Reference Guide

DeviceLock™

SmartLine, Inc.

Contents

Using this guide

This guide 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. Also, we use 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.

We strongly recommend to read this guide very carefully and thoroughly. It was designed around the understanding that its users already have basic network knowledge as well as the ability and know-how to install a Local Area Network (LAN).

1. Overview

1.1 General Information

Preventing the introduction 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.

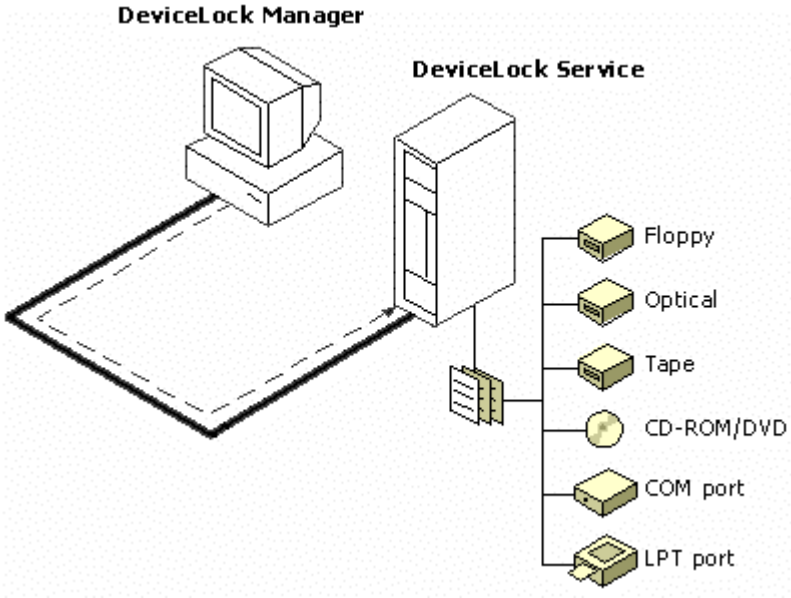
DeviceLock is easy to install and administrators can have instant access from the remote computers when necessary. There are no physical keys to store and manage - only software solution.

The administrator of the machine or domain can designate user access to floppy drives, other removable media, CD-ROM drives, tape devices or serial and parallel ports. Any types of the file systems are supported.

DeviceLock consists of two parts: DeviceLock Service (*dlservice.exe*) and DeviceLock Manager (*dlmanager.exe*).

DeviceLock Service is the core of DeviceLock. It is installed on each client system that you want to protect. DeviceLock Service runs automatically and provides device protection on the client machine while remaining invisible to that computer’s local users.

DeviceLock Manager is the control interface Systems Administrators use to remotely manage each network computer that has DeviceLock Service.



1.2 Security

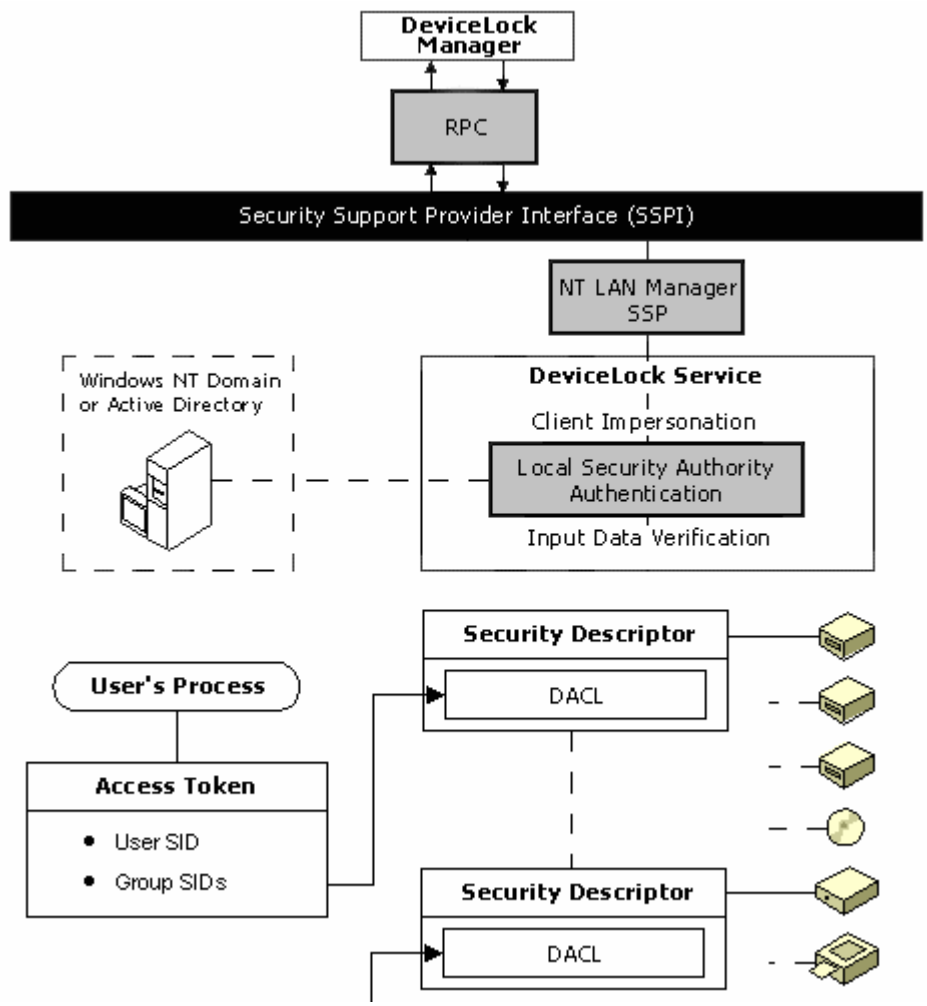
Reliable access control functionality is the primary focus of DeviceLock.

DeviceLock uses *Remote Procedure Call* (RPC) technology for communication between the service and the manager. It uses the Windows NT/2000/XP user-level security subsystem for authentication.

DeviceLock's security is integrated into the Windows NT/2000/XP access control subsystem. Remote computers with an installed DeviceLock Service can only be accessed by someone with administrator privileges.

Because DeviceLock uses standard protocols, it operates like any other Windows NT/2000/XP administrative tool such as *User Manager, Server Manager*, *Event Viewer*, etc.

The DeviceLock Service on each client machine checks all input data for size and type making it impossible for buffer overflow attacks.



1.3 Requirements

DeviceLock works on any computer using Windows NT/2000/XP.

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. But, if you are going to use DeviceLock throughout your network, you must have domain administrative 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.

1.4 Main Purpose

- DeviceLock gives network administrators control over which users can access what devices (floppies, Magneto-Optical disks, CD-ROMs, DVDs, ZIPs, serial and parallel ports, tape devices, etc.) on a local computer.
- Once DeviceLock is installed, administrators can control access to floppies, CD-ROMs or any other device, depending on the time of day and day of the week.
- DeviceLock enhances access control for Windows System Administrators and helps control removable disk usage.
- It can protect network and local computers against viruses, trojans and other malicious programs often injected from removable disks.
- DeviceLock can protect disks from accidental or intentional formatting.
- DeviceLock allows administrators control over which users can eject what removable devices.
- Network administrators can also use DeviceLock to flush a storage device's buffers.

2. DeviceLock Manager

2.1 Installation

DeviceLock Manager can be installed to any computer running Windows NT/2000/XP.

To install DeviceLock Manager just run Setup (*setup.exe*).

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

You have two choices: install both DeviceLock Manager and DeviceLock Service using Typical setup or you can install only DeviceLock Manager using Custom setup, then selecting the *DeviceLock Manager* component.

After a successful install, you can run DeviceLock Manager by selecting the *DeviceLock Manager* item from the *Programs* menu.

2.2 Interface

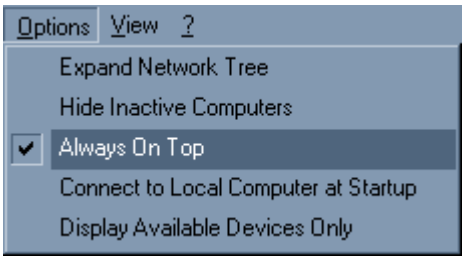
DeviceLock Manager has a user-friendly, easy-to-use interface. All functions can be accessed with either a mouse or keyboard.

In any dialog you can press the *F1* button to get specific help.

The main window of DeviceLock Manager can be resized. DeviceLock Manager saves its size and position, and restores these at its next startup.

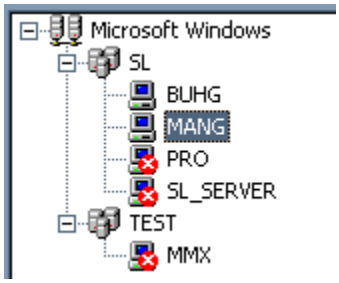
DeviceLock Manager has a menu at the top of its main window. Many functions are accessible through this menu.

You can select *Always on Top* from the *View* menu to keep the DeviceLock Manager on top (above) any other applications.



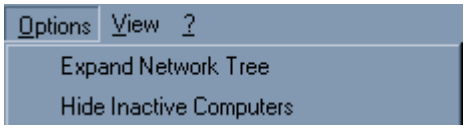
2.3 Main Dialog

When you start DeviceLock Manager it displays its main dialog where you can select a computer to control.



The left side of the Main dialog shows a list of the computers available in your network. This listing is called the *computer tree*. Each computer that is running DeviceLock Service has an icon of a computer. Each computer without DeviceLock Service running on it has an icon of a computer overlaid by a red circle containing a white **X**, indicating the computer is inactive. A computer will also show as inactive if you do not have the system privileges to connect to it.

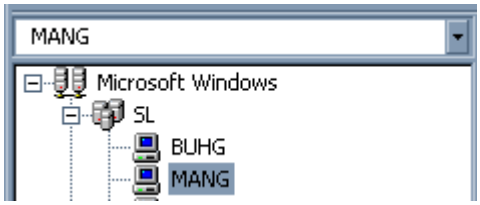
If you want a listing of only active computers — computers with running and accessible DeviceLock Service — select *Hide Inactive Computers* in the *Options* menu. If you do not want the computer tree to expand automatically, unselect *Expand Network Tree* in the *Options* menu.



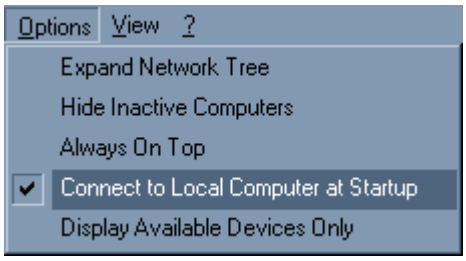
To refresh a list of computers, press F5 or select *Refresh Network Tree* from the *View* menu. Also, you can refresh the state (whether active or inactive) of a selected computer by pressing Shift+F5 or selecting *Refresh Selected Computer* from the *View* menu.

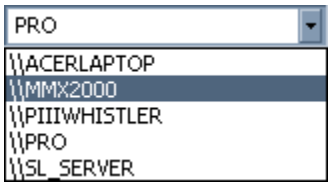
If your computer is not connected to a network, the list of computers will be empty or may contain only a single record — "Microsoft Windows Network" (or similar message).

To access a remote computer, it needs to have DeviceLock Service installed and running, and it needs to have a connection to your computer. To access a remote computer, simply select it from the computer tree. DeviceLock Manager automatically connects to the computer immediately after it has been selected. You can use a mouse to select the computer or you can use the keyboard's arrow keys and press Enter on a selected computer. Alternatively, you can type in the computer's name in the field above the computer tree, then press Enter.



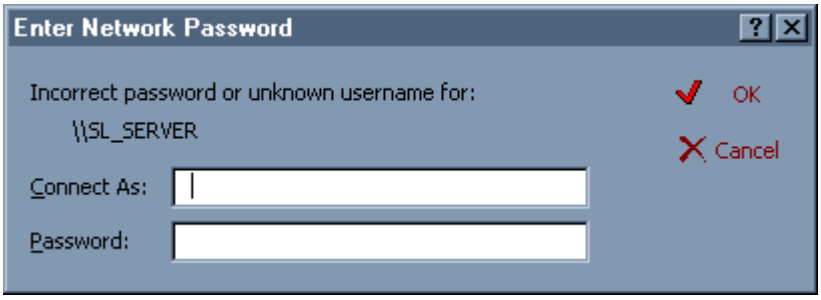
To connect to the local computer, do not specify a computer name. If *Connect to Local Computer at Startup* is enabled in the *Options* menu, DeviceLock Manager automatically connects to the local computer each time it starts up.



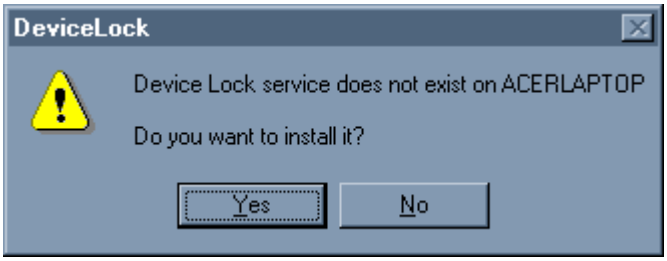


All frequently used computers are added automatically to the most recently used (MRU) list so they can be easily accessed.

If you don't have administrative privileges on the selected computer, DeviceLock Manager will show the **Enter Network Password** dialog and you'll be able to connect under the account of any other user. The **Enter Network Password** dialog appears when you attempt to connect to a computer, but the domain controller (DC) does not recognize the user account you have used to log on. This often occurs when you are logged on as the administrator of a local computer and attempt to access domain resources. To access the domain resources, you must provide a valid user account and password that the domain recognizes. User accounts are a domain name followed by a backslash (\) and the user name, e.g. *D1\John*.

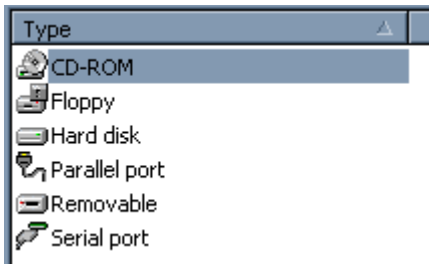


DeviceLock Service should be installed on the computer so you can control the access to devices on that computer. DeviceLock supports remote installing. This lets a Systems Administrator set up a service on distant machines without having to physically go to them. If the DeviceLock Service isn't installed on the remote system you are trying to connect to, DeviceLock Manager will suggest that you install the service. Select the DeviceLock Service executable file (*dlservice.exe*) and DeviceLock Manager will copy it to the remote computer's Windows system directory (e.g. *c:\winnt\system32*). If the service is on the client system but is outdated, DeviceLock Manager replaces it.

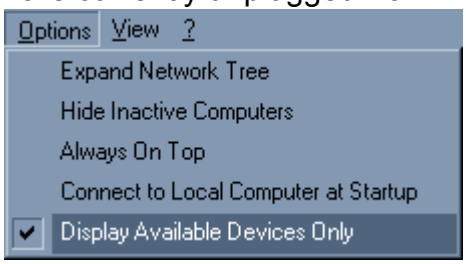


DeviceLock Manager automatically starts DeviceLock Service if it's stopped on the system.

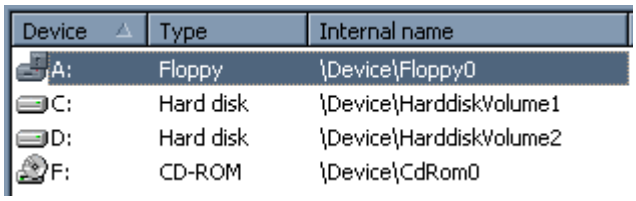
If you successfully connect to a computer, its name appears in the status bar of DeviceLock Manager. All major DeviceLock Manager functions become available only if you are connected to a computer.



The list of device types (floppy, removable, serial port, etc.) appears at the top-right side of the Main dialog. If *Display Available Devices Only* is enabled in the *Options* menu, DeviceLock Manager shows only those types of devices that are currently available from your computer. Otherwise, you will see every type of device that DeviceLock supports. This is useful when you want to set permissions to devices that are not yet installed or are currently unplugged from the computer. ***DeviceLock Service automatically detects new devices and set permissions (if any) for them. DeviceLock Service recognizes new devices, not by their user-mode names or letters (such as A:, COM1) but by their internal names (such as \Device\Floppy0, \Device\Serial0) so it works even with unnamed devices.***



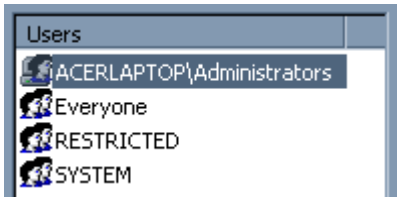
To set permissions for a device type, highlight it on the list (use Ctrl and/or Shift to select several types simultaneously) and select *Set Permissions* from the *File* menu or simply press F2. Alternatively, you can press the appropriate button at the top-right side of the main dialog box. Below the list of types, DeviceLock Manager displays the devices that are available for a selected device type. In this list you can see the devices that are currently available for local users on the remote computer. If there are no devices currently available for the selected type, this list is empty. To see a listing of all the devices that are available to the remote computer, select all records in the list of types, using Ctrl and/or Shift.



Please note that 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 floppy drives).

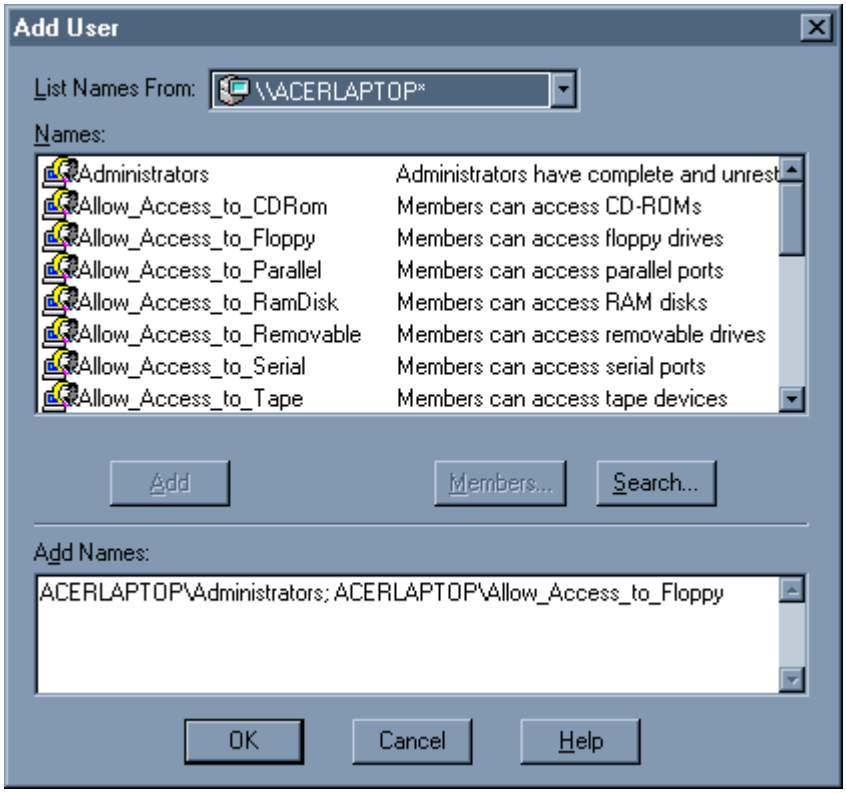
2.4 Permissions Dialog

This dialog lets you control the access to devices. You can set permissions to a device type or to a group of types and define the users and times (day of the month and/or day of the week) each can be accessed.



The names of the users and user groups assigned to a device type are shown in the list of accounts at the 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.

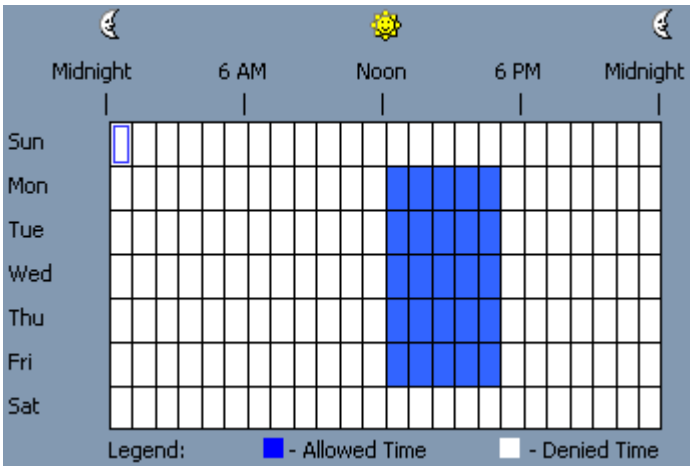


To delete a record from the list of accounts, use the *Delete* button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

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

- The *Everyone* account has **Full access** rights except for the **Allow Format** privilege.
- Members of the *Administrators* group and the *SYSTEM* account have **Full access** rights including the **Allow Format** and **Allow Eject** privileges.

Using special time control you can define a time when a selected user or user group will have 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. ***Note that each user can have his/her own allowed/denied time.***

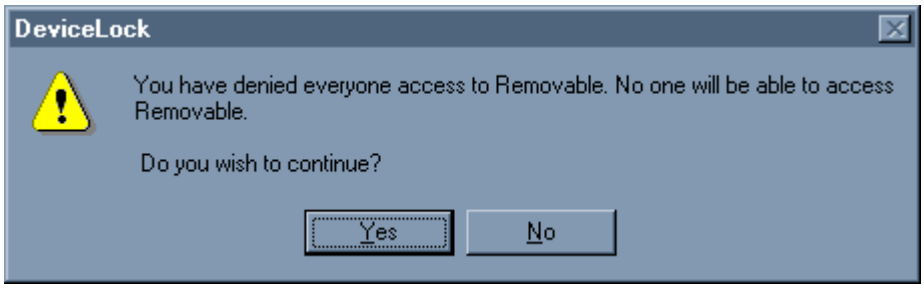


To define which actions on devices are to be allowed for a user or user group, set the appropriate rights and privileges:

- **Full access** – to enable the reading, writing, deleting, executing, etc. of files and directories.
- **Allow Format** – to enable the formatting, checking and any other direct access of drives. ***Please note that you can enable this privilege only if Full access right is selected. This privilege is not available for CD-ROMs, DVDs, serial and parallel ports, tape devices and RAM disks.***
- **Allow Eject** – to enable ejection of the media. ***Please note that you can enable this privilege only if Full access right is selected. This privilege controls only ejection via software. Hardware ejection using the Eject button on a device's front panel cannot be safeguarded against.***
- **No access** – user cannot access a device.

If you want to deny all actions for a selected user or user group, you must select the **No access** right. Also, to deny all actions you can set the denied time for all periods.

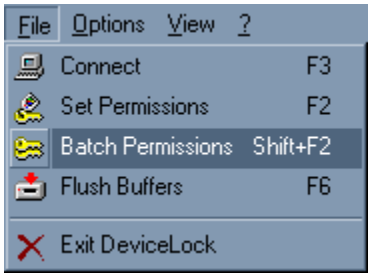
To deny access to devices for all users and user group, add only the one *Everyone* user to an account's list and select the **No access** right or set the denied time for all periods. Also, you can remove all records from an account's list and set empty permissions so nobody can access devices.



2.5 Batch Permissions

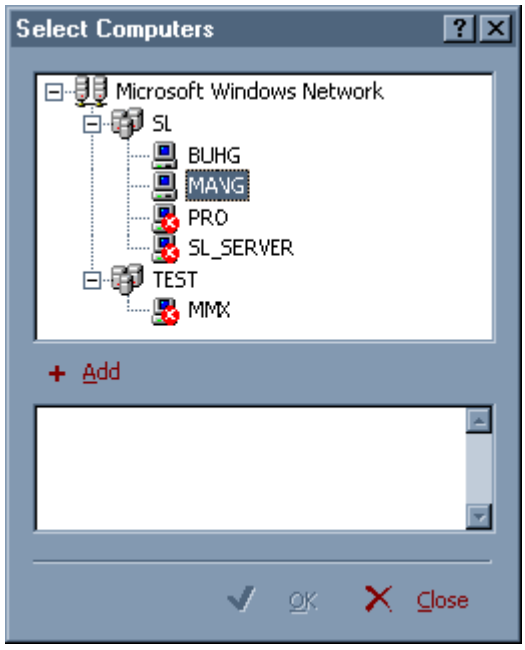
Batch Permissions is one of the most powerful and useful functions. Usually, midsize and large networks contain many similar computers with similar devices (e.g. all computers have floppy drives and CD-ROMs) and network administrators can set permissions for each of them very quickly by using the batch mode.

Batch Permissions is available for use right after DeviceLock Manager is loaded. You do not need to connect to any computer directly to use this function. ***Please note that any permission you set using Batch Permissions, will overwrite all previously assigned permissions on those same devices.***



To access Batch Permissions you should select the *Batch Permissions* item from the *File* menu or press Shift+F2. Also, you can press the appropriate button at the top, right-side of the main dialog.

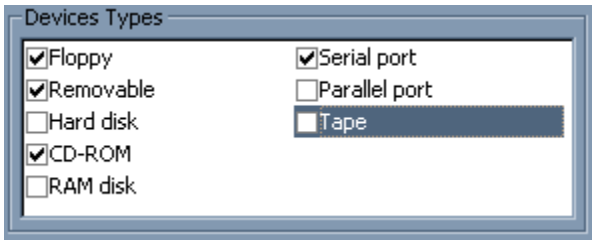
First, you need to select the computers that you want to include in the batch processing. To add computers to the list, press the *Add* button. This opens a dialog with the computer tree where you can select any computer that is available on your network. Double click on the computer name in the computer tree to add this computer or type the computer's name manually and press the *OK* button to include selected computers to the list.



Also, you can load computers from an external file. Press the *Load* button and select a file that contains the list of computers. Two file formats are supported — text file (.txt) and comma separated values (.csv). A text file must contain each computer's name on separate lines. Computer names in a .csv file must be separated by commas or semicolons.

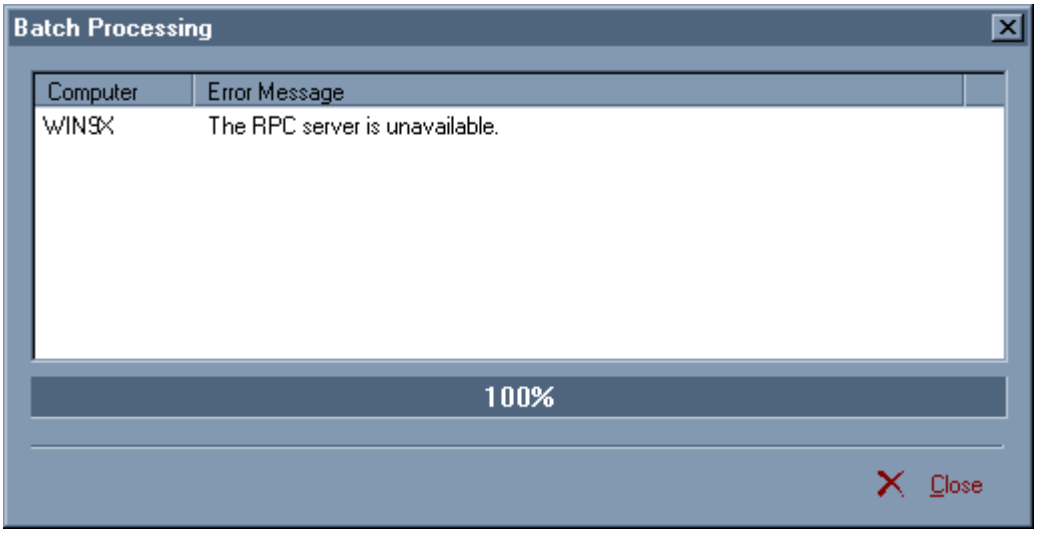
To save a computer listing to an external file, press the *Save* button. Select the type of the file — .txt or .csv.

Then add users or user group to the account's list. Define allowed/denied times on the time control and set the appropriate rights and privileges for each user and users group as described in **Section 2.4**.



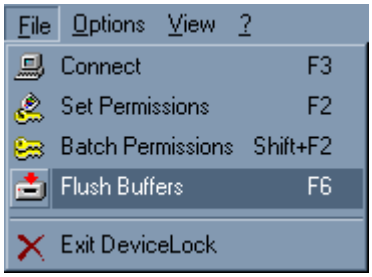
The final step is selecting the devices you want to process. There are few types of devices available in the DeviceLock Manager: Floppy, Removable, CD-ROM, and so on. Each of these types represents all the devices of this category, i.e. Floppy represents all floppy drives that are available on the computer, Removable — all removable drives, and so on.

To start batch processing, press the *Set Permissions* button.



2.6 Flush Buffers

DeviceLock allows you to saves a disk's cache and unsaved buffers to selected device.



To flush the buffers, highlight the device in the devices list (use Ctrl or/and Shift to select several devices simultaneously) and then select *Flush Buffers* from the *File* menu or press F6. Also, you can press the appropriate button at the bottom-right side of the main dialog. Flush Buffers is available only for devices that support write-operations, e.g. floppies, ZIPs, JAZZs, etc. Flush Buffers cannot be used for devices such as CD-ROMs.

Note that if you select a device with a removable media, you have to make sure that this device has the media inserted and it isn't marked as read-only.

Flush Buffers is very useful for removable medias, i.e. floppies, ZIPs, Magneto-Optical disks, etc. It can prevent your data from being lost because of a write-behind cache. Windows gives you the option to use write-behind caching to improve the performance of removable disk drives but sometimes it may be a reason for data loss on those drives. It is recommended to force the flushing of a disk's cache from time to time, especially before ejecting disks.

3. DeviceLock Service

3.1 Installation

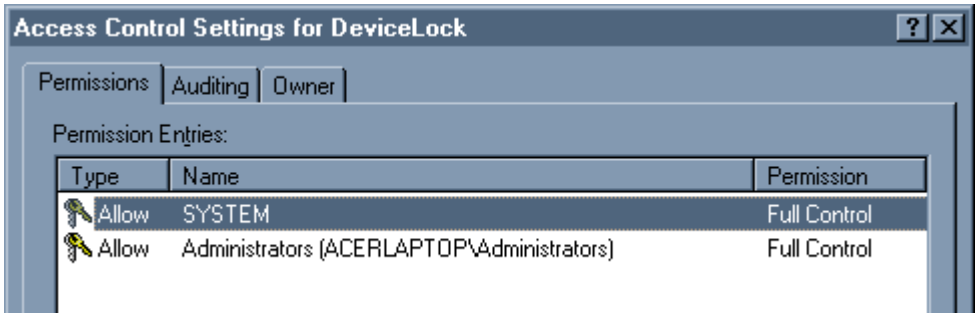
DeviceLock Service can be installed on any computer running Windows NT/2000/XP.

To install DeviceLock Service run Setup (*setup.exe*).

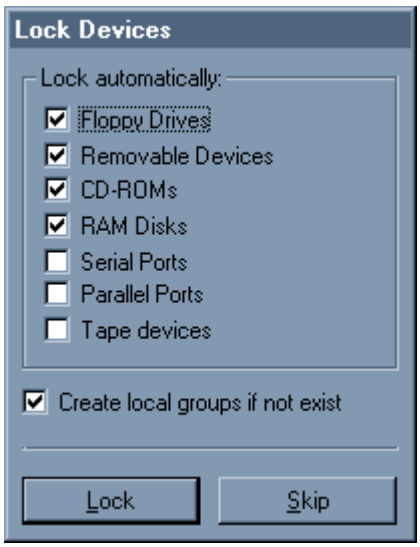
DeviceLock Service installs to the directory of your choice. Setup tries to find a DeviceLock Service installation and if one exists, Setup suggests that you install DeviceLock Service to the same directory. If a previous installation does not exist, Setup suggests that DeviceLock Service be installed 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.

You have the following two choices: either install both DeviceLock Service and DeviceLock Manager using Typical setup or install only DeviceLock Service using Custom setup and select the *DeviceLock Service* component.

If you install DeviceLock on an NTFS partition, Set-up protects DeviceLock's directory and files by allowing only members of the *Administrators* group or the *SYSTEM* account to access DeviceLock's files or to uninstall DeviceLock.



During the installation process, Setup suggests that you set permissions to the local devices. Check the *Create local groups if not existing* checkbox and Setup will 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. Select the devices you would like to automatically lock during installation and press the *Lock* button. Set-up assigns the **Full access** right including the **Allow Format** and **Allow Eject** privileges for members of the *Administrators* group and the *SYSTEM* account. Members of the *Allow_Access_To_* group will have the **Full access** right without the **Allow Format** and **Allow Eject** privileges. Press the *Skip* button if you prefer to wait until after installation to set permissions to these devices using DeviceLock Manager.



Setup 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*. *Devicelock.ini* must be in the same directory where *setup.exe* is located. With this file, you can customize the installation parameters. For example, to install only DeviceLock Service, *devicelock.ini* should look like:

[Install]
Service = 1
Manager = 0
Documents = 0

To automatically lock devices during installation, specify the *Lock Devices* parameters:

[Lock Devices]
Floppy = 1
Removable = 1
CDROM = 1
RamDisk = 1
Serial = 1
Parallel = 1
Tape = 1
CreateGroups = 1

If you have purchased a license for DeviceLock, you can also specify the location of its registration file in the *devicelock.ini* file so Setup automatically registers new versions of a service:

RegFileDir = C:\Directory

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

You can also specify a destination directory for DeviceLock:

InstallDir = C:\Program Files\DeviceLock

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

[Misc]
Run = C:\mybatchfile.bat

DeviceLock supports remote installation to help a Systems Administrator to set up a service on remote machines without ever having to physically go to them. If the DeviceLock Service isn't installed on the remote system you are trying to connect to, DeviceLock Manager will suggest that you install the service. Select the DeviceLock Service executable file (*dlservice.exe*) and DeviceLock Manager will copy it to the remote computer. 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, DeviceLock Manager will copy the executable file to the directory of the old file and the old file will be replaced.

DeviceLock can also be installed 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.

4. Appendix

4.1 Permission Examples

a) To prevent anyone from accessing a device at any time:

Add the *Everyone* user to an account list and select the **No access** right or select the **Full access** right and set the denied time to all periods. Alternatively, you can remove all records from an account list and set empty permissions.

b) So that only members of the *Administrators* group and the *SYSTEM* account can access a device at any time:

Add only the *SYSTEM* user and the *Administrators* local group to an account list, select the **Full access** right and set the allowed time for all periods for each record in the account list.

c) So that anyone can access a device at any time but only members of the *Administrators* group can perform formatting and checking of the media of the device:

Add only the *Everyone* user and the *Administrators* local group to an account list, select the **Full access** right and set the allowed time for all periods for each record in the account list. Uncheck the **Allow Format** privilege for the *Everyone* user and check this privilege for the *Administrators* group.

d) So that members of the *Users* group can access a device only from Monday till Friday and between 12pm and 5pm but *Administrator* can access this device at any time:

Add only the *Users* local group and the *Administrator* user to an account list and select the **Full access** right for each. Set the allowed time for all periods for the *Administrator* user. Set the time as shown on the picture below for the *Users* group. ***Make sure that the Administrator user does not belong to the Users group.***