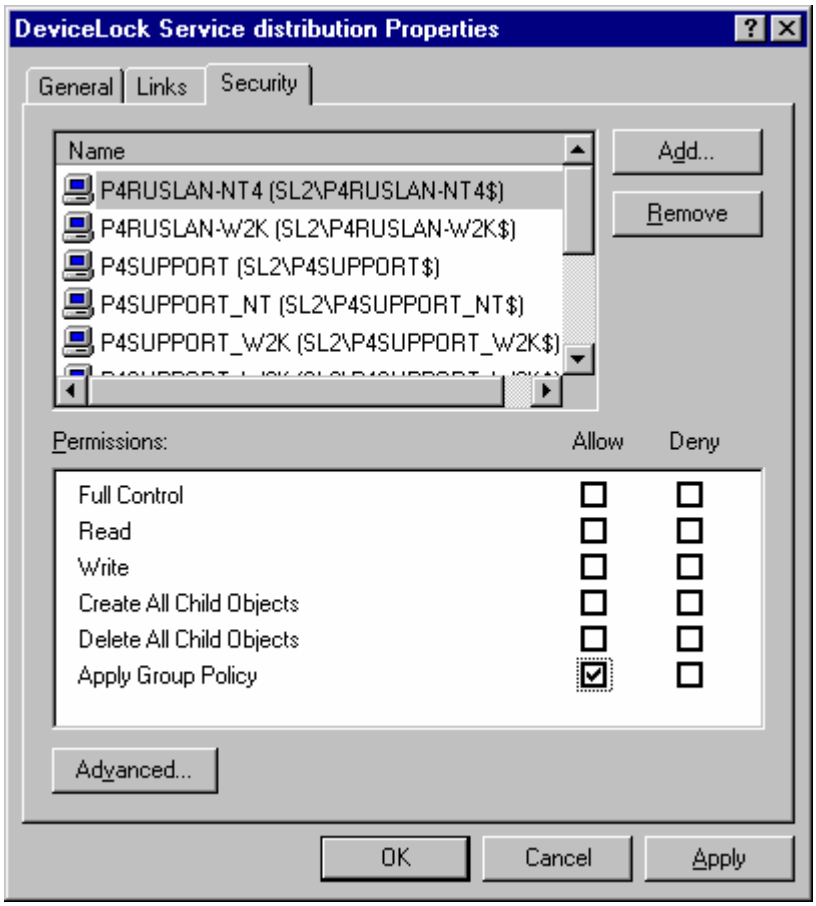
3. Click the *Group Policy* tab, and then click *New*.

4. Type the name that you want to call this policy (for example: "*DeviceLock Service distribution*"), and then press *ENTER*.




5. Click *Properties*, and then click the *Security* tab.

6. Click on the *Deny* check box next to *Apply Group Policy* for the security groups that you want to prevent from having this policy applied. Click on the *Allow* check box for the groups to which you want to apply this policy. When you are finished, click *OK*.

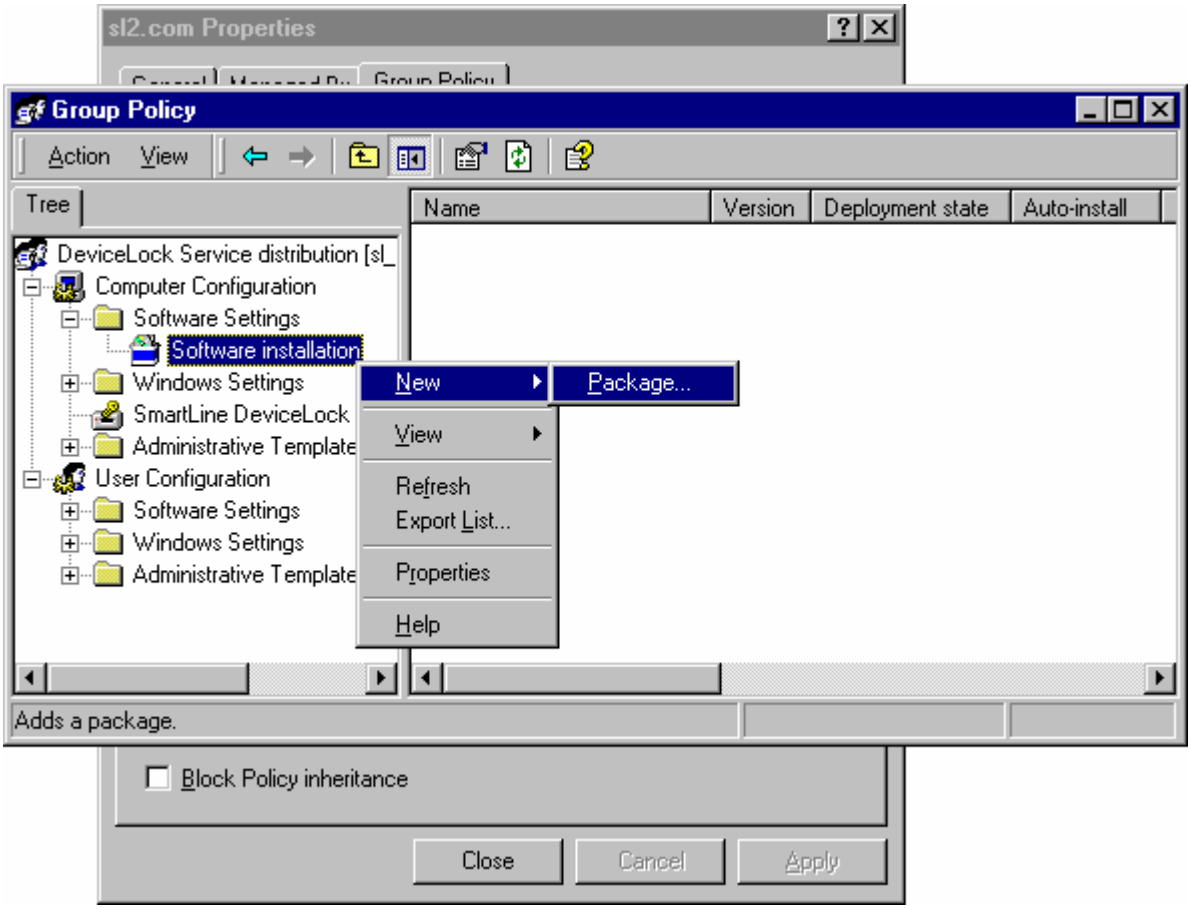



- Assign a Package

To assign DeviceLock Service to computers that are running Windows 2000 or later:

1. Start the *Active Directory Users and Computers* snap-in.
2. In the console tree, right-click your domain, and then click *Properties*.
3. Click the *Group Policy* tab, select the group policy object that you want, and then click *Edit*.
4. Under *Computer Configuration*, expand *Software Settings*.

5. Right-click *Software installation*, point to *New*, and then click *Package*.

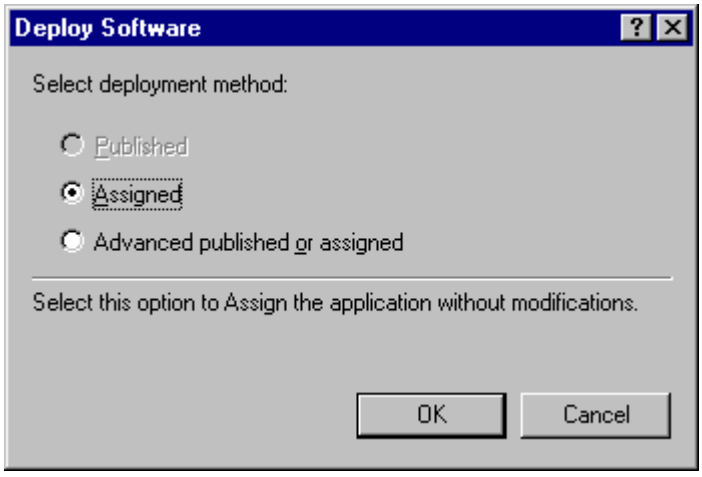



6. In the *Open* dialog box, type the full Universal Naming Convention (UNC) path to the shared folder that contains the DeviceLock Service MSI package. For example: *\\file server\share\DeviceLock Service.msi*.

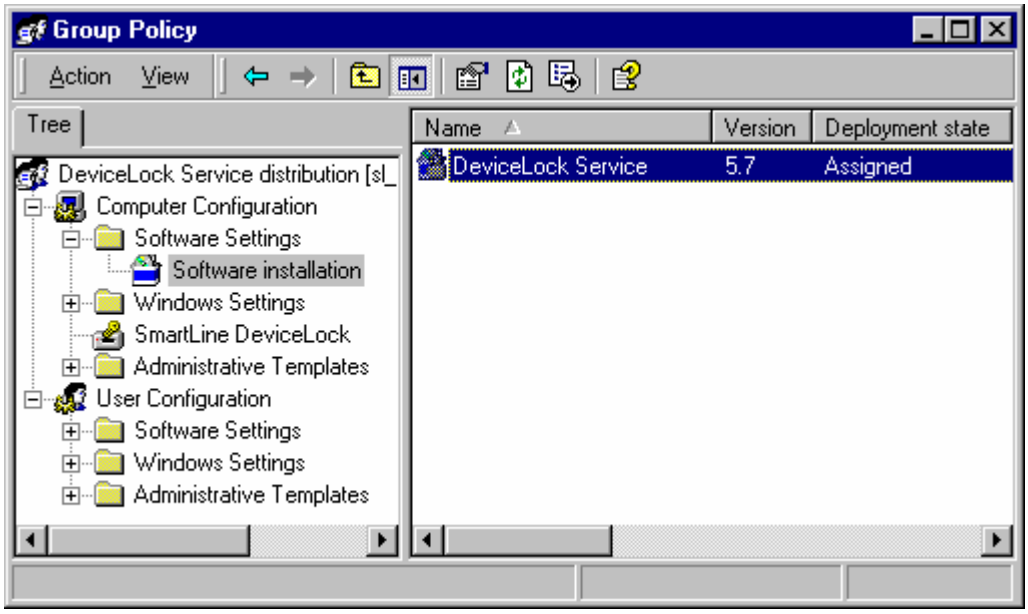
   ***IMPORTANT: Do not browse to the location. Ensure that you use the UNC path to the shared folder.***

7. Click *Open*.

8. Click *Assigned*, and then click *OK*. The package is listed in the right pane of the *Group Policy* window.



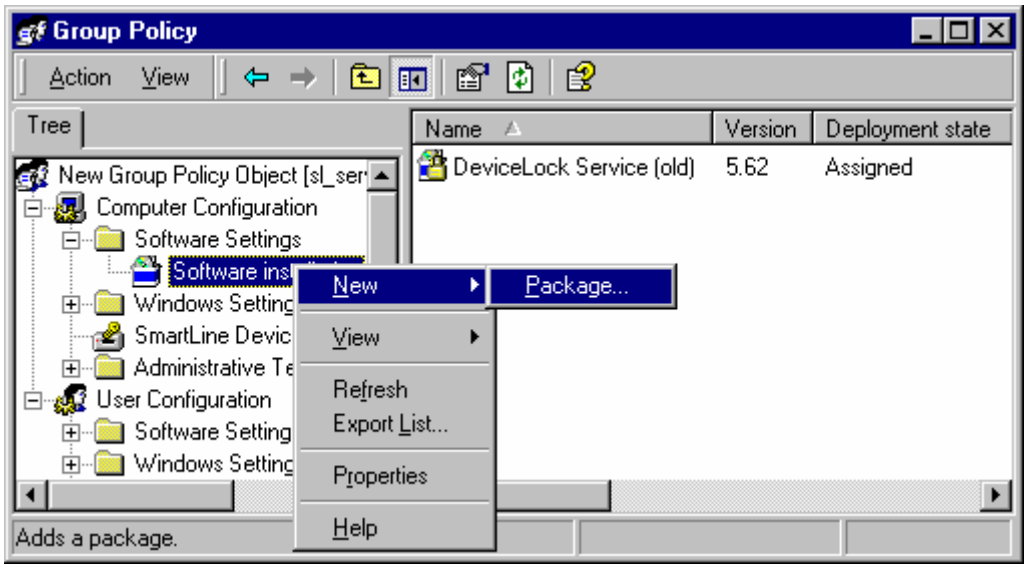
9. Close the *Group Policy* snap-in, click *OK*, and then quit the *Active Directory Users and Computers* snap-in. When the client computer starts, DeviceLock Service is automatically installed.




- Upgrade a Package

  If the previous version of DeviceLock Service was already deployed and you want to upgrade it to the new one:

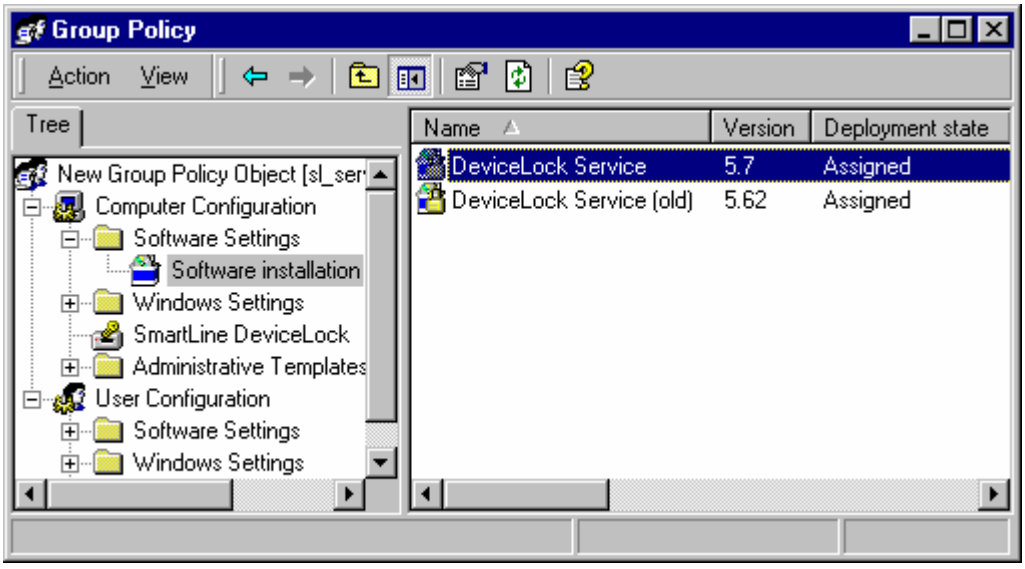
  1. Start the *Active Directory Users and Computers* snap-in.
  2. In the console tree, right-click your domain, and then click *Properties*.
  3. Click the *Group Policy* tab, select the group policy object that contains the old DeviceLock Service package, and then click *Edit*.
  4. Under *Computer Configuration*, expand *Software Settings*.
  5. Right-click *Software installation*, point to *New*, and then click *Package*.



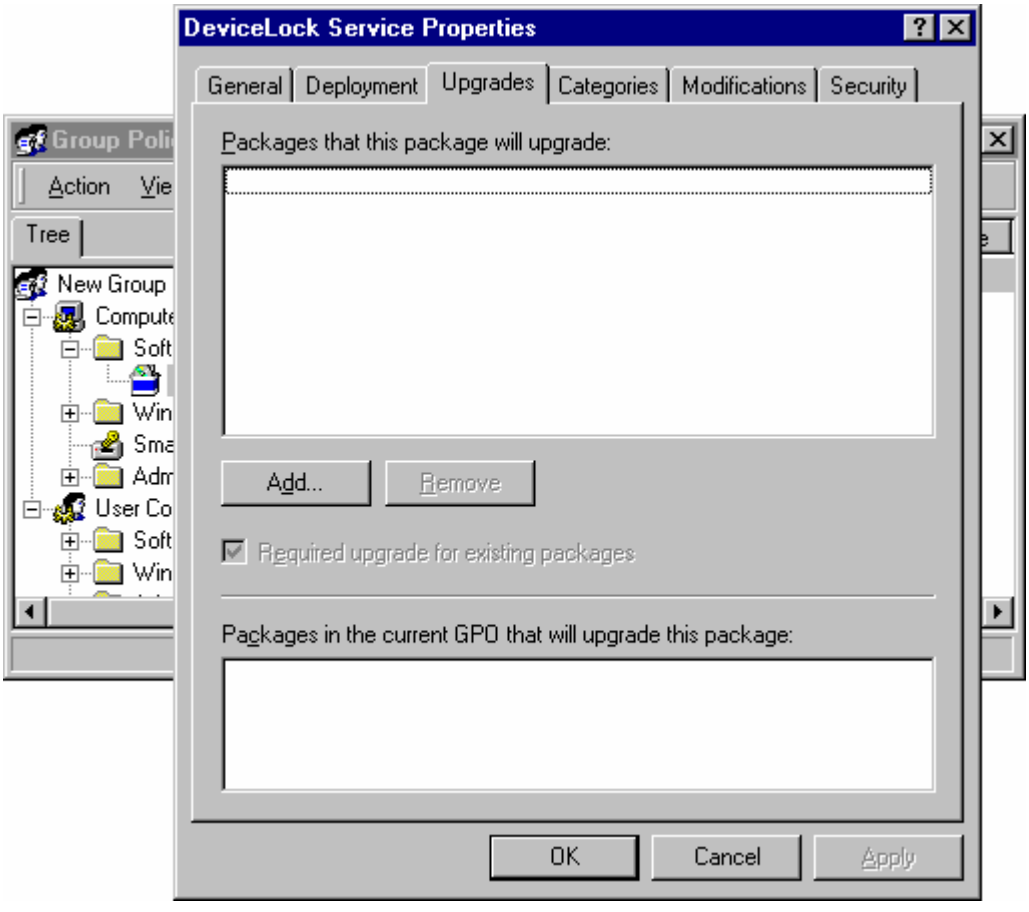
6. In the *Open* dialog box, type the full Universal Naming Convention (UNC) path to the shared folder that contains the new DeviceLock Service MSI package. For example: *file server**share**DeviceLock Service.msi*.

7. Click *Open*.

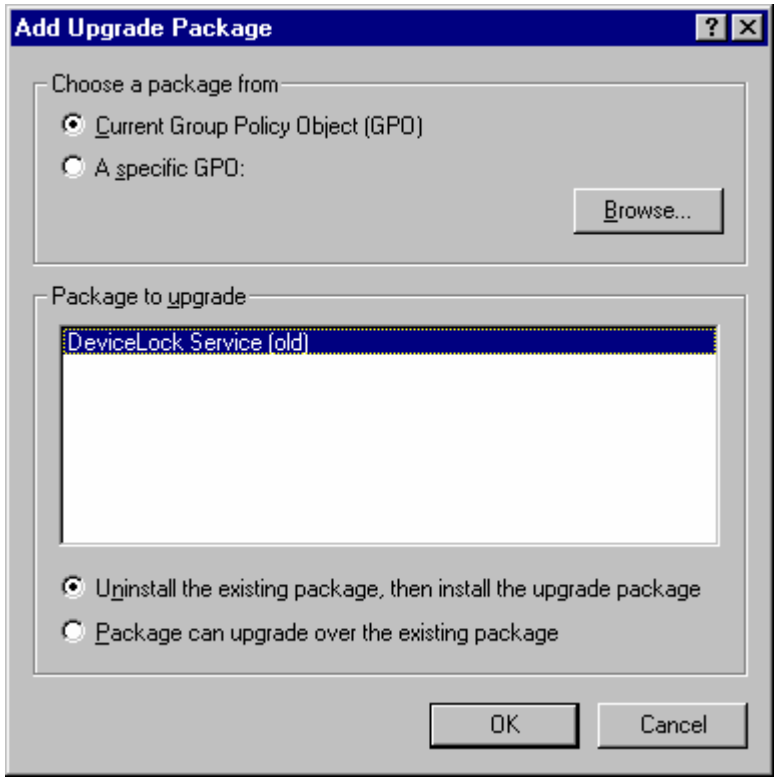
8. Click *Assigned*, and then click *OK*. The new package is listed in the right pane of the *Group Policy* window.



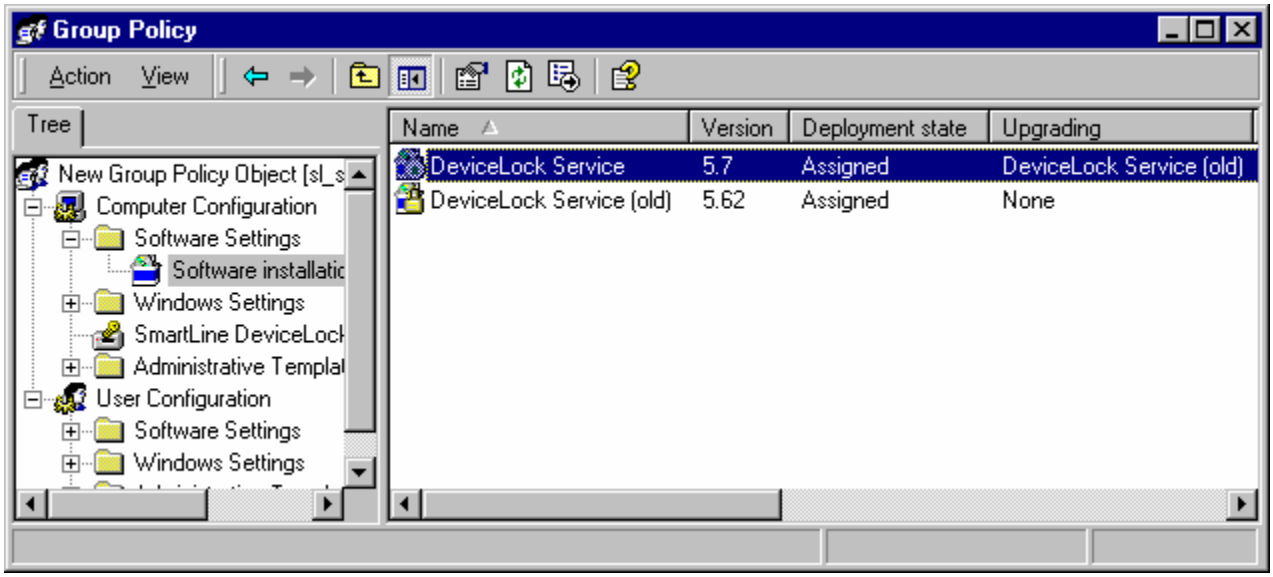

9. Right-click the new package, click *Properties*, and then click the *Upgrades* tab.



10. Click *Add*, select the old DeviceLock Service package you want to upgrade, click *Uninstall the existing package, then install the upgrade package*, and then click *OK*.




11. Click *OK* to close the *Properties* window, close the *Group Policy* snap-in, click *OK*, and then quit the *Active Directory Users and Computers* snap-in. When the client computer starts, DeviceLock Service is automatically upgraded.



- Redeploy a Package

  In some cases you may want to redeploy DeviceLock Service. To redeploy a package:

  1. Start the *Active Directory Users and Computers* snap-in.
  2. In the console tree, right-click your domain, and then click *Properties*.
  3. Click the *Group Policy* tab, click the group policy object with which you deployed the package, and then click *Edit*.
  4. Expand the *Software Settings* container that contains the *Software installation* item with which you deployed the package.
  5. Click the *Software installation* container that contains the package.
  6. In the right pane of the *Group Policy* window, right-click the program, point to *All Tasks*, and then click *Redeploy application*. The following message is displayed: "*Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?*"
  7. Click *Yes*.
  8. Quit the *Group Policy* snap-in, click *OK*, and then quit the *Active Directory Users and Computers* snap-in.

- Remove a Package

  To remove DeviceLock Service:

  1. Start the *Active Directory Users and Computers* snap-in.
  2. In the console tree, right-click your domain, and then click *Properties*.
  3. Click the *Group Policy* tab, click the group policy object with which you deployed the package, and then click *Edit*.
  4. Expand the *Software Settings* container that contains the *Software installation* item with which you deployed the package.
  5. Click the *Software installation* container that contains the package.
  6. In the right pane of the *Group Policy* window, right-click the program. Point to *All Tasks*, and then click *Remove*.
  7. Click *Immediately uninstall the software from users and computers*, and then click *OK*.
  8. Quit the *Group Policy* snap-in, click *OK*, and then quit the *Active Directory Users and Computers* snap-in.

Please keep in mind:

- Deployment occurs only when the computer starts up, not on a periodic basis. This prevents undesirable results, such as uninstalling or upgrading an application that is in use.

- DeviceLock Service will be copied to the Windows system directory (e.g. *c:\winnt\system32*) if this service doesn't exist on the system. If the service exists on this system but is too old, DeviceLock Service will be copied to the directory of the old version and the old version will be replaced.

- If DeviceLock Service is installed on an NTFS partition, an installation routine protects the service's file by allowing only members of the *Administrators* group or the *SYSTEM* account to access this file.

- An installation routine also protects DeviceLock Service by allowing only members of the *Administrators* group or the *SYSTEM* account to start, stop, or delete the service.

# 3. DeviceLock Group Policy Manager

## 3.1 Installation

DeviceLock Group Policy Manager can be installed on any computer running Windows 2000/XP or Windows Server 2003.

DeviceLock Group Policy Manager includes DeviceLock Management Console that is similar to DeviceLock Manager. It can be used to directly manage computers with running DeviceLock Service. DeviceLock Management Console can be installed on the computer running Windows NT 4 but Microsoft Management Console had to be installed as well. To download Microsoft Management Console for Windows NT 4, visit the Microsoft's website:
http://www.microsoft.com/downloads/details.aspx?familyid=3F620A07-C996-4A81-AAD8-30134A43EC46&displaylang=en

To install DeviceLock Group Policy Manager, run Setup (*setup_gp.exe*).

DeviceLock Group Policy Manager installs to the directory of your choice. Setup tries to find a DeviceLock Group Policy Manager installation and, if one exists, Setup suggests you install DeviceLock Group Policy Manager to the same directory. If a previous installation does not exist, Setup suggests you install DeviceLock Group Policy Manager to the Program Files directory on the system drive (e.g. *C:\Program Files\DeviceLock Group Policy Manager*). You can select another directory for installation.

After a successful install, you can open DeviceLock Group Policy Manager by running the Windows Group Policy Object editor.

To run DeviceLock Management Console, select the *DeviceLock Management Console* item from the *Programs* menu.

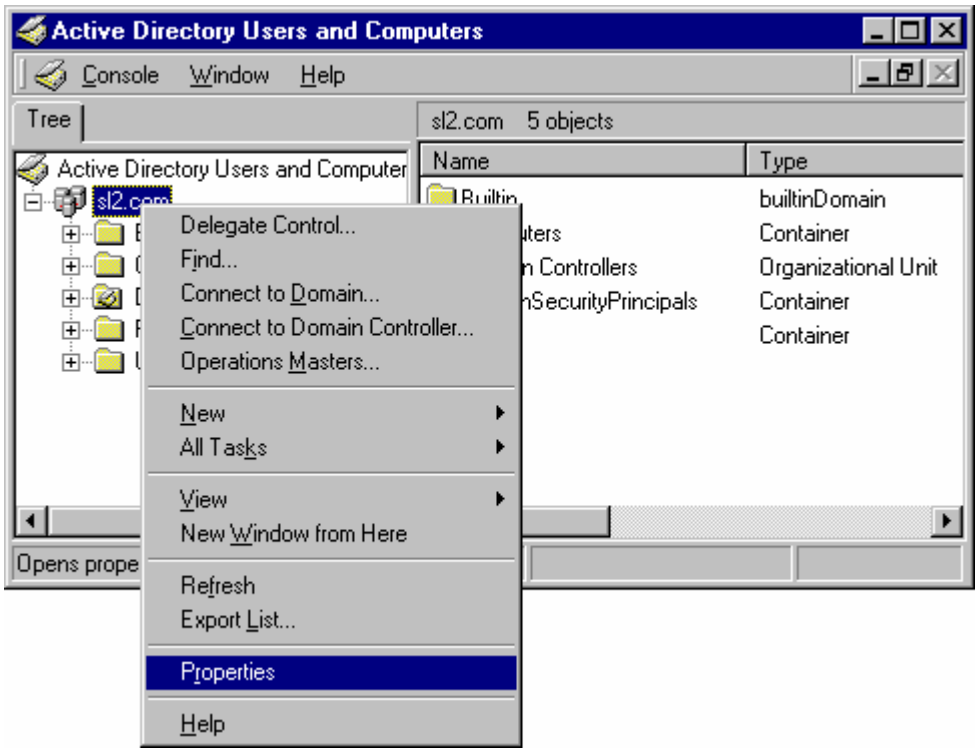
## 3.2 Usage

You can use DeviceLock Group Policy Manager to control DeviceLock's permissions and settings via Group Policy in an Active Directory domain. DeviceLock Group Policy Manager integrates into the Group Policy Object (GPO) editor.

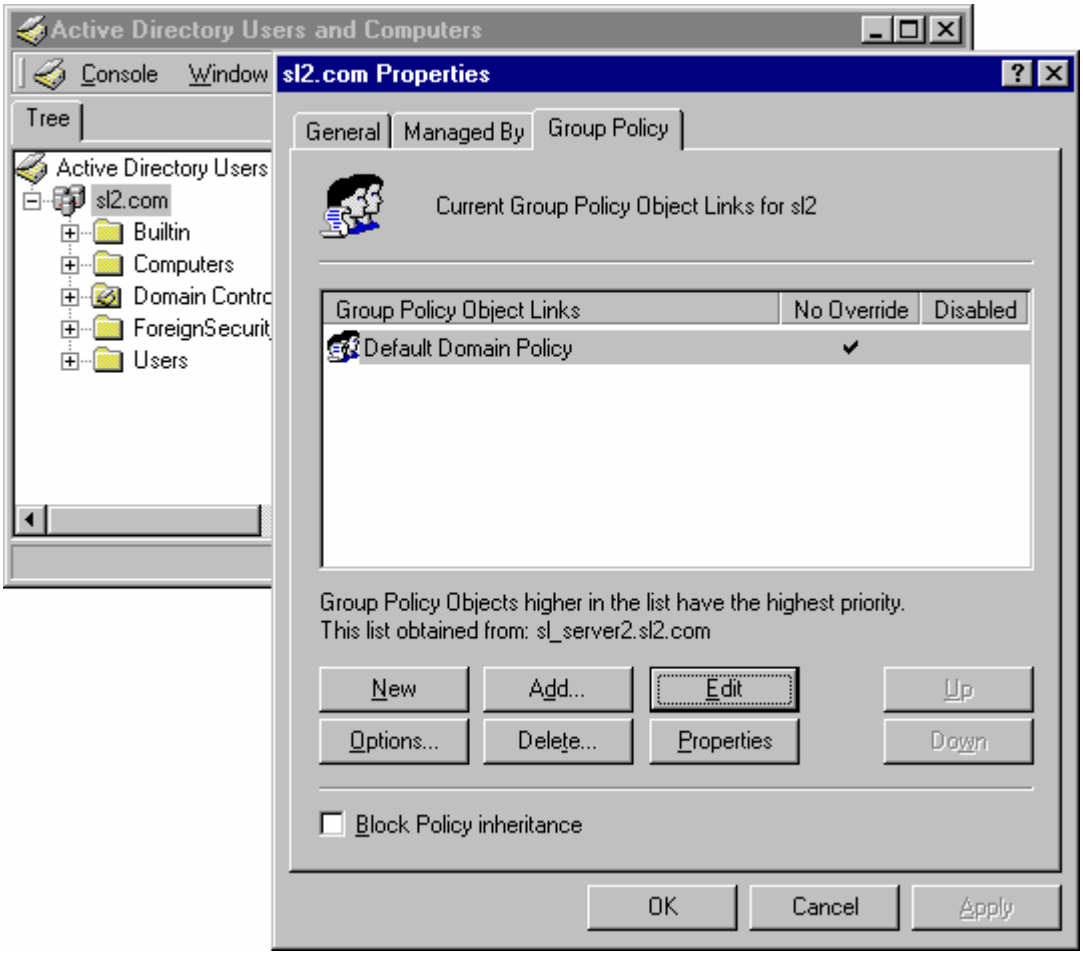
To open DeviceLock Group Policy Manager:

1. Start the *Active Directory Users and Computers* snap-in.

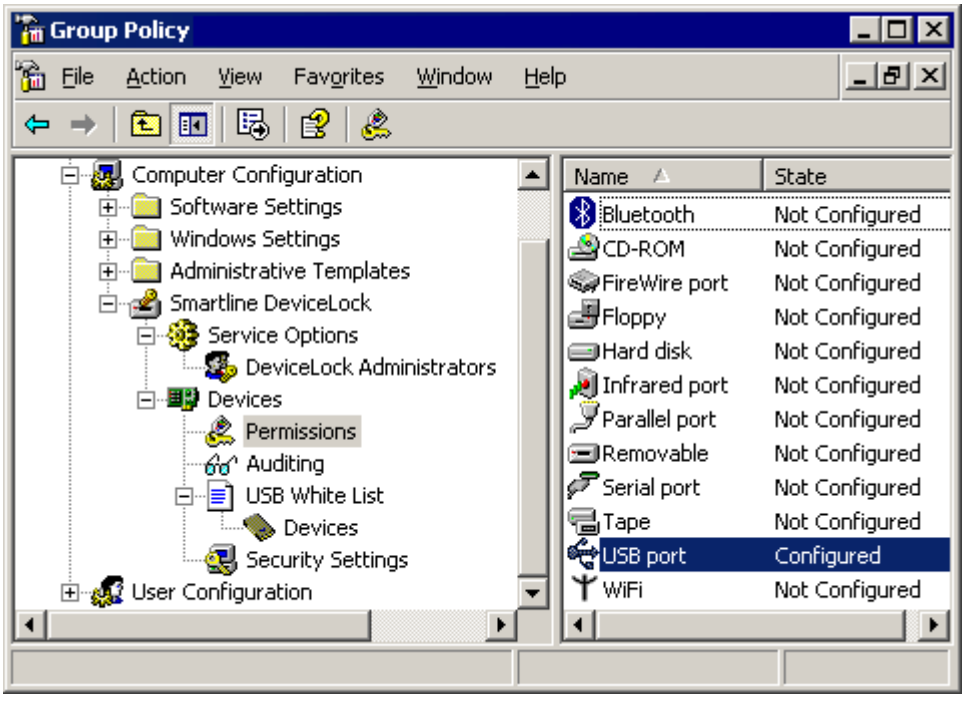
2. In the console tree, right-click your domain, and then click *Properties*.



3. Click the *Group Policy* tab, select the group policy object that you want, and then click *Edit*. If you wish to create the new group policy object, click *Add*.



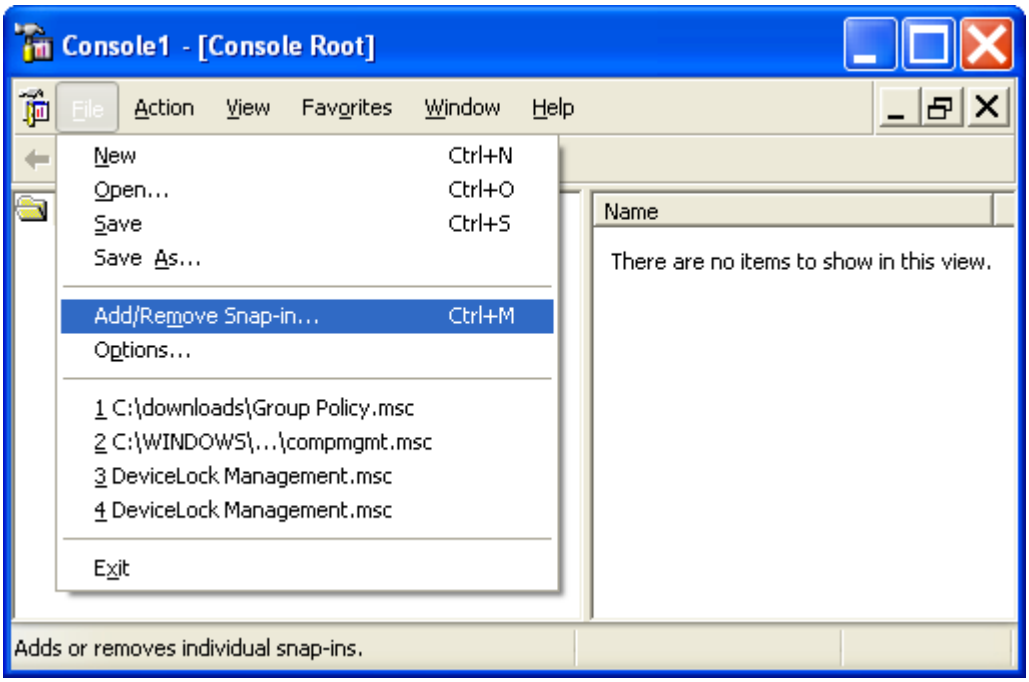

4. Under *Computer Configuration*, select *SmartLine DeviceLock*.



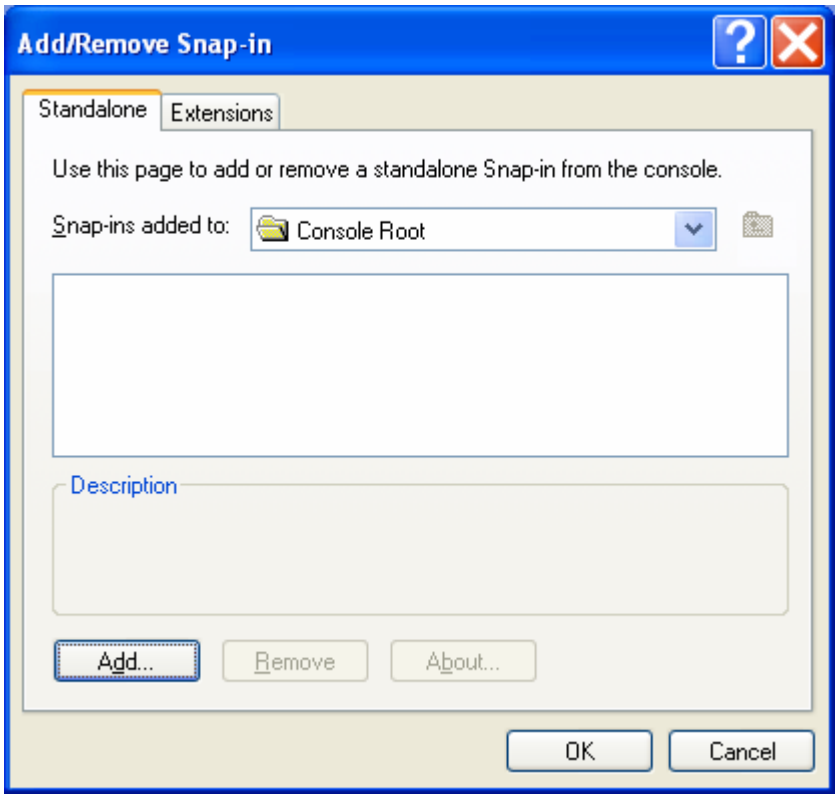
Alternatively, you can start MMC and add the Group Policy snap-in manually:

1. Run *mmc* from the command line or use the *Run* menu to execute this command.

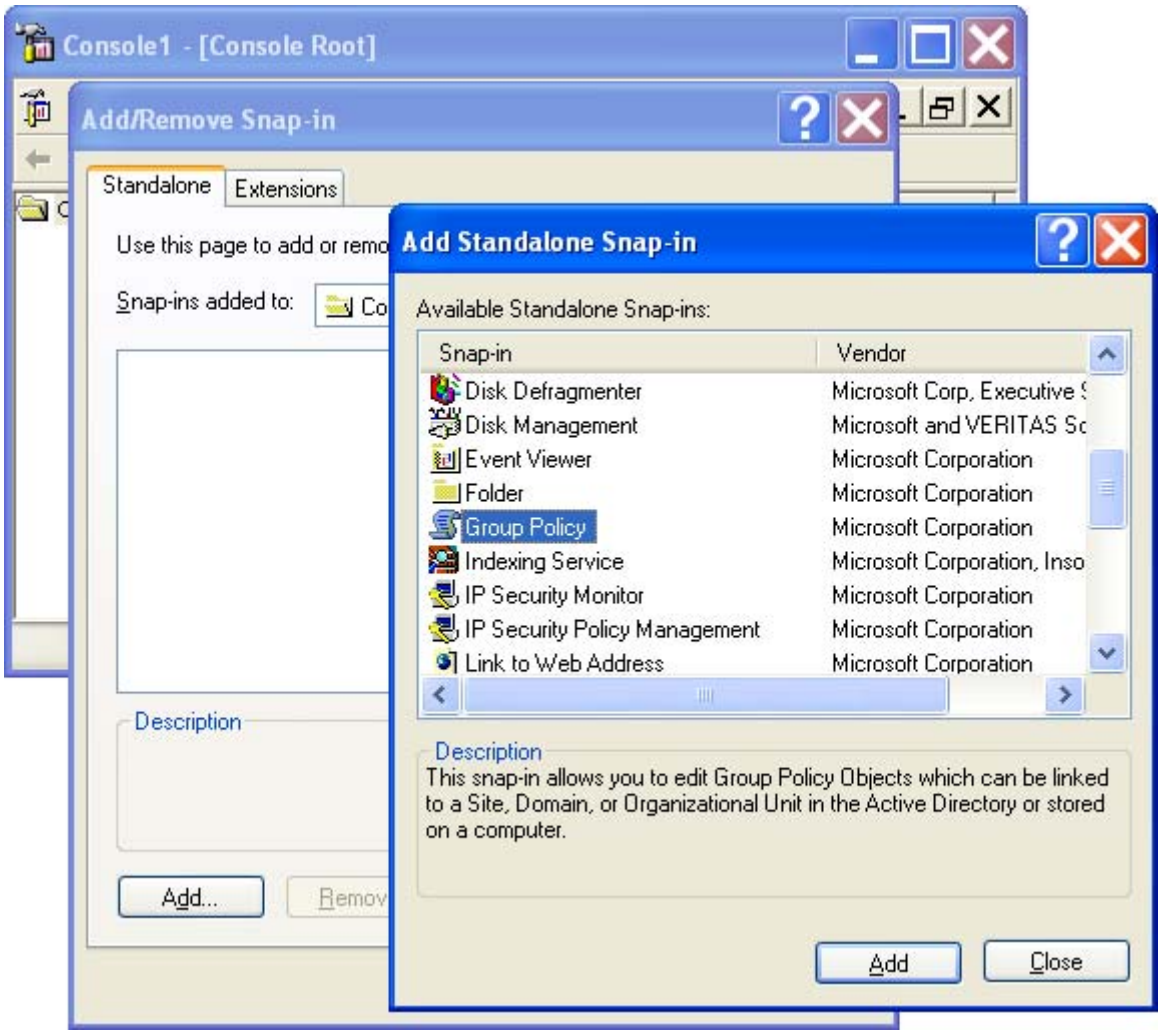
2. Open the *File* menu, and then click *Add/Remove snap-in*.



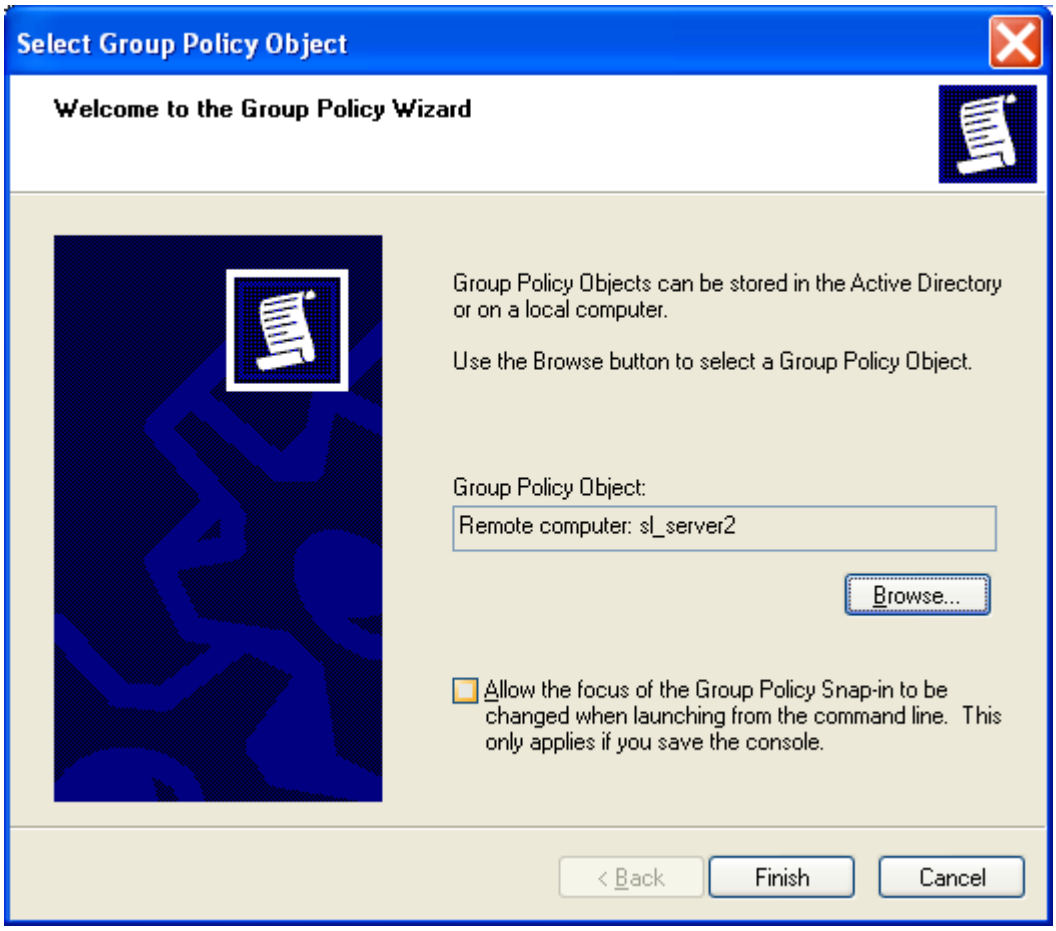

3. Click the *Standalone* tab, and then click *Add*.



4. Select *Group Policy* from the list, then click *Add*.



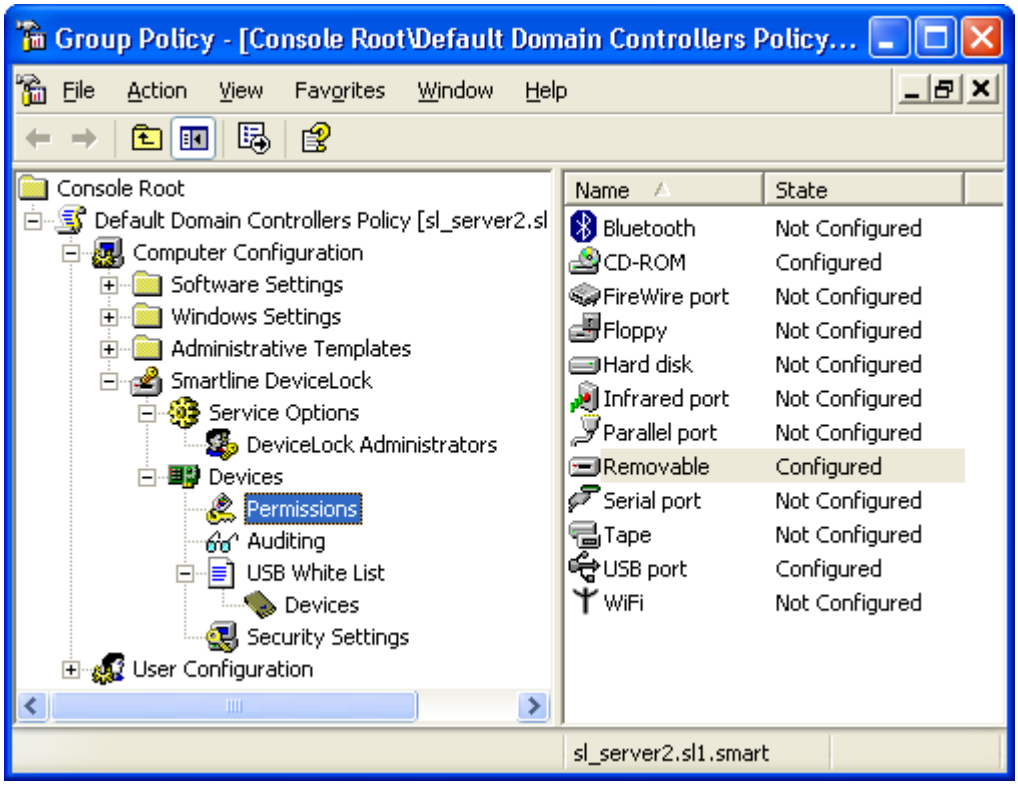
5. Select a Group Policy Object either from the Active Directory or a local computer, and then click *Finish*.




6. Click *Close* to close the *Add Standalone Snap-in* window.

7. Click *OK* to add the snap-in.

8. Expand the *Computer Configuration* container, and then select *SmartLine DeviceLock*.




There is no difference between the procedure for defining DeviceLock's permissions and audit rules in DeviceLock Manager and in DeviceLock Group Policy Manager. Just select a device type and set permissions and/or audit rules for it as described in the *DeviceLock Manual.pdf* document.

If you want to disallow changing permissions and audit rues for individual computers (without the GPO editor), enable *Override Local Policy* in *Service Options*. It enables the Group Policy mode for all the computers in GPO, such that the Local Policy mode can't be enabled for these computers.

***NOTE: In order to change DeviceLock's permissions and settings via Group Policy, DeviceLock Service must be installed and started on all the computers belonging to the GPO. For more information about service installation, please read the DeviceLock Service Deployment section of this document.***

***Also, don't forget that Group Policy is reapplied on a periodic basis (by default, every 90 minutes) so your changes do not take effect immediately. For more information, read the Applying Group Policy section.***