Help Contents

DeviceLock Manager

for Windows NT 4.0/2000/XP and Windows Server 2003

General Information:

Introduction

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.

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.

License

END-USER LICENSE AGREEMENT FOR DeviceLock®:

- All copyrights to DeviceLock® are exclusively owned by SmartLine Inc.
- DeviceLock® is a registered trademark of SmartLine Inc.
- Anyone may use this software during a trial period of 30 days only, on one computer of a local network, at any single time. Following this trial period of 30 days, if you wish to continue to use DeviceLock® then you MUST register.
- A registered user is granted a non-exclusive license to use DeviceLock® on one computer at a time, for any legal purpose. The registered DeviceLock® software may not be rented nor leased, but may be permanently transferred, if the person receiving it agrees to the terms of this license. If the software is an update, the transfer must include all updates and all previous versions of the DeviceLock® software.
- An unregistered, evaluation version of DeviceLock® may be freely distributed, provided the distribution package is not modified. No person nor company may charge a fee for the distribution of DeviceLock® without written permission from the copyright holder SmartLine Inc.
- To register, you must complete the registration form and send it, with the registration fee, to one of the authorized registration sites.
- DeviceLock® IS DISTRIBUTED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE IT AT YOUR OWN RISK. THE AUTHOR OR SMARTLINE INC WILL NOT BE HELD LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS NOR ANY OTHER KIND OF LOSS AS A RESULT OF OR WHILE USING OR MISUSING THIS SOFTWARE.
- You may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, nor transfer the licensed program, nor any subset of the licensed program, except as provided for in this agreement. Any such unauthorized use shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution. All rights not expressly granted here are reserved by SmartLine Inc.
- This Agreement and any dispute relating to DeviceLock® or to this Agreement shall be governed by the laws of the Russian Federation. You agree and consent that jurisdiction and proper venue for all claims, actions and proceedings of any kind relating to SmartLine Inc or the matters in this Agreement shall be exclusively in courts located in Moscow. Installing and using DeviceLock®

signifies acceptance of these terms and conditions of the license.

- If you do not agree with the terms of this license you must remove DeviceLock® files from your storage devices and cease to use the product.

How to Register

Why You Need to Register

A registered user may use DeviceLock:

- in any environment including commercial
- to control access to devices on one or more computers in the network, depending on the number of licenses
- without nag screens
- with access support and assistance
- including ALL updates that will be released within 1 year from the date of purchase

How to Purchase

- **Single** license (ID #151781)

1. Order Through the World Wide Web

http://www.protect-me.com/dl/register.html

IMPORTANT! Be sure to give us the correct e-mail address when filling out the order form. We are unable to process incomplete order forms.

All registrations use **SECURE** protocols making it impossible for a third party to intercept your credit card information.

2. Invoices/Purchase orders

US and Canadian customers: You can fax a Purchase Order to us at **(925) 891-9152**, or send it to:

AdvancedForce InfoSecurity Solutions, Inc.
2010 Crow Canyon Place, Suite 100
San Ramon, CA 94583, USA

European customers: You can fax a Purchase Order to us at **+49 221-31088-29**, or send it to:

element 5 AG
Vogelsanger Strasse 78

50823 Koeln

Germany

IMPORTANT! We accept orders on account only from established companies that have faxed us a signed Purchase Order on their company letterhead. We allow an established customer a payment deadline of 30 days from purchase.

3. Fax And Phone Orders

US and Canadian customers: You can place an order by calling our ***toll-free*** order number **1-866-6-NTLOCK (1-866-668-5625)** (available weekdays from 9am to 5pm PST). Orders may also be sent by fax to **(925) 891-9152**.

European customers: You can fax your order to us at **+49 221-31088-29**, or call us at **+49 221-31088-30**.

IMPORTANT! Please make sure to have the program ID for DeviceLock ready (see above).

4. Check And Cash Orders

If you prefer to pay by cash or check, please send payment to:

US and Canadian customers:
AdvancedForce InfoSecurity Solutions, Inc.
2010 Crow Canyon Place, Suite 100
San Ramon, CA 94583, USA

IMPORTANT! Please make U.S. checks payable to **AdvancedForce InfoSecurity Solutions, Inc.** (***Note:*** *Canadian checks are not accepted unless they are drawn on a US-Dollar account*)

European customers:
element 5 AG
Vogelsanger Strasse 78

50823 Koeln
Germany

IMPORTANT! Please make checks payable to **element 5 AG** (***Note:*** *send only guaranteed bank checks such as money orders or Cashier's Checks*)

5. Resellers and Distributors

SmartLine Inc works with all major software procurement companies like *Software House International*, *SoftChoice*, *PC-Ware Group*.

DeviceLock may be ordered through one of our *Authorized Partners*. To review the list of our partners, please visit: http://www.protect-me.com/partners.html

Support

We strongly recommend that you read these Frequently Asked Questions:

- http://www.protect-me.com/dl/faq.html

If you have questions, comments or bug reports, please use our online helpdesk. The helpdesk automatically logs your support requests and assigns each a unique identifier. Our support specialists will process your requests as soon as possible.:

- http://www.protect-me.com/support/ticket_list.php

You can also contact our technical support team at: +1-925-231-0042. Phone support hours are Monday to Friday, 8am - 5pm PT.

Please give the following info:

- Product's version (see the About dialog)
- Product's serial number (if you're a registered user)
- Windows version (including service packs and other installed fixes or patches), US or International
- Your computer information: CPU type and speed, installed memory
- Description of the problem (as much detail as possible so we can duplicate the problem)

SmartLine's Software

The software development company SmartLine Inc, is dedicated to providing effective and economical solutions to small, medium and large-scale business. Our products help network administrators and systems integrators with their job of providing well-integrated and cost-effective network management solutions:

INFORMATION SECURITY SOLUTIONS:

- **PortsLock®** is a personal firewall for Windows NT/2000/XP that fully supports user-level security. Once PortsLock is installed, administrators can control which users can access what TCP/IP based protocols (HTTP, FTP, SMTP, POP3, Telnet, etc.) on a local computer, depending on the time of day and day of the week. PortsLock lets you set allowed/denied TCP/UDP ports and IP-addresses for incoming and outgoing connections. *More information is available at* http://www.protect-me.com/pl/

NETWORK MANAGEMENT SOLUTIONS:

- **Active Network Monitor®** runs under Windows NT/2000/XP and allows Systems Administrators to gather information from all the computers (even from the Windows 9x/Me computers) in the network without installing server-side applications on these computers. It is the leading enterprise network monitoring solution for corporate networks. ANM significantly reduces the total cost of network management in enterprise environments by enabling IT personnel to monitor installed service packs and hot fixes, services, devices, processes, installed applications, disks, shared resources, hardware resources (IRQs, I/O, DMA and Memory), users, local groups, global groups, and so on. *More information is available at* http://www.protect-me.com/anm/

- **Remote Task Manager®** is a systems control interface that can be run from any remote Windows NT/2000/XP computer. This enables a Systems Administrator to control most aspects of a remote environment. The simple-to-use, tabbed interface separates applications, services, devices, processes, events, shared resources and performance monitor, making each of these very easy to control. A Systems Administrator can start or stop services or devices, add new services or devices, manage the run level and adjust the security (permissions, auditing and owner). The Process Function and the Task Manager allows remote termination and adjusting of priority. An Event Viewer lets the Administrator view all events as though they were being run on the host computer. The Performance Monitor displays a dynamic overview of the computer's performance (CPU and memory usage). RTM even supports remote installs, enabling a Systems Administrator to set up a service on remote machines without ever having to physically go to them. RTM adds the ability to lock/shutdown/reboot and to create processes on remote computers. *More information is available at*

http://www.protect-me.com/rtm/

A wildcard character is a keyboard character such as an asterisk (*) or a question mark (?) that is used to represent one or more characters when you are defining a filter. Wildcard characters are often used in place of one or more characters when you do not know what the real character is or you do not want to type the entire name.

Uses:

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*.

By default, DeviceLock Service is using dynamic ports for the RPC communication with the management console. The ports change every time DeviceLock Service is started, making it difficult to configure a firewall. To overcome this difficulty, you can instruct DeviceLock Service to use a fixed port. To do so, open Regedit and set the following entry:

- Key: *HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLock*
- Name: *ncacn_ip_tcp[port number]*
- Type: *REG_SZ*
- Value: *not used (can be empty)*

port number - the fixed TCP port number that you want to use for the communication between DeviceLock Service and the management console.

You should restart DeviceLock Service for the setting to take effect.

Please note that when you connect to DeviceLock Service using a fixed port, the remote install/update function is disabled, i.e. you can't install or update DeviceLock Service on remote computers without using dynamic ports.

Flush Buffers

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.

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: If you select a device with a removable media, make sure that this device has the media inserted and isn't marked as read-only.

About

Displays information about the DeviceLock version and your licenses.

Please include this information when reporting any problems to SmartLine's technical support.

Permissions

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.

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.

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.

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

  - **Write** - to enable the 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.

  - **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.

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.

Enter Network Password

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

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.

Auditing & Shadowing

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*.

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.

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 *Audit* 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.

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.

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.

The audit log stores events generated by a user's device-related activities that fall under the audit rules. 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.

When you need to force moving the audit data from the current computer to the server, use *Send Data to Server*. This function is available only if DeviceLock Enterprise Server is defined in *Service Options* and *DeviceLock Log* or *Event & DeviceLock Logs* is selected in the *Audit log type* parameter in *Service Options.*

Use *Refresh* to refresh the list of events.

To clear all events from the audit log, select *Clear*.

To filter records in this list, select *Filter*.

Audit Log Settings (Service)

Use this dialog to define a maximum log size and what Windows should do if the service's audit log becomes full.

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.

Audit Log Filter (Service)

You can filter data in Audit Log Viewer (Service) so only records that meet specific conditions are displayed in the list.

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.

To save filter's settings from the current tab (*Include* or *Exclude*) to an external file, press the *Save* button.

To load a previously saved filter settings to a current tab, press the *Load* button and select a file.

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.

Shadow Log Viewer (Service)

There is a built-in shadow log viewer that allows you to retrieve the shadow log from DeviceLock Service.

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.

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.

When you are opening the large file, you can press the *Cancel* button on the progress bar to abort the opening process. In this case the application will get only that part of the data which was received before you aborted the opening process.

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.

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. 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).

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.

View

To open the data in the built-in viewer, use *View* from the context menu.

When you are opening the large file, you can press the *Cancel* button on the progress bar to abort the opening process. In this case the viewer will show only that part of the data which was received before you aborted the opening process.

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.

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.

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.

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.

Shadow Log Filter (Service)

You can filter data in Shadow Log Viewer (Service) such that only records that meet certain conditions are displayed in the list.

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.

Media Database

In the *Media Database* dialog you can add new media to the database and edit existing records.

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.

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.

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.

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.

Shadow File Viewer

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.

Press the *Save* button to save the data from the viewer to an external file.

Local Connections

When the 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.

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 the management console. To avoid this conflict you must first delete your existing connection.

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 the management console. In this case you need to run the 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 the management console under another user.

Security Settings

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.

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.

USB Devices Database

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

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.

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.

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

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.

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.