Help Contents

DeviceLock Management Console and Group Policy Manager
for Windows NT 4.0/2000/XP and Windows Server 2003

General Information:

- Introduction
- License
- How To Register
- Technical Support
- Frequently Asked Questions
- SmartLine's Software

- DeviceLock Group Policy Manager
  - Standard GPO Inheritance Rules in Organizational Units

- DeviceLock Management Console
- DeviceLock Service Settings Editor

Dialogs & Views:

- Service Options
  - DeviceLock Administrators
  - Auditing & Shadowing
  - Anti-keylogger
  - Encryption
  - PGP Whole Disk Encryption
  - Lexar SAFE PSD

- Devices
  - Permissions
  - Auditing & Shadowing
  - USB Devices White List
  - USB Devices Database
  - Media White List
  - Media Database
  - Security Settings

- Audit Log Viewer
  - DeviceLock Log Settings
  - Audit Log Filter
- Shadow Log Viewer (Service)
  - Shadow File Viewer
  - Shadow Log Filter
- Server Options
  - Server Administrators
- Shadow Log Viewer (Server)
  - Shadow File Viewer
  - Deleted Shadow Data Log
  - Shadow Log Filter
- Server Log Viewer
  - Server Log Filter
- About

DeviceLock Group Policy Manager

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.
- 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.

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.

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*.

DeviceLock Management Console

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.

DeviceLock Service Settings Editor

DeviceLock Service Settings Editor is using for creating and modifying external XML files with settings, permissions, audit and shadowing rules for DeviceLock Service.

There is almost no difference between the procedures for defining policies via DeviceLock Management Console versus via DeviceLock Service Settings Editor.

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.

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.

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

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

Standard GPO Inheritance Rules in Organizational Units

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.

Any unconfigured settings are ignored during application, so the GPO comes into play only when settings have actually been set.

Read more in Standard GPO Inheritance Rules in Organizational Units

SmartLine DeviceLock View

You can use the context menu available via a right mouse click on the *SmartLine DeviceLock* tree item:

- *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. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

- *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, DeviceLock Group Policy Manager or DeviceLock Service Settings Editor. Since the signature is not validated at this step, it can be either a signed or non-signed file. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

- *Save Service Settings* - exports all settings from the currently connected DeviceLock Service to an external XML file. Later this file can be loaded via DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor. 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. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

- *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. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

- *Certificate Generation Tool* - runs the special tool that allows you to generate DeviceLock Certificates.

- *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.

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

Service Options View

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.

- *DeviceLock Administrators* - allows you to define the list of user accounts with administrative access rights to DeviceLock Service.

- *Auditing & Shadowing* - allows you to tune up auditing and shadowing for DeviceLock Service.

- *Anti-keylogger* - allows you to tune up DeviceLock's ability to detect hardware keyloggers and to define what DeviceLock Service should do when a keylogger is found.

- *Encryption* - allows you to tune up DeviceLock's ability to detect disks (USB flash drives and other removable media) encrypted by third-party products and apply special "encrypted" permissions to them..

- *USB/FireWire blocked message* - allows you to define a custom message to be displayed to users when an attempt made to plug in a USB or FireWire device is denied.

- *Expired message* - allows you to 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.

- *DeviceLock Enterprise Server(s)* - allows you to specify the name or IP address of the DeviceLock Enterprise Server's computer.

- *Log Policy changes and Start/Stop events* - allows you to 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.

- *DeviceLock certificate* - allows you to install or remove a DeviceLock Certificate (the public key).

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

  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.

Available only in DeviceLock Management Console and DeviceLock Service Settings Editor.

- *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.

  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.

  Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

- *Fast servers first* - 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.

- *Traffic priority* - allows you to define bandwidth limits for sending audit and shadow logs from DeviceLock Service to DeviceLock Enterprise Server.

  This parameter can be changed 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.

In DeviceLock Group Policy Manager and DeviceLock Service Settings Editor*,* if you want to reset these parameters to the unconfigured state, select *Undefine* from the context menu.

DeviceLock Administrators View

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

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

In DeviceLock Group Policy Manager and DeviceLock Service Settings Editor*,* if you want to reset this parameter to the unconfigured state, select *Undefine* from the context menu.

Devices View

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

In DeviceLock Management Console you can 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.

Permissions View

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

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.

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.

In DeviceLock Group Policy Manager and DeviceLock Service Settings Editor*,* if you want to reset permissions to the unconfigured state, select *Undefine* from the context menu.

Auditing & Shadowing View

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

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 and then can be transferred to DeviceLock Enterprise Server to store it in the SQL database.

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.

In DeviceLock Group Policy Manager and DeviceLock Service Settings Editor*,* if you want to reset audit rules to the unconfigured state, select *Undefine* from the context menu.

White Listed Devices View

Here you can see the list of white listed devices that were assigned to a certain account (user or group).

You can use the context menu, available via a right mouse click:

- *Reinitialize* - check this flag to to force the white listed device to reinitialize (replug) when the new user is logged in. 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.

- *Control As Type* - when this 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 this 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.

- *Delete* - deletes the device from the white list of a certain account.

- *Delete User* - deletes the user or group from the white list with all the devices assigned to it.

- *Manage* - opens the dialog where you can add devices from the *USB Devices Database* to the white list.

- *Load* - loads a previously saved white list from an external file.

- *Save* - saves the white list to an external file.

- *USB Devices Database* - opens the dialog where you can add devices to the *USB Devices Database* list, making them available for adding to the white list.

Security Settings View

There is a list of additional security parameters that affect permissions and audit rules for some devices types.

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.

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.

In DeviceLock Group Policy Manager and DeviceLock Service Settings Editor, if you want to reset these parameters to the unconfigured state, select *Undefine* from the context menu.

USB Devices White List View

Here you can see the list of accounts (users and groups) that were added to the devices white list. Devices in the white list can be defined individually for every user and group.

You can use the context menu available via a right mouse click:

- *Delete User* - deletes the user or group from the white list with all the devices assigned to it.

- *Manage* - opens the dialog where you can add devices from the *USB Devices Database* to the white list.

- *Load* - loads a previously saved white list from an external file.

- *Save* - saves the white list to an external file.

- *Undefine* - resets the entire white list to the unconfigured state. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

- *USB Devices Database* - opens the dialog where you can add devices to the *USB Devices Database* list, making them available for adding to the white list.

Media White List View

Here you can see the list of accounts (users and groups) that were added to the media white list. Media in the white list can be defined individually for the every user and group.

You can use the context menu available via a right mouse click:

- *Delete User* - deletes the user or group from the white list with all the media assigned to it.

- *Manage* - opens the dialog where you can add media from the *Media Database* to the white list.

- *Load* - loads a previously saved white list from an external file.

- *Save* - saves the white list to an external file.

- *Undefine* - resets the entire white list to the unconfigured state. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

- *Media Database* - opens the dialog where you can add media to the *Media Database* list, making them available for adding to the white list.

White Listed Media View

Here you can see the list of white listed media that were assigned to a certain account (user or group).

You can use the context menu, available via a right mouse click:

- *Delete* - deletes the media from the white list of a certain account.
- *Delete User* - deletes the user or group from the white list with all the media assigned to it.
- *Manage* - opens the dialog where you can add media from the *Media Database* to the white list.
- *Load* - loads a previously saved white list from an external file.
- *Save* - saves the white list to an external file.
- *Media Database* - opens the dialog where you can add media to the *Media Database* list, making them available for adding to the white list.

DeviceLock Enterprise Server View

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.

- *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.

- *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.

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

Server Options View

These parameters allow you to tune up the DeviceLock Enterprise Server configuration.

- *Server Administrators* - allows you to define the list of user accounts with administrative access rights to DeviceLock Enterprise Server.

- *DeviceLock Certificate* - allows you to install or remove a DeviceLock Certificate (the private key).

- *Service startup account* - allows you to define 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.

- *TCP port* - allows you to instruct DeviceLock Enterprise Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall.

- *Database name* - allows you to specify the name of the database in SQL Server that will be used to store the DeviceLock Enterprise Server data.

- *Connection type* - allows you to define a connection type for SQL Server.

- *SQL Server name* - allows you to define the name of SQL Server.

- *Data Source Name* - allows you to specify the predefined system data source.

- *SQL Server login* - allows you to define the SQL user name (login).

- *Store path* - allows you to define where on the disk binary data must be located.

- *Store shadow files in SQL Server* - allows you to define where to store binary data: in SQL Server or on the disk.

- *DeviceLock license(s)* - allows you to load your DeviceLock licenses.

- *Stream compression* - by enabling this 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 available by a right mouse click on every parameter to open a dialog where you can change this parameter. Alternatively, you can double-click on the parameter to open its dialog.

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.

Server Administrators View

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

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

Shadow Log Viewer (Server)

The shadow log viewer allows you to retrieve the shadow log stored on DeviceLock Enterprise Server.

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.

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.

To define a maximum log size and instruct DeviceLock Enterprise Server regarding what it should do if the shadow log becomes full, select *Settings* from the context menu available with a right mouse click.

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.

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 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.

To clear all records from this log, select *Clear* from the context menu or press the appropriate button on the toolbar.

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.

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.).

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*").

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.

To define a maximum log size and instruct DeviceLock Enterprise Server regarding what it should do if the server's log becomes full, select *Settings* from the context menu available with a right mouse click.

Auditing & Shadowing View

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

- *Local storage directory* - allows you to define where on the local disk shadowed data is stored.

- *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).

- *Cleanup files older than (days)* - allows you to define the number of days that should pass before shadowed data can be automatically deleted from the local storage.

- *Local storage quota (%)* - allows you to define a disk quota for shadowed data.

- *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.

- *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.

- *Audit log type* - allows you to define what log should be used to store audit records.

In DeviceLock Group Policy Manager*,* if you want to reset these parameters to the unconfigured state, select *Undefine* from the context menu.

DeviceLock Service View

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

You can use the context menu available via a right mouse click on the *DeviceLock Service* tree item:

- *Connect* - connects to any computer that you specify.

- *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, DeviceLock Group Policy Manager or DeviceLock Service Settings Editor. 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 loaded via DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor. 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.

- *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.

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

Anti-keylogger View

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

- *Treat any USB hub as keylogger* - if enabled, instructs 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.

- *PS/2 keyboard scrambling* - allows you to 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.***

- *Notify user* - allows you to define a custom message to be displayed to users when DeviceLock Service detects hardware USB keyloggers.

- *Log event* - if enabled, instructs DeviceLock Service to write an event to the audit log when the hardware USB keylogger is detected.

- *Block keyboard* - if enabled, instructs DeviceLock Service to block the keyboard connected to the hardware keylogger when it is detected.

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.

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.

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.

To define a maximum log size and instruct DeviceLock Enterprise Server regarding what it should do if the audit log becomes full, select *Settings* from the context menu available with a right mouse click.

Encryption View

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 the removable storage devices:

- PGP® Whole Disk Encryption

- Lexar™ SAFE PSD S1100

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.

PGP Whole Disk Encryption View

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.

If you don't want to allow DeviceLock Service to detect the third-party encryption product and to apply special "encrypted" permissions to storage devices encrypted by it, disable the *Integration* flag.

For more information on PGP® Whole Disk Encryption, please visit PGP's website: www.pgp.com/products/wholediskencryption/index.html.

Lexar SAFE PSD View

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.

If you don't want to allow DeviceLock Service to detect the third-party encryption product and to apply special "encrypted" permissions to storage devices encrypted by it, disable the *Integration* flag.

For more information on Lexar™ SAFE PSD S1100, please visit Lexar's website: www.lexar.com/enterprise/safe_psd_S1100.html.

Local storage directory

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

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).

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.

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

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.

Using the semicolon (;) as a separator you can specify several DeviceLock Enterprise Servers to uniformly spread the network load. At its startup, DeviceLock Service randomly 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.

Local storage quota (%)

You can define a disk quota for shadowed data.

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).

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.

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.

Traffic Priority

Use this dialog 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.

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.

Audit Log Filter (Server)

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

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.

Audit Log Type

Use this dialog to define what log should be used to store audit records.

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.

Select Computer

Use this dialog to select the computer you want to manage.

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

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.

DeviceLock Administrators

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.

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.

Blocked/Expired 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. Also, 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.

To enable the "USB/FireWire blocked 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.

To enable the "Expired 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.

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

DeviceLock Certificate

Use this dialog to install or remove a DeviceLock Certificate.

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.

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 keylogger.

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.

Test Connection

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*.

Log On As and Connection Settings

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.

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.

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.

Server Administrators and DeviceLock Certificate

Server Administrators

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.

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.

DeviceLock Licenses

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.

Database and SQL Server Settings

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*.

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*.

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.

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.

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.

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.

Log Settings (Server)

Use this dialog to define a maximum log size and what DeviceLock Enterprise Server should do if the log becomes full.

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 or shadow log and there is nothing to delete then DeviceLock Enterprise Server doesn't remove data from remote users' computers. This prevents you from loosing the data due to lack of space in the log. When some space becomes available in the log, DeviceLock Enterprise Server moves the remaining data from users' computers to this log. It's best to avoid accumulating shadowed or audit 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.

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 audit records in this way, we recommend that you monitor DeviceLock Enterprise Server's log   on a periodic basis and watch for warning messages there.

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.

Shadow Log Filter (Server)

You can filter data in Shadow Log Viewer (Server) and Deleted Shadow Data Log so that only records that meet specified conditions are displayed in the list.

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.

Finish

If there are no errors, press the *Finish* button to apply changes and close the wizard.

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 old format, you should upgrade the database* - the database specified in the *Database name* parameter already exists but is outdated.

- *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 in **Test Connection** may be displayed here as well.

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