User Manual

# DeviceLock®

## 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 Overview

## 1.1 General Information

Preventing unauthorized downloading as well as the uploading of inappropriate software and data is important when trying to protect and administer a company's computer network. The traditional solution has been a physical lock on the floppy drive. DeviceLock eliminates the need for physical locks and has a number of advantages.

DeviceLock is easy to install. Administrators can have instant access from remote computers when necessary. The administrator of the machine or domain can designate user access to floppy drives, CD-ROM drives, other removable media, tape drives, WiFi, and Bluetooth adapters, or USB, FireWire, infrared, and serial and parallel ports. All types of file systems are supported.

DeviceLock can audit user activity for a particular device type on a local computer. Based on the user's security context, this capability allows you to audit activities that belong to a certain user or user group. DeviceLock employs the standard event logging subsystem and writes audit records to the Windows event log.

DeviceLock supports data shadowing – the ability to mirror all data copied to external storage devices or transferred through serial and parallel ports. A full copy of the files can be saved into the SQL database. Shadowing, like auditing, can be defined on a per-user basis.

Moreover, the DeviceLock data shadowing function is compatible with the National Software Reference Library maintained by the National Institute of Standards and Technology (NIST) and with the Hashkeeper Database designed and maintained by U.S. DOJ National Drug Intelligence Center (NDIC).

The data logged by DeviceLock can be checked against hash databases (collections of digital signatures of known, traceable data) and used in computer forensics.

You may also create your own database with digital signatures (SHA-1, MD5 and CRC32 are supported) of critical files and then use it for tracing purposes. For example, you can trace which users are copying signatured files, at what time, and with which devices.

For information on how to use hash databases in cooperation with DeviceLock, please contact our technical support team.

More information about hash databases and their samples can be found at the National Software Reference Library’s website: http://www.nsrl.nist.gov.

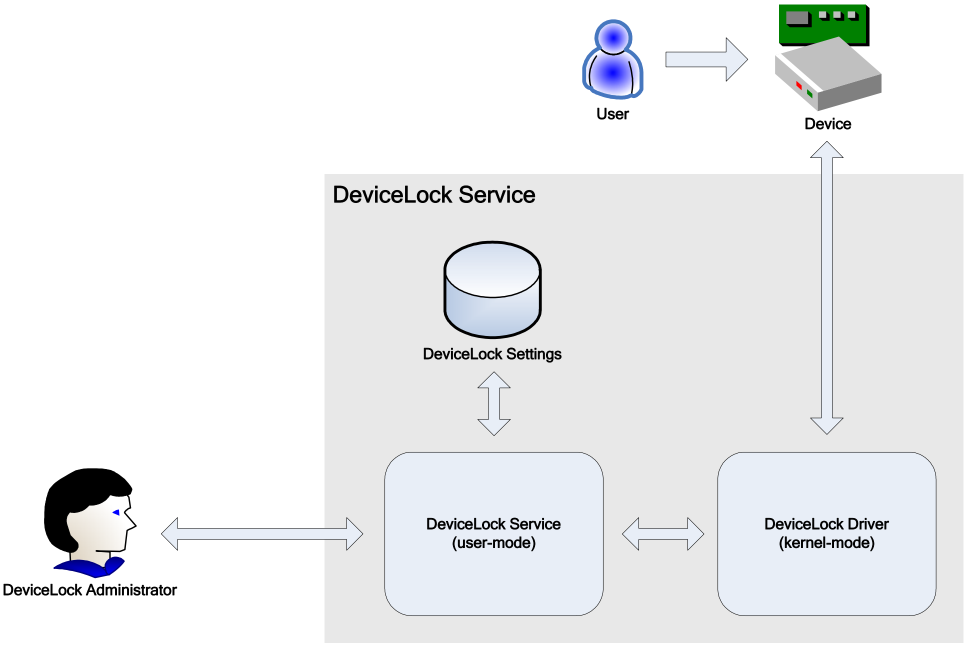
In addition to the standard (per computer) way of managing permissions, DeviceLock also provides you with a more powerful mechanism – permissions and settings can be changed and deployed via Group Policy in an Active Directory domain.

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.

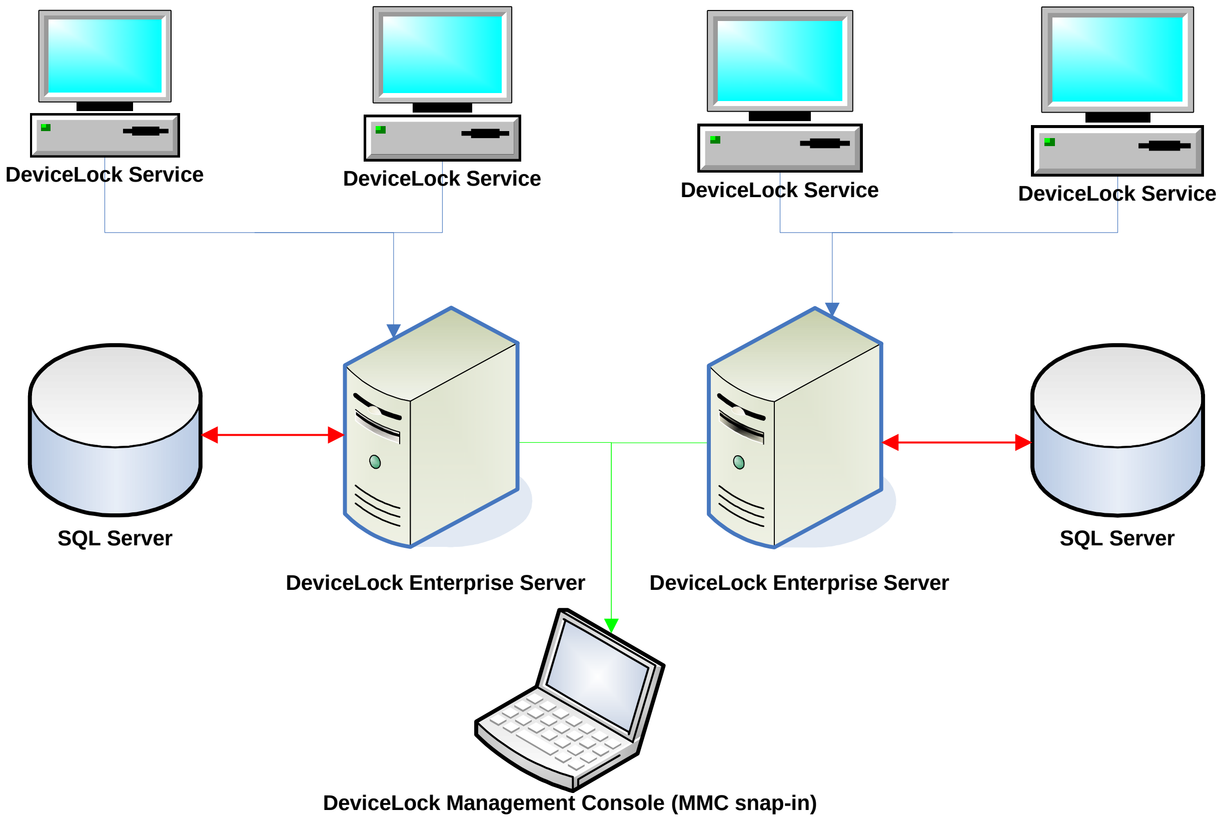
Integration into the Active Directory eliminates the need to install more third-party applications for centralized management and deployment. DeviceLock does not need to have its own server-based version to control the entire network, instead it uses standard functions provided by the Active Directory.

DeviceLock consists of three parts: the agent (DeviceLock Service), the server (DeviceLock Enterprise Server) and the management console (DeviceLock Management Console, DeviceLock Group Policy Manager or DeviceLock Enterprise Manager):

1. DeviceLock Service is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.

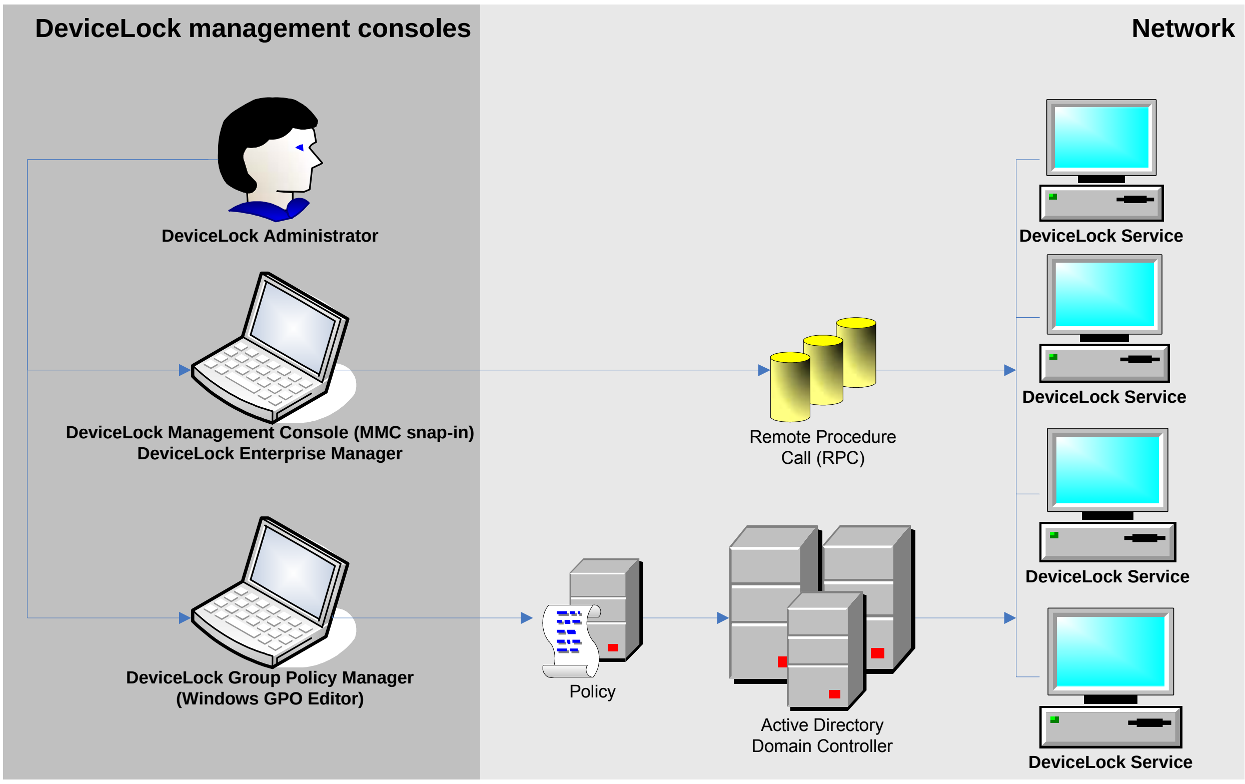


2. DeviceLock Enterprise Server is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data. You can install several DeviceLock Enterprise Servers to uniformly spread the network load.



DeviceLock Service
DeviceLock Service
DeviceLock Service
DeviceLock Service
SQL Server
DeviceLock Enterprise Server
DeviceLock Enterprise Server
SQL Server
DeviceLock Management Console (MMC snap-in)

3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor). DeviceLock Management Console is also used to manage DeviceLock Enterprise Server.

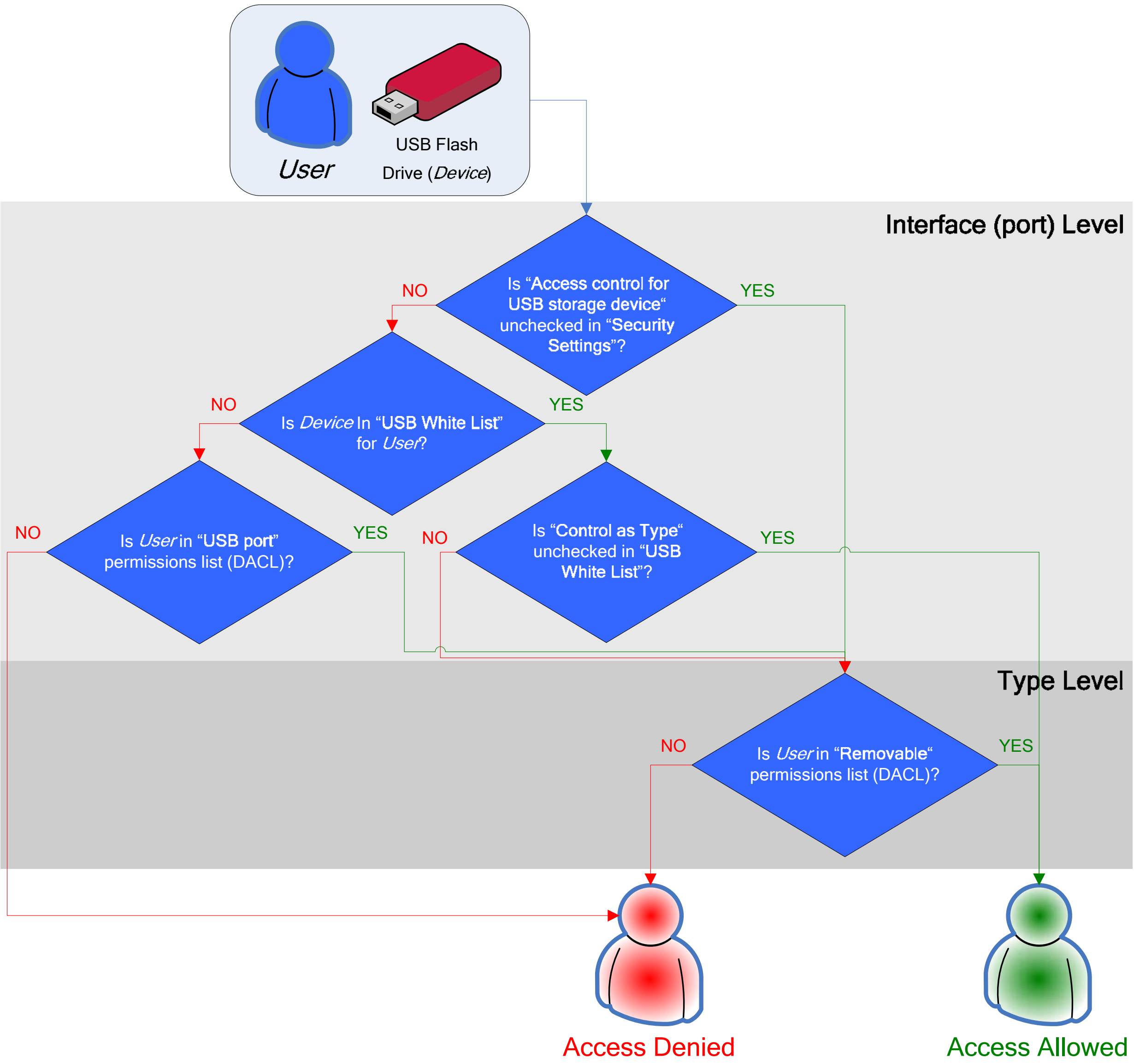


DeviceLock management consoles
Network
DeviceLock Administrator
DeviceLock Management Console (MMC snap-in)
DeviceLock Enterprise Manager
DeviceLock Group Policy Manager
(Windows GPO Editor)
Policy
Remote Procedure Call (RPC)
Active Directory Domain Controller
DeviceLock Service
DeviceLock Service
DeviceLock Service
DeviceLock Service

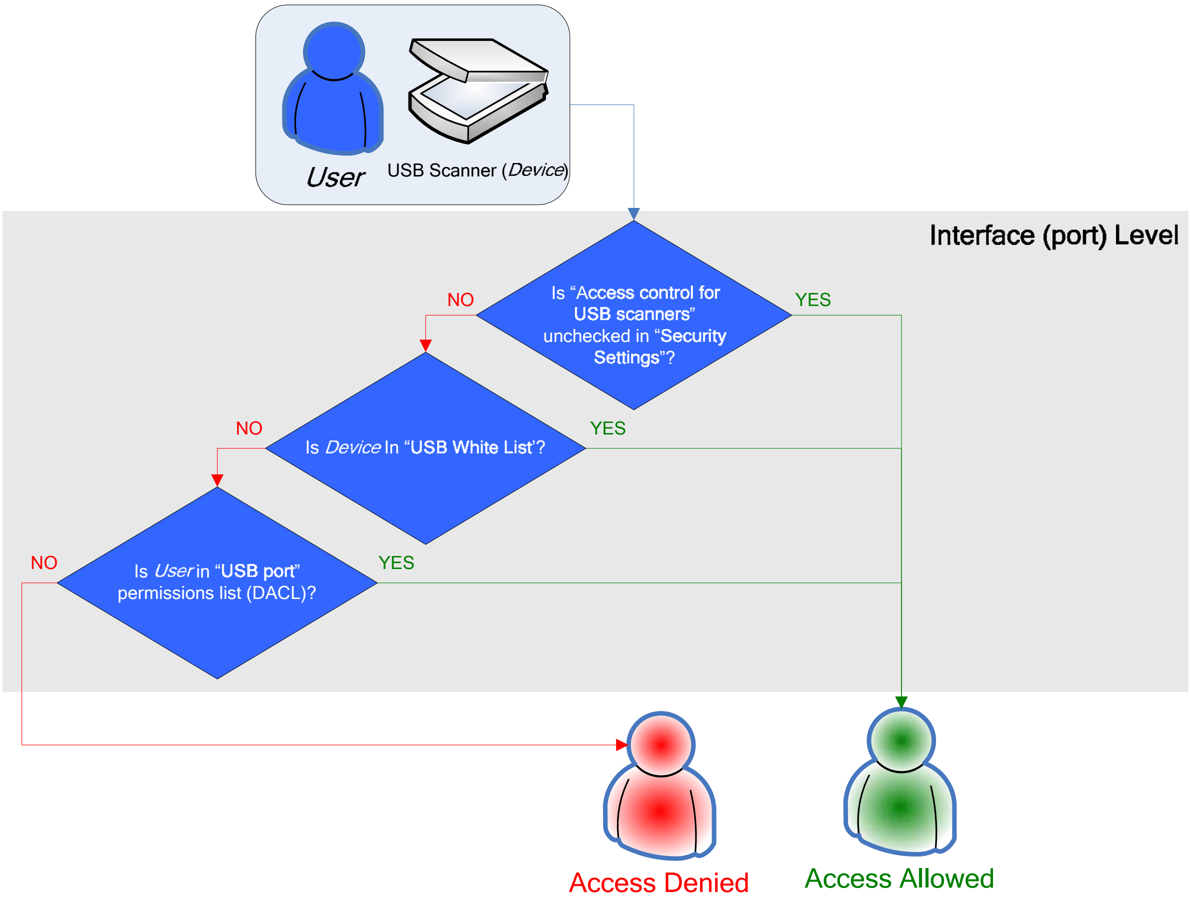
## 1.2 Managed Access Control

Every time the user wants to access a device, DeviceLock intercepts this request at the kernel level of the OS. Depending on the device's type and the connection interface (e.g. USB), DeviceLock checks the user rights in the appropriate Access Control List (ACL). If the user does not have the right to access this device, an "access denied" error is returned.

Access checking can occur at two levels: the interface (port) level and the type level. Some devices are checked at both levels, while others only at one level – either interface (port) or type.


User
USB Flash Drive (Device)
Interface (port) Level
Is "Access control for USB storage device" unchecked in "Security Settings"?
NO
YES
Is Device In "USB White List" for User?
NO
YES
Is User in "USB port" permissions list (DACL)?
NO
YES
Is "Control as Type" unchecked in "USB White List"?
NO
YES
Type Level
Is User in "Removable" permissions list (DACL)?
NO
YES
Access Denied
Access Allowed

Consider the case of a user connecting a USB flash drive to the USB port. Here DeviceLock would first check whether the USB port is open or locked at the interface level. Next, because Windows recognizes a USB flash drive as a removable storage device, DeviceLock will also check permissions at the type level (Removable). In contrast, a USB scanner would only be checked at the interface level (USB port), as DeviceLock doesn't distinguish scanners at the type level.


User
USB Scanner (Device)
Interface (port) Level
Is “Access control for USB scanners” unchecked in “Security Settings”?
NO
YES
Is Device In “USB White List”?
NO
YES
Is User in “USB port” permissions list (DACL)?
NO
YES
Access Denied
Access Allowed

There are additional Security Settings that can turn off access control for classes of devices (e.g. all USB printers) while others remain under control. In the case of a device belonging to a class for which control is disabled, DeviceLock allows all requests to connect this device at the interface (port) level.

Also, DeviceLock supports the white listing of specific devices; in other words, you can turn off access control for only specific devices (e.g. certain USB printer).

***NOTE: If access to a device is denied at the interface (port) level, DeviceLock does not check permissions at the type level. However, if access is granted at the interface (port) level, DeviceLock also checks permissions at the type level. Only when access is granted at both levels, can the user connect the device.***

## 1.3 Recommended Basic Security Measures

Following is a series of basic security rules that should be met for computers that you want to install in a corporate network:

a. **Change the boot sequence.** The hard disk must be the first boot device. Change the boot sequence in the BIOS so that the computer does not boot from the floppy, USB drive or CD-ROM. If the hard disk is not the first boot device, someone can use a bootable CD or USB Flash Drive to directly access the hard disk drive.

b. **Protect the BIOS with a password.** The password should be set to the BIOS so only an authorized person can make changes there. If the BIOS is not password protected, someone can change the boot sequence and use a bootable CD, floppy or USB Flash Drive (*see above*).

c. **Seal computer cases and chassis.** Protect the hardware with a seal. Otherwise, it is possible to plug an external boot device directly to the computer and access the hard disk.

   Moreover, if someone can physically access the motherboard, it is very easy to locate the CMOS reset jumper and clear the BIOS password (*see above*).

d. **Do not give Administrative rights to regular users.** Regular local users should not be members of the local *Administrators* group. It is not a good practice to grant users administrative rights to their computers.

   However, if for some reason users in your network have administrator privileges on their local computers, DeviceLock does provide another level of protection. No one except authorized DeviceLock administrators can connect to, stop, or uninstall DeviceLock Service. Even members of the local *Administrators* group can't disable DeviceLock if they are not in the list of authorized DeviceLock administrators.

e. **Remove the Recovery Console.** If the Windows Recovery Console is installed on the local computer, someone can boot to the recovery mode and workaround any number of security measures including disabling DeviceLock Service (however, this requires the local administrator password).

   For this reason we recommend deleting the Recovery Console. For more information on how to install, remove and use the Recovery Console, please refer to the Microsoft's on-line article: http://support.microsoft.com/default.aspx?scid=kb;en-us;307654.

# 2 Installation

## 2.1 Requirements

DeviceLock works on any computer using Windows NT 4.0 SP6/2000/XP and Windows Server 2003.

To install and use DeviceLock, you MUST have administrative privileges. If you are going to use DeviceLock only on a local computer, you must have local administrative privileges. If you are going to use DeviceLock throughout your network, you must have domain administrator privileges.

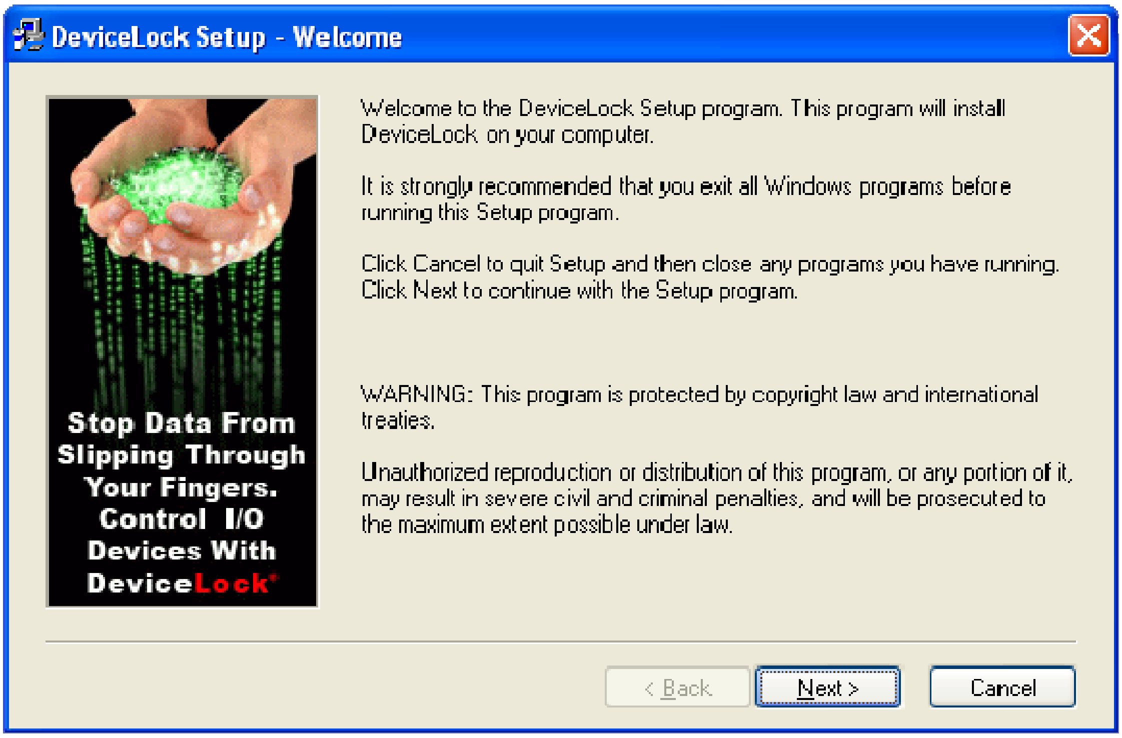
If you want to use DeviceLock on your network, you must have a functioning TCP/IP network protocol. However, DeviceLock can also work on stand-alone computers. A network is needed only if you want to control DeviceLock Service from a remote computer.

## 2.2 Deploying DeviceLock Service

DeviceLock Service should be installed on the computer so you can control the access to devices on that computer. There are multiple ways to deploy DeviceLock Service to client systems.

### 2.2.1 Interactive Installation

Run Setup (*setup.exe*) and follow the instructions that appear on the screen.


DeviceLock Setup - Welcome
Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock®
< Back
Next >
Cancel

Welcome to the DeviceLock Setup program. This program will install DeviceLock on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

You should run *setup.exe* on each computer that is to be controlled with DeviceLock Service.

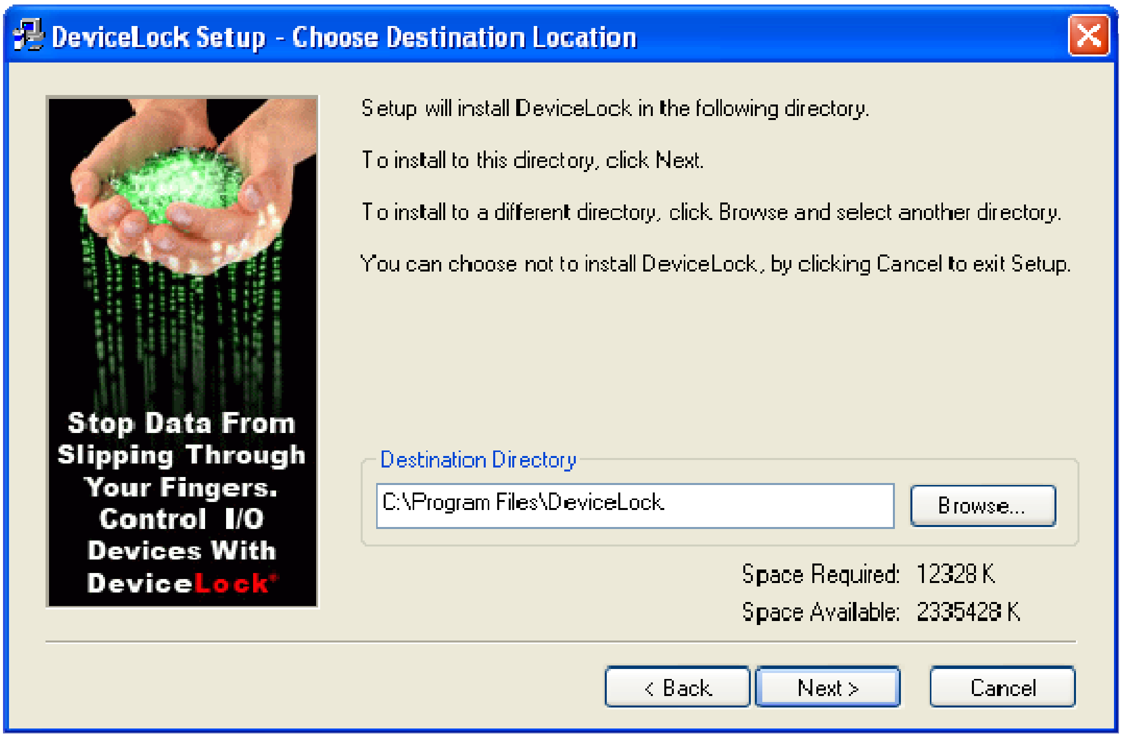
If you are upgrading a previous version, make sure that you have administrative access to DeviceLock Service, otherwise you will not be able to continue installation.

You must accept DeviceLock's End User License Agreement to continue the installation process.

DeviceLock installs to the directory of your choice. Setup tries to find a DeviceLock installation and if one exists, Setup suggests that you install DeviceLock to the same directory.

If a previous installation does not exist, Setup suggests that DeviceLock be installed to the Program Files directory on the system drive (e.g. *C:\Program Files\DeviceLock*).

In any case, you can select another directory for installation.



DeviceLock Setup - Choose Destination Location

Setup will install DeviceLock in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install DeviceLock, by clicking Cancel to exit Setup.

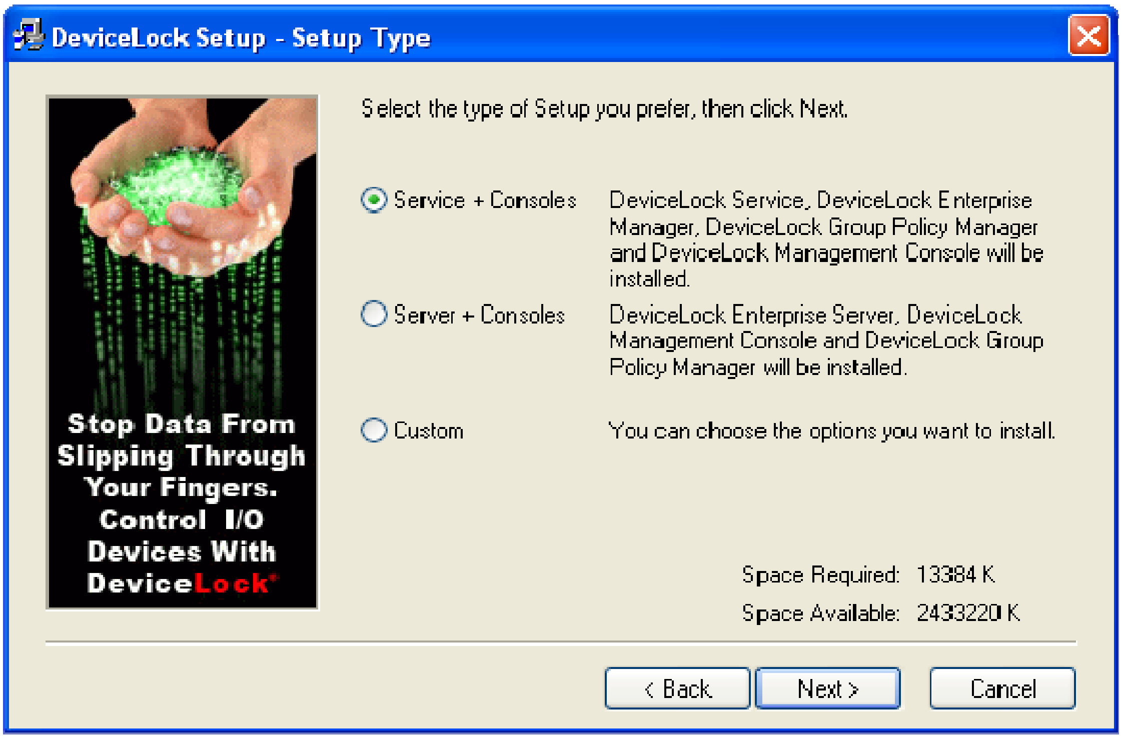
Destination Directory: C:\Program Files\DeviceLock

Space Required: 12328 K

Space Available: 2335428 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock
Browse...
< Back
Next >
Cancel

You have the following two choices: either install both DeviceLock Service and DeviceLock management consoles using the *Service + Consoles* option or install only DeviceLock Service using the *Custom* option and select the *DeviceLock Service* component.



DeviceLock Setup - Setup Type

Select the type of Setup you prefer, then click Next.

● Service + Consoles — DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.

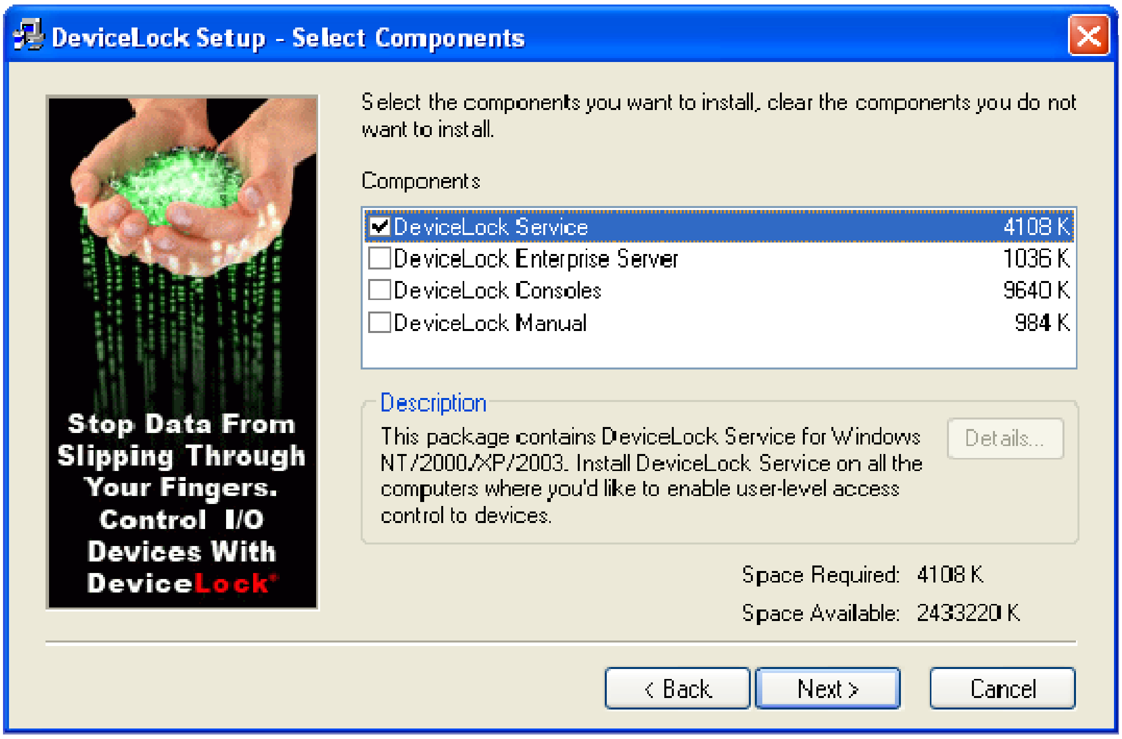
○ Server + Consoles — DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.

○ Custom — You can choose the options you want to install.

Space Required: 13384 K

Space Available: 2433220 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock®
< Back
Next >
Cancel



DeviceLock Setup - Select Components

Select the components you want to install, clear the components you do not want to install.

Components

| | |
|---|---|
| ☑ DeviceLock Service | 4108 K |
| □ DeviceLock Enterprise Server | 1036 K |
| □ DeviceLock Consoles | 9640 K |
| □ DeviceLock Manual | 984 K |

Description

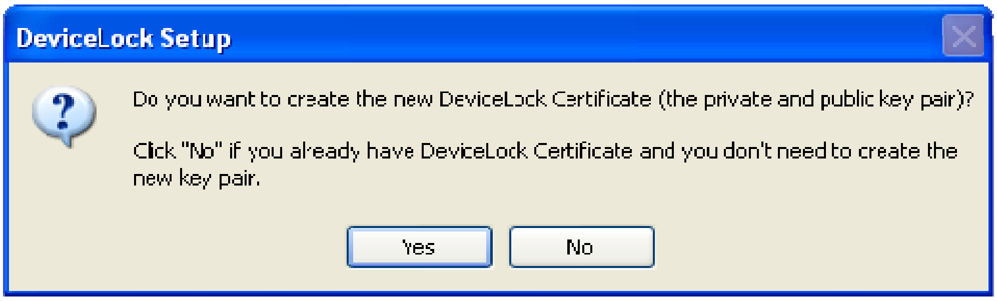
This package contains DeviceLock Service for Windows NT/2000/XP/2003. Install DeviceLock Service on all the computers where you'd like to enable user-level access control to devices.

Space Required: 4108 K

Space Available: 2433220 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock®
Details...
< Back
Next >
Cancel

If you choose to install DeviceLock management consoles as well, Setup may suggest that you generate a new DeviceLock Certificate.



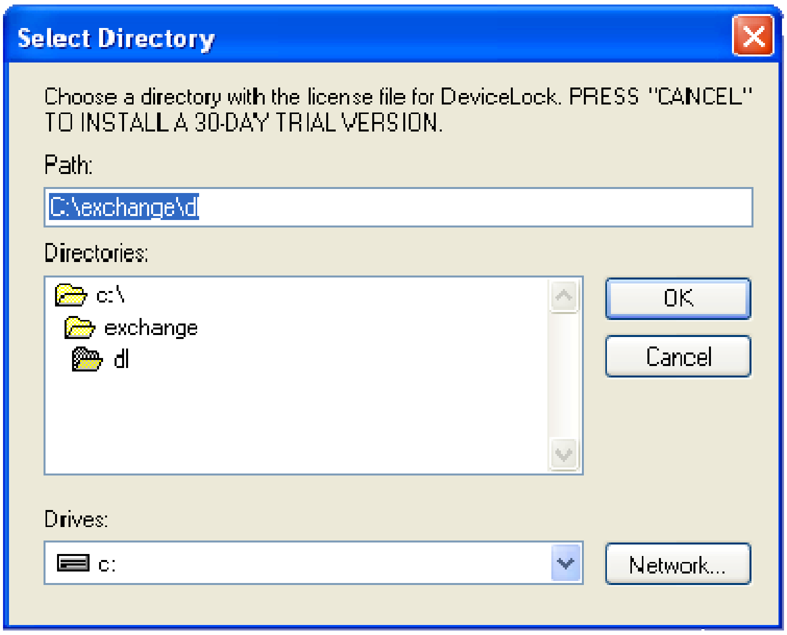
DeviceLock Setup

Do you want to create the new DeviceLock Certificate (the private and public key pair)?

Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.

You can always generate a new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just press the *No* button and continue the installation.

Also, if you select *Service* + *Consoles*, Setup may suggest that you load the license file to register your copy of DeviceLock management consoles. If you don't have the license file, press the *Cancel* button to install DeviceLock in a 30-day trial mode.



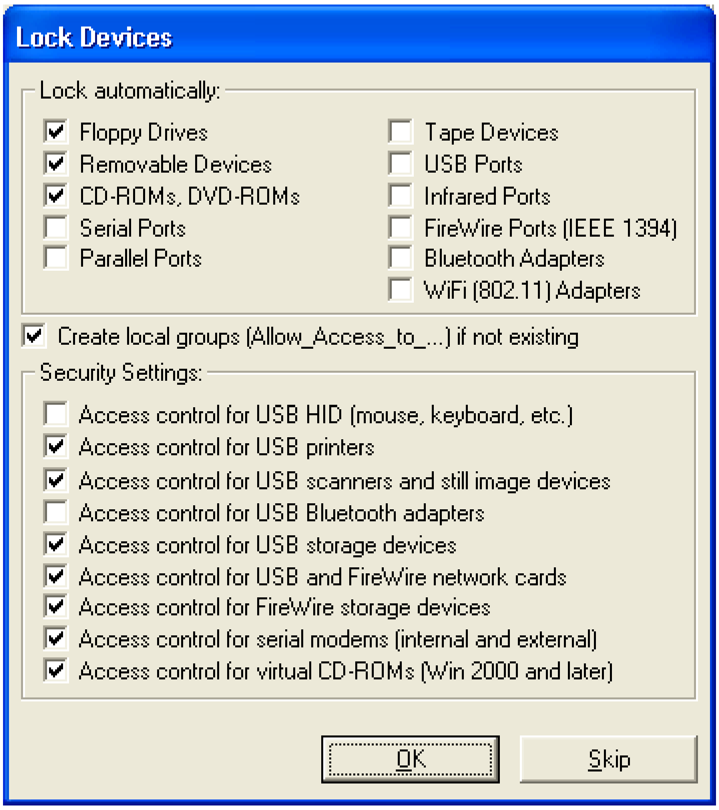
Choose a directory with the license file for DeviceLock. PRESS "CANCEL" TO INSTALL A 30-DAY TRIAL VERSION.

Path: C:\exchange\dl

Directories: c:\ exchange dl

Drives: c:

During the installation process, you can set special permissions for local devices.



Lock automatically:

- ☑ Floppy Drives
- ☑ Removable Devices
- ☑ CD-ROMs, DVD-ROMs
- □ Serial Ports
- □ Parallel Ports
- □ Tape Devices
- □ USB Ports
- □ Infrared Ports
- □ FireWire Ports (IEEE 1394)
- □ Bluetooth Adapters
- □ WiFi (802.11) Adapters

☑ Create local groups (Allow_Access_to_...) if not existing

Security Settings:

- □ Access control for USB HID (mouse, keyboard, etc.)
- ☑ Access control for USB printers
- ☑ Access control for USB scanners and still image devices
- □ Access control for USB Bluetooth adapters
- ☑ Access control for USB storage devices
- ☑ Access control for USB and FireWire network cards
- ☑ Access control for FireWire storage devices
- ☑ Access control for serial modems (internal and external)
- ☑ Access control for virtual CD-ROMs (Win 2000 and later)

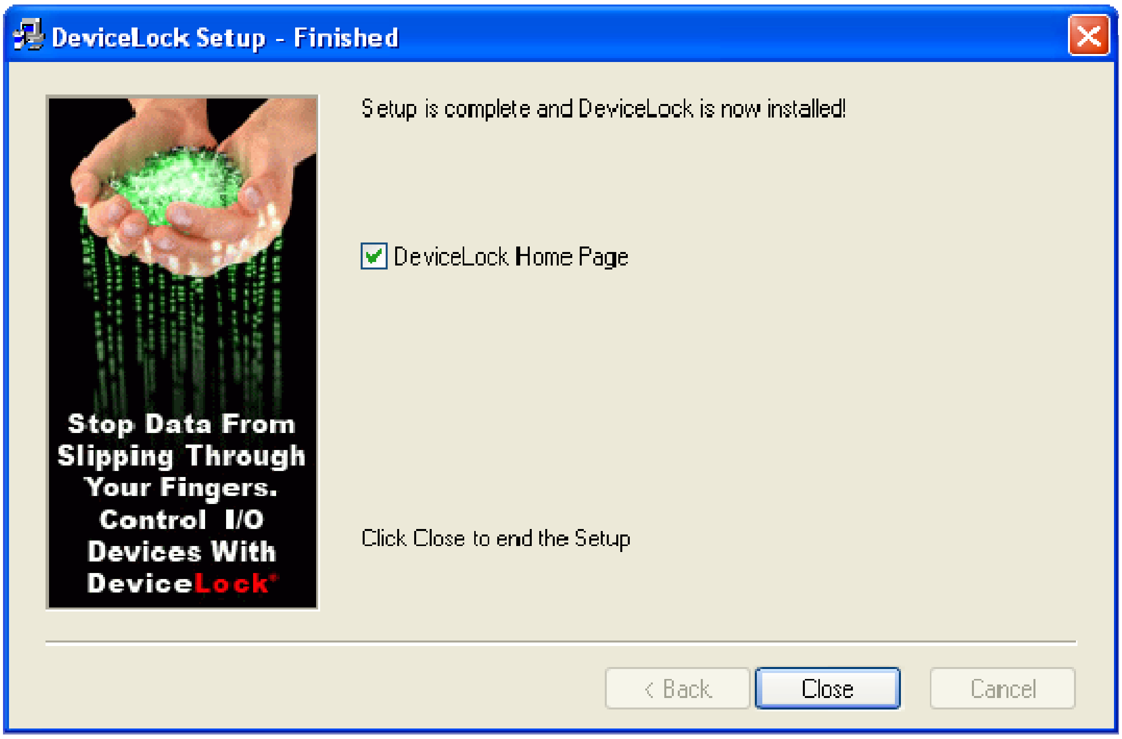
Check devices you would like to set permissions to. Check the *Create local groups if not existing* flag to instruct Setup to create the special local user group *Allow_Access_To_* for each device type (e.g. *Allow_Access_To_Floppy* for floppy drives), if these do not exist on the local computer.

Setup assigns **Read**, **Write**, **Format** and **Eject** generic rights to members of the *Administrators* group and the *SYSTEM* account. Members of the *Allow_Access_To_* group will have **Read**, **Write** and **Eject** generic rights.

Also, you can define Security Settings to exclude certain types of devices from the access check. Check *Access control for USB HID*, *Access control for USB printers*, *Access control for USB scanners and still image devices*, *Access control for USB Bluetooth adapters*, *Access control for USB storage devices* or *Access control for FireWire storage devices* to allow DeviceLock Service to control security for Human Interface Devices (mouse, keyboard, etc.), printers, scanners and still image devices, Bluetooth adapters or storage devices (such as flash drives) plugged into the USB and FireWire port. To allow access control for USB and FireWire network cards, check *Access control for USB and FireWire network cards*. Otherwise, even if ports (USB and/or FireWire) are locked, these devices continue to function as usual. To allow access control for serial modems *(*internal and/or external*)*, check *Access control for serial modems*. To disable locking of virtual (software emulated) CD-ROMs on Windows 2000 and later systems, uncheck *Access control for virtual CD-ROMs*.

Press the *OK* button to apply changes. Press the *Skip* button if you prefer to wait until after installation to set permissions to these devices using DeviceLock management consoles.

As soon as Setup has installed DeviceLock, it suggests that you point your default Internet browser to the DeviceLock website.


DeviceLock Setup - Finished
Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock
< Back
Close
Cancel

Setup is complete and DeviceLock is now installed!

☑ DeviceLock Home Page

Click Close to end the Setup

Uncheck the *DeviceLock Home Page* flag if you do not want to visit the DeviceLock website.

Press the *Close* button to finish the installation.

### 2.2.2 Unattended Installation

DeviceLock also supports unattended (silent) setups. This provides an installation method that can be used from within a batch file. To install DeviceLock Service without user intervention, run Setup with the */s* parameter (e.g. *c:\setup.exe /s*). There is a special configuration file for silent setups named *devicelock.ini*. The d*evicelock.ini* file must be in the same directory as *setup.exe*. With this file, you can customize the installation parameters.

You can open and edit *devicelock.ini* in any text editor, for example in Notepad. Remove a semicolon (;) before the parameter to assign a new value or leave it to assign the default value.

There are two sections (*[Install]* and *[Misc]*) in this configuration file and each section has its own parameters:

1. *[Install]*

To install DeviceLock Service, specify the *Service* parameter:

*Service = 1*

You can also install DeviceLock management consoles and the documentation, using *Manager* and *Documents* parameters.

If you want to just upgrade DeviceLock Service and do not want to change existing settings, use the *OnlyUpgradeService* parameter:

*OnlyUpgradeService = 1*

In this case Setup ignores all specified settings and only copies the new DeviceLock Service executable file (*dlservice.exe* or *dlservice_x64.exe*) over the existing one.

You can also define a destination directory for DeviceLock:

InstallDir = C:\Program Files\DeviceLock

Setup uses this directory if it can't find the previous installation of DeviceLock.

If you have purchased a license for DeviceLock, you can also specify the location of the license file:

*RegFileDir = C:\Directory*

where *C:\Directory* is where your license file is located.

You do not need to load the license, if you are installing only DeviceLock Service. It is required for DeviceLock management consoles.

To instruct DeviceLock Service to use a fixed port, specify the *FixedPort* parameter:

*FixedPort* = [*port number*]

where *port number* – the fixed TCP port number that you want to use for the communication between DeviceLock Service and management consoles. To use dynamic ports for the RPC communication, specify 0 as a port number.

If the *CreateGroups* parameter is set to “1”, Setup creates the special local user group *Allow_Access_To_* for each device type (e.g. *Allow_Access_To_Floppy* for floppy drives), if these do not exist on the local computer.

To apply settings, permissions, audit and shadowing rules to DeviceLock Service, specify the path to the previously saved XML file in the *SettingsFile* parameter:

*SettingsFile = C:\settings.dls*

This settings file can be created using DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor.

*2. [Misc]*

If you want to run a program (e.g. batch file) after a successful install, you can specify the *Run* parameter:

*Run = C:\mybatchfile.bat*

To suppress an automatic restart even if Setup needs it, set the *DisableRestart* parameter to “1”.

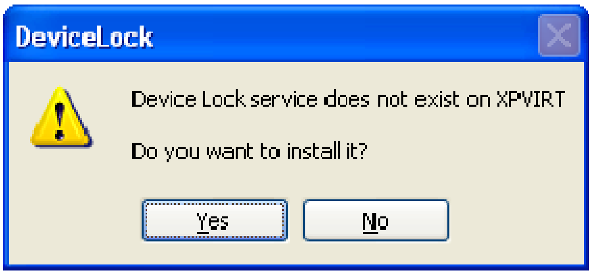
### 2.2.3 Installation via Microsoft Systems Management Server

The unattended installation allows you to deploy DeviceLock Service using Microsoft Systems Management Server (SMS). Use the package definition files (*DevLock.pdf* for SMS version 1.x and *DevLock.sms* for SMS version 2.0 and later) supplied with DeviceLock, located in the *sms.zip* file.

### 2.2.4 Remote Installation via DeviceLock Management Console

DeviceLock Management Console (the MMC snap-in) supports remote installation to help system administrators set up a service on remote machines without ever having to physically go to them.

When you’re trying to connect to a computer where DeviceLock Service is not installed or is outdated, the management console suggests that you install or update it.

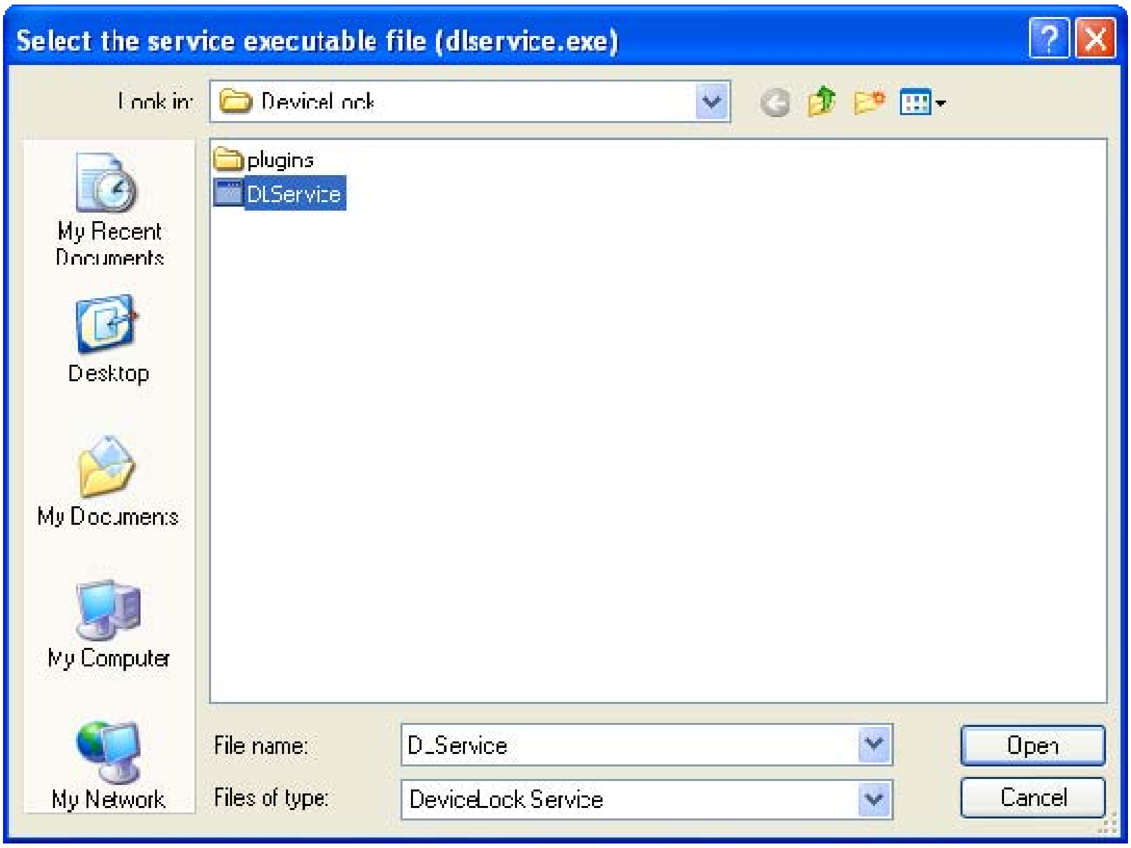


DeviceLock

Device Lock service does not exist on XPVIRT

Do you want to install it?

Select the DeviceLock Service executable file (*dlservice.exe* or *dlservice_x64.exe*) and the management console will copy it to the remote computer.



Select the service executable file (dlservice.exe)

Look in: DeviceLock

plugins

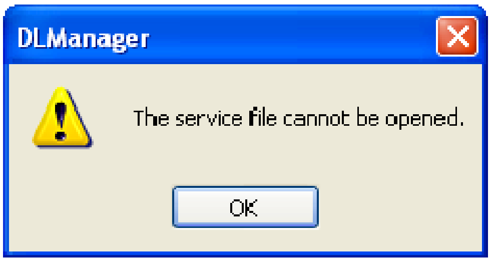
DLService

File name: DLService

Files of type: DeviceLock Service

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

Please note that if DeviceLock Service is running on the same computer as your management console and DeviceLock Security is enabled (the *Enable Default Security* flag is unchecked in DeviceLock Administrators) to protect the service against users with local administrative privileges, neither the management console nor any other application will be able to access the service's executable file (*dlservice.exe* or *dlservice_x64.exe*).

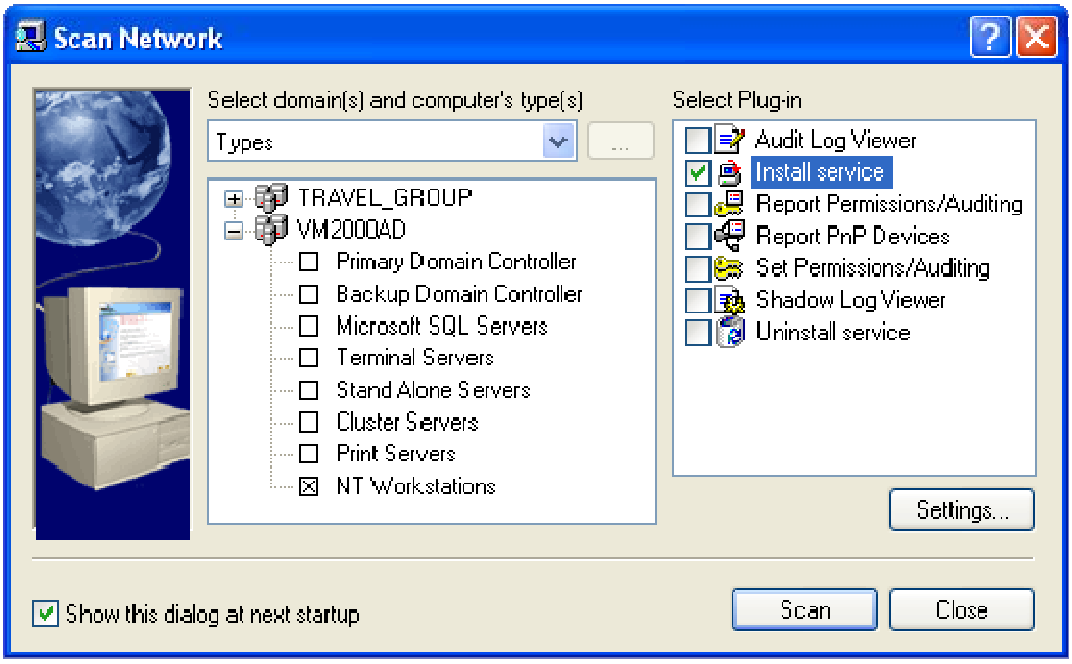


The service file cannot be opened.

To prepare for this scenario, you can copy the service's executable files (*dlservice.exe* and *dlservice_x64.exe*) to another directory before turning on DeviceLock Security and use the copy for remote deployment.

### 2.2.5 Remote Installation via DeviceLock Enterprise Manager

DeviceLock Enterprise Manager contains the *Install service* plug-in that allows you to deploy DeviceLock Service automatically on all the selected computers in your network.



Select domain(s) and computer's type(s)

Types

- TRAVEL_GROUP
- VM2000AD
  - □ Primary Domain Controller
  - □ Backup Domain Controller
  - □ Microsoft SQL Servers
  - □ Terminal Servers
  - □ Stand Alone Servers
  - □ Cluster Servers
  - □ Print Servers
  - ☒ NT Workstations

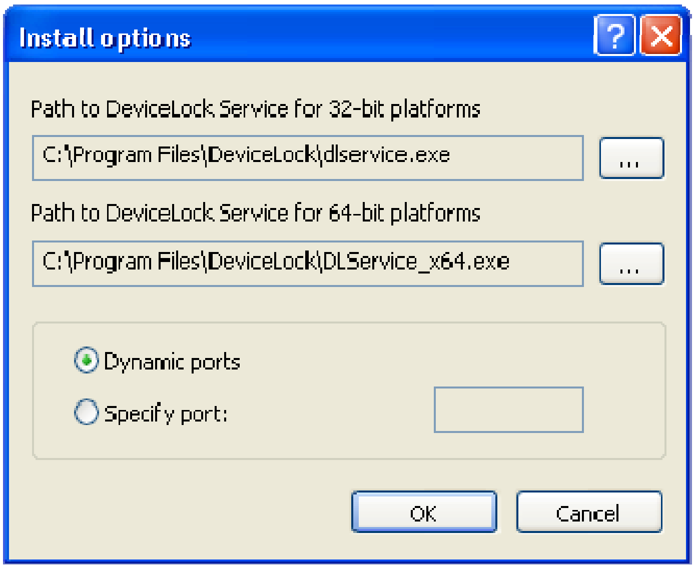
Select Plug-in

- □ Audit Log Viewer
- ☑ Install service
- □ Report Permissions/Auditing
- □ Report PnP Devices
- □ Set Permissions/Auditing
- □ Shadow Log Viewer
- □ Uninstall service

☑ Show this dialog at next startup

First, select computers where DeviceLock Service must be installed. DeviceLock Enterprise Manager allows you to select computers by their types and names. You can also load the computers list from an external file or select them from any LDAP tree (Active Directory, Novell eDirectory, OpenLDAP and so on).

Then, select the *Install service* plug-in and press the *Settings* button to locate the service executable files (*dlservice.exe* and *dlservice_x64.exe*). You can also instruct DeviceLock Service to use the fixed TCP port for the communication with management consoles. To use dynamic ports for the RPC communication, select the *Dynamic ports* option.



Install options

Path to DeviceLock Service for 32-bit platforms

C:\Program Files\DeviceLock\dlservice.exe

Path to DeviceLock Service for 64-bit platforms

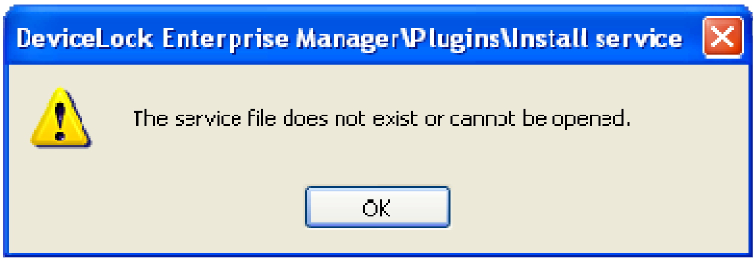
C:\Program Files\DeviceLock\DLService_x64.exe

● Dynamic ports

○ Specify port:

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

Please note that if DeviceLock Service is running on the same computer as DeviceLock Enterprise Manager and DeviceLock Security is enabled to protect the service against users with local administrative privileges, neither DeviceLock Enterprise Manager nor any other application will be able to access the service's executable file (*dlservice.exe* or *dlservice_x64.exe*).



DeviceLock Enterprise Manager\Plugins\Install service

The service file does not exist or cannot be opened.

To prepare for this scenario, you can copy the service's executable files (*dlservice.exe* and *dlservice_x64.exe*) to another directory before turning on DeviceLock Security and use the copy for the *Install service* plug-in.

### 2.2.6 Installation via Group Policy

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* and *DeviceLock Service x64.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* and/or *DeviceLock Service x64.msi*) to the distribution point.

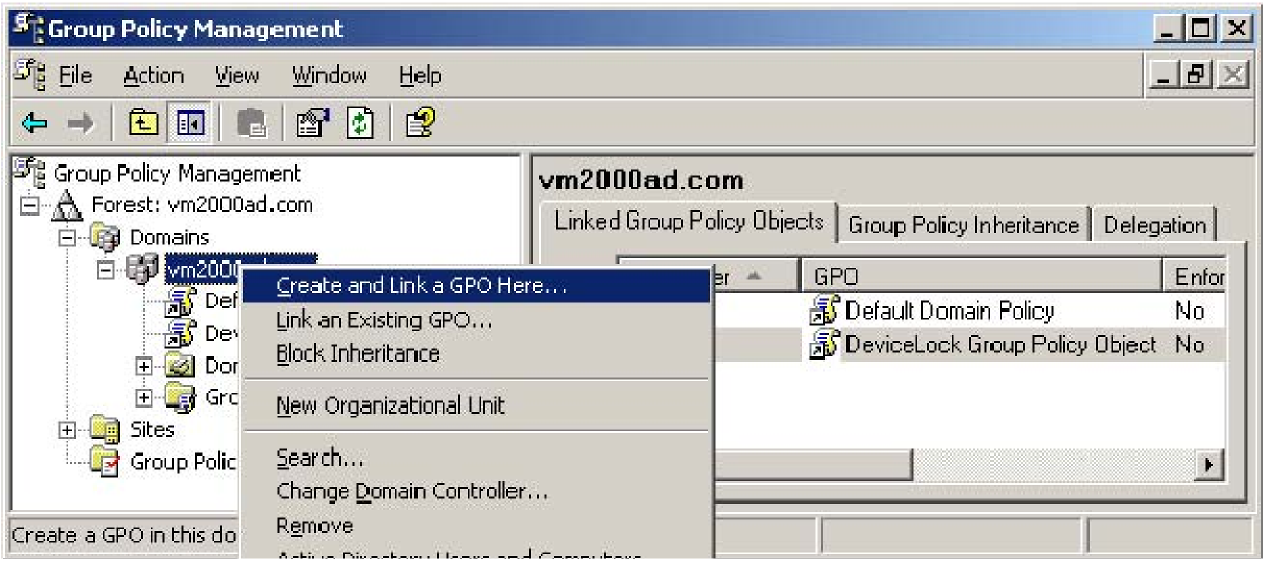
- Create a Group Policy Object

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

  1. Start the *Group Policy Management* snap-in.

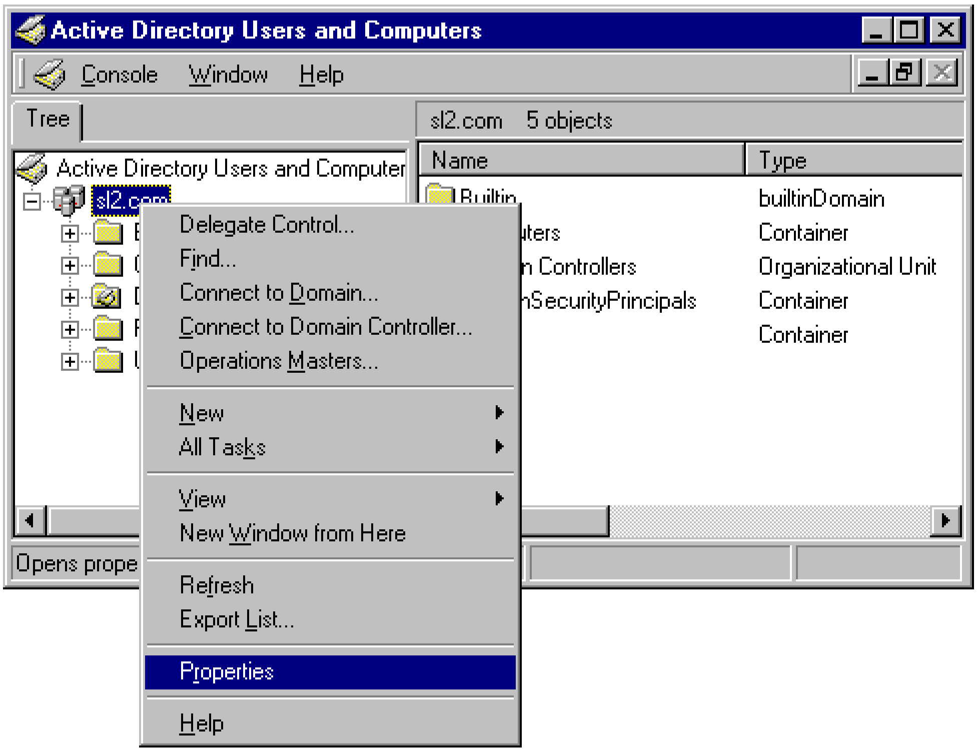
     If the *Group Policy Management* snap-in is not installed on your computer, you may use the *Active Directory Users and Computers* snap-in instead.

  2. In the console tree, select your domain.

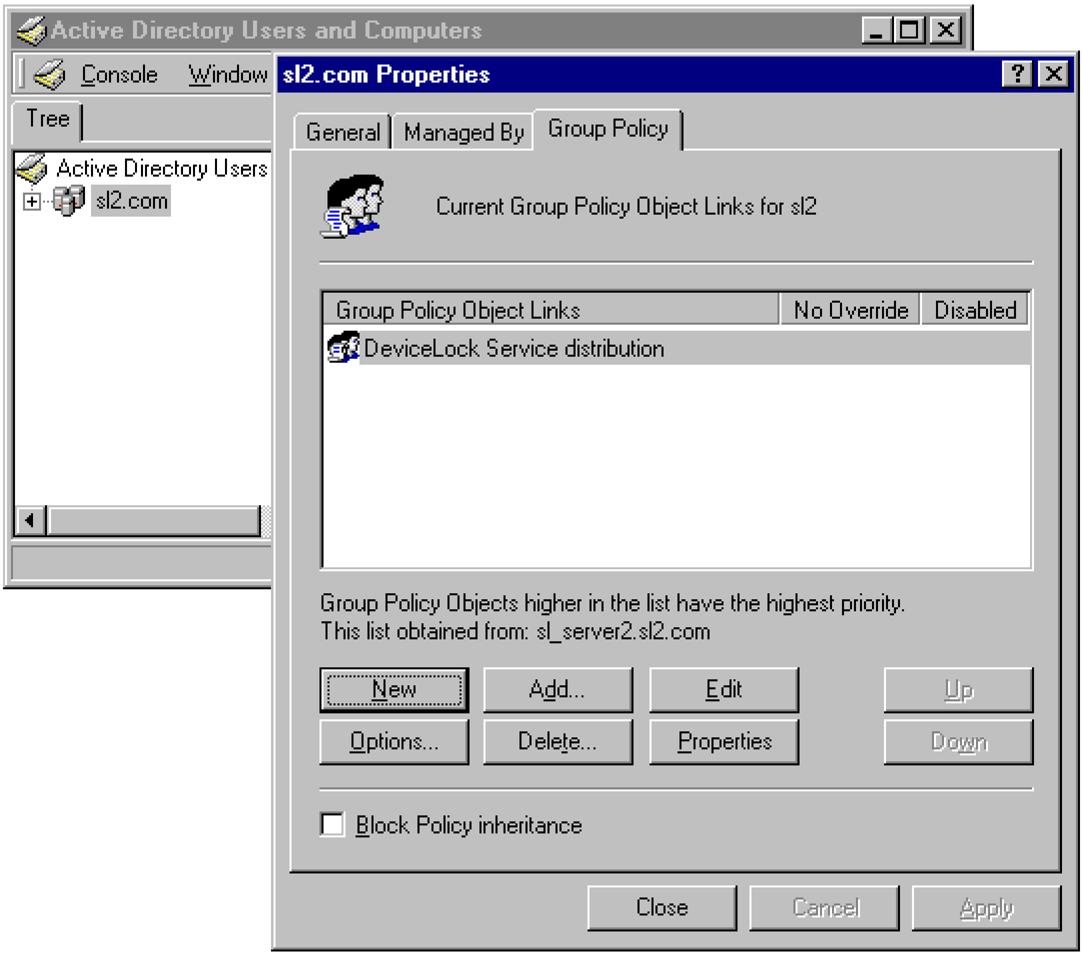


  3. Click *Create and Link a GPO Here* from the context menu of the domain item.

     If you are using the *Active Directory Users and Computers* snap-in, right-click your domain, then click *Properties*, click the *Group Policy* tab, and then click *New*.



| Name | Type |
|---|---|
| Builtin | builtinDomain |
| ...ters | Container |
| ...n Controllers | Organizational Unit |
| ...nSecurityPrincipals | Container |
| | Container |



Current Group Policy Object Links for sl2

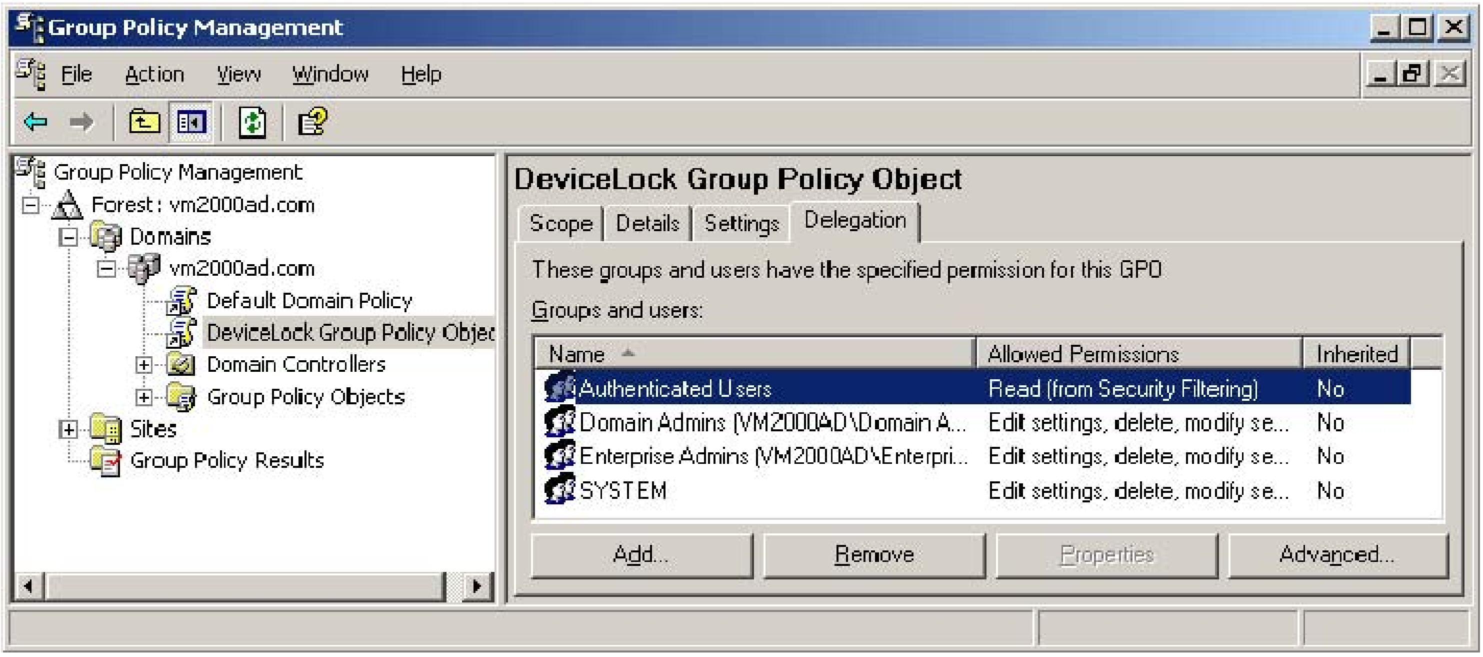
| Group Policy Object Links | No Override | Disabled |
|---|---|---|
| DeviceLock Service distribution | | |

Group Policy Objects higher in the list have the highest priority.
This list obtained from: sl_server2.sl2.com

□ Block Policy inheritance

4. Type the name that you want to call this policy, and then press *ENTER*.

5. In the console tree, select your group policy object, click the *Delegation* tab, and then click *Advanced*.



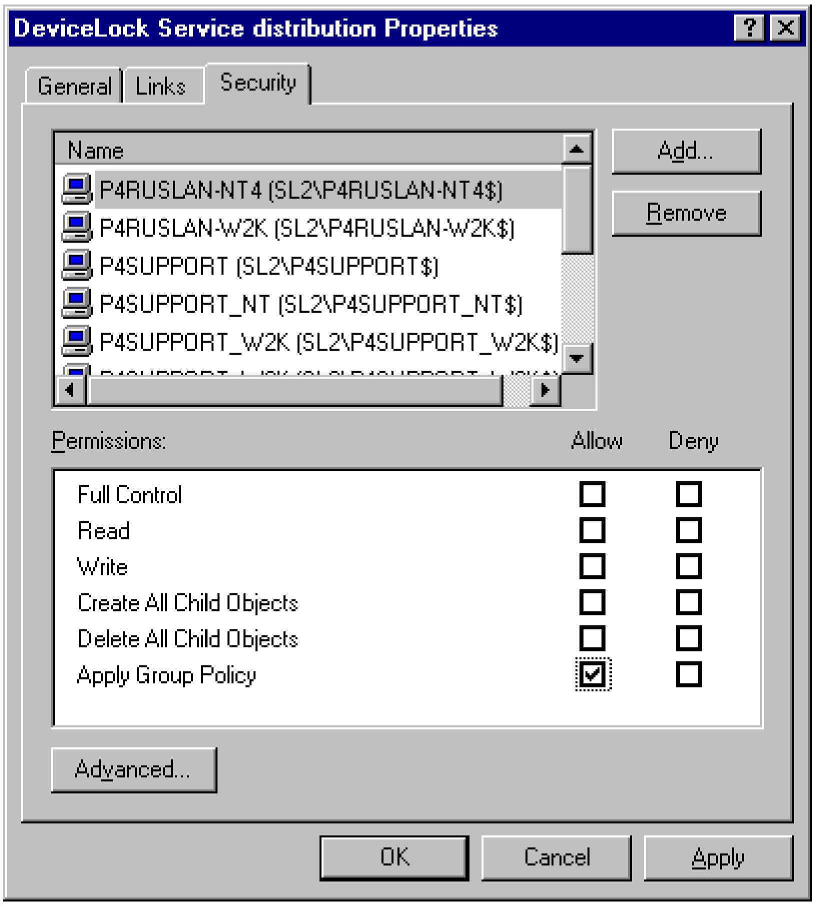
DeviceLock Group Policy Object

These groups and users have the specified permission for this GPO

Groups and users:

| Name | Allowed Permissions | Inherited |
|---|---|---|
| Authenticated Users | Read (from Security Filtering) | No |
| Domain Admins (VM2000AD\Domain A... | Edit settings, delete, modify se... | No |
| Enterprise Admins (VM2000AD\Enterpri... | Edit settings, delete, modify se... | No |
| SYSTEM | Edit settings, delete, modify se... | No |

If you are using the *Active Directory Users and Computers* snap-in, click *Properties* on the *Group Policy* tab, and then click the *Security* tab.



Name
- P4RUSLAN-NT4 (SL2\P4RUSLAN-NT4$)
- P4RUSLAN-W2K (SL2\P4RUSLAN-W2K$)
- P4SUPPORT (SL2\P4SUPPORT$)
- P4SUPPORT_NT (SL2\P4SUPPORT_NT$)
- P4SUPPORT_W2K (SL2\P4SUPPORT_W2K$)

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | □ | □ |
| Write | □ | □ |
| Create All Child Objects | □ | □ |
| Delete All Child Objects | □ | □ |
| Apply Group Policy | ☑ | □ |

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*.

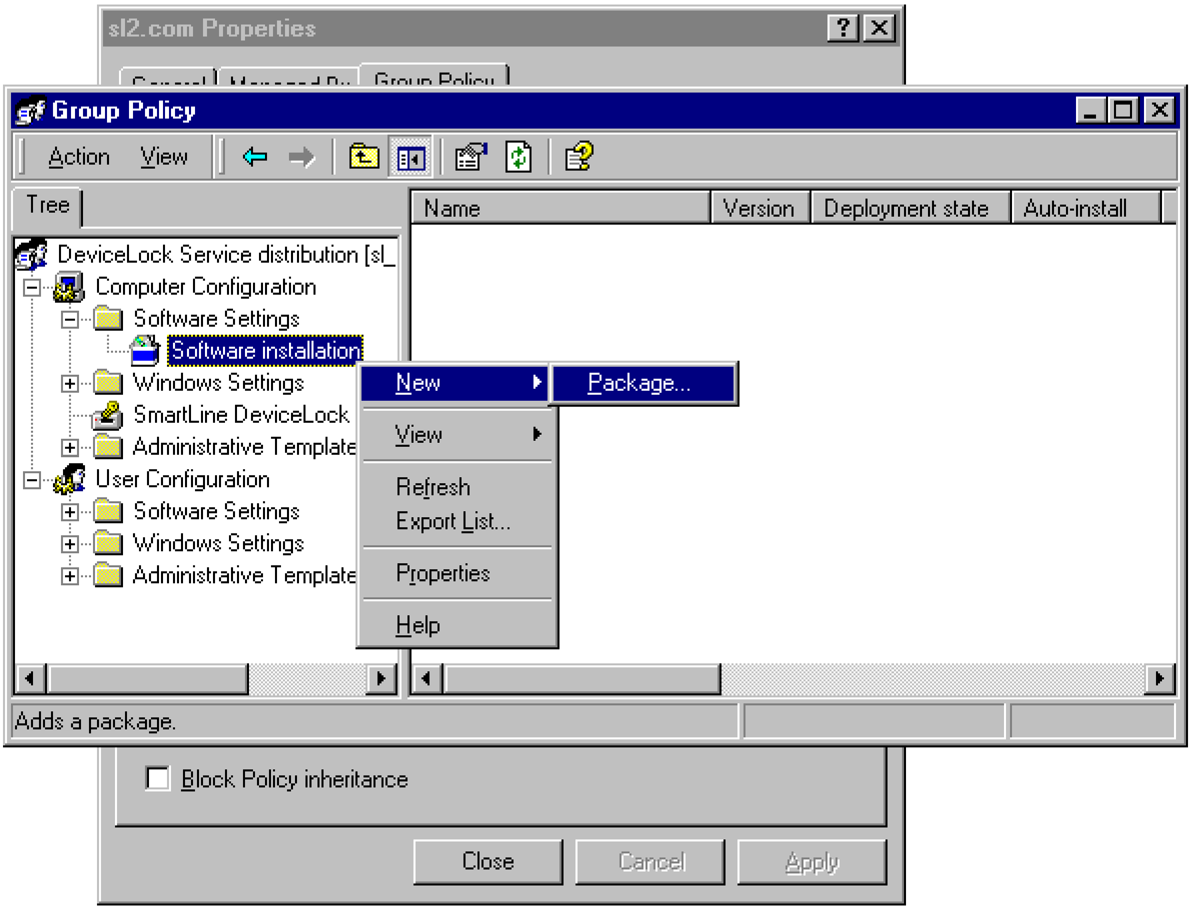
- Assign a Package

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

  1. Open the group policy object that you need in the Windows Group Policy Object editor (use either the *Group Policy Management* or *Active Directory Users and Computers* snap-in).

  2. Under *Computer Configuration*, expand *Software Settings*.

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



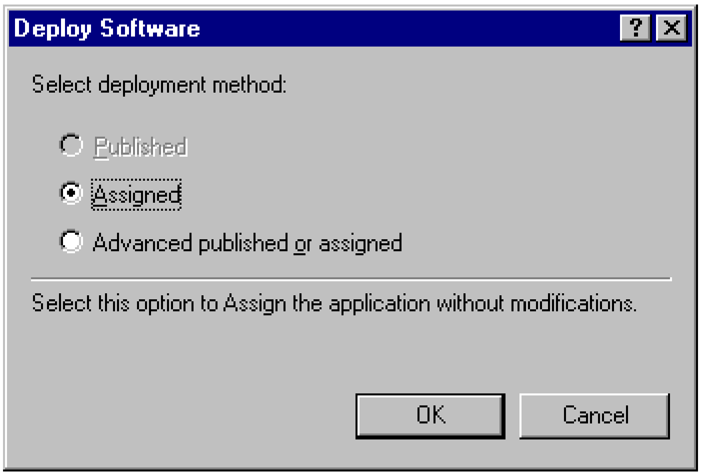
Adds a package.

  4. 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.***

  5. Click *Open*.

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

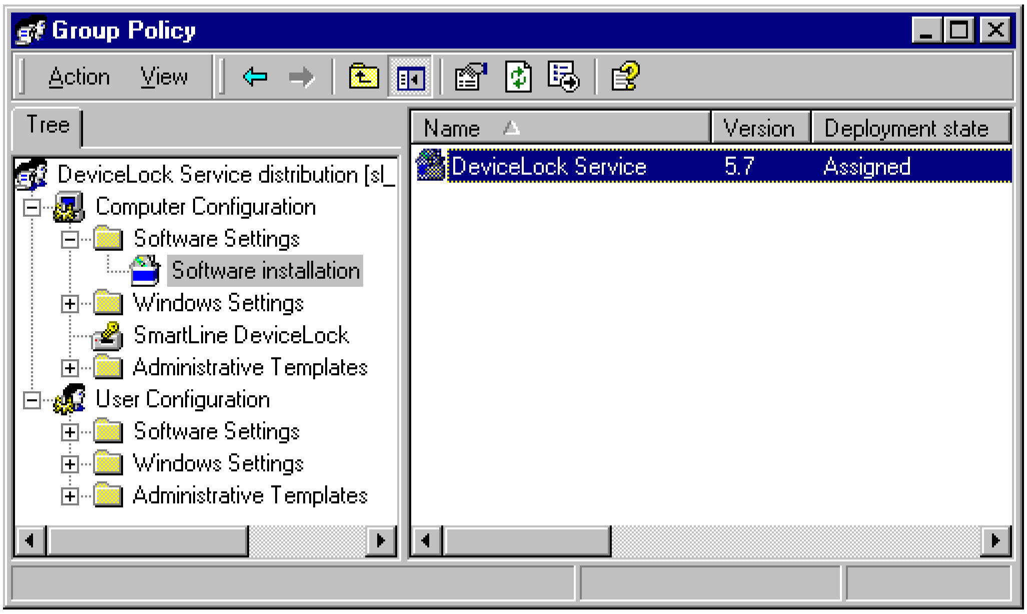


Select deployment method:

○ Published
● Assigned
○ Advanced published or assigned

Select this option to Assign the application without modifications.

7. Close the Windows Group Policy Object editor. When the client computer starts, DeviceLock Service is automatically installed.



| Name | Version | Deployment state |
|---|---|---|
| DeviceLock Service | 5.7 | Assigned |

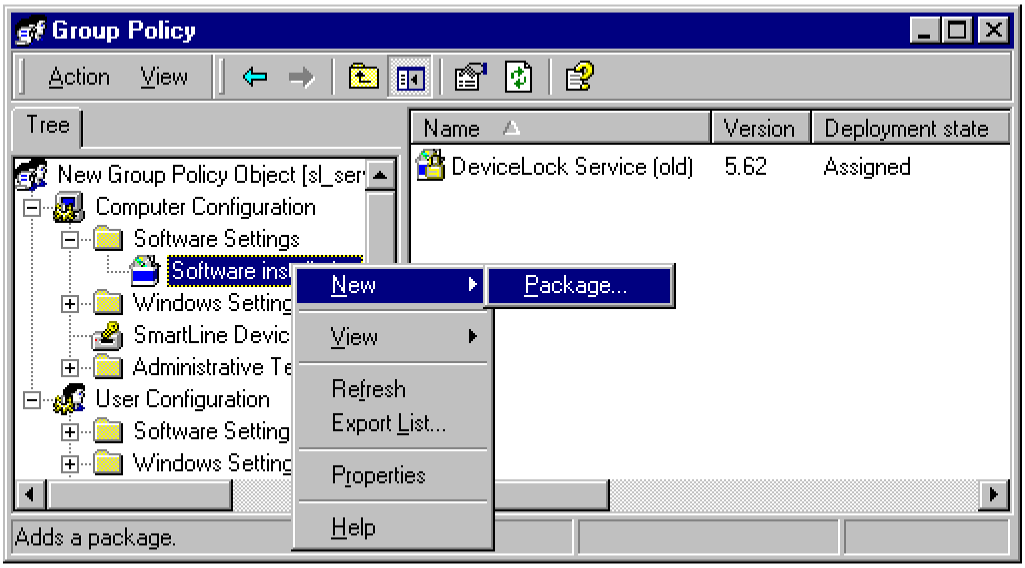
- Upgrade a Package

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

1. Open the group policy object that contains the old DeviceLock Service package in the Windows Group Policy Object editor (use either the *Group Policy Management* or *Active Directory Users and Computers* snap-in).

2. Under *Computer Configuration*, expand *Software Settings*.

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



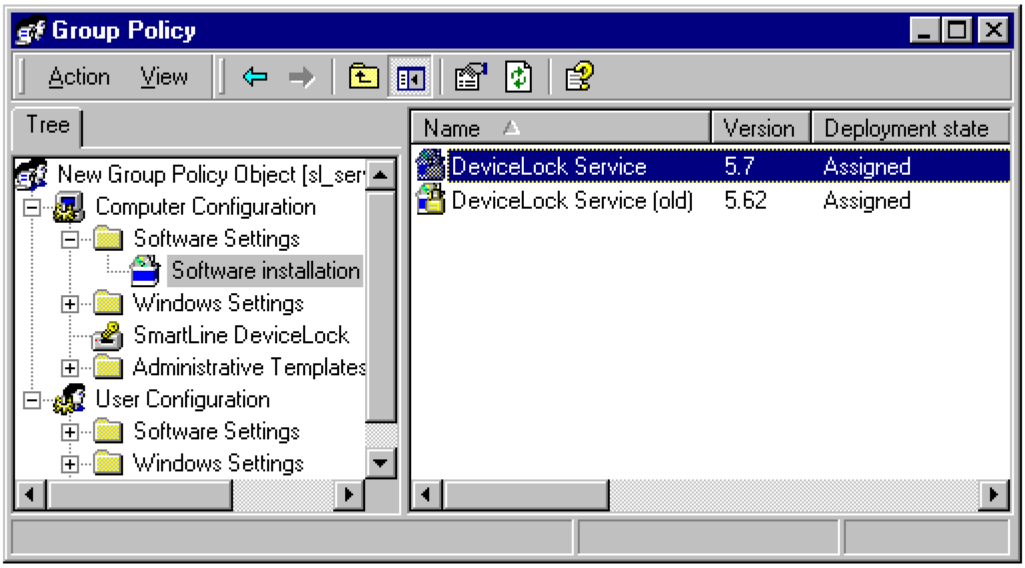
| Name | Version | Deployment state |
|---|---|---|
| DeviceLock Service (old) | 5.62 | Assigned |

Adds a package.

4. 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*.

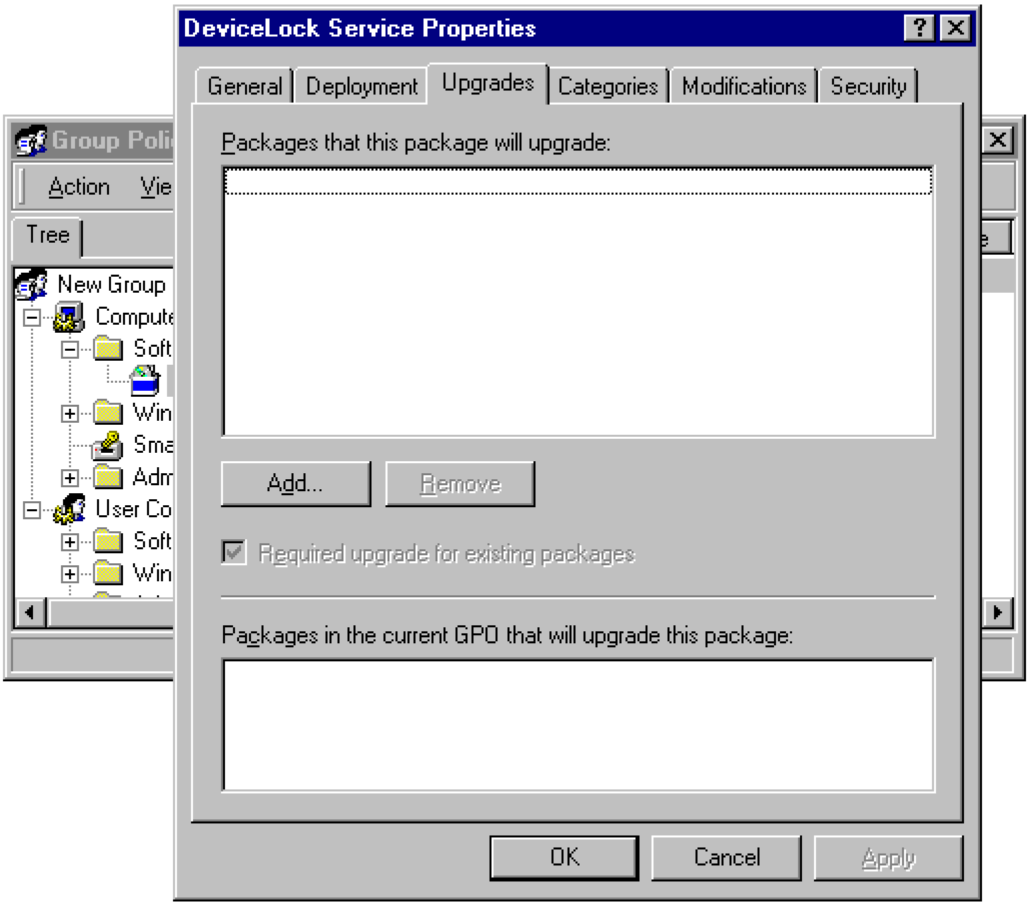
5. Click *Open*.

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



| Name | Version | Deployment state |
|---|---|---|
| DeviceLock Service | 5.7 | Assigned |
| DeviceLock Service (old) | 5.62 | Assigned |

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

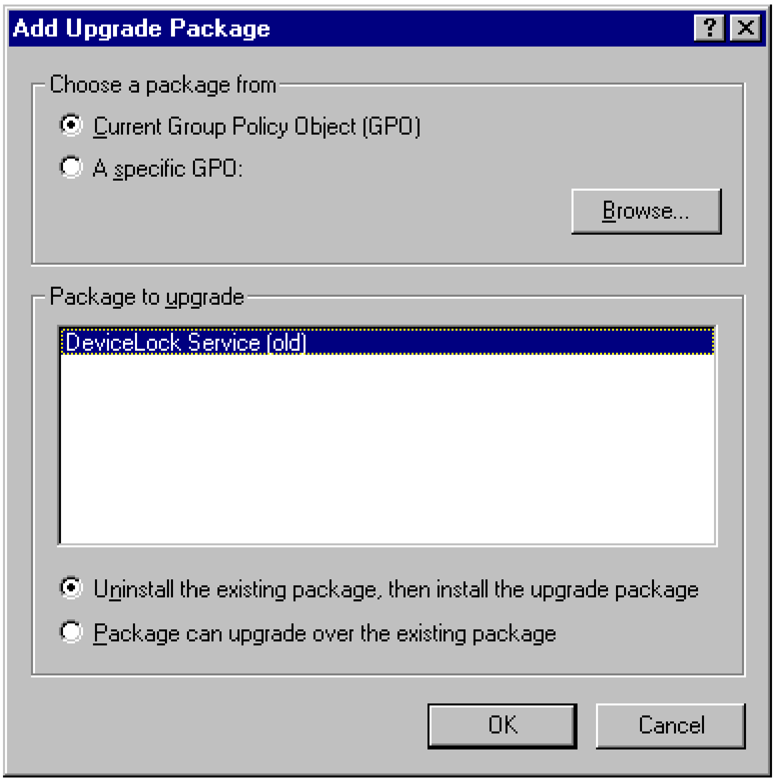


Packages that this package will upgrade:

☑ Required upgrade for existing packages

Packages in the current GPO that will upgrade this package:

8. 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*.



Choose a package from

● Current Group Policy Object (GPO)

○ A specific GPO:

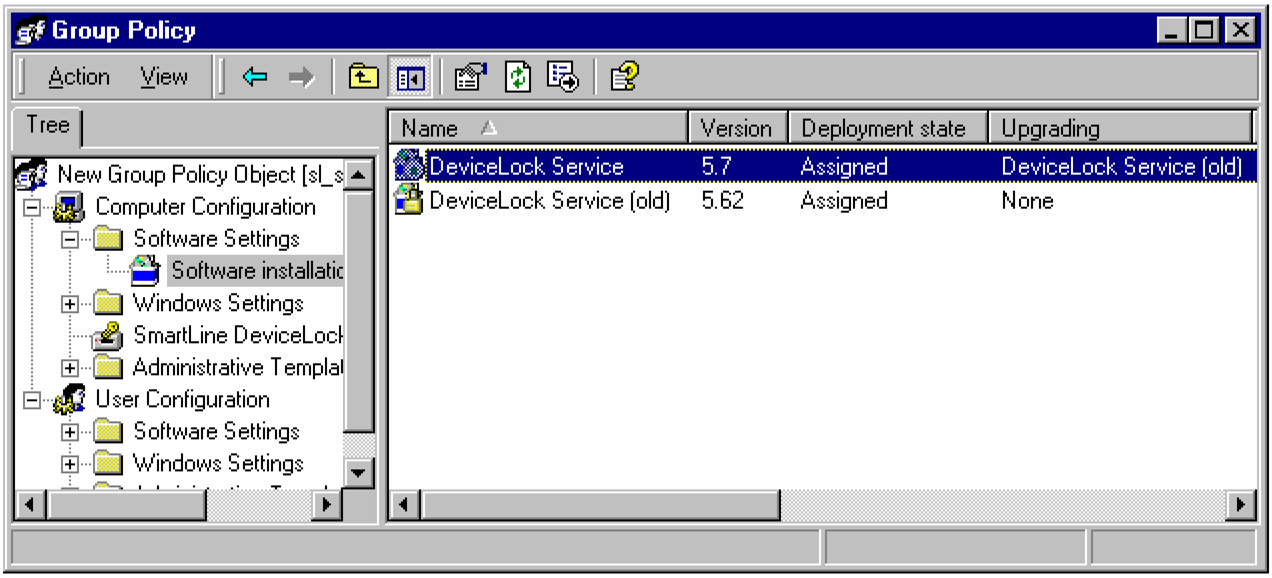
Package to upgrade

DeviceLock Service (old)

● Uninstall the existing package, then install the upgrade package

○ Package can upgrade over the existing package

9. Click *OK* to close the *Properties* window, close the Windows Group Policy Object editor. When the client computer starts, DeviceLock Service is automatically upgraded.



| Name | Version | Deployment state | Upgrading |
|---|---|---|---|
| DeviceLock Service | 5.7 | Assigned | DeviceLock Service (old) |
| DeviceLock Service (old) | 5.62 | Assigned | None |

***Note: Usually when you upgrade, the new DeviceLock Service MSI package detects its previously assigned package in GPO and automatically performs steps 7 and 8 described above.***

- Redeploy a Package

  In some cases you may want to redeploy DeviceLock Service.

  To redeploy a package:

  1. Open the group policy object which contains the deployed package in the Windows Group Policy Object editor (use either the *Group Policy Management* or *Active Directory Users and Computers* snap-in).

  2. Expand the *Software Settings* container that contains the *Software installation* item with which you deployed the package.

  3. Click the *Software installation* container that contains the package.

  4. 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?*"

  5. Click *Yes*.

  6. Close the Windows Group Policy Object editor.

- Remove a Package

  To remove DeviceLock Service:

  1. Open the group policy object which contains the deployed package in the Windows Group Policy Object editor (use either the *Group Policy Management* or *Active Directory Users and Computers* snap-in).

  2. Expand the *Software Settings* container that contains the *Software installation* item with which you deployed the package.

  3. Click the *Software installation* container that contains the package.

  4. In the right pane of the *Group Policy* window, right-click the program. Point to *All Tasks*, and then click *Remove*.

  5. Click *Immediately uninstall the software from users and computers*, and then click *OK*.

  6. Close the Windows Group Policy Object editor.

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.

For more information on how to use the *Group Policy Management* snap-in, please read "*New ways to do familiar tasks using GPMC*" found at: http://technet2.microsoft.com/WindowsServer/en/library/7c73c060-3c97-4aad-95d3-2182d4692ded1033.mspx?mfr=true

If you are not using the *Group Policy Management* snap-in, you may be interested in "*New ways to do familiar Group Policy tasks (pre-GPMC)*" found at: http://technet2.microsoft.com/WindowsServer/en/library/f5860815-522a-4159-906b-bc606335948e1033.mspx?mfr=true

You may also want to read the article "*Deploying and upgrading software*": http://technet2.microsoft.com/WindowsServer/en/library/fdbf74c6-2b98-4a79-815b-d831d8d757b51033.mspx?mfr=true

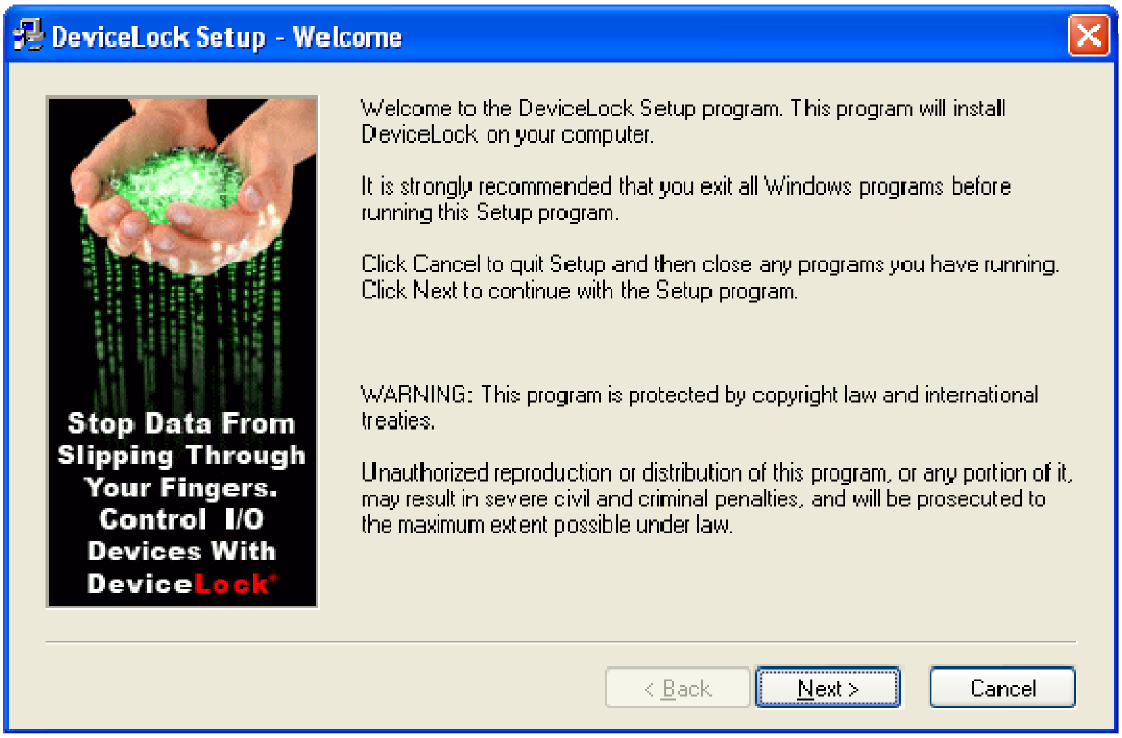
## 2.3 Installing Management Consoles

Management consoles are the control interfaces that systems administrators use to remotely manage DeviceLock Service and DeviceLock Enterprise Server.

DeviceLock management consoles should be installed on the computer from which the administrator is going to manage DeviceLock's settings and run reports. It is not necessary to install management consoles on the server (domain controller or others), even if you are going to use DeviceLock Group Policy Manager to manage settings via Active Directory Group Policy – you can do it from your local workstation (proper privileges required).

***NOTE: In order to use DeviceLock Management Console (the MMC snap-in) and DeviceLock Service Settings Editor on computers with Windows NT 4.0, you should install the Microsoft Management Console update. You can download this update for free from the Microsoft's website: http://www.microsoft.com/downloads/details.aspx?familyid=3F620A07-C996-4A81-AAD8-30134A43EC46&displaylang=en.***

Run Setup (*setup.exe*) and follow the instructions that appear on the screen.


DeviceLock Setup - Welcome
Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock®
< Back
Next >
Cancel

Welcome to the DeviceLock Setup program. This program will install DeviceLock on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

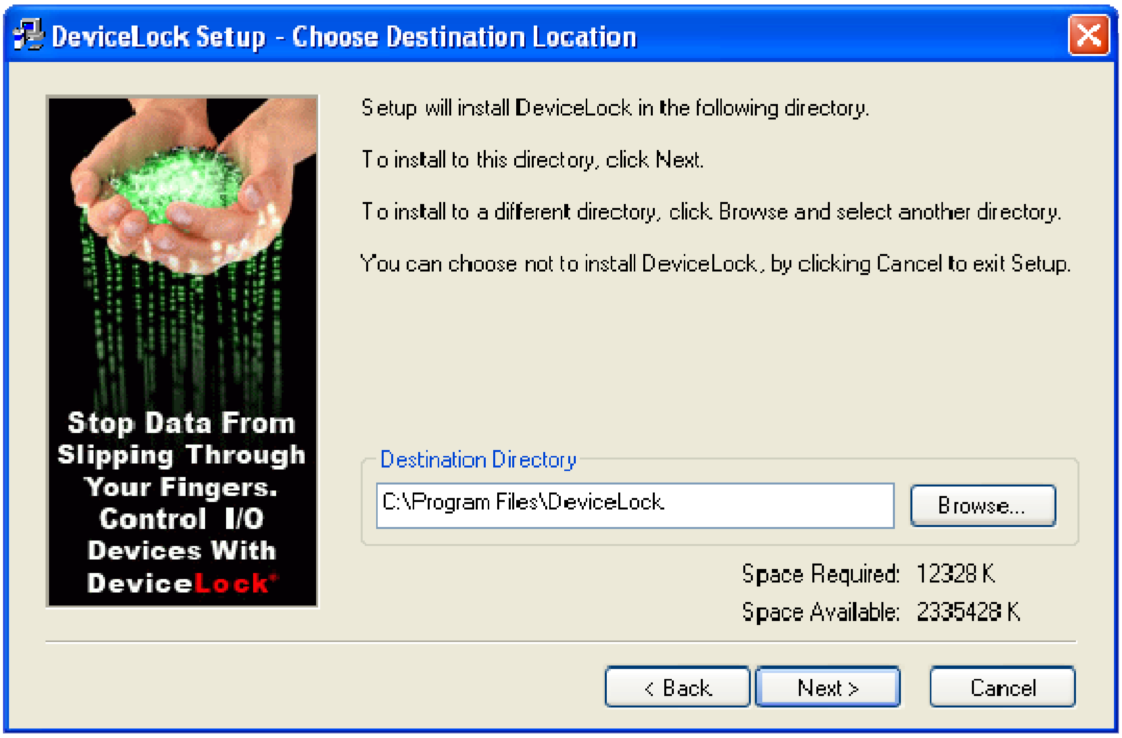
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

You must accept the DeviceLock's End User License Agreement before continuing the installation process.

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



DeviceLock Setup - Choose Destination Location

Setup will install DeviceLock in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

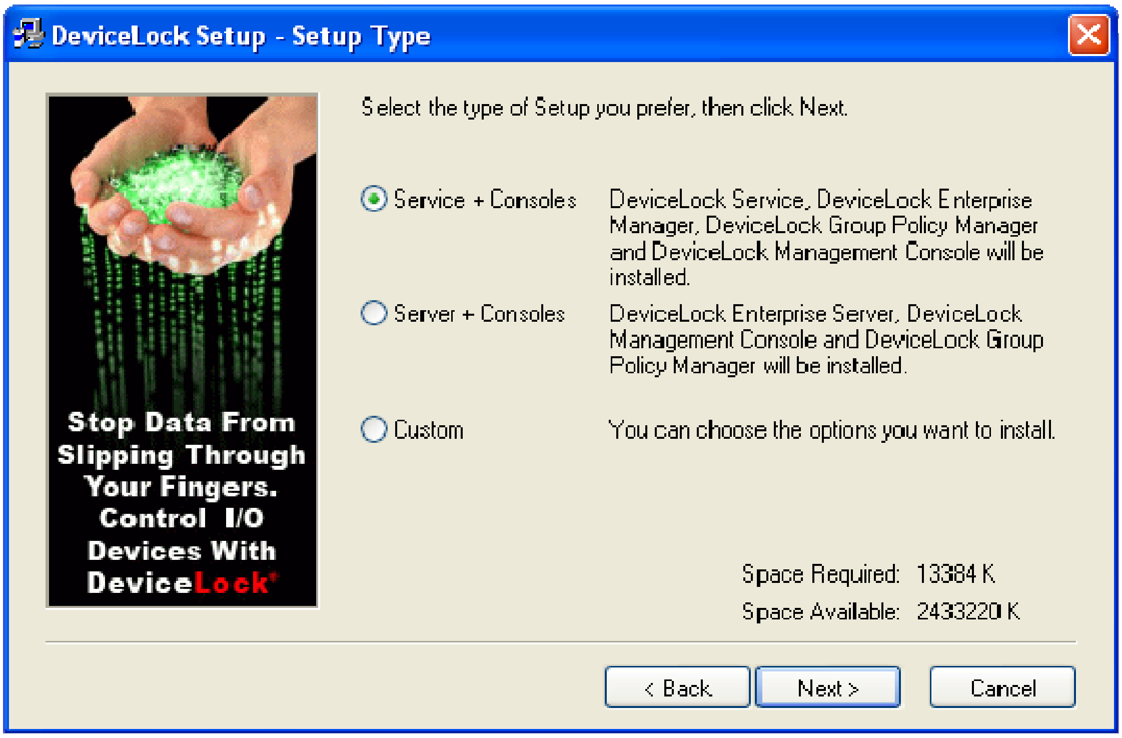
You can choose not to install DeviceLock, by clicking Cancel to exit Setup.

Destination Directory: C:\Program Files\DeviceLock

Space Required: 12328 K
Space Available: 2335428 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock
Browse...
< Back
Next >
Cancel

You have the following three choices: install both DeviceLock Service and DeviceLock management consoles using the *Service + Consoles* option, install both DeviceLock Enterprise Server and DeviceLock management consoles using the *Server + Consoles* option or install only DeviceLock management consoles using the *Custom* option and select the *DeviceLock Consoles* component.



DeviceLock Setup - Setup Type

Select the type of Setup you prefer, then click Next.

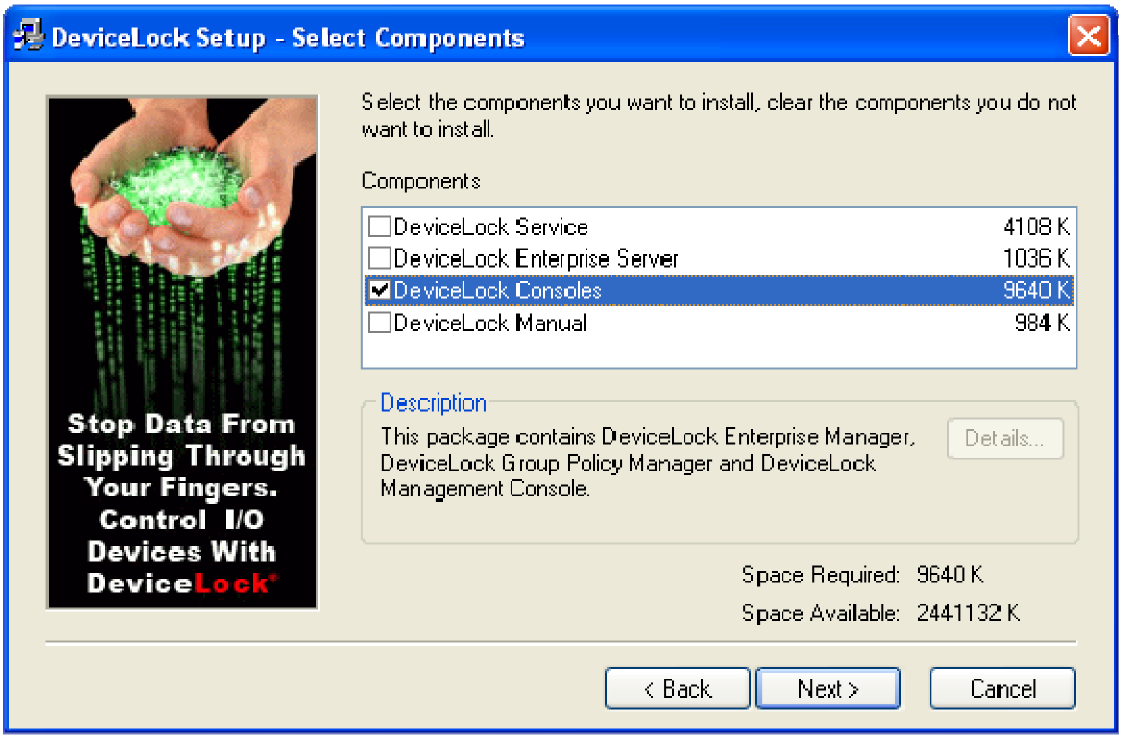
● Service + Consoles — DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.

○ Server + Consoles — DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.

○ Custom — You can choose the options you want to install.

Space Required: 13384 K
Space Available: 2433220 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock
< Back
Next >
Cancel



DeviceLock Setup - Select Components

Select the components you want to install, clear the components you do not want to install.

Components

| | |
|---|---|
| □ DeviceLock Service | 4108 K |
| □ DeviceLock Enterprise Server | 1036 K |
| ☑ DeviceLock Consoles | 9640 K |
| □ DeviceLock Manual | 984 K |

Description

This package contains DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console.

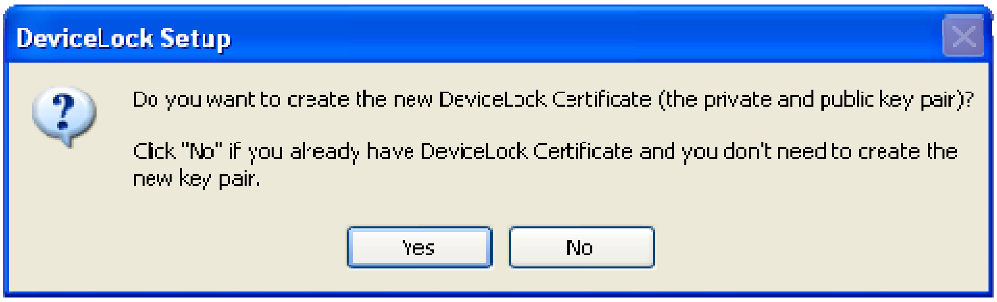
Space Required: 9640 K

Space Available: 2441132 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock®
Details...
< Back
Next >
Cancel

DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor). Installed together with other management consoles is DeviceLock Service Settings Editor, a tool used for creating and modifying external XML files with settings, permissions, audit and shadowing rules for DeviceLock Service.

Setup may suggest that you generate a new DeviceLock Certificate.



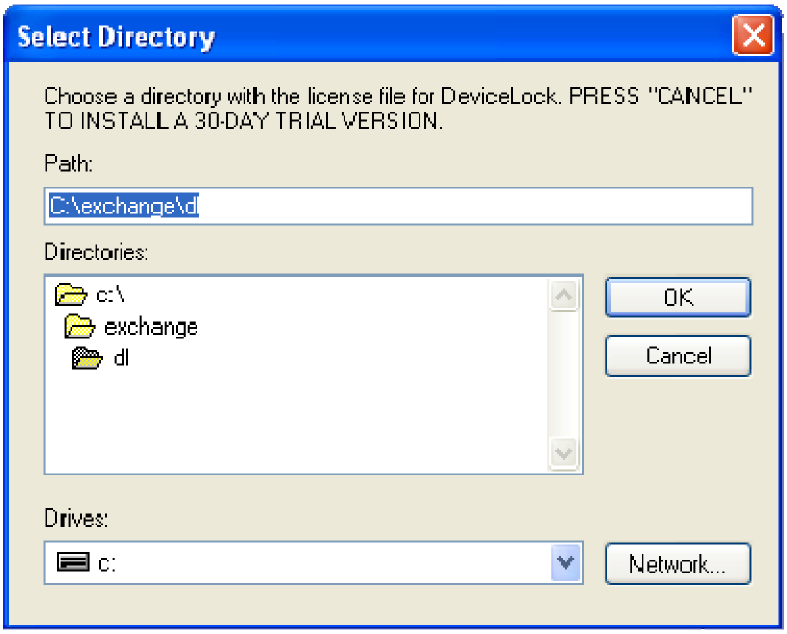
DeviceLock Setup

Do you want to create the new DeviceLock Certificate (the private and public key pair)?

Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.

You can always generate the new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just press the *No* button and continue the installation.

Also, Setup may suggest that you load the license file to register your copy of DeviceLock management consoles. If you don't have the license file, press the *Cancel* button to install DeviceLock in a 30-day trial mode.



Select Directory

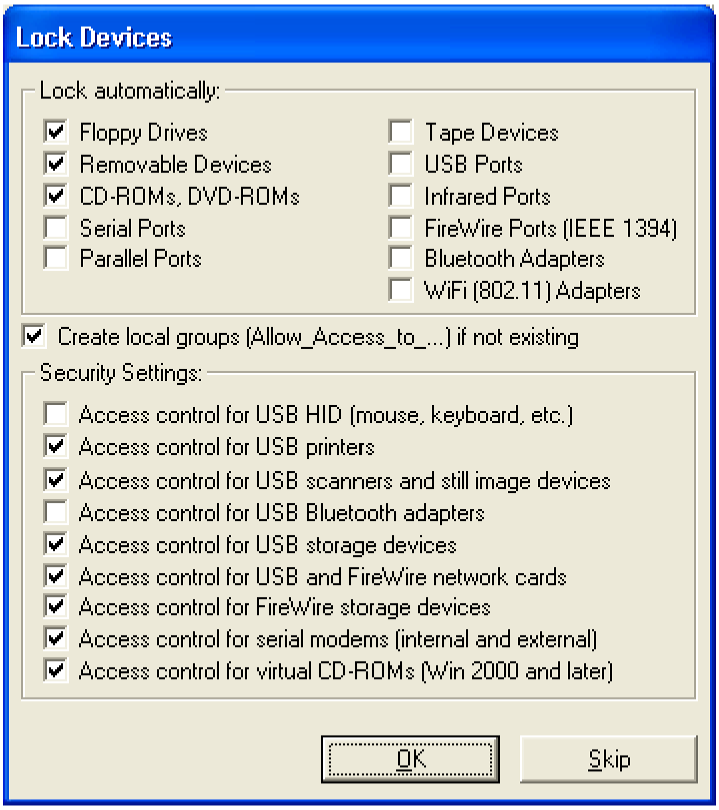
Choose a directory with the license file for DeviceLock. PRESS "CANCEL" TO INSTALL A 30-DAY TRIAL VERSION.

Path: C:\exchange\dl

Directories:
c:\
exchange
dl

Drives: c:

If you opted to install DeviceLock Service as well, Setup suggests that you set special permissions for local devices.



Lock Devices

Lock automatically:

| | |
|---|---|
| ☑ Floppy Drives | □ Tape Devices |
| ☑ Removable Devices | □ USB Ports |
| ☑ CD-ROMs, DVD-ROMs | □ Infrared Ports |
| □ Serial Ports | □ FireWire Ports (IEEE 1394) |
| □ Parallel Ports | □ Bluetooth Adapters |
| | □ WiFi (802.11) Adapters |

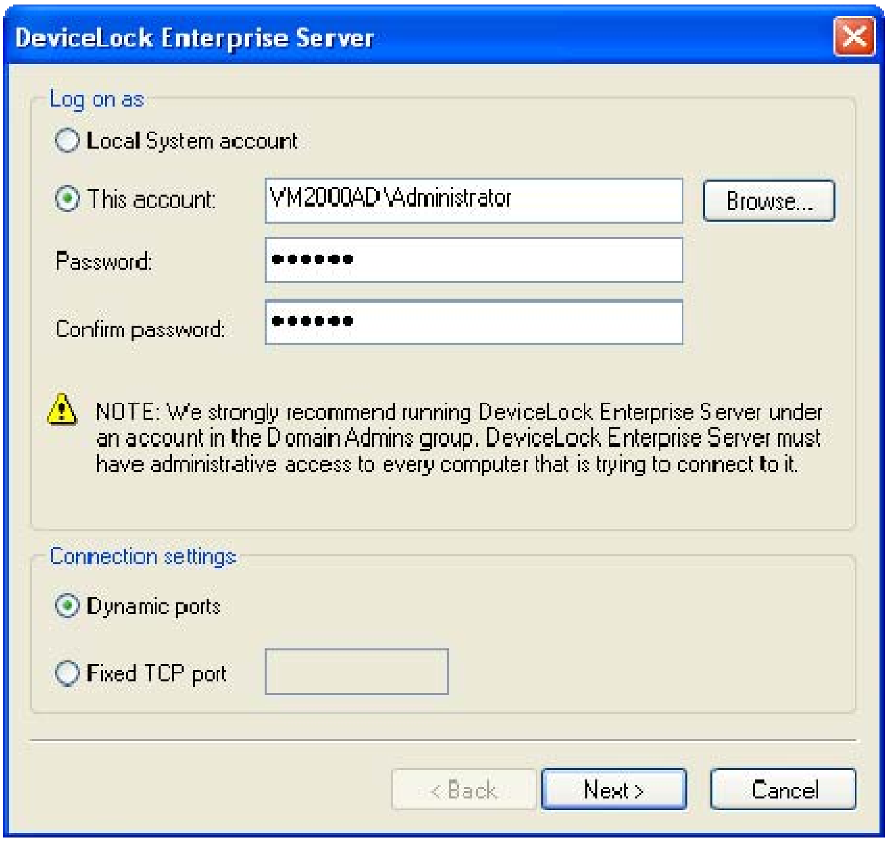
☑ Create local groups (Allow_Access_to_...) if not existing

Security Settings:

□ Access control for USB HID (mouse, keyboard, etc.)
☑ Access control for USB printers
☑ Access control for USB scanners and still image devices
□ Access control for USB Bluetooth adapters
☑ Access control for USB storage devices
☑ Access control for USB and FireWire network cards
☑ Access control for FireWire storage devices
☑ Access control for serial modems (internal and external)
☑ Access control for virtual CD-ROMs (Win 2000 and later)

Press the *Skip* button if you prefer to wait until after installation to set permissions for devices using DeviceLock management consoles. For more information regarding these settings, please read the **Deploying DeviceLock Service** section of this manual.

If you opted to install DeviceLock Enterprise Server as well, Setup suggests that you define its settings using the configuration wizard.



DeviceLock Enterprise Server

Log on as

○ Local System account

● This account: VM2000AD\Administrator

Password: ••••••

Confirm password: ••••••

NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.

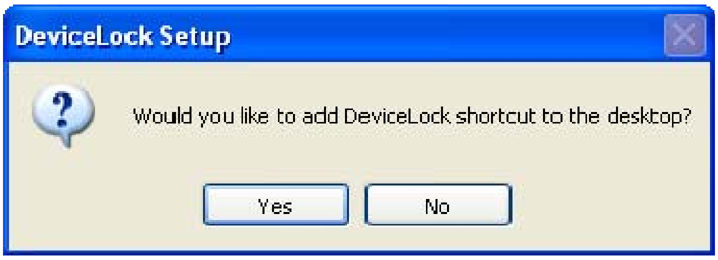
Connection settings

● Dynamic ports

○ Fixed TCP port

For more information regarding these settings, please read the **Installing DeviceLock Enterprise Server** section of this manual.

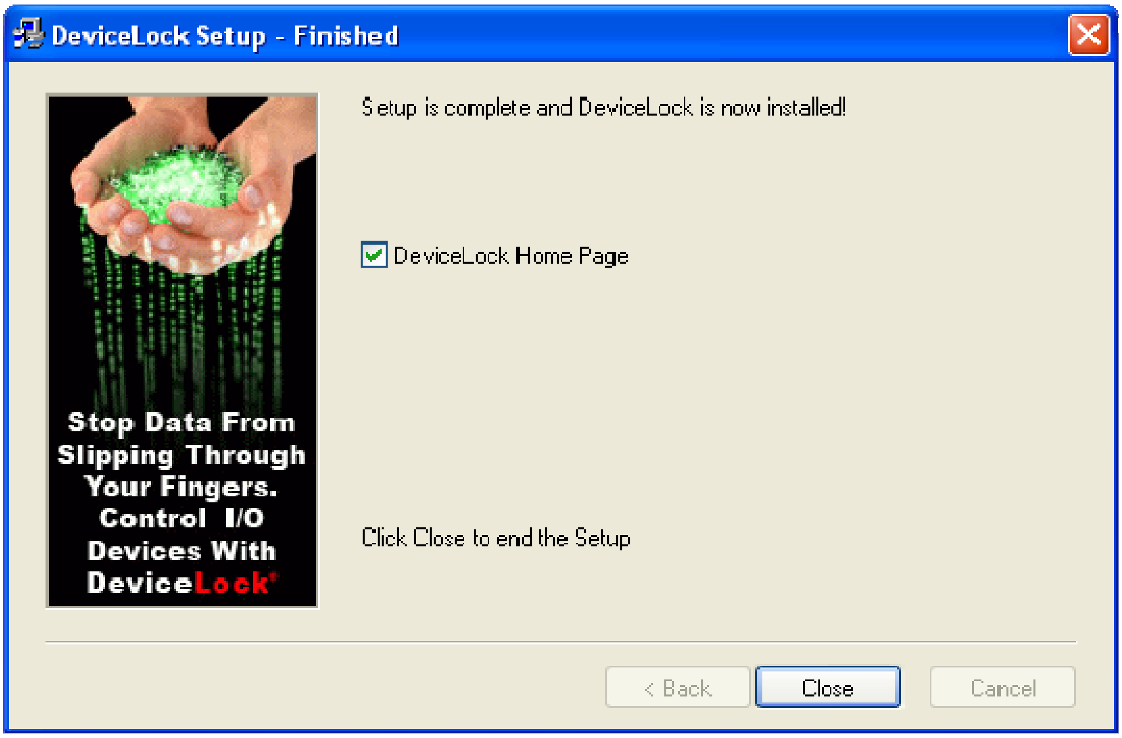
You can add DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Service Settings Editor shortcuts to your current desktop.



DeviceLock Setup

Would you like to add DeviceLock shortcut to the desktop?

As soon as Setup has installed DeviceLock, it suggests that you point your default Internet browser to the DeviceLock website.



DeviceLock Setup - Finished
Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock®

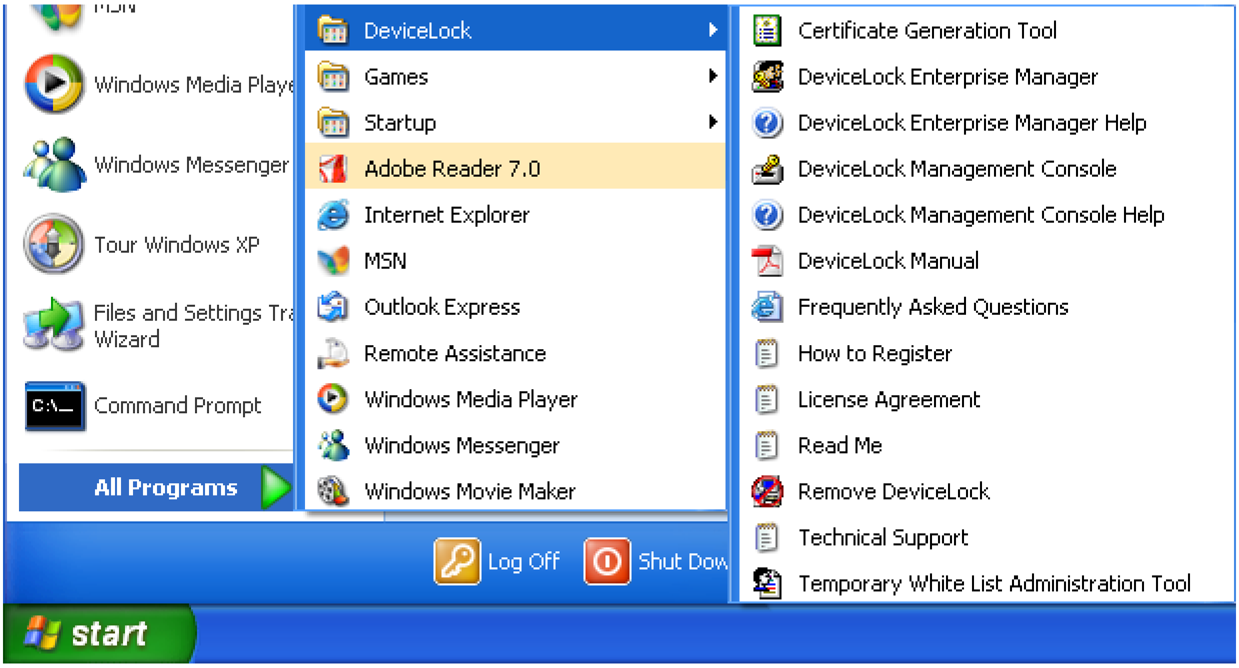
Setup is complete and DeviceLock is now installed!

☑ DeviceLock Home Page

Click Close to end the Setup

Uncheck the *DeviceLock Home Page* flag if you do not want to visit the DeviceLock website. Press the *Close* button to finish the installation.

You can locate and run DeviceLock management consoles from the *Programs* menu available by clicking the Windows *Start* button.



***NOTE: DeviceLock Group Policy Manager integrates into Windows Group Policy Editor and is not available as a stand-alone application. In order to use DeviceLock Group Policy Manager, you must run the standard Windows Group Policy Editor.***

## 2.4 Installing DeviceLock Enterprise Server

DeviceLock Enterprise Server is the optional component for centralized collection and storage of shadow data and audit logs.

In order to use DeviceLock Enterprise Server on Windows NT 4.0 SP6 and Windows 2000 computers, you should install Microsoft Data Access Components (MDAC) version 2.8 or later. MDAC is available for free download at the Microsoft website: http://www.microsoft.com/downloads/details.aspx?familyid=78cac895-efc2-4f8e-a9e0-3a1afbd5922e&displaylang=en.

### 2.4.1 Planning Infrastructure

You can install several DeviceLock Enterprise Servers on different computers across your network to uniformly spread the network load.

DeviceLock Enterprise Server uses MS SQL Server to store its data. Hence, it is necessary to have MS SQL Server installed and started in your network before installing DeviceLock Enterprise Server. If you don't have MS SQL Server, you can install the free edition called SQL Server Express Edition available for free download at the Microsoft website: http://msdn.microsoft.com/vstudio/express/sql/download/.

It is not necessary to run MS SQL Server and DeviceLock Enterprise Server on the same machine. Moreover, for performance and reliability reasons, it is better to install DeviceLock Enterprise Server on a separate computer.

There are three scenarios for connecting DeviceLock Enterprise Server and MS SQL Server. You should decide which scenario best fits your needs before installing DeviceLock Enterprise Server:

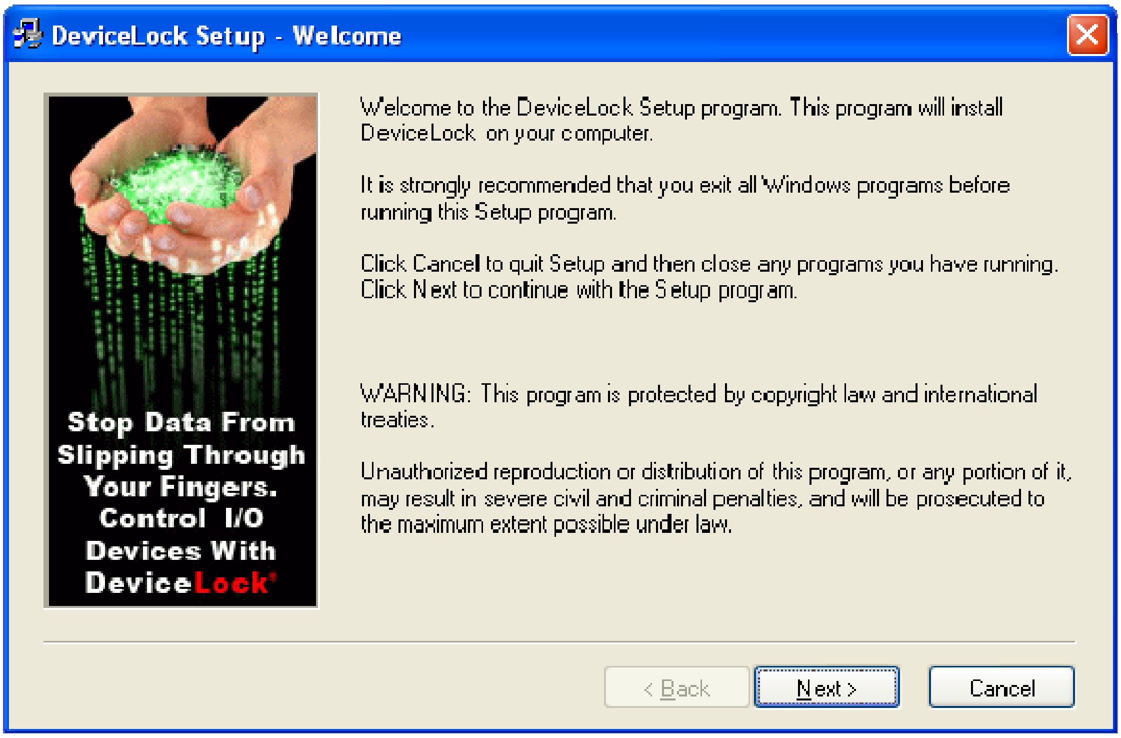
1. ONE-TO-ONE: you install one DeviceLock Enterprise Server and connect it to one MS SQL Server. This scenario is most appropriate for small networks (up to several hundreds of computers).

2. MANY-TO-MANY: you install several DeviceLock Enterprise Servers and connect each of them to its own MS SQL Server. This scenario is typical for medium and large networks geographically distributed across a variety of segments.

3. MANY-TO-ONE: you install several DeviceLock Enterprise Servers and connect all of them to the one MS SQL Server. This scenario could be used for medium and large networks with a powerful (large amount of memory and free storage space) dedicated machine for MS SQL Server.

### 2.4.2 Interactive Installation

Run Setup (*setup.exe*) and follow the instructions that appear on the screen. You must run *setup.exe* on each computer targeted for DeviceLock Enterprise Server installation.


DeviceLock Setup - Welcome
Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock
< Back
Next >
Cancel

Welcome to the DeviceLock Setup program. This program will install DeviceLock on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

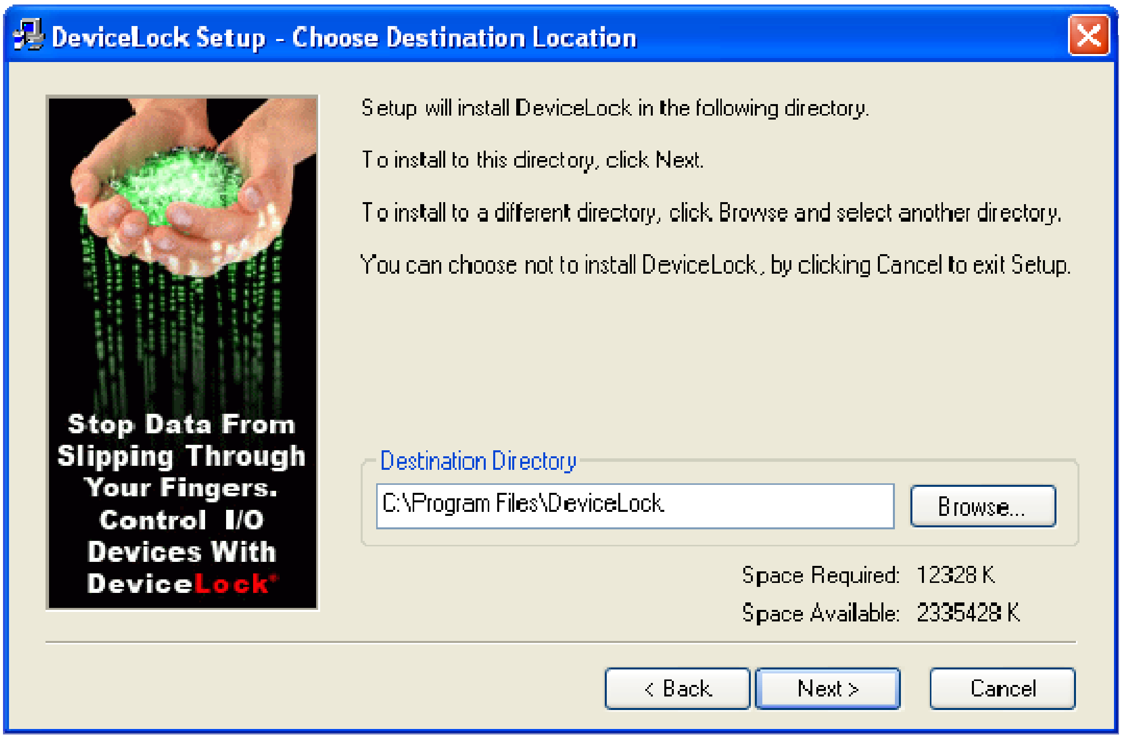
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

You must accept the DeviceLock End User License Agreement before continuing the installation process.

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



DeviceLock Setup - Choose Destination Location

Setup will install DeviceLock in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

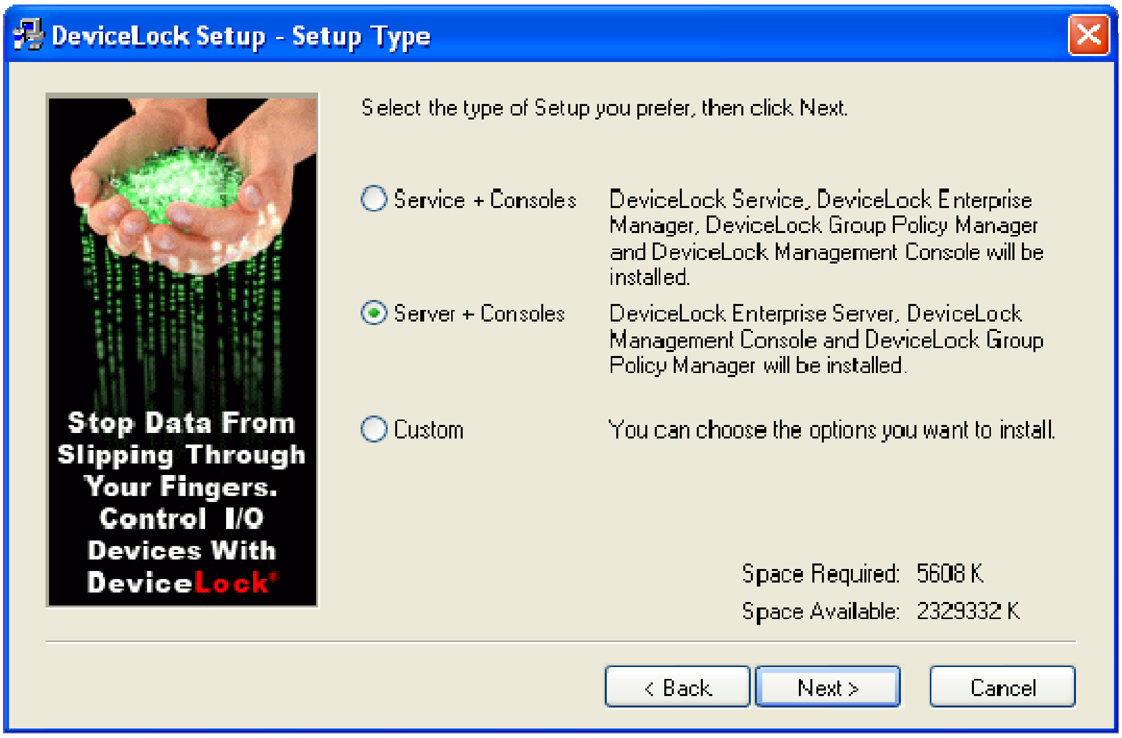
You can choose not to install DeviceLock, by clicking Cancel to exit Setup.

Destination Directory: C:\Program Files\DeviceLock

Space Required: 12328 K
Space Available: 2335428 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock
Browse...
< Back
Next >
Cancel

You have the following two choices: either install both DeviceLock Enterprise Server and DeviceLock management consoles using the *Server + Consoles* option or install only DeviceLock Enterprise Server using the *Custom* option and select the *DeviceLock Enterprise Server* component.



DeviceLock Setup - Setup Type

Select the type of Setup you prefer, then click Next.

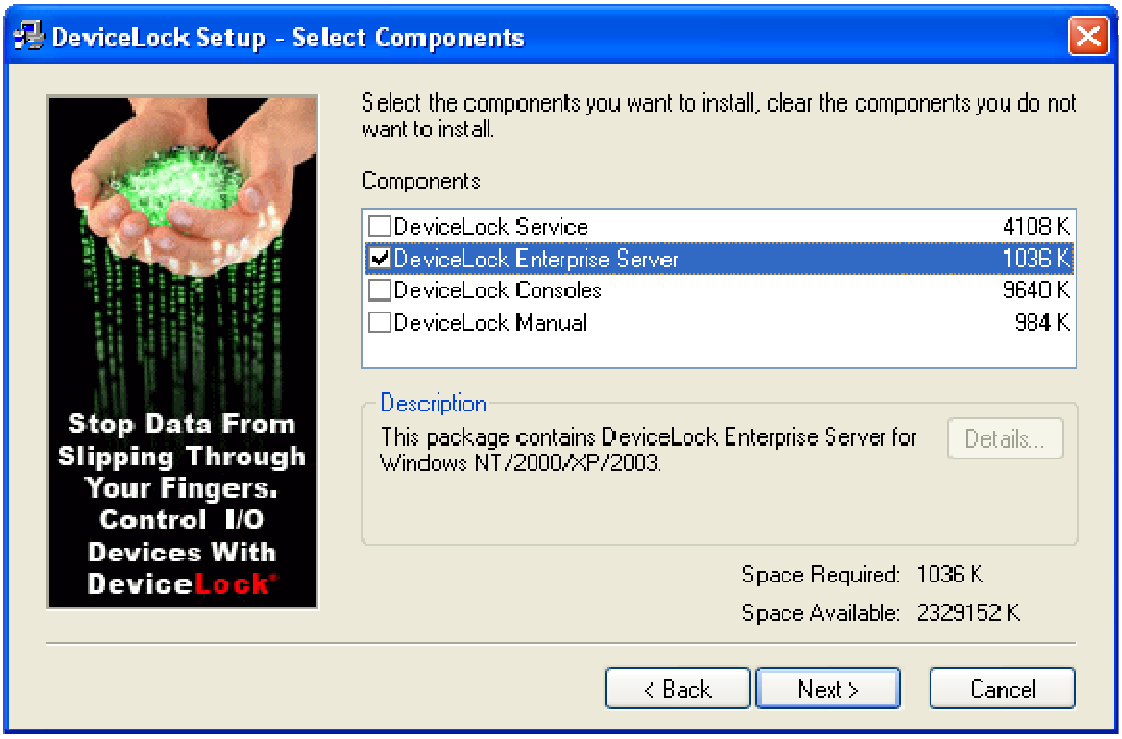
○ Service + Consoles — DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.

● Server + Consoles — DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.

○ Custom — You can choose the options you want to install.

Space Required: 5608 K
Space Available: 2329332 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock
< Back
Next >
Cancel


DeviceLock Setup - Select Components

Select the components you want to install, clear the components you do not want to install.

Components

| | |
|---|---|
| □ DeviceLock Service | 4108 K |
| ☑ DeviceLock Enterprise Server | 1036 K |
| □ DeviceLock Consoles | 9640 K |
| □ DeviceLock Manual | 984 K |

Description

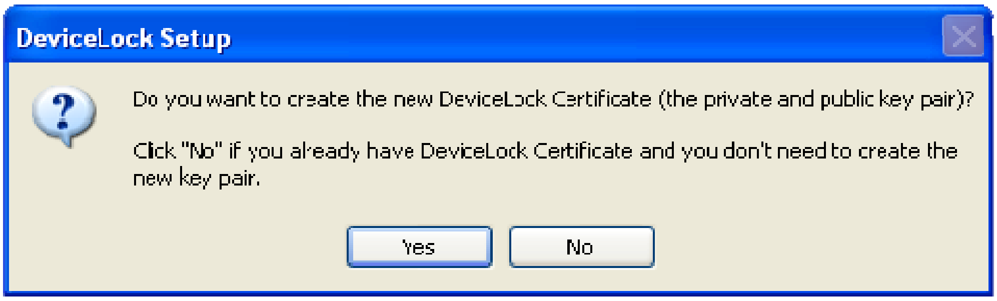
This package contains DeviceLock Enterprise Server for Windows NT/2000/XP/2003.

Space Required: 1036 K

Space Available: 2329152 K

Stop Data From Slipping Through Your Fingers. Control I/O Devices With DeviceLock®
Details...
< Back
Next >
Cancel

If you selected to install DeviceLock management consoles as well, Setup may suggest that you generate a new DeviceLock Certificate.

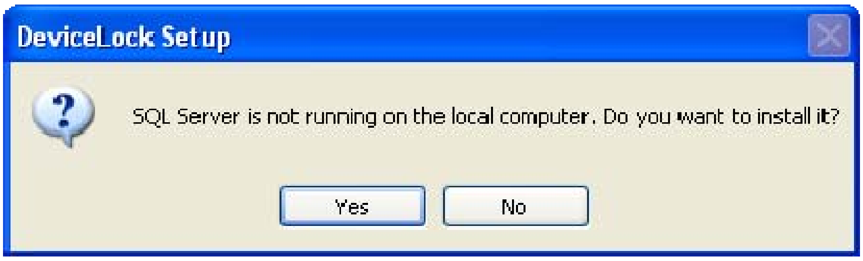

DeviceLock Setup

Do you want to create the new DeviceLock Certificate (the private and public key pair)?

Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.

You can always generate the new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just press the *No* button and continue the installation.

If Setup detects that MS SQL Server is not running on the local computer but its installation package is available, Setup suggests that you run the MS SQL Server installation.



SQL Server is not running on the local computer. Do you want to install it?

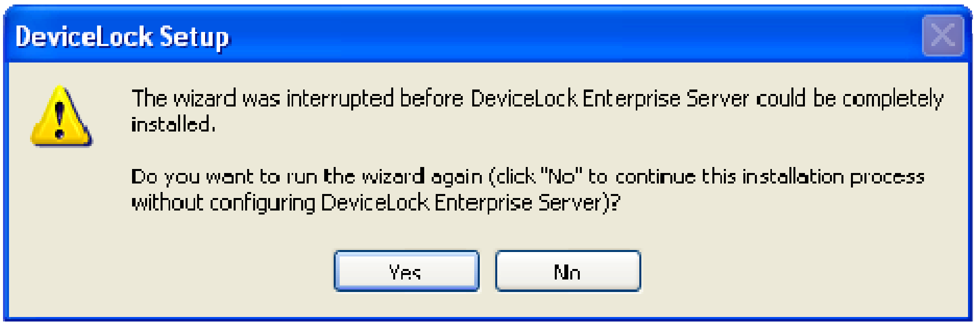
If you don't want to install MS SQL Server on the local computer or it is already installed but just not started, press the *No* button.

During the installation process, you must configure DeviceLock Enterprise Server and define its main settings using the special wizard.

If you are installing an upgrade or just reinstalling DeviceLock Enterprise Server and want to keep its current configuration, you don't need to go through this wizard again – just press the *Cancel* button to close the wizard and keep all existing settings unchanged.

In case you need to change some parameters but keep others – edit only needed parameters and go through all the wizard's pages up to the *Finish* button on the very last page.

***NOTE: If you are installing DeviceLock Enterprise Server for the first time (there are no existing settings on this computer yet) and you cancel the configuration wizard upon opening, Setup will not be able to install DeviceLock Enterprise Server's service, so you'll need to run the configuration wizard again.***

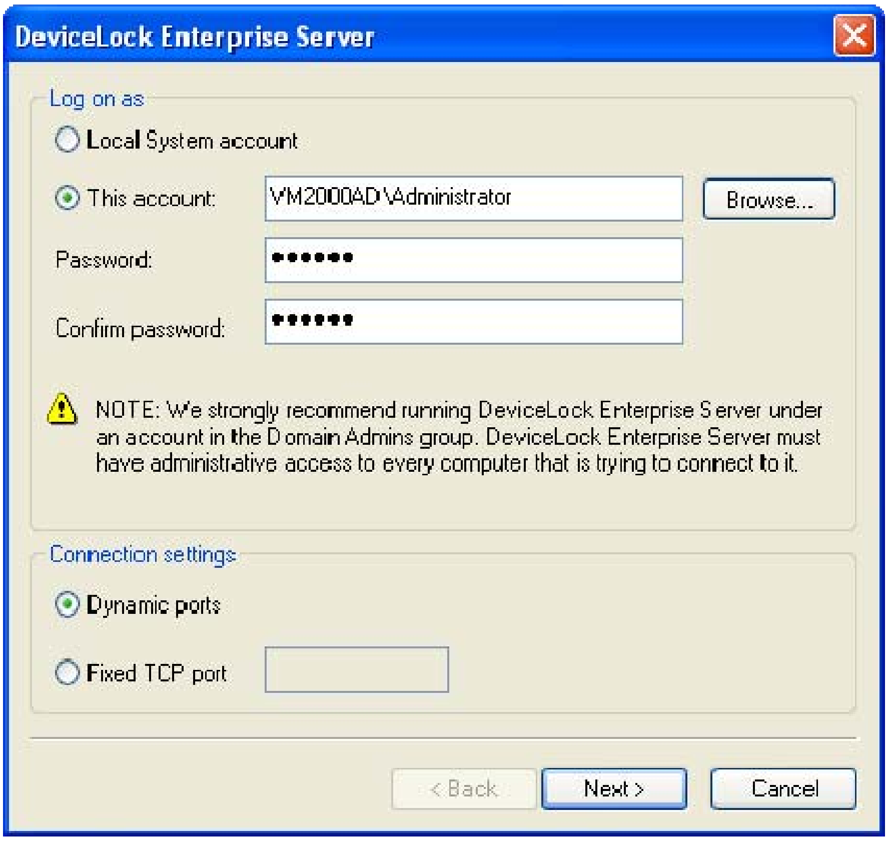


The wizard was interrupted before DeviceLock Enterprise Server could be completely installed.

Do you want to run the wizard again (click "No" to continue this installation process without configuring DeviceLock Enterprise Server)?

***If you press the No button to continue without installing the DeviceLock Enterprise Server's service, you will need to run Setup later and install the service anyway.***

On the first page of the wizard you can opt to install DeviceLock Enterprise Server's service and define its startup parameters.



DeviceLock Enterprise Server

Log on as

○ Local System account

● This account: VM2000AD\Administrator

Password: ••••••

Confirm password: ••••••

NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.

Connection settings

● Dynamic ports

○ Fixed TCP port

## 1.1. Log on as

First of all, you should choose an account under which the DeviceLock Enterprise Server's service will start. As many other Windows services, the DeviceLock Enterprise Server's service can start under the special local system account (the *SYSTEM* user) and on behalf of any user.

To start the service under the *SYSTEM* user, select the *Local System account* option. Keep in mind that the process working under the *SYSTEM* user can't access shared network resources and authenticates on remote computers as an anonymous user. Therefore, DeviceLock Enterprise Server configured to run under the *SYSTEM* user is not able to store shadow files on the remote computer (e.g. on the file server) and it must use DeviceLock Certificate for authentication on DeviceLock Services running on remote computers.

For more information about authentication methods, please read the description of the Certificate Name parameter.

To start the service on behalf of the user, select the *This account* option, enter the user's account name and the password. It is recommended to use a user account that has administrative privileges on all the computers where DeviceLock Service is running. Otherwise, you will need to use DeviceLock Certificate authentication.

If you're installing DeviceLock Enterprise Server in the domain environment, we recommend that you use a user account that is a member of the *Domain Admins* group. Since *Domain Admins* is a member of the local group *Administrators* on every computer in the domain, members of *Domain Admins* will have full access to DeviceLock Service on every computer.

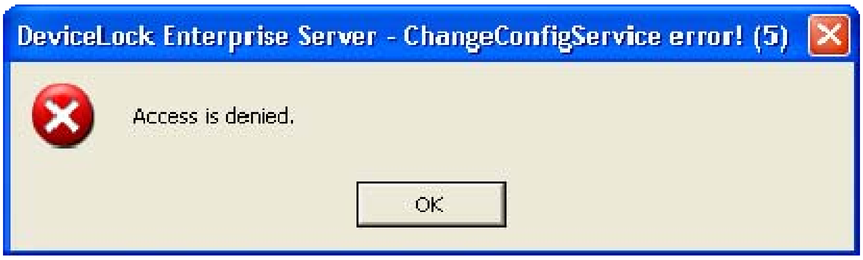
Also, don't forget that if DeviceLock Security is enabled on remotely running DeviceLock Services to protect them against local users with administrative privileges, the user's account specified in the *This account* option must be also in the list of DeviceLock Administrators with **Full access** rights. Otherwise, you'll need to use DeviceLock Certificate authentication.

### 1.2. Connection settings

You can instruct DeviceLock Enterprise Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall. Type the port number in *Fixed TCP port*. To use dynamic ports for RPC communication, select the *Dynamic ports* option.

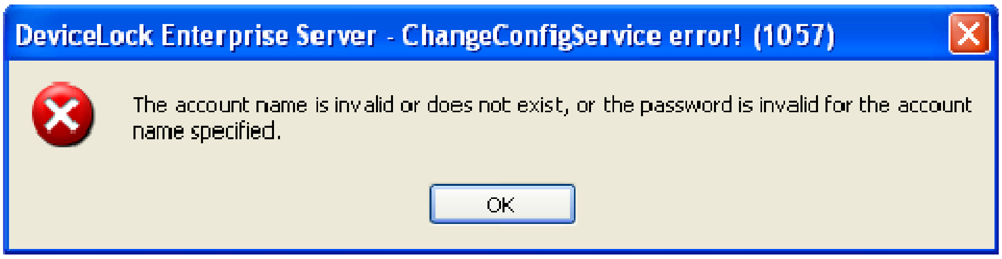
Press the *Next* button to start the DeviceLock Enterprise Server's service and to proceed to the second page.

If the current user doesn't have full administrative access to DeviceLock Enterprise Server (in case it already exists and you're installing an upgrade), the configuration wizard will not be able to install the service and apply changes. Also, the similar error may occur when the current user doesn't have local administrative privileges on the computer where DeviceLock Enterprise Server is installing.


DeviceLock Enterprise Server - ChangeConfigService error! (5)

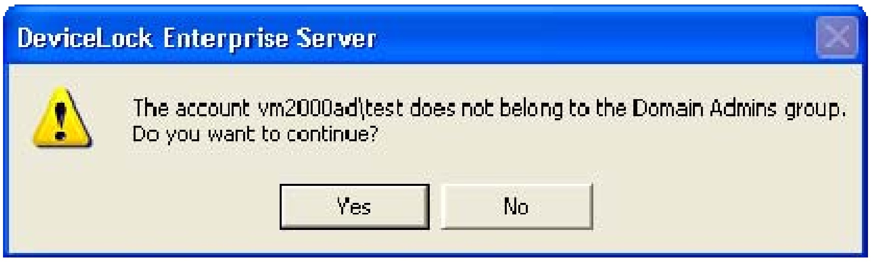
Access is denied.

If you've specified an incorrect user name for the *This account* option or the wrong user password, DeviceLock Enterprise Server will not be able to start.


DeviceLock Enterprise Server - ChangeConfigService error! (1057)

The account name is invalid or does not exist, or the password is invalid for the account name specified.

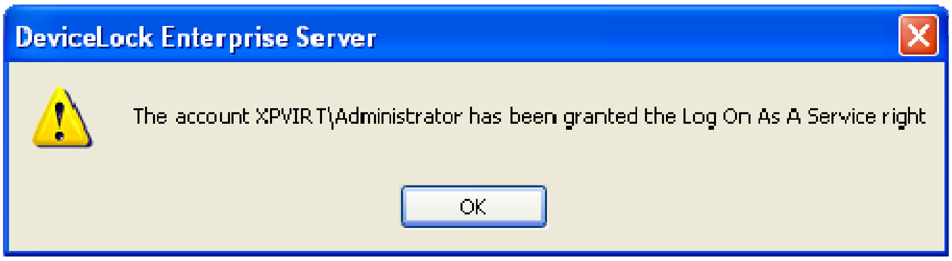
You will be notified if the user's account specified for the *This account* option is not a member of the *Domain Admins* group.


DeviceLock Enterprise Server

The account vm2000ad\test does not belong to the Domain Admins group.
Do you want to continue?

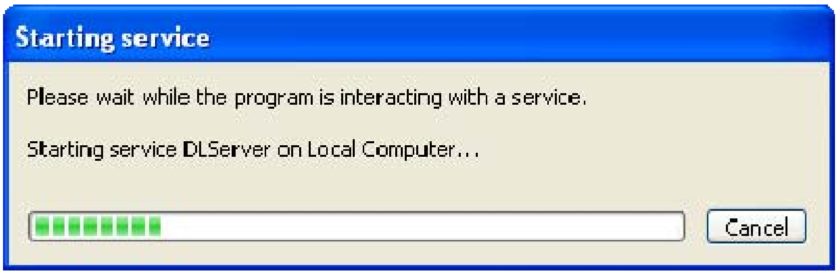
You may continue by pressing the *Yes* button. However keep in mind that in this case either the specified user must have full administrative access to all remotely running DeviceLock Services or DeviceLock Certificate (the *public* key) must be installed on every computer with DeviceLock Service.

If the user's account specified for the *This account* option doesn't have the *Log On As A Service* system privilege, the wizard automatically assigns it. This privilege is needed to start the service on behalf of the user.


DeviceLock Enterprise Server

The account XPVIRT\Administrator has been granted the Log On As A Service right

If all of the service's startup parameters were specified correctly, the wizard starts DeviceLock Enterprise Server.

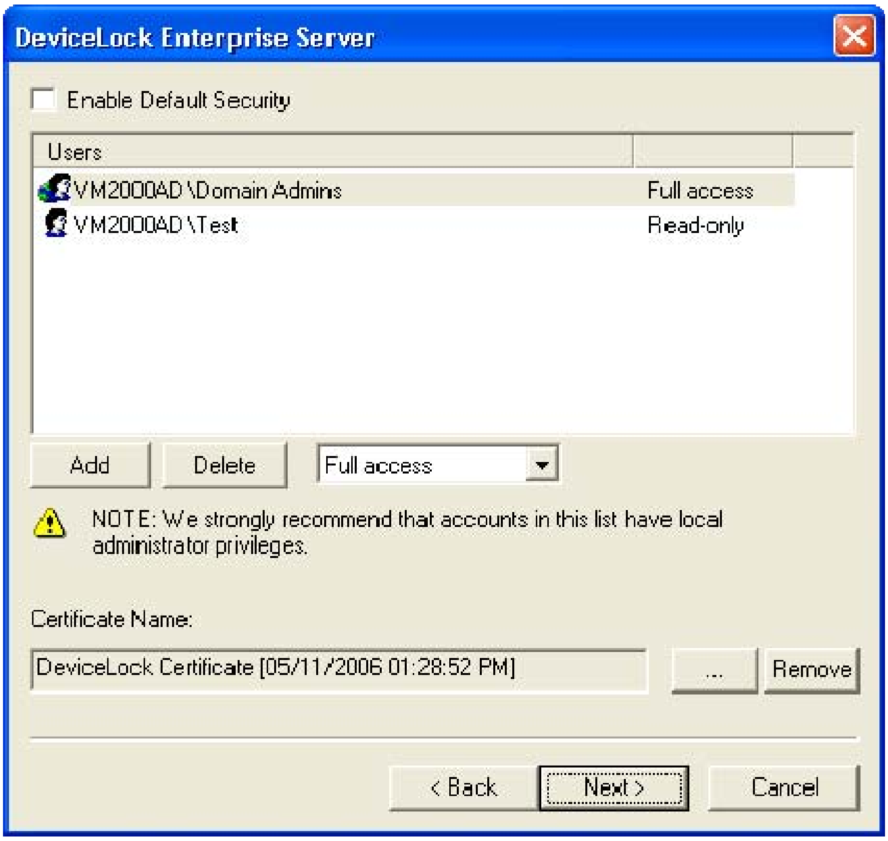

Starting service

Please wait while the program is interacting with a service.

Starting service DLServer on Local Computer...

It takes some time (up to a minute) before the DeviceLock Enterprise Server's service is started and the wizard's second page is displayed.

On the second page, you can define the list of users that have administrative access to DeviceLock Enterprise Server and install DeviceLock Certificate (the *private* key).



DeviceLock Enterprise Server

☐ Enable Default Security

| Users | |
|---|---|
| VM2000AD \Domain Admins | Full access |
| VM2000AD \Test | Read-only |

NOTE: We strongly recommend that accounts in this list have local administrator privileges.

Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

## 2.1. Enable Default Security

In the default security configuration all users with local administrator privileges (i.e. members of the local *Administrators* group) can connect to DeviceLock Enterprise Server using a management console and change its setting and run reports.

To turn on the default security, check the *Enable Default Security* flag.

If you need to define more granular access to DeviceLock Enterprise Server, turn off the default security by unchecking the *Enable Default Security* flag.

Then you need to specify authorized accounts (users and/or groups) that can connect to DeviceLock Enterprise Server. To add a new user or user group to the list of accounts, click on the *Add* button. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the *Delete* button. Using *Ctrl* and/or *Shift* you can highlight and remove several records simultaneously.

To define which actions are to be allowed for a user or user group, set the appropriate rights:

- **Full access** – to enable full access to DeviceLock Enterprise Server. Users can change settings and run reports.
- **Change** – to enable change access to DeviceLock Enterprise Server. Users can change settings, install/uninstall DeviceLock Enterprise Server and run reports, but they can't add new users to the list of authorized accounts that can connect to DeviceLock Enterprise Server or change access rights for existing users in this list.
- **Read-only** – to enable only read access to DeviceLock Enterprise Server. Users can run reports and view settings, but can't modify anything.

***NOTE: We strongly recommend that accounts included in this list have local administrator privileges because, in some instances, installing, updating and uninstalling DeviceLock Enterprise Server's service may require access rights to Windows Service Control Manager (SCM) and shared network resources.***

### 2.2. Certificate Name

You may need to deploy the *private* key to DeviceLock Enterprise Server if you want to enable authentication based on DeviceLock Certificate.

There are two methods of DeviceLock Enterprise Server authentication on remotely running DeviceLock Services:

a. *User authentication* – the DeviceLock Enterprise Server's service is running under the user's account that has full administrative access to DeviceLock Service on the remote computer. For more information on how to run DeviceLock Enterprise Server on behalf of the user, please read the description of the Log on as parameter.

b. *DeviceLock Certificate authentication* – in situations when the user under which DeviceLock Enterprise Server is running can't access DeviceLock Service on the remote computer, you must authenticate based on a DeviceLock Certificate.

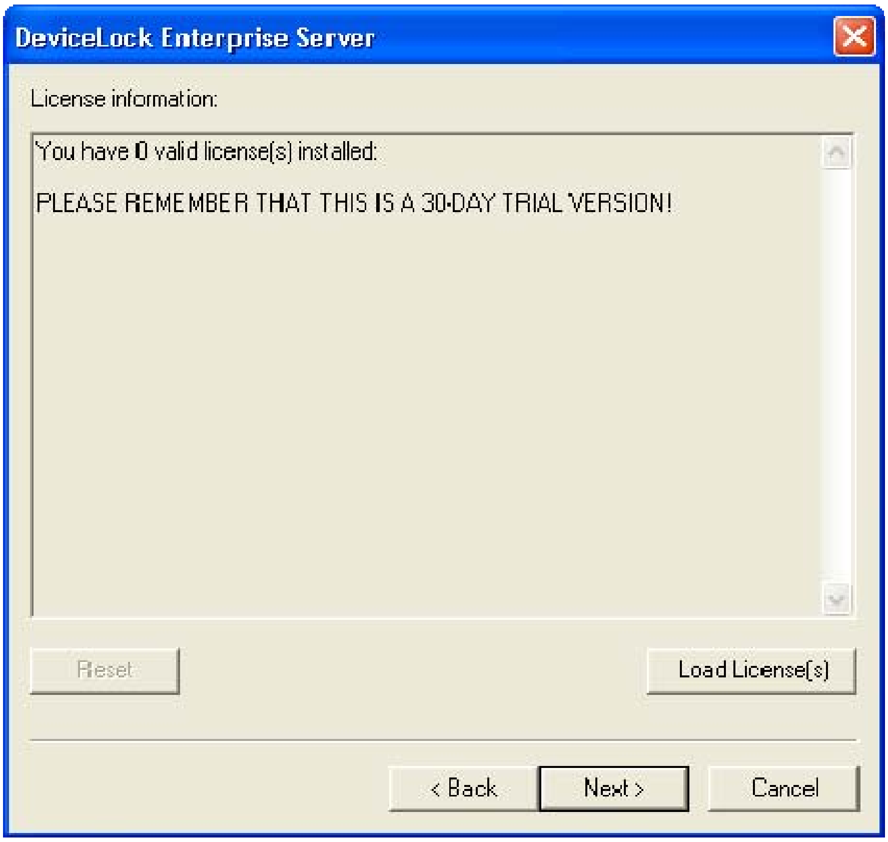
   The *public* key should be installed on DeviceLock Service and the corresponding *private* key on DeviceLock Enterprise Server.

To install DeviceLock Certificate, press the **...** button, and select the file with a *private* key. To remove DeviceLock Certificate, press the *Remove* button.

For more information regarding DeviceLock Certificate, please read the **DeviceLock Certificates** section of this manual.

Press the *Next* button to apply changes and proceed to the third page of the configuration wizard.

From this page, you can load your DeviceLock licenses.



You have 0 valid license(s) installed:

PLEASE REMEMBER THAT THIS IS A 30-DAY TRIAL VERSION!

## 3.1. License information

If you've purchased a license for DeviceLock, you should load this license into DeviceLock Enterprise Server.

DeviceLock Enterprise Server handles only the licensed number of DeviceLock Services. For example, if you have a license for 100 computers but there are 101 DeviceLock Services working in your network, DeviceLock Enterprise Server will work with only first 100 DeviceLock Services and ignore the remaining one.

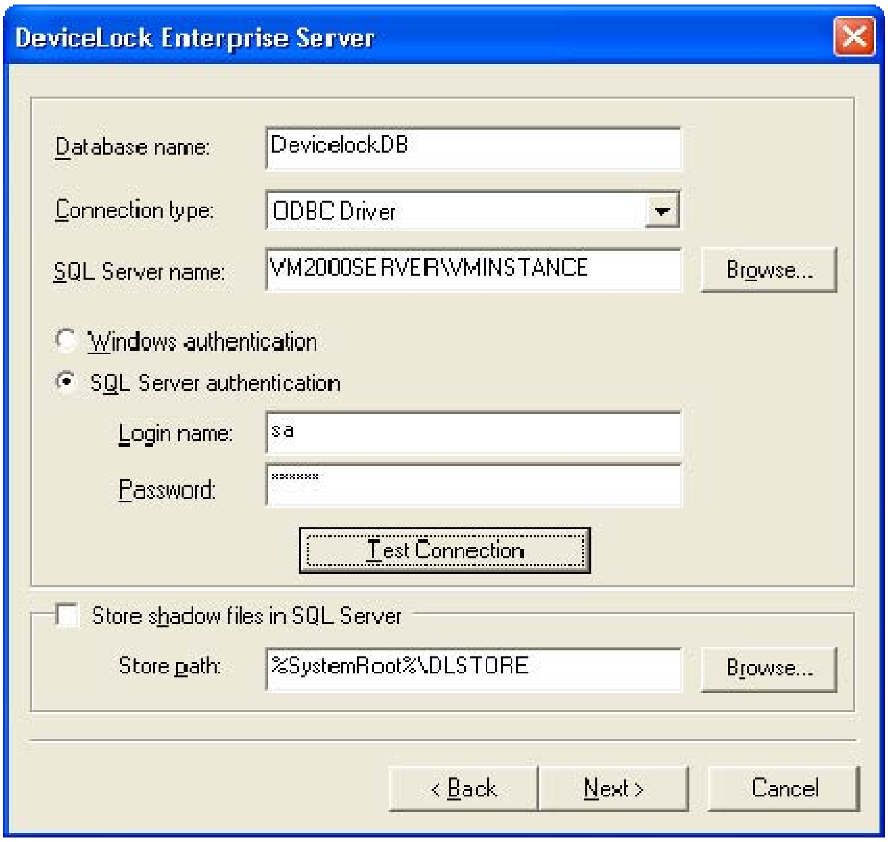
To load the license, press the *Load License(s)* button and select the license file.

You can load several license files in series – one by one.

If there are no valid licenses loaded, DeviceLock Enterprise Server works in the trial mode and can handle only two DeviceLock Services.

Press the *Next* button to install licenses and proceed to the fourth page.

On the fourth page, you can configure database parameters.



DeviceLock Enterprise Server

Database name: DevicelockDB

Connection type: ODBC Driver

SQL Server name: VM2000SERVER\VMINSTANCE

○ Windows authentication

● SQL Server authentication

Login name: sa

Password: ******

□ Store shadow files in SQL Server

Store path: %SystemRoot%\DLSTORE

4.1. Database name

You must specify the name of the database in SQL Server that will be used to store the DeviceLock Enterprise Server data. The default name suggested by the wizard is *DeviceLockDB*.

4.2. Connection type

There are two ways to define a connection to SQL Server:

a. *ODBC Driver* – you enter the name of SQL Server in *SQL Server name* and select the authentication mode (*Windows* or *SQL Server*).

   The *SQL Server name* parameter must contain not just the name of the computer where SQL Server is running but the name of SQL Server itself. Usually the SQL Server name consists of two parts: the computer name and the instance name divided by a backslash (e.g. *computer\instance*). Sometimes the instance name is empty (default) and you can use the computer name as an SQL Server name. To retrieve SQL Server names available in your local network, press the *Browse* button. (You should have access to the remote registry of the SQL Server machine to retrieve the instance name.)

   If the *SQL Server name* parameter is empty, it means that SQL Server is running on the same computer as DeviceLock Enterprise Server and has an empty (default) instance name.

To establish a connection to SQL Server, you must also configure authentication parameters.

Select the *Windows authentication* option to authenticate on SQL Server under the account used to run DeviceLock Enterprise Server's service.

If the service is running under the *SYSTEM* user and SQL Server is located on the remote computer, service will not be able to connect to SQL Server since the *SYSTEM* user doesn't have a right to access the network. For more information on how to run DeviceLock Enterprise Server on behalf of the user, please read the description of the Log on as parameter.

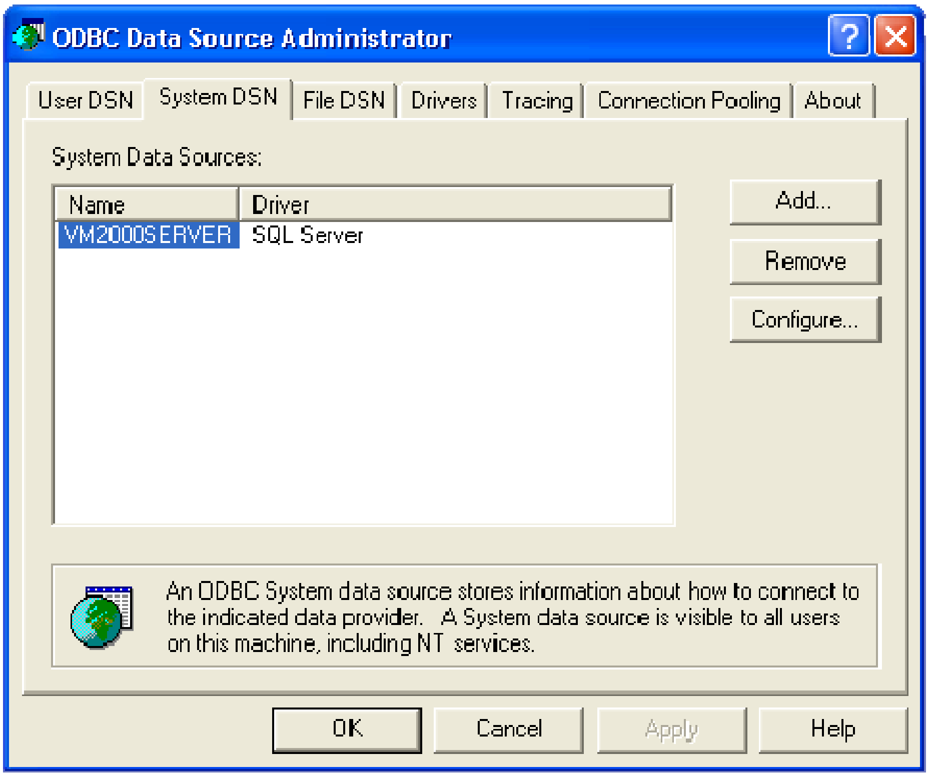
Select the *SQL Server authentication* option to allow SQL Server to perform the authentication itself by checking the login and password previously defined. Before selecting the *SQL Server authentication* option, make sure that your SQL Server was configured to use mixed-mode authentication.

Enter the SQL user name (login) in *Login name* and its password in *Password*.

***NOTE: Windows Authentication is much more secure than SQL Server Authentication. When possible, you should use Windows Authentication.***

b. *System Data Source* – you select the predefined system data source from the *Data Source Name* list.

To define data sources, use the *Data Sources (ODBC)* applet from *Control Panel -> Administrative Tools*.



System Data Sources:

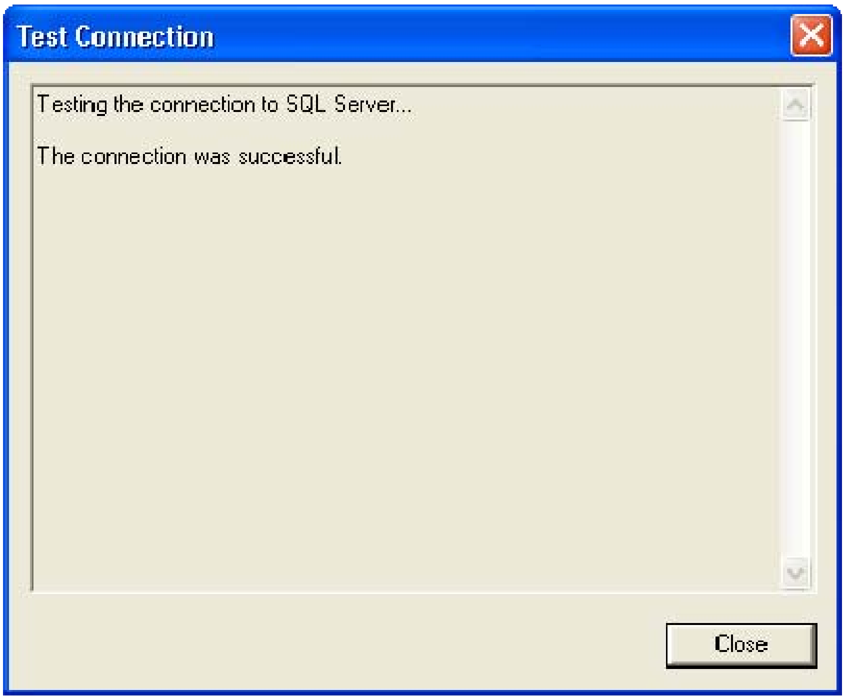
| Name | Driver |
|---|---|
| VM2000SERVER | SQL Server |

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

If, in the data source configuration, SQL Server Authentication was chosen, then you also need to specify the SQL user name (login) in *Login name* and its password in *Password*. If Windows Authentication was selected, then you should leave these fields blank.

To refresh the *Data Source Name* list, press the *Refresh* button.

When connection to SQL Server is defined you may want to test it. Press the *Test Connection* button to make sure that all the parameters were specified correctly.



Testing the connection to SQL Server...

The connection was successful.

Please note that it only checks connectivity and your access rights to SQL Server. If there are problems with the database or your access rights to this database, you don’t see those problems in the *Test Connection* dialog.

If some connection parameters were specified incorrectly, you may see one of these errors:

- *SQL Server does not exist or access denied* – you’ve specified an incorrect name of SQL Server in the *SQL Server name* parameter or the remote SQL Server’s computer is not accessible. It is possible that you’ve specified the name of the computer where SQL Server is running but this SQL Server also has an instance name which should be specified as well (e.g. *computer\instance*).

- *Login failed for user 'COMPUTER_NAME$'* – you’ve selected Windows Authentication but the user account  used to run the DeviceLock Enterprise Server service can’t get access to the computer with SQL Server. It may happen when the service starts either under the *SYSTEM* user or on behalf of a user that doesn’t have local administrative privileges on the remote SQL Server’s computer.

- *Login failed for user 'user_name'* – you've selected SQL Server Authentication and either specified an incorrect SQL user name (login) or the wrong password for it. Please note that SQL users are different from Windows users and you can't use the regular Windows account in the *Login name* parameter. SQL users exist only in SQL Server and to manage them you should use SQL Server management consoles (such as Microsoft SQL Server Management Studio).

- *Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection* – you've selected SQL Server Authentication but your SQL Server doesn't support this mode. You should either use Windows Authentication or allow your SQL Server to work in the mixed mode (SQL Server and Windows Authentication mode).

- *Login failed for user ''. The user is not associated with a trusted SQL Server connection* – the data source you've specified in *Data Source Name* was configured to use the SQL Server Authentication mode but the *Login name* parameter is empty.

- *Data source name not found and no default driver specified* – you've selected *System Data Source* from the *Connection type* list and specified either an empty or non-existent name in *Data Source Name*.

## 4.3. Store shadow files in SQL Server

There are two modes of storing binary data: data can be stored in SQL Server or it can be stored on the disk.

To store data in SQL Server, check the *Store shadow files in SQL Server* flag.

If you decided to store binary data in SQL Server, we recommend that you dramatically increase the maximum file size parameter for the transaction log of the database specified in *Database name*. Otherwise, SQL Server may fail to handle the large amount of data (hundreds of megabytes) in one transaction. Also, it is recommended that you increase the maximum amount of memory available for SQL Server and turn on the PAE (Physical Address Extension) feature.

For more information on how to tune up your SQL Server for storing large amounts of data, please read the article available at the Microsoft website: http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/rdbmspft.mspx.

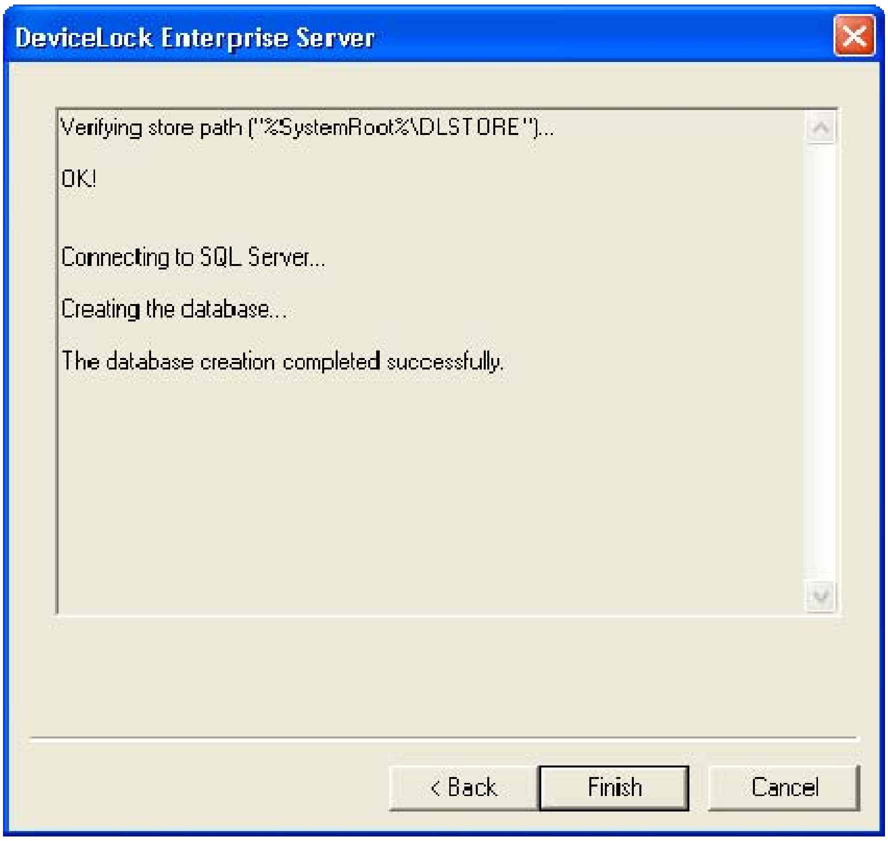
To store data on the disk, uncheck the *Store shadow files in SQL Server* flag. In this case only links to the binary data and some additional information are stored in SQL Server.

When stored on the disk, data files are located by the path specified in the *Store path* parameter. To choose the folder where files should be stored, you can use the *Browse* button.

You can also specify the network shared resource (e.g. *\\server\dlstore*) that will be used as storage. Make sure that the user account used to run the DeviceLock Enterprise Server service has full access to this network resource.

***NOTE: It is recommended to store binary data on the disk.***

Press the *Next* button to apply changes and proceed to the last page.



```
Verifying store path ("%SystemRoot%\DLSTORE")...

OK!


Connecting to SQL Server...

Creating the database...

The database creation completed successfully.
```

It takes some time to create the database specified in *Database name* if it does not exist on this SQL Server yet. If the database already exists and it has the proper format (i.e. was created by DeviceLock Enterprise Server) then DeviceLock Enterprise Server keeps all existing data and uses this database.

If some parameters on the previous wizard's page were specified incorrectly, you may see one of these errors:

- *[2] The system cannot find the file specified* – you've configured DeviceLock Enterprise Server to store binary data on the disk but the path specified in *Store path* is incorrect. If you've specified the shared network resource then it is possible that this network resource is not accessible.

- *Failed to verify store path. [5] Access is denied* – the path specified in the *Store path* parameter is correct, but the user account used to run the DeviceLock Enterprise Server service doesn't have full access to files by this path.

- *CREATE DATABASE permission denied in database 'name'* – the user's account (login) used to connect to SQL Server doesn't have enough privileges to create the database. The login should have at least the *dbcreator* Server role (see *Server Roles* in *Login Properties* of Microsoft SQL Server Management Studio).

- *The server principal "user_name" is not able to access the database "name" under the current security context* – the user's account (login) used to connect to SQL Server doesn't have access to the existing database. The login should be mapped to this database (see *User Mapping* in *Login Properties* of Microsoft SQL Server Management Studio).

- *SELECT permission denied on object 'name', database 'name', schema 'name'* – the user's account (login) used to connect to SQL Server doesn't have read/write access to the existing database. The login should have at least *db_datareader* and *db_datawriter* Database roles (see *User Mapping* in *Login Properties* of Microsoft SQL Server Management Studio).

- *Invalid object name 'name'* – the database specified in the *Database name* parameter already exists in this SQL Server but has an incorrect format. It happens when you are trying to use the database that was not created by DeviceLock Enterprise Server or if the database was corrupted.

- *DeviceLock Database has an unsupported format* – the database specified in the *Database name* parameter already exists but is outdated. This existing database has an unsupported format so it can't be automatically upgraded to the new format. You should either use another database or create a new one.

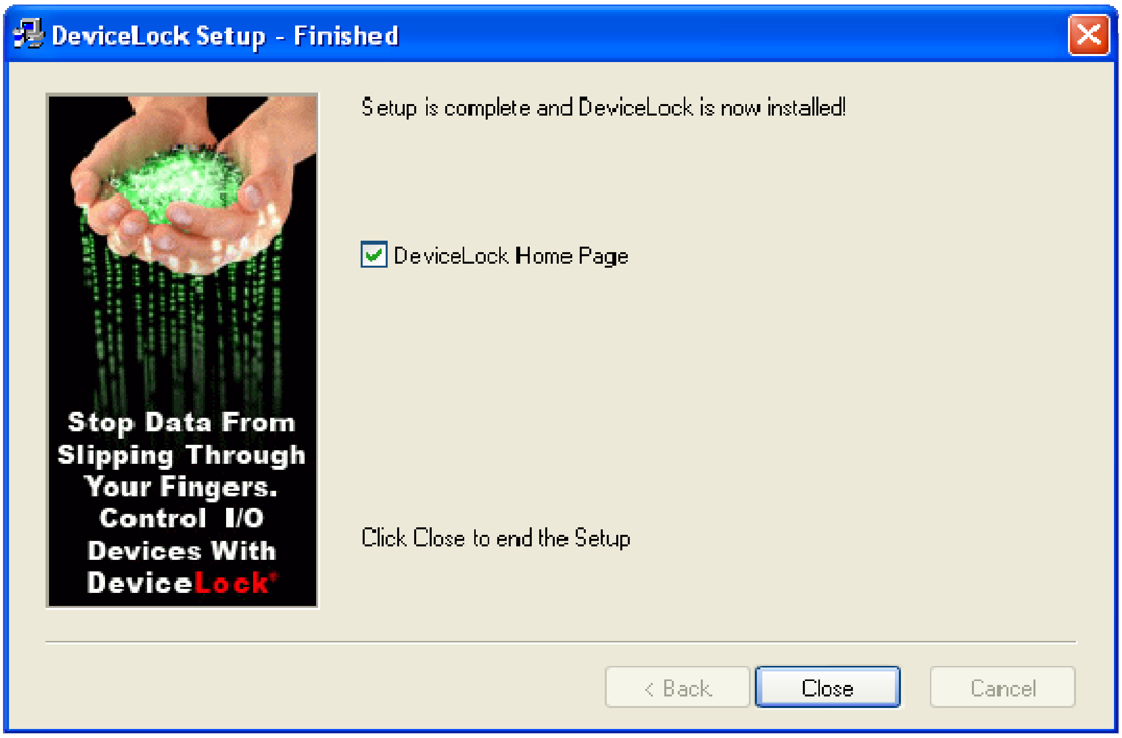
- *DeviceLock Database has a format that is not supported by the current server version* – the database specified in the *Database name* parameter already exists but it was created by the more recent version of DeviceLock Enterprise Server. You should either use the latest version of DeviceLock Enterprise Server or use another database (or create a new one).

Also, some of the SQL Server connection errors described above may be displayed here as well.

Use the *Back* button to return to the previous page and make necessary changes.

If there are no errors, press the *Finish* button to close the wizard and continue the installation process.

As soon as Setup has installed DeviceLock, it prompts you to point your default Internet browser to the DeviceLock website.



DeviceLock Setup - Finished

Setup is complete and DeviceLock is now installed!

☑ DeviceLock Home Page

Click Close to end the Setup

Uncheck the *DeviceLock Home Page* flag if you do not want to visit the DeviceLock website. Press the *Close* button to finish the installation.

# 3 DeviceLock Certificates

## 3.1 Overview

DeviceLock Certificate is a cryptographic certificate that consists of two keys (the key pair): *private* and *public*:

- The *private* key must be stored on the administrator's computer and only the administrator must be able to access it. Also, the *private* key may be installed on DeviceLock Enterprise Server. ***NOTE: Make sure that non-administrative users can't get access to the private key.***

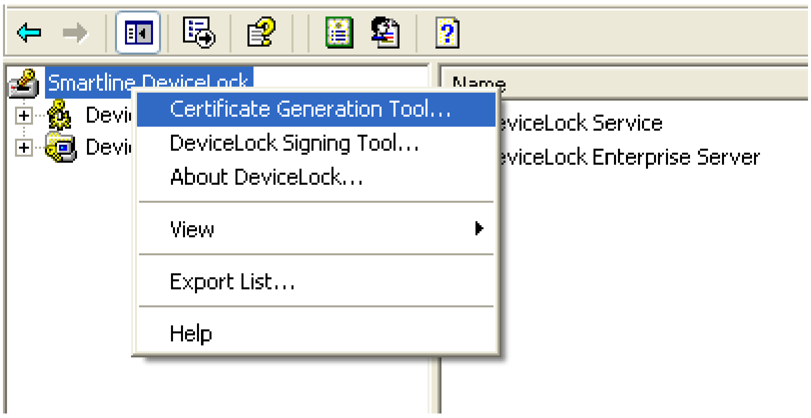
- The *public* key is installed on every computer where DeviceLock Service is running. If the *public* key has not been preinstalled on the user's computer, there is no way to use the Temporary White List function or DeviceLock Certificate authentication on DeviceLock Enterprise Server.

## 3.2 Generating DeviceLock Certificates

DeviceLock's Certificate Generation Tool allows you to generate DeviceLock Certificates.

We recommend that you generate only one DeviceLock Certificate and deploy its *public* key to all user computers. It is necessary to generate and install a new certificate only if the *private* key was either compromised (e.g. stolen) or lost.

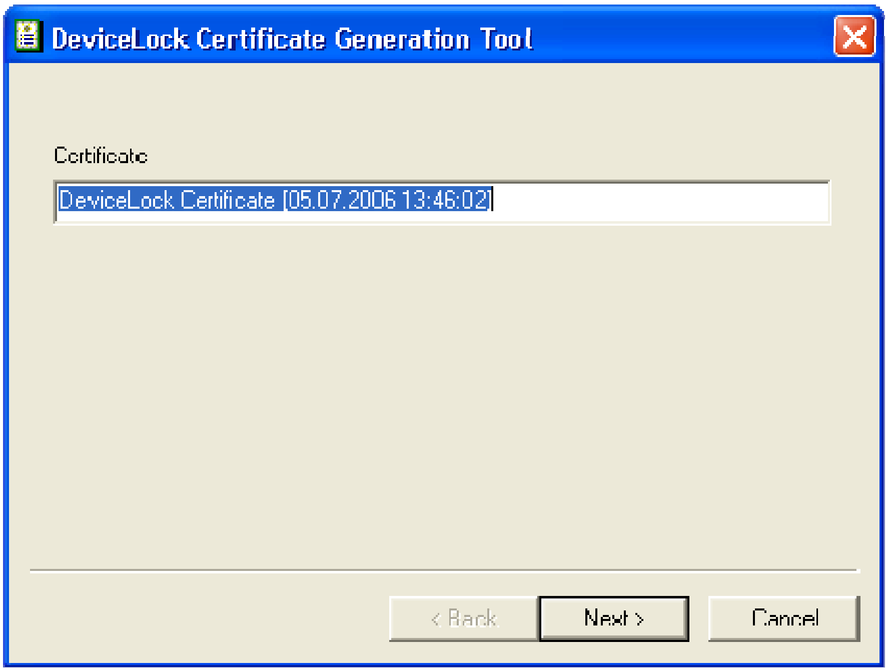
To run the Certificate Generation Tool, select the *Certificate Generation Tool* item from the *File* menu in DeviceLock Enterprise Manager. To run the Certificate Generation Tool from DeviceLock Management Console (the MMC snap-in) and DeviceLock Group Policy Manager, use the context menu available by a right mouse click.



The Certificate Generation Tool will run automatically when DeviceLock management consoles are installed on an administrator's computer that has no DeviceLock Certificate.

There are two simple steps to generate the key pair:

1. Define the name of the DeviceLock Certificate.

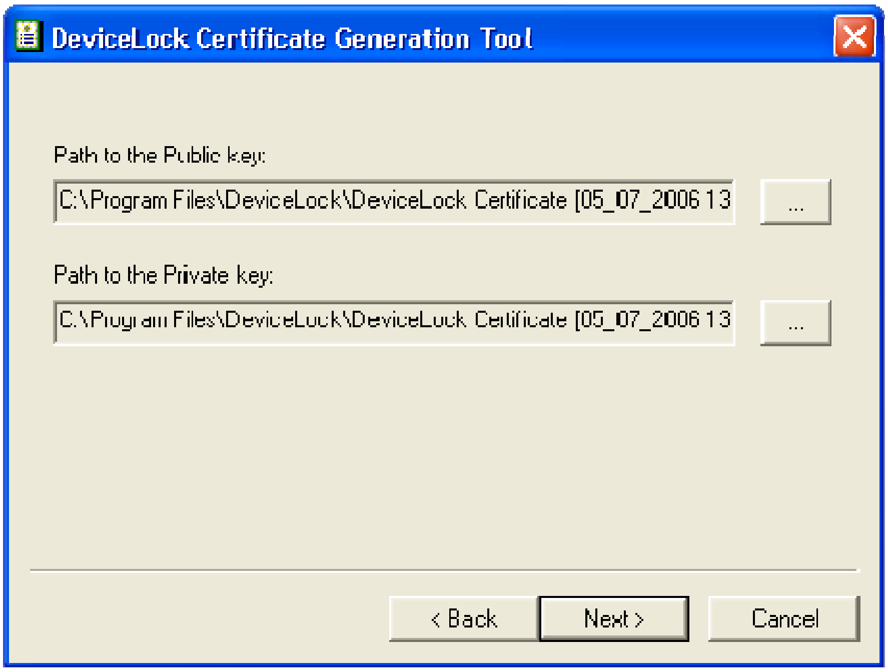


Certificate

DeviceLock Certificate [05.07.2006 13:46:02]

The Certificate Generation Tool auto-generates a name based on the current date and time, but you can type any other name.

2. Define the path and file names for *private* and *public* keys.



Path to the Public key:

C:\Program Files\DeviceLock\DeviceLock Certificate [05_07_2006 13

Path to the Private key:

C:\Program Files\DeviceLock\DeviceLock Certificate [05_07_2006 13

As soon as the DeviceLock Certificate is generated, you can start deploying the *public* key to users' computers.

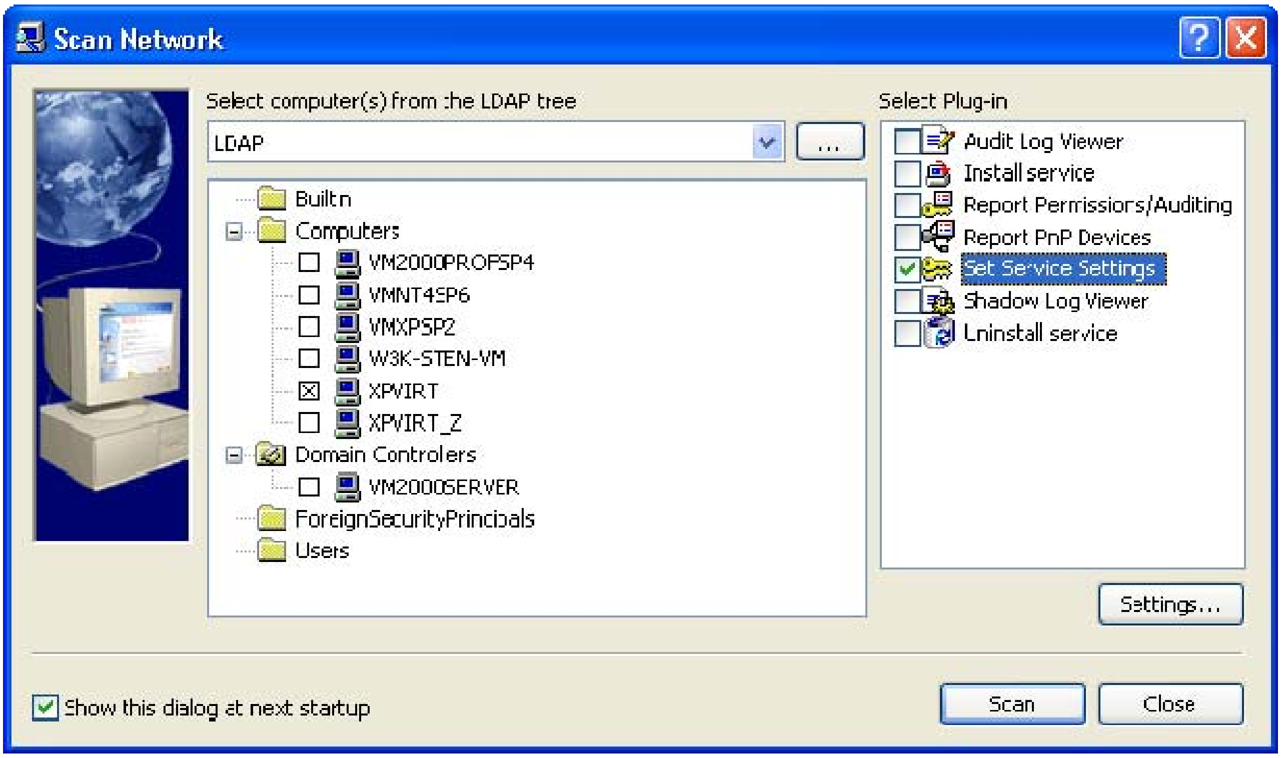
***NOTE: A newly generated DeviceLock Certificate does not automatically install on computers from the Certificate Generation Tool. You must deploy it manually from a DeviceLock management console.***

## 3.3 Installing/Removing DeviceLock Certificate

To install/remove the *public* key on/from user computers running DeviceLock Services, you can use any DeviceLock management console:

a. <u>DeviceLock Enterprise Manager</u>

On the *Scan Network* dialog, select the computers targeted for installation/removal of the *public* key and select the *Set Service Settings* plug-in.



Scan Network

Select computer(s) from the LDAP tree

LDAP

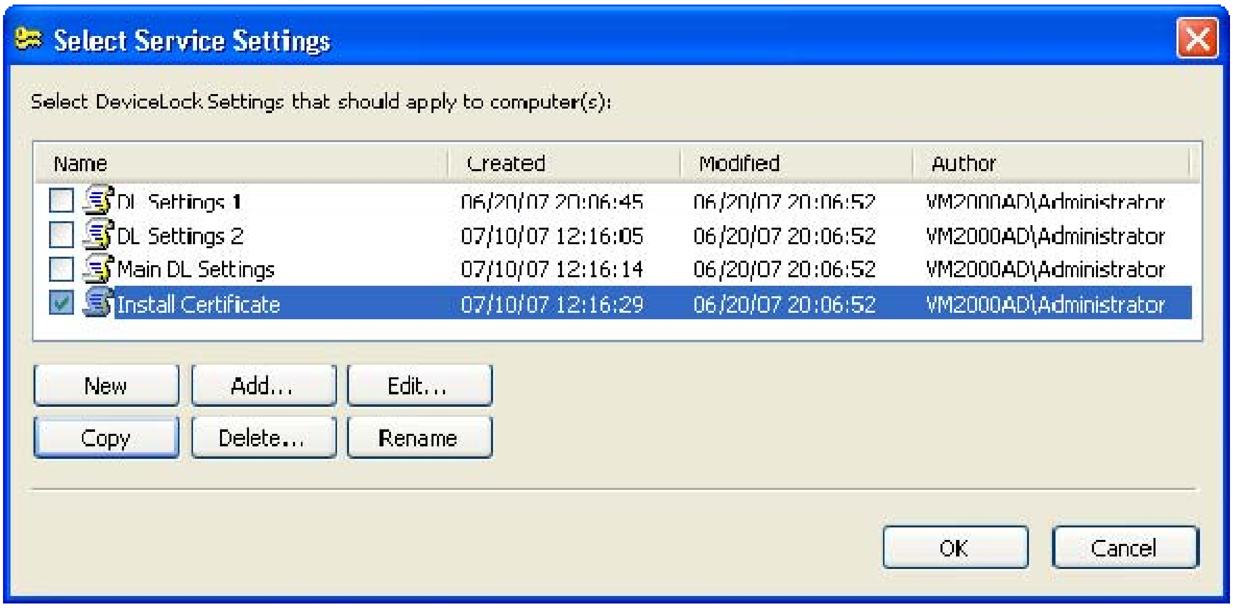
- Builtin
- Computers
  - □ VM2000PROFSP4
  - □ VMNT4SP6
  - □ VMXPSP2
  - □ W3K-STEN-VM
  - ☒ XPVIRT
  - □ XPVIRT_Z
- Domain Controllers
  - □ VM2000SERVER
- ForeignSecurityPrincipals
- Users

Select Plug-in

- □ Audit Log Viewer
- □ Install service
- □ Report Permissions/Auditing
- □ Report PnP Devices
- ☑ Set Service Settings
- □ Shadow Log Viewer
- □ Uninstall service

☑ Show this dialog at next startup

Press the *Settings* button or double-click on the plug-in's record to open the configuration dialog.



Select Service Settings

Select DeviceLock Settings that should apply to computer(s):

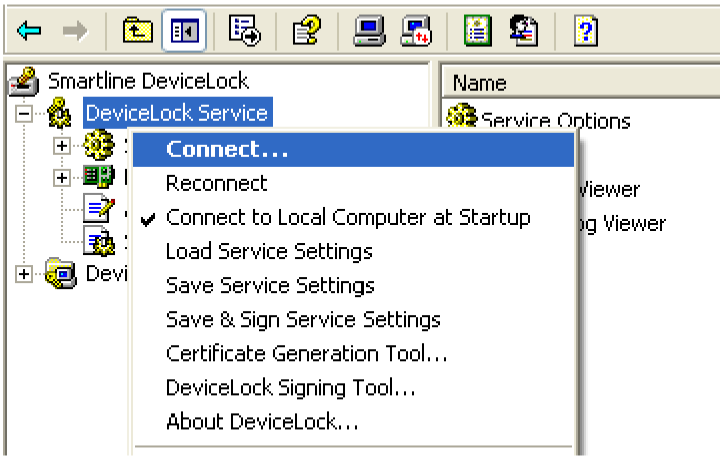
| Name | Created | Modified | Author |
|---|---|---|---|
| □ DL Settings 1 | 06/20/07 20:06:45 | 06/20/07 20:06:52 | VM2000AD\Administrator |
| □ DL Settings 2 | 07/10/07 12:16:05 | 06/20/07 20:06:52 | VM2000AD\Administrator |
| □ Main DL Settings | 07/10/07 12:16:14 | 06/20/07 20:06:52 | VM2000AD\Administrator |
| ☑ Install Certificate | 07/10/07 12:16:29 | 06/20/07 20:06:52 | VM2000AD\Administrator |

Create the new XML file or use the existing one to define the policy needed to install/remove the certificate. Highlight the file in the list and then press the *Edit* button to modify the policy as described in the next section (below). When finished modifying the policy, select its file by enabling the checkmark next to the file's name in the list.

Press the *OK* button to close the configuration dialog and then press the *Scan* button on the *Scan Network* dialog to start the DeviceLock Certificate installation/removal process.

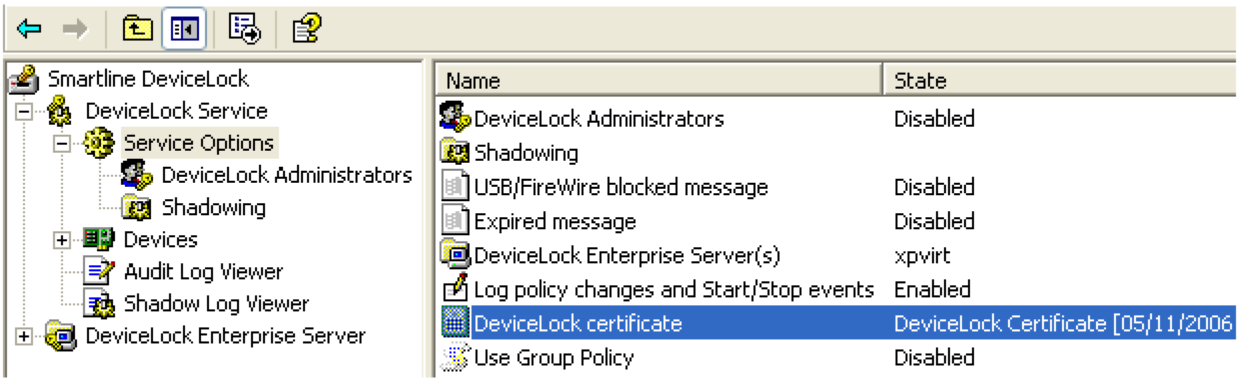
b. DeviceLock Management Console, DeviceLock Group Policy Manager and DeviceLock Service Settings Editor

If you are using DeviceLock Management Console (the MMC snap-in), first you need to connect it to the computer running DeviceLock Service. Use the context menu available by a right mouse click.



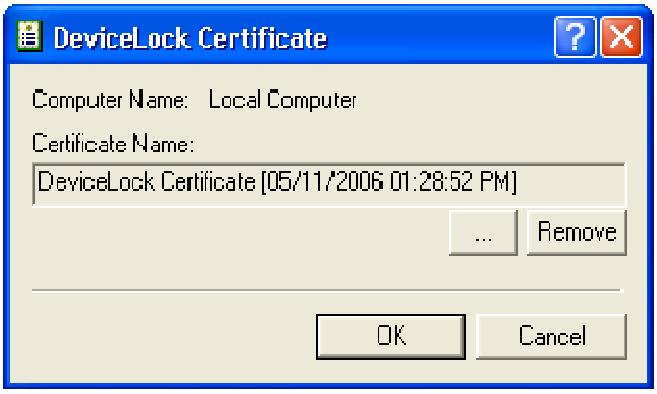
When DeviceLock Group Policy Manager is used, you don't need to connect to any computer since it connects to the Group Policy Object. Also, you don't need to connect to the computer when modifying the policy in the XML file using DeviceLock Service Settings Editor.

Activate the *Service Options* item.



| Name | State |
|---|---|
| DeviceLock Administrators | Disabled |
| Shadowing | |
| USB/FireWire blocked message | Disabled |
| Expired message | Disabled |
| DeviceLock Enterprise Server(s) | xpvirt |
| Log policy changes and Start/Stop events | Enabled |
| DeviceLock certificate | DeviceLock Certificate [05/11/2006 |
| Use Group Policy | Disabled |

Double-click the *DeviceLock certificate* parameter to open the configuration dialog.



Computer Name: Local Computer

Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

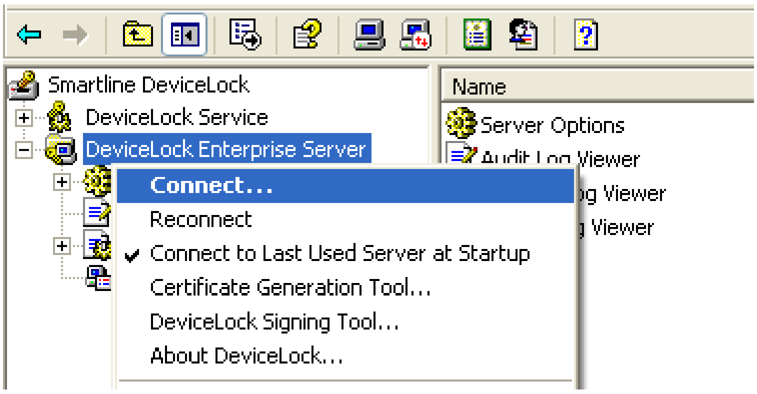
Specify the path to the *public* key in the *Certificate Name* parameter if you want to install the certificate. You can use the **...** button to select the file with a *public* key.

To remove the *public* key, use the *Remove* button.

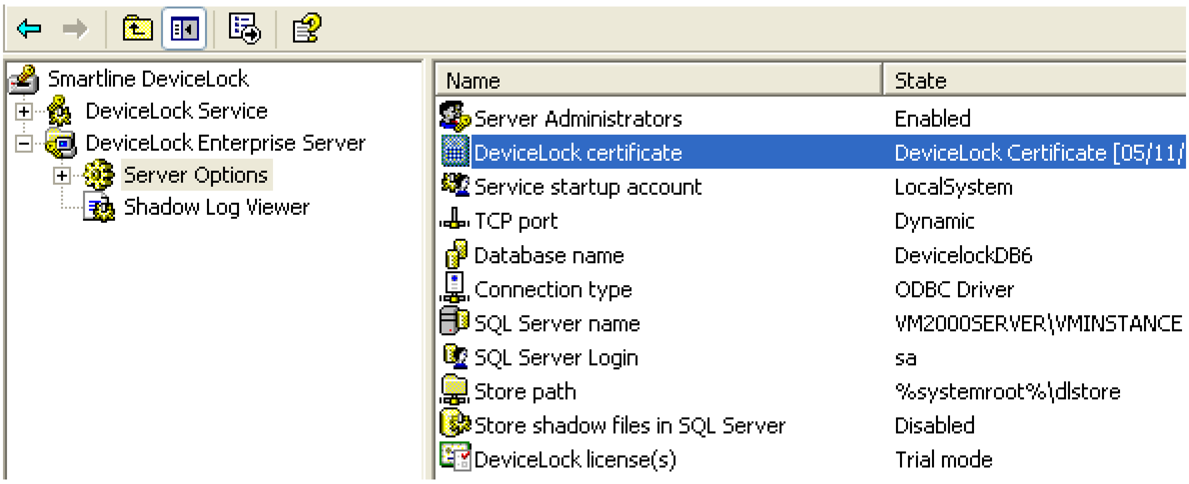
Press the OK button to close the configuration dialog and apply changes.

To install/remove the *private* key on/from DeviceLock Enterprise Server, you can use DeviceLock Management Console (the MMC snap-in).

You need to connect DeviceLock Management Console to the computer running DeviceLock Enterprise Server. Use the context menu available by a right mouse click.

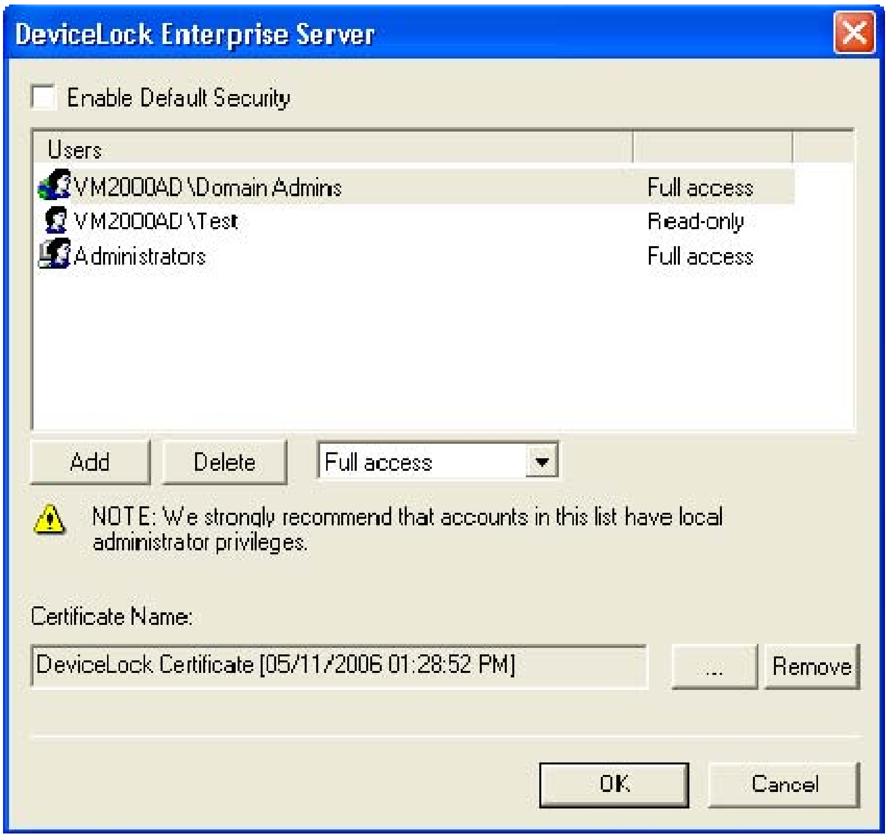

Smartline DeviceLock
DeviceLock Service
DeviceLock Enterprise Server
Name
Server Options
Audit Log Viewer
g Viewer
Viewer
Connect...
Reconnect
✓ Connect to Last Used Server at Startup
Certificate Generation Tool...
DeviceLock Signing Tool...
About DeviceLock...

Activate the *Server Options* item.



| Name | State |
|---|---|
| Server Administrators | Enabled |
| DeviceLock certificate | DeviceLock Certificate [05/11/ |
| Service startup account | LocalSystem |
| TCP port | Dynamic |
| Database name | DevicelockDB6 |
| Connection type | ODBC Driver |
| SQL Server name | VM2000SERVER\VMINSTANCE |
| SQL Server Login | sa |
| Store path | %systemroot%\dlstore |
| Store shadow files in SQL Server | Disabled |
| DeviceLock license(s) | Trial mode |

Double-click the *DeviceLock certificate* parameter to open the configuration dialog.



DeviceLock Enterprise Server

□ Enable Default Security

| Users | |
|---|---|
| VM2000AD\Domain Admins | Full access |
| VM2000AD\Test | Read-only |
| Administrators | Full access |

Full access

NOTE: We strongly recommend that accounts in this list have local administrator privileges.

Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

Specify the path to the *private* key in the *Certificate Name* parameter if you want to install the certificate. You can use the **...** button to select the file with a *private* key.

To remove the *private* key, use the *Remove* button.

Press the OK button to close the configuration dialog and apply changes.

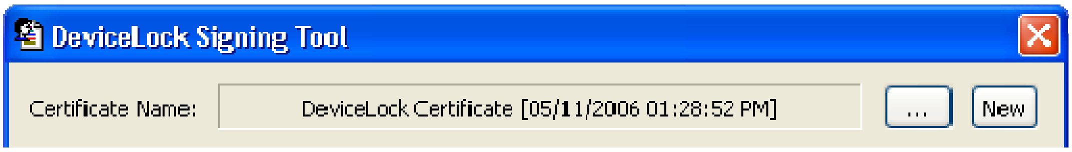
For more information regarding installing the *private* key on DeviceLock Enterprise Server, please read the **Installing DeviceLock Enterprise Server** section of this manual.

# 4 DeviceLock Signing Tool

## 4.1 Overview

The DeviceLock Signing Tool is used to grant users temporary access to requested devices and sign XML files containing DeviceLock Service settings exported from DeviceLock Management Console or DeviceLock Group Policy Manager.

To run the DeviceLock Signing Tool, select *DeviceLock Signing Tool* from the *File* menu in DeviceLock Enterprise Manager or from the context menu in DeviceLock Management Console (the MMC snap-in), DeviceLock Group Policy Manager or DeviceLock Service Settings Editor.



Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

First of all you should load the corresponding DeviceLock Certificate (the *private* key).

The DeviceLock Signing Tool must use the *private* key that belongs to the same certificate as the *public* key installed on the user's computer.

By default, the DeviceLock Signing Tool automatically loads the last certificate used. You can load another certificate by pressing the **...** button and selecting a file with the *private* key.

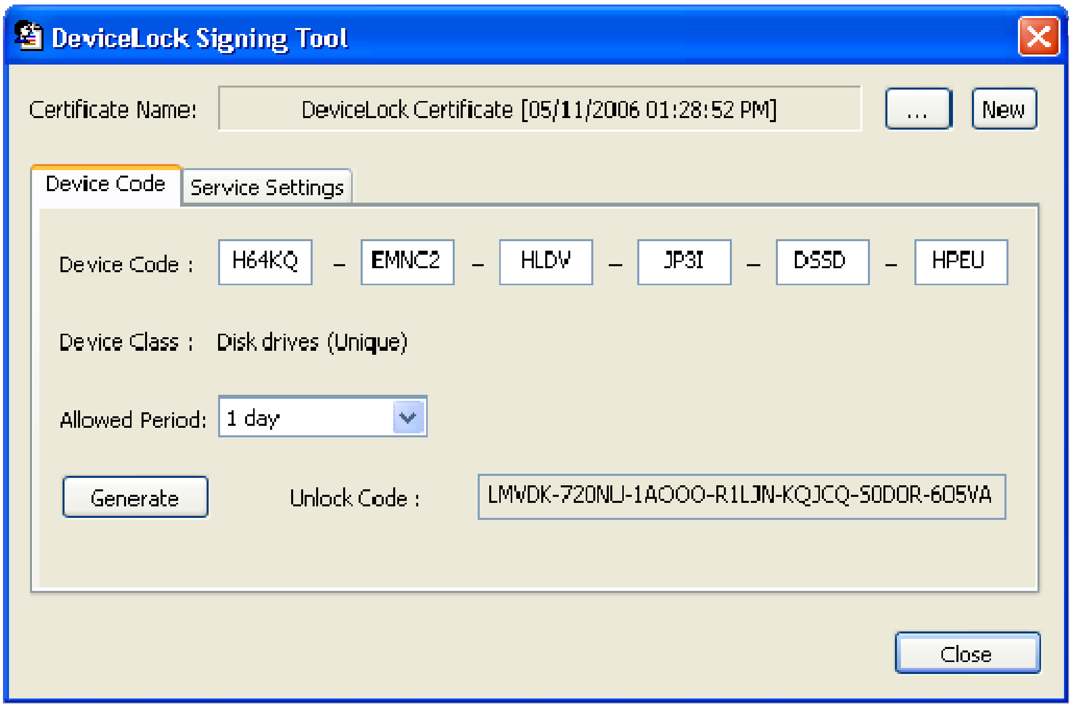
To generate the new certificate you can run the Certificate Generation Tool directly from the DeviceLock Signing Tool. To do so, you should press the *New* button. However, please keep in mind that if you generate a new certificate and intend to use its new *private* key in the DeviceLock Signing Tool, you must also deploy the corresponding *public* key on the user's computer.

Then, decide what action you want to perform: generate an **Unlock Code** or sign an XML file containing DeviceLock Service settings.

## 4.2 Device Code

To grant the user temporary access to a requested device you should generate an **Unlock Code** upon receiving the **Device Code** from this user.

For more information on using temporary white list, please read the **Temporary White List** section of this manual.



Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

Device Code : H64KQ – EMNC2 – HLDV – JP3I – DSSD – HPEU

Device Class : Disk drives (Unique)

Allowed Period: 1 day

Unlock Code : LMVDK-720NU-1AOOO-R1LJN-KQJCQ-S0D0R-605VA

There are four simple steps to generating an **Unlock Code** for the user:

1. Load the corresponding DeviceLock Certificate (*see above*)

2. Enter the **Device Code**, the user provides to you.

   As soon as the correct **Device Code** is entered, you can see the class of the device the user wants access to in the *Device Class* field. The device class information helps you to control what kind of device the user is going to use. If, for example, a user tells the administrator that he/she is going to use a USB scanner but actually is trying to obtain access to a USB flash drive, the administrator would recognize the discrepancy.

   There is also a field (in round brackets) showing whether the requested device can be authorized as a unique device (*Unique*) or can be authorized only as a model (*Model*), i.e. whether or not it has a serial number. If you authorize the device as a model, then the user is granted access to all devices of this model. For more information on this, please read the **USB Devices White List** section of this manual.

3. Select the period when the requested device will be allowed. In *Allowed Period*, you can select several predefined periods: 5, 15, 30, 60 minutes, 5 hours, 1 or 2 days, 1 or 2 weeks, 1 month or until the device is unplugged.

   When you select a fixed time period (e.g. 10 minutes), the user is granted access to the requested device for only this period. As soon as the allowed time expires, access to the device is denied again. It doesn't matter what the user is doing with this device – even if he/she is still copying files onto the USB disk or printing a document on the USB printer, all operations will be aborted.

To allow the user to use a requested device without any time limitations, select *until unplug* in *Allowed Period*. The user is then granted access to the device while it is plugged into the port. As soon as the user unplugs this device, access to it is denied again.

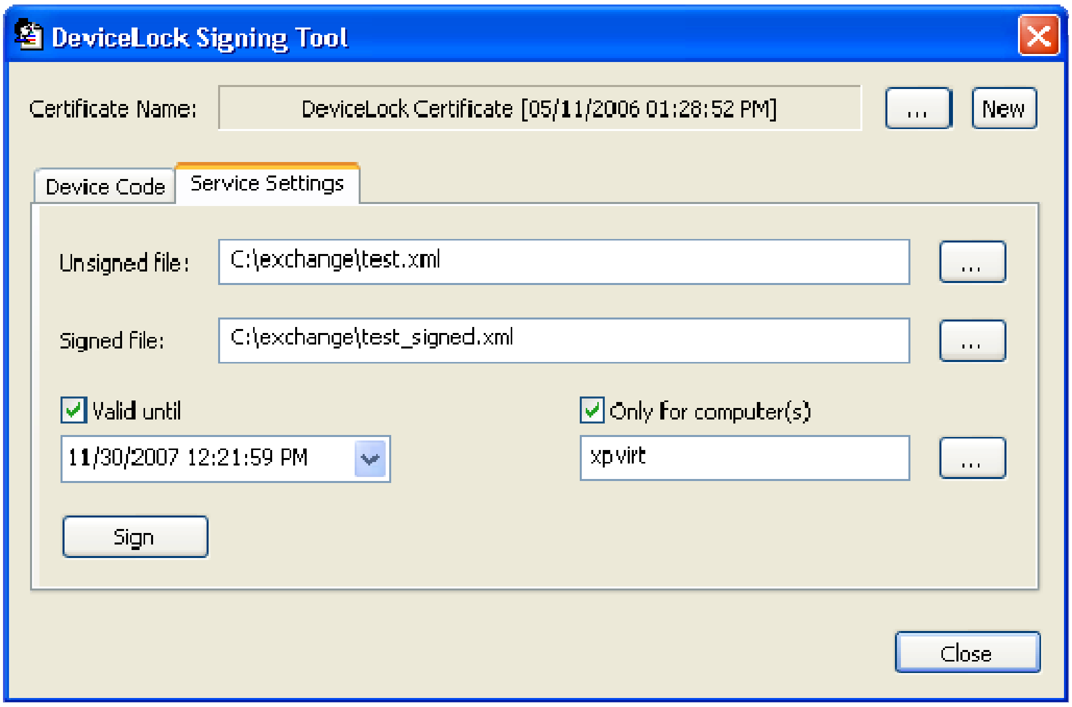
4. Press the *Generate* button to create an **Unlock Code**. Provide this code to the user over the phone or in any other suitable way.

   The process of generating an **Unlock Code** can be a time-consuming operation. It depends on your computer's processing speed and could take as long as several seconds.

## 4.3 Service Settings

To avoid unauthorized modification you can sign an XML file containing DeviceLock Service settings exported from DeviceLock Management Console or DeviceLock Group Policy Manager or created using DeviceLock Service Settings Editor.

Later this file can be sent to users whose computers are not online and thus out-of-reach via management consoles.



Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

Unsigned file: C:\exchange\test.xml

Signed File: C:\exchange\test_signed.xml

☑ Valid until 11/30/2007 12:21:59 PM

☑ Only for computer(s) xpvirt

There are six simple steps to signing an XML file:

1. Load the corresponding DeviceLock Certificate (see above)

2. Load the file with DeviceLock Service settings you need to sign.

   The full path to this file must be specified in the *Unsigned file* field. You can use the **…** button to select the file.

The XLM file with DeviceLock Service settings can be created using *Save Service Settings* from the context menu in DeviceLock Management Console, DeviceLock Group Policy Manager or DeviceLock Service Settings Editor.

3. In the *Signed file* field, specify the resultant file. You can use the **…** button to select the folder where this file will be created.

4. Decide whether the resultant file should contain expiration information or not.

   If you want to allow users to import settings from this file without any time limitations, disable the *Valid until* flag.

   If you enable the *Valid until* flag and specify the date/time, then the expiration information writes to the resultant file and users can import settings from this file only before the specified date/time.

   Please note that this parameter affects only users that are trying to import DeviceLock Service settings via the *DeviceLock* applet from the Windows *Control Panel*. When an XML file with settings is loaded using *Load Service Settings* from the context menu in DeviceLock Management Console or DeviceLock Group Policy Manager, the expiration information (if any) is ignored.

5. Decide whether the resultant file can be used only on specific computers or not.

   If you want to allow users to import settings from this file on any computers, disable the *Only for computer(s)* flag.

   If you enable the *Only for computer(s)* flag and specify the computer name then users will be able to import settings from this file only on this specified computer. Using the semicolon (;) as a separator, you can specify several computer names such that the resultant file can be used on any of these computers.

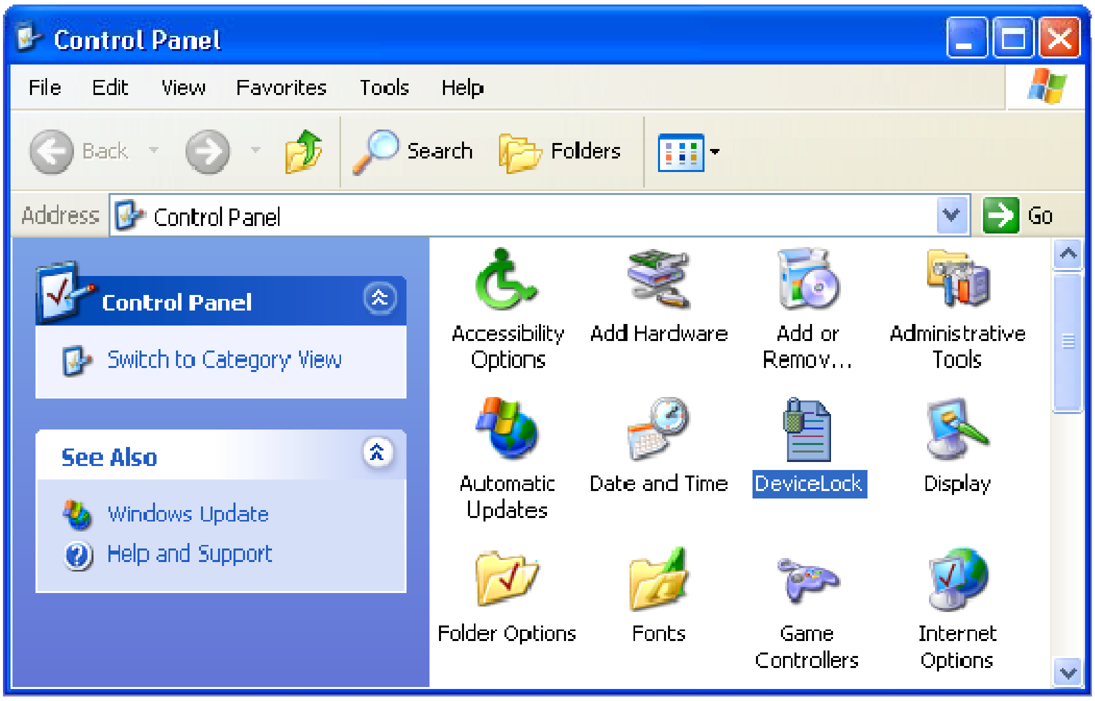
   ***NOTE: You can't use the computer's IP address in this parameter. You must specify the computer name exactly as it is displayed in the System applet from the Windows Control Panel.***

   You can also load a predefined list of computers from the external text file. To open an external file, press the **…** button. This text file must contain each computer's name on separate lines.

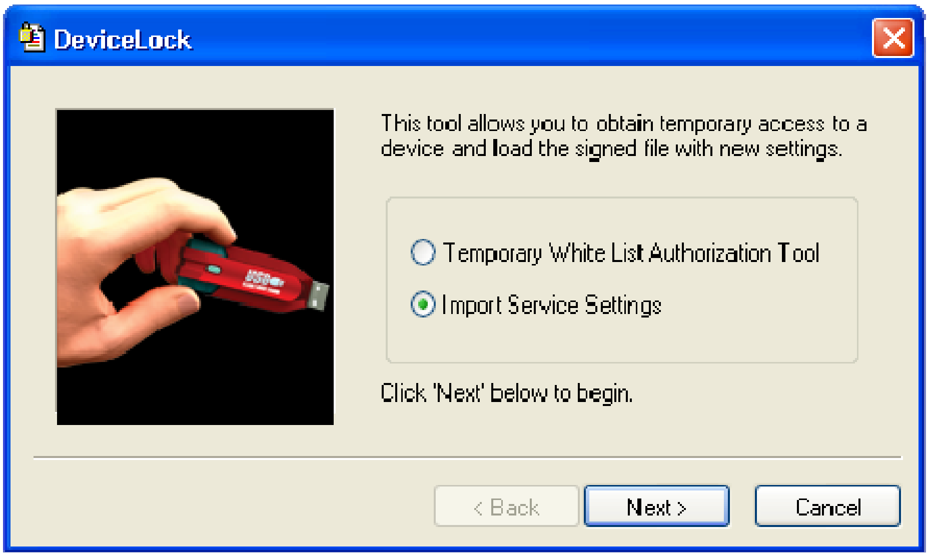
   Please note that this parameter affects only users that are trying to import DeviceLock Service settings via the *DeviceLock* applet from the Windows *Control Panel*. When an XML file with settings is loaded using *Load Service Settings* from the context menu in DeviceLock Management Console or DeviceLock Group Policy Manager, the computer's name information is ignored.

6. Press the *Sign* button to create a signed file with DeviceLock Service settings. Provide this file to the user in any suitable way.
   The process of file signing can be a time-consuming operation. It depends on your computer's processing speed and could take as long as several seconds.

When the user wants to apply DeviceLock Service settings from this signed file, he/she should run the *DeviceLock* applet from the *Control Panel* and select the *Import Service Settings* option.



***NOTE: On Windows XP and later, the user must switch the Control Panel to Classic View in order to view all available applets.***



This tool allows you to obtain temporary access to a device and load the signed file with new settings.

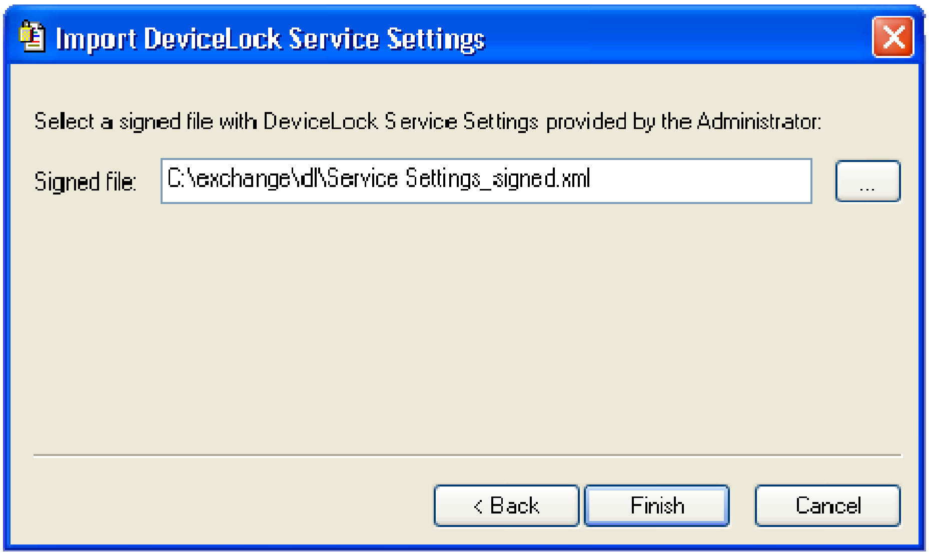
○ Temporary White List Authorization Tool

● Import Service Settings

Click 'Next' below to begin.

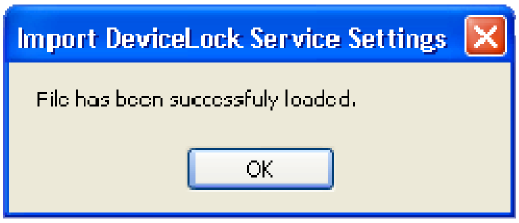
There are two simple steps for the user to import DeviceLock Service settings from the signed file:

1. In the *Signed file* field, specify the full path to this signed file. Use the **...** button to select the file.



Import DeviceLock Service Settings
Select a signed file with DeviceLock Service Settings provided by the Administrator:
Signed file:
C:\exchange\dl\Service Settings_signed.xml
...
< Back
Finish
Cancel

2. Press the *Finish* button. If the digital signature in the file is valid, then the new settings will be applied to DeviceLock Service immediately.



Import DeviceLock Service Settings
File has been successfuly loaded.
OK

The user can also load the signed file with DeviceLock Service settings using the command line:

*DLTempAccess.cpl -s <path to signed file>*

where *<path to signed file>* is the path to the signed file with DeviceLock Service settings. For example:

*DLTempAccess.cpl -s “C:\Program Files\DeviceLock\settings_signed.dls”*

All successfully attempts to load settings are logged, if logging of changes is enabled in the Service Options.

# 5 DeviceLock Management Console

## 5.1 Overview

DeviceLock Management Console is a snap-in for Microsoft Management Console (MMC).

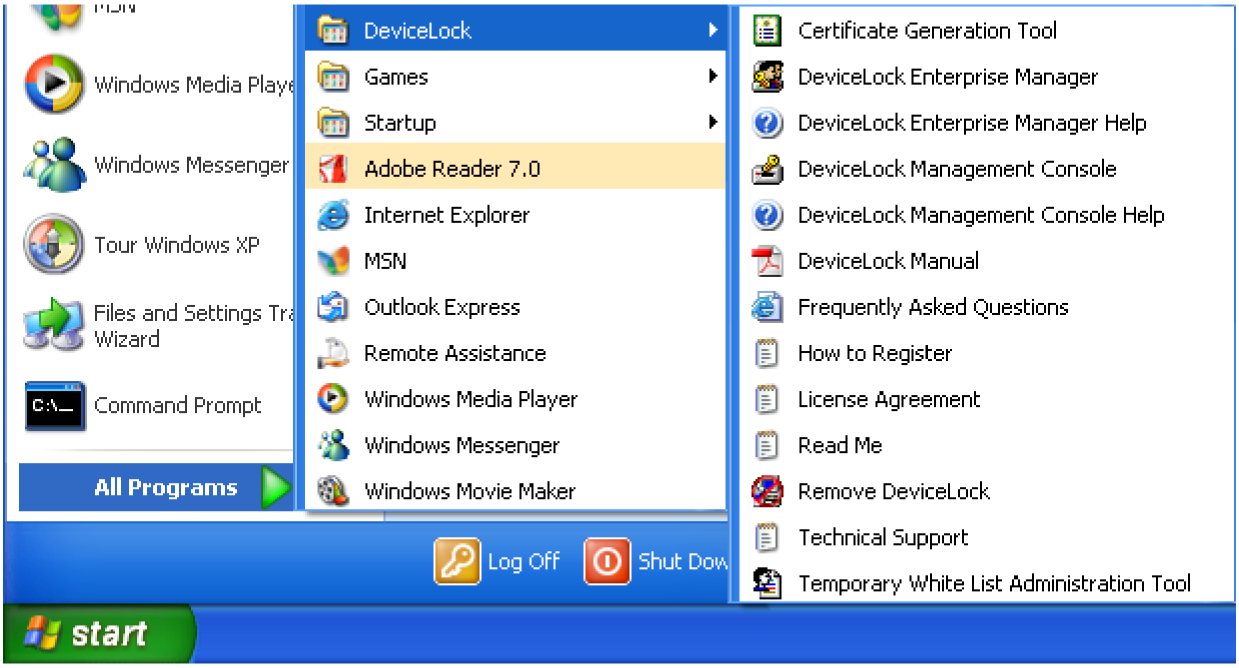
Using DeviceLock Management Console, you can view and change permissions and audit rules, install and update DeviceLock Service as well as view audit records for individual computers.

Also, DeviceLock Management Console is used for viewing logs stored on DeviceLock Enterprise Server and for managing this server.

DeviceLock Management Console should be used on the computer from which the administrator is managing DeviceLock Services and DeviceLock Enterprise Servers in the network.

For information on how to install DeviceLock Management Console, please read the **Installing Management Consoles** section of this manual.

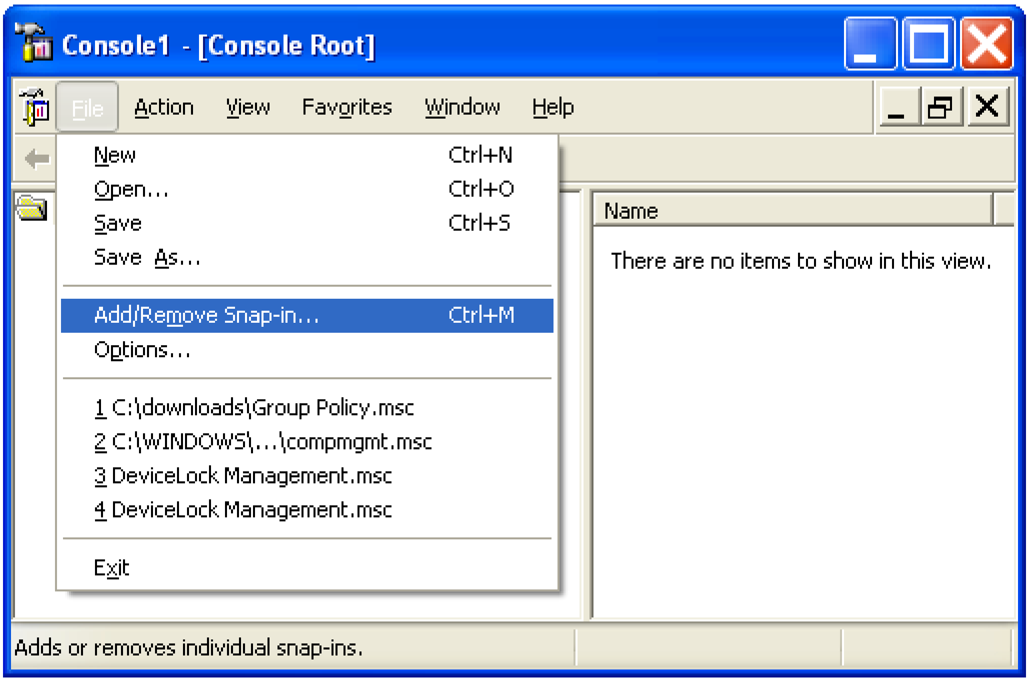
To run DeviceLock Management Console, select the appropriate shortcut from the *Programs* menu available by clicking the Windows *Start* button.



Alternatively, you can start MMC and add the DeviceLock Management Console snap-in manually:

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

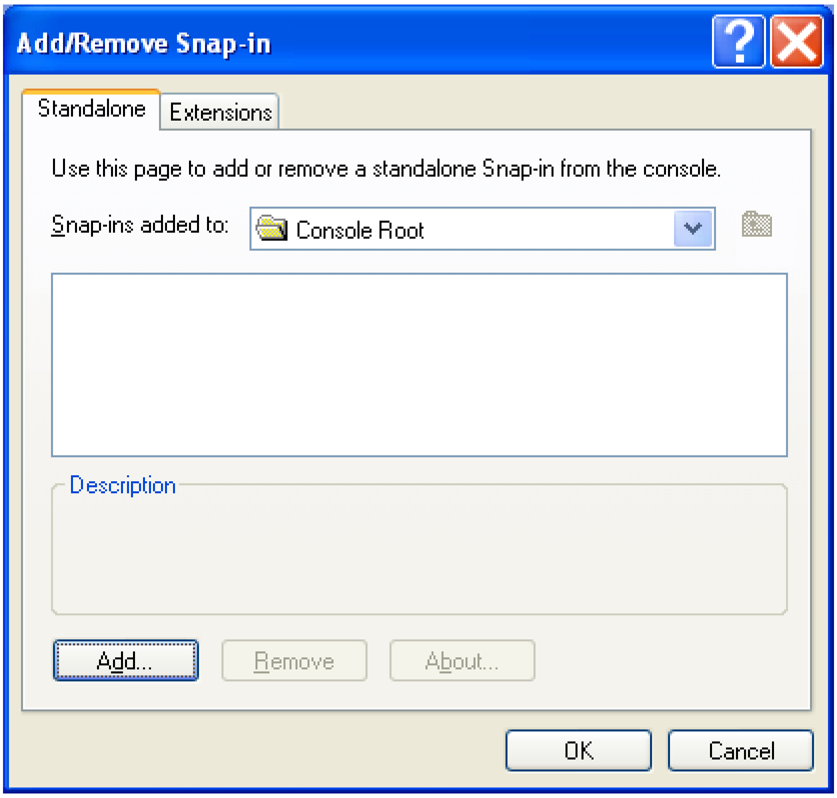
2. Open the *File* menu, and then click *Add/Remove snap-in*.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\downloads\Group Policy.msc
2 C:\WINDOWS\...\compmgmt.msc
3 DeviceLock Management.msc
4 DeviceLock Management.msc
Exit
Name

There are no items to show in this view.

Adds or removes individual snap-ins.

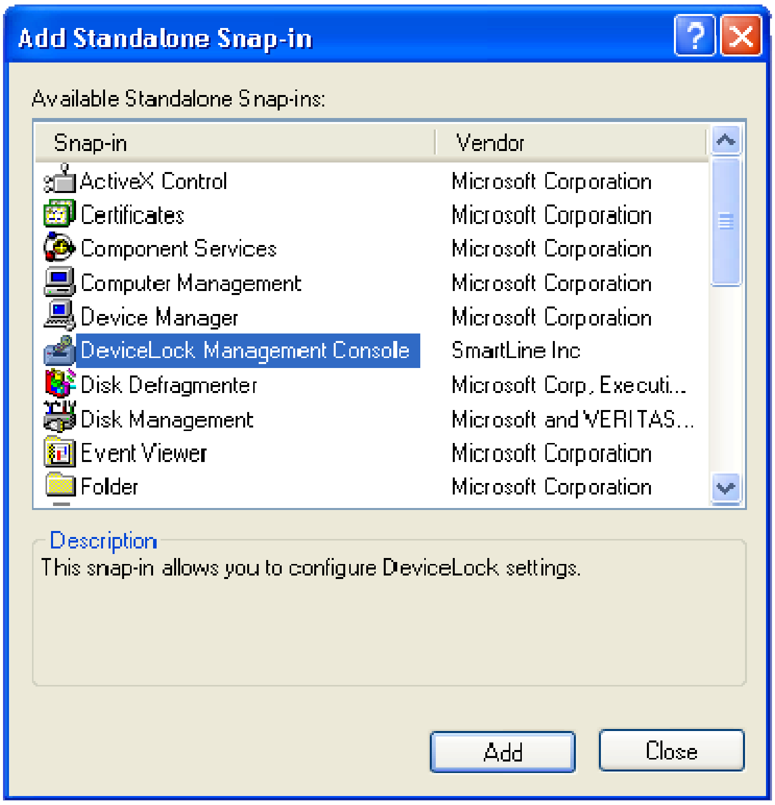
3. Click the *Standalone* tab, and then click *Add*.



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

4. Select *DeviceLock Management Console* from the list, then click *Add*.



Available Standalone Snap-ins:

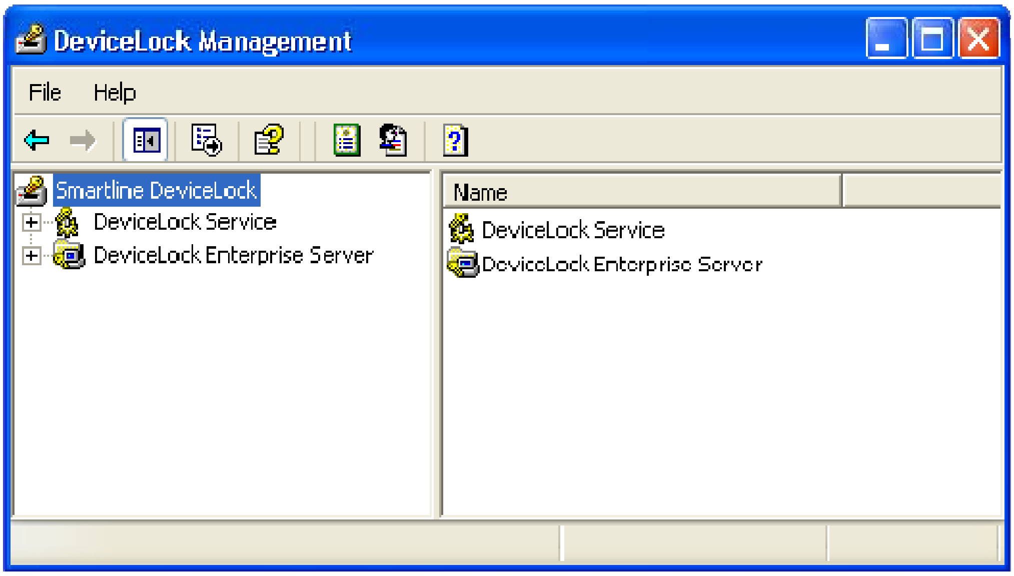
| Snap-in | Vendor |
|---|---|
| ActiveX Control | Microsoft Corporation |
| Certificates | Microsoft Corporation |
| Component Services | Microsoft Corporation |
| Computer Management | Microsoft Corporation |
| Device Manager | Microsoft Corporation |
| DeviceLock Management Console | SmartLine Inc |
| Disk Defragmenter | Microsoft Corp, Executi... |
| Disk Management | Microsoft and VERITAS... |
| Event Viewer | Microsoft Corporation |
| Folder | Microsoft Corporation |

Description

This snap-in allows you to configure DeviceLock settings.

## 5.2 Interface

DeviceLock Management Console has a user-friendly, easy-to-use standard interface provided by Microsoft Management Console (MMC). At any time, you can press the *F1* key to get context-specific help.



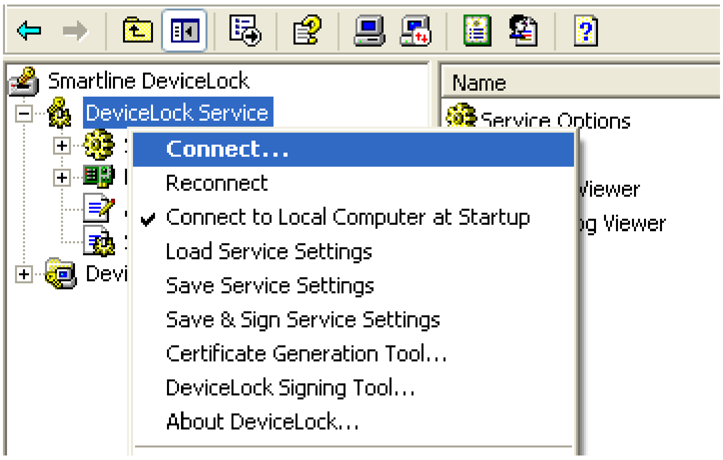
There are two independent parts in DeviceLock Management Console:

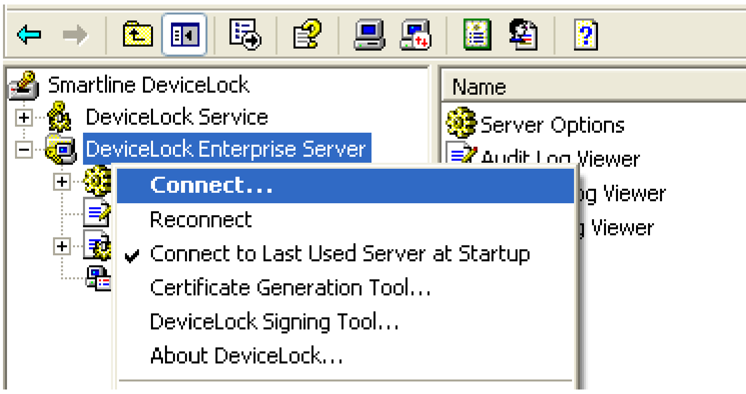
1. *DeviceLock Service* – allows you to connect to and manage DeviceLock Services running on remote and local computers.

2. *DeviceLock Enterprise Server* – allows you to connect to and manage DeviceLock Enterprise Servers running on remote and local computers.

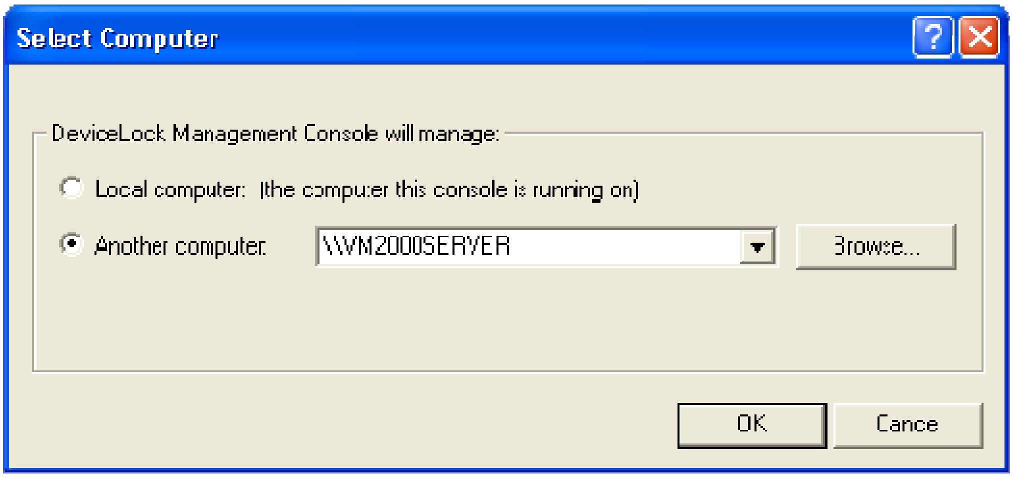
## 5.3 Connecting to Computers

First of all, you should connect to the computer where DeviceLock Service or DeviceLock Enterprise Server is running. Use the context menu *Connect* item or the appropriate button on the toolbar.




Smartline DeviceLock
DeviceLock Service
DeviceLock Enterprise Server
Name
Server Options
Audit Log Viewer
g Viewer
Viewer
Connect...
Reconnect
✓ Connect to Last Used Server at Startup
Certificate Generation Tool...
DeviceLock Signing Tool...
About DeviceLock...

You can simultaneously connect to both DeviceLock Service and DeviceLock Enterprise Server even if they are running on the different computers.


Select Computer

DeviceLock Management Console will manage:

○ Local computer: (the computer this console is running on)

● Another computer: \\VM2000SERVER

Specify the remote computer name or IP address you want to connect to in the *Another computer* parameter. To browse for available computers in your network, use the *Browse* button.

To connect DeviceLock Management Console to the computer where DeviceLock Service or DeviceLock Enterprise Server was configured using a fixed port, you should specify this port in square brackets next to the computer name, e.g. *\\computer_name[port number]*.

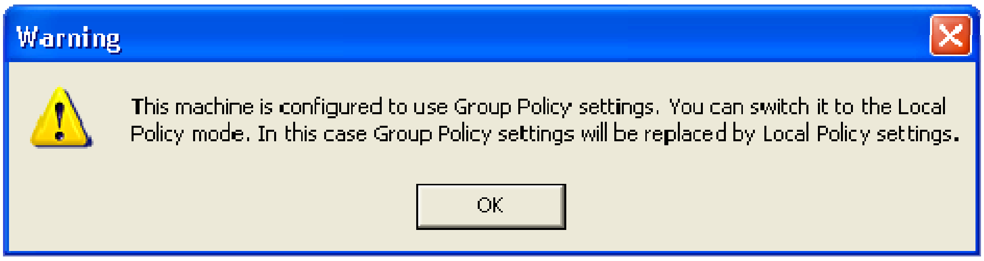
To connect to the local computer, use the *Local computer* option.

Press the *OK* button to connect to the selected computer.

***NOTE: Make sure that the remote computer you've selected to connect to is accessible from the computer where DeviceLock Management Console is running. The remote computer must work under a DeviceLock-compatible OS (Windows NT 4.0 SP6 and later). It must have a functioning TCP/IP protocol. In case a firewall (including built-in Windows Firewall) is installed on the remote computer, it must be properly configured to allow connection with DeviceLock Service and/or DeviceLock Enterprise Server.***

When you're trying to connect to DeviceLock Service on a computer where it is not installed or is outdated, DeviceLock Management Console suggests that you install or update the service. For more information regarding the remote service deployment, please read the **Remote Installation via DeviceLock Management Console** section of this manual.

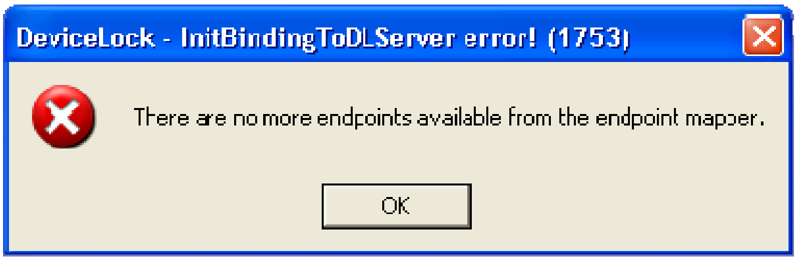
You receive the warning message when you connect to DeviceLock Service configured to work in the *Group Policy* mode.


Warning

This machine is configured to use Group Policy settings. You can switch it to the Local Policy mode. In this case Group Policy settings will be replaced by Local Policy settings.

If you change some parameter using DeviceLock Management Console, it will revert to its original state (defined in GPO) on the next Group Policy update. For more information, please read the **Service Options** section of this manual.

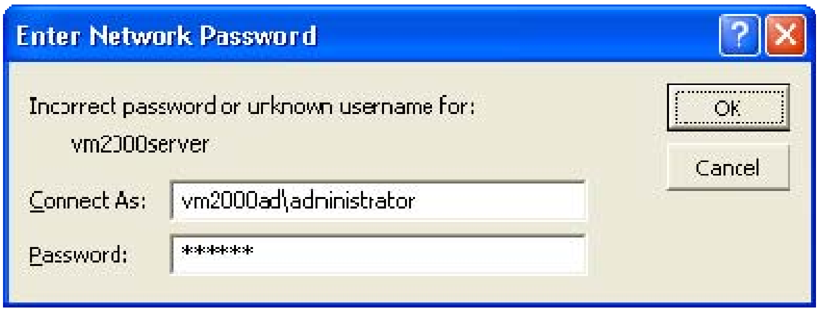
If you're trying to connect to DeviceLock Enterprise Server on a computer where it is not installed or stopped, you receive a connection error.


DeviceLock - InitBindingToDLServer error! (1753)

There are no more endpoints available from the endpoint mapper.

DeviceLock Enterprise Server must be installed and started before DeviceLock Management Console can connect to it. For more information regarding the server deployment, please read the **Installing DeviceLock Enterprise Server** section of this manual.

If you don't have administrative privileges on the selected computer, DeviceLock Management Console suggests that you connect under the account of another user.


Enter Network Password

Incorrect password or unknown username for:
vm2000server

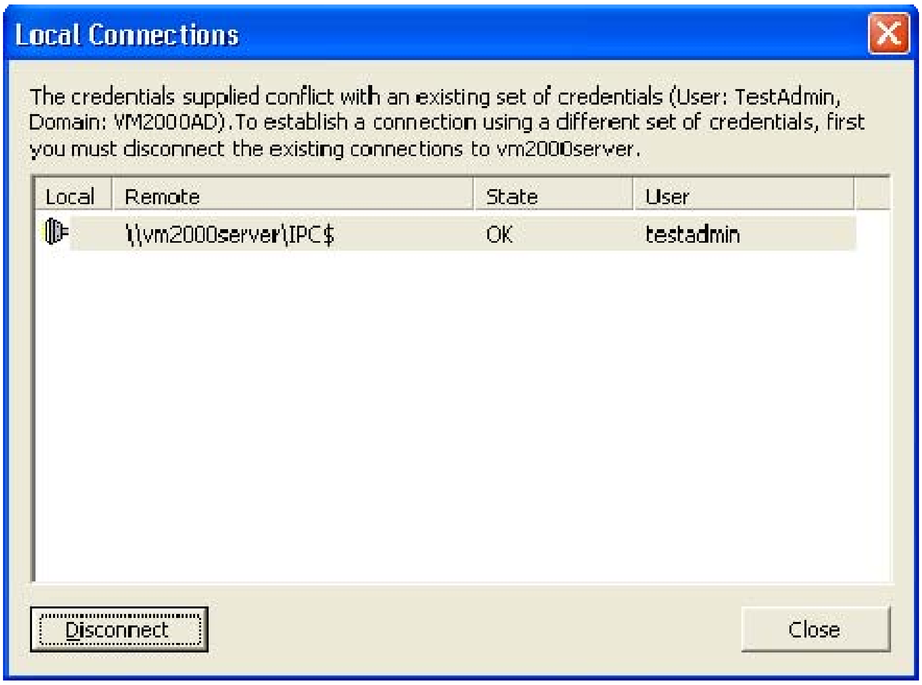
Connect As: vm2000ad\administrator

Password: ******

In the *Connect As* parameter you can specify a user account with administrative privileges. This account should also be on the list of DeviceLock Administrators in case this administrator safeguard feature is enabled for DeviceLock Service or DeviceLock Enterprise Server.

A "credentials conflict" can result if, after connecting to ( i.e., you have a mapped network disk, opened shared resource, etc.) a selected computer under a user that can't access DeviceLock Service or DeviceLock Enterprise Server, you then try to use another user in DeviceLock Management Console.  To avoid this conflict you must first delete your existing connection.

When DeviceLock Management Console detects a credentials conflict it displays a list of existing connections on your local computer and suggests that you delete some of them.


Local Connections

The credentials supplied conflict with an existing set of credentials (User: TestAdmin, Domain: VM2000AD). To establish a connection using a different set of credentials, first you must disconnect the existing connections to vm2000server.

| Local | Remote | State | User |
|---|---|---|---|
|  | \\vm2000server\IPC$ | OK | testadmin |

Highlight all existing connections to the computer you want to connect to and press the *Disconnect* button.

Press the *Close* button and then try to connect to this computer again.

***NOTE: Sometimes the existing connection can't be terminated thus preventing you from connecting under a different user account in DeviceLock Management Console. In this case you need to run DeviceLock Management Console under a user that either has enough privileges to access DeviceLock Service or DeviceLock Enterprise Server or has no connections to the selected computer at all. You may use the Run As function (run RUNAS from the command line) available in Windows 2000 and later to run DeviceLock Management Console under another user.***

### 5.3.1 Possible Connection Errors

When you're trying to connect to a computer with DeviceLock Service or DeviceLock Enterprise Server you may receive some of these errors:

- *(1722) The RPC server is unavailable* – you're trying to connect to a computer that either does not exist (the wrong name or IP address) or is not accessible. Make sure that the computer name you've specified is correct. Try to ping this computer by its name and IP address and connect to it using any standard Windows administrative tool (such as *Computer Management*, *Services* and so on). Make sure that this computer is working under a DeviceLock-compatible OS (Windows NT 4.0 and later).

  Also, it is possible that a firewall is blocking access to this computer. You would need to configure your firewall to allow some ports needed for DeviceLock. You could also instruct DeviceLock to use the fixed TCP port, making it easier to configure a firewall. For more information, please refer to the Frequently Asked Questions section of our website.

- *(1753) There are no more endpoints available from the endpoint mapper* – you're trying to connect to a computer where DeviceLock Service or DeviceLock Enterprise Server is not accessible. First of all, make sure that DeviceLock Service or DeviceLock Enterprise Server is installed and started on the remote computer.

  It is possible that this computer was just booted and Windows is still initializing its services. The *Remote Procedure Call (RPC)* service may not be running yet.

  Also, a firewall could be blocking access to DeviceLock Service or DeviceLock Enterprise Server. For more information, please read the above desription of the 1722 error.

  To troubleshoot RPC Endpoint Mapper errors, please read this Microsoft article: http://support.microsoft.com/kb/839880/en-us

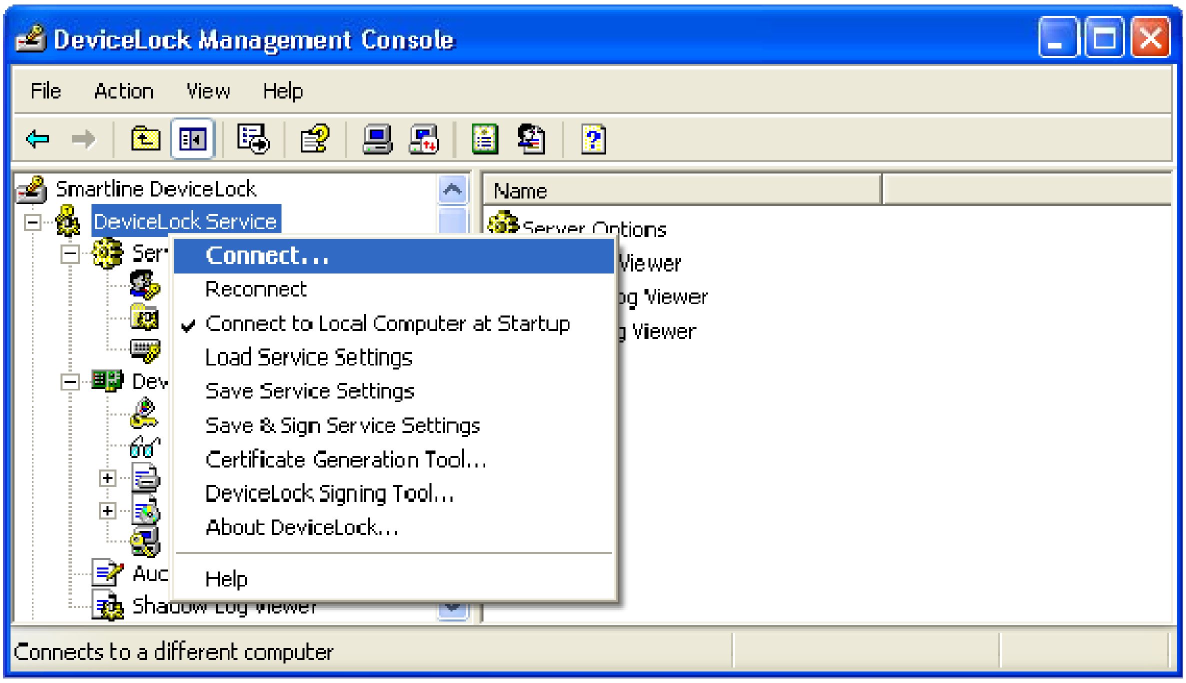
- *(5) Access is denied* – you don't have enough privileges on the remote computer. Make sure that DeviceLock Management Console is trying to connect to the remote computer under a user with local administrator privileges on that computer.

  You may also need to run DeviceLock Management Console under a different user that can authenticate on the remote computer as a local admin.

- *(7045) You must have administrative privileges to perform this operation* – you don't have enough privileges to access DeviceLock Service or DeviceLock Enterprise Server because the user is not in the list of DeviceLock Administrators. Make sure that DeviceLock Management Console is trying to connect to the remote computer under the user that is in the list of DeviceLock Administrators on that computer.

## 5.4 Managing DeviceLock Service

Expand the *DeviceLock Service* item to access all of the service function and configuration parameters.



There is a context menu available via a right mouse click on the *DeviceLock Service* item:

- *Connect* – connects to any computer that you specify. For more information please read the **Connecting to Computers** section of this manual.

- *Reconnect* – connects to the currently connected computer once again.

- *Connect to Local Computer at Startup* – check this flag to instruct DeviceLock Management Console to automatically connect to the local computer each time it starts up.

- *Load Service Settings* – loads previously saved settings from the XML file and applies these settings to the currently connected DeviceLock Service. You need to select the file that was created either by DeviceLock Management Console or DeviceLock Group Policy Manager. Since the signature is not validated at this step, it can be either a signed or non-signed file.

- *Save Service Settings* – exports all settings from the currently connected DeviceLock Service to an external XML file. Later this file can be modified using DeviceLock Service Settings Editor and loaded via DeviceLock Management Console and/or DeviceLock Group Policy Manager. Also, this file can be sent to users whose computers are not online and thus out-of-reach via management consoles. To avoid unauthorized modification the file should be signed with the DeviceLock Certificate (the *private* key) using the DeviceLock Signing Tool.

- *Save & Sign Service Settings* – exports all settings from the currently connected DeviceLock Service to an external XML file and automatically signs it with the most recent DeviceLock Certificate (the *private* key). This menu item is disabled when the DeviceLock Signing Tool has no previously loaded *private* key.

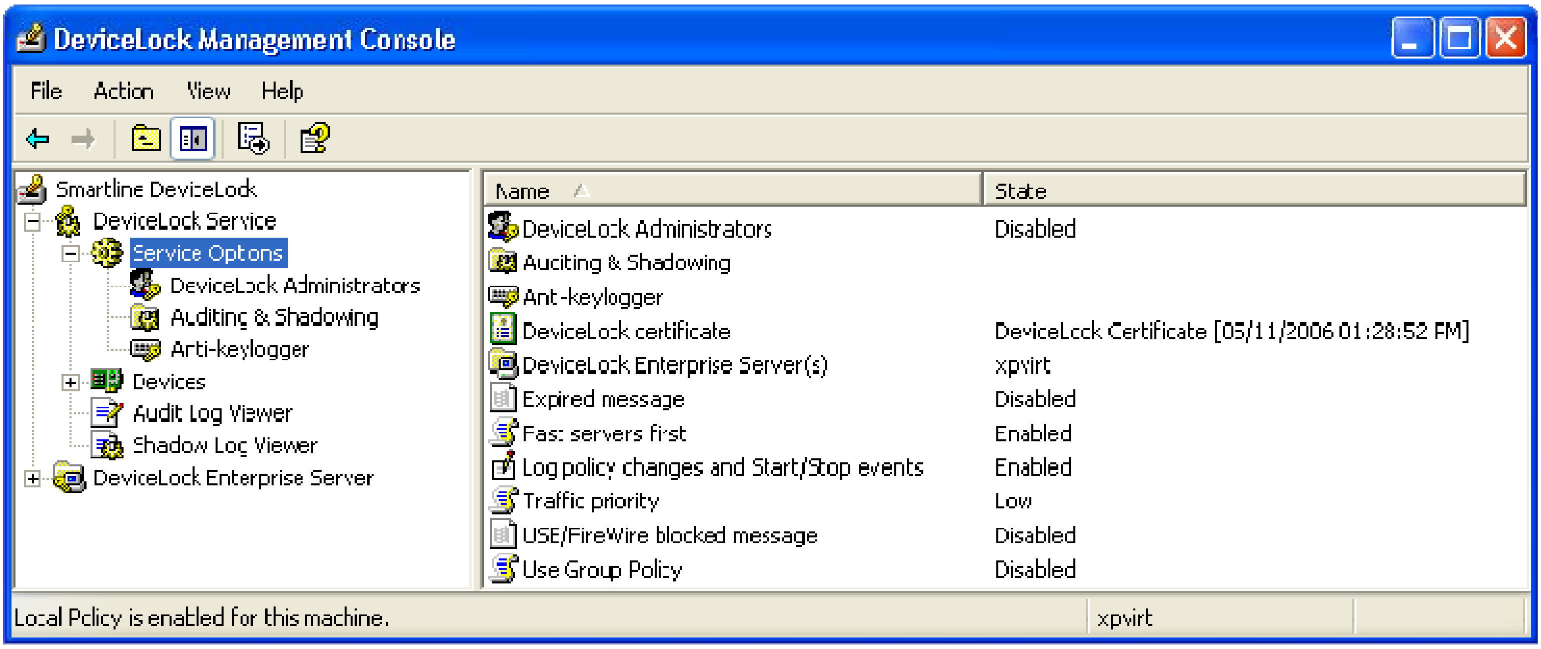
- *Certificate Generation Tool* – runs the special tool that allows you to generate DeviceLock Certificates. For more information please read the **Generating DeviceLock Certificates** section of this manual.

- *DeviceLock Signing Tool* – runs the special tool that allows you to grant users temporary access to requested devices and sign XML files with DeviceLock Service settings. For more information please read the **DeviceLock Signing Tool** section of this manual.

- *About DeviceLock* – displays a dialog with information about the DeviceLock version and your licenses.

### 5.4.1 Service Options

These additional parameters allow you to tune up the DeviceLock Service configuration. Use the context menu available by a right mouse click on every parameter.



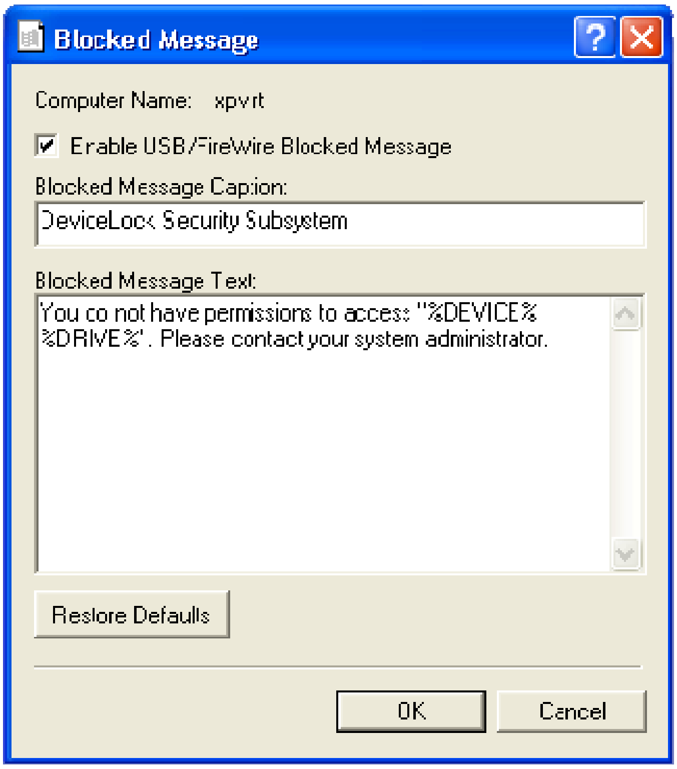
| Name | State |
|---|---|
| DeviceLock Administrators | Disabled |
| Auditing & Shadowing | |
| Anti-keylogger | |
| DeviceLock certificate | DeviceLock Certificate [05/11/2006 01:28:52 PM] |
| DeviceLock Enterprise Server(s) | xpvirt |
| Expired message | Disabled |
| Fast servers first | Enabled |
| Log policy changes and Start/Stop events | Enabled |
| Traffic priority | Low |
| USB/FireWire blocked message | Disabled |
| Use Group Policy | Disabled |

Local Policy is enabled for this machine.

xpvirt

a. USB/FireWire blocked message

You can define a custom message to be displayed to users when an attempt made to plug in a USB or FireWire device is denied.



Computer Name: xpvrt

☑ Enable USB/FireWire Blocked Message

Blocked Message Caption:

DeviceLock Security Subsystem

Blocked Message Text:

You do not have permissions to access "%DEVICE% %DRIVE%". Please contact your system administrator.

To enable this custom message, check the *Enable USB/FireWire Blocked Message* flag.

***NOTE: The custom message will only be shown when access to a device is blocked on the port (USB or FireWire) level. If some device is blocked only on the type (e.g. Removable) level, DeviceLock will not display the custom message.***

Also, you can define additional parameters, such as:

- *Blocked Message Caption* – the text to be displayed as a caption. You can use three predefined macros within the text:

  1. *%TYPE%* – inserts the port name (*USB port*, *FireWire port*) where the device is plugged.

  2. *%DEVICE%* – inserts the name of the device (e.g. *USB Mass Storage Device*) received from the system.

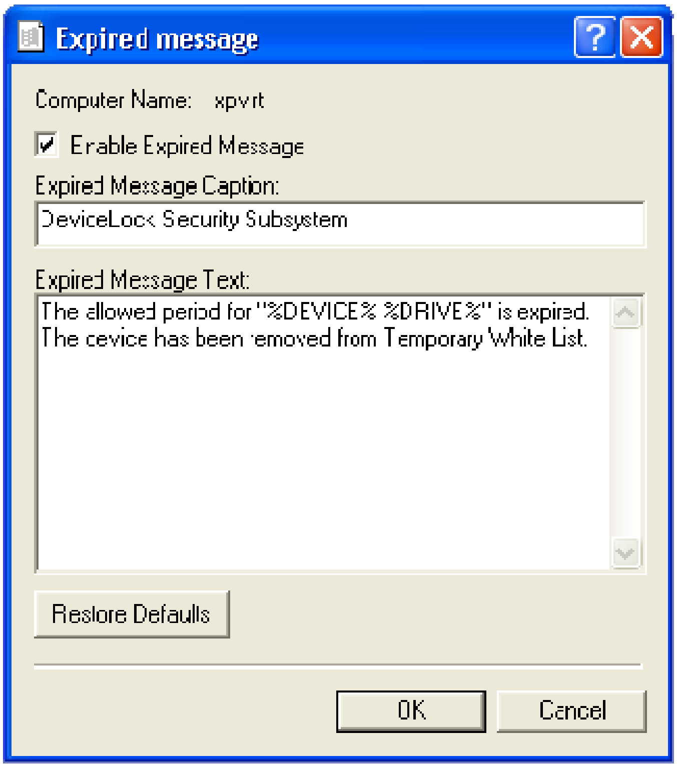
  3. *%DRIVE%* – inserts the drive letter of the storage device (e.g. *F:*). If the device doesn't have a letter, then this macro inserts an empty string.

  Using these macros you can create more informative messages for users.

- *Blocked Message Text* – the main text of the message. You can use the predefined macros described above within the text.

b. Expired message

You can define a custom message to be displayed to users when the allowed period for temporary white listed devices is expired and devices have been removed from Temporary White List.



Computer Name: xpvrt

☑ Enable Expired Message

Expired Message Caption: DeviceLock Security Subsystem

Expired Message Text: The allowed period for "%DEVICE% %DRIVE%" is expired. The device has been removed from Temporary White List.

To enable this custom message, check the *Enable Expired Message* flag.

Also, you can define additional parameters, such as:

- *Expired Message Caption* – the text to be displayed as a caption. You can use two predefined macros within the text:

  1. *%DEVICE%* – inserts the name of the device (e.g. *USB Mass Storage Device*) received from the system.

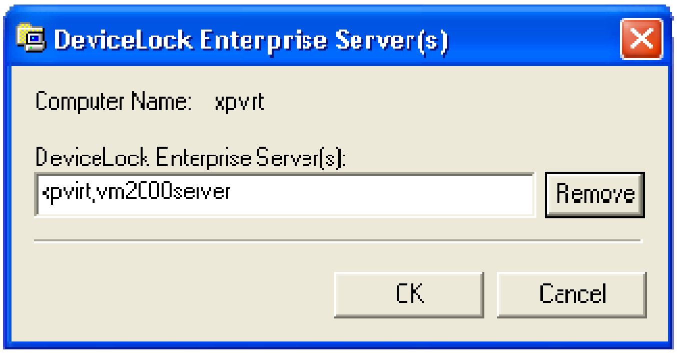
  2. *%DRIVE%* – inserts the drive letter of the storage device (e.g. *F:*). If the device doesn't have a letter, then this macro inserts an empty string.

  Using these macros you can create more informative messages for users.

- *Expired Message Text* – the main text of the message. You can use the predefined macros described above within the text.

c. DeviceLock Enterprise Server(s)

If you want to allow DeviceLock Service to send its logs to DeviceLock Enterprise Server, specify the name or IP address of this server's computer.



Computer Name: xpvrt

DeviceLock Enterprise Server(s): xpvirt;vm2000server

Using the semicolon (;) as a separator you can specify several DeviceLock Enterprise Servers to uniformly spread the network load. At its startup, DeviceLock Service chooses one server for sending logs. If the selected server is unavailable, DeviceLock Service tries to choose another one from the list.

Make sure that DeviceLock Enterprise Server is properly installed and accessible for DeviceLock Service, otherwise logs will not be stored in the centralized database. For more information on how to install DeviceLock Enterprise Server, please read the **Installing DeviceLock Enterprise Server** section of this manual.

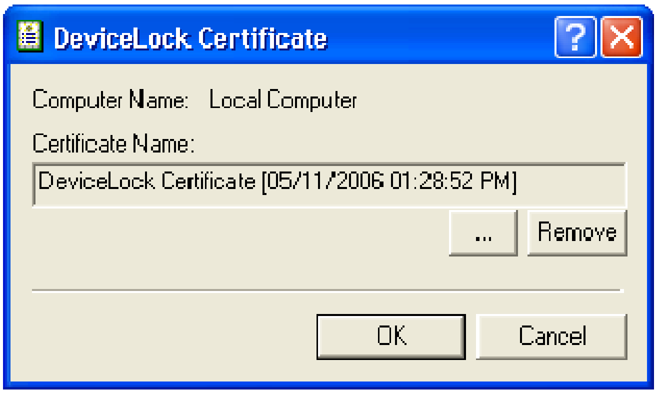
d. Log Policy changes and Start/Stop events

You can enable the logging of changes in DeviceLock Service's configuration and report the time when DeviceLock Service starts and stops. It is possible to log changes in permissions, audit rules, white lists and in other settings.

To allow this logging, enable the *Log Policy changes and Start/Stop events* parameter.

e. DeviceLock certificate

Use this parameter to install or remove a DeviceLock Certificate.



Computer Name: Local Computer

Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

Specify the path to the *public* key in the *Certificate Name* parameter if you want to install the certificate. You can use the **...** button to select the file with a *public* key.

To remove the *public* key, use the *Remove* button.

For more information about DeviceLock Certificates, please read the **DeviceLock Certificates** section of this manual.

### f. Use Group Policy

If DeviceLock Service is configured to work with Group Policy in an Active Directory domain, you can control the effective policy mode (*Group Policy* or *Local Policy*).

To activate the *Group Policy* mode for this DeviceLock Service, enable the *Use Group Policy* parameter. In this mode, all settings that you set via DeviceLock Management Console and DeviceLock Enterprise Manager are replaced by Group Policy settings.

To activate the *Local Policy* mode for this DeviceLock Service, disable the *Use Group Policy* parameter. In this mode, all settings that you set via DeviceLock Management Console and DeviceLock Enterprise Manager have a priority over Group Policy settings and replace them.

If DeviceLock Service was not configured to work with Group Policy, the *Use Group Policy* parameter is disabled and unavailable for changing.

If the *Use Group Policy* parameter is enabled but unavailable for changing, it means that the *Group Policy* mode always has a priority (the *Override Local Policy* parameter was enabled in DeviceLock Group Policy Manager) and the *Local Policy* mode can't be enabled for this DeviceLock Service. For more information, please read the **Using DeviceLock Group Policy Manager** section of this manual.

### g. Fast servers first

DeviceLock Service can choose the fastest available DeviceLock Enterprise Server from the list of servers.

When this parameter is enabled, all servers specified in the *DeviceLock Enterprise Server(s)* parameter are divided into three groups depending on their network speed and preference is given to the fastest. If all of the fastest servers are unavailable, DeviceLock Service attempts to select a server from the group of next fastest servers and so on.

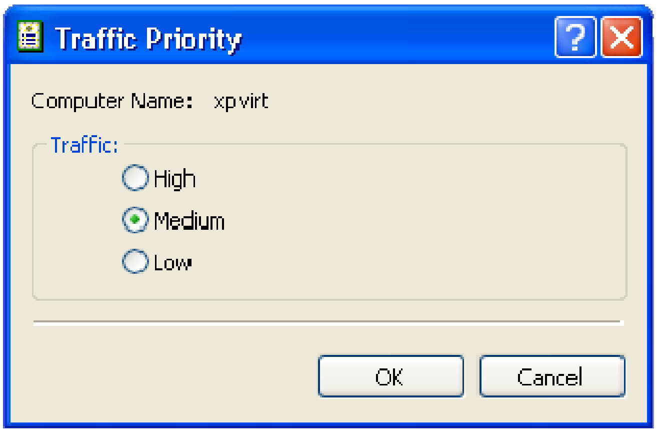
If the *Fast servers first* parameter is disabled, DeviceLock Service randomly selects a server from the list.

This parameter has an effect only if there is more than one server specified in the *DeviceLock Enterprise Server(s)* parameter.

### h. Traffic priority

DeviceLock supports traffic shaping, allowing you to define bandwidth limits for sending audit and shadow logs from DeviceLock Service to DeviceLock Enterprise Server.

You can set three types of traffic priority: high, medium and low.



Computer Name: xpvirt

Traffic:

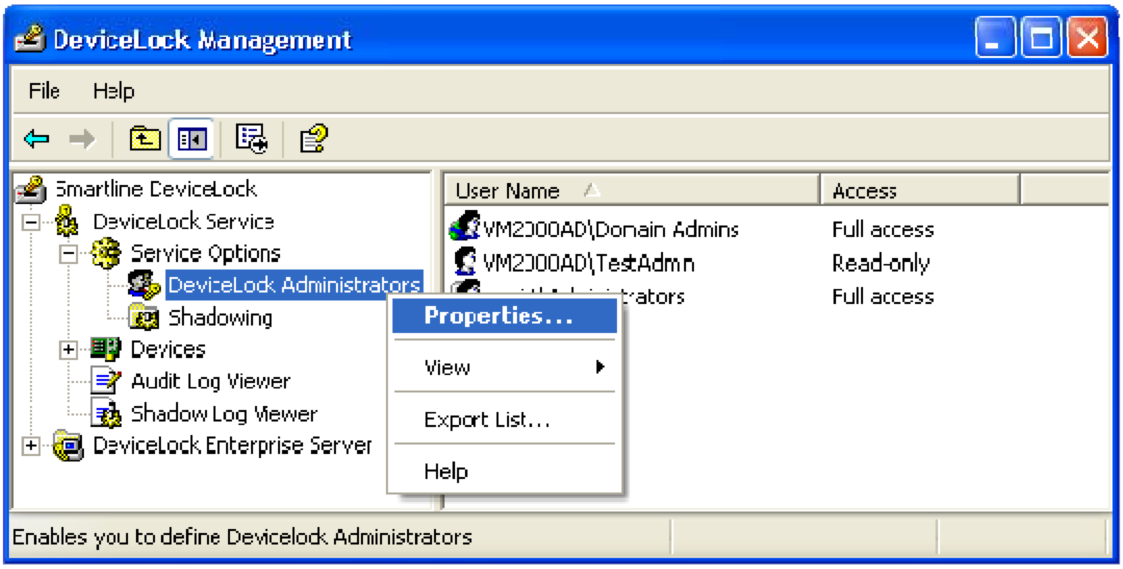
○ High
● Medium
○ Low

When *High* is selected it means that 100% of bandwidth can be used. To allow use of only up to 50% of bandwidth, select *Medium*. Select *Low* to allow use of just up to 10% of bandwidth.

Please note that medium and low priorities have an effect only if the Quality of Service Packet Scheduler (QoS Packet Scheduler) component is installed on a computer running DeviceLock Service. Otherwise, the *Traffic priority* parameter is disabled and 100% of bandwidth is used. For more information on QoS, please refer to Microsoft's on-line article: http://www.microsoft.com/technet/network/qos/default.mspx.

### 5.4.1.1 DeviceLock Administrators

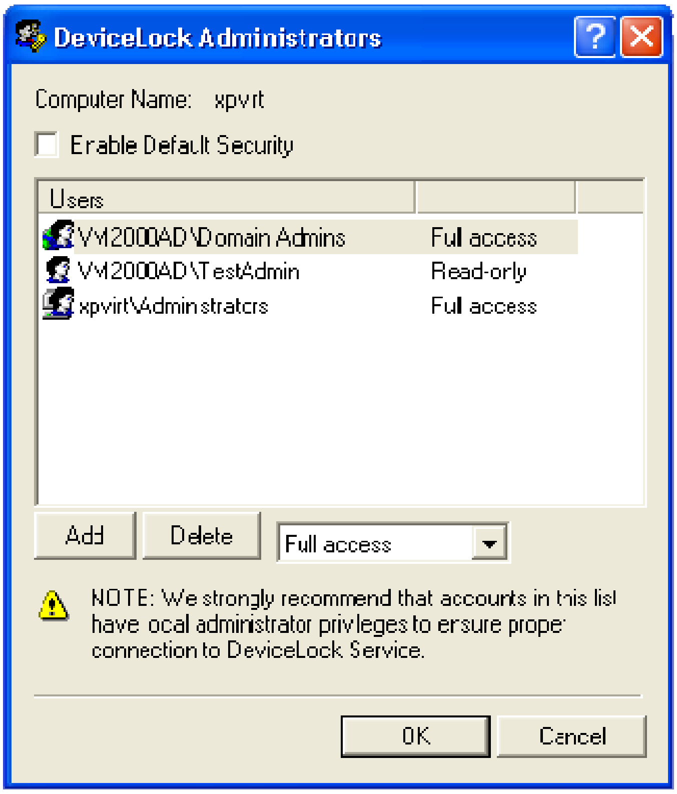
This parameter allows you to define the list of user accounts with administrative access rights to DeviceLock Service.



| User Name | Access |
|---|---|
| VM2300AD\Domain Admins | Full access |
| VM2300AD\TestAdmn | Read-only |
| ...trators | Full access |

Enables you to define Devicelock Administrators

Use the context menu available by a right mouse click on the *DeviceLock Administrators* item to open the configuration dialog.



Computer Name: xpvirt

☐ Enable Default Security

| Users | |
|---|---|
| VM2000AD\Domain Admins | Full access |
| VM2000AD\TestAdmin | Read-only |
| xpvirt\Administrators | Full access |

Full access

NOTE: We strongly recommend that accounts in this list have local administrator privileges to ensure proper connection to DeviceLock Service.

DeviceLock’s default security configuration is based on Windows *Access Control Lists* (ACL). A user without administrative privileges can't connect to DeviceLock Service, modify its settings or remove it. Everything is controlled by the Windows security subsystem.

To turn on the default security based on Windows ACL, check the *Enable Default Security* flag.

***NOTE: As described in the Recommended Basic Security Measures section of this manual, giving administrative privileges to regular users is strongly discouraged.***

Users with local administrator privileges (i.e. members of the local *Administrators* group) can connect to DeviceLock Service using a management console and change permissions, auditing and other parameters. Moreover, such users can uninstall DeviceLock from their computers, disable or delete DeviceLock Service, modify a service's registry keys, delete a service's executable file, and so on. In other words, users with local administrator privileges can circumvent the default security based on Windows ACL.

However, if for some reason, users in your network have administrator privileges on their local computers, DeviceLock does provide another level of protection – DeviceLock Security. When DeviceLock Security is enabled, no one except authorized users can connect to DeviceLock Service or stop and uninstall it. Even members of the local *Administrators* group (if they are not on the list of authorized DeviceLock administrators) can't circumvent DeviceLock Security.

To turn on DeviceLock Security, uncheck the *Enable Default Security* flag.

Then you need to specify authorized accounts (users and/or groups) that can administer DeviceLock Service. To add a new user or user group to the list of accounts, click on the *Add* button. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the *Delete* button. Using *Ctrl* and/or *Shift* you can highlight and remove several records simultaneously.

To define which DeviceLock administrative actions are to be allowed for a user or user group, set the appropriate rights:

- **Full access** – to enable full access to DeviceLock Service. Users can modify permissions, auditing and other parameters, remove and update DeviceLock Service.

- **Change** – to enable change access to DeviceLock Service. Users can change settings, install, and uninstall DeviceLock Service, but they can't add new users to the list of authorized accounts that can administer DeviceLock Service or change access rights for existing users in this list.

- **Read-only** – to enable only the reading of permissions, auditing and other parameters. Users can run reports, view defined parameters but can't modify anything or remove/update DeviceLock Service.

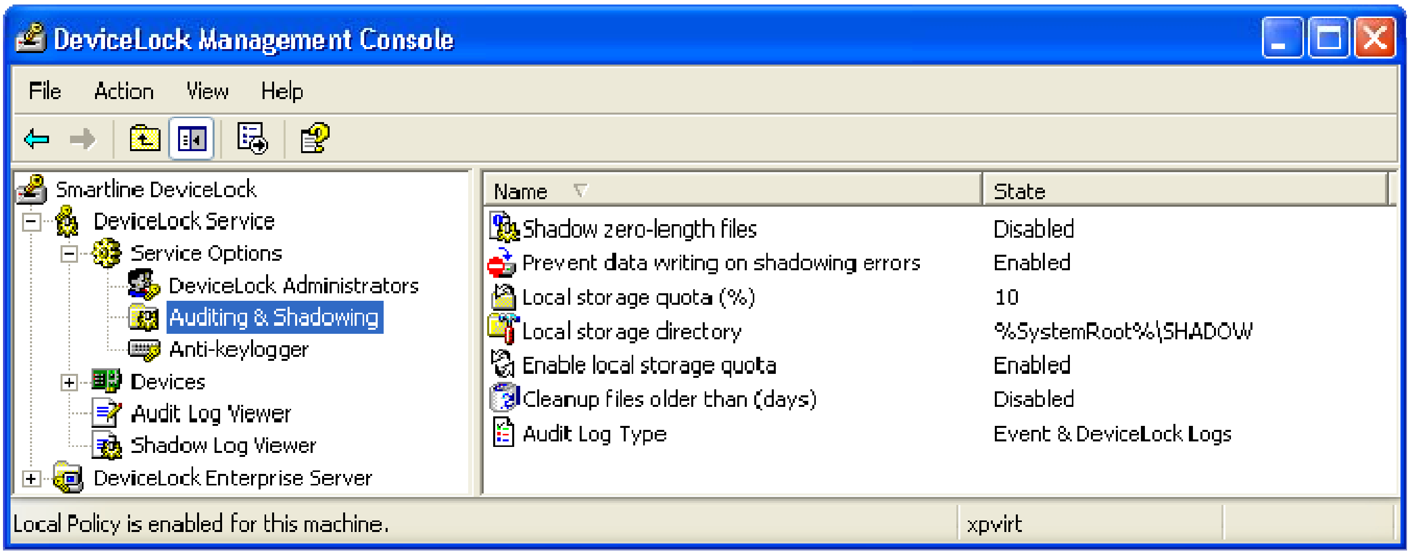
***NOTE: We strongly recommend that accounts included in this list have local administrator privileges because, in some instances, installing, updating and uninstalling DeviceLock Service may require access rights to Windows Service Control Manager (SCM) and shared network resources.***

Here is just one example of how to properly define a DeviceLock Administrators list: add a *Domain Admins* group with **Full access** rights. Because *Domain Admins* is a member of the local group *Administrators* on every computer in the domain, all members of *Domain Admins* will have full access to DeviceLock Service on every computer. However, other members of the local group *Administrators* will not be able to administer DeviceLock Service or disable it.

Please note that if DeviceLock Service is installed and running on the same computer as your DeviceLock management console and DeviceLock Security is enabled, neither the DeviceLock management console nor any other application will be able to access the service's executable file (*dlservice.exe* or *dlservice_x64.exe*). This happens because DeviceLock Service is protecting its executable file from modification by the user with local administrator privileges.  It may be necessary to access *dlservice.exe* or *dlservice_x64.exe* when you deploy DeviceLock Service to remote computers from your machine. To prepare for this scenario, you can copy the service's executable files (*dlservice.exe* and *dlservice_x64.exe*) to another directory before turning on DeviceLock Security and use the copy for remote deployment.

### 5.4.1.2 Auditing & Shadowing

These parameters allow you to tune up auditing and shadowing for DeviceLock Service.



- Smartline DeviceLock
  - DeviceLock Service
    - Service Options
      - DeviceLock Administrators
      - Auditing & Shadowing
      - Anti-keylogger
    - Devices
    - Audit Log Viewer
    - Shadow Log Viewer
  - DeviceLock Enterprise Server

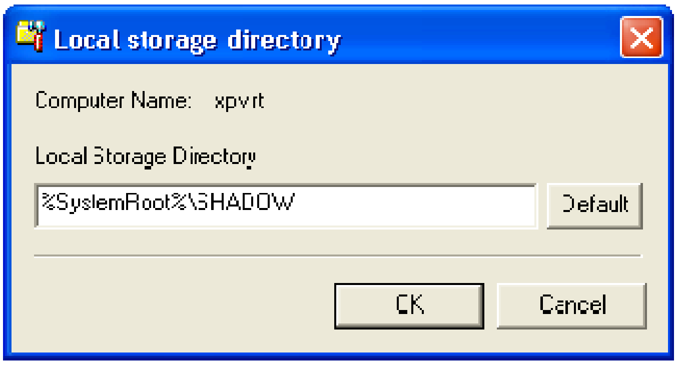
| Name | State |
|---|---|
| Shadow zero-length files | Disabled |
| Prevent data writing on shadowing errors | Enabled |
| Local storage quota (%) | 10 |
| Local storage directory | %SystemRoot%\SHADOW |
| Enable local storage quota | Enabled |
| Cleanup files older than (days) | Disabled |
| Audit Log Type | Event & DeviceLock Logs |

Local Policy is enabled for this machine. xpvirt

Use the context menu available via a right mouse click on every parameter.

a. Local storage directory

Use this parameter to define where on the local disk shadowed data is stored.



Computer Name: xpvrt

Local Storage Directory

%SystemRoot%\SHADOW

By default, DeviceLock Service uses the *%SystemRoot%\SHADOW* directory to store shadowed data on the local computer. *%SystemRoot%* is a standard environment variable that expands to a path to the Windows root folder (e.g. *C:\Windows*). You can specify any other directory on any locally accessible hard disk.

DeviceLock Service protects this directory so regular users can't access files inside it.

Make sure that there is enough space to store the data (if the user copies 1GB to the flash drive, then you need approximately 2GB available in local storage).

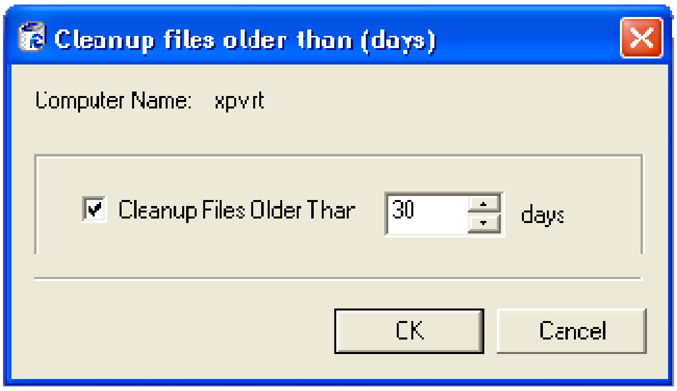
b. Enable local storage quota

Enable this parameter to allow automatic cleanup of the locally stored shadowed data.

When this parameter is enabled you can also configure *Cleanup files older than (days)* and *Local storage quota (%)* parameters (see below).

c. Cleanup files older than (days)

You can define the number of days that should pass before shadowed data can be automatically deleted from the local storage.



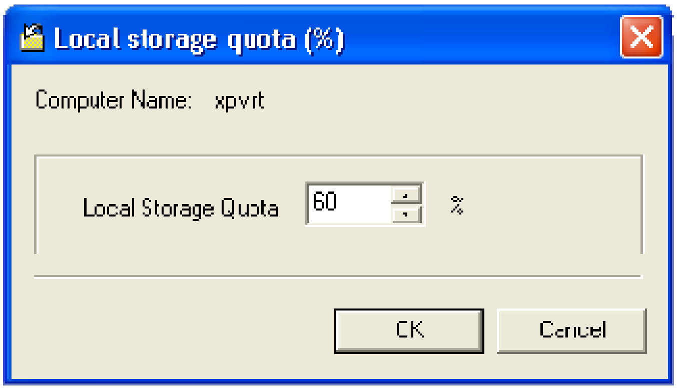
Computer Name: xpvrt

☑ Cleanup Files Older Thar 30 days

Check the *Cleanup Files Older Than* flag and specify the number of days to allow automatic cleanup.

d. Local storage quota (%)

You can define a disk quota for shadowed data.



Computer Name: xpvrt

Local Storage Quota 60 %

Specify the maximum percentage (from 5 to 100) of free disk space that can be used by shadowed data in the *Local Storage Quota* parameter.

If the quota is not used (i.e. the *Enable local storage quota* parameter is disabled) then DeviceLock Service uses all available space on the disk where the directory specified in the *Local storage directory* parameter is located.

When the total size of the directory specified in the *Local storage directory* parameter reaches the quota, DeviceLock Service either starts deleting old data (if the *Cleanup files older than (days)* parameter is enabled) or stops data shadowing (if the *Cleanup files older than (days)* parameter is disabled or there is nothing to delete).

e. Shadow zero-length files

Enable this parameter to allow shadowing of files whose size is zero.

Even if the file contains no data at all, it is still possible to transfer some information in its name and path (up to several kilobytes) that's why you may need to enable shadowing for zero-length files.

f. Prevent data writing on shadowing errors

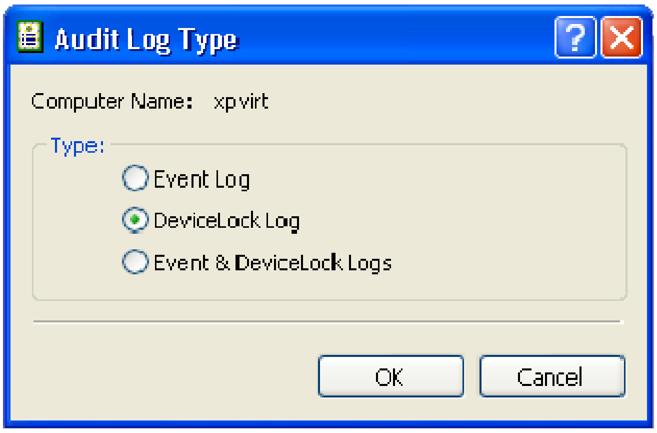
By enabling this parameter, you can prevent users from writing data when shadowing is not possible.

You can be sure that users can transfer information only when shadowing is working normally (e.g. there is enough local disk space to store shadow data).

When the *Prevent data writing on shadowing errors* parameter is enabled, the total size of the directory specified in the *Local storage directory* parameter reaches the quota specified in *Local storage quota (%)* and there is no data that can be deleted, DeviceLock Service stops shadowing and blocks any user attempt to copy the data.

g. Audit log type

Using this parameter you can define what log should be used to store audit records.



Computer Name: xpvirt

Type:

○ Event Log
● DeviceLock Log
○ Event & DeviceLock Logs

There are three options to choose:

1. *Event Log* – only the standard local Windows Event Log is used to store audit records.

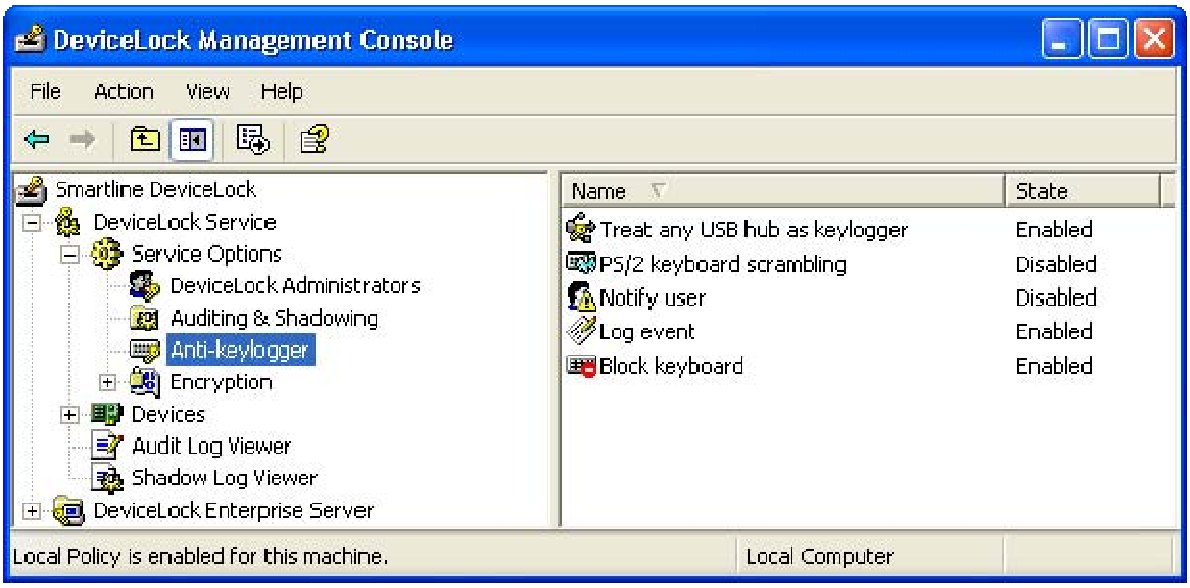
2. *DeviceLock Log* – only the protected proprietary log is used to store audit records. The data from this log is sent to DeviceLock Enterprise Server and is stored centrally in the database.

3. *Event & DeviceLock Logs* – both logs are used to store audit records.

### 5.4.1.3 Anti-keylogger

These parameters allow you to tune up DeviceLock's ability to detect hardware keyloggers and to define what DeviceLock Service should do when a keylogger is found.

Hardware keyloggers are devices that record keystrokes. DeviceLock Service can detect USB keyloggers and block keyboards connected to them. Also, DeviceLock Service can block PS/2 keyloggers.



| Name | State |
|---|---|
| Treat any USB hub as keylogger | Enabled |
| PS/2 keyboard scrambling | Disabled |
| Notify user | Disabled |
| Log event | Enabled |
| Block keyboard | Enabled |

Local Policy is enabled for this machine. Local Computer

Use the context menu available via a right mouse click on every parameter.

a. <u>Treat any USB hub as keylogger</u>

By enabling this parameter, you can instruct DeviceLock Service to treat any external USB hub to which the keyboard is connected as a hardware keylogger.

Otherwise, DeviceLock Service detects only those hub keyloggers that exist in its internal database.

b. <u>PS/2 keyboard scrambling</u>

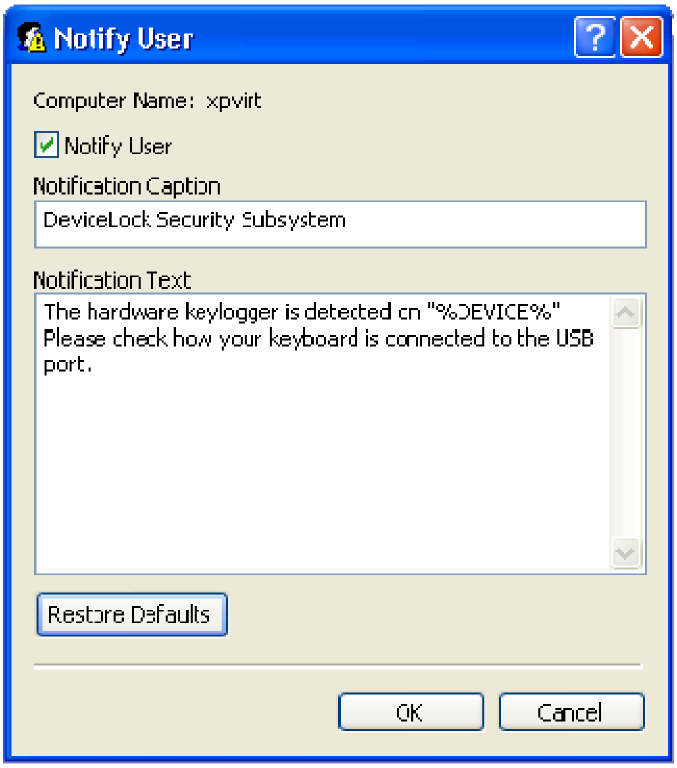
By enabling this parameter, you can prevent PS/2 keyloggers from recording keystrokes. DeviceLock Service is unable to detect PS/2 keyloggers and notify users about their presence but it obfuscates PS/2 keyboard's input and forces PS/2 keyloggers (if any) to record some garbage instead of the real keystrokes.

***NOTE: When PS/2 keyboard scrambling is enabled while working with the PS/2 KVM switch, the switching between computers will not work from the keyboard.***

c. Notify user

You can define a custom message to be displayed to users when DeviceLock Service detects hardware USB keyloggers.

Since DeviceLock Service starts before the user logs in to Windows, this message can alert the user and prevent him/her from typing the password on the keyboard connected to the USB keylogger.



Computer Name: xpvirt

☑ Notify User

Notification Caption: DeviceLock Security Subsystem

Notification Text: The hardware keylogger is detected on "%DEVICE%". Please check how your keyboard is connected to the USB port.

To enable this custom message, check the *Notify User* flag.

Also, you can define additional parameters, such as:

- *Notification Caption* – the text to be displayed as a caption. You can use the predefined macros within the text: *%DEVICE%* – inserts the name of the keyboard's device (e.g. *USB Keyboard*) received from the system.

- *Notification Text* – the main text of the message. You can use the predefined macros described above within the text.

d. Log event

You can instruct DeviceLock Service to write an event to the audit log when the hardware USB keylogger is detected.

e. Block keyboard

Enable this parameter to block the keyboard connected to the hardware USB keylogger when it is detected.

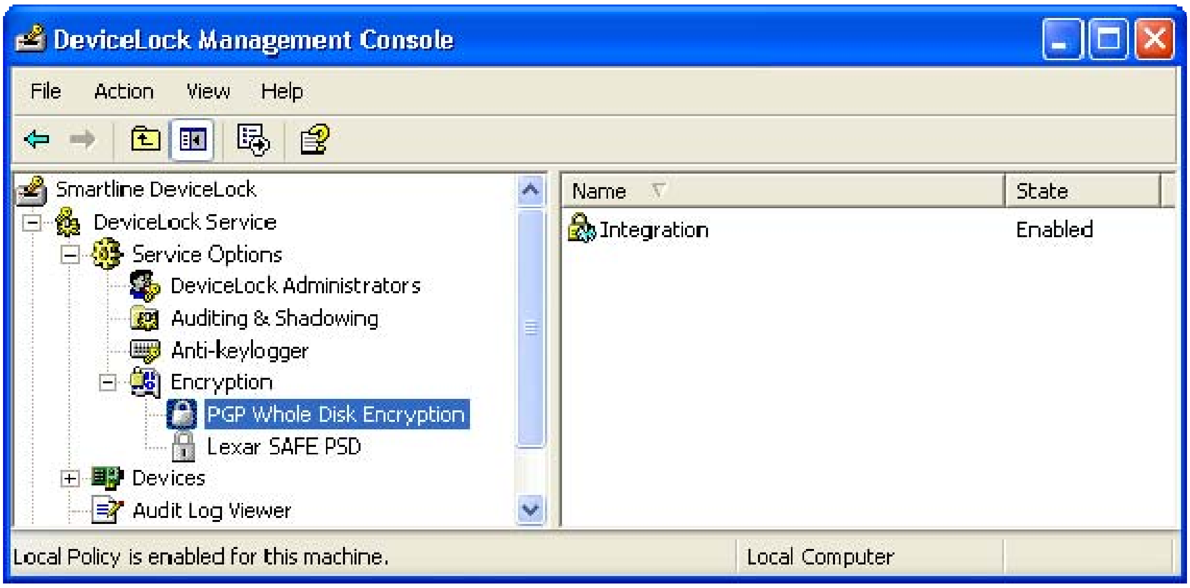
Since DeviceLock Service starts before the user logs in to Windows, it can block the keyboard and prevent the user from typing the password.

***NOTE: Some hardware keyloggers continue to record keystrokes even if the keyboard is blocked and not functioning in Windows. This happens because such keyloggers are standalone devices and don't require any OS or drivers.***

### 5.4.1.4 Encryption

DeviceLock Service can detect disks (USB flash drives and other removable media) encrypted by third-party products and apply special "encrypted" permissions to them.

This feature allows you to define more flexible access control policies and helps to prevent writing sensitive data to unencrypted media.



Currently DeviceLock supports these third-party products for encrypting data on removable storage devices:

- *PGP Whole Disk Encryption* – DeviceLock Service can detect PGP-encrypted removable storage devices and apply special "encrypted" permissions to them when the PGP® Whole Disk Encryption product is installed on the computer where DeviceLock Service is running and the *Integration* flag is enabled. For more information on PGP® Whole Disk Encryption, please visit PGP's website: www.pgp.com/products/wholediskencryption/index.html.

- *Lexar SAFE PSD* – DeviceLock Service can detect Lexar™ SAFE PSD S1100 USB flash drives and apply special "encrypted" permissions to them when users plug these devices into computers where DeviceLock Service is running and the *Integration* flag is enabled. For more information on Lexar™ SAFE PSD S1100, please visit Lexar's website: www.lexar.com/enterprise/safe_psd_S1100.html.

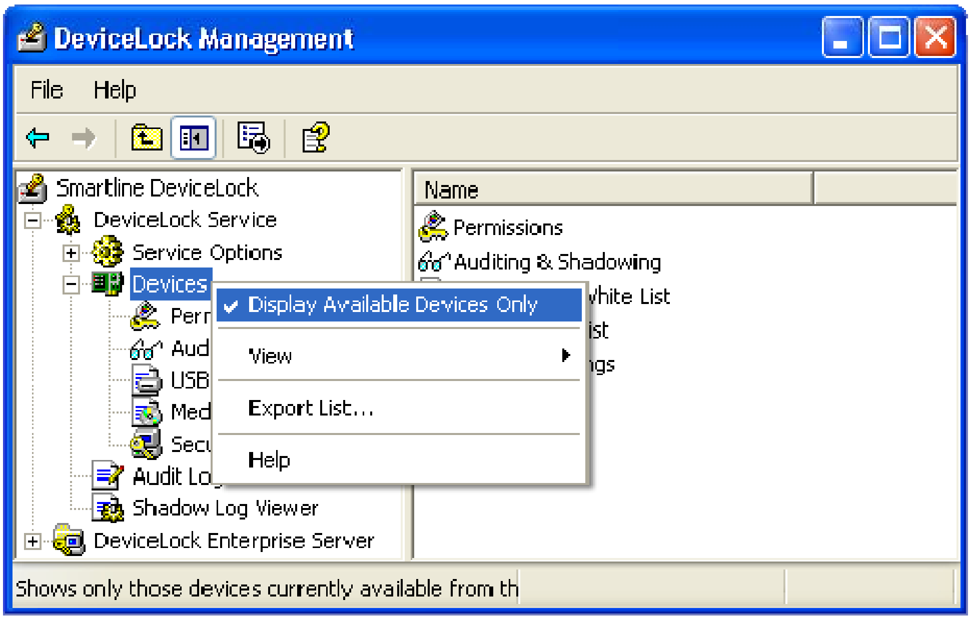
If you don't want to allow DeviceLock Service to detect one of the encryption products listed above and to apply special "encrypted" permissions to storage devices encrypted by it, disable the *Integration* flag under the product's section in the management console.

For more information on "encrypted" permissions, please read the **Permissions** section of this manual.

***NOTE: DeviceLock doesn't ship with third-party encryption products and doesn't require them for its own functioning. The integrated functioning of DeviceLock and a third-party encryption product will only work when the third-party product is properly installed, configured and running on the same computer where DeviceLock Service is running.***

## 5.4.2 Devices

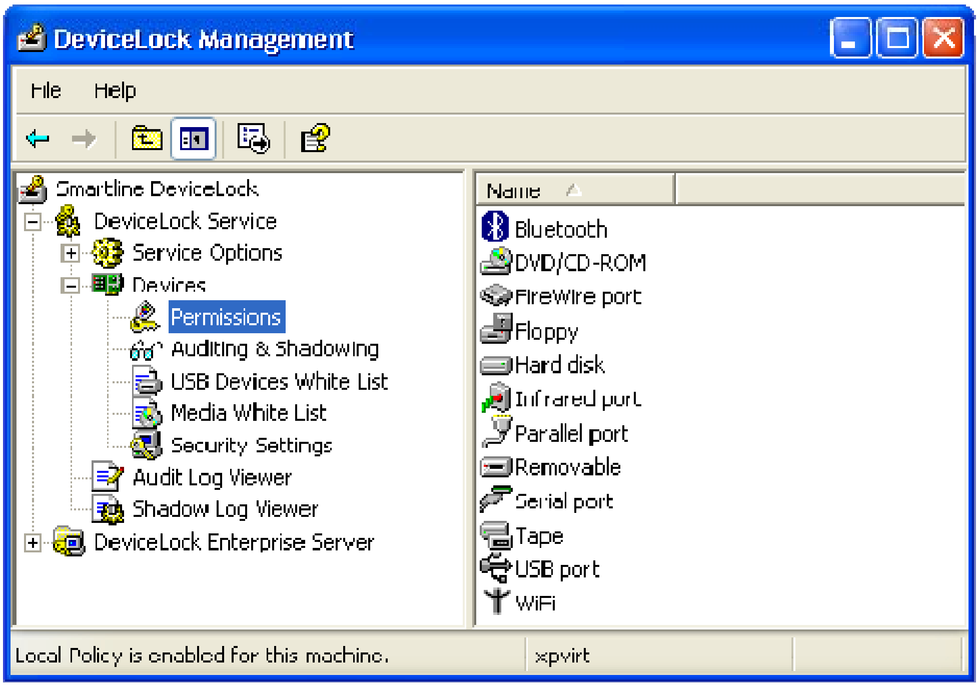
Configuration parameters available under this item allow you to access main functions of DeviceLock – permissions, auditing, shadowing, white lists and so on.



Use the context menu available with a right mouse click on the *Devices* item to access the *Display Available Devices Only* flag. If it is checked, DeviceLock Management Console shows only those device types currently available on the current computer. Otherwise, you will see every type of device that DeviceLock supports. This is useful when you want to set permissions to device types that are not yet installed or are currently unplugged from the computer.

### 5.4.2.1 Permissions

There is a list of device types for which you can define user-level permissions.



Local Policy is enabled for this machine.

***NOTE: When you set permissions for a device type, you set these permissions for every device belonging to that type. It is impossible to set different permissions for two different devices if they are of the same type (e.g. both are removable drives). To define different permissions for USB devices even if they are of the same type, use the White List function.***

There are two levels of control: the interface (port) level and the type level. Some devices are checked at both levels, while others only at the one level – either interface (port) or type.

For more information on how access control works, please read the **Managed Access Control** section of this manual.

DeviceLock supports the following types of devices:

1. *Bluetooth* (type level) – includes all internal and external Bluetooth devices with any type of the connection interface (USB, PCMCIA, etc.) to the computer.

2. *DVD/CD-ROM* (type level) – includes all internal and external CD/DVD devices (readers and writers) with any connection interface (IDE, SATA, USB, FireWire, PCMCIA, etc).

3. *FireWire port* (interface level) – includes all devices that can be plugged into the FireWire (IEEE 1394) port, except the hub devices.

4. *Floppy* (type level) – includes all internal and external floppy drives with any connection interface (IDE, USB, PCMCIA, etc.). It is possible that some non-standard floppy drives are recognized by Windows as removable devices, in this case DeviceLock treats such floppy drives as the *Removable* type as well.

5. *Hard disk* (type level) – includes all internal hard drives with any connection interface (IDE, SATA, SCSI, etc). DeviceLock treats all external USB, FireWire and PCMCIA hard drives as the *Removable* type. Also, DeviceLock treats as *Removable* some internal hard drives (usually SATA and SCSI) if they support the hot plug feature and Windows is not installed and running on them.

   ***NOTE: Even if you deny access to the Hard disk type, users with local administrative privileges (the SYSTEM user and members of the local Administrators group) still can access the partition where Windows is installed and running.***

6. *Infrared port* (interface level) – includes all devices that can be connected to the computer via the infrared (IrDA) port.

7. *Parallel port* (interface level) – includes all devices that can be connected to the computer via the parallel (LPT) ports.

8. *Removable* (type level) – includes all internal and external devices with any connection interface (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc) that are recognized by Windows as removable devices (e.g. USB flash drives, ZIP drives, card readers, magneto-optical drives, etc.). DeviceLock treats all external USB, FireWire and PCMCIA hard drives as the *Removable* type as well. Also, DeviceLock treats as *Removable* some internal hard drives (usually SATA and SCSI) if they support the hot plug feature and Windows is not installed and running on them.

9. *Serial port* (interface level) – includes all devices that can be connected to the computer via the serial (COM) ports, including internal modems.

10. *Tape* (type level) – includes all internal and external tape drives with any connection interface (SCSI, USB, IDE, etc).

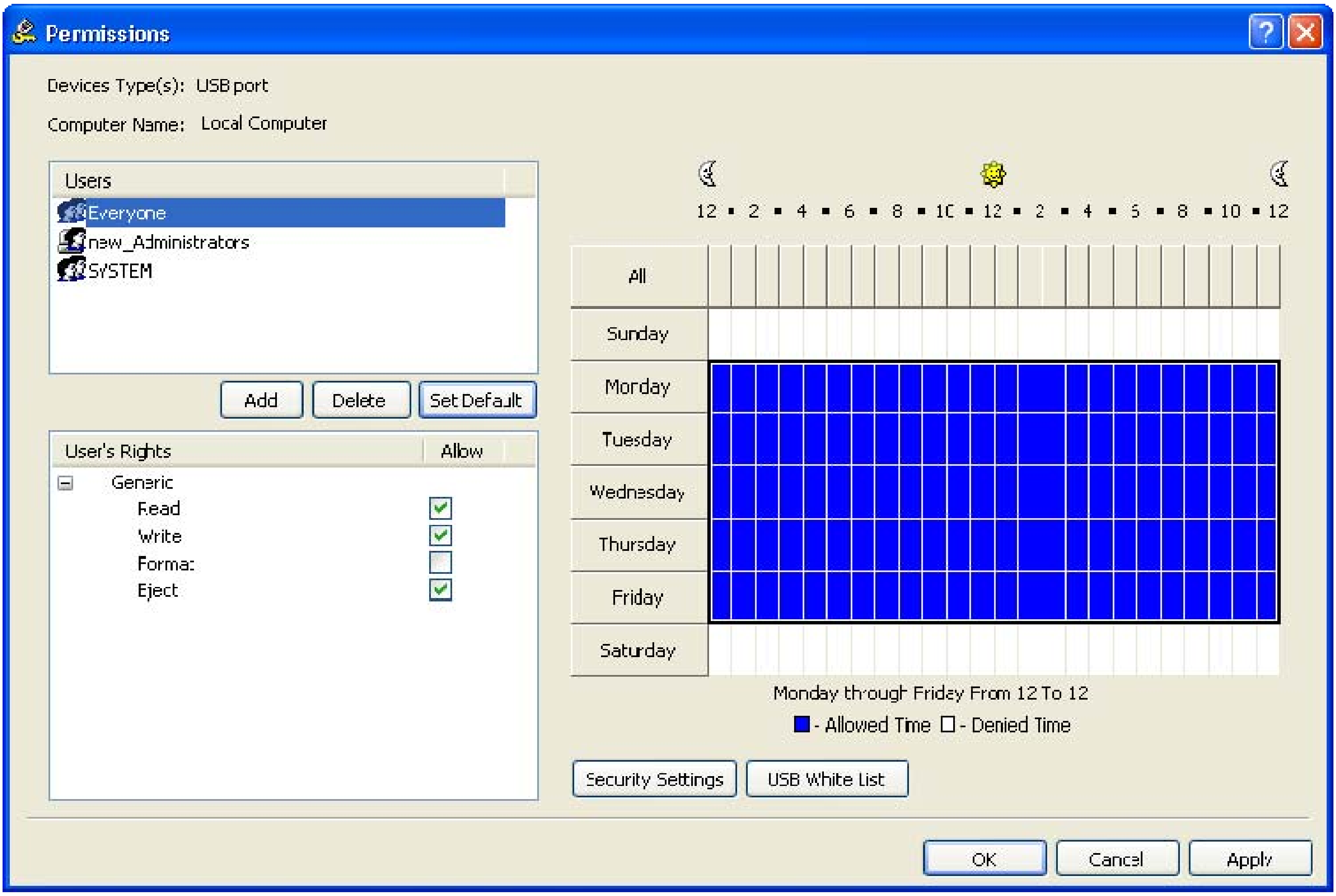
11. *USB port* (interface level) – includes all devices that can be plugged into the USB port, except the hub devices.

12. *WiFi* (type level) – includes all internal and external WiFi devices with any type of connection interface (USB, PCMCIA, etc.) to the computer.

    ***NOTE: Using the WiFi type you can control user access to the hardware device but not to the network.***

13. *Windows Mobile* (type level) – includes all Windows Mobile devices with any type of connection interface (USB, COM, IrDA, Bluetooth, WiFi) to the computer. DeviceLock controls Windows Mobile devices that are working with a PC through the Microsoft ActiveSync application or its API.

To set permissions for a device type, highlight it (use *Ctrl* and/or *Shift* to select several types simultaneously) and select *Set Permissions* from the context menu available by a right mouse click. Alternatively, you can press the appropriate button on the toolbar.



Permissions

Devices Type(s): USB port

Computer Name: Local Computer

| Users |
|---|
| Everyone |
| new_Administrators |
| SYSTEM |

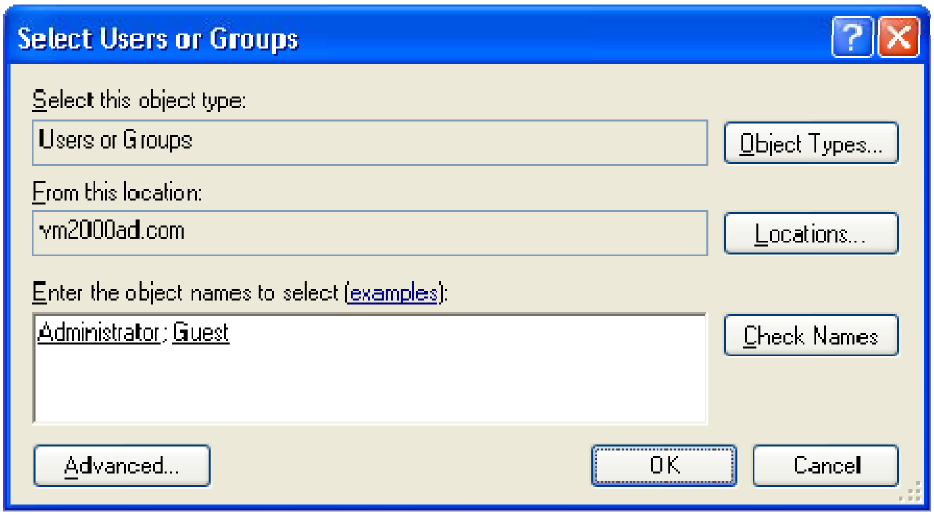
| User's Rights | Allow |
|---|---|
| ⊟ Generic | |
| Read | ☑ |
| Write | ☑ |
| Format | □ |
| Eject | ☑ |

Monday througr Friday From 12 To 12

■ - Allowed Time □ - Denied Time

The names of the users and user groups assigned to a device type are shown in the list of accounts on the top left-hand side of the *Permissions* dialog.

To add a new user or user group to the list of accounts, click on the *Add* button. You can add several accounts simultaneously.



Select Users or Groups

Select this object type: Users or Groups

From this location: vm2000ad.com

Enter the object names to select (examples): Administrator; Guest

To delete a record from the list of accounts, use the *Delete* button. Using *Ctrl* and/or *Shift* you can highlight and remove several records simultaneously.

Use the *Set Default* button to set default permissions for devices. Default permissions are enabled by using the following access selections:

| Account<br>Device Type | Everyone | Administrators | SYSTEM |
|---|---|---|---|
| Bluetooth | *Generic*: Read, Write | *Generic*: Read, Write | *Generic*: Read, Write |
| DVD/CD-ROM | *Generic*: Read, Write, Eject | *Generic*: Read, Write, Eject | *Generic*: Read, Write, Eject |
| FireWire port | *Generic*: Read, Write, Eject | *Generic*: Read, Write, Format, Eject | *Generic*: Read, Write, Format, Eject |
| Floppy | *Generic*: Read, Write, Eject | *Generic*: Read, Write, Format, Eject | *Generic*: Read, Write, Format, Eject |
| Hard disk | *Generic*: Read, Write | *Generic*: Read, Write, Format | *Generic*: Read, Write, Format |
| Infrared port | *Generic*: Read, Write | *Generic*: Read, Write | *Generic*: Read, Write |
| Parallel port | *Generic*: Read, Write | *Generic*: Read, Write | *Generic*: Read, Write |
| Removable | *Generic*: Read, Write, Eject<br>*Encrypted*: Read, Write, Format | *Generic*: Read, Write, Format, Eject<br>*Encrypted*: Read, Write, Format | *Generic*: Read, Write, Format, Eject<br>*Encrypted*: Read, Write, Format |
| Serial port | *Generic*: Read, Write | *Generic*: Read, Write | *Generic*: Read, Write |
| Tape | *Generic*: Read, Write | *Generic*: Read, Write | *Generic*: Read, Write |
| USB port | *Generic*: Read, Write, Eject | *Generic*: Read, Write, Format, Eject | *Generic*: Read, Write, Format, Eject |
| WiFi | *Generic*: Read, Write | *Generic*: Read, Write | *Generic*: Read, Write |
| Windows Mobile | *Generic*: Read, Write, Execute | *Generic*: Read, Write, Execute | *Generic*: Read, Write, Execute |

Using special time control, you can define a time when the selected user or user group will or will not have access to devices. Time control appears at the top-right side of the *Permissions* dialog. Use the left mouse button and select the allowed time. To select a denied time use the right mouse button. Also, you can use the keyboard to set times – arrow keys for navigation and the spacebar to toggle allowed/denied time.

To define which actions on devices are to be allowed for a user or user group, set the appropriate rights. All rights are divided into three groups: *Generic*, *Encrypted* and *Special Permissions*. Each group has its own set of rights:

- **Generic** – Generic rights do not apply to devices that are recognized by DeviceLock Service as encrypted devices. For more information on encryption integration, please read the **Encryption** section of this manual.

  - **Read** – enable data reading from the device. Applies to all devices types.

  - **Write** – to enable data writing to the device. With the exception of *Windows Mobile*, this right can be enabled for all devices only if **Read** is selected in the *Generic* group. It can't be disabled for *Bluetooth*, *Infrared port*, *Parallel port*, *Serial port* and *WiFi* devices types. When **Write** is disabled for USB and FireWire ports it has the following effects: storage devices such as flash drives, floppies, hard disks, DVD/CD-ROMs, etc. can be read, but not written to; non-storage devices such as printers, scanners, etc. can't be accessed**.**

  - **Format** – to enable the formatting, checking, and any other direct access of drives. You can enable this right only if **Read** is selected in the *Generic* group. Applies only to *FireWire port*, *Floppy*, *Hard disk*, *Removable* and *USB port* devices types. When this right is enabled for USB and FireWire ports it affects only storage devices plugged into these ports.

  - **Eject** – to enable ejection of the media. You can enable this right only if **Read** is selected in the *Generic* group. This right controls only ejection via software. Hardware ejection using the eject button on a device's front panel can't be prevented. Applies only to *DVD/CD-ROM*, *FireWire port*, *Floppy*, *Removable* and *USB port* devices types. When this right is enabled for USB and FireWire ports it affects only storage devices plugged into these ports.

  - **Execute** – to enable the remote code execution on the device's side. Applies only to the *Windows Mobile* device type.

- **Encrypted** – encrypted rights only apply to devices that are recognized by DeviceLock Service as encrypted devices. For more information on encryption integration, please read the **Encryption** section of this manual.

  - **Read** – to enable data reading from an encrypted device. Applies only to the *Removable* device type.

  - **Write** – to enable data writing to an encrypted device. You can enable this right only if **Read** is selected in the *Encrypted* group. Applies only to the *Removable* device type.

  - **Format** – to enable the formatting, checking, and any other direct access of encrypted drives. You can enable this right only if **Read** is selected in the *Encrypted* group. Applies only to the *Removable* device type.

- **Special Permissions** – these rights only apply to the *Windows Mobile* device type. The content types (*Calendar*, *Contacts*, *Tasks*, etc.) that are controlled by these rights represent the same content types that exist in the Microsoft ActiveSync application.

  - **Read Calendar** – to enable reading the calendar on a Windows Mobile device from a PC.

  - **Write Calendar** – to enable writing to a calendar on a Windows Mobile device from a PC.

- **Read Contacts** – to enable reading contacts on a Windows Mobile device from a PC.

- **Write Contacts** – to enable writing contacts from a PC to a Windows Mobile device.

- **Read E-mail** – to enable reading e-mails on a Windows Mobile device from a PC.

- **Write E-mail** – to enable writing e-mails from a PC to a Windows Mobile device.

- **Read Attachments** – to enable reading e-mail attachments on a Windows Mobile device from a PC. You can enable this right only if **Read E-mail** is selected in the *Special Permissions* group.

- **Write Attachments** – to enable writing e-mail attachments from a PC to a Windows Mobile device. You can enable this right only if **Write E-mail** is selected in the *Special Permissions* group.

- **Read Favorites** – to enable reading favorites on a Windows Mobile device from a PC.

- **Write Favorites** – to enable writing favorites from a PC to a Windows Mobile device.

- **Read Files** – to enable reading files on a Windows Mobile device from a PC.

- **Write Files** – to enable writing files from a PC to a Windows Mobile device.

- **Read Media** – to enable reading media content using Windows Media Player on a Windows Mobile device from a PC. You can enable this right only if **Read Files** is selected in the *Special Permissions* group and **Execute** is selected in the *Generic* group.

- **Write Media** – to enable writing media content using Windows Media Player from a PC to a Windows Mobile device. You can enable this right only if **Write Files** is selected in the *Special Permissions* group and **Execute** is selected in the *Generic* group.

- **Read Notes** – to enable reading notes on a Windows Mobile device from a PC.

- **Write Notes** – to enable writing notes from a PC to a Windows Mobile device.

- **Read Pocket Access** – to enable reading Pocket Access databases on a Windows Mobile device from a PC.

- **Write Pocket Access** – to enable writing Pocket Access databases from a PC to a Windows Mobile device.

- **Read Tasks** – to enable reading tasks on a Windows Mobile device from a PC.

- **Write Tasks** – to enable writing tasks from a PC to a Windows Mobile device.

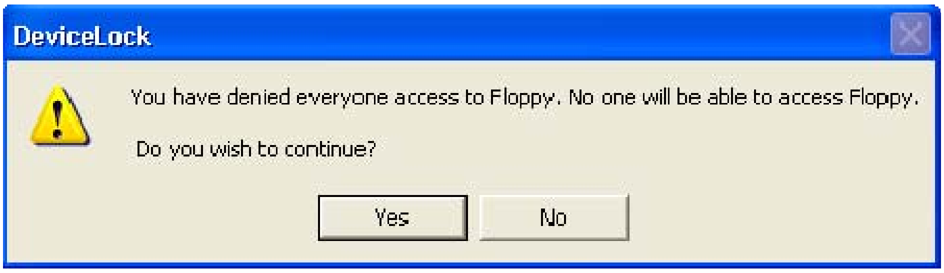
- **Read Unknown Content** – to enable reading any other uncategorized content type on a Windows Mobile device from a PC.

- **Write Unknown Content** – to enable writing any other uncategorized content type from a PC to a Windows Mobile device.

If all rights are enabled for the user account it means that this account has "full access" rights to a device. If all rights are disabled for the user account it means that this account has "no access" rights to a device.

***NOTE: The "no access" right has a priority over all other rights. It means that if the group to which some user belongs has the "no access" right but this user has "full access", the user still can't access a device. If you want to deny access for some user or group, you can just remove it from the account's list, it is not necessary to add it with "no access".***

***Also, the Everyone user has a priority over all other accounts. It means that if Everyone has the "no access" right, no one can access a device.***


DeviceLock

You have denied everyone access to Floppy. No one will be able to access Floppy.

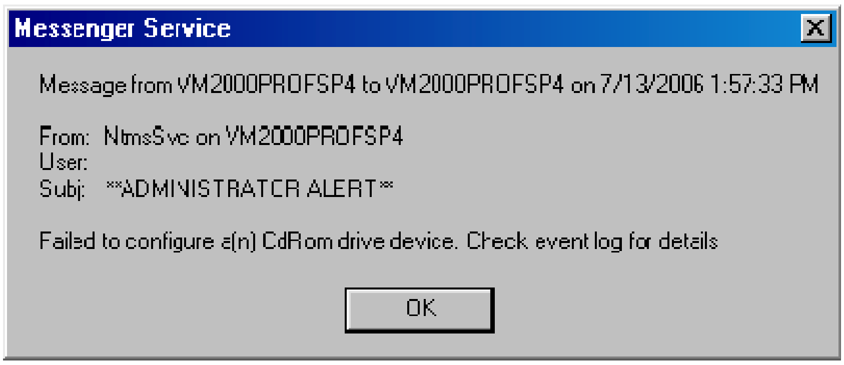
Do you wish to continue?

Even if you deny access to hard disks, users with local administrative privileges (the *SYSTEM* user and members of the local *Administrators* group) still can access the partition where Windows is installed and running.

We recommend that you add only those accounts (users and/or groups) to the list which should be able to access a device. If the account's list is empty (contains no records at all) then no one can access a device.

Also, it is recommended to add the *SYSTEM* user with "full access" to hard disks and DVD/CD-ROMs.

On some systems, users may receive the following message when they log in.


Messenger Service

Message from VM2000PROFSP4 to VM2000PROFSP4 on 7/13/2006 1:57:33 PM

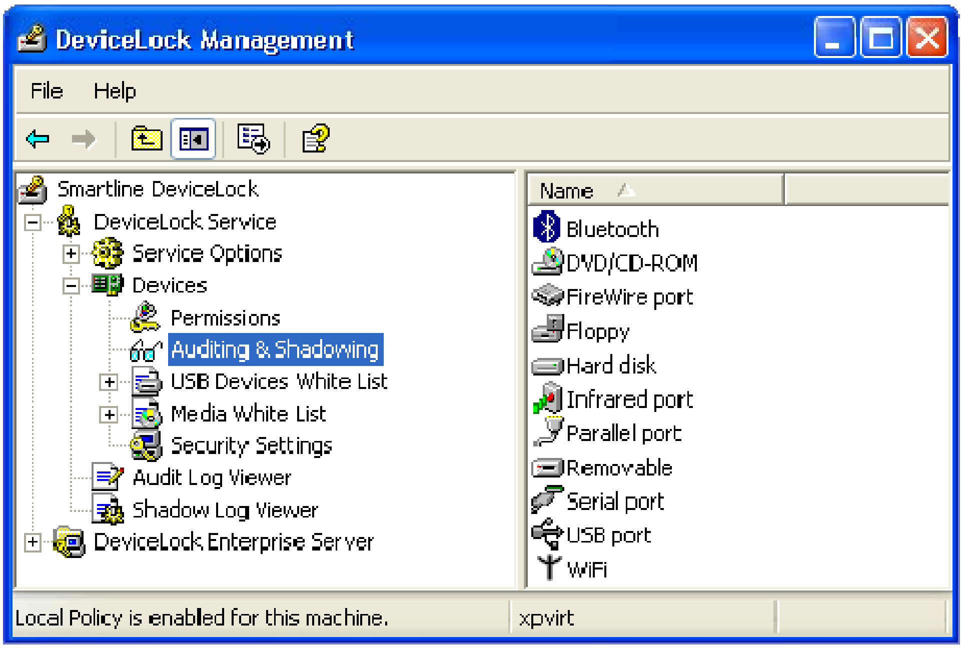
From: NtmsSvc on VM2000PROFSP4
User:
Subj: **ADMINISTRATOR ALERT**

Failed to configure a(n) CdRom drive device. Check event log for details

It means that the *SYSTEM* user can't access DVD/CD-ROM. To avoid this message, set the "full access" right for *SYSTEM* on DVD/CD-ROM.

### 5.4.2.2 Auditing & Shadowing

There is a list of device types for which you can define user-level audit and shadowing rules.



Local Policy is enabled for this machine.

There is not much difference between setting up permissions and defining audit and shadowing rules so at fist read the **Permissions** section of this manual.

DeviceLock Service can use the standard Windows event logging subsystem to log a device's information. It is extremely useful for system administrators because they can use any event log reading software to view the DeviceLock audit log. You can use the standard *Event Viewer*, for example. Also, DeviceLock Service can use its own protected proprietary log. The data from this log is sent to DeviceLock Enterprise Server and stored centrally in the database. To define what log should be used set the *Audit log type* parameter in Service Options.

DeviceLock Management Console has its own built-in audit log viewer that represents information from the event log in a more convenient form. For more information please see the **Audit Log Viewer (Service)** section of this manual.

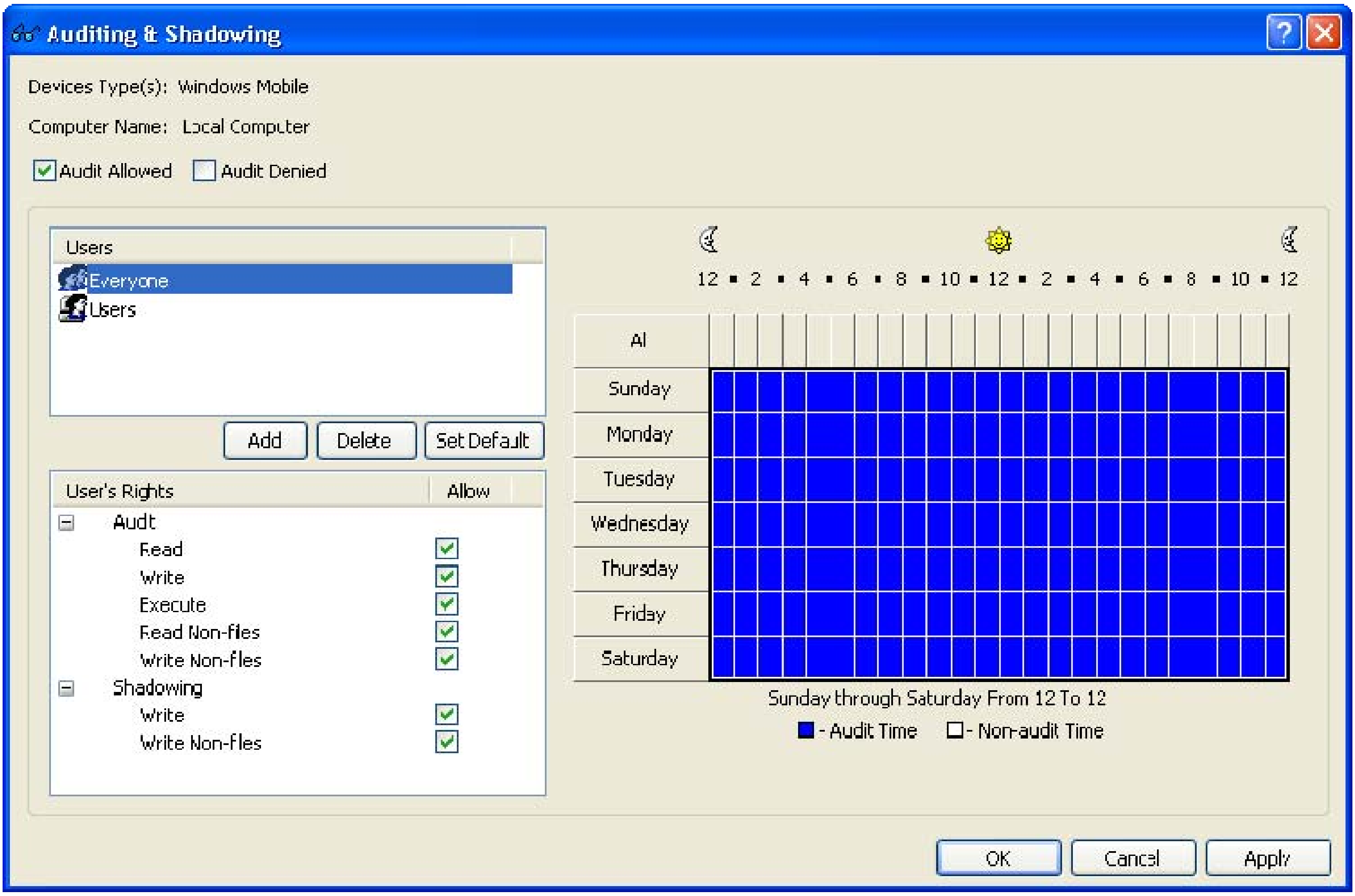
To view the audit log stored on DeviceLock Enterprise Server, use the server's audit log viewer.

Also there is an extended audit's feature called data shadowing – the ability to mirror all data copied to external storage devices or transferred through serial and parallel ports. A full copy of the data is logged. The shadow log is stored locally in the special directory (see Service Options) and then can be transferred to DeviceLock Enterprise Server specified in Service Options to store it in the SQL database.

To view the locally stored shadow log, use DeviceLock Management Console's built-in shadow log viewer. For more information please read the **Shadow Log Viewer (Service)** section of this manual.

To view the shadow log stored on DeviceLock Enterprise Server, use the server's shadow log viewer.

To define audit and shadowing rules for a device type, highlight it (use *Ctrl* and/or *Shift* to select several types simultaneously) and select *Set Auditing & Shadowing* from the context menu available by the right mouse click. Alternatively, you can press the appropriate button on the toolbar.



Devices Type(s): Windows Mobile

Computer Name: Local Computer

☑ Audit Allowed ☐ Audit Denied

Users

- Everyone
- Users

| User's Rights | Allow |
|---|---|
| ⊟ Audt | |
| Read | ☑ |
| Write | ☑ |
| Execute | ☑ |
| Read Non-fles | ☑ |
| Write Non-fles | ☑ |
| ⊟ Shadowing | |
| Write | ☑ |
| Write Non-fles | ☑ |

Sunday through Saturday From 12 To 12

There are two types of user access that can be logged to the audit log:

- *Allowed* – all access attempts that were permitted by DeviceLock Service, i.e. the user was able to access a device.
- *Denied* – all access attempts that were blocked by DeviceLock Service, i.e. the user was not able to access a device.

To enable logging to the audit log for one or both of these access types, check *Audit Allowed* and/or *Audit Denied*. These flags are not linked to users/groups, they are related to a whole device type.

The names of the users and user groups assigned to a device type are shown in the list of accounts on the top left-hand side of the *Auditing & Shadowing* dialog.

To add a new user or user group to the list of accounts, click on the *Add* button. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the *Delete* button. Using *Ctrl* and/or *Shift* you can highlight and remove several records simultaneously.

Use the *Set Default* button to set default audit and shadowing rules for devices: members of the *Users* group and the *Everyone* account have **Read** and **Write** audit rights and shadowing is disabled for them.

Using special time control, you can define a time when the audit rule for the selected user or user group will or will not be active. Time control appears at the top-right side of the *Auditing & Shadowing* dialog. Use the left mouse button and select the time when the rule is active (audit time). To select a time when the rule is not active (non-audit time), use the right mouse button. Also, you can use the keyboard to set times – arrow keys for navigation and the spacebar to toggle audit/non-audit time.

To define which user’s actions on devices are to be logged to either the audit or shadow log, set the appropriate audit rights. All rights are divided into two groups: *Audit* and *Shadowing*. Each group has its own set of rights:

- **Audit** – rights that belong to this group are responsible for actions logged into the audit log.

    - **Read** – to log the read access attempts. For *Bluetooth*, *FireWire port*, *Infrared port*, *Parallel port*, *Serial port*, *USB port* and *WiFi* devices types you can enable this right only if **Write** is selected in the *Audit* group.

    - **Write** – to log the write access attempts. For *Bluetooth*, *FireWire port*, *Infrared port*, *Parallel port*, *Serial port*, *USB port* and *WiFi* devices types you can enable this right only if **Read** is selected in the *Audit* group.

    - **Execute** – to log access attempts to remotely execute a code on the device’s side. Applies only to the *Windows Mobile* device type.

    - **Read Non-files** – to log the read access attempts for non-file objects (*Calendar*, *Contacts*, *Tasks*, etc.). Applies only to the *Windows Mobile* device type.

    - **Write Non-files** – to log the write access attempts for non-file objects (*Calendar*, *Contacts*, *Tasks*, etc.). Applies only to the *Windows Mobile* device type.

- **Shadowing** – rights that belong to this group are responsible for actions logged into the shadow log.

- **Write** – to enable shadowing of all data written by the user. Applies only to *DVD/CD-ROM*, *Floppy*, *Parallel port*, *Removable*, *Serial port* and *Windows Mobile* devices types.

- **Write Non-files** – to enable shadowing of all non-file objects (*Calendar*, *Contacts*, *Tasks*, etc.) written by the user. Applies only to the *Windows Mobile* device type.

In the following table you may see what audit rights can be assigned to what devices types and what is written to the log. For all events DeviceLock Service logs event's type, date and time, device's type, user name and process information as well as the specific event's information described in the table below:

| Rights / Device Type | Audit: Read | Audit: Write | Audit: Execute | Audit: Read Non-files | Audit: Write Non-files | Shadowing: Write | Shadowing: Write Non-files |
|---|---|---|---|---|---|---|---|
| Bluetooth | *Device Access* action is written to the audit log | *Device Access* action is written to the audit log | - | - | - | - | - |
| DVD/CD-ROM | *Open*, *Device Access* and *Direct Access* events, file names and flags (*Read*, *DirectRead, Eject*, *DirList*) write to the audit log | *Open*, *Device Access* and *Direct Access* events and flags (*Write*, *Del*, *DirectWrite*) write to the audit log | - | - | - | CD/DVD images in the CUE format and/or files write to the shadow log | - |
| FireWire port | *Insert*, *Remove* and *Device Access* actions and device names write to the audit log | *Insert*, *Remove* and *Device Access* actions and device names write to the audit log | - | - | - | - | - |

| Rights<br>Device Type | Audit: Read | Audit: Write | Audit: Execute | Audit: Read Non-files | Audit: Write Non-files | Shadowing: Write | Shadowing: Write Non-files |
|---|---|---|---|---|---|---|---|
| Floppy | *Open*, *Mount*, *Unmount* and *Direct Access* actions, file names and flags (*Read*, *DirectRead, Eject*, *DirList*) write to the audit log | *Direct Access*, *Delete*, *Rename* and *Create new* actions, file names and flags (*Write*, *DirectWrite*, *Format*, *Del*, *DirCreate*) write to the audit log | - | - | - | Files are written to the shadow log | - |
| Hard disk | *Open*, *Mount*, *Unmount* and *Direct Access* actions, file names and flags (*Read*, *DirectRead, Eject*, *DirList*) write to the audit log | *Direct Access*, *Delete*, *Rename* and *Create new* actions, file names and flags (*Write*, *DirectWrite*, *Format*, *Del*, *DirCreate*) write to the audit log | - | - | - | - | - |
| Infrared port | *Device Access* action writes to the audit log | *Device Access* action writes to the audit log | - | - | - | - | - |
| Parallel port | *Device Access* action writes to the audit log | *Device Access* action writes to the audit log | - | - | - | All data sent to the port is written to the shadow log | - |

| Rights / Device Type | Audit: Read | Audit: Write | Audit: Execute | Audit: Read Non-files | Audit: Write Non-files | Shadowing: Write | Shadowing: Write Non-files |
|---|---|---|---|---|---|---|---|
| Removable | *Open*, *Mount*, *Unmount* and *Direct Access* actions, file names and flags (*Read*, *DirectRead, Eject*, *DirList*) write to the audit log | *Direct Access*, *Delete*, *Rename* and *Create new* actions, file names and flags (*Write*, *DirectWrite*, *Format*, *Del*, *DirCreate*) write to the audit log | - | - | - | Files are written to the shadow log | - |
| Serial port | *Mount*, *Unmount*, *Insert*, *Remove* and *Device Access* actions write to the audit log | *Mount*, *Unmount*, *Insert*, *Remove* and *Device Access* actions write to the audit log | - | - | - | All data sent to the port is written to the shadow log | - |
| Tape | *Open*, *Device Access* and *Direct Access* actions and flags (*Read*, *DirectRead*) write to the audit log | *Open*, *Device Access* and *Direct Access* actions and flags (*Write*, *DirectWrite*) write to the audit log | - | - | - | - | - |
| USB port | *Insert*, *Remove* and *Device Access* actions and device names write to the audit log | *Insert*, *Remove* and *Device Access* actions and device names write to the audit log | - | - | - | - | - |
| WiFi | *Device Access* action writes to the audit log | *Device Access* action writes to the audit log | - | - | - | - | - |

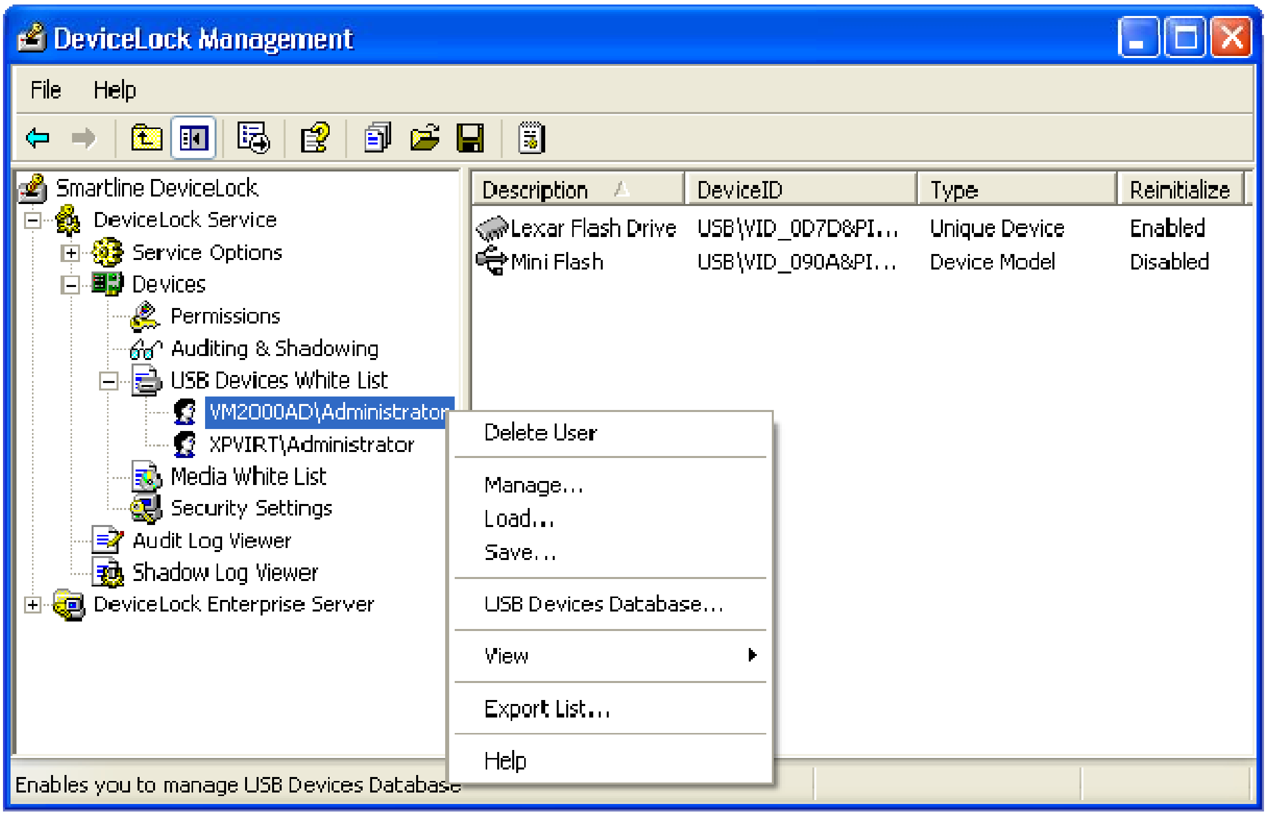
| Rights / Device Type | Audit: Read | Audit: Write | Audit: Execute | Audit: Read Non-files | Audit: Write Non-files | Shadowing: Write | Shadowing: Write Non-files |
|---|---|---|---|---|---|---|---|
| Windows Mobile | *Read File*, *Get File Attributes*, *Create New File*, *Overwrite/Create File*, *Open File* and *Open/Create File* actions, file names and flags write to the audit log | *Write File*, *Delete File*, *Rename File*, *Create File*, *Create New File*, *Overwrite/ Create File*, *Open File*, *Open/Create File*, *Overwrite*, *Set File Attributes*, *Create Shortcut* and *Copy File* actions, file names and flags write to the audit log | *Invoke* and *Execute* actions, file names and function (procedure) names write to the audit log | *Read Calendar*, *Read Contact*, *Read Favorite*, *Read E-mail*, *Read Attachment*, *Read Note*, *Read Task*, *Read Media*, *Read Pocket Access* and *Read Unknown* actions and object names write to the audit log | *Write Calendar*, *Delete Calendar*, *Write Contact*, *Delete Contact*, *Write Favorite*, *Delete Favorite*, *Write E-mail*, *Delete E-Mail*, *Write Attachment*, *Delete Attachment*, *Write Note*, *Delete Note*, *Write Task*, *Delete Task*, *Write Media*, *Delete Media*, *Write Pocket Access*, *Delete Pocket Access*, *Write Unknown* and *Delete Unknown* actions and object names write to the audit log | Files are written to the shadow log | All data that contains in non-files objects (*Calendar*, *Contacts*, *Tasks*, etc.) is written to the shadow log |

***NOTE: Until either Audit Allowed or Audit Denied is checked for the device type, logging to the audit log is disabled for that device in spite of defined audit rules.***

***Also logging to the audit log is disabled for devices that are in the white list and for a whole class of devices if the access control for that class is turned off in Security Settings.***

### 5.4.2.3 USB Devices White List

The devices white list allows you to authorize only specific devices that will not be locked regardless of any other settings. The intention is to allow special devices but lock all other devices.



| Description | DeviceID | Type | Reinitialize |
|---|---|---|---|
| Lexar Flash Drive | USB\VID_0D7D&PI... | Unique Device | Enabled |
| Mini Flash | USB\VID_090A&PI... | Device Model | Disabled |

Enables you to manage USB Devices Database

Devices in the white list can be defined individually for every user and group.

For more information on how the devices white list works, please read the **Managed Access Control** section of this manual.

There are two ways to identify devices in the white list:

1. **Device Model** – represents all devices of the same model. Each device is identified by a combination of *Vendor Id* (*VID*) and *Product Id* (*PID*).

   This combination of VID and PID describes a unique device model but not a unique device unit. It means that all devices belonging to the certain model of the certain vendor will be recognized as the one authorized device.

2. **Unique Device** – represents a unique device unit. Each device is identified by a combination of *Vendor Id* (*VID*), *Product Id* (*PID*) and *Serial Number* (*SN*).

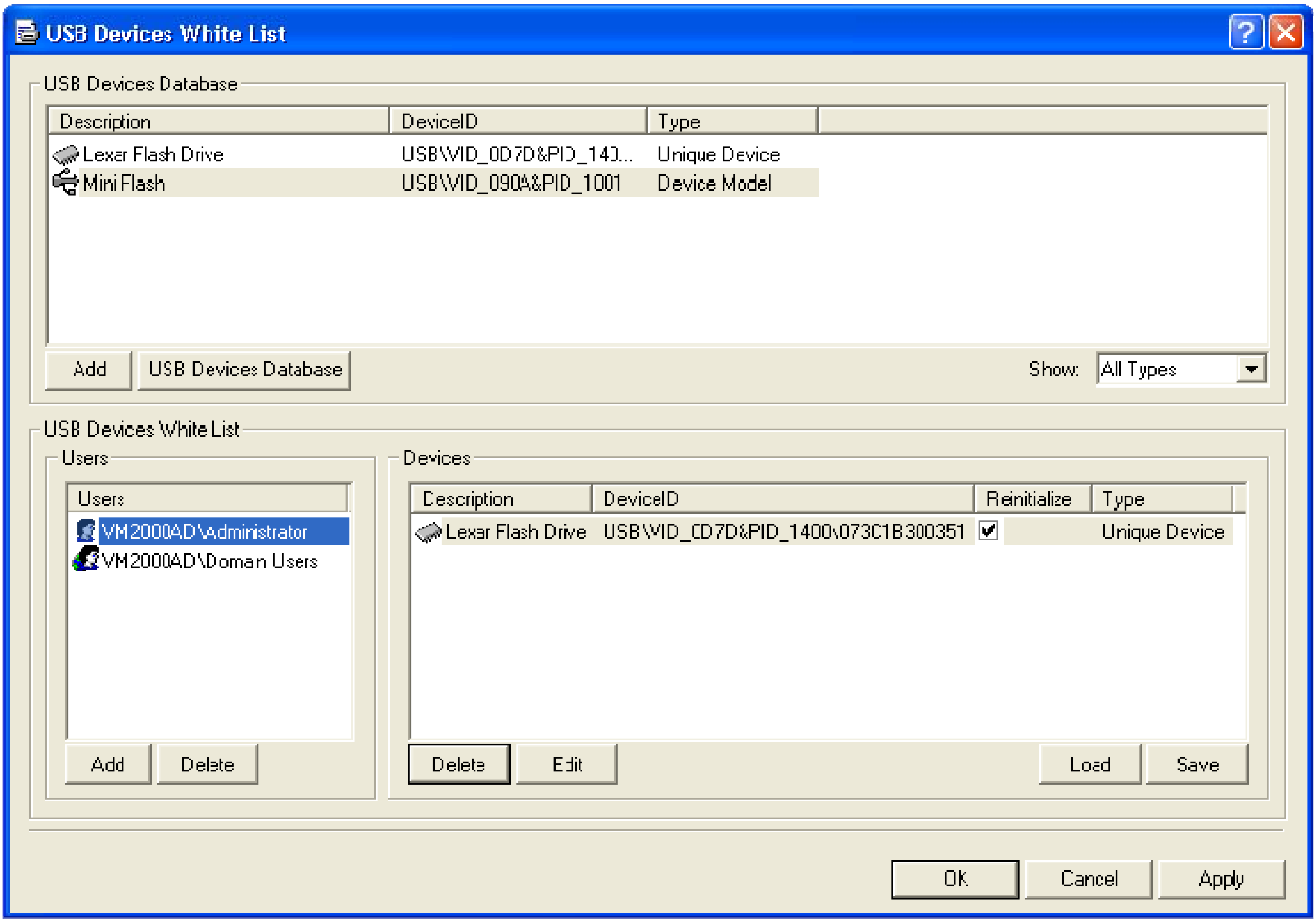
   Not all devices have serial numbers assigned. A device can be added to the white list as a **Unique Device** only if its manufacturer has assigned a serial number to it at the production stage.

Two steps are required to authorize a device:

1. Add the device to the devices database, making it available for adding to the white list.

2. Add the device to the white list for the specified user/group. In effect, this designates the device as authorized and allows it for this user/group at the interface (USB) level.

To define the white list, select *Manage* from the context menu available with a right mouse click. Alternatively, you can press the appropriate button on the toolbar.



| Description | DeviceID | Type |
|---|---|---|
| Lexar Flash Drive | USB\VID_0D7D&PID_14J... | Unique Device |
| Mini Flash | USB\VID_090A&PID_1001 | Device Model |

Show: All Types

| Users |
|---|
| VM2000AD\Administrator |
| VM2000AD\Doman Users |

| Description | DeviceID | Reinitialize | Type |
|---|---|---|---|
| Lexar Flash Drive | USB\VID_CD7D&PID_1400\073C1B300351 | ☑ | Unique Device |

In the *USB Devices Database* list at the top of the dialog, you can see devices that were added to the database.

Once devices are added from the database to the white list of a certain user, they become authorized devices for which access control is disabled when this user is logged in.

You can add a device to the *USB Devices White List* in two steps:

1. Select a user or user group for which this device should be allowed.

   Press the *Add* button under the *Users* list to add the user/group. To delete the record from the *Users* list, press the *Delete* button.

2. Select the appropriate device record in the *USB Devices Database* list and press the *Add* button.

   If the device has an assigned serial number, it can be added to the white list two times: as **Device Type** and as **Unique Device**. In this case **Device Type** has a priority over **Unique Device**.

When the *Control as Type* flag is checked, access control for white listed devices is disabled only on the interface (USB) level. If the white listed device (e.g. USB Flash Drive) belongs to both levels: interface (USB) and type (Removable), the permissions (if any) for the type level will be applied anyway.

Otherwise, if the *Control as Type* flag is unchecked, access control on the type level is also disabled. For example, by disabling the *Control as Type* flag for the USB Flash Drive you can bypass security checking on the Removable level.

If it is necessary to force the white listed device to reinitialize (replug) when the new user is logged in, check the *Reinitialize* flag.

Some USB devices (like the mouse) won't work without being reinitialized, so it is recommended to keep this flag checked for non-storage devices.

It is recommended to keep the *Reinitialize* flag unchecked for storage devices (such as flash drives, CD/DVD-ROMs, external hard drives and so on).

Some USB devices can't be reinitialized from DeviceLock Service. It means that their drivers do not support the software replug. If such a device was white listed but doesn't work, the user should remove it from the port and then insert it again manually to restart the device's driver.

To edit a device's description, select the appropriate record in *USB Devices White List* and press the *Edit* button.

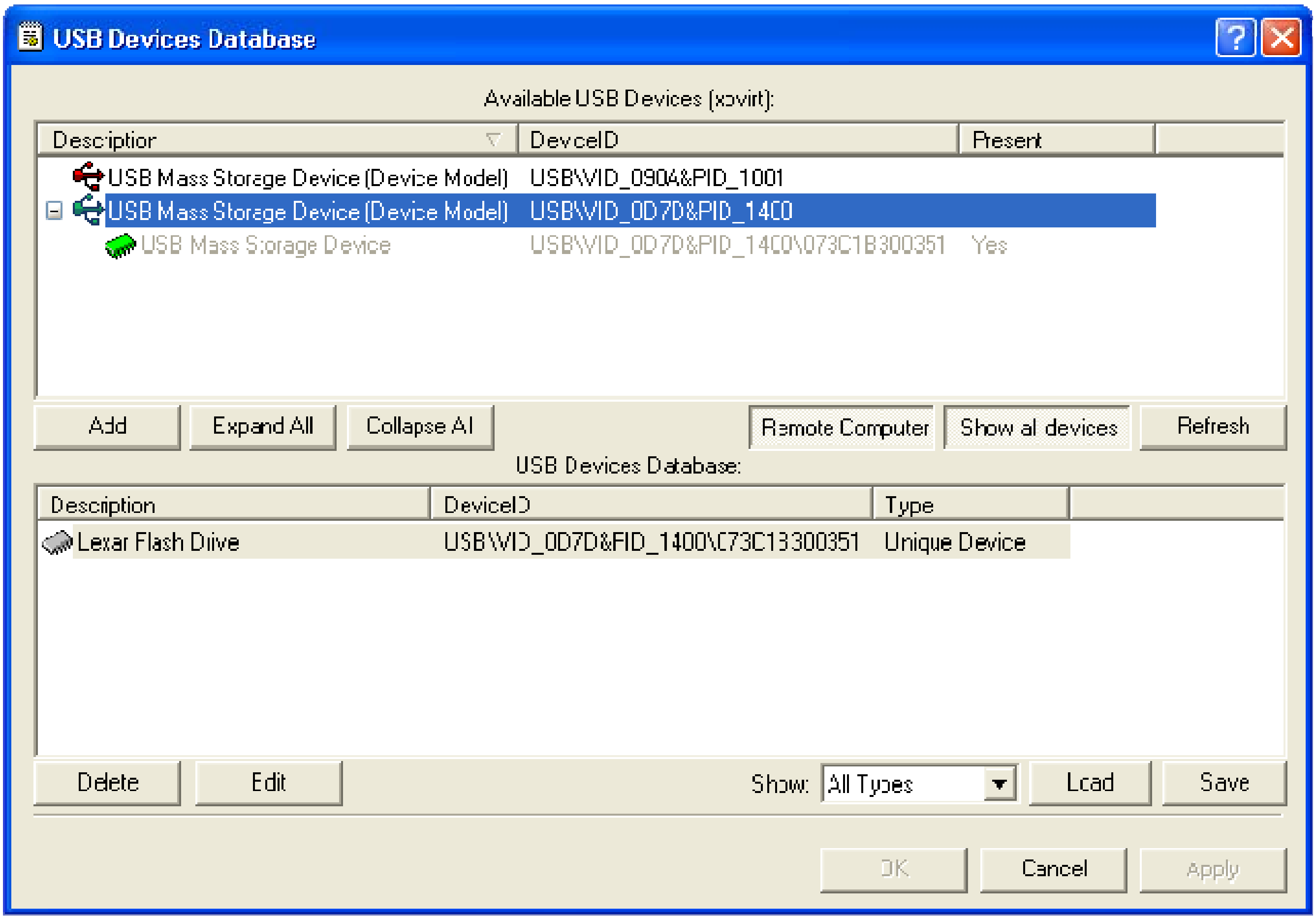
Press the *Delete* button to delete a selected device's record (use *Ctrl* and/or *Shift* to select several records simultaneously).

To save the white list to an external file, press the *Save* button, then select the name of the file. To load a previously saved white list, press the *Load* button and select a file that contains the list of devices.

If you need to manage the devices database, you can press the *USB Devices Database* button and open the appropriate dialog.

### 5.4.2.3.1 USB Devices Database

In the *USB Devices Database* dialog you can add new devices to the database and edit existing records.



Available USB Devices (xovirt):

| Description | DeviceID | Present |
|---|---|---|
| USB Mass Storage Device (Device Model) | USB\VID_090A&PID_1001 | |
| ⊟ USB Mass Storage Device (Device Model) | USB\VID_0D7D&PID_1400 | |
| USB Mass Storage Device | USB\VID_0D7D&PID_1400\073C1B300351 | Yes |

USB Devices Database:

| Description | DeviceID | Type |
|---|---|---|
| Lexar Flash Drive | USB\VID_0D7D&PID_1400\073C1B300351 | Unique Device |

Show: All Types

Before the device can be authorized in the white list, it must be added to the database.

In the *Available USB Devices* list at the top of the dialog, you can see all devices available on the computer.

Devices are displayed in the form of a simple tree, where the parent item represents **Device Model** and the child item represents **Unique Device**. If there is no **Unique Device** item, then this device doesn't have an assigned serial number.

This list displays either all currently plugged-in devices (if the *Show all devices* button is not pressed) or all the devices ever plugged into the port on this computer (if the *Show all devices* button is pressed).

The list of available devices is automatically refreshed and displays new devices as soon as they arrive. To manually refresh this list, press the *Refresh* button.

To retrieve devices from the remote computer, press the *Remote Computer* button. This button is unavailable when you are connected to the local computer.

In the *USB Devices Database* list at the bottom of the dialog, you can see devices that are already in the database.

You can add devices to this list by selecting the desired device's record in the *Available USB Devices* list and pressing the *Add* button. If the device is already in the database, it can't be added there a second time.

To edit a device description, select the appropriate record in the *USB Devices Database* list and press the *Edit* button.

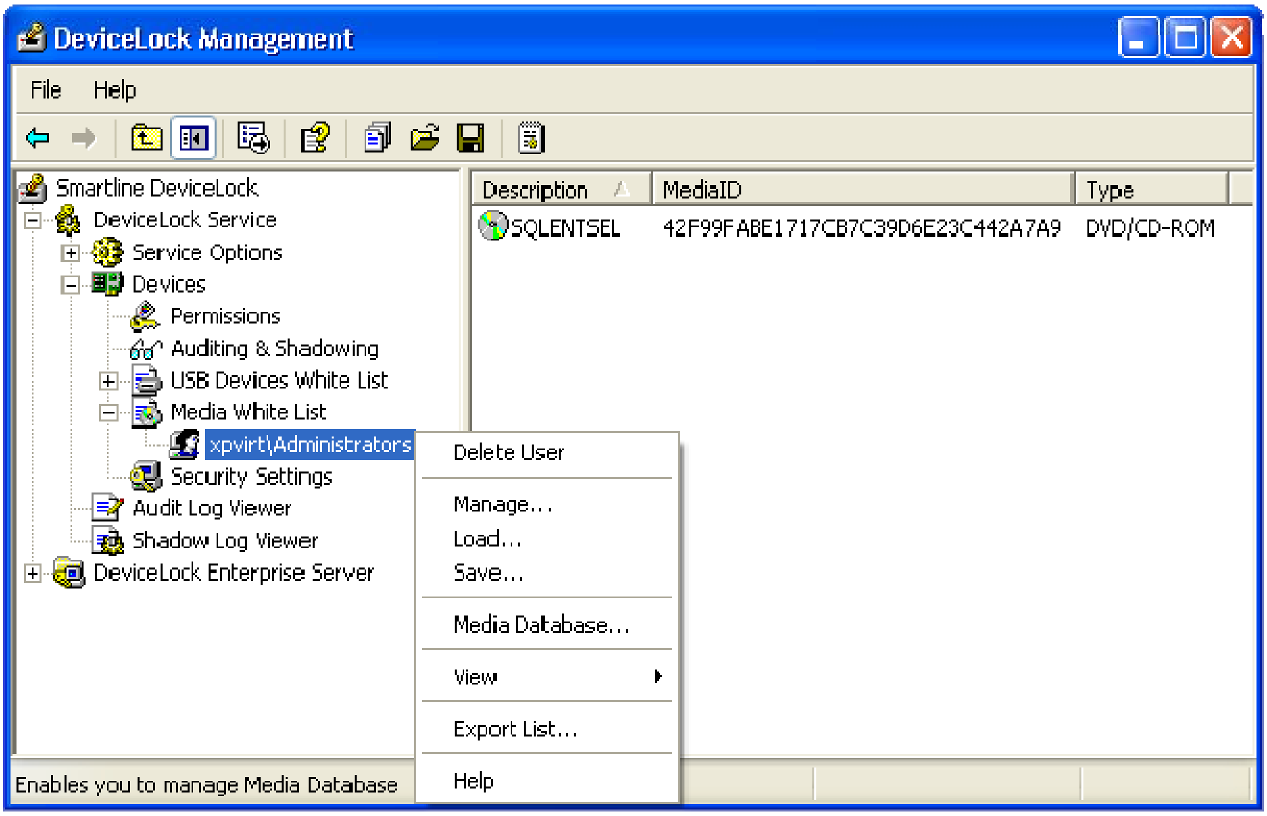
Press the *Delete* button to delete a selected device's record (use *Ctrl* and/or *Shift* to select several records simultaneously).

You can also save a current database to an external file. To save the database to an external file, press the *Save* button, then select the type of the file —.txt or .csv.

To load a previously saved database, press the *Load* button and select a file that contains the list of devices.

### 5.4.2.4 Media White List

The media white list allows you to uniquely identify a specific DVD/CD-ROM disk by the data signature and authorize read access to it, even when DeviceLock Service has otherwise blocked DVD/CD-ROM drives.



| Description | MediaID | Type |
|---|---|---|
| SQLENTSEL | 42F99FABE1717CB7C39D6E23C442A7A9 | DVD/CD-ROM |

The media white list can be configured to grant access to a collection of approved DVD/CD-ROM disks by certain users and groups, so that only authorized users are able to use the approved information.

Any change to the content of the media will change the data signature, thus invalidating authorization. If the user copies the authorized media without any changes in the original content (byte-to-byte copy) then such a copy is accepted as the authorized media.

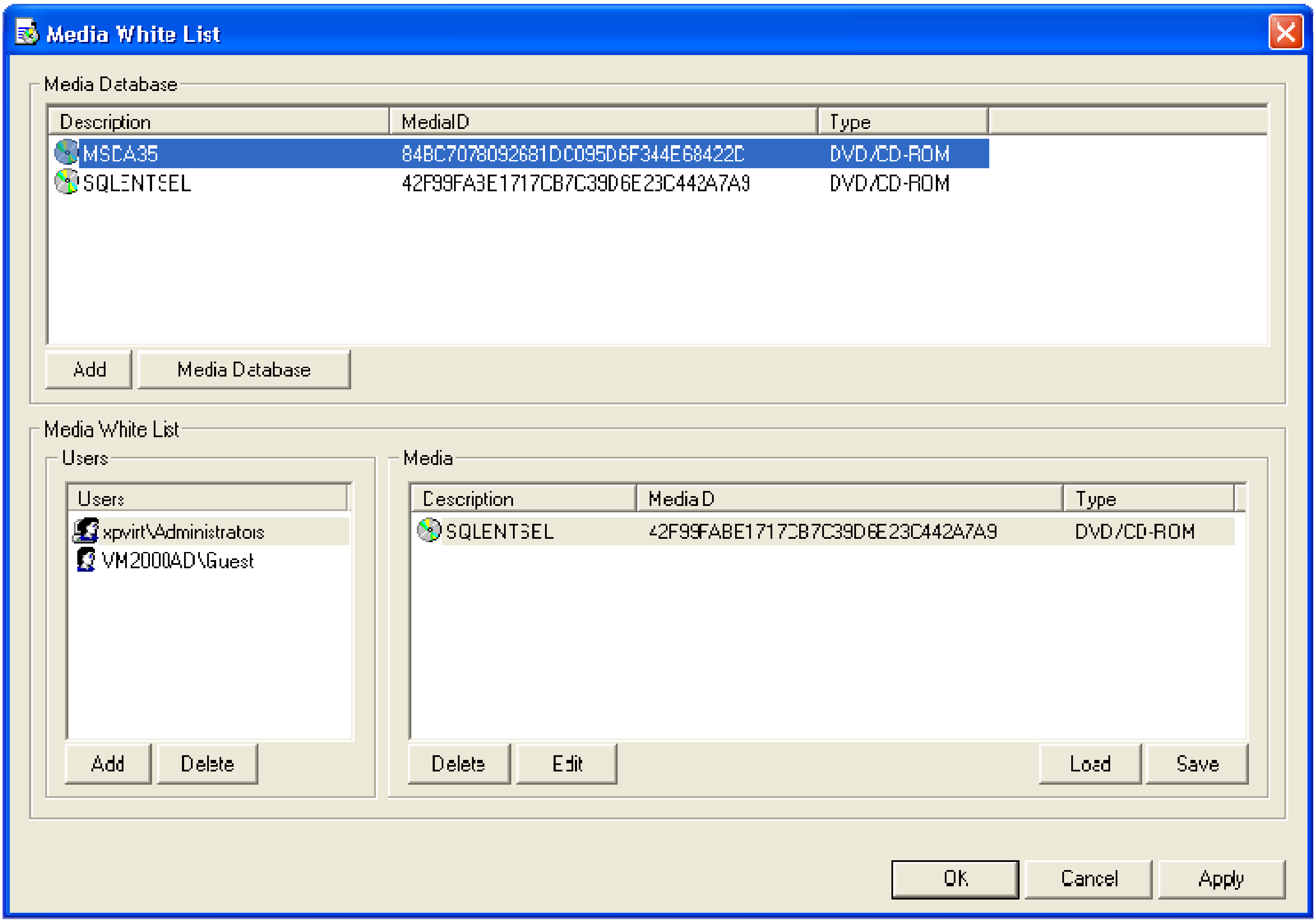
***NOTE: Access to white listed media can be granted only on the type (DVD/CD-ROM) level. If the DVD/CD drive plugs into the port (USB or FireWire) and access to this port is denied, then access to the white listed media is denied too.***

Two steps are required to authorize media:

1. Add the media to the media database, making it available for adding to the white list.

2. Add the media to the white list for the specified user/group. In effect, this designates the media as authorized and allows it (read access) for this user/group at the type (DVD/CD-ROM) level.

To define a media white list, select *Manage* from the context menu available with a right mouse click. Alternatively, you can press the appropriate button on the toolbar.



| Description | MediaID | Type |
|---|---|---|
| MSCA35 | 84BC7078092681DC095D6F344E68422C | DVD/CD-ROM |
| SQLENTSEL | 42F99FA3E1717CB7C39D6E23C442A7A9 | DVD/CD-ROM |

| Users |
|---|
| xpvirt\Administrators |
| VM2000AD\Guest |

| Description | MediaID | Type |
|---|---|---|
| SQLENTSEL | 42F99FABE1717CB7C39D6E23C442A7A9 | DVD/CD-ROM |

In the *Media Database* list at the top of the dialog, you can see all media that were added to the database.

Once media are added from the database to the white list of a certain user, they become authorized media for which access control is disabled when this user is logged in.

You can add media to the *Media White List* in two steps:

1. Select a user or user group for which this media should be allowed.

   Press the *Add* button under the *Users* list to add the user/group. To delete the record from the *Users* list, press the *Delete* button.

2. Select the appropriate media record in the *Media Database* list and press the *Add* button.

To edit a media's description, select the appropriate record in *Media White List* and press the *Edit* button.

Press the *Delete* button to delete a selected media's record (use *Ctrl* and/or *Shift* to select several records simultaneously).

To save the media white list to an external file, press the *Save* button, then select the name of the file.

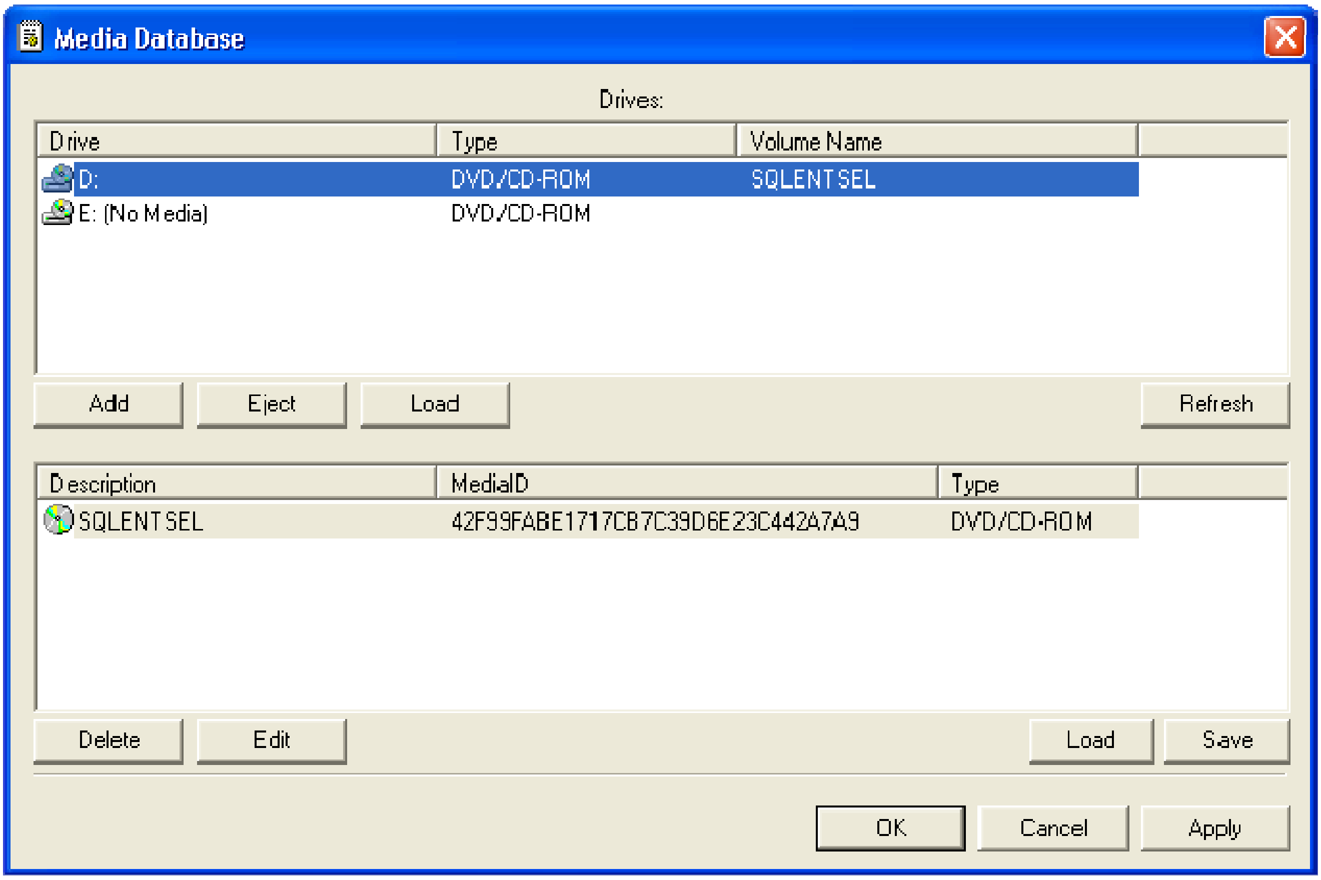
To load a previously saved white list, press the *Load* button and select a file that contains the list of medias.

If you need to manage the media database, you can press the *Media Database* button and open the appropriate dialog.

***NOTE: Using the media white list you can only allow read access to authorized media. It is impossible to authorize media for writing.***

### 5.4.2.4.1 Media Database

In the *Media Database* dialog you can add new media to the database and edit existing records.



| Drive | Type | Volume Name |
|---|---|---|
| D: | DVD/CD-ROM | SQLENTSEL |
| E: (No Media) | DVD/CD-ROM | |

| Description | MediaID | Type |
|---|---|---|
| SQLENTSEL | 42F99FABE1717CB7C39D6E23C442A7A9 | DVD/CD-ROM |

Before the media can be authorized in the white list, it must be added to the database.

In the *Drives* list at the top of the dialog, you can see all drives available on the local computer that can contain medias.

The list is automatically refreshed and displays new medias as soon as they arrive. To manually refresh this list, press the *Refresh* button.

In the list at the bottom of the dialog, you can see media that are already in the database.

You can add media to this list by selecting the desired record in the *Drives* list and pressing the *Add* button. It takes some time (depending on the media size) to authorize the media. If the media is already in the database, it can’t be added there a second time.

To edit a media description, select the appropriate record in the list and press the *Edit* button.

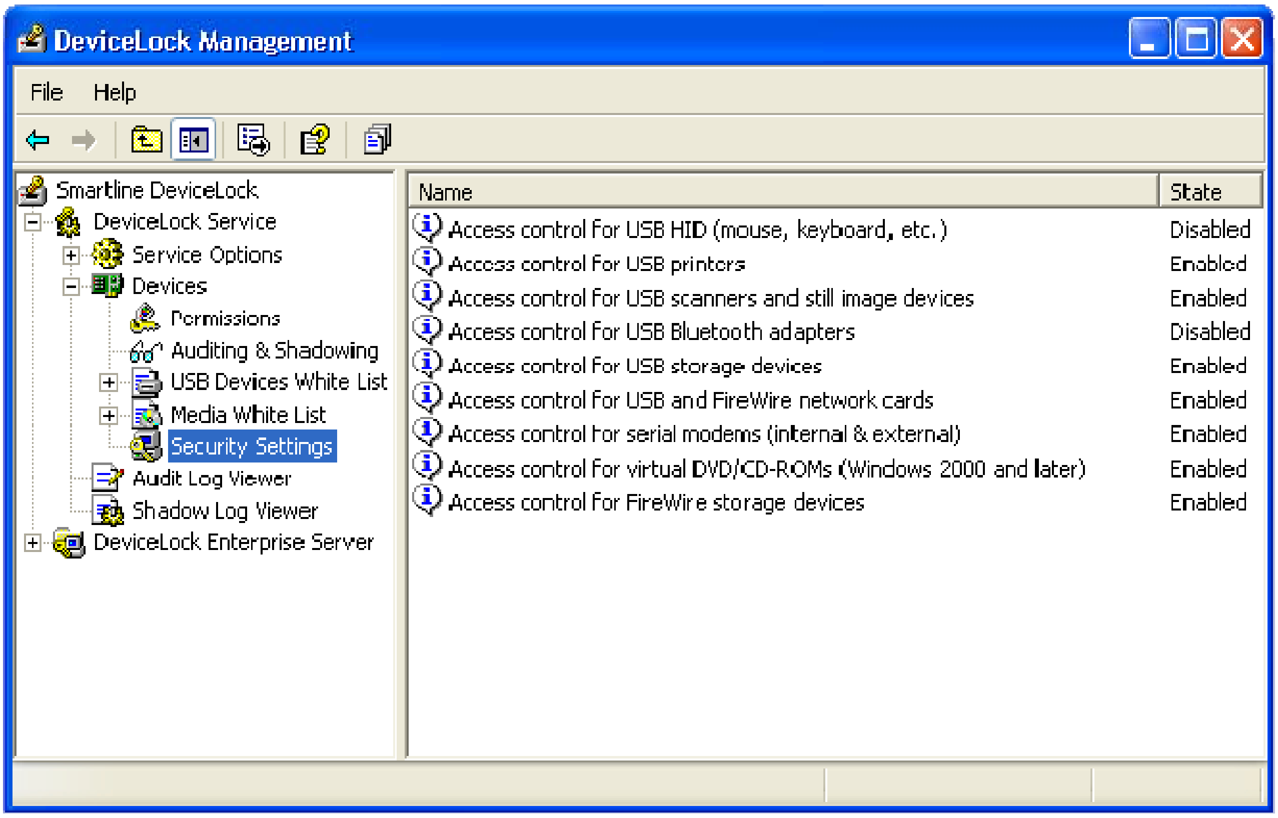
Press the *Delete* button to delete a selected record (use *Ctrl* and/or *Shift* to select several records simultaneously).

You can also save a current database to an external file. To save the database to an external file, press the *Save* button, then select the type of the file —.txt or .csv.

To load a previously saved database, press the *Load* button and select a file that contains the list of medias.

### 5.4.2.5 Security Settings

There is a list of additional security parameters that affect permissions and audit rules for some devices types.



| Name | State |
|---|---|
| Access control for USB HID (mouse, keyboard, etc.) | Disabled |
| Access control for USB printers | Enabled |
| Access control for USB scanners and still image devices | Enabled |
| Access control for USB Bluetooth adapters | Disabled |
| Access control for USB storage devices | Enabled |
| Access control for USB and FireWire network cards | Enabled |
| Access control for serial modems (internal & external) | Enabled |
| Access control for virtual DVD/CD-ROMs (Windows 2000 and later) | Enabled |
| Access control for FireWire storage devices | Enabled |

These security parameters enable you to keep some device types completely locked, but allow the use of certain device classes without need to authorize every device in the white list.

For example, you can disallow using all USB devices except any mouse and keyboard devices that connect through the USB.

DeviceLock supports these additional security parameters:

- *Access control for USB HID* – if checked, allows DeviceLock Service to audit and control access to Human Interface Devices (mouse, keyboard, etc.) plugged into the USB port. Otherwise, even if the USB port is locked, Human Interface Devices continue to function as usual and audit is not performed for these devices.

- *Access control for USB printers* – if checked, allows DeviceLock Service to audit and control access to printers plugged into the USB port. Otherwise, even if the USB port is locked, printers continue to function as usual and audit is not performed for these devices.

- *Access control for USB scanners and still image devices* – if checked, allows DeviceLock Service to audit and control access to scanners and still image devices plugged into the USB port. Otherwise, even if the USB port is locked, these devices continue to function as usual and audit is not performed for these devices.

- *Access control for USB Bluetooth adapters* – if checked, allows DeviceLock Service to audit and control access to Bluetooth adapters plugged into the USB port. Otherwise, even if the USB port is locked, Bluetooth adapters continue to function as usual and audit is not performed for these devices.

  This parameter affects audit and access control on the interface (USB) level only. If the device belongs to both levels, the permissions and audit rules (if any) for the type (Bluetooth) level will be applied anyway.

- *Access control for USB storage devices* – if checked, allows DeviceLock Service to audit and control access to storage devices (such as flash drives) plugged into the USB port. Otherwise, even if the USB port is locked, storage devices continue to function as usual and audit is not performed for these devices.

  This parameter affects audit and access control on the interface (USB) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the type (Removable, Floppy, DVD/CD-ROM or Hard disk) level will be applied anyway.

- *Access control for USB and FireWire network cards* – if checked, allows DeviceLock Service to audit and control access to network cards plugged into the USB or FireWire (IEEE 1394) port. Otherwise, even if the USB or FireWire port is locked, network cards continue to function as usual and audit is not performed for these devices.

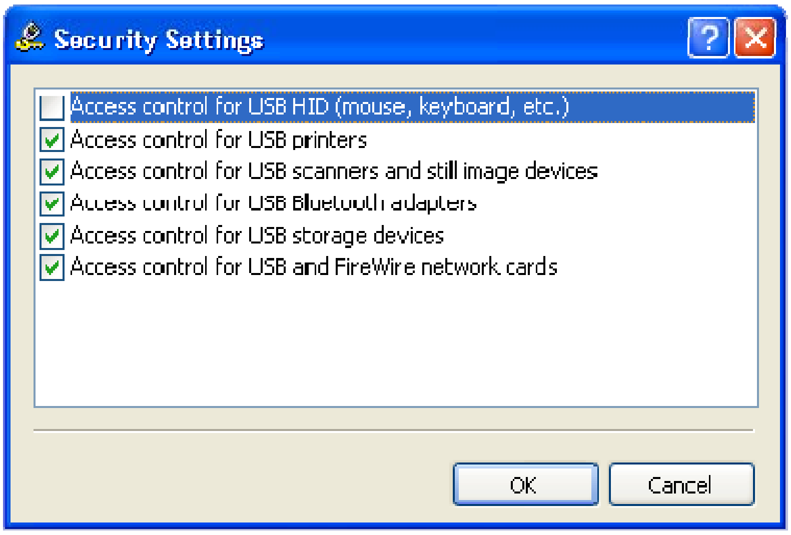
- *Access control for FireWire storage devices* – if checked, allows DeviceLock Service to audit and control access to storage devices plugged into the FireWire port. Otherwise, even if the FireWire port is locked, storage devices continue to function as usual and audit is not performed for these devices.

  This parameter affects audit and access control on the interface (FireWire) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the type (Removable, Floppy, DVD/CD-ROM or Hard disk) level will be applied anyway.

- *Access control for serial modems (internal & external)* – if checked, allows DeviceLock Service to audit and control access to modems plugged into the COM port. Otherwise, even if the COM port is locked, modems continue to function as usual and audit is not performed for these devices.

- *Access control for virtual CD-ROMs* – if checked, allows DeviceLock Service to audit and control access to virtual (software emulated) CD-ROMs. Otherwise, even if the CD-ROM device is locked, virtual drives continue to function as usual and audit is not performed for these devices. This parameter is effective only for Windows 2000 and later systems.

To change these security parameters, double-click the parameter's record to switch its state (enable/disable). Alternatively, you can select *Manage* from the context menu available with a right mouse click or press the appropriate button on the toolbar.



□ Access control for USB HID (mouse, keyboard, etc.)
☑ Access control for USB printers
☑ Access control for USB scanners and still image devices
☑ Access control for USB Bluetooth adapters
☑ Access control for USB storage devices
☑ Access control for USB and FireWire network cards

Security Settings are similar to the device white list but there are three major differences:

1. Using Security Settings you can only allow a whole class of device. You can't allow only a specific device model, while locking out all other devices of the same class.

   For example, by disabling *Access control for USB storage devices*, you allow the use of all USB storage devices, no matter their model and vendor. By specifying the one USB Flash Drive model you want to allow on the devices white list, you ensure that all other USB storage devices remain locked out.

2. Using Security Settings you can only select from the predefined device classes. If the device doesn't belong to one of the predefined classes, then it can't be allowed.

   For example, there is no specific class for smart card readers in Security Settings, so if you want to allow a smart card reader when the port is locked, you should use the devices white list.

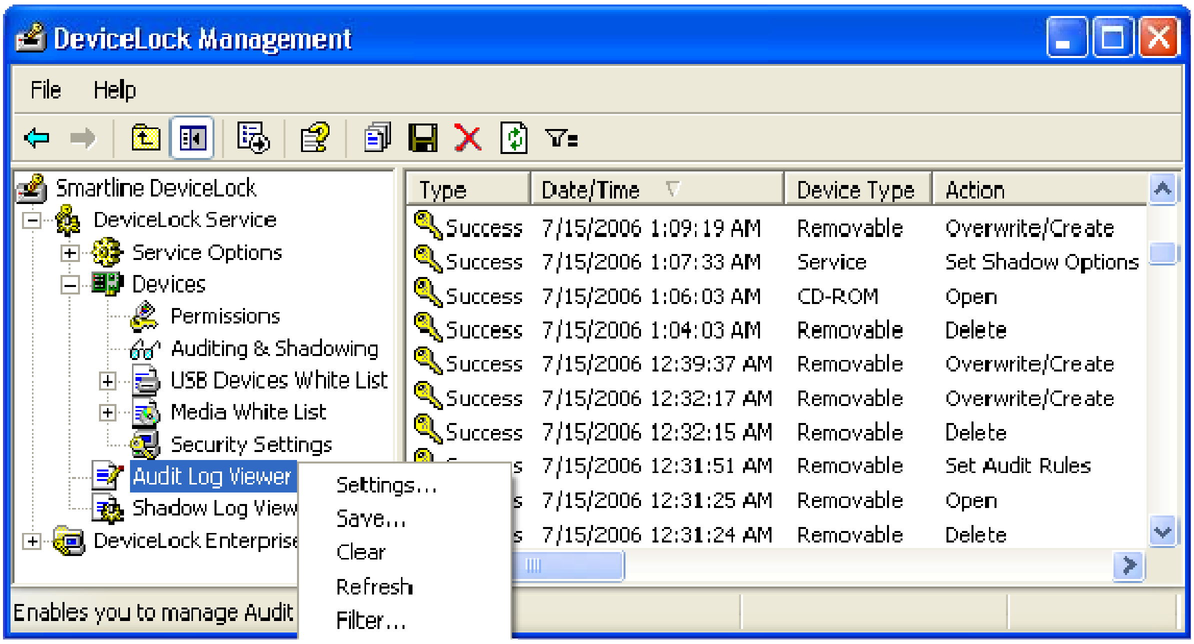
3. Security Settings can't be defined on a per user basis; they affect all users of the local computer. However, devices in the white list can be defined individually for the every user and group.

***NOTE: Security Settings work only for those devices that are using standard Windows drivers. Some devices are using proprietary drivers and their classes can't be recognized by DeviceLock Service. Hence, access control to such devices can't be disabled via Security Settings. In this case you may use the devices white list to authorize such devices individually.***

### 5.4.3 Audit Log Viewer (Service)

There is a built-in audit log viewer that allows you to retrieve DeviceLock audit log records from a computer's local Windows event logging subsystem.

The standard Windows event logging subsystem is used to store audit records, only if *Event Log* or *Event & DeviceLock Logs* is selected in the *Audit log type* parameter in Service Options. Otherwise, audit records are stored in the proprietary log and can be viewed using the server's audit log viewer.



| Type | Date/Time | Device Type | Action |
|---|---|---|---|
| Success | 7/15/2006 1:09:19 AM | Removable | Overwrite/Create |
| Success | 7/15/2006 1:07:33 AM | Service | Set Shadow Options |
| Success | 7/15/2006 1:06:03 AM | CD-ROM | Open |
| Success | 7/15/2006 1:04:03 AM | Removable | Delete |
| Success | 7/15/2006 12:39:37 AM | Removable | Overwrite/Create |
| Success | 7/15/2006 12:32:17 AM | Removable | Overwrite/Create |
| Success | 7/15/2006 12:32:15 AM | Removable | Delete |
| s | 7/15/2006 12:31:51 AM | Removable | Set Audit Rules |
| s | 7/15/2006 12:31:25 AM | Removable | Open |
| s | 7/15/2006 12:31:24 AM | Removable | Delete |

The audit log stores events generated by a user's device-related activities that fall under the audit rules. For more information please read the **Auditing & Shadowing** section of this manual.

Also, changes in a DeviceLock Service's configuration generate events in the audit log, if the appropriate flag is enabled in Service Options.

The columns of this viewer are defined as follows:

- *Type* – the class of an event, either *Success* for allowed access or *Failure* for denied access.
- *Date/Time* – the date and the time when an event was received by DeviceLock Service.
- *Device Type* – the type of device involved.
- *Action* – the user's activity type.
- *Name* – the name of the object (file, USB device, etc.).
- *Information* – other device-specific information for the event, such as the access flags, devices names, and so on.

- *User* – the name of the user associated with this event.

- *PID* – the identifier of the process associated with this event.

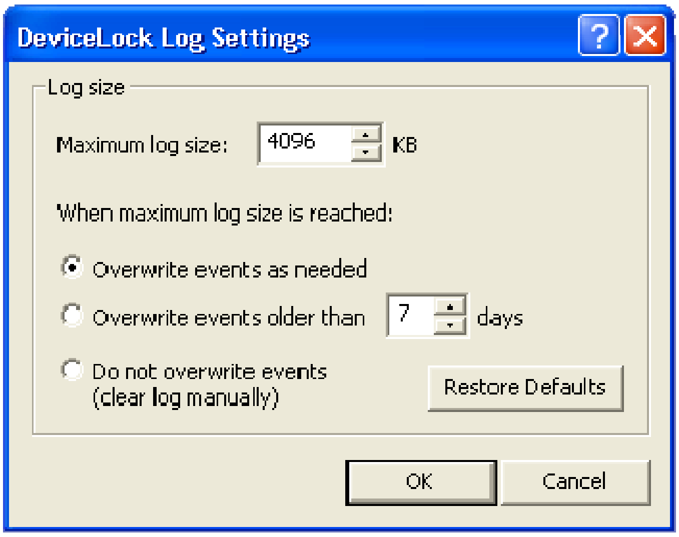
- *Process* – the fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path.

To refresh the list of events, select *Refresh* from the context menu available by a right mouse click or press the appropriate button on the toolbar.

To clear all events from the audit log, select *Clear* from the context menu or press the appropriate button on the toolbar.

### 5.4.3.1 Audit Log Settings (Service)

To define a maximum log size and what Windows should do if the audit log becomes full, use *Settings* from the context menu of Audit Log Viewer or press the appropriate button on the toolbar.



DeviceLock Log Settings

Log size

Maximum log size: 4096 KB

When maximum log size is reached:

● Overwrite events as needed

○ Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

In the *Maximum log size* parameter you can specify the maximum size of the log file (in kilobytes). The log file is creating and used only by the Windows Event Log service. This file is usually located in the *%SystemRoot%\system32\config* directory and has the *DeviceLo.evt* name.

To specify what Windows should do when an event log is full (when *Maximum log size* is reached) select one of these options:

- *Overwrite events as needed* – the system will overwrite old events if *Maximum log size* is reached.

- *Overwrite events older than* – specifies that records that are newer than this value will not be overwritten (specified in days).

- *Do not overwrite events (clear log manually)* – the system will not overwrite old events if *Maximum log size* is reached and you will need to clear events manually.

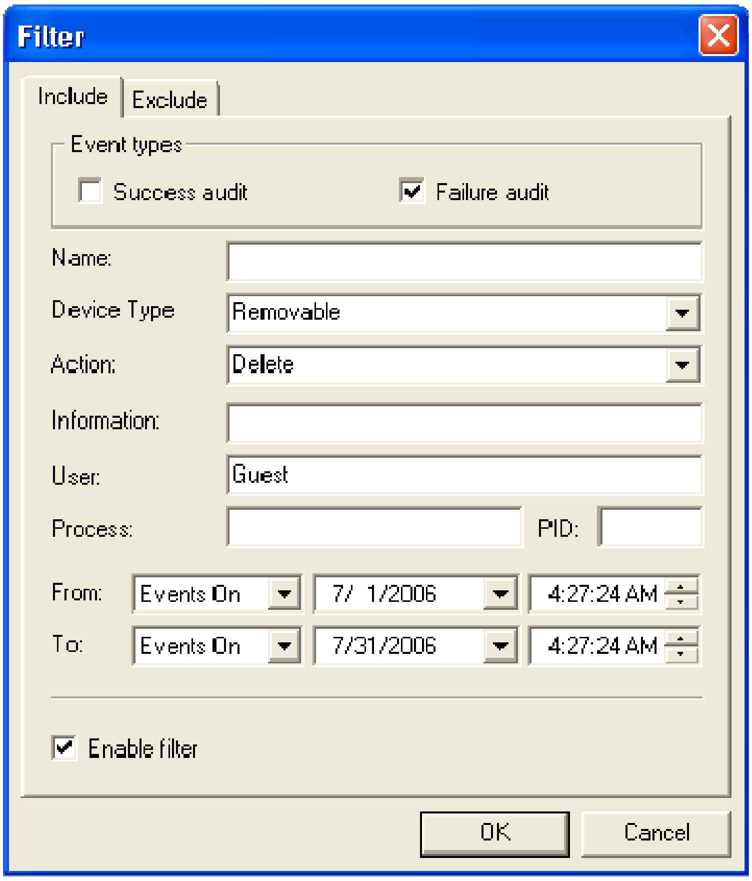
***NOTE: When the event log is full and there are no records that Windows can overwrite, then DeviceLock Service is unable to write new audit records to this log.***

If you wish to reset current settings to the default values, use the *Restore Defaults* button. Default values are:

- The *Maximum log size* parameter is set to 512 kilobytes.
- The *Overwrite events older than* option is selected and set to 7 days.

### 5.4.3.2 Audit Log Filter (Service)

You can filter data in Audit Log Viewer so only records that meet specific conditions are displayed in the list.



Filter

Include | Exclude

Event types

☐ Success audit ☑ Failure audit

Name:

Device Type: Removable

Action: Delete

Information:

User: Guest

Process: PID:

From: Events On 7/ 1/2006 4:27:24 AM

To: Events On 7/31/2006 4:27:24 AM

☑ Enable filter

To open the *Filter* dialog, use *Filter* from the context menu of the Audit Log Viewer or press the appropriate button on the toolbar.

There are two types of filters:

- **Include** – only entries that match conditions specified on the *Include* tab are shown in the list.
- **Exclude** – entries that match conditions specified on the *Exclude* tab are not shown in the list.

To use any filter, you should activate it first. Check the *Enable filter* flag to make a filter active. To temporary deactivate the filter, uncheck the *Enable filter* flag.

When the filter is active you can define its condition by entering values into the following fields:

- *Success audit* – specifies whether to filter device access attempts that were successful.
- *Failure audit* – specifies whether to filter device access attempts that failed.
- *Name* – the text that matches a value in the Audit Log Viewer's *Name* column. This field is not case-sensitive and you may use wildcards.
- *Device Type* – the text that matches a value in the Audit Log Viewer's *Device Type* column. This field is not case-sensitive and you may use wildcards.
- *Action* – the text that matches a value in the Audit Log Viewer's *Action* column. This field is not case-sensitive and you may use wildcards.
- *Information* – the text that matches a value in the Audit Log Viewer's *Information* column. This field is not case-sensitive and you may use wildcards.
- *User* – the text that matches a value in the Audit Log Viewer's *User* column. This field is not case-sensitive and you may use wildcards.
- *Process* – the text that matches a value in the Audit Log Viewer's *Process* column. This field is not case-sensitive and you may use wildcards.
- *PID* – the number that matches a value in the Audit Log Viewer's *PID* column.
- *From* – specifies the beginning of the interval of events that you want to filter. Select *First Event* to see events starting with the first event recorded in the log. Select *Events On* to see events that occurred starting with a specific time and date.
- *To* – specifies the end of the range of events that you want to filter. Select *Last Event* to see events ending with the last event recorded in the log. Select *Events On* to see events that occurred ending with a specific time and date.

The AND logic is applied to all specified fields and between active filters (Include/Exclude). It means that the filter's result includes only those records that comply with all defined conditions.

If you don't want to include a field to the filter's condition, just leave this field empty.

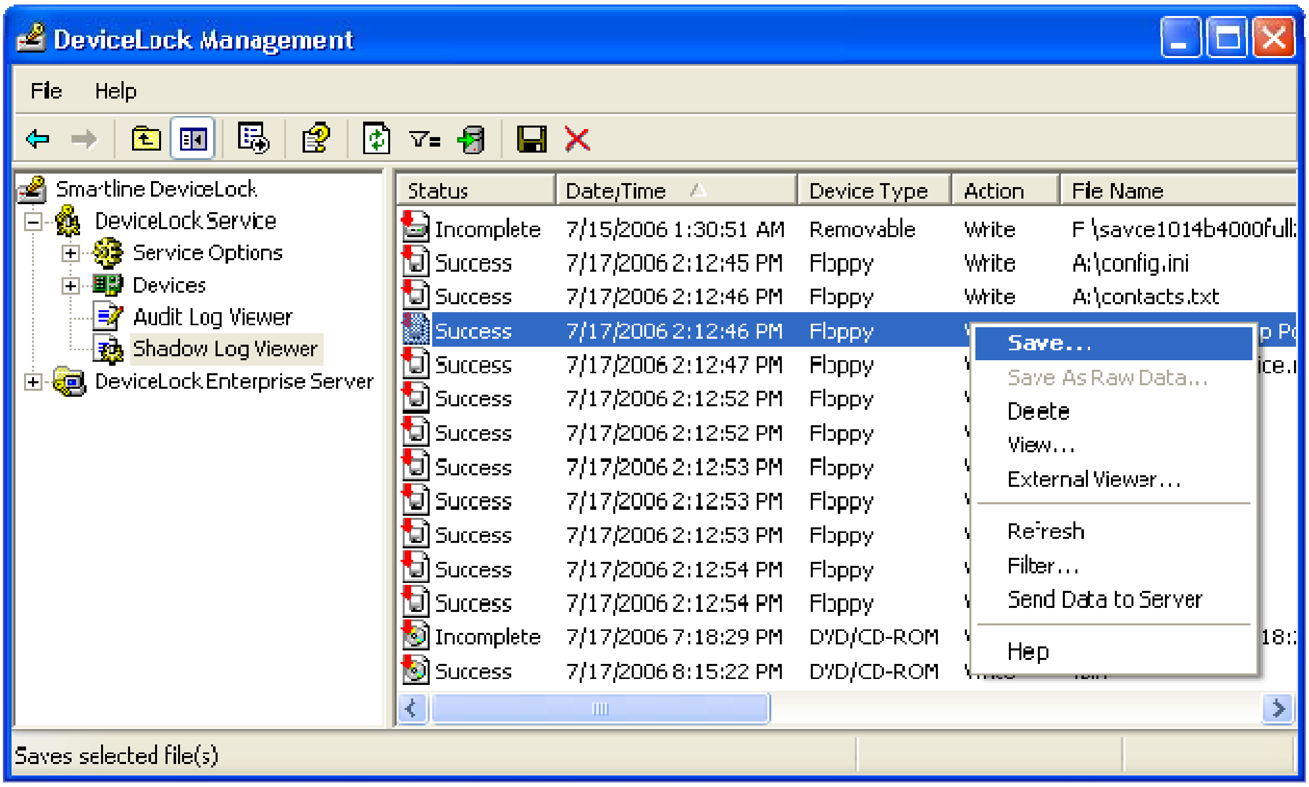
For some fields you can use wildcards. A wildcard is a character such as an asterisk (*) or a question mark (?) that is used to represent one or more characters when you are defining a filter.

Use the asterisk as a substitute for zero or more characters. If you are looking for a name that you know starts with "*win*" but you cannot remember the rest of the name, type the following: *win**. This locates all names that begin with "*win*" including *Windows*, *Winner*, and *Wind*.

Use the question mark as a substitute for a single character in a name. For example, if you type *win?*, you will locate *Wind* but not *Windows* or *Winner*.

## 5.4.4 Shadow Log Viewer (Service)

There is a built-in shadow log viewer that allows you to retrieve the shadow log from DeviceLock Service.



| Status | Date/Time | Device Type | Action | File Name |
|---|---|---|---|---|
| Incomplete | 7/15/2006 1:30:51 AM | Removable | Write | F:\savce1014b4000full: |
| Success | 7/17/2006 2:12:45 PM | Floppy | Write | A:\config.ini |
| Success | 7/17/2006 2:12:46 PM | Floppy | Write | A:\contacts.txt |
| Success | 7/17/2006 2:12:46 PM | Floppy | | p P |
| Success | 7/17/2006 2:12:47 PM | Floppy | | ice.i |
| Success | 7/17/2006 2:12:52 PM | Floppy | | |
| Success | 7/17/2006 2:12:52 PM | Floppy | | |
| Success | 7/17/2006 2:12:53 PM | Floppy | | |
| Success | 7/17/2006 2:12:53 PM | Floppy | | |
| Success | 7/17/2006 2:12:53 PM | Floppy | | |
| Success | 7/17/2006 2:12:54 PM | Floppy | | |
| Success | 7/17/2006 2:12:54 PM | Floppy | | |
| Incomplete | 7/17/2006 7:18:29 PM | DVD/CD-ROM | | 18: |
| Success | 7/17/2006 8:15:22 PM | DVD/CD-ROM | | |

Saves selected file(s)

The typical DeviceLock configuration assumes that the shadow data is stored on DeviceLock Enterprise Server. In this case all shadow data which is originally logged and cached by DeviceLock Service on the local computer is periodically moved to the server. The local shadow log is cleared as soon as the data is successfully moved to the server, so to view this data, you should use the server's shadow log viewer.

However, in some cases you may need to view the shadow log of a certain computer. This need arises when, for example, you do not use DeviceLock Enterprise Server at all or when the server is being used, but for some reason the data still exists on the client computer.

The columns of this viewer are defined as follows:

- *Status* – indicates the status of the record, either *Success* when data is successfully logged or *Incomplete* when data is possibly not completely logged.

- *Date/Time* – the date and the time when the data was transferred.
- *Device Type* – the type of device involved.
- *Action* – the user's activity type.
- *File Name* – the original path to the file or the auto-generated name of the data that originally was not a file (such as CD/DVD images, data written directly to the media or transferred through the serial/parallel ports).
- *File Size* – the size of the data.
- *User* – the name of the user transferred the data.
- *PID* – the identifier of the process used to transfer the data.
- *Process* – fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path.

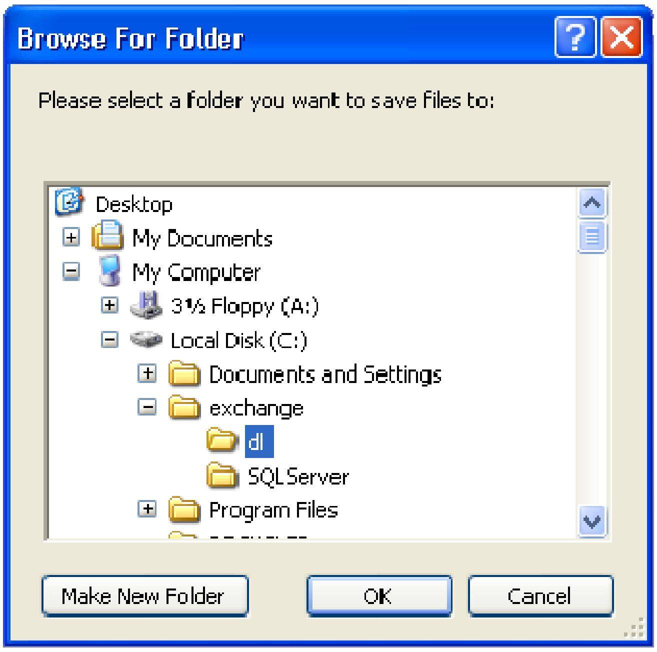
Use the context menu available via a right mouse click on every record.

a. Open

To open the file from a selected record with its associated application, use *Open* from the context menu. If there is no associated application then the 'Open With' dialog is shown. In case the record has no associated data (its size is 0 or it was not logged), *Open* is disabled.

b. Save

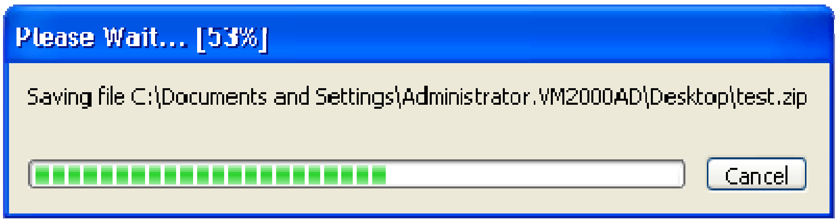
If you need to save data from a selected record to your local computer, use *Save* from the context menu or press the appropriate button on the toolbar. Using *Ctrl* and/or *Shift* you can highlight and save the data from several records simultaneously.


Browse For Folder

Please select a folder you want to save files to:

In case the record has no associated data (its size is 0 or it was not logged), *Save* is disabled in the context menu and on the toolbar.

The progress bar appears when you are saving a large file.



Saving file C:\Documents and Settings\Administrator.VM2000AD\Desktop\test.zip

You may press the *Cancel* button at any time to abort the saving process. In this case the resultant file on the local computer will be incomplete and will contain only that part of the data which was received before you aborted the saving process.

If the data was transferred by the user as a file, it is stored in the shadow log as a file and can be saved to the local computer as a file too.

When a user has written data to a CD/DVD disk, all data is stored in a shadow log as a single CD/DVD image (one image per each written CD/DVD disk or session) in the CUE format.

CD/DVD images as well as other data that originally was not transferred as files (direct media access or serial/parallel ports transfer) have auto-generated names based on the action's type, drive's letter or device's name and time/date (e.g. *direct_write(E:) 19:18:29 17.07.2006.bin*).

Each CD/DVD image is saving to the local computer as two files: the data file with the *.bin* extension (e.g. *direct_write(E_) 19_18_29 17_07_2006.bin*) and the cue sheet file that has the same name as its data file with the *.cue* extension (e.g. *direct_write(E_) 19_18_29 17_07_2006_bin.cue*). These both files are necessary to open the CD/DVD image in the external application that supports the CUE format (such as Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO and many others).

### c. Save As Raw Data

When you select a record that contains the data originally written as an additional session to a multi-session CD/DVD disk, the *Save As Raw Data* item is available in the context menu. It allows you to save the data to the local computer as is (without fixing references to the data in previous sessions).

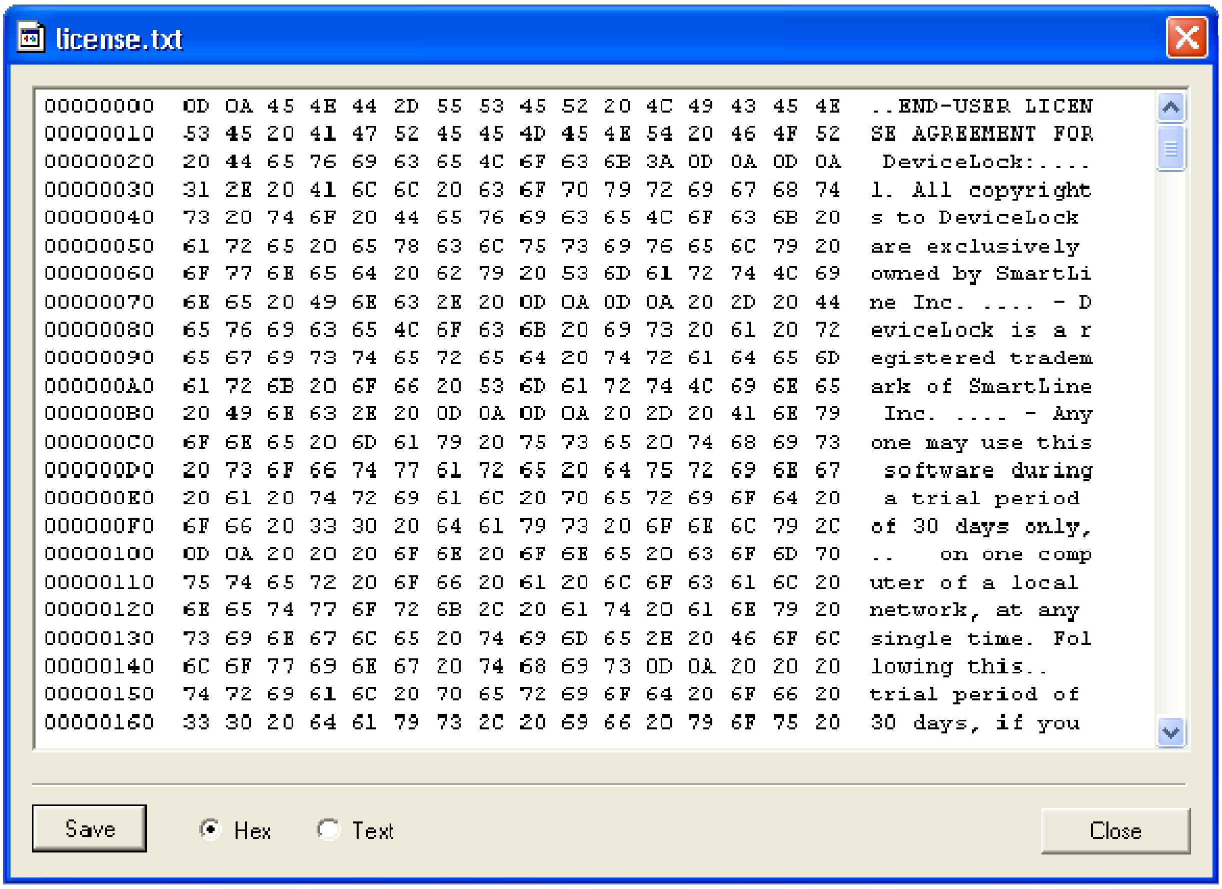
If you are using the regular saving function (the *Save* menu item or the toolbar's button), DeviceLock Management Console detects that the CD/DVD image contains a session that refers to the data in other (previous) sessions. Since the previous sessions are not available (they could be written on the computer where DeviceLock Service is not installed), DeviceLock Management Console locates and fixes all references to these non-existent sessions to make the *.cue* file readable by applications that support this format.

However, if you need to get the data that wasn't modified by DeviceLock Management Console, use *Save As Raw Data*. In this case the resultant *.cue* file may be unreadable by applications that support the CUE format.

When saving large files, you can press the *Cancel* button on the progress bar to abort the saving process. In this case the resultant file on the local computer will contain only that part of the data which was received before you aborted the saving process.

d. View

To open the data in the built-in viewer, use *View* from the context menu.



license.txt

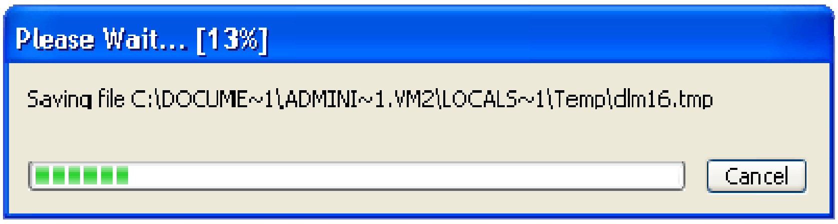
```
00000000  0D 0A 45 4E 44 2D 55 53 45 52 20 4C 49 43 45 4E  ..END-USER LICEN
00000010  53 45 20 41 47 52 45 45 4D 45 4E 54 20 46 4F 52  SE AGREEMENT FOR
00000020  20 44 65 76 69 63 65 4C 6F 63 6B 3A 0D 0A 0D 0A   DeviceLock:....
00000030  31 2E 20 41 6C 6C 20 63 6F 70 79 72 69 67 68 74  1. All copyright
00000040  73 20 74 6F 20 44 65 76 69 63 65 4C 6F 63 6B 20  s to DeviceLock
00000050  61 72 65 20 65 78 63 6C 75 73 69 76 65 6C 79 20  are exclusively
00000060  6F 77 6E 65 64 20 62 79 20 53 6D 61 72 74 4C 69  owned by SmartLi
00000070  6E 65 20 49 6E 63 2E 20 0D 0A 0D 0A 20 2D 20 44  ne Inc. .... - D
00000080  65 76 69 63 65 4C 6F 63 6B 20 69 73 20 61 20 72  eviceLock is a r
00000090  65 67 69 73 74 65 72 65 64 20 74 72 61 64 65 6D  egistered tradem
000000A0  61 72 6B 20 6F 66 20 53 6D 61 72 74 4C 69 6E 65  ark of SmartLine
000000B0  20 49 6E 63 2E 20 0D 0A 0D 0A 20 2D 20 41 6E 79   Inc. .... - Any
000000C0  6F 6E 65 20 6D 61 79 20 75 73 65 20 74 68 69 73  one may use this
000000D0  20 73 6F 66 74 77 61 72 65 20 64 75 72 69 6E 67   software during
000000E0  20 61 20 74 72 69 61 6C 20 70 65 72 69 6F 64 20   a trial period
000000F0  6F 66 20 33 30 20 64 61 79 73 20 6F 6E 6C 79 2C  of 30 days only,
00000100  0D 0A 20 20 20 6F 6E 20 6F 6E 65 20 63 6F 6D 70  ..   on one comp
00000110  75 74 65 72 20 6F 66 20 61 20 6C 6F 63 61 6C 20  uter of a local
00000120  6E 65 74 77 6F 72 6B 2C 20 61 74 20 61 6E 79 20  network, at any
00000130  73 69 6E 67 6C 65 20 74 69 6D 65 2E 20 46 6F 6C  single time. Fol
00000140  6C 6F 77 69 6E 67 20 74 68 69 73 0D 0A 20 20 20  lowing this..
00000150  74 72 69 61 6C 20 70 65 72 69 6F 64 20 6F 66 20  trial period of
00000160  33 30 20 64 61 79 73 2C 20 69 66 20 79 6F 75 20  30 days, if you
```

This simple viewer supports two modes:

1. **Hexadecimal/Textual** – select the *Hex* option to display information in the mixed mode as shown on the screenshot above.

2. **Textual** – select the *Text* option to display information in a pure textual mode.

When you are opening the large file, you can press the *Cancel* button on the progress bar to abort the opening process.



Please Wait... [13%]

Saving file C:\DOCUME~1\ADMINI~1.VM2\LOCALS~1\Temp\dlm16.tmp

In this case the viewer will show only that part of the data which was received before you aborted the opening process.

Press the *Save* button to save the data from the viewer to an external file.

e. External Viewer

Also, you can define the external program that will be used to view the shadow data. If such an external application is defined, *External Viewer* is enabled in the context menu. To define it, open Regedit and set the following entry on the computer where DeviceLock Management Console is running:

- Key: *HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager*
- Name: *ExternalShadowViewer*
- Type: *REG_SZ*
- Value: *<full_path_to_viewer> %1*

where *<full_path_to_viewer>* must be replaced by the full path to the external application. If this path contains spaces, use quotation marks. For example: *"C:\Program Files\Microsoft Office\OFFICE11\winword.exe" %1*.

When you are opening a large file, you can press the *Cancel* button on the progress bar to abort the opening process. In this case the external application will receive only that part of the data which was received before you aborted the opening process.

f. Delete

To delete a record, select *Delete* from the context menu or press the appropriate button on the toolbar. Using *Ctrl* and/or *Shift* you can highlight and remove several records simultaneously.

g. Refresh

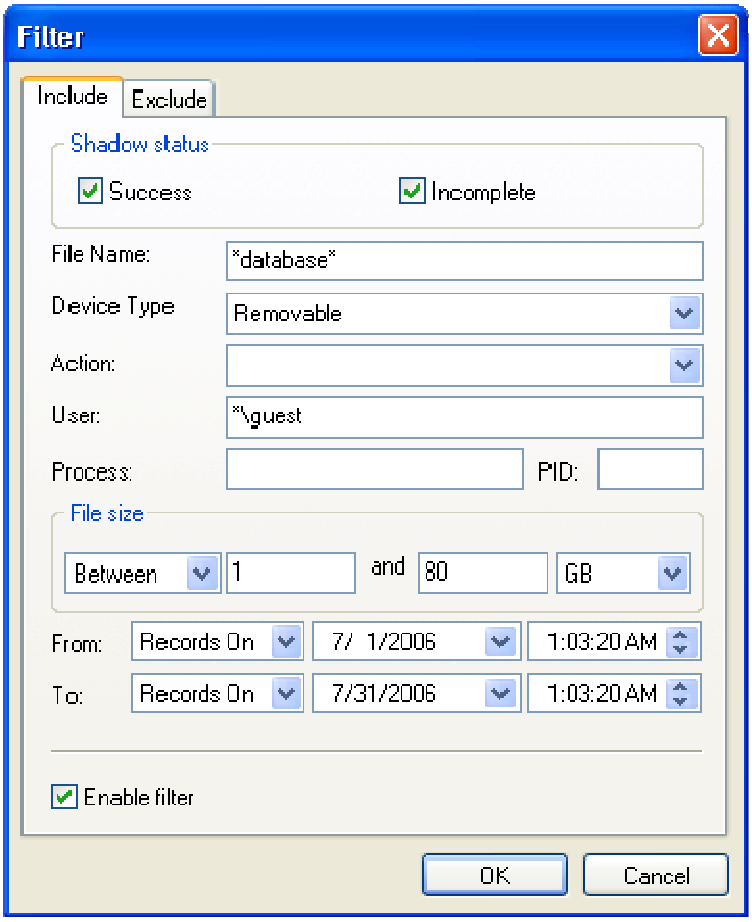
To refresh the list, select *Refresh* from the context menu available via a right mouse click or press the appropriate button on the toolbar.

h. Send Data to Server

When DeviceLock Enterprise Server is defined in Service Options and you need to force moving the shadow data from the current computer to the server, use *Send Data to Server* from the context menu available by a right mouse click or press the appropriate button on the toolbar.

### 5.4.4.1 Shadow Log Filter (Service)

You can filter data in Shadow Log Viewer such that only records that meet certain conditions are displayed in the list.



Shadow status

☑ Success ☑ Incomplete

File Name: *database*

Device Type: Removable

Action:

User: *\guest

Process: PID:

File size

Between 1 and 80 GB

From: Records On 7/ 1/2006 1:03:20 AM

To: Records On 7/31/2006 1:03:20 AM

☑ Enable filter

To open the *Filter* dialog, use *Filter* from the context menu of Shadow Log Viewer or press the appropriate button on the toolbar.

There is no big difference between defining Audit Log Filter and Shadow Log Filter, so first read the **Audit Log Filter (Service)** section of this manual.

When the filter is active you can define its condition by entering values into the following fields:

- *Success* – specifies whether to filter the successfully logged data.

- *Incomplete* – specifies whether to filter the data that was logged incompletely.

- *File Name* – the text that matches a value in the Shadow Log Viewer's *File Name* column. This field is not case-sensitive and you may use wildcards.

- *Device Type* – the selection that matches a value in the Audit Log Viewer's *Device Type* column.

- *Action* – the selection that matches a value in the Audit Log Viewer's *Action* column.

- *User* – the text that matches a value in the Shadow Log Viewer's *User* column. This field is not case-sensitive and you may use wildcards.

- *Process* – the text that matches a value in the Shadow Log Viewer's *Process* column. This field is not case-sensitive and you may use wildcards.

- *PID* – the number that matches a value in the Shadow Log Viewer's *PID* column.

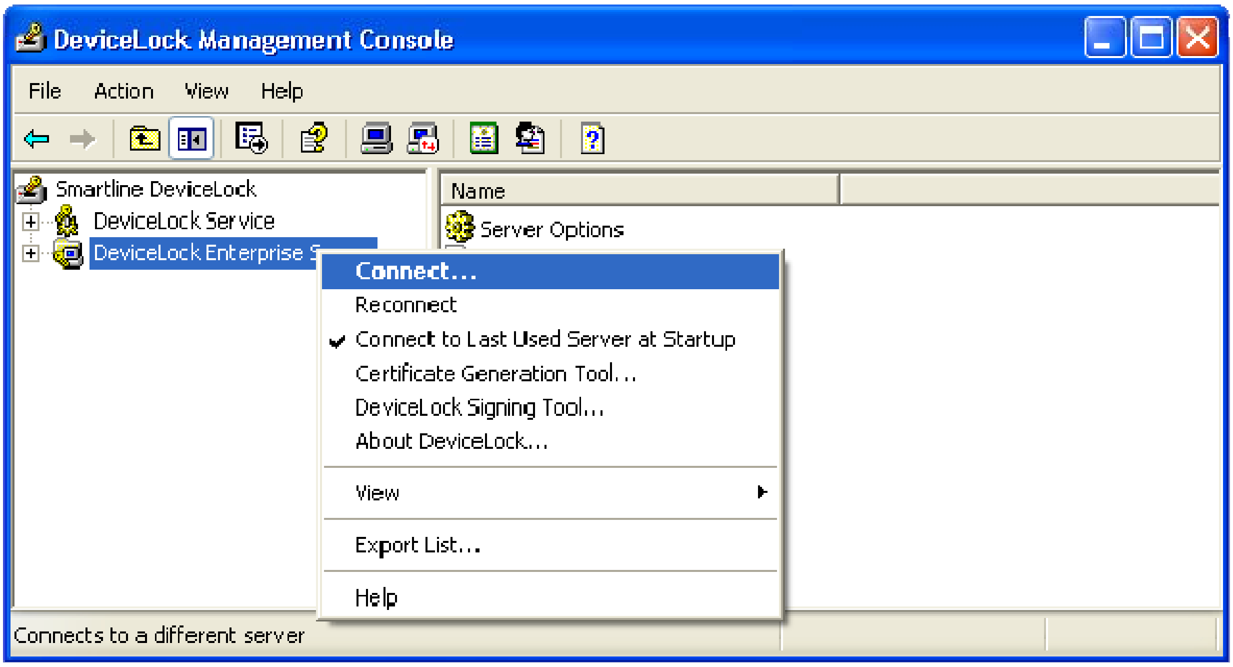
- *File size* – the number or the region of numbers that matches a value in the Shadow Log Viewer's *File Size* column.

- *From* – specifies the beginning of the interval of records that you want to filter. Select *First Record* to see records starting with the first record written to the log. Select *Records On* to see records that were written starting with a specific time and date.

- *To* – specifies the end of the range of records that you want to filter. Select *Last Record* to see records ending with the last record written to the log. Select *Records On* to see records that were written ending with a specific time and date.

## 5.5 Managing DeviceLock Enterprise Server

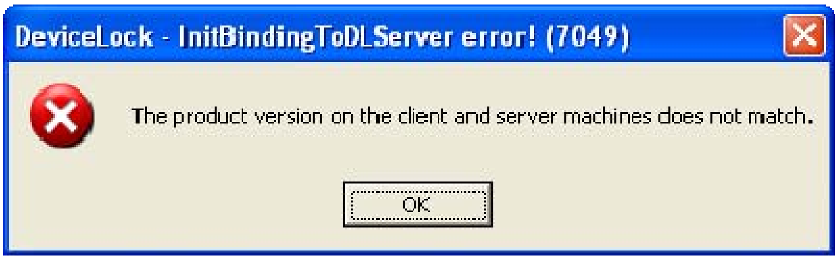
Expand the *DeviceLock Enterprise Server* item to get access to all of a server's functions and configuration parameters.



There is a context menu available by a right mouse click on the *DeviceLock Enterprise Server* item:

- *Connect* – connects to any computer that you specify. For more information please read the **Connecting to Computers** section of this manual.

  When you connect to a computer where an old version of DeviceLock Enterprise Sever is installed, you may receive the following message.


DeviceLock - InitBindingToDLServer error! (7049)

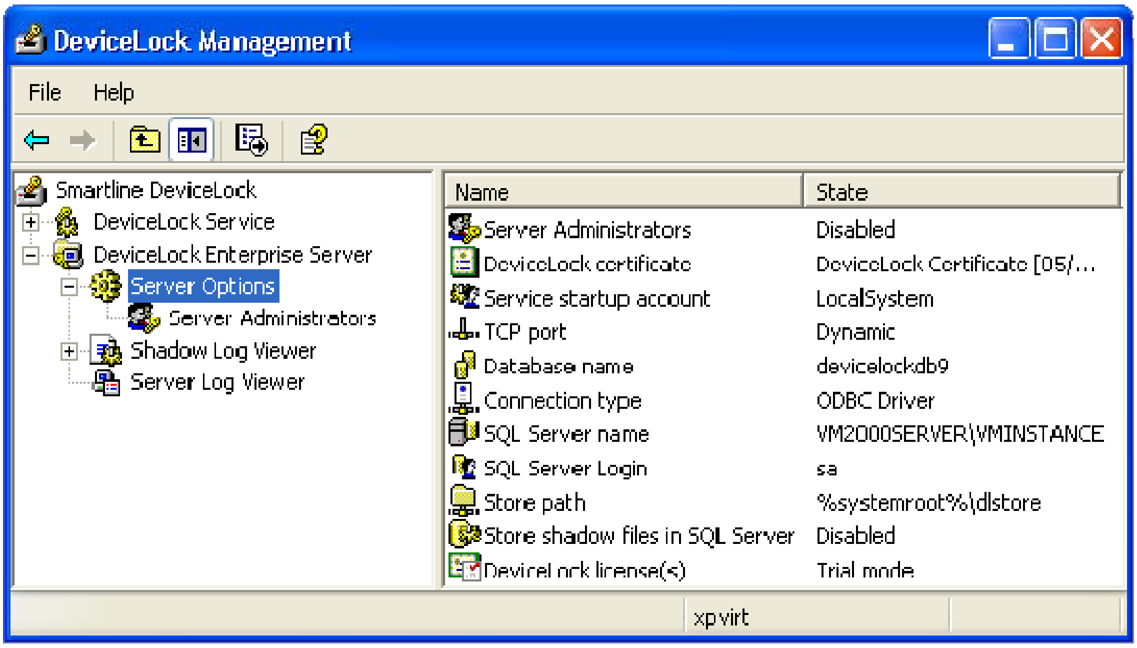
The product version on the client and server machines does not match.

In this case you need to install the new version DeviceLock Enterprise Server on this computer. For information on how to install DeviceLock Enterprise Server, please read the **Installing DeviceLock Enterprise Server** section of this manual.

- *Reconnect* – connects to the currently connected computer once again.
- *Connect to Last Used Server at Startup* – check this flag to instruct DeviceLock Management Console to automatically connect to the last used server each time console starts up.
- *Certificate Generation Tool* – runs the special tool that allows you to generate DeviceLock Certificates. For more information please read the **Generating DeviceLock Certificates** section of this manual.
- *DeviceLock Signing Tool* – runs the special tool that allows you to grant users temporary access to requested devices and sign XML files with DeviceLock Service settings. For more information please read the **DeviceLock Signing Tool** section of this manual.
- *About DeviceLock* – displays the dialog with information about the DeviceLock version and your licenses.

### 5.5.1 Server Options

These parameters allow you to tune up the DeviceLock Enterprise Server configuration.



| Name | State |
|---|---|
| Server Administrators | Disabled |
| DeviceLock certificate | DeviceLock Certificate [05/... |
| Service startup account | LocalSystem |
| TCP port | Dynamic |
| Database name | devicelockdb9 |
| Connection type | ODBC Driver |
| SQL Server name | VM2000SERVER\VMINSTANCE |
| SQL Server Login | sa |
| Store path | %systemroot%\dlstore |
| Store shadow files in SQL Server | Disabled |
| DeviceLock license(s) | Trial mode |

Use the context menu available by a right mouse click or double-click on the *Stream compression* parameter to enable or disable it. By enabling the *Stream compression* parameter you instruct DeviceLock to compress audit logs and shadow data sending from DeviceLock Services to DeviceLock Enterprise Server. Doing this decreases the size of data transfers and thus reduces the network load.

Use the context menu on other parameters to open dialogs that enable making changes. Alternatively, you can double-click on the parameter to open its dialog.

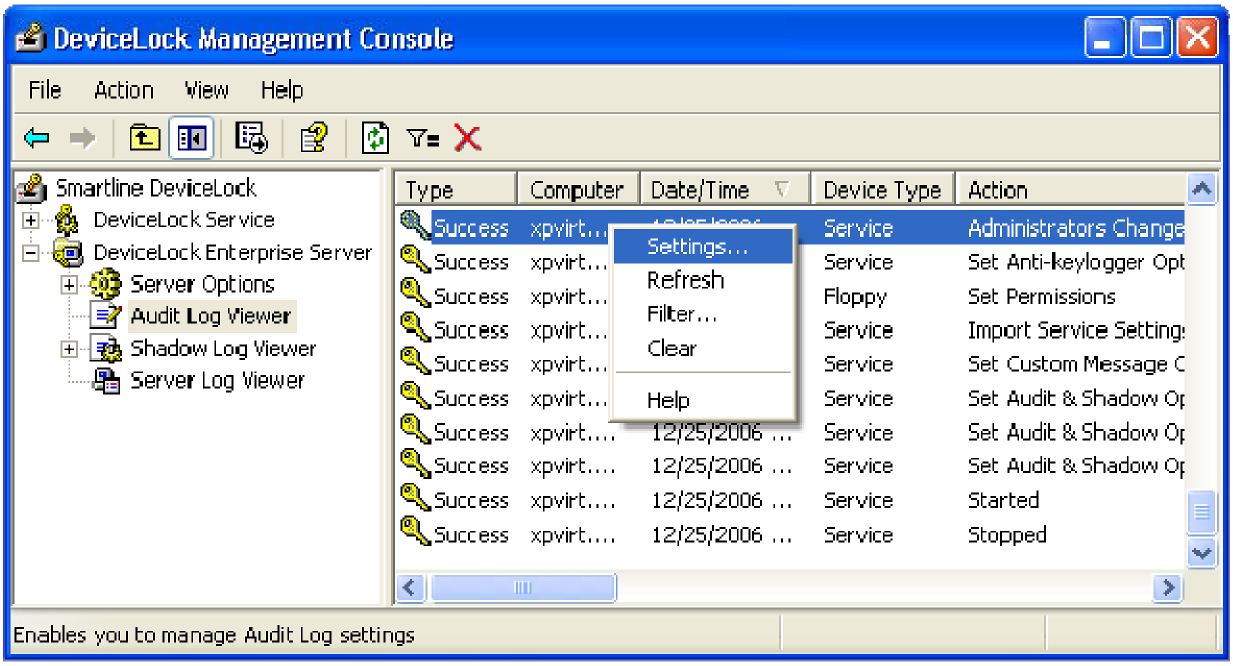
All these parameters are described in detail in the **Installing DeviceLock Enterprise Server** section of this manual.

To run the configuration wizard and review or set all these parameters step by step, use the *Properties* item from the context menu of Server Options. The configuration wizard is also described in the **Installing DeviceLock Enterprise Server** section of this manual.

## 5.5.2 Audit Log Viewer (Server)

The audit log viewer allows you to retrieve the audit log stored on DeviceLock Enterprise Server.

DeviceLock Enterprise Server stores audit records received from a remote computer, only if *DeviceLock Log* or *Event & DeviceLock Logs* is selected in the *Audit log type* parameter in Service Options on that computer. Otherwise, audit records are stored in the local Windows event logging subsystem of the remote computer and can be viewed using the service's audit log viewer.



| Type | Computer | Date/Time | Device Type | Action |
|---|---|---|---|---|
| Success | xpvirt... | | Service | Administrators Change |
| Success | xpvirt... | | Service | Set Anti-keylogger Opt |
| Success | xpvirt... | | Floppy | Set Permissions |
| Success | xpvirt... | | Service | Import Service Setting: |
| Success | xpvirt... | | Service | Set Custom Message C |
| Success | xpvirt... | | Service | Set Audit & Shadow Op |
| Success | xpvirt.... | 12/25/2006 ... | Service | Set Audit & Shadow Op |
| Success | xpvirt.... | 12/25/2006 ... | Service | Set Audit & Shadow Op |
| Success | xpvirt.... | 12/25/2006 ... | Service | Started |
| Success | xpvirt.... | 12/25/2006 ... | Service | Stopped |

Enables you to manage Audit Log settings

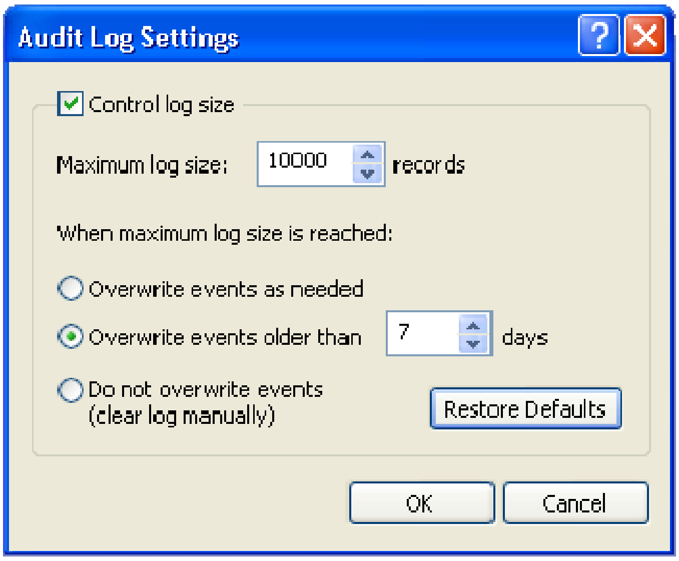
There is not much difference between the service's audit log viewer and the server's audit log viewer, so first read the **Audit Log Viewer (Service)** section of this manual.

In comparison with the service's audit log viewer, the server's viewer has only two additional columns:

- *Computer* – the name of the computer from which audit logs were received.
- *Event* – a number identifying the particular event type.

### 5.5.2.1 Audit Log Settings (Server)

To define a maximum log size and what DeviceLock Enterprise Server should do if the audit log becomes full, use *Settings* from the context menu of Audit Log Viewer.



☑ Control log size

Maximum log size: 10000 records

When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

***NOTE: These settings are stored in the database and they are specific to the log but not to DeviceLock Enterprise Server. This means that, if there are several DeviceLock Enterprise Servers using one database, all have the same log settings.***

Enable the *Control log size* flag to allow DeviceLock Enterprise Server to control the number of records in the log and delete outdated records (if necessary) to clean up the space for new ones. Otherwise, if the *Control log size* flag is disabled, DeviceLock Enterprise Server uses all available space for the SQL Server's database to store the log.

In the *Maximum log size* parameter you can specify the maximum number of records that this log can contain. Please note that, if there is more than one DeviceLock Enterprise Server using this database, then the actual number of records in the log can be a little larger (by a couple of records) than the specified value.

To specify what DeviceLock Enterprise Server should do when the log is full (when *Maximum log size* is reached) select one of these options:

- *Overwrite events as needed* – the server will overwrite old events if *Maximum log size* is reached.

- *Overwrite events older than* – specifies that records that are newer than this value will not be overwritten (specified in days).

- *Do not overwrite events (clear log manually)* – the server will not overwrite old events if *Maximum log size* is reached and you will need to clear events manually.

If you wish to reset current settings to the default values, use the *Restore Defaults* button. Default values are:

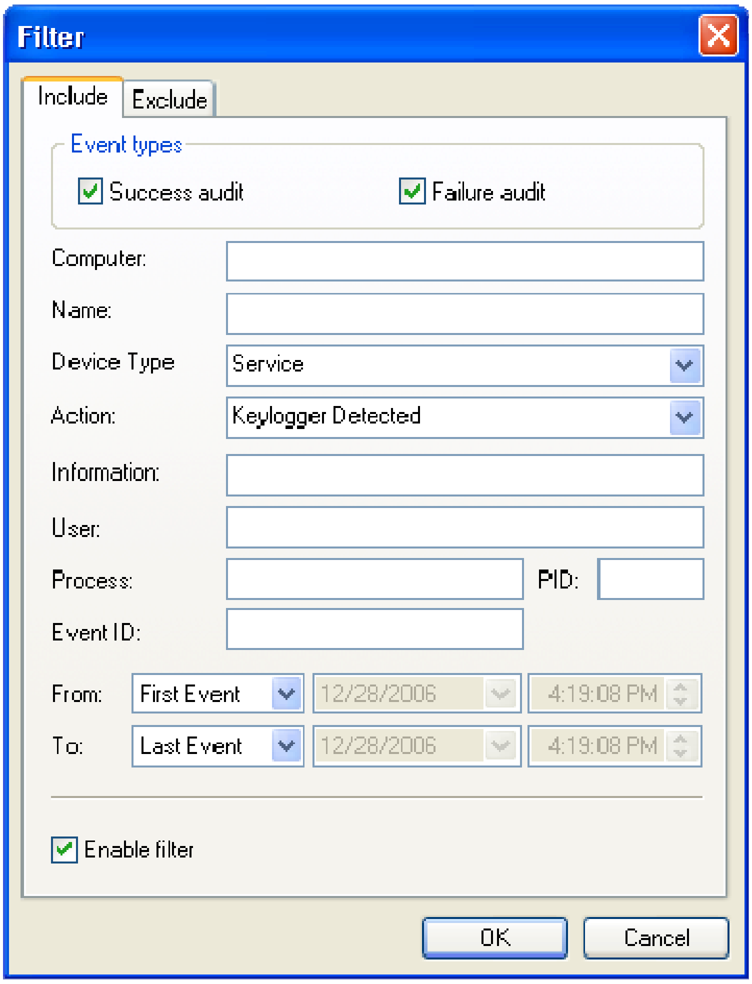
- The *Maximum log size* parameter is set to 10000 records.

- The *Overwrite events older than* option is selected and set to 7 days.

If there is no space for new records in the audit log and there is nothing to delete then DeviceLock Enterprise Server doesn't remove audit data from remote users' computers. This prevents you from loosing the audit data due to lack of space in the log. When some space becomes available in the log, DeviceLock Enterprise Server moves the remaining audit data from users' computers to this log.

### 5.5.2.2 Audit Log Filter (Server)

You can filter data in Audit Log Viewer so that only records that meet specified conditions are displayed in the list.



Event types

☑ Success audit ☑ Failure audit

Computer:

Name:

Device Type: Service

Action: Keylogger Detected

Information:

User:

Process: PID:

Event ID:

From: First Event 12/28/2006 4:19:08 PM

To: Last Event 12/28/2006 4:19:08 PM

☑ Enable filter

To open the *Filter* dialog, use *Filter* from the context menu of Audit Log Viewer or press the appropriate button on the toolbar.

There is not much difference between the service's audit log filter and the server's audit log filter, so first read the **Audit Log Filter (Service)** section of this manual.

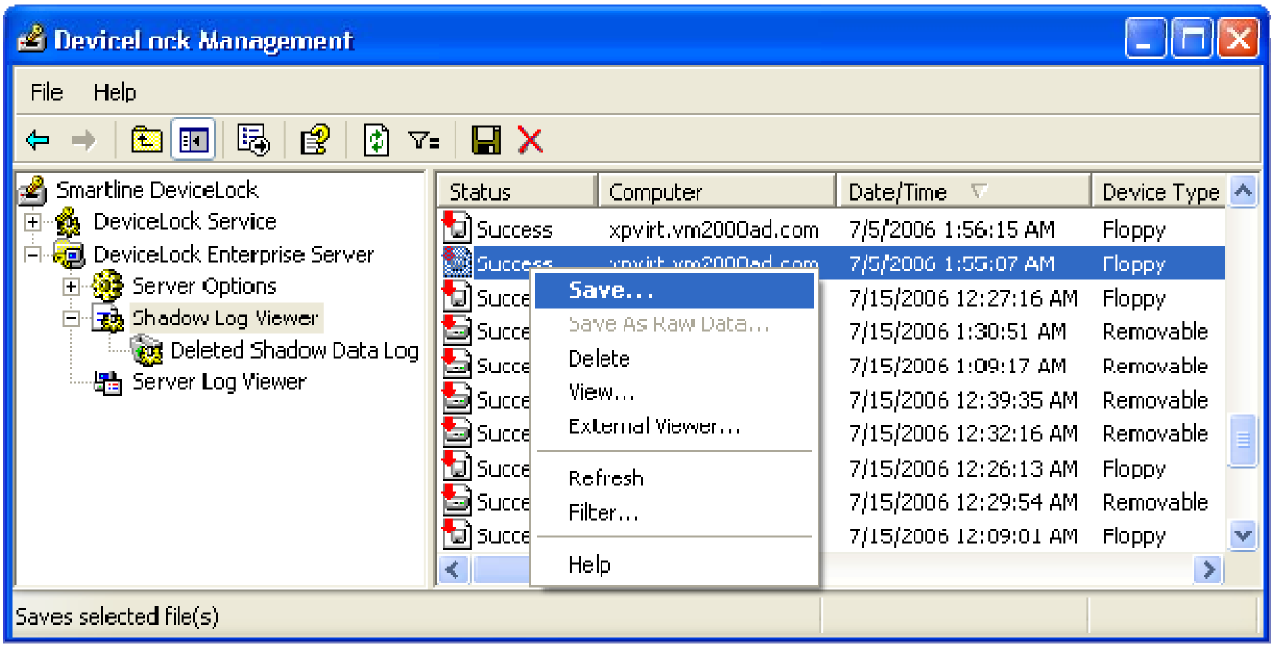
In comparison with the service's audit log filter, the server's filter has only two additional fields:

- *Computer* – this text matches a value in the Audit Log Viewer's *Computer* column. This field is not case-sensitive and you may use wildcards.

- *Event ID* – this number matches a value in the Audit Log Viewer's *Event* column.

### 5.5.3 Shadow Log Viewer (Server)

The shadow log viewer allows you to retrieve the shadow log stored on DeviceLock Enterprise Server.



| Status | Computer | Date/Time | Device Type |
|---|---|---|---|
| Success | xpvirt.vm2000ad.com | 7/5/2006 1:56:15 AM | Floppy |
| Success | xpvirt.vm2000ad.com | 7/5/2006 1:55:07 AM | Floppy |
| Succe | | 7/15/2006 12:27:16 AM | Floppy |
| Succe | | 7/15/2006 1:30:51 AM | Removable |
| Succe | | 7/15/2006 1:09:17 AM | Removable |
| Succe | | 7/15/2006 12:39:35 AM | Removable |
| Succe | | 7/15/2006 12:32:16 AM | Removable |
| Succe | | 7/15/2006 12:26:13 AM | Floppy |
| Succe | | 7/15/2006 12:29:54 AM | Removable |
| Succe | | 7/15/2006 12:09:01 AM | Floppy |

There is not much difference between the service's shadow log viewer and the server's shadow log viewer, so first read the **Shadow Log Viewer (Service)** section of this manual.

In comparison with the service's shadow log viewer, the server's viewer has only one additional column:

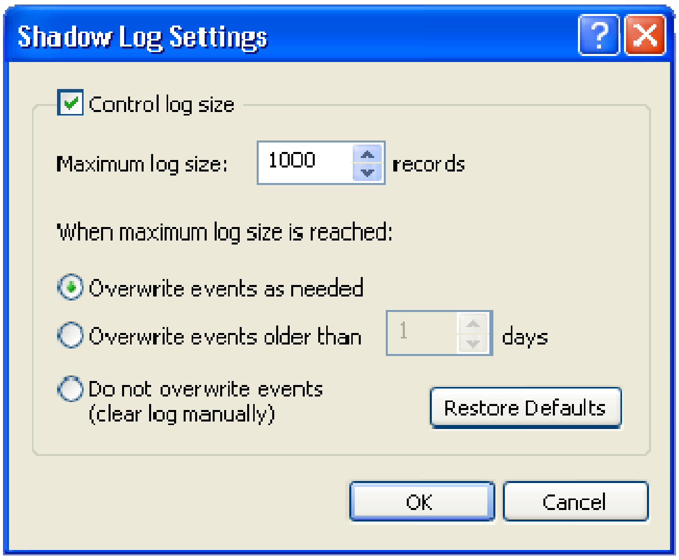
- *Computer* – the name of the computer from which shadow logs were received.

Also, unlike the service's shadow log viewer, when you delete a record in the server's viewer, the record's binary data is removed from the database or from the disk (it depends on the *Store shadow files in SQL Server* flag) but all other information (such as the file name and size, user name, date/time, process and so on) is moved to the special log called Deleted Shadow Data Log.

This Deleted Shadow Data Log is used when you don't need the content of the shadow data anymore and you want to clean up storage (either SQL Server or the disk), but you need to keep information about the data transfer.

### 5.5.3.1 Shadow Log Settings

To define a maximum log size and what DeviceLock Enterprise Server should do if the shadow log becomes full, use *Settings* from the context menu of Shadow Log Viewer.



Shadow Log Settings

☑ Control log size

Maximum log size: 1000 records

When maximum log size is reached:

● Overwrite events as needed

○ Overwrite events older than 1 days

○ Do not overwrite events (clear log manually)

For information on these settings, please read the **Audit Log Settings (Server)** section of this manual.

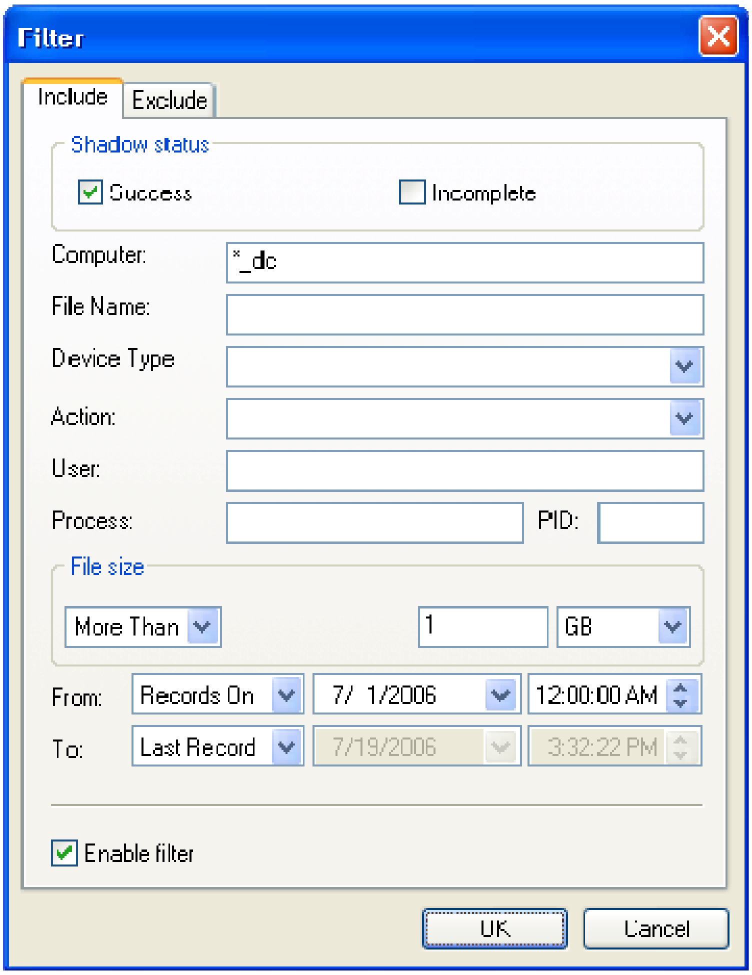
When DeviceLock Enterprise Server needs to remove some old records from the shadow log because of defined parameters (*Overwrite events as needed* and *Overwrite events older than*), these records are moved to the Deleted Shadow Data Log.

If there is no space for new records in the shadow log and there is nothing to delete then DeviceLock Enterprise Server doesn't remove shadowed data from remote users' computers. This prevents the loss of shadowed data due to lack of space in the log. When some space becomes available in the log, DeviceLock Enterprise Server moves the remaining shadowed data from users' computers to this log.

It's best to avoid accumulating shadowed data on users' computers. We recommend that you monitor the DeviceLock Enterprise Server's log on a periodic basis, watch for warning messages and adjusting log settings appropriately.

### 5.5.3.2 Shadow Log Filter (Server)

You can filter data in Shadow Log Viewer so that only records that meet specified conditions are displayed in the list.



Shadow status

☑ Success ☐ Incomplete

Computer: *_dc

File Name:

Device Type:

Action:

User:

Process: PID:

File size

More Than 1 GB

From: Records On 7/ 1/2006 12:00:00 AM

To: Last Record 7/19/2006 3:32:22 PM

☑ Enable filter

To open the *Filter* dialog, use *Filter* from the context menu of Shadow Log Viewer or press the appropriate button on the toolbar.

There is not much difference between the service's shadow log filter and the server's shadow log filter, so first read the **Shadow Log Filter (Service)** section of this manual.

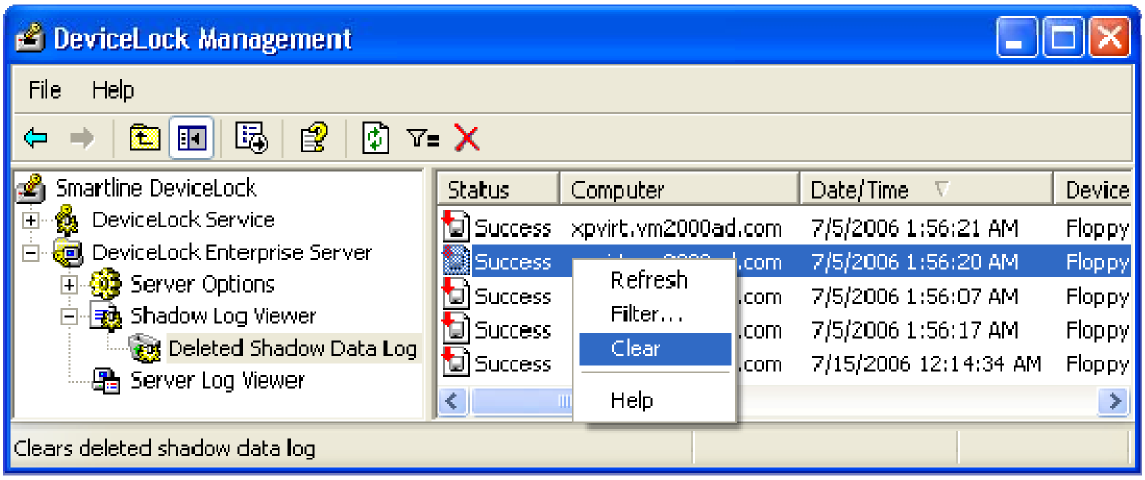
In comparison with the service's shadow log filter, the server's filter has only one additional field:

- *Computer* – the text that matches a value in the Shadow Log Viewer's *Computer* column. This field is not case-sensitive and you may use wildcards.

### 5.5.3.3 Deleted Shadow Data Log

This viewer allows you to retrieve information about deleted shadow log records.

When a record is removed from the log in Shadow Log Viewer, the record’s binary data is deleted but all other information (such as the file name and size, user name, date/time, process and so on) is moved to this log.



| Status | Computer | Date/Time | Device |
|---|---|---|---|
| Success | xpvirt.vm2000ad.com | 7/5/2006 1:56:21 AM | Floppy |
| Success | .com | 7/5/2006 1:56:20 AM | Floppy |
| Success | .com | 7/5/2006 1:56:07 AM | Floppy |
| Success | .com | 7/5/2006 1:56:17 AM | Floppy |
| Success | .com | 7/15/2006 12:14:34 AM | Floppy |

Clears deleted shadow data log

This log is used when you don’t need the content of the shadow data anymore and you want to clean up the storage (either SQL Server or the disk) but at the same time you need to keep the information about the data transfer.

To define a maximum log size and instruct DeviceLock Enterprise Server regarding what it should do if the deleted shadow data log becomes full, select *Settings* from the context menu available with a right mouse click. This log’s settings are similar to the audit log’s settings so read the **Audit Log Settings (Server)** section of this manual for more information.

If there is no space for new records in the deleted shadow data log and there is nothing to remove, then DeviceLock Enterprise Server just drops any new records. To avoid loosing records in this way, we recommend that you monitor DeviceLock Enterprise Server’s log on a periodic basis and watch for warning messages there.

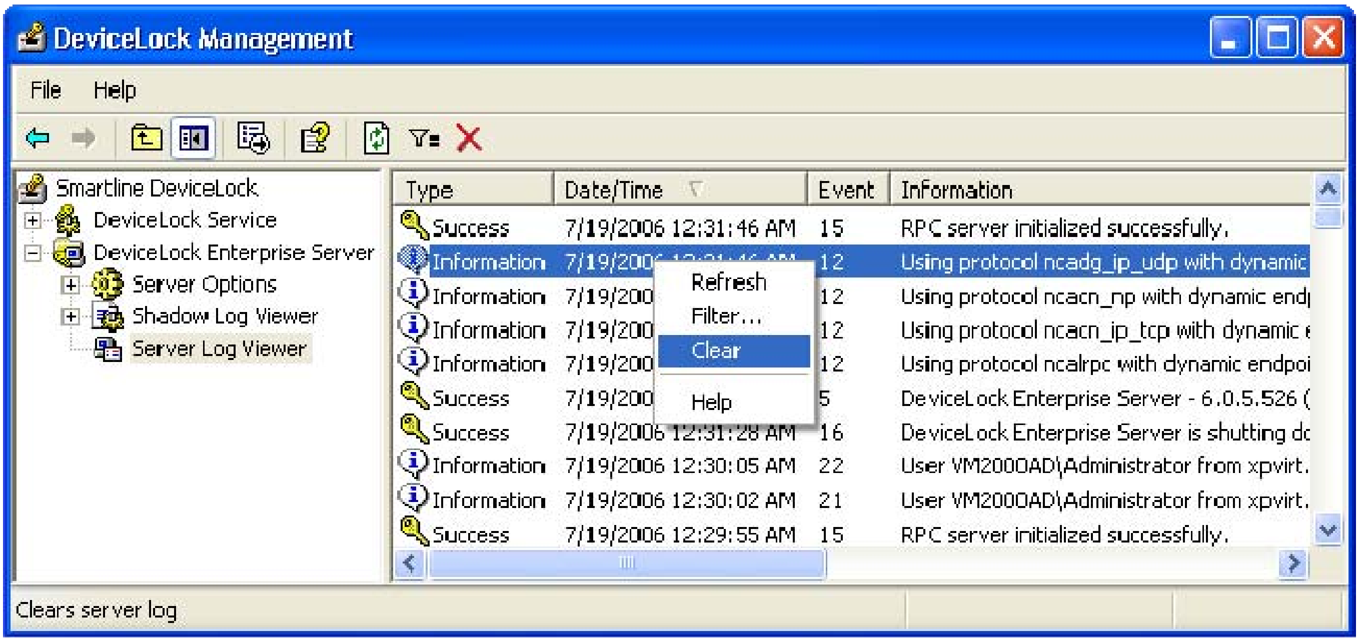
To refresh the list, select *Refresh* from the context menu available with a right mouse click or by pressing the appropriate button on the toolbar.

To filter records in this list, select *Filter* from the context menu available with a right mouse click or by pressing the appropriate button on the toolbar. The same filter is used by the Shadow Log Viewer, so read the **Shadow Log Filter (Server)** section of this manual for more information.

To clear all records from this log, select *Clear* from the context menu or press the appropriate button on the toolbar.

### 5.5.4 Server Log Viewer

This viewer allows you to retrieve the internal DeviceLock Enterprise Server's log. The server uses this log to write errors, warnings and other important information (such as configuration changes, start/stop events, version, etc.).



| Type | Date/Time | Event | Information |
|---|---|---|---|
| Success | 7/19/2006 12:31:46 AM | 15 | RPC server initialized successfully. |
| Information | 7/19/200 | 12 | Using protocol ncadg_ip_udp with dynamic |
| Information | 7/19/200 | 12 | Using protocol ncacn_np with dynamic end |
| Information | 7/19/200 | 12 | Using protocol ncacn_ip_tcp with dynamic e |
| Information | 7/19/200 | 12 | Using protocol ncalrpc with dynamic endpoi |
| Success | 7/19/200 | 5 | DeviceLock Enterprise Server - 6.0.5.526 ( |
| Success | 7/19/2006 12:31:28 AM | 16 | DeviceLock Enterprise Server is shutting dc |
| Information | 7/19/2006 12:30:05 AM | 22 | User VM2000AD\Administrator from xpvirt. |
| Information | 7/19/2006 12:30:02 AM | 21 | User VM2000AD\Administrator from xpvirt. |
| Success | 7/19/2006 12:29:55 AM | 15 | RPC server initialized successfully. |

You may use the information from this log to diagnose problems (if any), to monitor changes in the server's configuration and to see who has cleared logs and when.

The columns of this viewer are defined as follows:

- *Type* – the class of an event: *Success*, *Information*, *Warning* or *Error*.
- *Date/Time* – the date and the time when an event has occurred.
- *Event* – a number identifying the particular event type.
- *Information* – event-specific information, such as error/warning descriptions, names and values of changed parameters, and so on.
- *Server* – the name of the server where an event occurred.
- *Record N* – the record number.

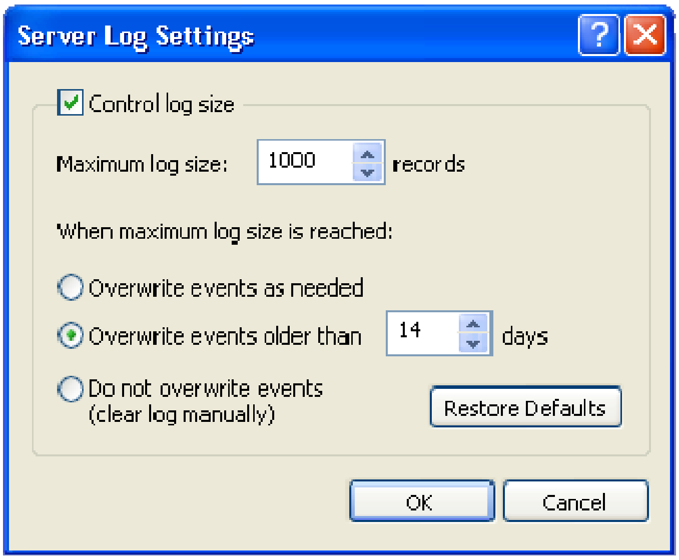
To refresh the list, select *Refresh* from the context menu available by clicking the right mouse button or by pressing the appropriate button on the toolbar.

To clear all records from this log, select *Clear* from the context menu or press the appropriate button on the toolbar.

After the server's log is cleared, the one event about this clearing action is written into the log (e.g. "*The Server Log (100 record(s)) was cleared by VM2000AD\Administrator from xpvirt.vm2000ad.com*").

### 5.5.4.1 Server Log Settings

To define a maximum log size and what DeviceLock Enterprise Server should do if the server's log becomes full, use *Settings* from the context menu of Server Log Viewer.



Server Log Settings

☑ Control log size

Maximum log size: 1000 records

When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 14 days

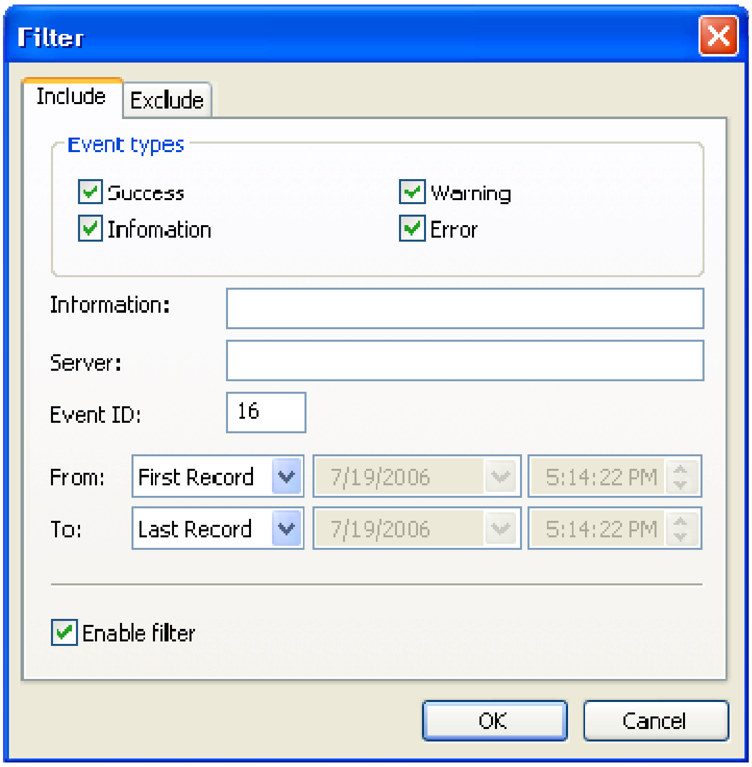
○ Do not overwrite events (clear log manually)

For information on these settings, please read the **Audit Log Settings (Server)** section of this manual.

If there is no space for new records in the server's log and there is nothing to remove, then DeviceLock Enterprise Server just drops any new records.

### 5.5.4.2 Server Log Filter

You can filter data in the Server Log Viewer such that only records that meet specified conditions are displayed in the list.



Filter

Include | Exclude

Event types

☑ Success ☑ Warning

☑ Infomation ☑ Error

Information:

Server:

Event ID: 16

From: First Record 7/19/2006 5:14:22 PM

To: Last Record 7/19/2006 5:14:22 PM

☑ Enable filter

To open the *Filter* dialog, use *Filter* from the context menu of the Server Log Viewer or press the appropriate button on the toolbar.

There are no big differences between defining an Audit Log Filter and a Server Log Filter, so for more information read the **Audit Log Filter (Service)** section of this manual.

When the filter is active you can define its condition by entering values into the following fields:

- *Success* – specifies whether to filter events of the *Success* class.

- *Information* – specifies whether to filter events of the *Information* class.

- *Warning* – specifies whether to filter events of the *Warning* class.

- *Error* – specifies whether to filter events of the *Error* class.

- *Information* – the text that matches a value in the Server Log Viewer's *Information* column. This field is not case-sensitive and you may use wildcards.

- *Server* – the text that matches a value in the Server Log Viewer's *Server* column. This field is not case-sensitive and you may use wildcards.

- *Event ID* – the number that matches a value in the Server Log Viewer's *Event* column.

- *From* – specifies the beginning of the interval of events that you want to filter. Select *First Event* to see events starting with the first event recorded in the log. Select *Events On* to see events that occurred starting with a specific time and date.

- *To* – specifies the end of the range of events that you want to filter. Select *Last Event* to see events ending with the last event recorded in the log. Select *Events On* to see events that occurred ending with a specific time and date.

# 6 DeviceLock Group Policy Manager

## 6.1 Overview

In addition to the standard way of managing permissions via DeviceLock Management Console, DeviceLock also provides you with a more powerful mechanism – settings can be changed and deployed via Group Policy in an Active Directory domain. System administrators can use policies to control DeviceLock's configurations from a single location on a network – no matter how large the network.

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.

Tighter integration into the Active Directory is a very important function of DeviceLock. It makes DeviceLock's 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 component 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, even those that are not currently running and new computers that are just connecting to the network.

  For more information regarding DeviceLock Service deployment, please read the **Installation via Group Policy** section of this manual.

- Control and configure DeviceLock Service on a large number of computers in different domains/organizational units simultaneously.

  Even if some computers are not currently running or they are new computers that are just connecting to the network, they are included in DeviceLock's  automatic deployment of predefined settings.

- View the policy currently being applied and predict what policy would be applied.

  For more information, please read the **Using Resultant Set of Policy (RSoP)** section of this manual.

***NOTE: In order 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.***

## 6.2 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 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.

## 6.3 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.

## 6.4 Starting DeviceLock Group Policy Manager

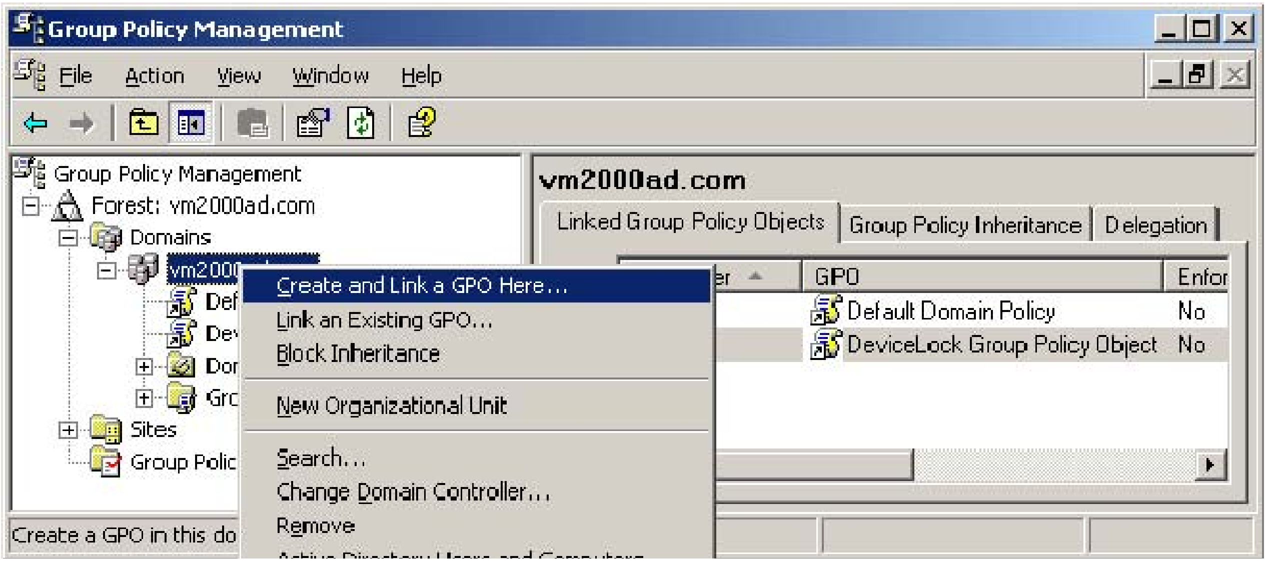
DeviceLock Group Policy Manager integrates into the Windows Group Policy Object (GPO) editor. To use DeviceLock Group Policy Manager on your local PC rather than on the domain controller, you need to have the GPO editor installed locally. We recommend that you install the Group Policy Management Console (GPMC). It can be downloaded from the Microsoft website: http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.

To open DeviceLock Group Policy Manager, you should run the GPO editor first:

1. Start the *Group Policy Management* snap-in.

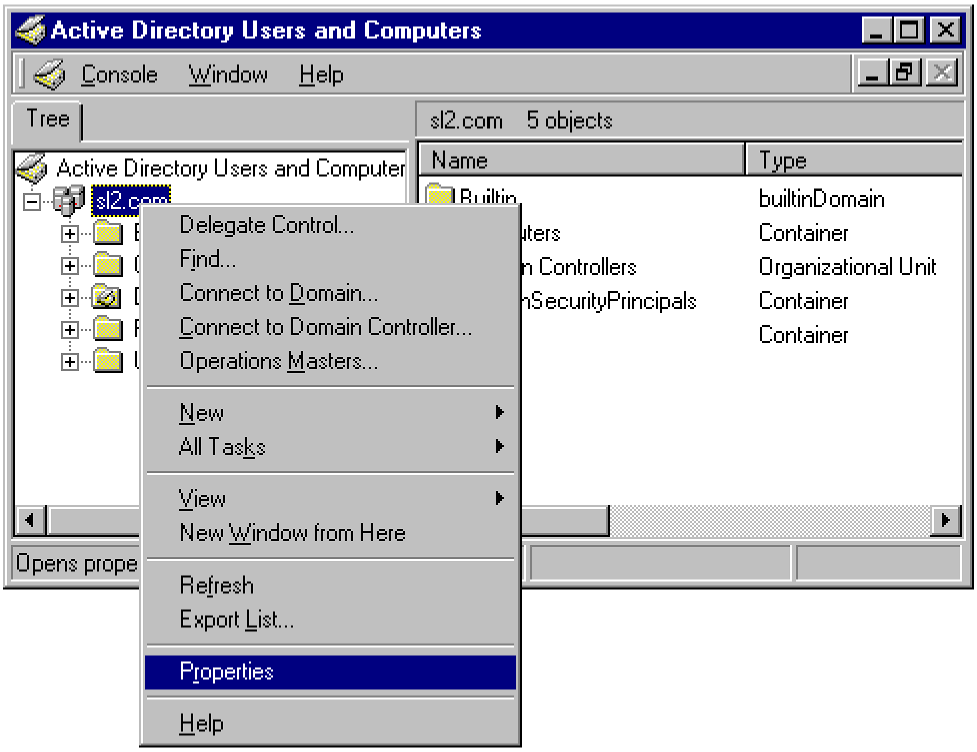
   If the *Group Policy Management* snap-in is not installed on your computer, you may use the *Active Directory Users and Computers* snap-in instead.

2. In the console tree, select your domain.

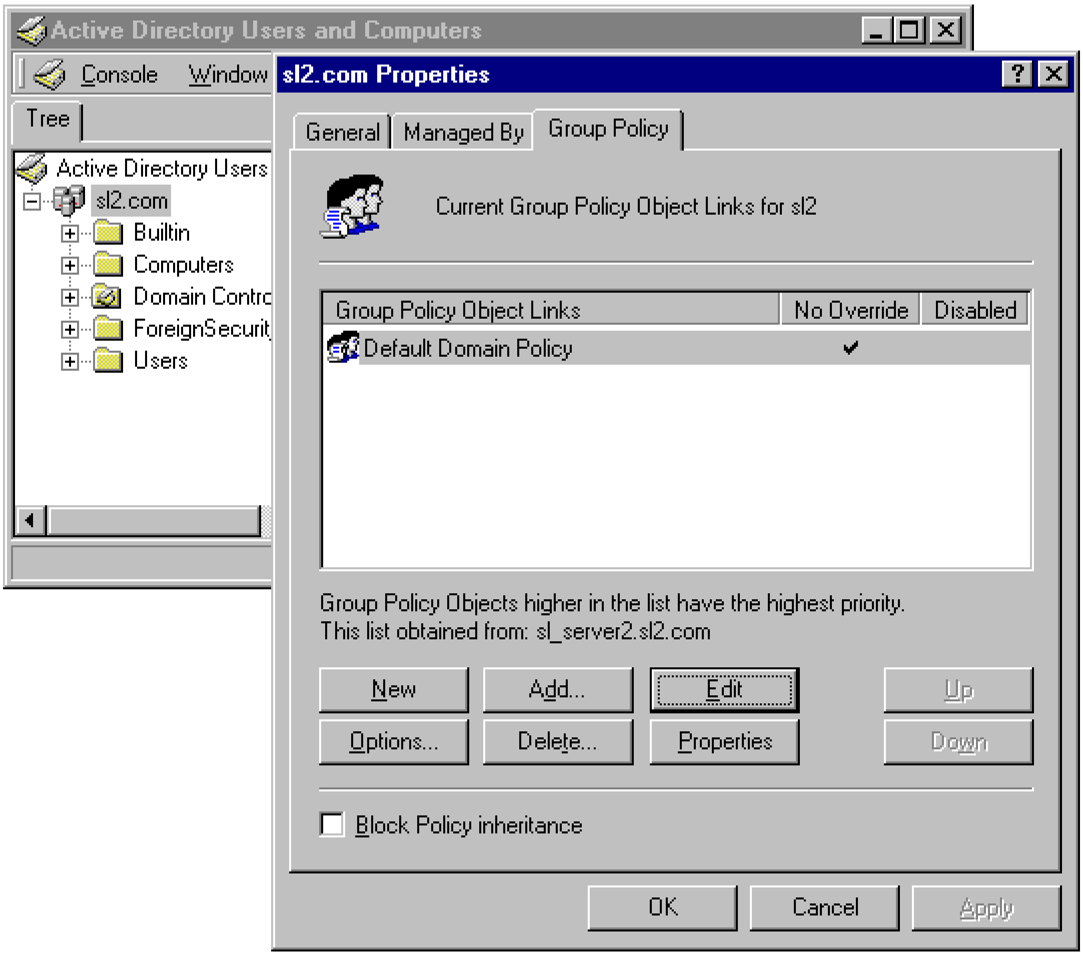


3. Select the group policy object that you need, and then click *Edit* in the context menu available by a right mouse click. If you wish to create a new group policy object, click *Create and Link a GPO Here* from the context menu of the domain item.

If you are using the *Active Directory Users and Computers* snap-in, right-click your domain, then click *Properties*.

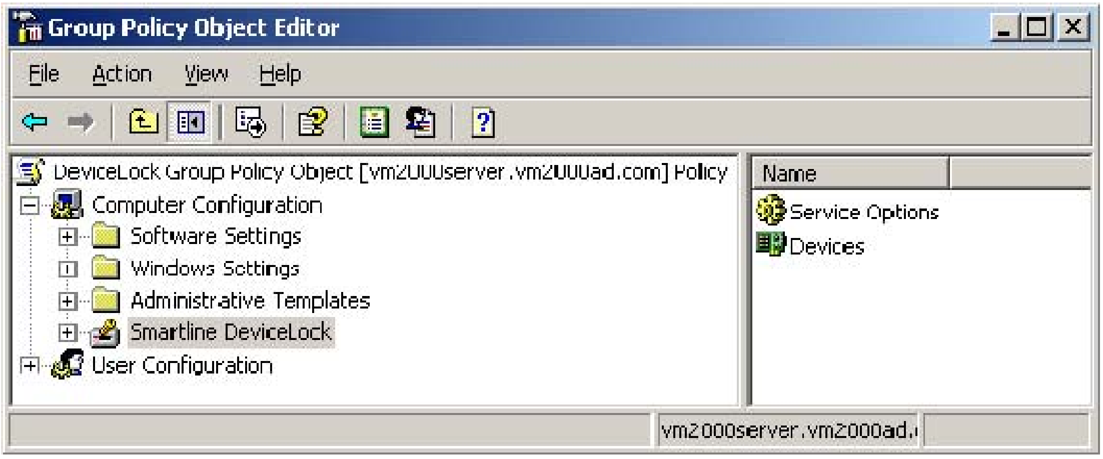


Click the *Group Policy* tab, select the group policy object that you need, and then click *Edit*. If you wish to create a new group policy object, click *Add*.



4. Wait until the GPO editor is started. It may take up to several seconds.

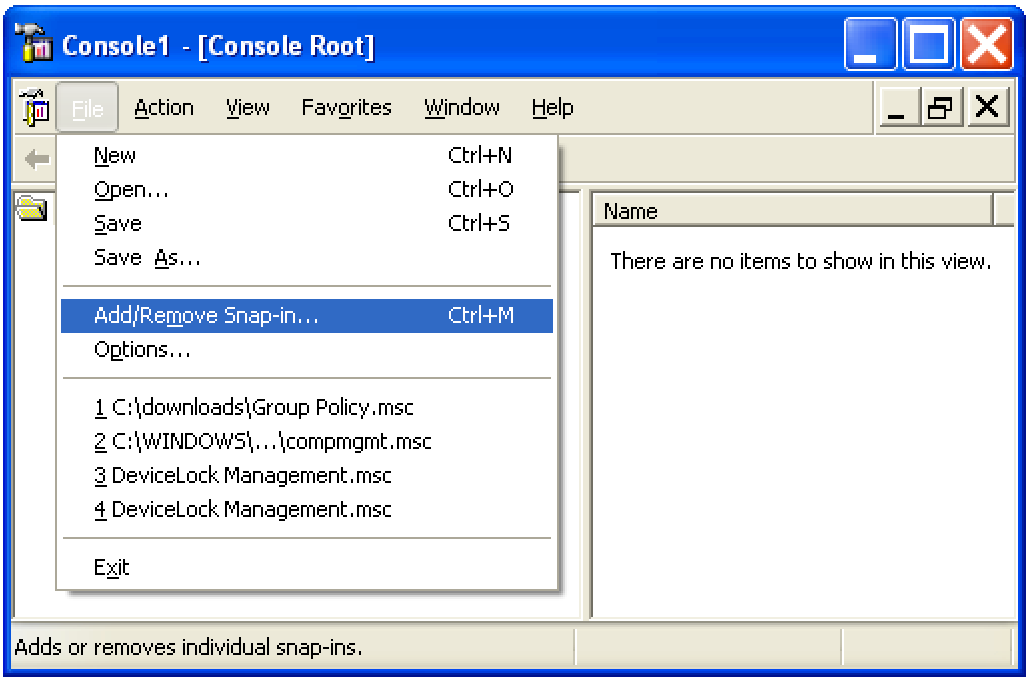
5. Under *Computer Configuration*, select *SmartLine DeviceLock*.



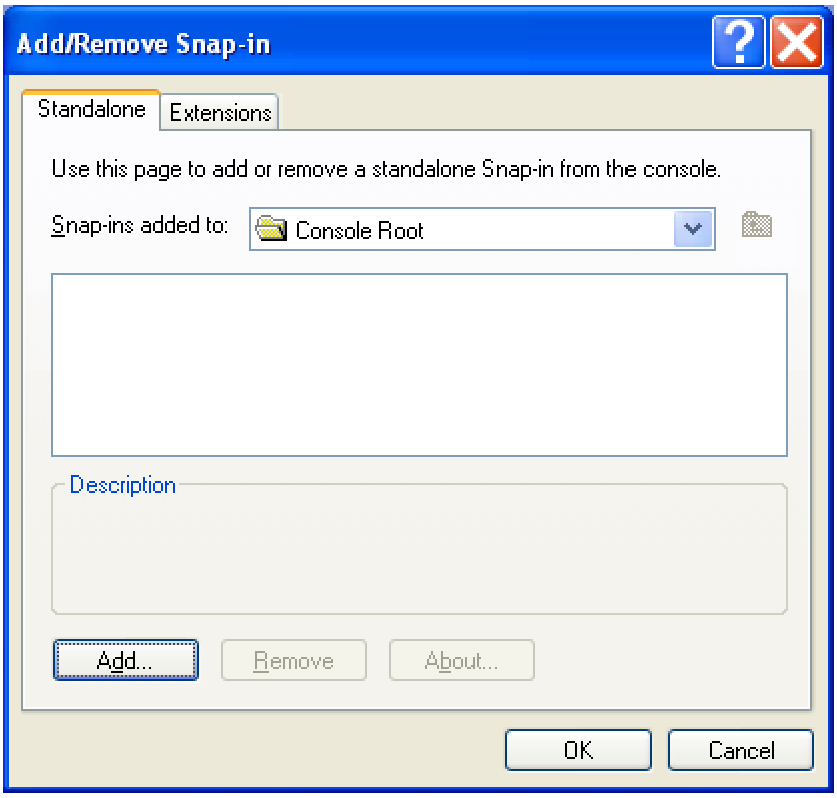
Alternatively, to run the GPO editor you can start MMC and add the *Group Policy* snap-in manually:

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*.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\downloads\Group Policy.msc
2 C:\WINDOWS\...\compmgmt.msc
3 DeviceLock Management.msc
4 DeviceLock Management.msc
Exit
Name
There are no items to show in this view.
Adds or removes individual snap-ins.

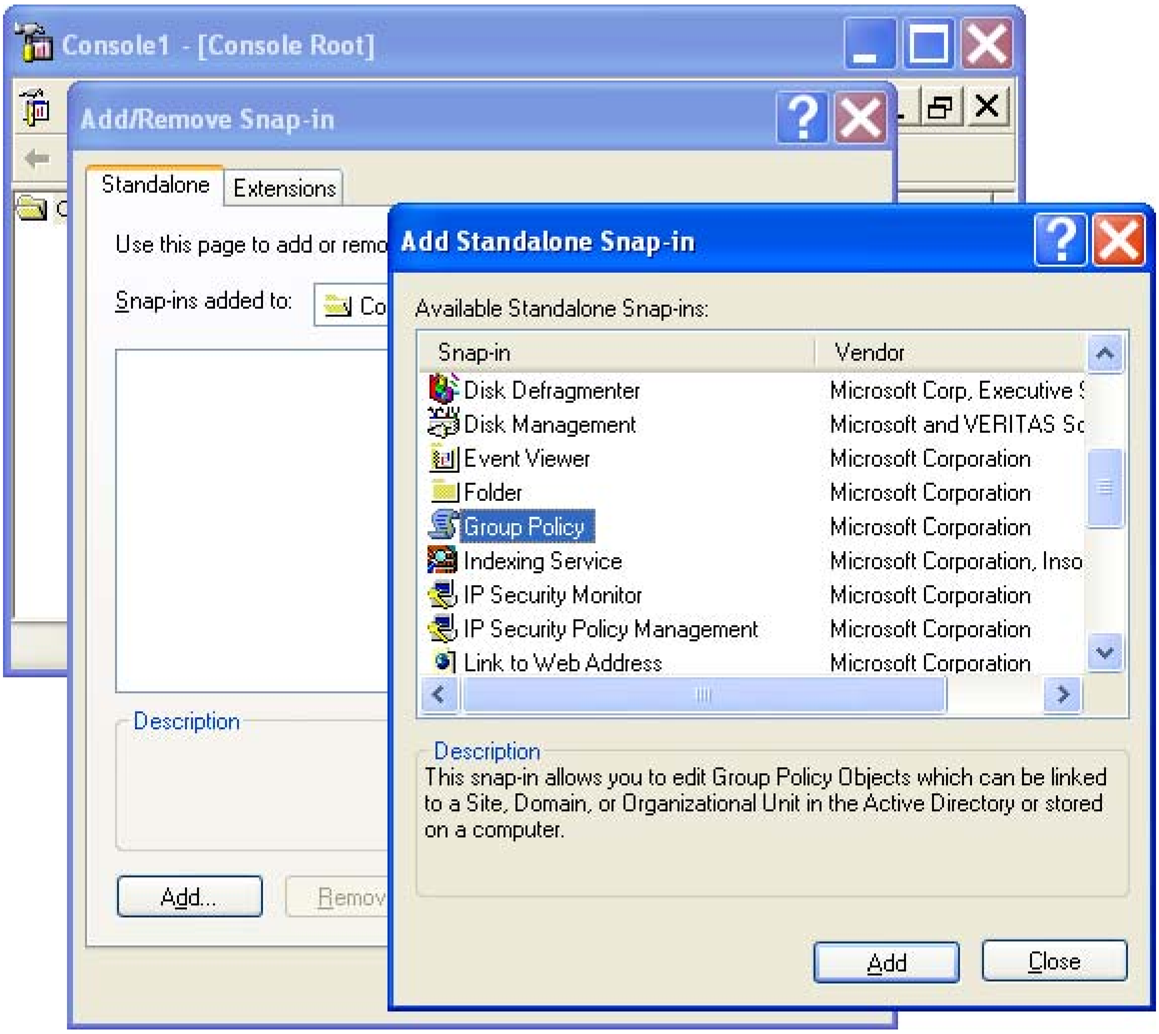
3. Click the *Standalone* tab, and then click *Add*.



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

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



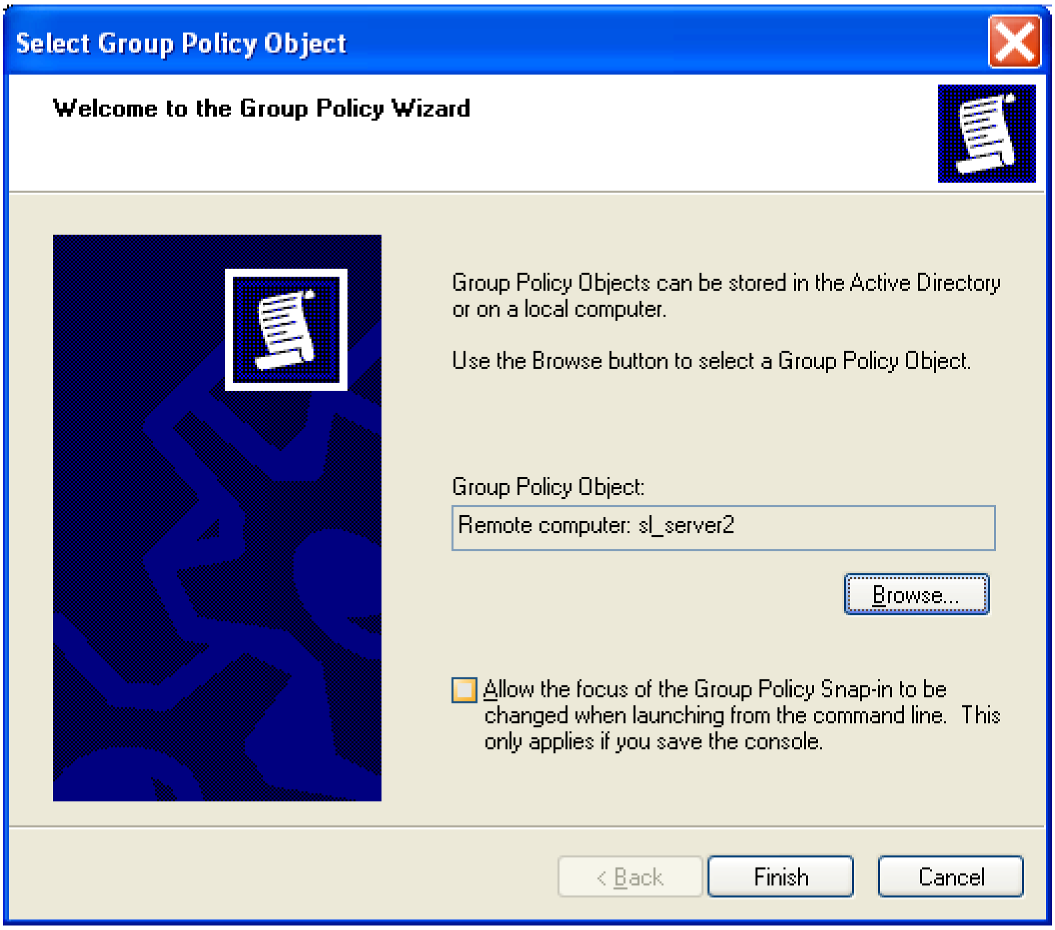
Available Standalone Snap-ins:

| Snap-in | Vendor |
|---|---|
| Disk Defragmenter | Microsoft Corp, Executive S |
| Disk Management | Microsoft and VERITAS Sc |
| Event Viewer | Microsoft Corporation |
| Folder | Microsoft Corporation |
| Group Policy | Microsoft Corporation |
| Indexing Service | Microsoft Corporation, Inso |
| IP Security Monitor | Microsoft Corporation |
| IP Security Policy Management | Microsoft Corporation |
| Link to Web Address | Microsoft Corporation |

Description

This snap-in allows you to edit Group Policy Objects which can be linked to a Site, Domain, or Organizational Unit in the Active Directory or stored on a computer.

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



Welcome to the Group Policy Wizard

Group Policy Objects can be stored in the Active Directory or on a local computer.

Use the Browse button to select a Group Policy Object.

Group Policy Object:

Remote computer: sl_server2

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

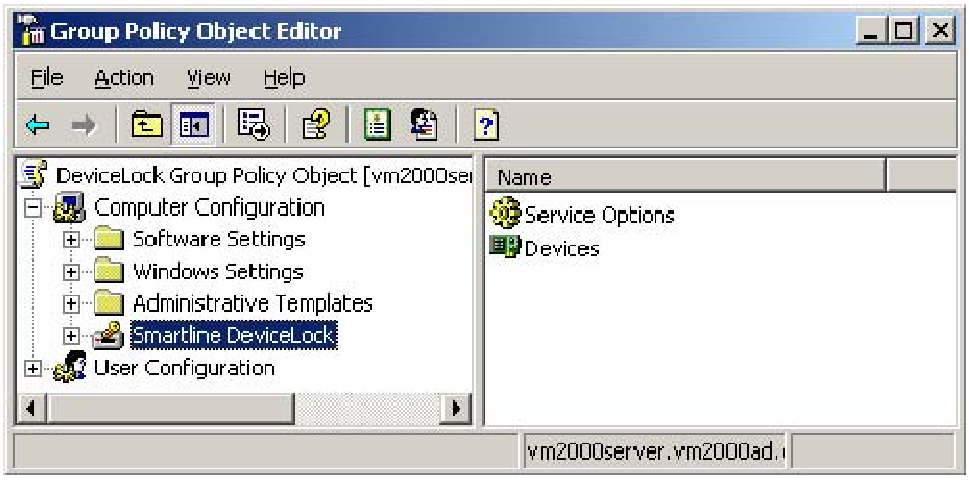
6. Click *Close* to close the *Add Standalone Snap-in* window.

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

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

## 6.5 Using DeviceLock Group Policy Manager

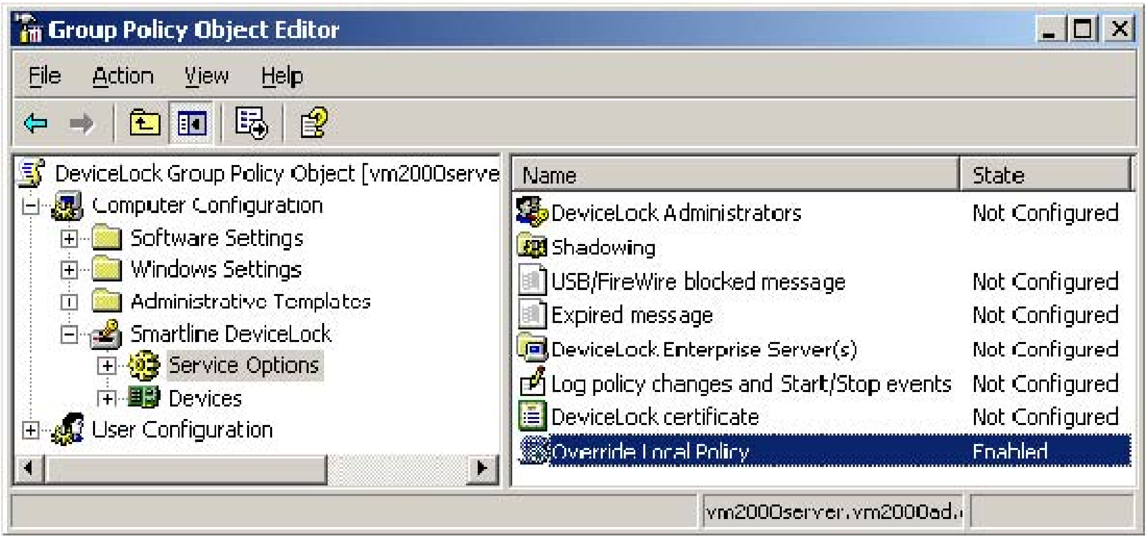
There is almost no difference between the procedure of managing DeviceLock Service via DeviceLock Management Console and via DeviceLock Group Policy Manager. For more information, please read the **Managing DeviceLock Service** section of this manual.



It is impossible to manage DeviceLock Enterprise Server and view audit and shadow logs using DeviceLock Group Policy Manager. For such operations you should use DeviceLock Management Console.

DeviceLock Service management via DeviceLock Group Policy Manager includes three additional features in comparison to DeviceLock Management Console:

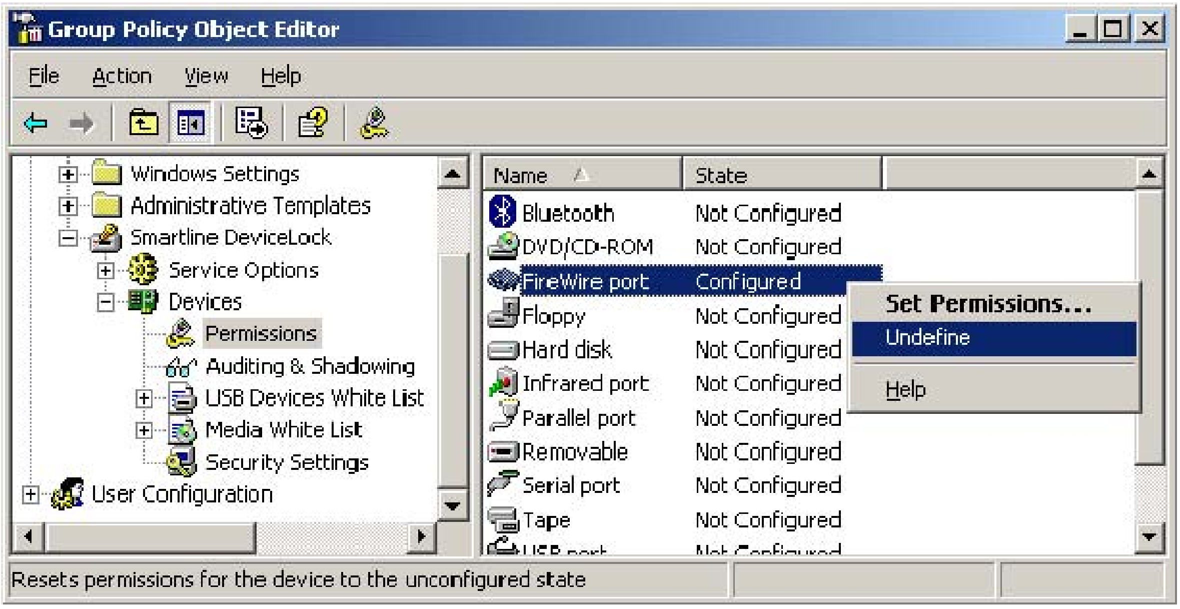
1. **Override Local Policy** – If you want to disallow changing settings, permissions and audit rules for individual computers (without the GPO editor), enable *Override Local Policy* in *Service Options*. This enables the *Group Policy* mode for all the computers in GPO, such that the *Local Policy*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



| Name | State |
|---|---|
| DeviceLock Administrators | Not Configured |
| Shadowing | |
| USB/FireWire blocked message | Not Configured |
| Expired message | Not Configured |
| DeviceLock Enterprise Server(s) | Not Configured |
| Log policy changes and Start/Stop events | Not Configured |
| DeviceLock certificate | Not Configured |
| Override Local Policy | Enabled |

If the *Override Local Policy* parameter is enabled, it means that the *Use Group Policy* parameter in *Service Options* of DeviceLock Management Console and DeviceLock Enterprise Manager can't be disabled.

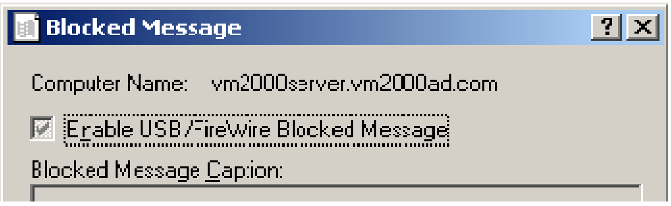
2. **Undefine** – you can reset any parameter to the unconfigured state. All undefined parameters are ignored in this GPO. For more information, please read the Standard GPO Inheritance Rules section of this manual.



| Name | State |
|---|---|
| Bluetooth | Not Configured |
| DVD/CD-ROM | Not Configured |
| FireWire port | Configured |
| Floppy | Not Configured |
| Hard disk | Not Configured |
| Infrared port | Not Configured |
| Parallel port | Not Configured |
| Removable | Not Configured |
| Serial port | Not Configured |
| Tape | Not Configured |
| USB port | Not Configured |

Resets permissions for the device to the unconfigured state

Use *Undefine* from the context menu of any parameter to reset this parameter to the unconfigured state. Also, for some parameters, you can use the intermediate state (gray) of the flag to make it unconfigured.

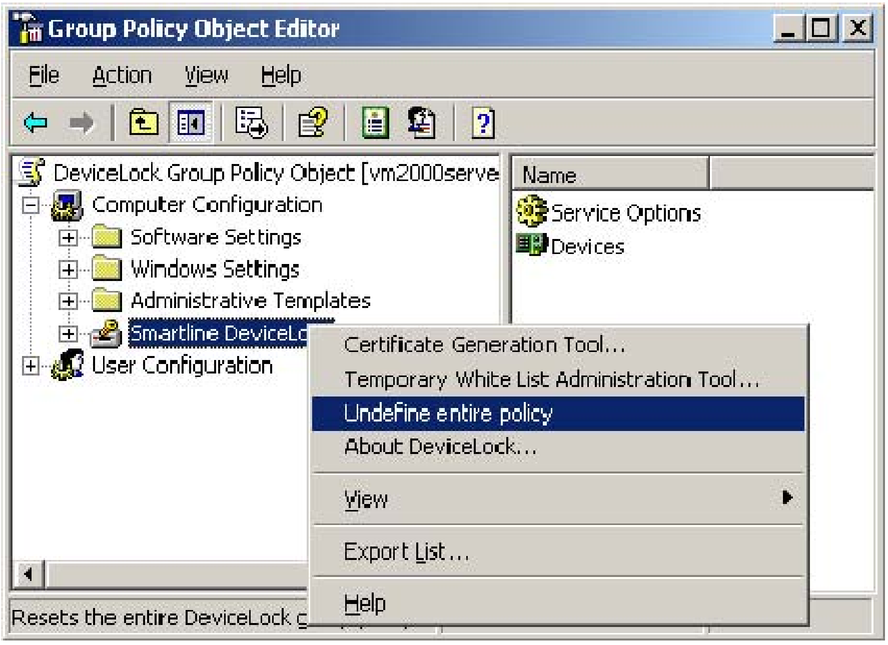


Computer Name: vm2000server.vm2000ad.com

☑ Enable USB/FireWire Blocked Message

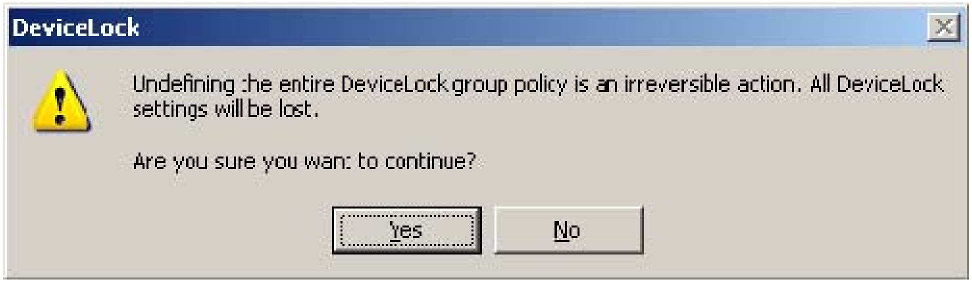
Blocked Message Caption:

3. **Undefine entire policy** – You can reset all parameters to the unconfigured state in one click. Selecting this has the same effect as resetting each parameter one by one (see above).



Resets the entire DeviceLock c

Use *Undefine entire policy* from the context menu of the *SmartLine DeviceLock* root item to reset all parameters to the unconfigured state.



Undefining the entire DeviceLock group policy is an irreversible action. All DeviceLock settings will be lost.

Are you sure you want to continue?

***NOTE: In order to manage DeviceLock Service 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 Deploying DeviceLock Service section of this manual.***

***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.***

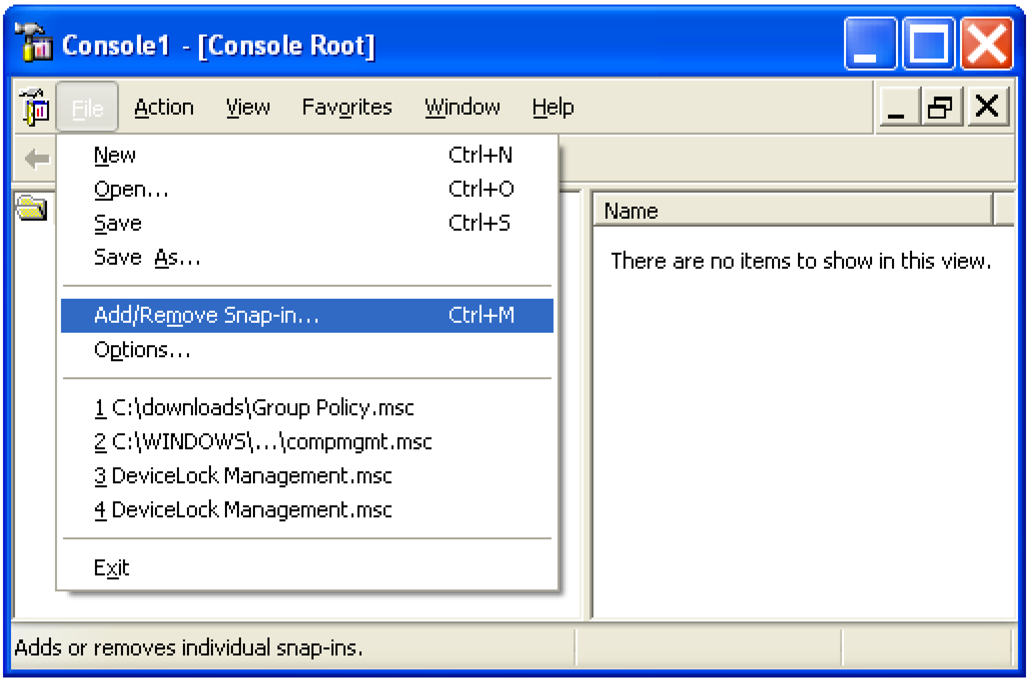
## 6.6 Using Resultant Set of Policy (RSoP)

DeviceLock supports Resultant Set of Policy so you can use the standard Windows snap-in to view the DeviceLock policy currently being applied, as well as to predict what policy would be applied to a chosen computer.

To use RSoP you should start MMC and add the *Resultant Set of 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*.



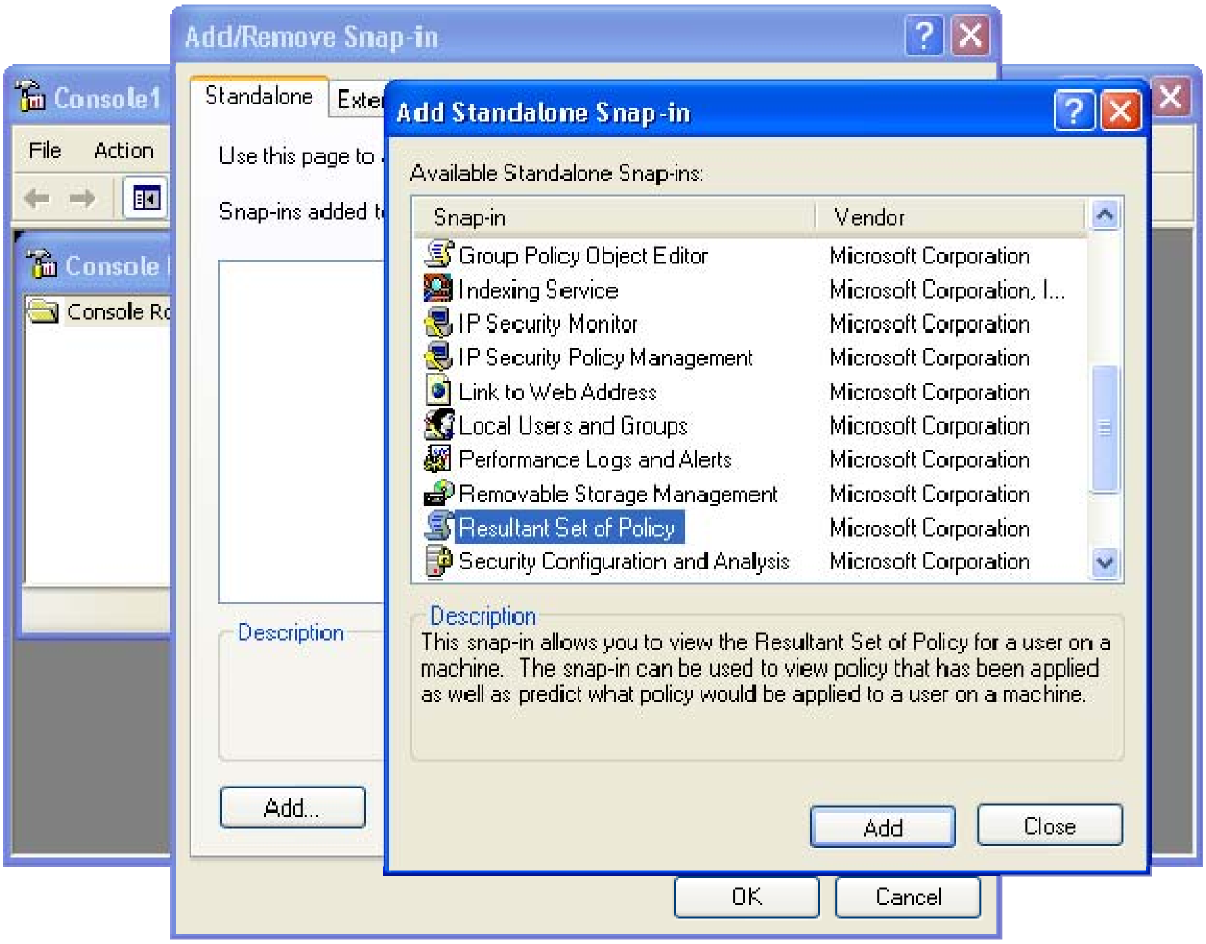
Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\downloads\Group Policy.msc
2 C:\WINDOWS\...\compmgmt.msc
3 DeviceLock Management.msc
4 DeviceLock Management.msc
Exit
Name

There are no items to show in this view.

Adds or removes individual snap-ins.

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

4. Select *Resultant Set of Policy* from the list, then click *Add*.



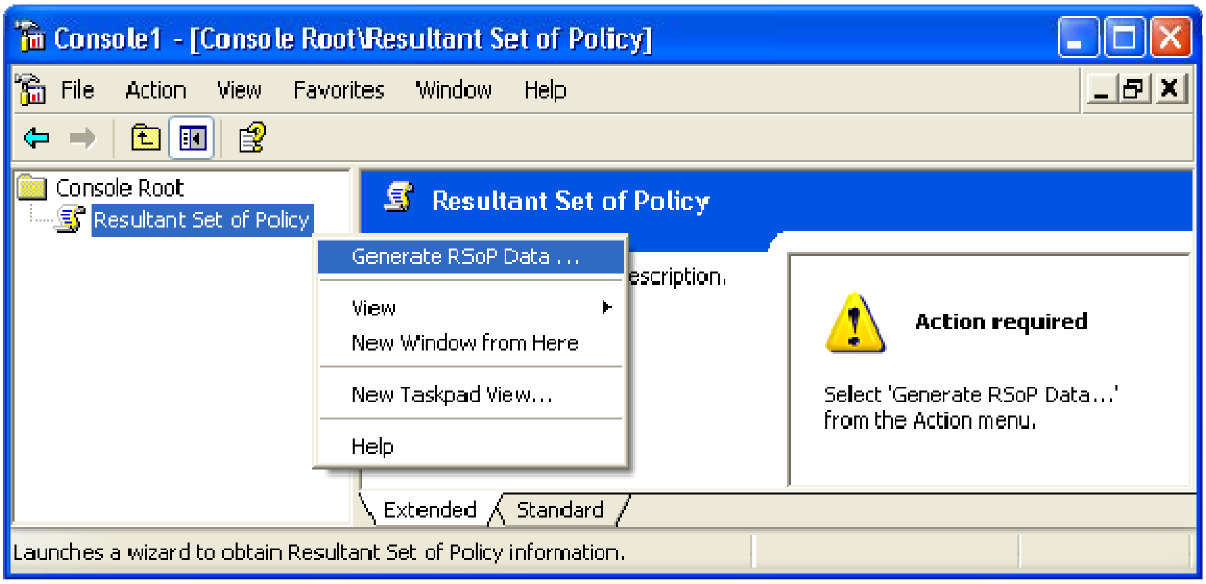
| Snap-in | Vendor |
|---|---|
| Group Policy Object Editor | Microsoft Corporation |
| Indexing Service | Microsoft Corporation, I... |
| IP Security Monitor | Microsoft Corporation |
| IP Security Policy Management | Microsoft Corporation |
| Link to Web Address | Microsoft Corporation |
| Local Users and Groups | Microsoft Corporation |
| Performance Logs and Alerts | Microsoft Corporation |
| Removable Storage Management | Microsoft Corporation |
| Resultant Set of Policy | Microsoft Corporation |
| Security Configuration and Analysis | Microsoft Corporation |

Description

This snap-in allows you to view the Resultant Set of Policy for a user on a machine. The snap-in can be used to view policy that has been applied as well as predict what policy would be applied to a user on a machine.

5. Click *Close* to close the *Add Standalone Snap-in* window and then click *OK* to add the snap-in.

6. In the console tree, select *Resultant Set of Policy*.



Action required

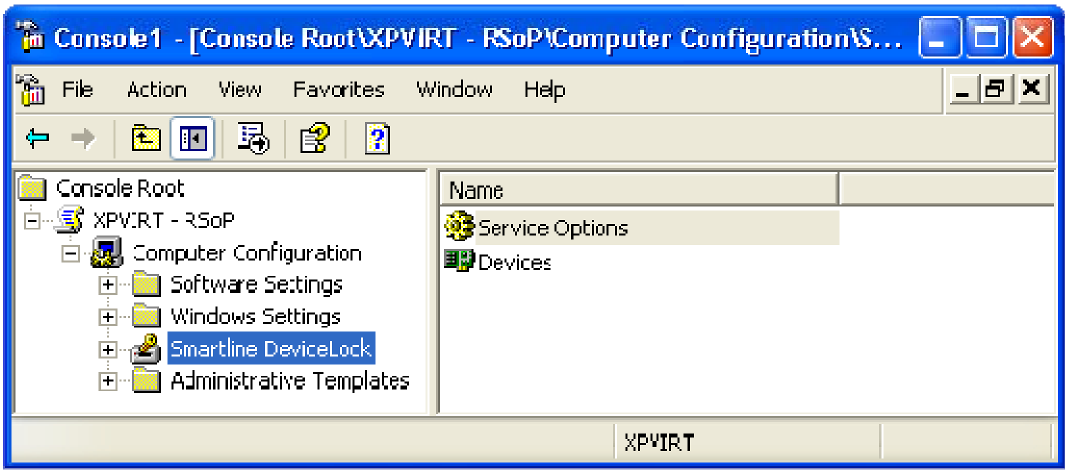
Select 'Generate RSoP Data...' from the Action menu.

Launches a wizard to obtain Resultant Set of Policy information.

7. Click *Generate RSoP Data* in the context menu available by a right mouse click.

8. Go through the *Resultant Set of Policy Wizard* to obtain RSoP information from the selected computer.

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



Please note that using RSoP you can't modify the policy – all parameters are in the read-only mode.

RSoP is very useful when you need to understand which particular GPO will be applied to the computer.

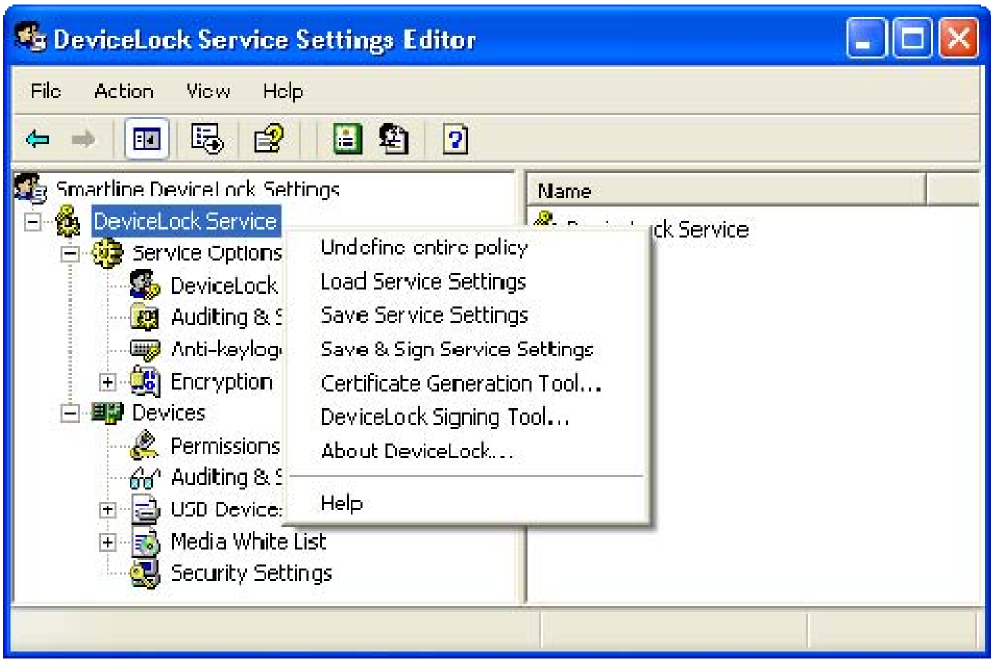
For more information on Resultant Set of Policy, please refer to the Microsoft's on-line article: http://technet2.microsoft.com/WindowsServer/en/library/1180b465-ea3b-4a73-8670-81fa5871a3c71033.mspx?mfr=true.

# 7 DeviceLock Service Settings Editor

## 7.1 Overview

DeviceLock Service Settings Editor is using for creating and modifying external XML files with settings, permissions, audit and shadowing rules for DeviceLock Service.

DeviceLock Service Settings Editor installs together with other management consoles.



There is almost no difference between the procedures for defining policies via DeviceLock Management Console versus via DeviceLock Service Settings Editor. For more information, please read the **Managing DeviceLock Service** section of this manual.

In comparison to DeviceLock Management Console in DeviceLock Service Settings Editor:

- You do not need to connect to any computer with DeviceLock Service. DeviceLock Service Settings Editor modifies and stores settings in external XML files and allows you to create/edit policies off-line. It works similar to DeviceLock Group Policy Manager but instead of GPOs it uses XML files.

- You can reset any parameter (or all parameters at once) to the unconfigured state. All undefined parameters are ignored when the policy is applied to DeviceLock Service.

To create the new policy from scratch, just run DeviceLock Service Settings Editor and start making changes in its default (empty) policy.

If you want to modify an existing policy, you should load the XML file with that policy to DeviceLock Service Settings Editor using the *Load Service Settings* context menu item and then make desired changes.

In any case to save the changes you made, you should use *Save Service Settings* from the context menu. Alternatively, you can use *Save & Sign Service Settings* from the context menu to save the policy to an external XML file and automatically sign it with the most recent DeviceLock Certificate (the *private* key). The *Save & Sign Service Settings* menu item is disabled when the DeviceLock Signing Tool has no previously loaded *private* key.

Later files with policies created using DeviceLock Service Settings Editor can be loaded via DeviceLock Management Console and/or DeviceLock Group Policy Manager.

Also, files with policies can be sent to users whose computers are not online and thus out-of-reach via management consoles. To avoid unauthorized modification these files should be signed with the DeviceLock Certificate (the *private* key) using the DeviceLock Signing Tool. For more information please read the **Service Settings** section of this manual.

DeviceLock Service Settings Editor is also using in the *Set Service Settings* plug-in of DeviceLock Enterprise Manager. This plug-in runs DeviceLock Service Settings Editor as an external application and opens it with the XML file selected in the plug-in's settings dialog.

When you make any policy changes (change parameters, set permissions, define white lists, etc.) in the XML file passed to the editor by the plug-in, DeviceLock Service Settings Editor automatically saves them to this file. As soon as you finish modifying the policy just close DeviceLock Service Settings Editor and return to the plug-in's settings dialog.

For more information read the **Set Service Settings** section of this manual.

# 8 DeviceLock Enterprise Manager

## 8.1 Overview

With DeviceLock Enterprise Manager you can view and change settings, permissions and audit rules; install, update and uninstall DeviceLock Service; and view audit and shadow logs for all the computers in a large network. We recommend using DeviceLock Enterprise Manager if you have a large network without Active Directory.

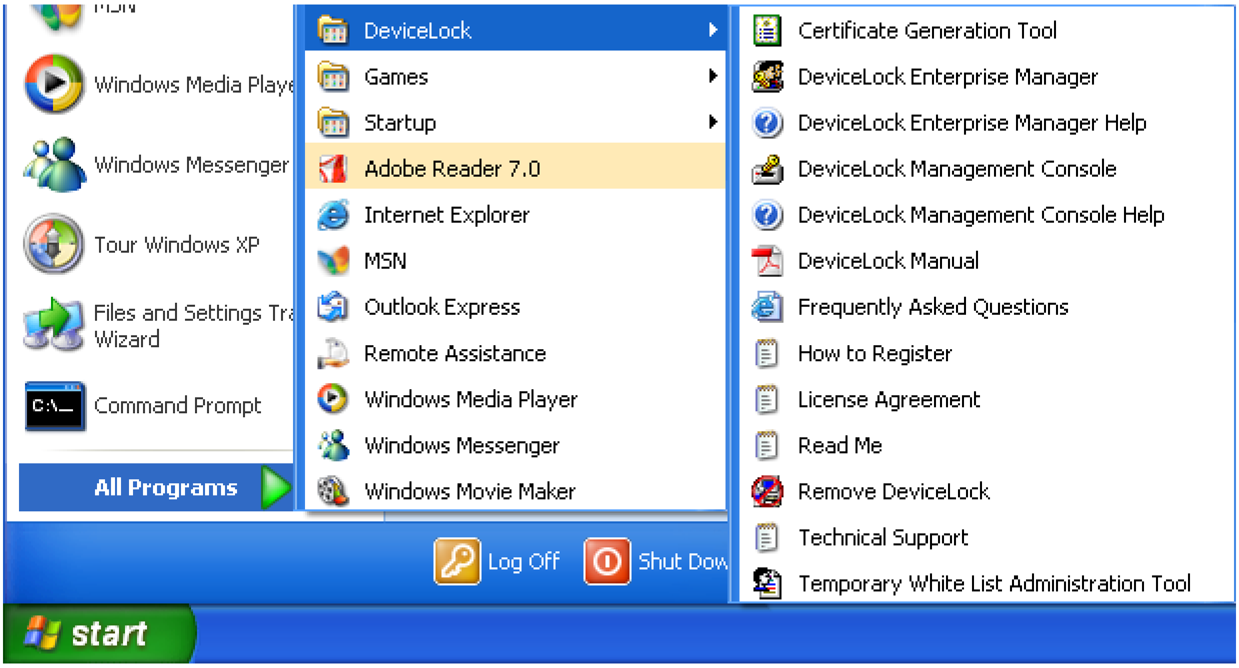
Based on a multi-threaded engine, using this console speeds up all activity for all the computers in the large network.

DeviceLock Enterprise Manager stores, compares and filters the data it receives from all the computers. Administrators can make "snapshots" of the systems for future comparison and notation of changes.

DeviceLock Enterprise Manager has a flexible plug-in based architecture that allows you to plug in necessary modules on demand. Each module (plug-in) performs a task and displays retrieved information in its own window.

For information on how to install DeviceLock Enterprise Manager, please read the **Installing Management Consoles** section of this manual.

To run DeviceLock Enterprise Manager, select the appropriate shortcut from the *Programs* menu available by clicking the Windows *Start* button.

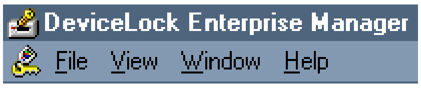


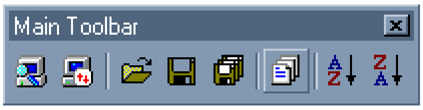
## 8.2 Interface

DeviceLock Enterprise Manager has a Multi Document Interface (MDI) structure, allowing you to keep each task in its own window.

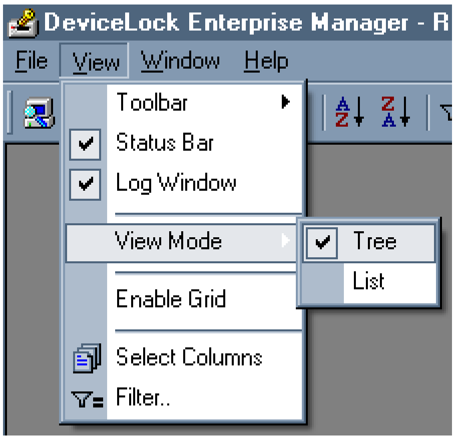
The main window of DeviceLock Enterprise Manager can be resized. DeviceLock Enterprise Manager saves its size and position, and restores these at its next startup.

There is a menu at the top of the main window. Many functions are accessible through this menu.





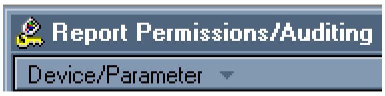
To change the columns displayed in the plug-in's windows, click *Select Columns* in the *View* menu or press the appropriate button on the *Main* toolbar.



By default, DeviceLock Enterprise Manager displays information received from the plug-ins in the form of a tree. However, information can also be displayed as a plain list. To change the mode, click *View Mode* in the *View* menu and select either *Tree* or *List*. Please note that View Mode must be set for each plug-in individually.

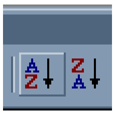
You can hide the status bar and/or the log window by deselecting appropriate items in the *View* menu.

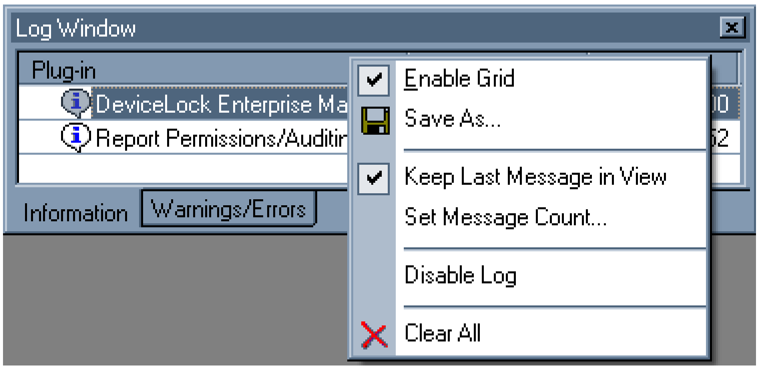
To enable the gridlines around items in the plug-in's window, select *Enable Grid* in the *View* menu. This mode sets for each plug-in individually.



To sort data in any plug-in's window, click the column heading you want to sort by. To reverse the sort order, click the column heading a second time.

If you need to sort the top-level tree's items (such as domains and computers), use appropriate buttons on the *Main* toolbar.



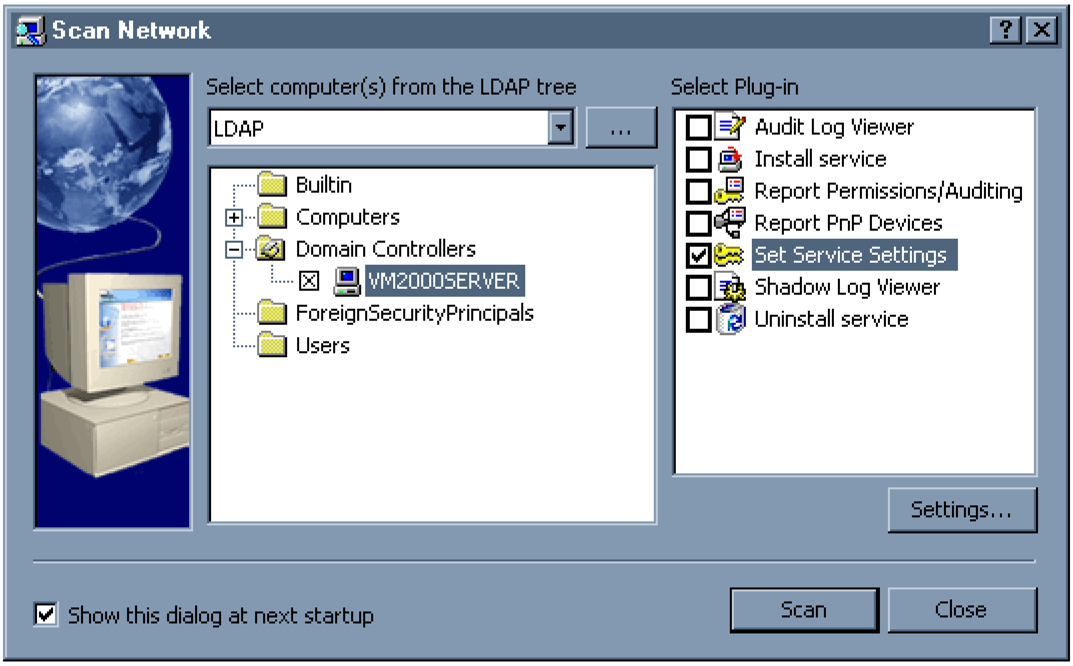


There is a log window at the bottom of the main window. The log window is used to display useful information about ongoing activity as well as diagnostic and error messages. There are two log lists: *Information* and *Warnings/Errors*.

You can click the right mouse button on the log window to open the useful context menu.

## 8.3 Scan Network Dialog

The *Scan Network* dialog allows you to select computers in your network and the action (install or remove DeviceLock Service, set permissions, and so on) which should be performed for these computers.



To open the *Scan Network* dialog, select *Scan Network* from the *File* menu or press the appropriate button on the *Main* toolbar. If the *Show this dialog at next startup* flag is checked, the *Scan Network* dialog will open automatically each time DeviceLock Enterprise Manager is started.

There are three simple steps, which enable you to manage DeviceLock Services across the network.

### 8.3.1 Selecting Computers

The first step is to select the computers to be processed.

You can use the context menu, available by right clicking, to select/deselect necessary items (computers types, domains, or computers).

DeviceLock Enterprise Manager provides several flexible ways to select network computers.

- Network computers can be selected by their types.

  Each type represents all of the computers belonging to the category:

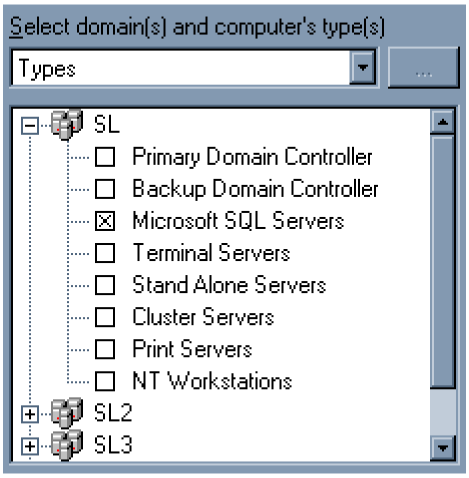
  - *Primary Domain Controller* – a primary domain controller.

  - *Backup Domain Controller* – a backup domain controller.

- *Microsoft SQL Servers* – any server running with Microsoft SQL Server.
- *Terminal Servers* – any server where Terminal Services are running.
- *Stand Alone Servers* – any server that is not a domain controller.
- *Cluster Servers* – server clusters available in the domain.
- *Print Servers* – any computer that is sharing the print queue.
- *NT Workstations* – any Windows NT/2000/XP workstation.

There are two ways to choose the type of computers:

1. *Types* – you select the network domain and then select types of computers which must be processed in this domain.



Select domain(s) and computer's type(s)

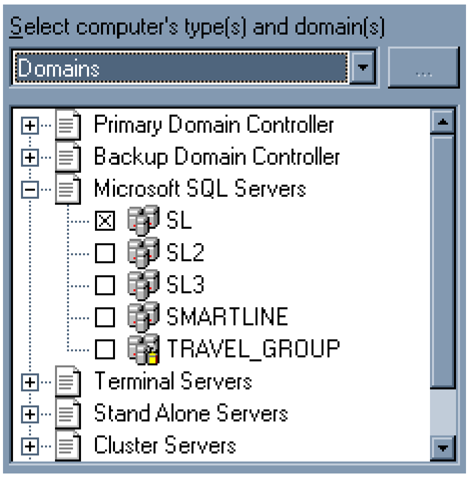
Types

SL
- ☐ Primary Domain Controller
- ☐ Backup Domain Controller
- ☒ Microsoft SQL Servers
- ☐ Terminal Servers
- ☐ Stand Alone Servers
- ☐ Cluster Servers
- ☐ Print Servers
- ☐ NT Workstations

SL2

SL3

2. *Domains* – you select the type of computer and then select network domains where computers of the selected type must be processed.



Select computer's type(s) and domain(s)

Domains

Primary Domain Controller

Backup Domain Controller

Microsoft SQL Servers
- ☒ SL
- ☐ SL2
- ☐ SL3
- ☐ SMARTLINE
- ☐ TRAVEL_GROUP

Terminal Servers

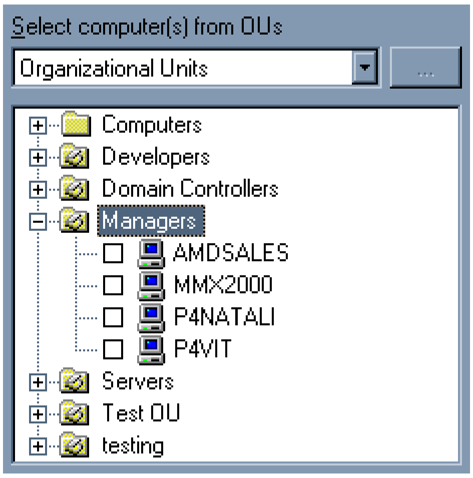
Stand Alone Servers

Cluster Servers

- Network computers can also be selected by their names.

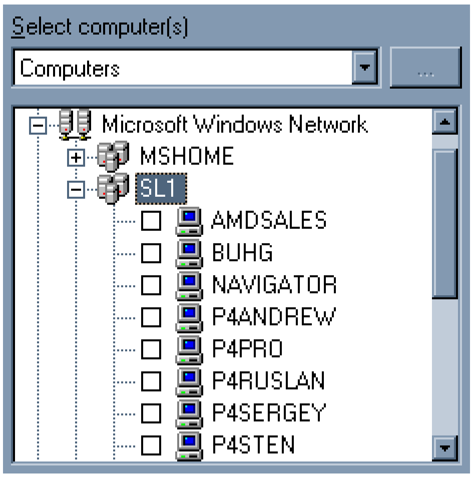
  There are several ways to choose computers by name:

  1. *Organizational Units* – you browse Active Directory organizational units (OUs) and select computers, which must be processed.



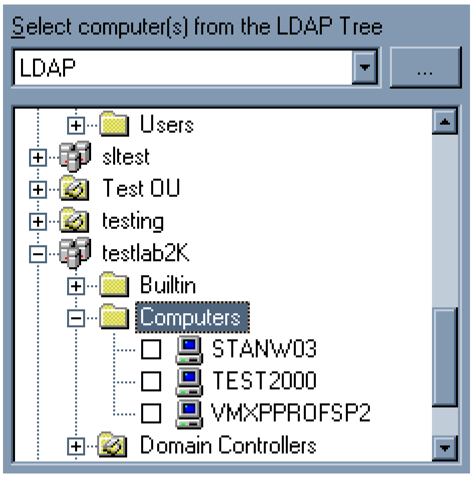
Select computer(s) from OUs: Organizational Units

  2. *Computers* – you browse the network tree and select computers.



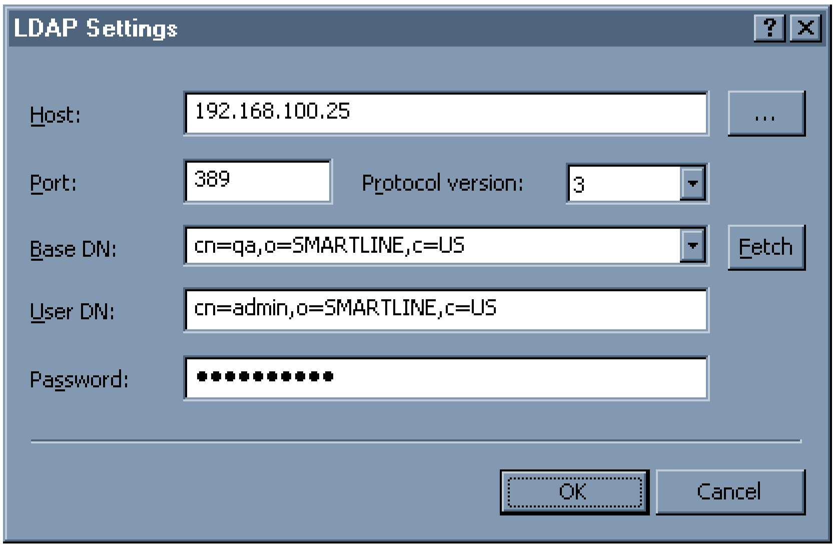
Select computer(s): Computers

  3. *LDAP* – you browse the LDAP (Lightweight Directory Access Protocol) tree and select computers from the directory.



Select computer(s) from the LDAP Tree: LDAP

To configure a connection to the LDAP server, press the **...** button.



LDAP Settings

Host: 192.168.100.25

Port: 389

Protocol version: 3

Base DN: cn=qa,o=SMARTLINE,c=US

User DN: cn=admin,o=SMARTLINE,c=US

Password: ●●●●●●●●●●●

- *Host* – the name or the IP address of the LDAP server to connect to.

- *Port* – the TCP port on which the LDAP server accepts connections. The default port is 389.

- *Protocol version* – the LDAP protocol version. Some servers are not fully compatible with the LDAP v.3 protocol and LDAP requests require certain adjustments for correct communication with such servers. Selecting *Version 2* makes sure that the server requests are adjusted according to the LDAP v.2 protocol requirements.

- *Base DN* – the starting point for you to browse the directory tree. You must use the LDAP string representation for distinguished names (for example, *cn=qa,o=SMARTLINE,c=US*). Leave the *Base DN* field blank to start browsing from the root.

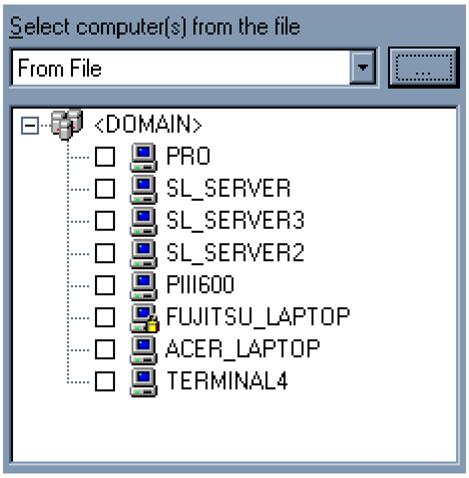
  By pressing the *Fetch* button, you can get all the published naming contexts.

- *User DN* – the distinguished name (DN) of the directory user that allows connection to the directory. You must use the LDAP string representation for distinguished names (for example, *cn=admin,o=SMARTLINE,c=US*).

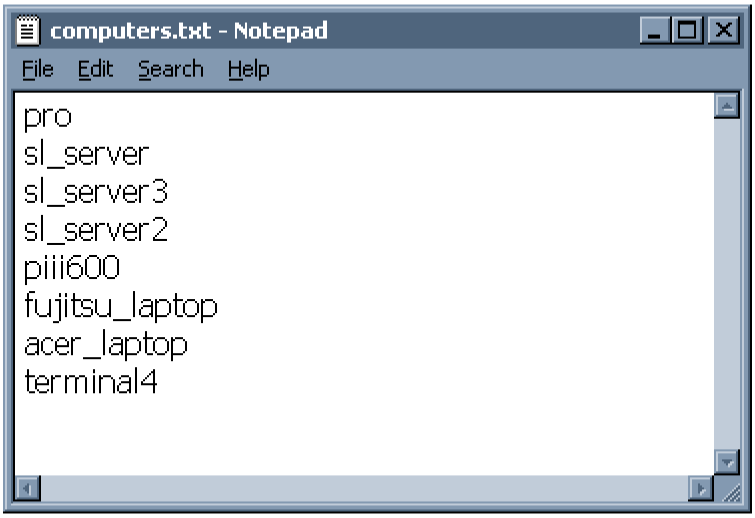
- *Password* – the user's password.

4. *From File* – you load a predefined list of computers from the external text file and then select the computers.

   To open an external file, press the **...** button.



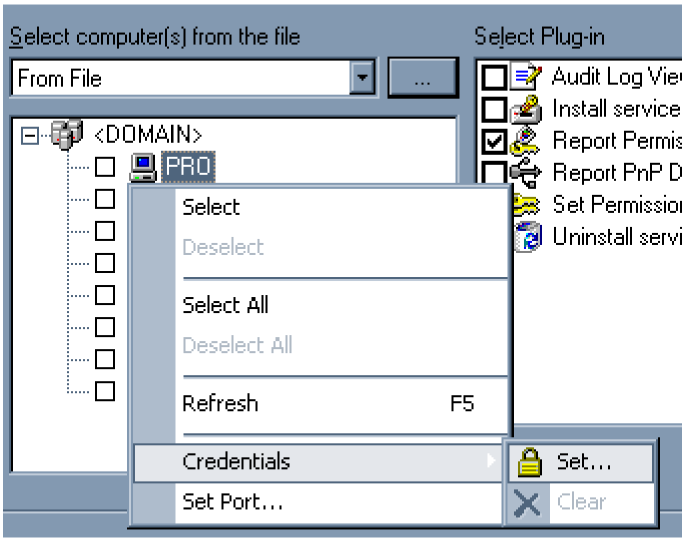
A text file must contain each computer’s name or IP address on separate lines and can be either Unicode or non-Unicode. A brief example of such a file follows:



```
pro
sl_server
sl_server3
sl_server2
piii600
fujitsu_laptop
acer_laptop
terminal4
```

### 8.3.1.1 Supplying Credentials

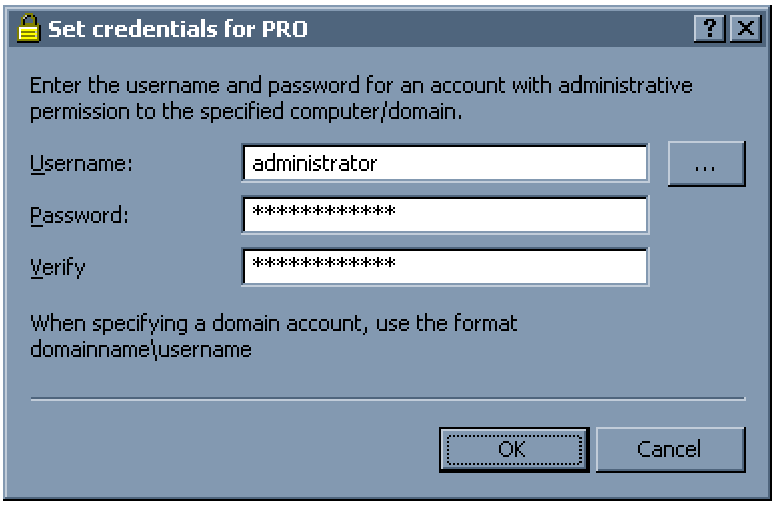
If you need to supply alternative credentials for the target computer(s), highlight the computer or network domain from the tree and use the *Credentials* sub-menu from the context menu.



You may assign credentials to individual computers and/or to network domains. To add credentials, use the *Set* item. To delete alternative credentials, use the *Clear* item.

Credentials consist of a user name and password pair used to authenticate the computers processed. By default, DeviceLock Enterprise Manager uses your currently logged on credentials to automatically log in and process the target computer(s). If the current logged-in user credentials do not have administrative rights on all of the target computers, you need to enter alternate credentials. DeviceLock Enterprise Manager will use these alternate credentials to automatically login to the target computers.

In all cases, credentials are stored with encryption techniques and are not available to anyone except the user with administrative privileges.

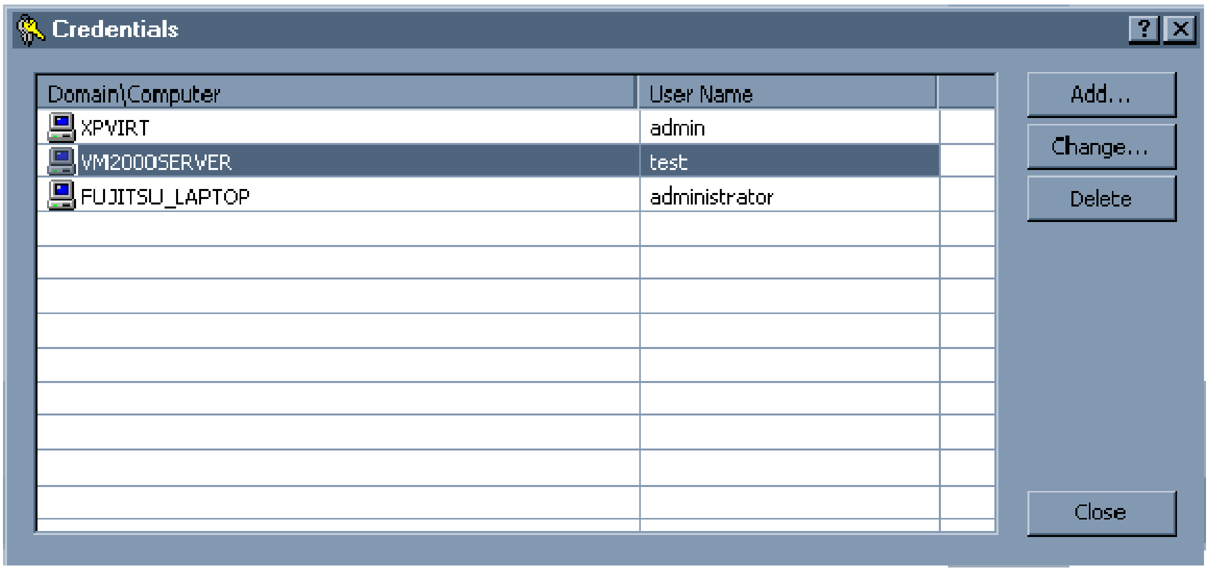


Enter the username and password for an account with administrative permission to the specified computer/domain.

Username: administrator
Password: ************
Verify ************

When specifying a domain account, use the format domainname\username

Credentials can also be supplied via the *Credentials* dialog. To open the *Credentials* dialog, you can select *Credentials* from the *File* menu.



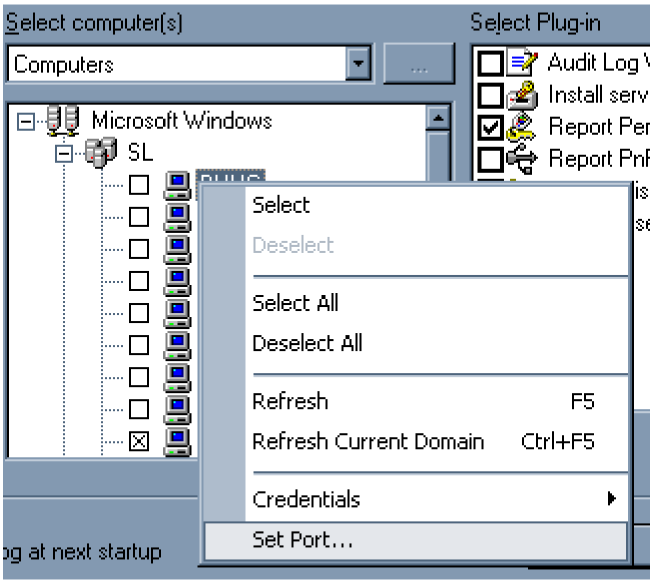
| Domain\Computer | User Name |
|---|---|
| XPVIRT | admin |
| VM2000SERVER | test |
| FUJITSU_LAPTOP | administrator |

Press the *Add* button to add new credentials. To change existing credentials, highlight the record in the list and press the *Change* button.

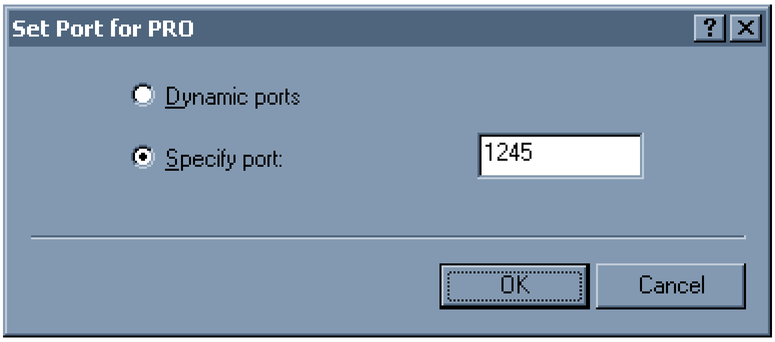
To delete credentials, highlight the record in the list and press the *Delete* button. Using *Ctrl* and/or *Shift* you can highlight and remove several records simultaneously.

### 8.3.1.2 Setting Port

You can instruct DeviceLock Enterprise Manager to use a fixed port, making it easier to configure a firewall. To do so, use *Set port* from the context menu.



By default, DeviceLock Enterprise Manager uses dynamic ports for RPC communication with DeviceLock Service. However, if DeviceLock Service is configured to accept connections on a fixed port, select the *Specify port* parameter.


Set Port for PRO

○ Dynamic ports

● Specify port: 1245

To use the dynamic ports binding, select *Dynamic ports*.

DeviceLock Service can be configured to use either a fixed port or dynamic ports during the installation process. For more information on this, please read **Unattended Installation** and **Remote Installation via DeviceLock Enterprise Manager** sections of this manual.

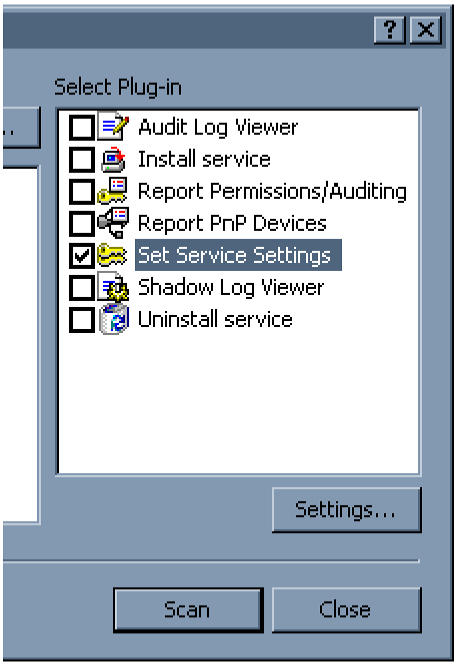
If you need to change the port configuration when DeviceLock Service is already installed, use the *Install service* plug-in.

For information on which ports are required for which actions, please read the **Plug-ins** section of this manual.

## 8.3.2 Selecting Plug-ins

The second step is to select a plug-in to process the network computers selected on the first step.

To select/deselect plug-ins, you can use the context menu available with a right mouse click.



To define parameters for the selected plug-in, use the *Settings* button below the plug-ins list. If the plug-in doesn't have additional parameters, this button is disabled.

Tasks are passed to the plug-in by DeviceLock Enterprise Manager.

The plug-in performs the task and returns the information to DeviceLock Enterprise Manager. Upon receipt of a plug-in's information, DeviceLock Enterprise Manager displays it in a separate window.

## 8.3.3 Starting a Scan

Once you have selected computers and the appropriate plug-in, the final step is starting the scan process. Press the *Scan* button to initiate the process.

Right after the scan process is initiated, you can start to explore the information that is already received from the plug-in.

Because the scan process runs in a separate thread, you do not need to wait until all computers are finished being scanned. You can also perform other tasks in the DeviceLock Enterprise Manager interface.

There are only a few things which you cannot do while the scan is running – you cannot close DeviceLock Enterprise Manager and you cannot run another scan process.

If, for some reason, you wish to abort the active scan process, you can select *Stop Scan* from the *File* menu or press the appropriate button on the *Main* toolbar. The scan process will be aborted as soon as a plug-in returns control to DeviceLock Enterprise Manager.

## 8.4 Plug-ins

DeviceLock Enterprise Manager has a flexible plug-in based architecture that allows you to plug in the necessary module on demand. DeviceLock Enterprise Manager loads the plug-ins on startup from the *Plugins* subdirectory, which is located in the main DeviceLock Enterprise Manager directory.

DeviceLock Enterprise Manager ships with standard plug-ins that require some network ports to be opened on remote computers, as described in the table below:

| Required Ports | Plug-ins affected |
|---|---|
| **TCP 139**<br>**UDP 137** – this port must be opened only when a connection is establishing by the computer name. If an IP address is used, this port isn't required. | Audit Log Viewer, Report PnP Devices |
| **TCP 139**<br>**TCP 135** – this port is required only when the *Dynamic ports* connection is used.<br>**TCP <*all ports above 1024*>** – these ports are required only when the *Dynamic ports* connection is used.<br>**TCP <*custom port*>** – this port is required only when the *Fixed port* connection is used.<br>**UDP 137** – this port must be opened only when a connection is established by the computer name. If an IP address is used, this port isn't required. | Install Service, Uninstall Service |
| **TCP 135** – this port is required only when the *Dynamic ports* connection is used.<br>**TCP <*all ports above 1024*>** – these ports are required only when the *Dynamic ports* connection is used.<br>**TCP <*custom port*>** – this port is required only when the *Fixed port* connection is used.<br>**UDP 137** – this port must be opened only when a connection is established by computer name. If an IP address is used, this port isn't required. | Report Permissions/Auditing, Set Service Settings, Shadow Log Viewer |

For information on how to use either the *Dynamic ports* or *Fixed port* connection in DeviceLock Enterprise Manager, please read the **Setting Port** section of this manual.

When a plug-in is connected to a remote computer it may receive some of these errors:

- *The product version on the client and server machines does not match (7049)* – you're trying to connect to a computer where an old version of DeviceLock Service is installed. You should upgrade the DeviceLock Service first using the Install Service plug-in.

- *The network path was not found (53)* – you're trying to connect to a computer that either does not exist (the wrong name or IP address) or is not accessible. Make sure that the computer name you've specified is correct. Try to access this computer with *Windows Explorer* and connect to it using any standard Windows administrative tool (such as *Computer Management*, *Services* and so on).

  This error also occurs when the standard Windows *Server* service is not running on the remote computer. Check the *Server* service status and start it if it is stopped.

More connection errors are described in the **Possible Connection Errors** section of this manual.

### 8.4.1 Audit Log Viewer

The *Audit Log Viewer* plug-in retrieves DeviceLock's audit log from the computer's local Windows event logging subsystem.

To define a maximum log size and what Windows should do if the audit log becomes full, use *Audit Log Settings* from the context menu.

To clear all events from the audit log, select *Clear Audit Log* from the context menu.

For more information, please read the **Audit Log Viewer (Service)** section of this manual.

### 8.4.2 Install Service

The *Install Service* plug-in installs or updates DeviceLock Service on computers.

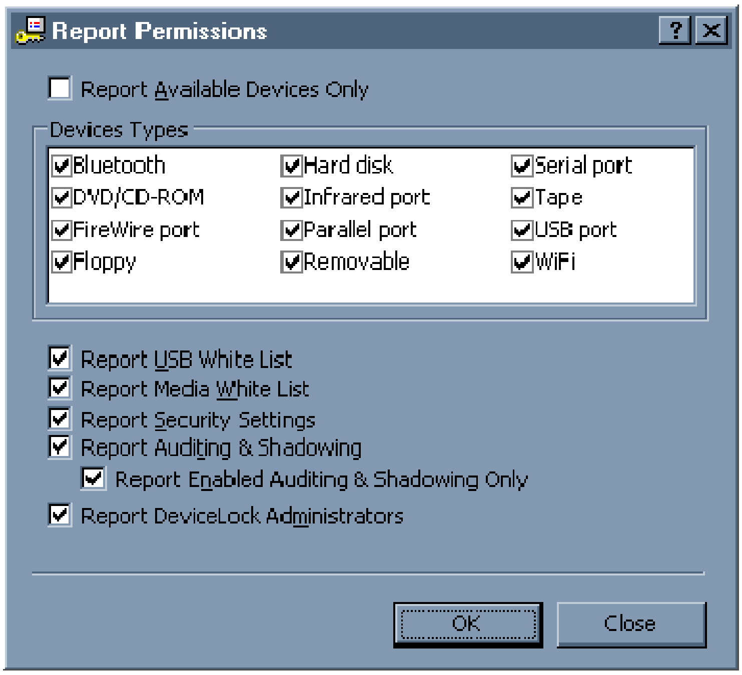
Before you can use this plug-in, you should specify the path to the DeviceLock Service executable files (*dlservice.exe* and *dlservice_x64.exe*). You can do this by pressing the *Settings* button below the plug-ins list on the *Scan Network* dialog (see **Selecting Plug-ins**).

For more information, please read the **Remote Installation via DeviceLock Enterprise Manager** section of this manual.

### 8.4.3 Report Permissions/Auditing

The *Report Permissions/Auditing* plug-in generates a report concerning settings, permissions and audit rules that have been set for DeviceLock Services across the network.

Before you can use this plug-in, you should select the information you want to include in the report. You can do this by pressing the *Settings* button below the plug-ins list on the *Scan Network* dialog (see **Selecting Plug-ins**).



Report Permissions

☐ Report Available Devices Only

Devices Types

☑Bluetooth ☑Hard disk ☑Serial port
☑DVD/CD-ROM ☑Infrared port ☑Tape
☑FireWire port ☑Parallel port ☑USB port
☑Floppy ☑Removable ☑WiFi

☑ Report USB White List
☑ Report Media White List
☑ Report Security Settings
☑ Report Auditing & Shadowing
☑ Report Enabled Auditing & Shadowing Only
☑ Report DeviceLock Administrators

- *Report Available Devices Only* – check this flag to report permissions and audit rules for only those devices currently available on the computer. Otherwise, you will see permissions and audit rules for every type of device that DeviceLock supports.

- *Report USB White List* – check this flag to include information about white listed devices (see USB Devices White List).

- *Report Media White List* – check this flag to include information about white listed media (see Media White List).

- *Report Security Settings* – check this flag to report what parameters are disabled via Security Settings.

- *Report Auditing & Shadowing* – check this flag to report audit and shadowing rules that have been set.

  Also when this flag is checked, you receive information about whether the *Log Policy changes and Start/Stop events* parameter is enabled in Service Options.

- *Report Enabled Auditing & Shadowing Only* – check this flag to exclude devices for which audit and shadowing rules are disabled from the report.

  This flag is available only if *Report Auditing & Shadowing* is checked.

- *Report DeviceLock Administrators* – check this flag to report accounts that can manage DeviceLock Service or view its settings and logs.

This report always includes information about an installed DeviceLock Certificate. Also, it always shows when the *Use Group Policy* parameter is enabled in Service Options.

### 8.4.4 Report PnP Devices

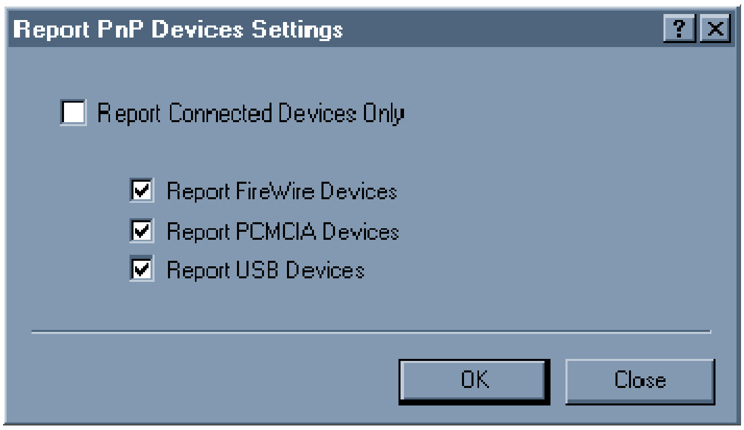
The *Report PnP Devices* plug-in generates a report displaying the USB, FireWire and PCMCIA devices currently connected to computers in the network and those that were connected.

The columns are defined as follows:

- *Description* – the description of the device provided by its vendor.
- *Device Information* – the additional information about the device provided by its vendor.
- *Connected to* – the interface where the device is connected (*USB*, *FireWire* or *PCMCIA*).
- *Class* – the class of the device provided by Windows.
- *Class description* – the description of the device's class provided by Windows.
- *Present* – indicates whether the device is currently connected or not (*Yes* or *No*).
- *DeviceID* – the unique identification string of the device provided by its vendor.
- *Driver* – the name of the driver that is controlling this device.

You can add reported USB devices to the USB Devices Database using the context menu available via a right mouse click.

Before you can use this plug-in, you should select the information you want to include in reports. You can do this by pressing the *Settings* button below the plug-ins list in the *Scan Network* dialog (see **Selecting Plug-ins**).



Report PnP Devices Settings

□ Report Connected Devices Only

☑ Report FireWire Devices

☑ Report PCMCIA Devices

☑ Report USB Devices

- *Report Connected Devices Only* – check this flag to report only those devices that are currently connected to the computer. Otherwise, you will see all devices that were ever connected to the computer.

- *Report FireWire Devices* – check this flag to report devices that are plugging into the FireWire port.

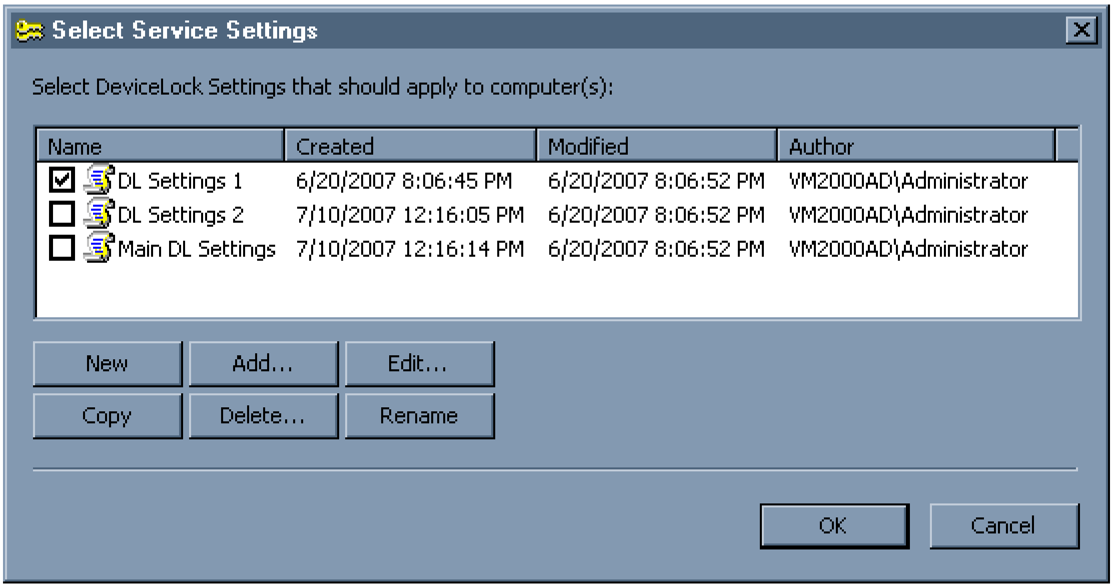
- *Report PCMCIA Devices* – check this flag to report devices that are plugging into the PCMCIA slot.

- *Report USB Devices* – check this flag to report devices that are plugging into the USB port.

### 8.4.5 Set Service Settings

The *Set Service Setting* plug-in reads the policy (settings, permissions, audit and shadowing rules) from the external XML file and deploys it to DeviceLock Services across the network.

Before you can use this plug-in, you should define settings, permissions and/or audit rules that you want to deploy. You can do this by pressing the *Settings* button below the plug-ins list in the *Scan Network* dialog (see **Selecting Plug-ins**).



Select DeviceLock Settings that should apply to computer(s):

| Name | Created | Modified | Author |
|---|---|---|---|
| ☑ DL Settings 1 | 6/20/2007 8:06:45 PM | 6/20/2007 8:06:52 PM | VM2000AD\Administrator |
| □ DL Settings 2 | 7/10/2007 12:16:05 PM | 6/20/2007 8:06:52 PM | VM2000AD\Administrator |
| □ Main DL Settings | 7/10/2007 12:16:14 PM | 6/20/2007 8:06:52 PM | VM2000AD\Administrator |

First of all you have to prepare the policy you want to deploy.

If there are no files in the list, then you can either create an empty file by pressing the *New* button or add an existing file by pressing the *Add* button.

Then highlight the file in the list and press the *Edit* button to open DeviceLock Service Settings Editor. DeviceLock Service Settings Editor is used for creating and modifying external XML files with settings, permissions, audit and shadowing rules for DeviceLock Service. For more information please read the **DeviceLock Service Settings Editor** section of this manual.

When finished modifying the policy, select its file by enabling the checkmark near by the file's name in the list. Then press the *OK* button to close the configuration dialog.

### 8.4.6 Shadow Log Viewer

The *Shadow Log Viewer* plug-in retrieves the shadow log from DeviceLock Service.

Use the context menu available by a right mouse click to access all this plug-in's functions.

For more information, please read the **Shadow Log Viewer (Service)** section of this manual.

### 8.4.7 Uninstall Service

The *Uninstall Service* plug-in removes DeviceLock Service and all its settings and components from computers.

If the user under which the DeviceLock Enterprise Manager is connecting to the computer doesn't have full administrative access to DeviceLock Service, the plug-in will not be able to remove the service.

Likewise, an error occurs when the user doesn't have local administrative privileges on the computer where DeviceLock Service is running.

## 8.5 Open / Save / Export

DeviceLock Enterprise Manager can store all information received from plug-ins.

The data is saved to external files and is ready for loading into DeviceLock Enterprise Manager when requested.

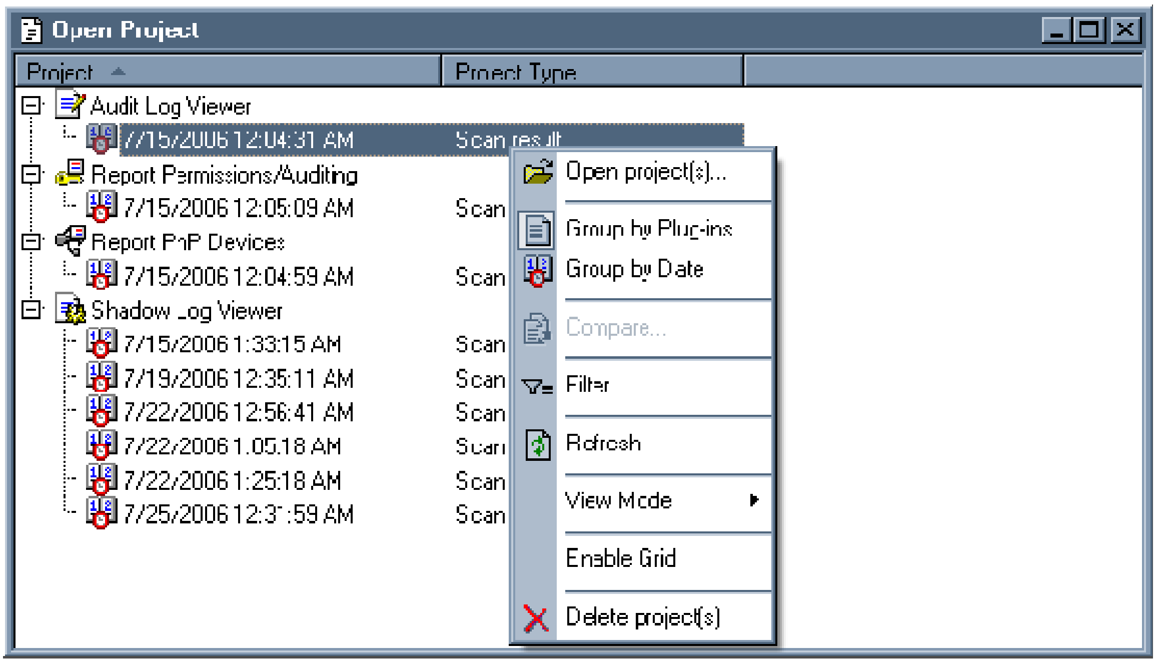
There are three ways to save and load data:

1. The handiest method to store received information is to save it as a project. When you are saving data as a project, DeviceLock Enterprise Manager saves each active plug-in's window to a separate file of its own format and places this file in the *Project* subdirectory.

   The names of the project's files are auto-generated and depend on the plug-in's names and the date and time when the scan was started.

   To save the data as a project, you can select *Save Project* from the *File* menu or press the appropriate button on the *Main* toolbar.

   To load previously saved projects, you can select *Open Project* from the *File* menu.



The *Open Project* window has its own toolbar and context menu available by a right mouse click.

You can group saved projects by the date when they were scanned and by the type of information they contain. Select *Group by Plug-ins* or *Group by Date* from the context menu or press appropriate buttons on the *Project* toolbar.

To open a saved project, select it from the list and press the *Open Project* button on the *Project* toolbar. Using *Ctrl* and/or *Shift* you can select and open several projects simultaneously.

2. Another way to save received information in the format of DeviceLock Enterprise Manager is select *Save As* from the *File* menu. This enables you to save a file of the *ANM* type to any place on your hard disk or any other media with any name you choose.

   To load previously saved files, you can select *Open* from the *File* menu or press the appropriate button on the *Main* toolbar. You will need to specify a file you wish to open. You can load files of the *ANM* type only.

3. If you need to pass received information to a third-party application, you can export it into an external file and then import it to this application. To export data into the external file, select *Save As* from the *File* menu and then select the file's type from the *Save as type* combo box. DeviceLock Enterprise Manager supports the export into MS Excel (if it's installed on the local computer) and two formats of text files – Tab Delimited (TXT) and Comma Delimited (CSV).

   If you export information into an external file, you will not be able to load it back to DeviceLock Enterprise Manager because DeviceLock Enterprise Manager can open and load only files of its own format. However, the ability to export into an external file is useful when you wish to exchange data between DeviceLock Enterprise Manager and other applications.

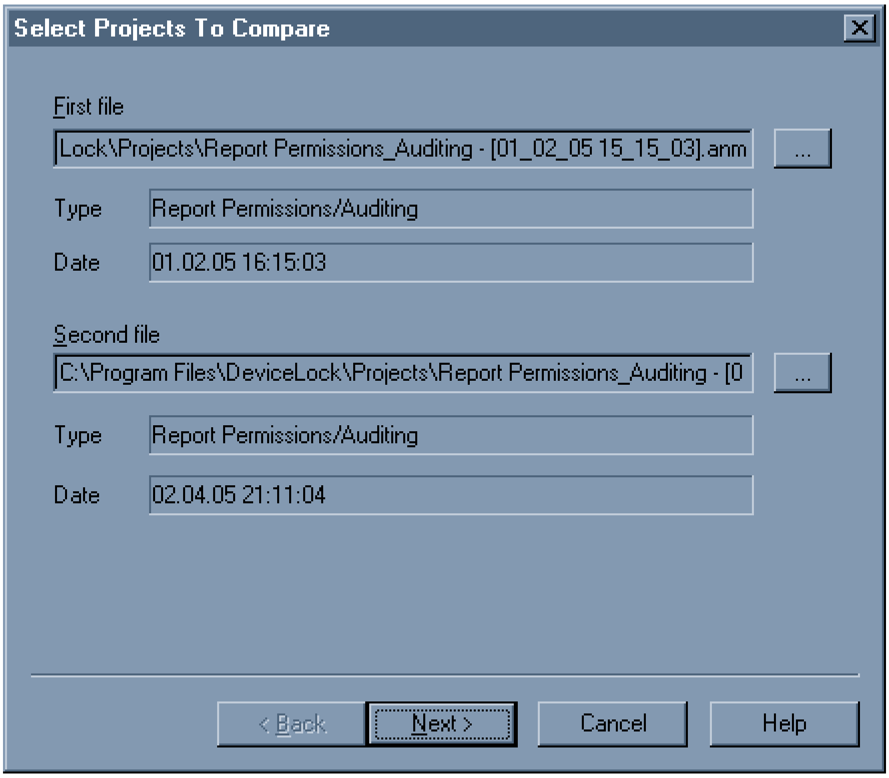
## 8.6 Comparing Data

DeviceLock Enterprise Manager allows you to track changes on network computers by comparing two previously saved projects. Tracking changes is important when managing a wide range of computers in one network.

DeviceLock Enterprise Manager provides a very useful and intuitive Wizard to compare two *ANM* files. To open this Wizard, select *Compare* from the *File* menu.

There are three simple steps, which enable you to compare two files using *Compare Wizard*:

1. The first step is to select the files you wish to compare.



First file: Lock\Projects\Report Permissions_Auditing - [01_02_05 15_15_03].anm

Type: Report Permissions/Auditing

Date: 01.02.05 16:15:03

Second file: C:\Program Files\DeviceLock\Projects\Report Permissions_Auditing - [0

Type: Report Permissions/Auditing

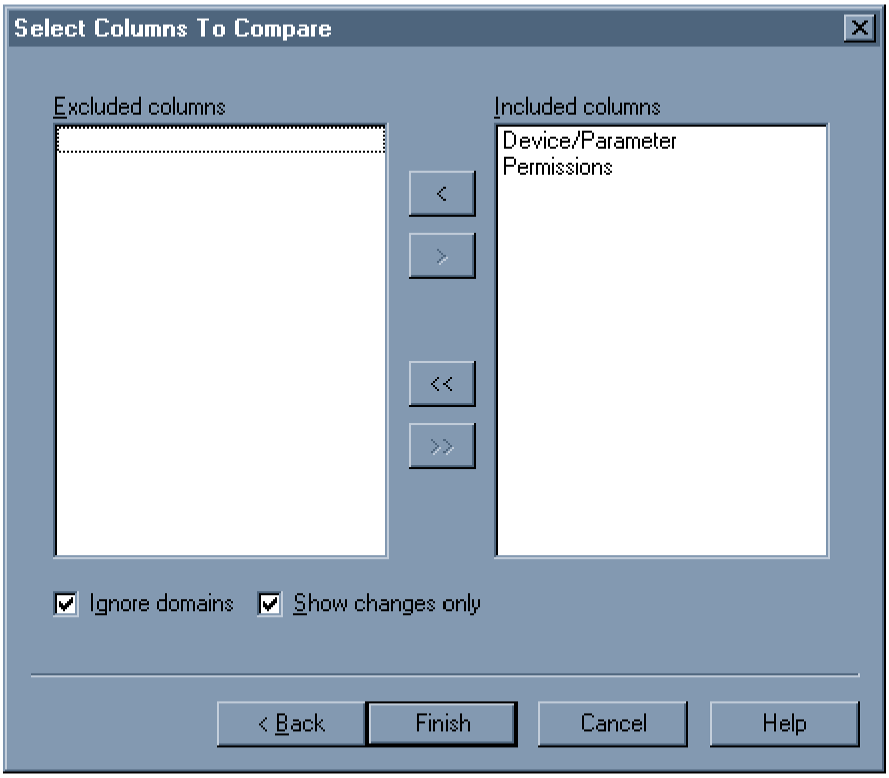
Date: 02.04.05 21:11:04

Select the first file and then select the second file by pressing **...** buttons.

Please note that you can compare files of the same type only. For example, you cannot compare information received from the *Report Permissions/Auditing* plug-in with information from the *Report PnP Devices* plug-in.

When you have selected two files, press the *Next* button to go to the Wizard's next page.

2. The second step is to select the columns you wish to include in the compare process.



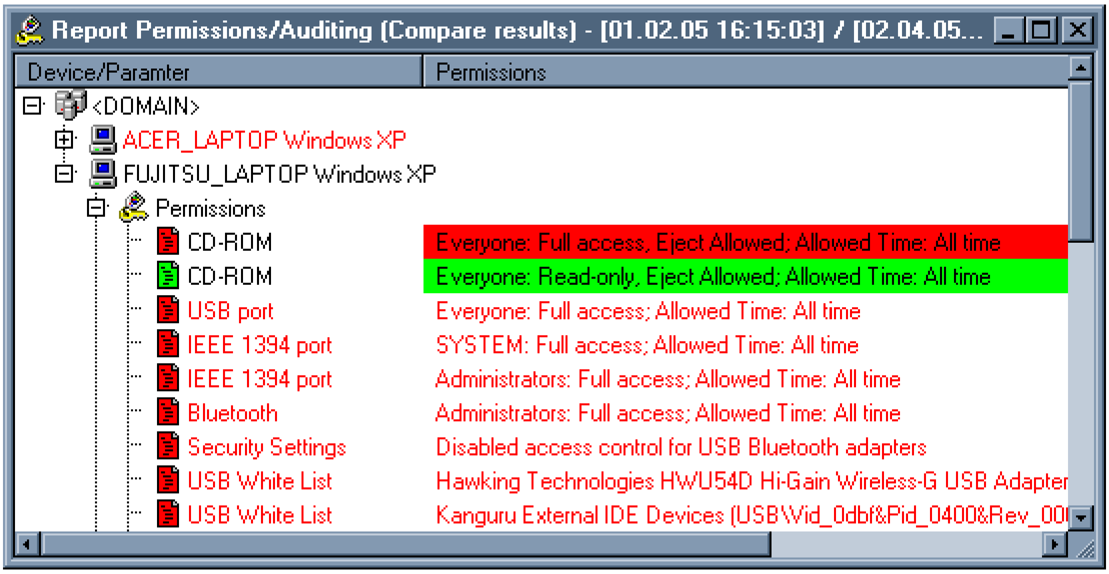
DeviceLock Enterprise Manager compares only those columns, which you have selected. If you need to exclude one column from the compare process, you have to move it from the *Included columns* list to the *Excluded columns* list. Excluded columns will be visible in the compare result, but the values they contain are ignored and don't affect the compare result.

By default, the compare result contains only records, which are different in the two files being compared. If you would like to see all of the records (even unchanged records), you can clear the *Show changes only* flag.

To include names of the network domains in the compare process, you can clear the *Ignore domains* flag. When the *Ignore domains* flag is checked, DeviceLock Enterprise Manager ignores domains and only compares computers and the information those computers contain.

3. The third and final step is to start the compare process. Press the *Finish* button to compare two selected files with each other.

DeviceLock Enterprise Manager displays the compare result in a separate window in the form of a tree exactly as it displays information received from a plug-in.



Report Permissions/Auditing (Compare results) - [01.02.05 16:15:03] / [02.04.05...

| Device/Paramter | Permissions |
|---|---|
| <DOMAIN> | |
| ACER_LAPTOP Windows XP | |
| FUJITSU_LAPTOP Windows XP | |
| Permissions | |
| CD-ROM | Everyone: Full access, Eject Allowed; Allowed Time: All time |
| CD-ROM | Everyone: Read-only, Eject Allowed; Allowed Time: All time |
| USB port | Everyone: Full access; Allowed Time: All time |
| IEEE 1394 port | SYSTEM: Full access; Allowed Time: All time |
| IEEE 1394 port | Administrators: Full access; Allowed Time: All time |
| Bluetooth | Administrators: Full access; Allowed Time: All time |
| Security Settings | Disabled access control for USB Bluetooth adapters |
| USB White List | Hawking Technologies HWU54D Hi-Gain Wireless-G USB Adapter |
| USB White List | Kanguru External IDE Devices (USB\Vid_0dbf&Pid_0400&Rev_00 |

The comparison is very simple and effective:

1. If the *Ignore domains* flag is cleared, the program enumerates network domains in the two selected files and tries to find each domain in both the older file and the recent file.

   If the domain exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing domain (along with all the computers contained in that domain as well as the information in those computers) into the comparison result and then writes all those records in red.

   If the domain does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing domain (along with all the computers contained in that domain as well as the information in those computers) into the comparison result and then writes all those records in green.

   If the domain exists in both files, DeviceLock Enterprise Manager enumerates all the computers the domain contains (see below).

2. If the *Ignore domains* flag is checked, DeviceLock Enterprise Manager ignores domains and enumerates all the computers in the two selected files and tries to find each computer in both older and recent files.

   If the computer exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing computer with all information it contains into the compare result and writes all these records in red.

   If the computer does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing computer with all information it contains into the compare result and writes all these records in green.

   If the computer exists in both files, DeviceLock Enterprise Manager enumerates all the information it contains (see below).

3. DeviceLock Enterprise Manager enumerates all information for a computer and tries to find each record in both the older and the recent file.

   If the record exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing record into the compare result and writes it in red.

   If the record does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing record into the compare result and writes it in green.

   If the record exists in both files, DeviceLock Enterprise Manager starts comparing each included column for this record:

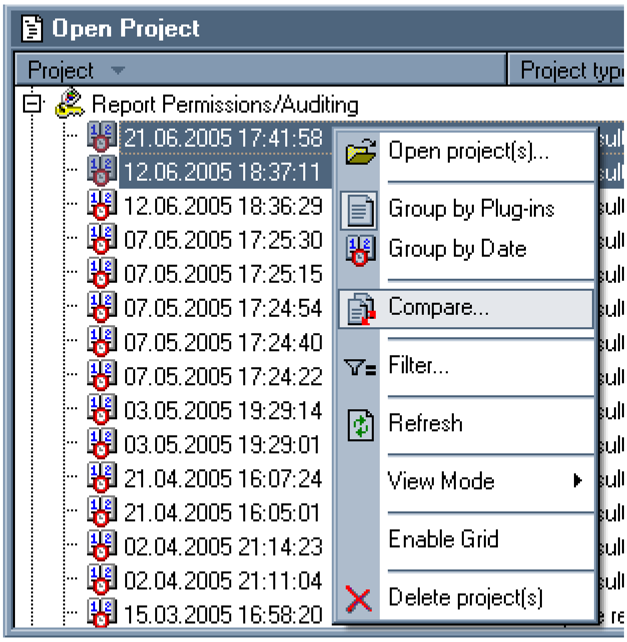
   - If the column's values for the older and the recent files are different, DeviceLock Enterprise Manager inserts both records in the compare result. The record from the recent file comes right after the record from the older one.

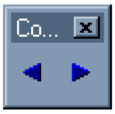
     The column that belongs to an older record is highlighted in red. The column that belongs to a recent record is highlighted in green. All excluded columns and columns with equal values are not highlighted and are written in the default color.

   - If all of a record's columns for both files contain equal values, DeviceLock Enterprise Manager either skips this record (the *Show changes only* flag is checked) or inserts this record into the compare result and writes it in the default color (the *Show changes only* flag is cleared).

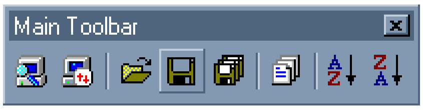
If you wish to compare two files, which were saved as projects, it is a good idea to use the special feature of the *Open Project* window.

Select *Open Project* from the *File* menu, highlight two projects you would like to compare (use *Ctrl* and/or *Shift* to highlight two projects simultaneously) and then select *Compare* from the context menu or press the appropriate button on the *Project* toolbar. ***Please note that you may select only two projects and both projects must be of the same type.***



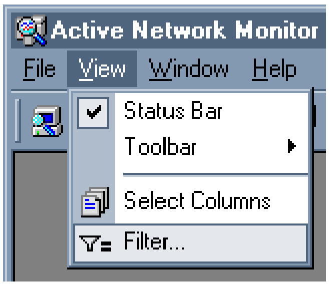


DeviceLock Enterprise Manager provides two buttons on the *Compare* toolbar, which help you to easily navigate through the compare result. Press the **<** button to highlight the previous record in the compare result that contains changes. Press the **>** button to highlight the next record in the compare result that contains changes.



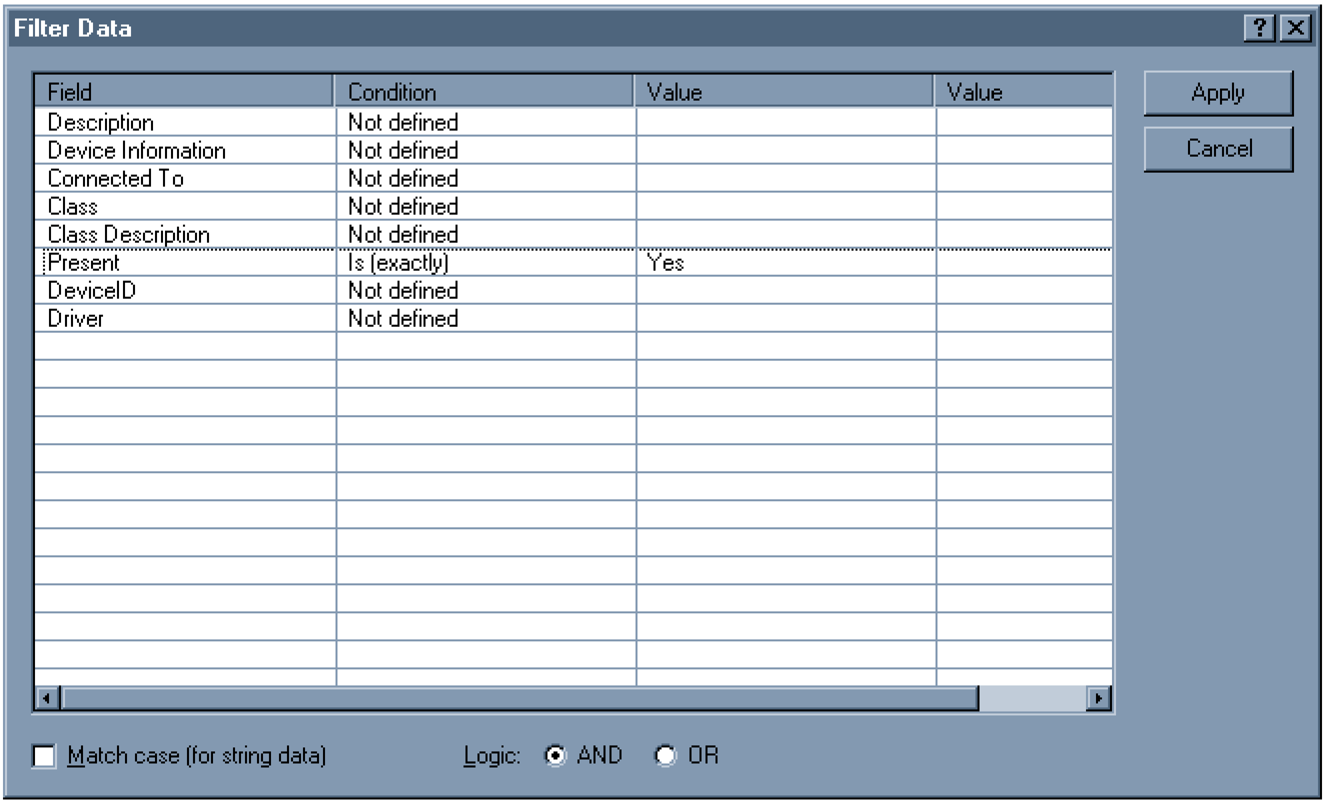
You can also save the compare result to an external *ANM* file or export it into MS Excel or the text file (TXT and CSV). Select *Save As* from the *File* menu or press the appropriate button on the *Main* toolbar to save or export the compare result. As with any other DeviceLock Enterprise Manager file, the saved compare result can be opened and loaded to DeviceLock Enterprise Manager. To load the previously saved compare result, you can select *Open* from the *File* menu or press the appropriate button on the *Main* toolbar. You will need to specify a file you wish to open. You can load files of *ANM* type only.

## 8.7 Filtering Data



DeviceLock Enterprise Manager provides very sophisticated data filtering, enabling you to narrow a scan or comparison result to only those data complying to your specific conditions.

To open the *Filter Data* dialog, you can select *Filter* from the *View* menu or press the appropriate button on the *Main* toolbar. ***Please note that the window with a scan or comparison result must be active to use data filtering.***



| Field | Condition | Value | Value |
|---|---|---|---|
| Description | Not defined | | |
| Device Information | Not defined | | |
| Connected To | Not defined | | |
| Class | Not defined | | |
| Class Description | Not defined | | |
| Present | Is (exactly) | Yes | |
| DeviceID | Not defined | | |
| Driver | Not defined | | |

□ Match case (for string data)    Logic: ● AND ○ OR

- The *Field* column contains all the fields available in the scan or comparison result that you want to filter. You can define the *AND-OR* logic for each field separately:

  *AND* – includes only those records that comply with all defined conditions. For example, *Process = “explorer.exe” AND PID = 3764* retrieves all data where both the *Process* is “*explorer.exe*” and *PID* is *3764*. It does not include data where the *Process* is “*explorer.exe*” and *PID* is not *3764* or where *PID* is *3764* but *Process* is not “*explorer.exe*”.

  *OR* – includes all records that comply with at least one condition. For example, *Process = “explorer.exe” OR PID = 3764* retrieves all data having one or both conditions, where Process = “*explorer.exe*” (no matter what *PID* is) or where *PID* is *3764* (no matter what *Process* is).

- The *Condition* column contains a list of logical operations that can be performed on a selected field. You can select only one logical operation for each field. DeviceLock Enterprise Manager supports two groups of logical operations, those for *string data* and *non-string data*.

  Logical operations that can be performed on *string data* (*target string* being the string you specify, e.g. “*Explorer.exe*”):

  - *Is (exactly)* – selects only data having fields with strings that are identical to the target string.

  - *Includes* – selects only data having fields with strings that include a defined target string.

  - *Is not* – selects only data having fields with strings that are different from the target string.

  - *Not includes* – selects only data having fields with strings that do not include the target string.

  - *Empty* – selects only data having fields with empty strings.

  - *Not Empty* – selects only data having fields with strings that are not empty.

  - *Regular expression* – selects only data having fields with strings matching an expression. The expression may contain wildcards (e.g. “*explorer**”).

  If you want to narrow the search to the string's exact case (e.g. "*Explorer.exe*" is different from "e*xplorer.exe*"), check the *Match case* flag. Otherwise, case is ignored (e.g. "*Explorer.exe*" and "*explorer.exe*" are identical).

  Logical operations that can be performed on *non-string data*:

  - *Equal to (=)* – selects data having field values that are identical to the defined value (e.g. *PID = 3764*).

- *Greater than (>)* – selects data having field values that are greater than the defined value (e.g. *PID > 4*).

- *Less than (<)* – selects data having field values that are less than the defined value (e.g. *PID < 4*).

- *Not Equal to (!=)* – selects data having field values that are different from the defined value (e.g. *PID != 0*).

- *Between (in)* – selects data having field values that are between the two defined values (e.g. *PID in 3000-4000*).

- *Not Between (out)* – selects data having field values that are outside of the two defined values (e.g. *PID out 3000-4000*).

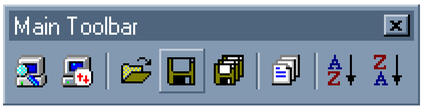
- *Regular expression* – selects only data having field values matching an expression. The expression may contain wildcards (e.g. *300**).

If you don't want to perform a logical operation for a field, select *Not defined* from the list of logical operations.

- *Value* columns contain user-defined arguments. The second *Value* column is used only when the *Between (in)* or *Not Between (out)* logical operation is selected. For all other logical operations only the first *Value* column is needed.

After you define a filtering expression, press the *Apply* button to start the filtering process.

You can save a filtered result in an external *ANM* file or export it to a text file (TXT and CSV) or MS Excel. Select *Save As* in the *File* menu or press the appropriate button on the *Main* toolbar to save or export the filtered result.

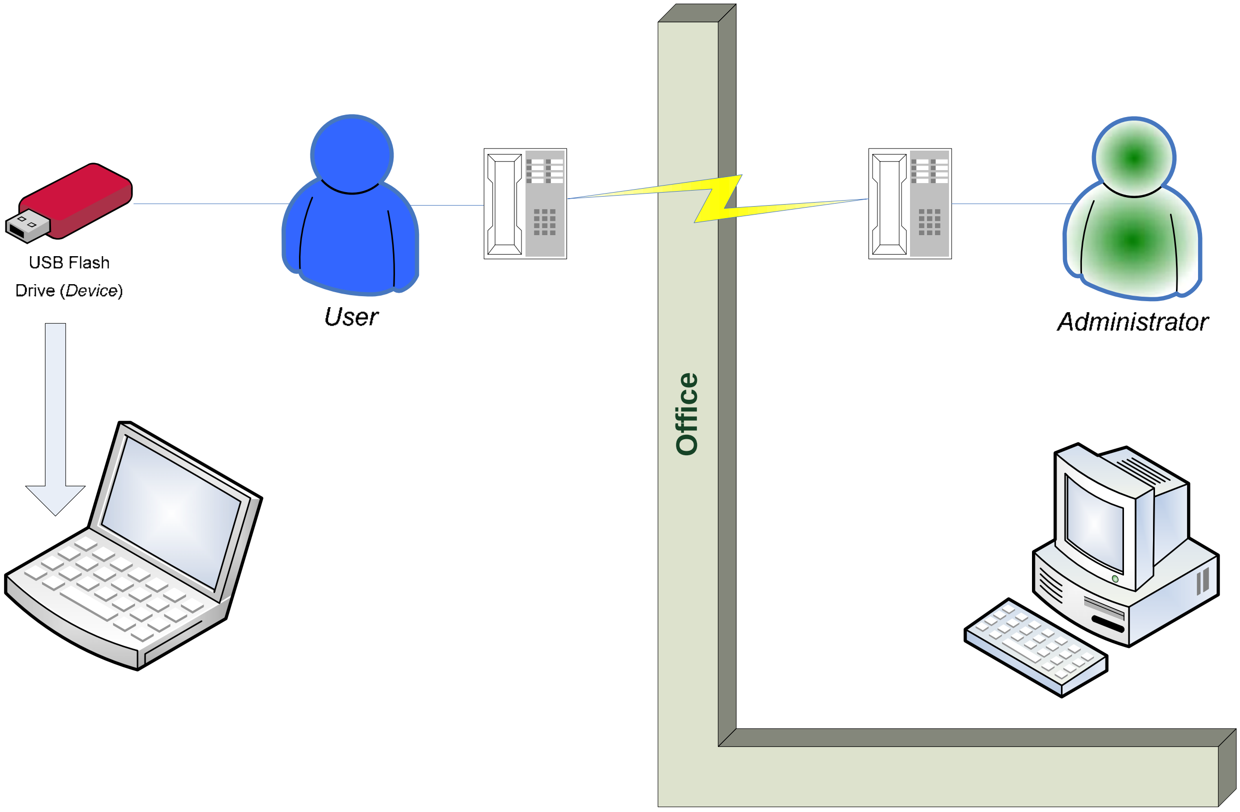


As with any other DeviceLock Enterprise Manager file, filtered data can be opened and loaded into DeviceLock Enterprise Manager. To load a file, select *Open* in the *File* menu or press the appropriate button on the *Main* toolbar. Then specify the file you wish to open. You can only load files that were previously saved by DeviceLock Enterprise Manager.

# 9 Temporary White List

## 9.1 Overview

The DeviceLock Temporary White List function enables the granting of temporary access to USB devices when there is no network connection. Administrators provide users with special access codes over the phone that temporarily unlock access to requested devices.



A Temporary White List works like a device white list, with the distinction that a network connection is not required to add devices and grant access to them.

***NOTE: Using Temporary White List it is possible to grant access to USB devices that were blocked on both levels: the USB port level and the type level. If some white listed device (e.g. USB Flash Drive) belongs to both levels: USB and type (Removable), the permissions (if any) for the type level are ignored as well as for the USB level.***

Creating and activating a Temporary White List is a matter of following these step-by-step instructions:

1. The administrator generates a cryptographic certificate (DeviceLock Certificate) using the Certificate Generation Tool. A DeviceLock Certificate consists of two keys: *private* and *public*.

2. The administrator deploys the DeviceLock Certificate (the *public* key) to a user's computer. This enables the Temporary White List on the user's computer.

3. When a user needs to access some USB device, he/she runs the Temporary White List Authorization Tool from the Windows *Control Panel*. Then the user selects the particular device from a list and a textual-numeric code (**Device Code**) is generated. The user can then provide this code to the DeviceLock Administrator over the phone or via an Internet chat session.

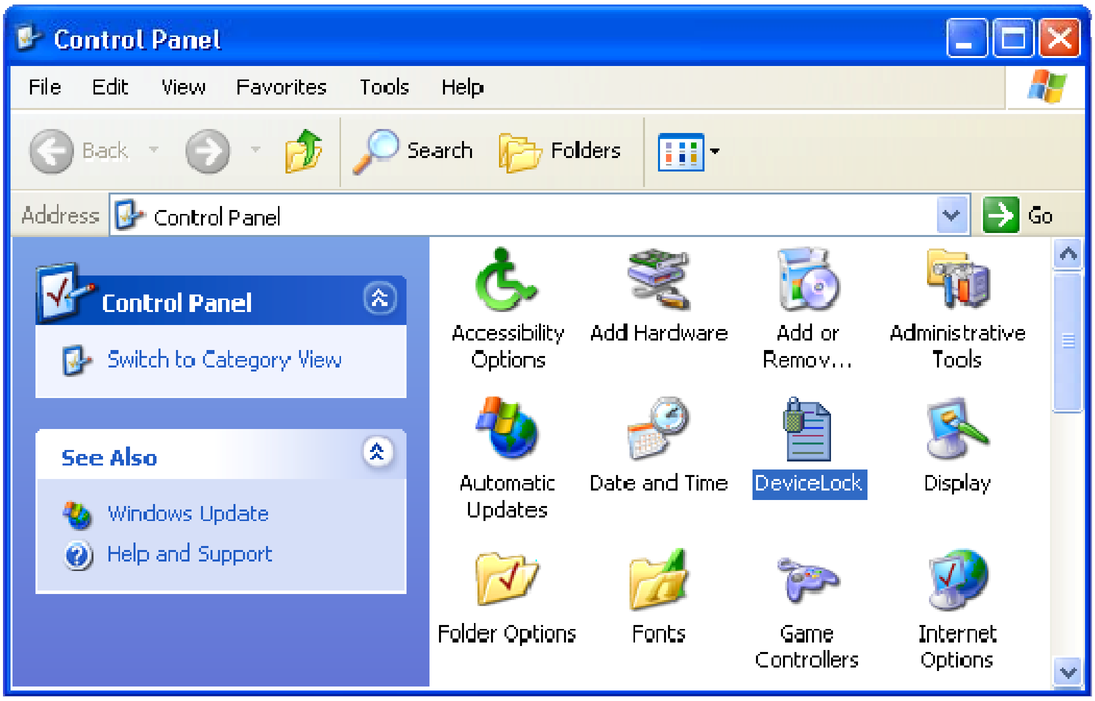
4. The administrator then runs the DeviceLock Signing Tool, loads the corresponding DeviceLock Certificate (the *private* key), enters the **Device Code**, selects an appropriate temporary access period (5, 15, etc. minutes or until the device is unplugged), generates an **Unlock Code**, and relays this **Unlock Code** to the user.

5. Upon receipt of the **Unlock Code**, the user enters it into Temporary White List Authorization Tool. Access to the requested device is then granted for the specified period.

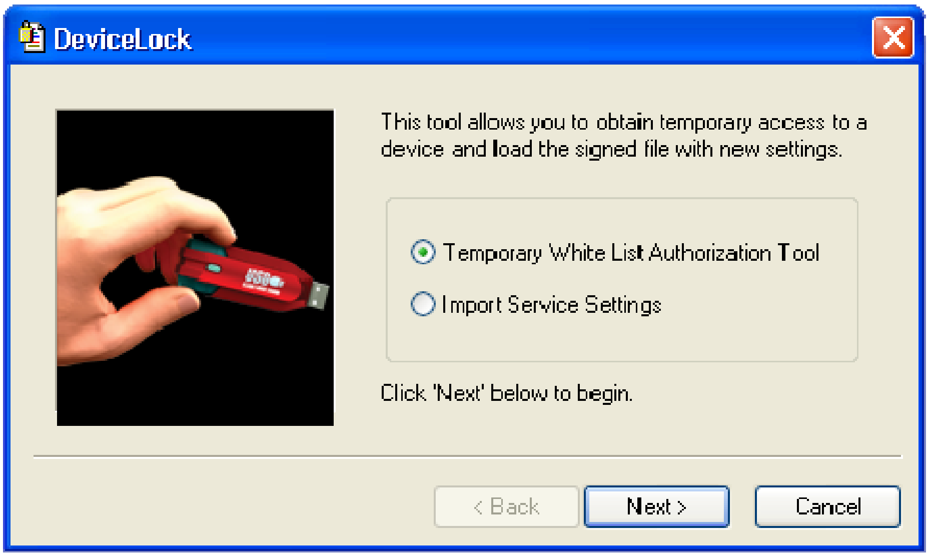
## 9.2 Temporary White List Authorization Tool

The Temporary White List Authorization Tool is a part of the Windows *Control Panel* applet that users should use to obtain temporary access to devices.

To run the Temporary White List Authorization Tool, the user should run the *DeviceLock* applet from the *Control Panel* and select the *Temporary White List Authorization Tool* option.



***NOTE: On Windows XP and later, the user must switch the Control Panel to Classic View in order to view all available applets.***


This tool allows you to obtain temporary access to a device and load the signed file with new settings.

● Temporary White List Authorization Tool

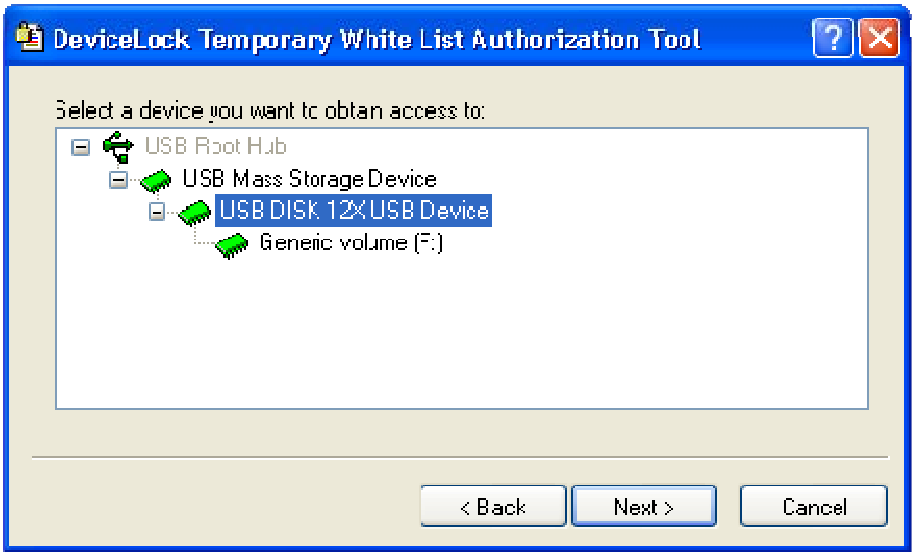
○ Import Service Settings

Click 'Next' below to begin.

There are five simple steps for the user to request and obtain temporary access to a device:

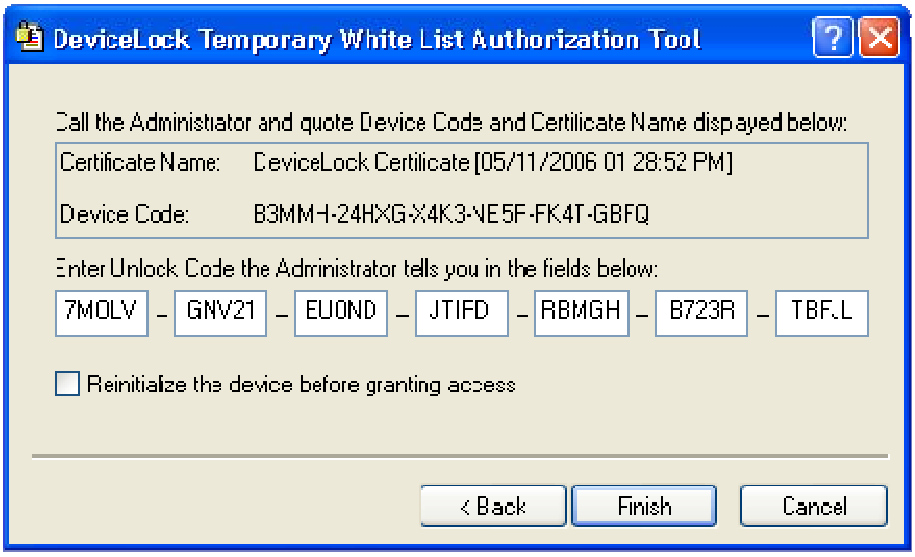
1. Plug the needed device into the USB port.

2. Select the device from the list of all available USB devices.


Select a device you want to obtain access to:

```
⊟ USB Root Hub
   ⊟ USB Mass Storage Device
      ⊟ USB DISK 12X USB Device
           Generic volume (F:)
```

3. Contact an Administrator and tell him/her the name of the certificate and the **Device Code**. Please note that the **Device Code** is only valid within 24 hours of the time it was generated by the applet.



Call the Administrator and quote Device Code and Certificate Name displayed below:

Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]

Device Code: B3MMH-24HXG-X4K3-NE5F-FK4T-GBFQ

Enter Unlock Code the Administrator tells you in the fields below:

7MOLV - GNV21 - EUOND - JTIFD - RBMGH - B723R - TBFJL

☐ Reinitialize the device before granting access

4. Enter an **Unlock Code** received from the Administrator.

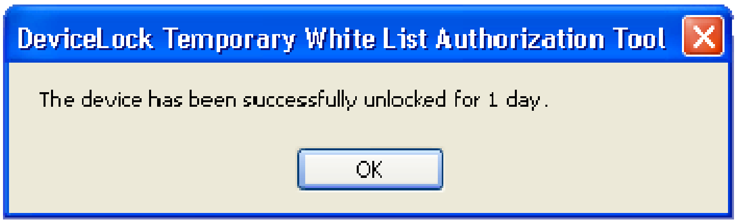
   If it is necessary to force the requested device to reinitialize (replug) before allowing access to it, select *Reinitialize device before granting access*.

   Some USB devices (like the mouse) won't work without being reinitialized, so it is recommended to keep this flag checked for non-storage devices.

   It is recommended to keep the *Reinitialize device before granting access* flag unchecked for storage devices (such as flash drives, CD/DVD-ROMs, external hard drives and so on).

   Some USB devices can't be reinitialized from DeviceLock Service. It means that their drivers do not support the software replug. If such a device was white listed but doesn't work, the user should remove it from the port and then insert it back manually to restart the device's driver.

5. Press the *Finish* button. If the **Unlock Code** is valid, then access to the device will be provided in several seconds.



The device has been successfully unlocked for 1 day.

All successfully attempts to add devices to a Temporary White List are logged, if logging of changes is enabled in the Service Options.

# 10 Appendix

## 10.1 Permissions and Audit Examples

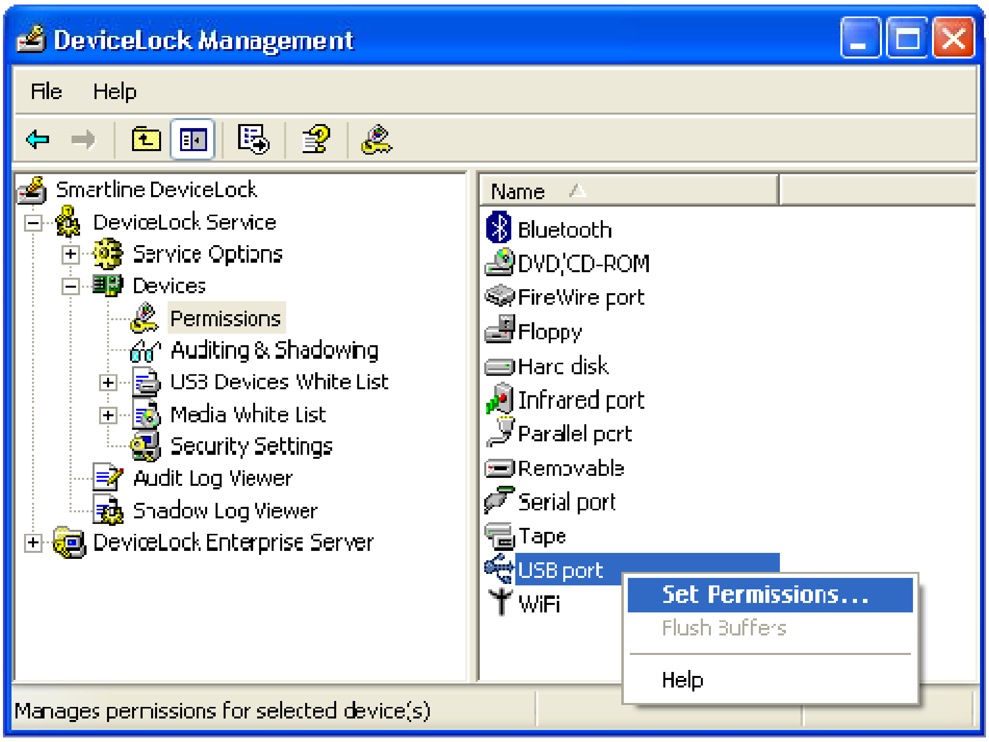
Using these following examples you can better understand how to properly define permissions, audit and shadowing rules in DeviceLock.

All examples assume that you are using DeviceLock Management Console (the MMC snap-in) and it is already connected to the computer where DeviceLock Service is running. For more information on how to use DeviceLock Management Console, please read the **DeviceLock Management Console** section of this manual.

### 10.1.1 Permissions Examples

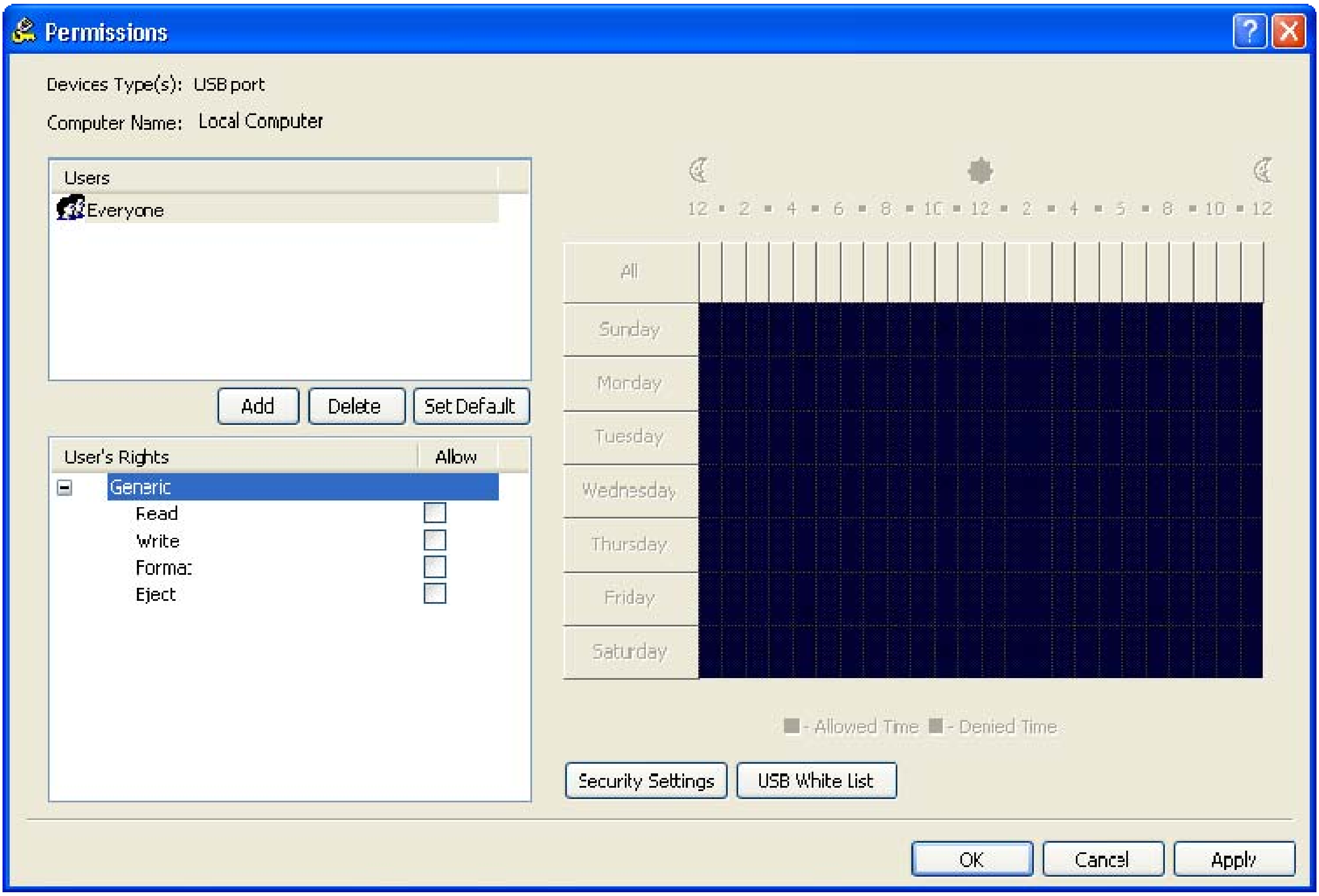
- **For all users all USB devices are denied except the mouse and keyboard:**

1. Select the *USB port* record from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.



Manages permissions for selected device(s)

2. Click the *Add* button on the *Permissions* dialog, add the *Everyone* user (type the name or browse for all available names and select the needed one), click *OK* to close the *Select Users or Groups* dialog, highlight the *Everyone* record and disable all rights in the *User's Rights* list.



Devices Type(s): USB port

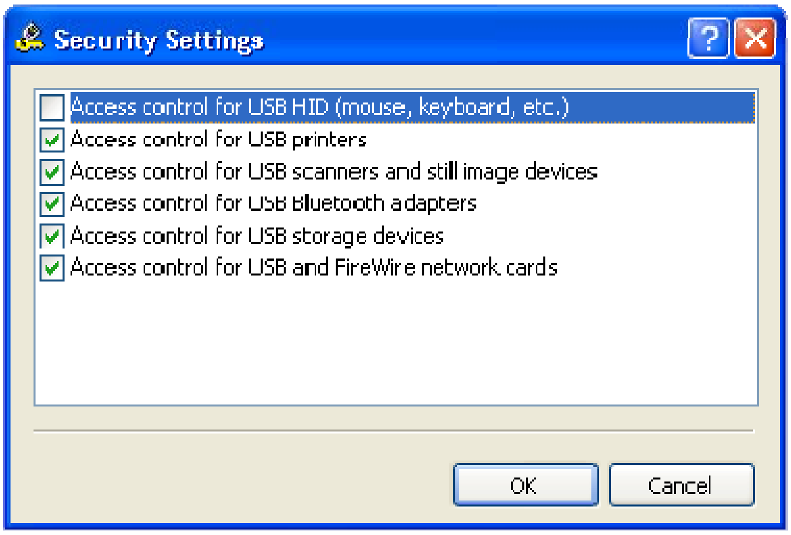
Computer Name: Local Computer

Users

Everyone

| User's Rights | Allow |
|---|---|
| Generic | |
| Read | □ |
| Write | □ |
| Format | □ |
| Eject | □ |

3. Click the *Security Settings* button on the *Permissions* dialog, and then uncheck *Access control for USB HID (mouse, keyboard, etc.)* as shown on the picture below.



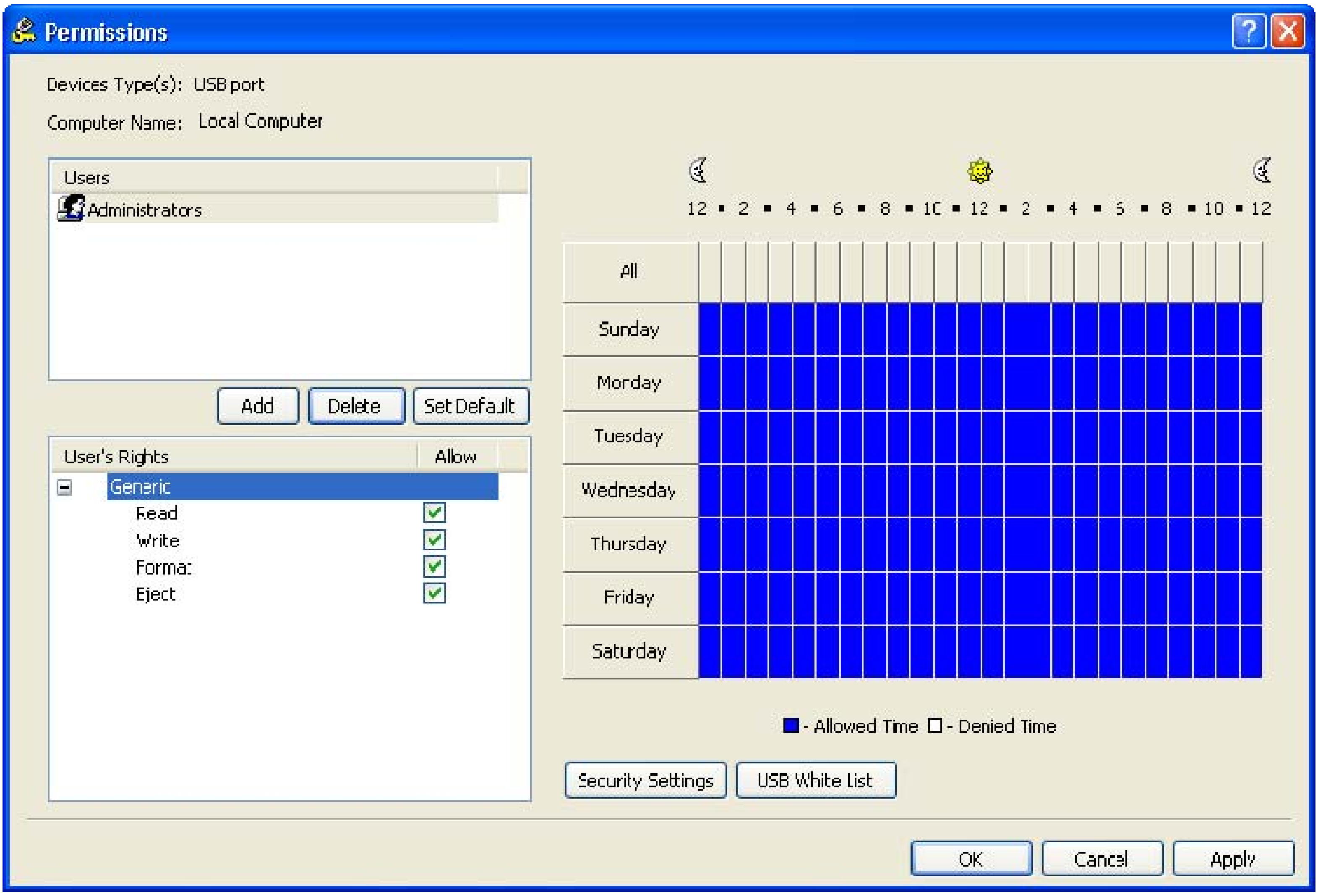
- □ Access control for USB HID (mouse, keyboard, etc.)
- ☑ Access control for USB printers
- ☑ Access control for USB scanners and still image devices
- ☑ Access control for USB Bluetooth adapters
- ☑ Access control for USB storage devices
- ☑ Access control for USB and FireWire network cards

4. Click *OK* to close the *Security Settings* dialog, click *OK* to apply changes and close the *Permissions* dialog, and then click *Yes* to confirm that you really want to deny all users access to the USB port.

- **For all users all USB devices are denied except the mouse and keyboard but members of the *Administrators* group can use all USB devices:**

1. Select the *USB port* record from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.

2. Click the *Add* button on the *Permissions* dialog, add the *Administrators* group (type the name or browse for all available names and select the needed one), click *OK* to close the *Select Users or Groups* dialog, highlight the *Administrator*s record and enable all rights in the *User's Rights* list.



Permissions

Devices Type(s): USB port

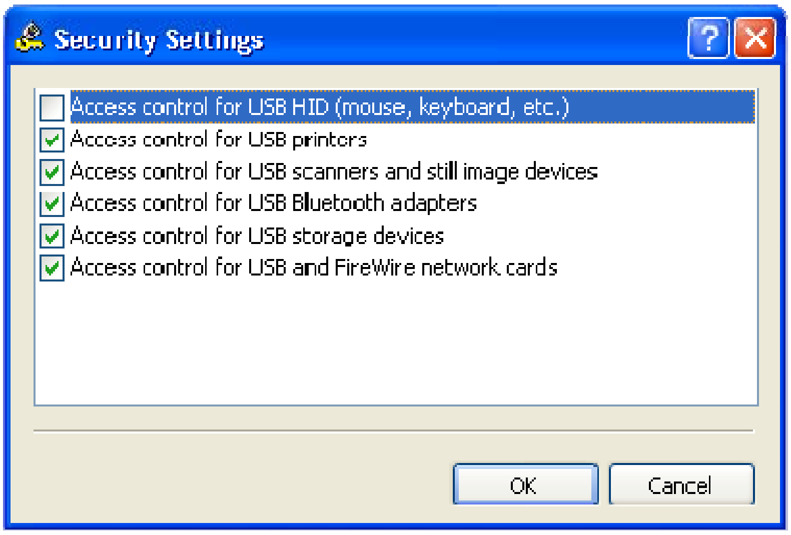
Computer Name: Local Computer

Users

Administrators

| User's Rights | Allow |
|---|---|
| ⊟ Generic | |
| Read | ☑ |
| Write | ☑ |
| Format | ☑ |
| Eject | ☑ |

3. Click the *Security Settings* button on the *Permissions* dialog, and then uncheck *Access control for USB HID (mouse, keyboard, etc.)* as shown on the picture below.



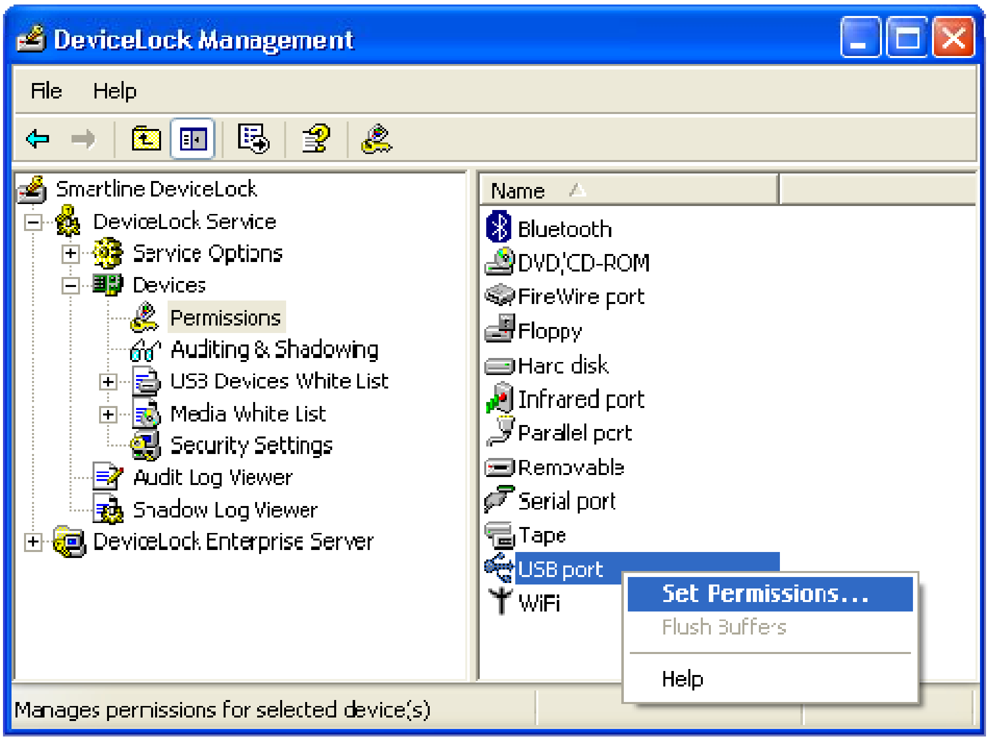
Security Settings

□ Access control for USB HID (mouse, keyboard, etc.)
☑ Access control for USB printers
☑ Access control for USB scanners and still image devices
☑ Access control for USB Bluetooth adapters
☑ Access control for USB storage devices
☑ Access control for USB and FireWire network cards

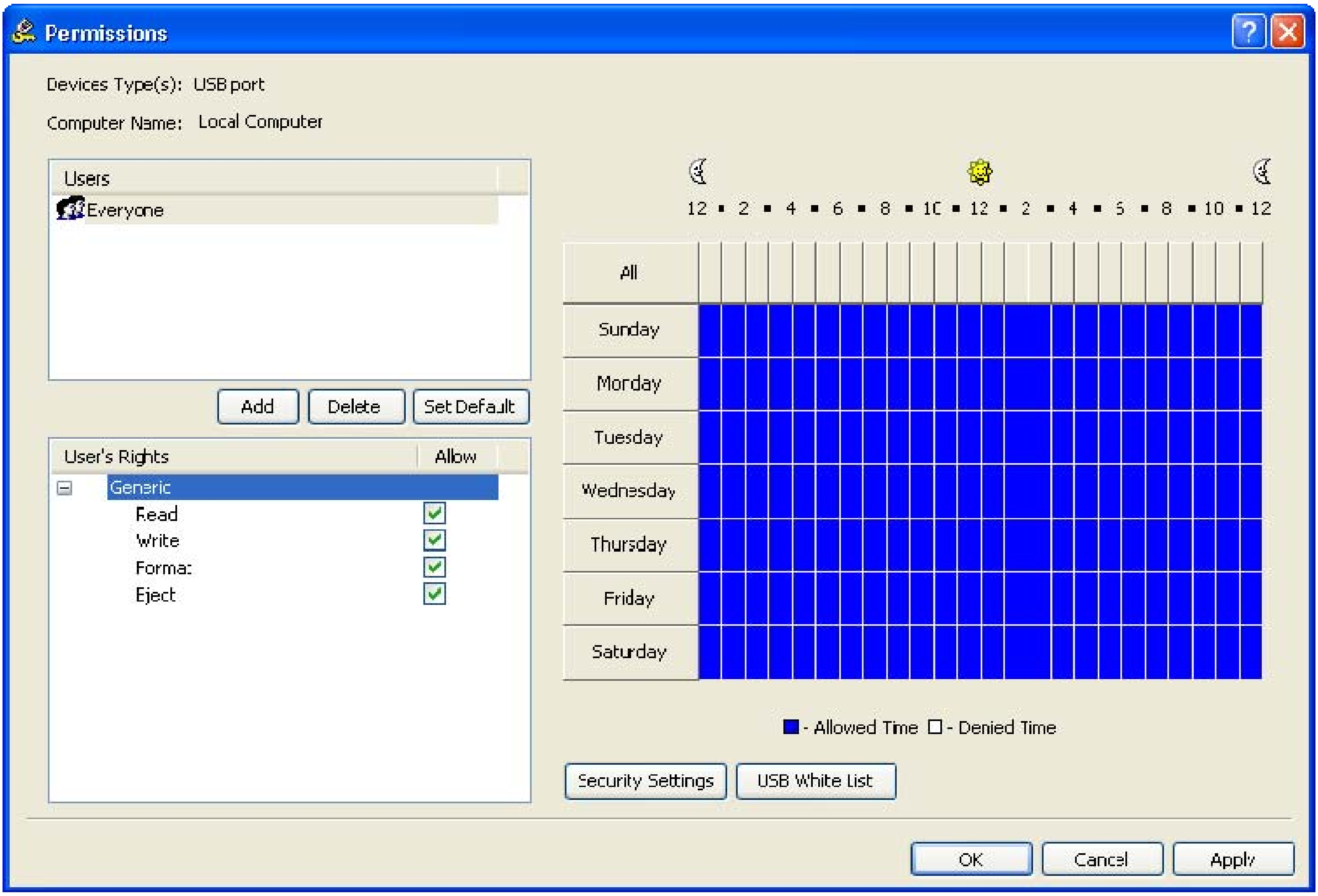
4. Click *OK* to close the *Security Settings* dialog, and then click *OK* to apply changes and close the *Permissions* dialog.

- **For all users all storage devices except fixed hard drives are denied but all non-storage USB devices are allowed:**

1. Select the *USB port* record from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.



2. Click the *Add* button on the *Permissions* dialog, add the *Everyone* user (type the name or browse for all available names and select the needed one), click *OK* to close the *Select Users or Groups* dialog, highlight the *Everyone* record and enable all rights in the *User's Rights* list.



Permissions

Devices Type(s): USB port

Computer Name: Local Computer

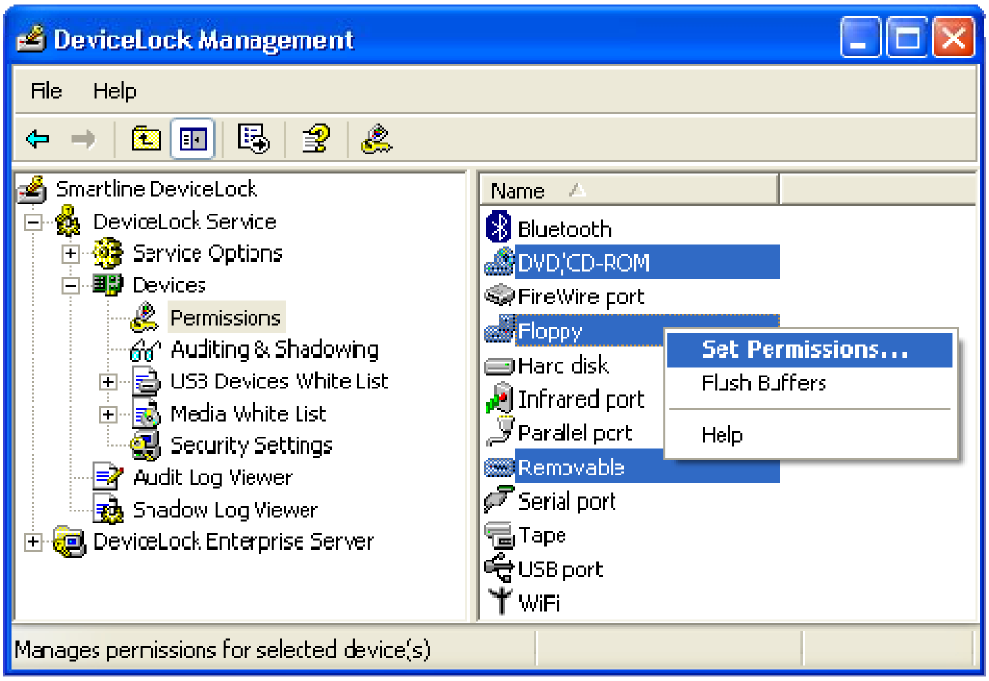
Users

Everyone

| User's Rights | Allow |
|---|---|
| ⊟ Generic | |
| Read | ☑ |
| Write | ☑ |
| Format | ☑ |
| Eject | ☑ |

3. Click *OK* to apply changes and close the *Permissions* dialog.

4. Select *DVD/CD-ROM*, *Floppy* and *Removable* records from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.



DeviceLock Management

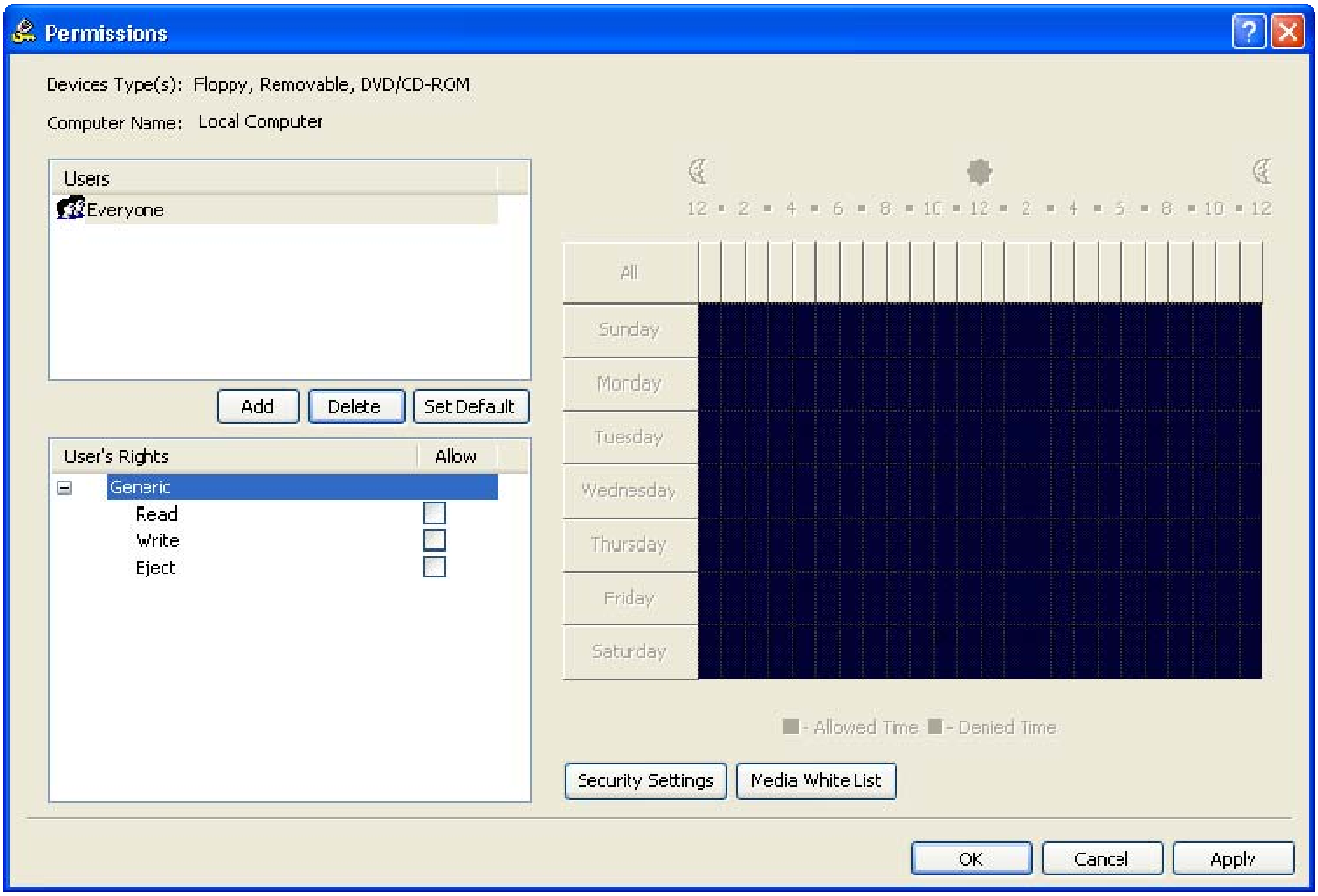
- Smartline DeviceLock
  - DeviceLock Service
    - Service Options
    - Devices
      - Permissions
      - Auditing & Shadowing
      - USB Devices White List
      - Media White List
      - Security Settings
    - Audit Log Viewer
    - Shadow Log Viewer
  - DeviceLock Enterprise Server

Name

- Bluetooth
- DVD/CD-ROM
- FireWire port
- Floppy
- Hard disk
- Infrared port
- Parallel port
- Removable
- Serial port
- Tape
- USB port
- WiFi

Manages permissions for selected device(s)

5. Click the *Add* button on the *Permissions* dialog, add the *Everyone* user (type the name or browse for all available names and select the needed one), click *OK* to close the *Select Users or Groups* dialog, highlight the *Everyone* record and disable all rights in the *User's Rights* list.



Permissions

Devices Type(s): Floppy, Removable, DVD/CD-ROM

Computer Name: Local Computer

Users: Everyone

| User's Rights | Allow |
|---|---|
| Generic | |
| Read | ☐ |
| Write | ☐ |
| Eject | ☐ |

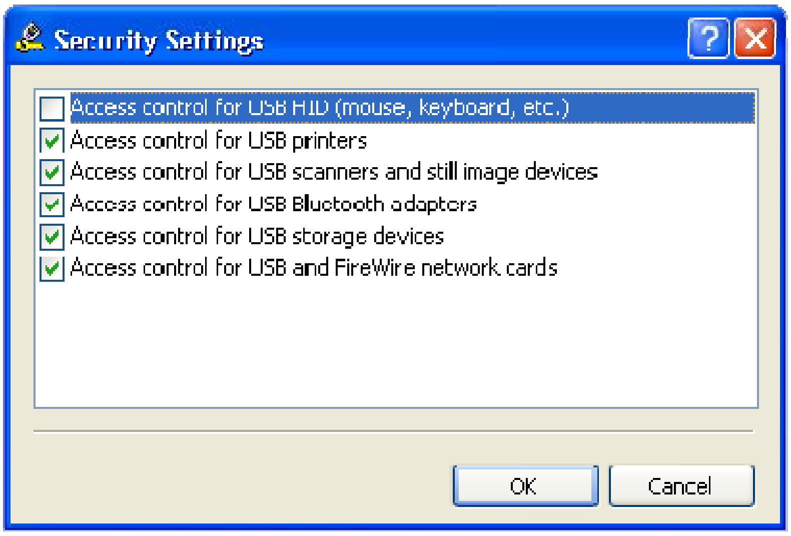
6. Click *OK* to apply changes and close the *Permissions* dialog, and then click *Yes* to confirm that you really want to deny access to these devices for all users.

- **For all users all USB devices are denied except the mouse and keyboard but members of the *Administrators* group can use an authorized model of USB storage devices:**

1. Select the *USB port* record from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.

2. Click the *Add* button on the *Permissions* dialog and add the *Everyone* user (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, highlight the *Everyone* record and disable all rights in the *User's Rights* list.

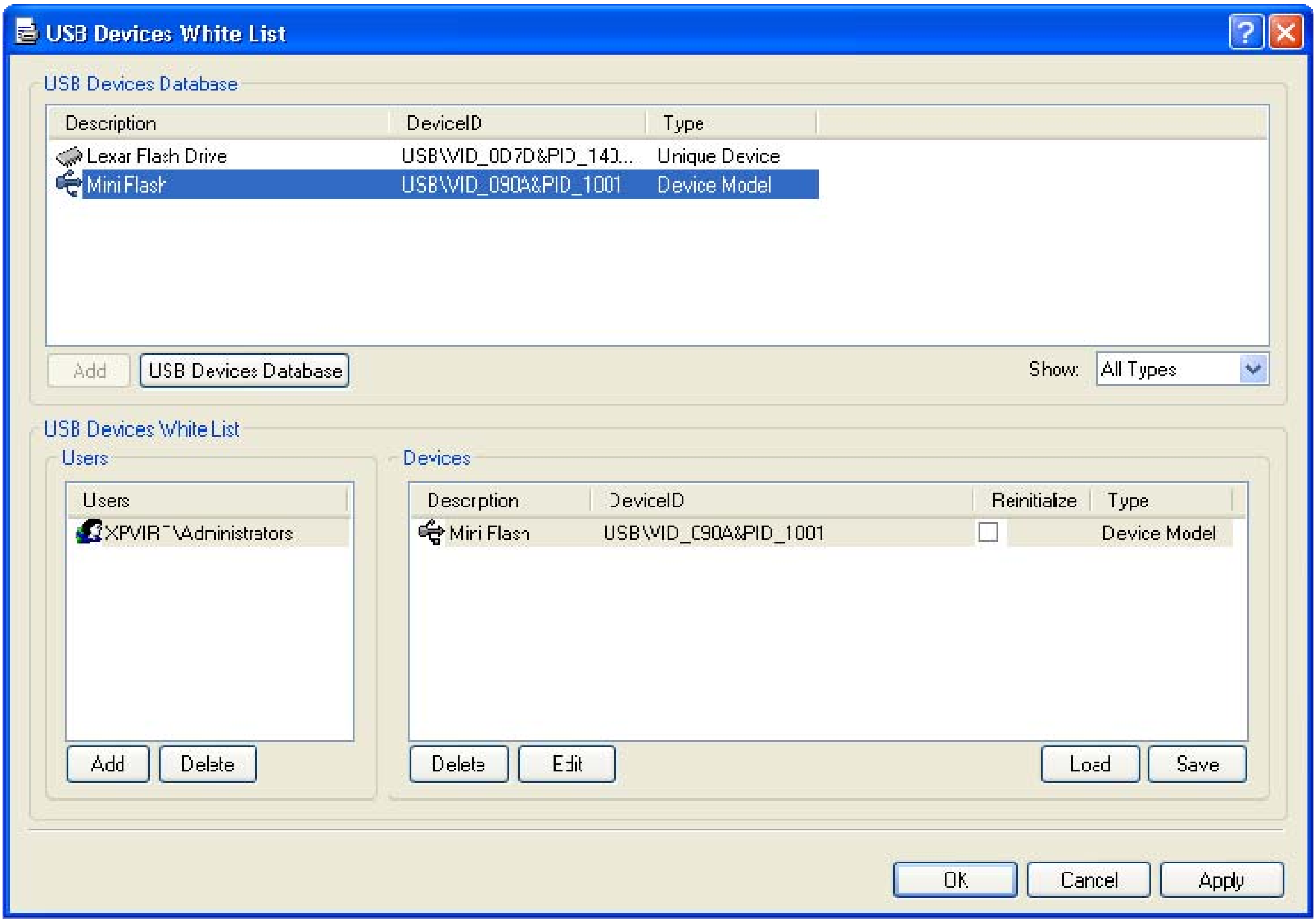
3. Click the *Security Settings* button on the *Permissions* dialog, and then uncheck *Access control for USB HID (mouse, keyboard, etc.)* as shown on the picture below.



Security Settings

- □ Access control for USB HID (mouse, keyboard, etc.)
- ☑ Access control for USB printers
- ☑ Access control for USB scanners and still image devices
- ☑ Access control for USB Bluetooth adaptors
- ☑ Access control for USB storage devices
- ☑ Access control for USB and FireWire network cards

4. Click *OK* to close the *Security Settings* dialog, and then click the *USB White List* button on the *Permissions* dialog.



USB Devices White List

USB Devices Database

| Description | DeviceID | Type |
|---|---|---|
| Lexar Flash Drive | USB\VID_0D7D&PID_14... | Unique Device |
| Mini Flash | USB\VID_090A&PID_1001 | Device Model |

Show: All Types

USB Devices White List

Users

| Users |
|---|
| XPVIRT\Administrators |

Devices

| Description | DeviceID | Reinitialize | Type |
|---|---|---|---|
| Mini Flash | USB\VID_090A&PID_1001 | □ | Device Model |

5. Click the *Add* button below the *Users* list, add the *Administrators* group (type the name or browse for all available names and select the needed one), click *OK* to close the *Select Users or Groups* dialog, and then highlight the *Administrator*s record.

6. Highlight the device model's record in the *USB Devices Database* list, and then click the *Add* button below this list.

   If you don't have devices in the *USB Devices Database* list, click the *USB Devices Database* button below this list, and then add devices as described in the **USB Devices Database** section of this manual. When you finished adding devices to the database, click *OK* to save this database and close the *USB Devices Database* dialog.

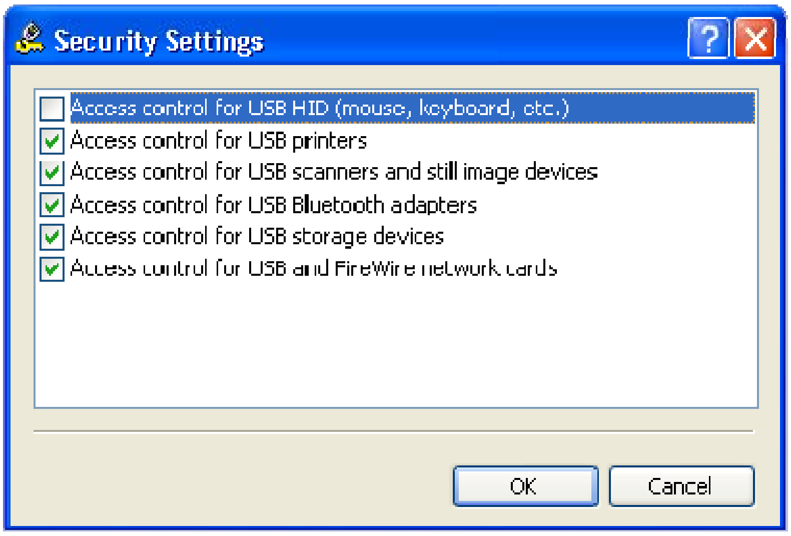
7. Click *OK* to apply the white list settings and close the *USB Devices White List* dialog, click *OK* to apply changes and close the *Permissions* dialog, and then click *Yes* to confirm that you really want to deny all users access to the USB port.

- **For all users all USB devices are denied except the mouse and keyboard but members of the *Administrators* group can use an authorized unique USB storage device:**

1. Select the *USB port* record from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.

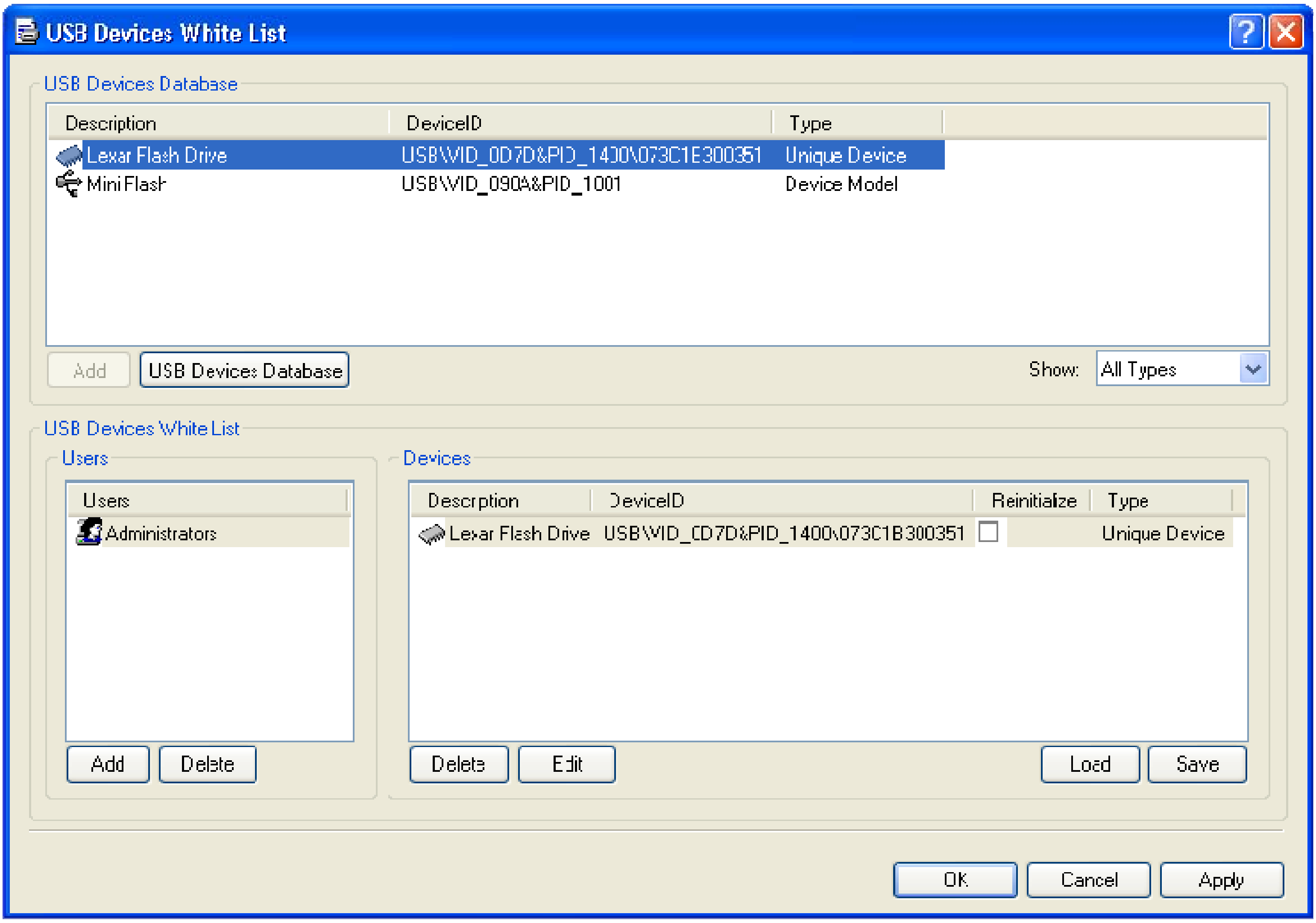
2. Click the *Add* button on the *Permissions* dialog and add the *Everyone* user (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, highlight the *Everyone* record and disable all rights in the *User's Rights* list.

3. Click the *Security Settings* button on the *Permissions* dialog, and then uncheck *Access control for USB HID (mouse, keyboard, etc.)* as shown on the picture below.



□ Access control for USB HID (mouse, keyboard, etc.)
☑ Access control for USB printers
☑ Access control for USB scanners and still image devices
☑ Access control for USB Bluetooth adapters
☑ Access control for USB storage devices
☑ Access control for USB and FireWire network cards

4. Click *OK* to close the *Security Settings* dialog, and then click the *USB White List* button on the *Permissions* dialog.



USB Devices White List

USB Devices Database

| Description | DeviceID | Type |
|---|---|---|
| Lexar Flash Drive | USB\VID_0D7D&PID_1400\073C1B300351 | Unique Device |
| Mini Flash | USB\VID_090A&PID_1001 | Device Model |

Show: All Types

USB Devices White List

Users

| Users |
|---|
| Administrators |

Devices

| Description | DeviceID | Reinitialize | Type |
|---|---|---|---|
| Lexar Flash Drive | USB\VID_0D7D&PID_1400\073C1B300351 | □ | Unique Device |

5. Click the *Add* button below the *Users* list and add the *Administrators* group (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, and then highlight the *Administrator*s record.

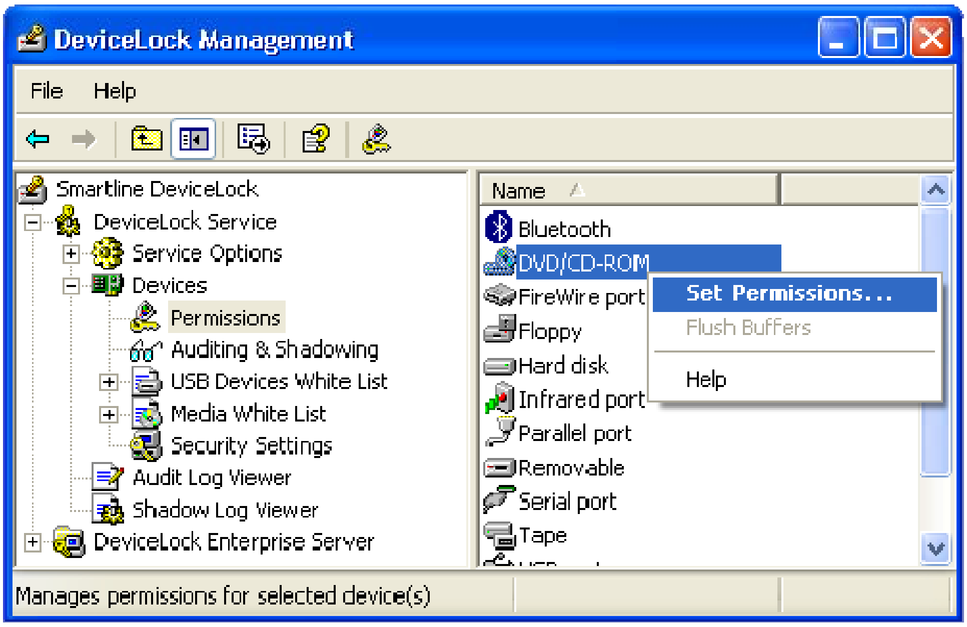
6. Highlight the unique device's record in the *USB Devices Database* list, and then click the *Add* button below this list.

   If you don't have devices in the *USB Devices Database* list, click the *USB Devices Database* button below this list, and then add devices as described in the **USB Devices Database** section of this manual. When you finish adding devices to the database, click *OK* to save this database and close the *USB Devices Database* dialog.

7. Click *OK* to apply the white list settings and close the *USB Devices White List* dialog, click *OK* to apply changes and close the *Permissions* dialog, and then click *Yes* to confirm that you really want to deny all users access to the USB port.

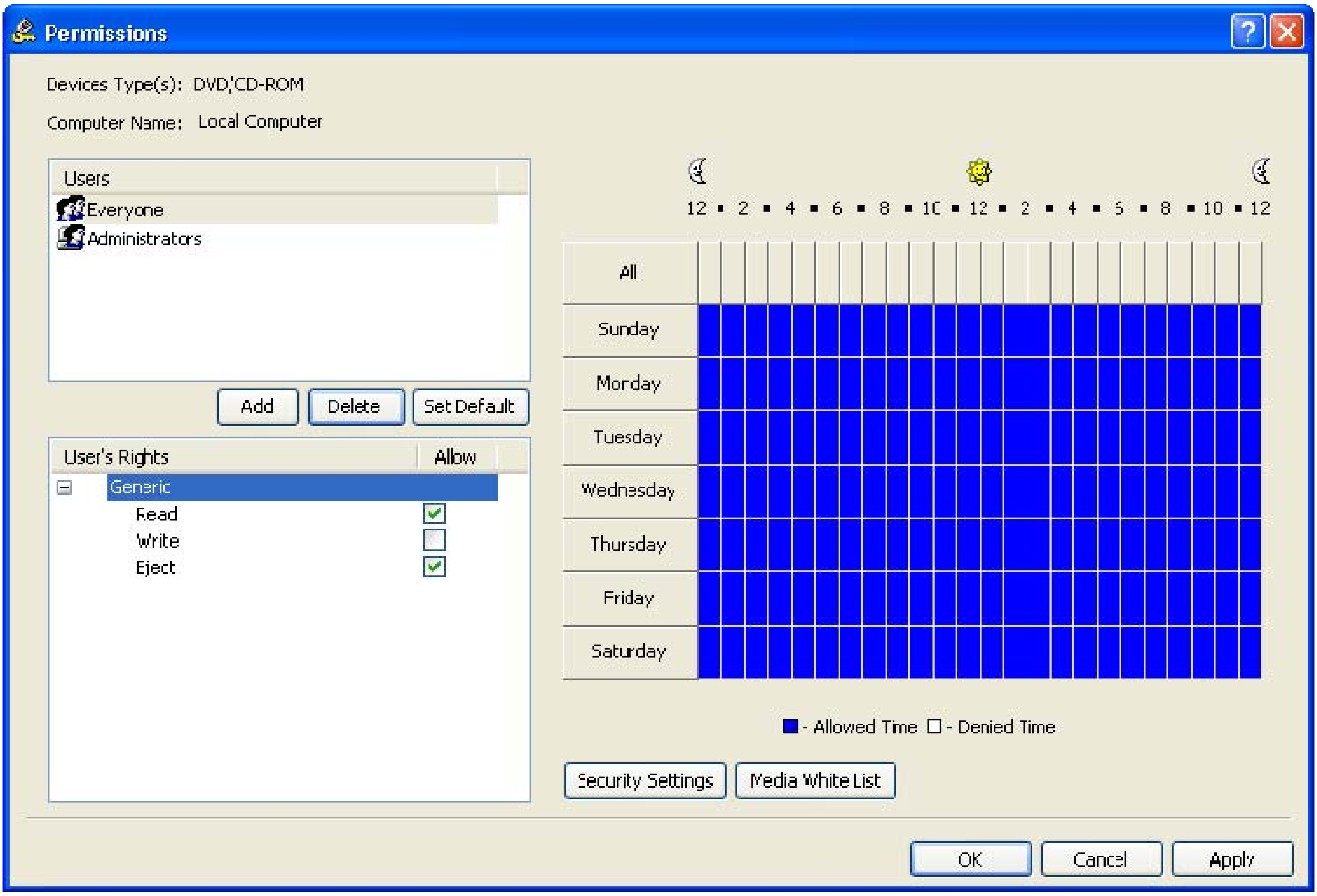
- **For all users all CD and DVD drives are set to the read-only mode but members of the *Administrators* group can burn (write) CD and DVD disks:**

1. Select the *DVD/CD-ROM* record from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.



2. Click the *Add* button on the *Permissions* dialog and add the *Administrators* group (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, highlight the *Administrators* record and enable all rights in the *User's Rights* list.

3. Click the *Add* button on the *Permissions* dialog and add the *Everyone* user (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog. Highlight the *Everyone* record and disable the **Write** right in the *User's Rights* list.



Permissions

Devices Type(s): DVD/CD-ROM

Computer Name: Local Computer

Users

- Everyone
- Administrators

| User's Rights | Allow |
|---|---|
| Generic | |
| Read | ☑ |
| Write | □ |
| Eject | ☑ |

■ - Allowed Time □ - Denied Time

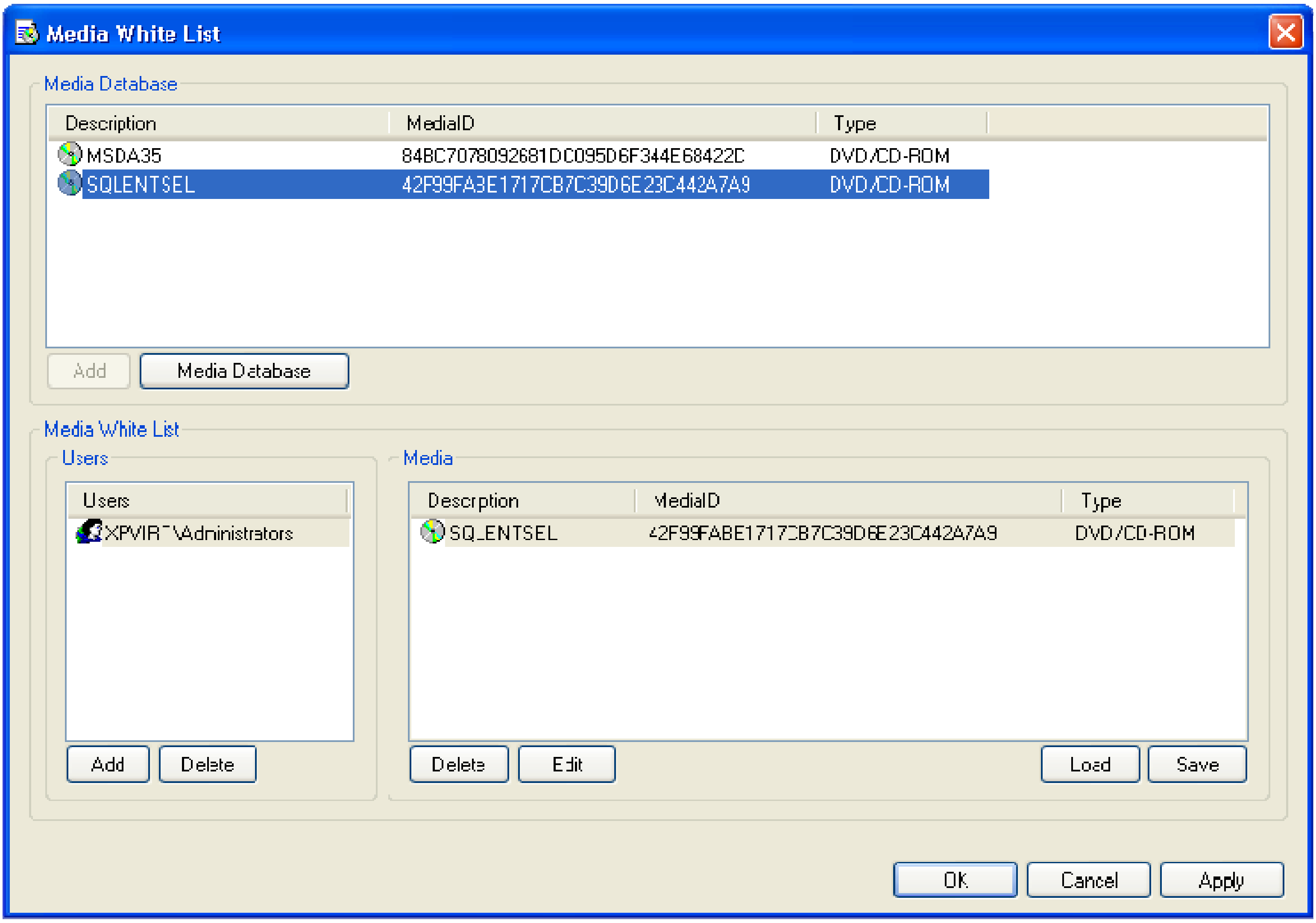
4. Click *OK* to apply changes and close the *Permissions* dialog.

- **For all users all CD and DVD drives are denied but members of the *Administrators* group can read a certain disk:**

1. Select the *DVD/CD-ROM* record from the list of device types under *Permissions*, and then select *Set Permissions* from the context menu available by a right mouse click.

2. Click the *Add* button on the *Permissions* dialog and add the *Everyone* user (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, highlight the *Everyone* record and disable all rights in the *User's Rights* list.

3. Click the *Media White List* button on the *Permissions* dialog.



| Description | MediaID | Type |
|---|---|---|
| MSDA35 | 84BC7078092681DC095D6F344E68422C | DVD/CD-ROM |
| SQLENTSEL | 42F99FA3E1717CB7C39D6E23C442A7A9 | DVD/CD-ROM |

| Users |
|---|
| XPVIRT\Administrators |

| Description | MediaID | Type |
|---|---|---|
| SQLENTSEL | 42F99FA3E1717CB7C39D6E23C442A7A9 | DVD/CD-ROM |

4. Click the *Add* button below the *Users* list and add the *Administrators* group (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, and then highlight the *Administrator*s record.

5. Highlight the media's record in the *Media Database* list, and then click the *Add* button below this list.

   If you don't have records in the *Media Database* list, click the *Media Database* button below this list, and then authorize a media as described in the **Media Database** section of this manual. When you finish authorizing a media, click *OK* to save the database and close the *Media Database* dialog.

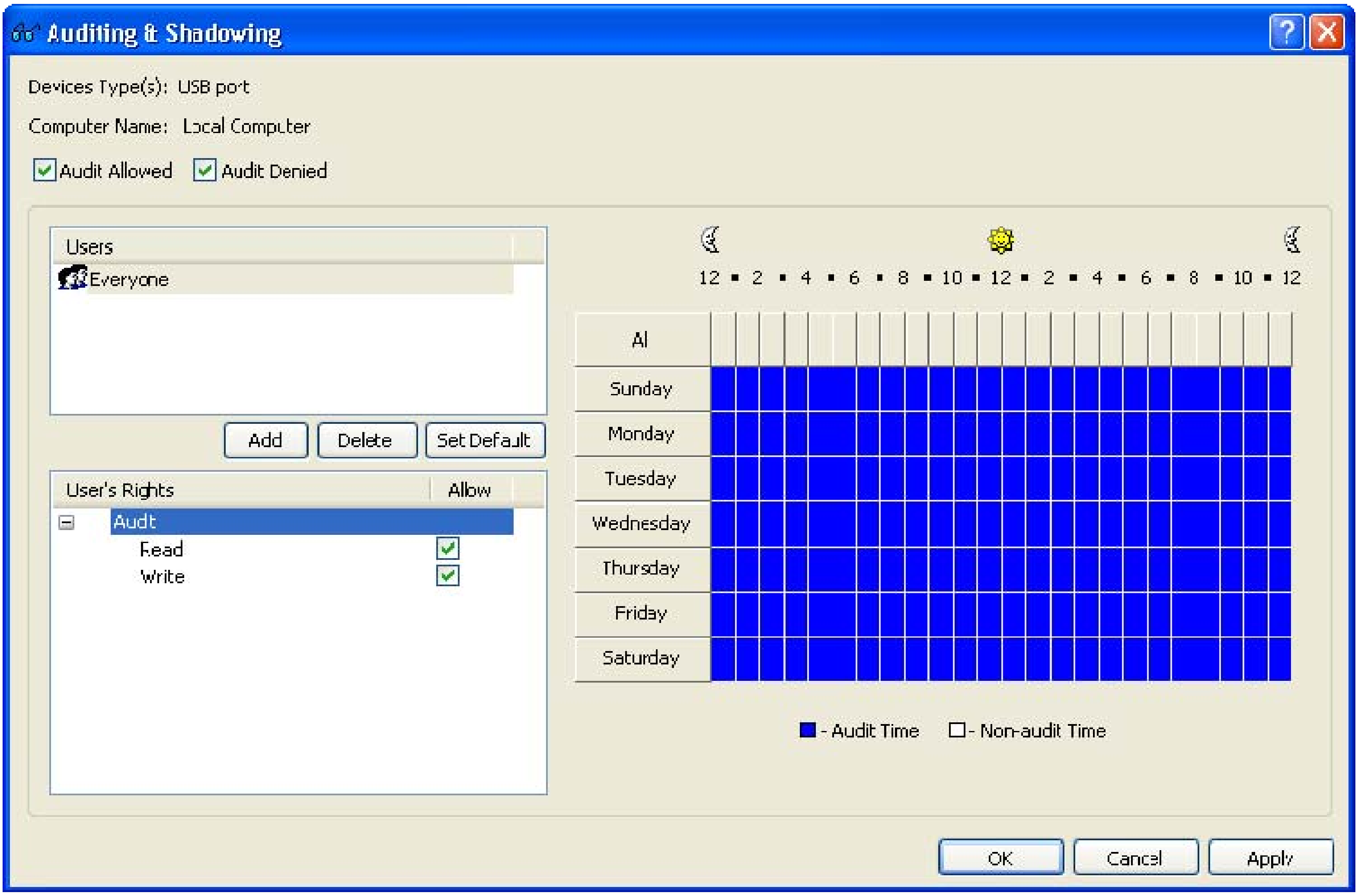
6. Click *OK* to apply the white list settings and close the *Media White List* dialog. Click *OK* to apply changes and close the *Permissions* dialog. Then click *Yes* to confirm that you really want to deny access to CD/DVD drives for all users.

### 10.1.2 Audit & Shadowing Rules Examples

- **Log insert, remove and access actions for USB devices for all users:**

1. Select the *USB port* record from the list of device types under *Auditing & Shadowing*, and then select *Set Auditing & Shadowing* from the context menu available by a right mouse click.

2. Click the *Add* button on the *Audit* dialog and add the *Everyone* user (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, highlight the *Everyone* record and enable **Read** and **Write** audit rights in the *User's Rights* list.



Auditing & Shadowing

Devices Type(s): USB port

Computer Name: Local Computer

☑ Audit Allowed ☑ Audit Denied

Users: Everyone

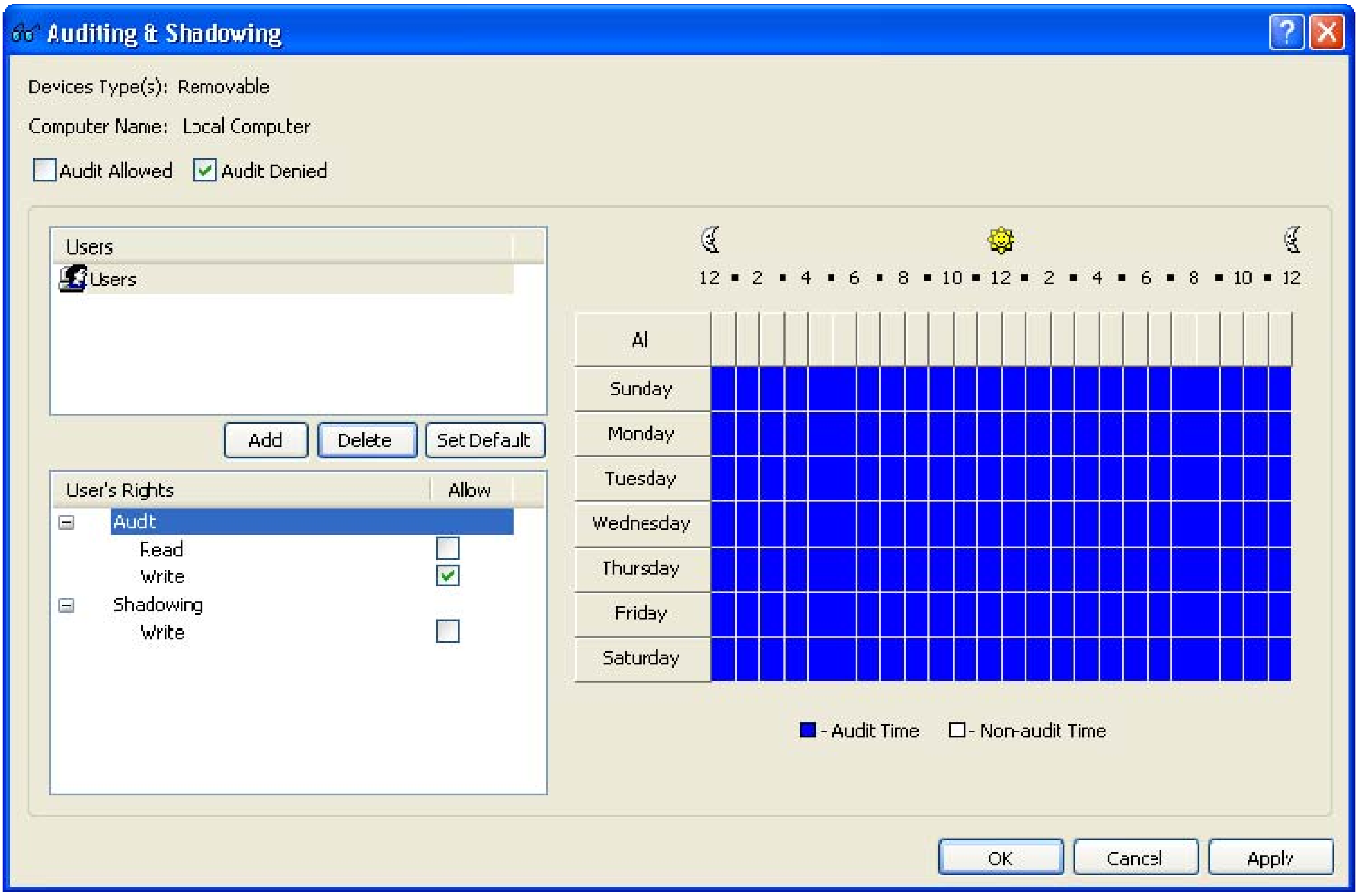
| User's Rights | Allow |
|---|---|
| Audit | |
| Read | ☑ |
| Write | ☑ |

3. Check *Audit Allowed* and *Audit Denied* at the top of the *Audit* dialog, and then click *OK* to apply changes and close the *Audit* dialog.

- **Log only files and folders names related to denied write actions for removable storage devices for members of the *Users* group:**

  1. Select the *Removable* record from the list of device types under *Auditing & Shadowing*, and then select *Set Auditing & Shadowing* from the context menu available by a right mouse click.

  2. Click the *Add* button on the *Audit* dialog and add the *Users* group (type the name or browse for all available names and select the needed one). Click *OK* to close the *Select Users or Groups* dialog, highlight the *Users* record and enable only the **Write** audit right in the *User's Rights* list.



Auditing & Shadowing

Devices Type(s): Removable

Computer Name: Local Computer

□ Audit Allowed ☑ Audit Denied

Users

Users

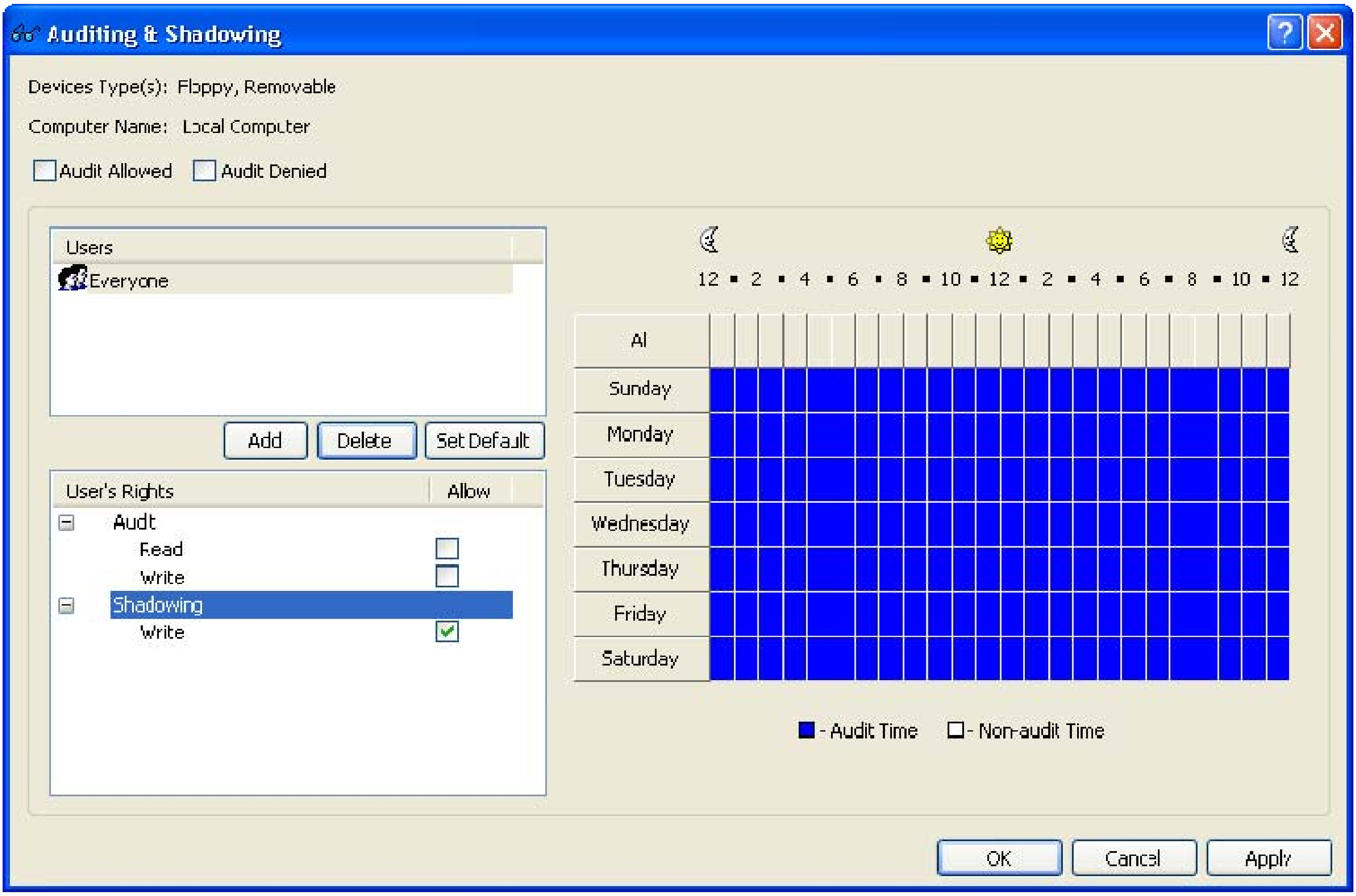
| User's Rights | Allow |
|---|---|
| ⊟ Audit | |
| Read | □ |
| Write | ☑ |
| ⊟ Shadowing | |
| Write | □ |

  3. Check only *Audit Denied* at the top of the *Audit* dialog, and then click *OK* to apply changes and close the *Audit* dialog.

- **Shadow all data writing to removable storage devices and floppies for all users:**

  1. Select *Floppy* and *Removable* records from the list of device types under *Auditing & Shadowing*, and then select *Set Auditing & Shadowing* from the context menu available by a right mouse click.

2. Click the *Add* button on the *Audit* dialog and add the *Everyone* user. Click *OK* to close the *Select Users or Groups* dialog and highlight the *Everyone* record. Disable all audit rights and enable only the **Write** shadowing right in the *User's Rights* list.



Auditing & Shadowing

Devices Type(s): Floppy, Removable

Computer Name: Local Computer

□ Audit Allowed □ Audit Denied

| Users |
|---|
| Everyone |

| User's Rights | Allow |
|---|---|
| ⊟ Audit | |
| Read | □ |
| Write | □ |
| ⊟ Shadowing | |
| Write | ☑ |

3. Click *OK* to apply changes and close the *Audit* dialog.