# Help Contents

## DeviceLock Enterprise Manager (DLEM)

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

General Information:



Dialogs & Windows:



Plug-ins:

# Open Project

To open the Open Project window, select *Open Project* from the *File* menu.

You can group saved projects by the date when they were scanned and by the type of information they contain. Select *Group by Plug-ins* or *Group by Date* from the context menu or press appropriate buttons on the *Project* toolbar.

To open a saved project, select it from the list and press the *Open Project* button on the *Project* toolbar. Using Ctrl and/or Shift you can select and open several projects simultaneously.

Select *Filter* from the context menu or press the appropriate button on the *Project* toolbar to open the **Filter Projects** dialog and filter existing projects.

You can compare two files, which were saved as projects. Highlight two projects you would like to compare (use Ctrl or/and Shift to highlight two projects simultaneously) and then select *Compare* from the context menu or press the appropriate button on the *Project* toolbar. ***Please note that you may select only two projects and both projects must be of the same type.*** For more information about projects comparing, see **Compare Wizard**.

To delete a project from the disk, select it from the list and press the *Delete Project(s)* button on the *Project* toolbar. Using Ctrl and/or Shift you can select and delete several projects simultaneously.

# Plug-ins: Overview

DeviceLock Enterprise Manager has a flexible plug-in based architecture that allows you to plug in the necessary module on demand. DeviceLock Enterprise Manager loads the plug-ins on startup from the *Plugins* subdirectory, which is located in the main DeviceLock Enterprise Manager directory.

All information that you receive from the plug-in can be saved to the external files and loaded into DeviceLock Enterprise Manager when you need it.

To save the data as a project, you can select *Save Project* from the *File* menu or press the appropriate button on the *Main* toolbar (see **Open Project**).

Another way to save scanned information in the format of DeviceLock Enterprise Manager is select *Save As* from the *File* menu. To load previously saved files, you can select *Open* from the *File* menu or press the appropriate button on the *Main* toolbar.

If you need to pass scanned information to an external application, you can export it into the text file and then import it to this application. To export data into the text file, select *Save As* from the *File* menu and then select the file's type from the *Save as type* combo box. DeviceLock Enterprise Manager supports the export into MS Excel and two formats of text files - *Tab Delimited* (TXT) and *Comma Delimited* (CSV).

DeviceLock Enterprise Manager includes following plug-ins:

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

# Compare Wizard

DeviceLock Enterprise Manager provides a very useful and intuitive Wizard to compare two previously saved projects. To open Compare Wizard, select *Compare* from the *File* menu.

There are three simple steps, which enable you to compare two files using Compare Wizard:

- The first step is to select the files you wish to compare. **More...**

  If you wish to compare two files, which were saved as projects, it is a good idea to use the special feature of the **Open Project** window.

- The second step is to select the columns you wish to include in the compare process. **More...**

- The third and final step is to start the compare process. Press the *Finish* button to compare two selected files with each other.

DeviceLock Enterprise Manager displays the compare result in a separate window in the form of a tree exactly as it displays information received from a plug-in during network scan.

There are two buttons on the *Compare* toolbar, which help you to easily navigate through the compare result. Press the **<** button to highlight the previous record in the compare result that contains changes. Press the **>** button to highlight the next record in the compare result that contains changes.

You can also save the compare result to an external DeviceLock Enterprise Manager file or export it into the text file (*TXT* and *CSV*). Select *Save As* from the *File* menu or press the appropriate button on the *Main* toolbar to save or export the compare result.

As with any other DeviceLock Enterprise Manager file, the saved compare result can be opened and loaded to DeviceLock Enterprise Manager. To load the previously saved compare result, you can select *Open* from the *File* menu or press the appropriate button on the *Main* toolbar. You will need to specify a file you wish to open. You can load files of DeviceLock Enterprise Manager type only.

To close this Wizard, use either the *Close* button or your keyboard's *Escape* Key.

# Set Service Settings

First of all you have to prepare the policy you want to deploy.

If there are no files in the list, then you can either create an empty file by pressing the *New* button or add an existing file by pressing the *Add* button.

Then highlight the file in the list and press the *Edit* button to open DeviceLock Service Settings Editor. DeviceLock Service Settings Editor is used for creating and modifying external XML files with settings, permissions, audit and shadowing rules for DeviceLock Service.

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.

When finished modifying the policy, select its file by enabling the checkmark near by the file's name in the list. Then press the *OK* button to close the configuration dialog.

# Scan Network

The *Scan Network* dialog allows you to select computers in your network and the action (install or remove DeviceLock Service, set permissions, and so on) which should be performed for these computers.

To open the *Scan Network* dialog, select *Scan Network* from the *File* menu or press the appropriate button on the *Main* toolbar. If the *Show this dialog at next startup* flag is checked, the *Scan Network* dialog will open automatically each time DeviceLock Enterprise Manager is started.

There are three simple steps, which enable you to manage DeviceLock Services across the network.

1. The first step is to select the computers to be processed.

You can use the context menu, available by right clicking, to select/deselect necessary items (computers types, domains, or computers).

DeviceLock Enterprise Manager provides several flexible ways to select network computers.

§ Network computers can be selected by their types.

Each type represents all of the computers belonging to the category:

- *Primary Domain Controller* - a primary domain controller.
- *Backup Domain Controller* - a backup domain controller.
- *Microsoft SQL Servers* - any server running with Microsoft SQL Server.
- *Terminal Servers* - any server where Terminal Services are running.
- *Stand Alone Servers* - any server that is not a domain controller.
- *Cluster Servers* - server clusters available in the domain.
- *Print Servers* - any computer that is sharing the print queue.
- *NT Workstations* - any Windows NT/2000/XP workstation.

There are two ways to choose the type of computers:

1. *Types* - you select the network domain and then select types of computers

which must be processed in this domain.

2. *Domains* - you select the type of computer and then select network domains where computers of the selected type must be processed.

§ Network computers can also be selected by their names.

There are several ways to choose computers by name:

1. *Organizational Units* - you browse Active Directory organizational units (OUs) and select computers, which must be processed.

2. *Computers* - you browse the network tree and select computers.

3. *LDAP* - you browse the LDAP (Lightweight Directory Access Protocol) tree and select computers from the directory. To configure a connection to the LDAP server, press the **...** button.

4. *From File* - you load a predefined list of computers from the external text file and then select the computers. To open an external file, press the **...** button. A text file must contain each computer's name or IP address on separate lines and can be either Unicode or non-Unicode.

2. The second step is to select a plug-in to process the network computers selected on the first step.

To select/deselect plug-ins, you can use the context menu available with a right mouse click.

To define parameters for the selected plug-in, use the *Settings* button below the plug-ins list. If the plug-in doesn't have additional parameters, this button is disabled.

Tasks are passed to the plug-in by DeviceLock Enterprise Manager.

The plug-in performs the task and returns the information to DeviceLock Enterprise Manager. Upon receipt of a plug-in's information, DeviceLock Enterprise Manager displays it in a separate window.

3. Once you have selected computers and the appropriate plug-in, the final step is starting the scan process. Press the *Scan* button to initiate the process.

Right after the scan process is initiated, you can start to explore the information that is already received from the plug-in.

Because the scan process runs in a separate thread, you do not need to wait until all computers are finished being scanned. You can also perform other tasks in the DeviceLock Enterprise Manager interface.

There are only a few things which you cannot do while the scan is running - you cannot close DeviceLock Enterprise Manager and you cannot run another scan process.

If, for some reason, you wish to abort the active scan process, you can select *Stop Scan* from the *File* menu or press the appropriate button on the *Main* toolbar. The scan process will be aborted as soon as a plug-in returns control to DeviceLock Enterprise Manager.

# Filter Data

DeviceLock Enterprise Manager provides very sophisticated data filtering, enabling you to narrow a scan or comparison result to only those data complying to your specific conditions.

To open the *Filter Data* dialog, you can select *Filter* from the *View* menu or press the appropriate button on the *Main* toolbar. ***Please note that the window with a scan or comparison result must be active to use data filtering.***

§ The *Field* column contains all the fields available in the scan or comparison result that you want to filter. You can define the *AND-OR* logic for each field separately:

*AND* - includes only those records that comply with all defined conditions. For example, *Process = "explorer.exe" AND PID = 3764* retrieves all data where both the *Process* is "*explorer.exe*" and *PID* is *3764*. It does not include data where the *Process* is "*explorer.exe*" and *PID* is not *3764* or where *PID* is *3764* but *Process* is not "*explorer.exe*".

*OR* - includes all records that comply with at least one condition. For example, *Process = "explorer.exe" OR PID = 3764* retrieves all data having one or both conditions, where Process = "*explorer.exe*" (no matter what *PID* is) or where *PID* is *3764* (no matter what *Process* is).

§ The *Condition* column contains a list of logical operations that can be performed on a selected field. You can select only one logical operation for each field. DeviceLock Enterprise Manager supports two groups of logical operations, those for *string data* and *non-string data*.

Logical operations that can be performed on *string data* (*target string* being the string you specify, e.g. "*Explorer.exe*"):

- *Is (exactly)* - selects only data having fields with strings that are identical to the target string.
- *Includes* - selects only data having fields with strings that include a defined target string.
- *Is not* - selects only data having fields with strings that are different from the target string.
- *Not includes* - selects only data having fields with strings that do not include the target string.

- *Empty* - selects only data having fields with empty strings.

- *Not Empty* - selects only data having fields with strings that are not empty.

- *Regular expression* - selects only data having fields with strings matching an expression. The expression may contain wildcards (e.g. "*explorer**").

If you want to narrow the search to the string's exact case (e.g. "*Explorer.exe*" is different from "e*xplorer.exe*"), check the *Match case* flag. Otherwise, case is ignored (e.g. "*Explorer.exe*" and "*explorer.exe*" are identical).

Logical operations that can be performed on *non-string data*:

- *Equal to (=)* - selects data having field values that are identical to the defined value (e.g. *PID = 3764*).
- *Greater than (>)* - selects data having field values that are greater than the defined value (e.g. *PID > 4*).

- *Less than (<)* - selects data having field values that are less than the defined value (e.g. *PID < 4*).

- *Not Equal to (!=)* - selects data having field values that are different from the defined value (e.g. *PID != 0*).

- *Between (in)* - selects data having field values that are between the two defined values (e.g. *PID in 3000-4000*).

- *Not Between (out)* - selects data having field values that are outside of the two defined values (e.g. *PID out 3000-4000*).

- *Regular expression* - selects only data having field values matching an expression. The expression may contain wildcards (e.g. *300**).

If you don't want to perform a logical operation for a field, select *Not defined* from the list of logical operations.

§ *Value* columns contain user-defined arguments. The second *Value* column is used only when the *Between (in)* or *Not Between (out)* logical operation is selected. For all other logical operations only the first *Value* column is needed.

After you define a filtering expression, press the *Apply* button to start the filtering process.

You can save a filtered result in an external *ANM* file or export it to a text file (TXT and CSV) or MS Excel. Select *Save As* in the *File* menu or press the appropriate button on the *Main* toolbar to save or export the filtered result.

As with any other DeviceLock Enterprise Manager file, filtered data can be opened and loaded into DeviceLock Enterprise Manager. To load a file, select *Open* in the *File* menu or press the appropriate button on the *Main* toolbar. Then specify the file you wish to open. You can only load files that were previously saved by DeviceLock Enterprise Manager.

# Select Columns

Shows the list of columns that you can display in the current plug-in's window. If a column is checked, it will be displayed in the plug-in's window.

Press the *OK* button to close this dialog and save any changes you have made.

To close this dialog without saving changes, use either the *Cancel* button or your keyboard's *Escape* Key.

# Windows

Lists all of the currently open windows.

You can activate a window by either double-clicking your selection in the *Select Window* list, or by selecting a window and then clicking the *Activate* button.

To close a selected window, press the *Close Window(s)* button.

Using Ctrl and/or Shift you can select several windows simultaneously.

To close this dialog, use either the *Cancel* button or your keyboard's *Escape* Key.

# Filter Projects

To open the Filter Projects dialog, you can select *Filter* from the context menu or press the appropriate button on the *Project* toolbar. ***Please note that the Open Project window must be active to use projects filtering.***

You can filter existing projects by the type of information they contain (*Audit Log Viewer*, *Report Permissions/Auditing*, etc.), by their type (*scan result*, *compare result* or *filter result*), and by their date.

After you define a filtering expression, press the *Apply* button to start the filtering process. To close the Filter Projects dialog, use the *Cancel* button.

# Select Columns To Compare

DeviceLock Enterprise Manager compares only those columns, which you have selected. If you need to exclude one column from the compare process, you have to move it from the *Included columns* list to the *Excluded columns* list. Excluded columns will be visible in the compare result but the values they contain are ignored and don't affect the compare result.

By default, the compare result contains only records, which are different in the two files being compared. If you would like to see all of the records (even unchanged records), you can clear the *Show changes only* checkbox.

To include names of the network domains in the compare process, you can clear the *Ignore domains* checkbox. When the *Ignore domains* checkbox is checked, DeviceLock Enterprise Manager ignores domains and only compares computers and the information those computers contain.

# Set Credentials

Credentials consist of a user name and password pair used to authenticate to computers scanned. Enter the username and password for an account with administrative permission to the selected computer or network domain.

- If you enter *Domain\User*, DeviceLock Enterprise Manager will use the domain account rights.
- If you enter *TargetComputer\User*, DeviceLock Enterprise Manager will use the target's local account rights.
- If you do not enter a computer or domain name, DeviceLock Enterprise Manager tries to use *LocalComputer\User*. If this is not successful, it will next attempt to use *RemoteComputer\User*.

# Credentials

You may assign credentials to individual computers and/or to network domains. To add credentials, use the *Set* item. To delete alternative credentials, use the *Clear* item.

Credentials consist of a user name and password pair used to authenticate the computers processed. By default, DeviceLock Enterprise Manager uses your currently logged on credentials to automatically log in and process the target computer(s). If the current logged-in user credentials do not have administrative rights on all of the target computers, you need to enter alternate credentials. DeviceLock Enterprise Manager will use these alternate credentials to automatically login to the target computers.

In all cases, credentials are stored with encryption techniques and are not available to anyone except the user with administrative privileges.

Press the *Add* button to add new credentials. To change existing credentials, highlight the record in the list and press the *Change* button.

To delete credentials, highlight the record in the list and press the *Delete* button. Using *Ctrl* and/or *Shift* you can highlight and remove several records simultaneously.

# Log Window

The Log Window is used to display useful information about ongoing activity as well as diagnostic and error messages. To show/hide the Log Window, use *Log Window* from the *View* menu.

The Log Window contains two log lists: *Information* and *Warnings/Errors*.

You can limit the number of records log lists retain by setting the maximum number of messages with *Set Message Count* from the context menu.

By default, log lists scroll so that they always show the most recent message. To disable auto-scrolling, uncheck the *Keep Last Message* in *View* item from the context menu.

To save all the messages currently in the log list to a file, select *Save As* from the context menu. DeviceLock Enterprise Manager then copies all the currently available messages from the active log list to the file that you specify.

# Select Domain/Computer

Select the computer or domain from the network tree and press the *OK* button to confirm your selection.

Also, you can type the computer or domain name in the *Name* box above the network tree.

# Tip of the Day

Tip of the Day contains a large number of tips of interest to both novices and experts. If you leave it turned on it will teach you something new every time you start DeviceLock Enterprise Manager.

You can quickly close Tip of the Day by pressing *Escape*. To see more tips, click the *Next Tip* button.

# Set Port

You can instruct DeviceLock Enterprise Manager to use a fixed port, making it easier to configure a firewall. To do so, use *Set port* from the context menu.

By default, DeviceLock Enterprise Manager uses dynamic ports for RPC communication with DeviceLock Service. However, if DeviceLock Service is configured to accept connections on a fixed port, select the *Specify port* parameter.

To use the dynamic ports binding, select *Dynamic* ports.

DeviceLock Service can be configured to use either a fixed port or dynamic ports during the installation process.

If you need to change the port configuration when DeviceLock Service is already installed, use the Install service plug-in.

# LDAP Settings

Use this dialog to configure a connection to the LDAP server.

- *Host* - the name or the IP address of the LDAP server to connect to.

- *Port* - the TCP port on which the LDAP server accepts connections. The default port is 389.

- *Protocol version* - the LDAP protocol version. Some servers are not fully compatible with the LDAP v.3 protocol and LDAP requests require certain adjustments for correct communication with such servers. Selecting *Version 2* makes sure that the server requests are adjusted according to the LDAP v.2 protocol requirements.

- *Base DN* - the starting point for you to browse the directory tree. You must use the LDAP string representation for distinguished names (for example, *cn=qa,o=SMARTLINE,c=US*). Leave the *Base DN* field blank to start browsing from the root.

  By pressing the *Fetch* button, you can get all the published naming contexts.

- *User DN* - the distinguished name (DN) of the directory user that allows connection to the directory. You must use the LDAP string representation for distinguished names (for example, *cn=admin,o=SMARTLINE,c=US*).

- *Password* - the user's password.

# Set Message Count

You can use this dialog to limit the number of records the Log Window list retains. Each Log Window list (*Information* and *Warnings/Errors*) has its own maximum number of records.

The number you specify determines the maximum number of records that DeviceLock Enterprise Manager will maintain in its buffer at any given time. After a defined number of lines have accumulated, the oldest records become unavailable.

# Select Projects To Compare

Select the first file and then select the second file by pressing **...** buttons.

***Please note that you can compare files of the same type only.*** For example, you cannot compare information received from the *Audit Log Viewer* plug-in with information from the *Report Permissions/Auditing* plug-in.

When you have selected two files, press the *Next* button to go to the next **Compare Wizard**'s page.

# Report PnP Devices Settings

Use this dialog to select the information you want to include in the reports generated by the *Report PnP Devices* plug-in.

- *Report Connected Devices Only* - check this flag to report only those devices that are currently connected to the computer. Otherwise, you will see all devices that were ever connected to the computer.

- *Report FireWire Devices* - check this flag to report devices that are plugging into the FireWire port.

- *Report PCMCIA Devices* - check this flag to report devices that are plugging into the PCMCIA slot.

- *Report USB Devices* - check this flag to report devices that are plugging into the USB port.

# Install Options

Use this dialog to specify the path to the DeviceLock Service executable files (*dlservice.exe* and *dlservice_x64.exe*) for the *Install Service* plug-in. Press **...** buttons and locate *dlservice.exe* and *dlservice_x64.exe* files.

Also, here you can change the port configuration for DeviceLock Service. To use the dynamic ports binding, select *Dynamic* ports. To instruct DeviceLock Service to use a fixed port, select the *Specify port* parameter.

# Report Permissions

Use this dialog to select the information you want to include in the reports generated by the *Report Permissions/Auditing* plug-in.

- *Report Available Devices Only* - check this flag to report permissions and audit rules for only those devices currently available on the computer. Otherwise, you will see permissions and audit rules for every type of device that DeviceLock supports.

- *Report USB White List* - check this flag to include information about white listed devices.

- *Report Media White List* - check this flag to include information about white listed media.

- *Report Security Settings* - check this flag to report what parameters are disabled via Security Settings.

- *Report Auditing & Shadowing* - check this flag to report audit and shadowing rules that have been set.

  Also when this flag is checked, you receive information about whether the *Log Policy changes and Start/Stop events* parameter is enabled in *Service Options*.

- *Report Enabled Auditing & Shadowing Only* - check this flag to exclude devices for which audit and shadowing rules are disabled from the report.

  This flag is available only if *Report Auditing & Shadowing* is checked.

- *Report DeviceLock Administrators* - check this flag to report accounts that can manage DeviceLock Service or view its settings and logs.

This report always includes information about an installed DeviceLock Certificate. Also, it always shows when the *Use Group Policy* parameter is enabled in *Service Options*.

# Plug-ins: Audit Log Viewer

The *Audit Log Viewer* plug-in retrieves DeviceLock's audit log from the computer's local Windows event logging subsystem.

To define a maximum log size and what Windows should do if the audit log becomes full, use *Audit Log Settings* from the context menu.

To clear all events from the audit log, select *Clear Audit Log* from the context menu.

For more information, please read the **Audit Log Viewer (Service)** section of this manual.

# Plug-ins: Report PnP Devices

The *Report PnP Devices* plug-in generates a report displaying the USB, FireWire and PCMCIA devices currently connected to computers in the network and those that were connected.

The columns are defined as follows:

- *Description* - the description of the device provided by its vendor.
- *Device Information* - the additional information about the device provided by its vendor.
- *Connected to* - the interface where the device is connected (*USB*, *FireWire* or *PCMCIA*).
- *Class* - the class of the device provided by Windows.
- *Class description* - the description of the device's class provided by Windows.
- *Present* - indicates whether the device is currently connected or not (*Yes* or *No*).
- *DeviceID* - the unique identification string of the device provided by its vendor.
- *Driver* - the name of the driver that is controlling this device.

You can add reported USB devices to the USB Devices Database using the context menu available via a right mouse click.

Before you can use this plug-in, you should select the information you want to include in reports. You can do this by pressing the *Settings* button below the plug-ins list in the *Scan Network* dialog.

# Plug-ins: Report Permissions/Auditing

The *Report Permissions/Auditing* plug-in generates a report concerning settings, permissions and audit rules that have been set for DeviceLock Services across the network.

Before you can use this plug-in, you should select the information you want to include in reports. You can do this by pressing the *Settings* button below the plug-ins list in the *Scan Network* dialog.

# Plug-ins: Install Service

The *Install Service* plug-in installs or updates DeviceLock Service on computers.

Before you can use this plug-in, you should specify the path to the DeviceLock Service executable files (*dlservice.exe* and *dlservice_x64.exe*). You can do this by pressing the *Settings* button below the plug-ins list on the *Scan Network* dialog.

# Plug-ins: Uninstall Service

The *Uninstall Service* plug-in removes DeviceLock Service and all its settings and components from computers.

If the user under which the DeviceLock Enterprise Manager is connecting to the computer doesn't have full administrative access to DeviceLock Service, the plug-in will not be able to remove the service.

Likewise, an error occurs when the user doesn't have local administrative privileges on the computer where DeviceLock Service is running.

# Plug-ins: Shadow Log Viewer

The *Shadow Log Viewer* plug-in retrieves the shadow log from DeviceLock Service.

Use the context menu available by a right mouse click to access all this plug-in's functions.

For more information, please read the **Shadow Log Viewer (Service)** section of this manual.

# Plug-ins: Set Service Settings

The *Set Service Setting* plug-in reads the policy (settings, permissions, audit and shadowing rules) from the external XML file and deploys it to DeviceLock Services across the network.

Before you can use this plug-in, you should define settings, permissions and/or audit rules that you want to deploy. You can do this by pressing the *Settings* button below the plug-ins list in the *Scan Network* dialog.