Руководство Пользователя

DeviceLock®

ЗАО “Смарт Лайн Инк”

Содержание

Использование Руководства

Использование руководства подразумевает, что вы знакомы с основными действиями типа клик, правый клик, двойной клик мышью и основами управления установленной операционной системой. Руководство также подразумевает, что вы имеете базовые понятия о настройке локальной сети. Настоятельно рекомендуем очень внимательно прочитать это руководство.

В руководстве используются следующие условные обозначения:

- *Italics* для имен файлов, путей к ним, кнопок, меню и пунктов меню.
- ***Bold Italics*** для заметок и комментариев.
- Объединение наименований клавиш клавиатуры знаком плюс означает, что их надо нажимать одновременно. Например: нажмите Ctrl+Alt+Delete для того, чтобы перезагрузить компьютер.

1. Краткий Обзор

1.1 Основная информация

Для защиты и администрирования компьютерной сети компании важно предотвратить запись информации на сменные носители и установку с них ненужных программ.

При помощи DeviceLock администратор компьютера или домена может контролировать доступ пользователей к дисководам, DVD/CD-ROM'ам, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM и LPT-портам.

Кроме функции контроля доступа, DeviceLock позволяет осуществлять протоколирование и аудит использования устройств на локальном компьютере как отдельными пользователями, так и группами. Для хранения записей аудита DeviceLock использует стандартный журнал Windows, что позволяет просматривать их как с помощью стандартной программы просмотра событий, так и встроенного средства.

DeviceLock поддерживает функцию теневого копирования – возможность сохранять точную копию данных, копируемых пользователем на внешние устройства хранения информации и передаваемых через COM и LPT-порты. Точные копии всех файлов и данных сохраняются в SQL-базе данных. Теневое копирование, как и аудит, может быть задано для отдельных пользователей и групп пользователей.

Кроме того, теневое копирование DeviceLock совместимо с библиотекой программного обеспечения, поддерживаемой национальным институтом стандартов и технологий США, а также с базой данных Hashkeeper, созданной и поддерживаемой министерством юстиции США. Данные теневого копирования могут быть проверены на вхождение в базы данных известных файлов, что позволяет их использовать в компьютерной криминалистике. Такие базы данных содержат цифровые "отпечатки" множества известных файлов (файлы операционных систем, прикладного программного обеспечения и т.п.).

Вы можете создать ваши собственные базы данных цифровых "отпечатков" (поддерживаются алгоритмы SHA-1, MD5 и CRC32) конфиденциальных файлов и затем использовать их для выявления фактов копирования пользователями этих конфиденциальных файлов.

За дополнительной информацией об использовании DeviceLock с базами данных цифровых "отпечатков" обращайтесь в службу технической поддержки DeviceLock.

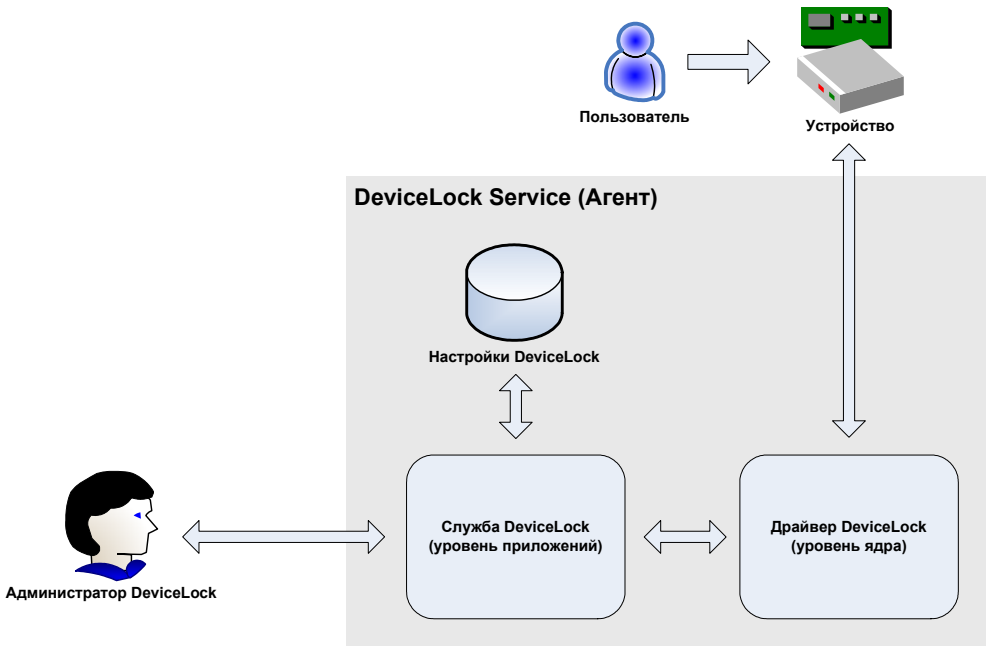
Дополнительную информацию о базах данных цифровых "отпечатков" известных файлов, а также примеры подобных баз данных можно найти на сайте национального института стандартов и технологий США: http://www.nsrl.nist.gov.

В дополнение к стандартным возможностям управления правами доступа и настройками, DeviceLock обеспечивает вас и более мощным механизмом: разрешения, правила аудита и настройки могут быть изменены и применены с использованием групповых политик службы управления каталогами Active Directory.

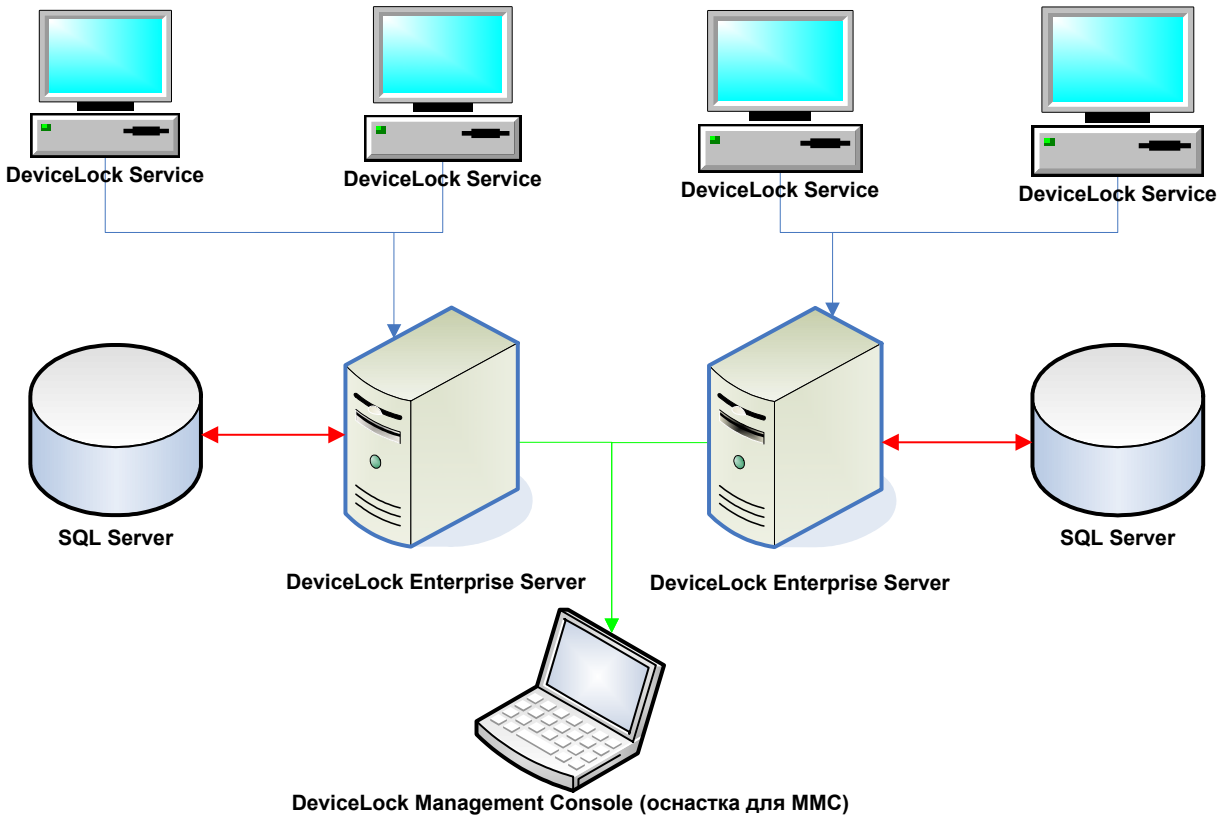
Глубокая интеграция в Active Directory – важная особенность DeviceLock. Она упрощает развертывание в больших сетях и более удобна для системных администраторов. Интеграция в Active Directory исключает необходимость установки дополнительных приложений для централизованного управления и развертывания. DeviceLock не требует своей собственной серверной версии для контроля за всей сетью, вместо этого используется стандартная функция, предоставляемая Active Directory.

DeviceLock состоит из трех частей: агента (DeviceLock Service), сервера (DeviceLock Enterprise Server) и консоли управления (DeviceLock Management Console, DeviceLock Group Policy Manager и DeviceLock Enterprise Manager):

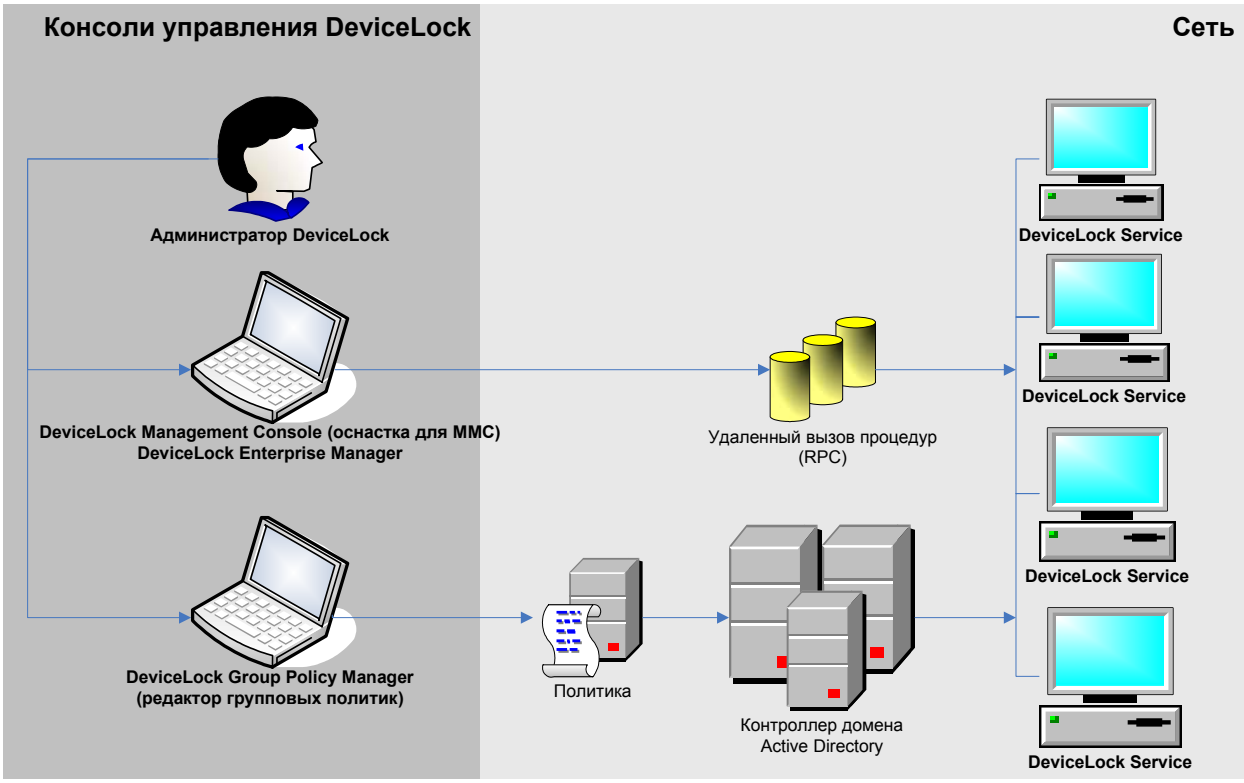
1. DeviceLock Service – это ядро системы DeviceLock. Агент устанавливается на каждый компьютер, автоматически запускается и обеспечивает защиту устройств на машине-клиенте, оставаясь в то же время невидимым для локального пользователя.



2. DeviceLock Enterprise Server – это дополнительный необязательный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита. DeviceLock Enterprise Server использует MS SQL Server для хранения данных. Вы можете установить несколько экземпляров DeviceLock Enterprise Server в вашей сети, чтобы равномерно распределить нагрузку.



3. Консоль управления – это интерфейс контроля, который системный администратор использует для удаленного управления любой системой, на которой установлен агент (DeviceLock Service). DeviceLock поставляется с тремя различными консолями управления: DeviceLock Management Console (оснастка для MMC), DeviceLock Enterprise Manager и DeviceLock Group Policy Manager (интегрирован в редактор групповых политик Windows). DeviceLock Management Console также используется для управления DeviceLock Enterprise Server'ом.

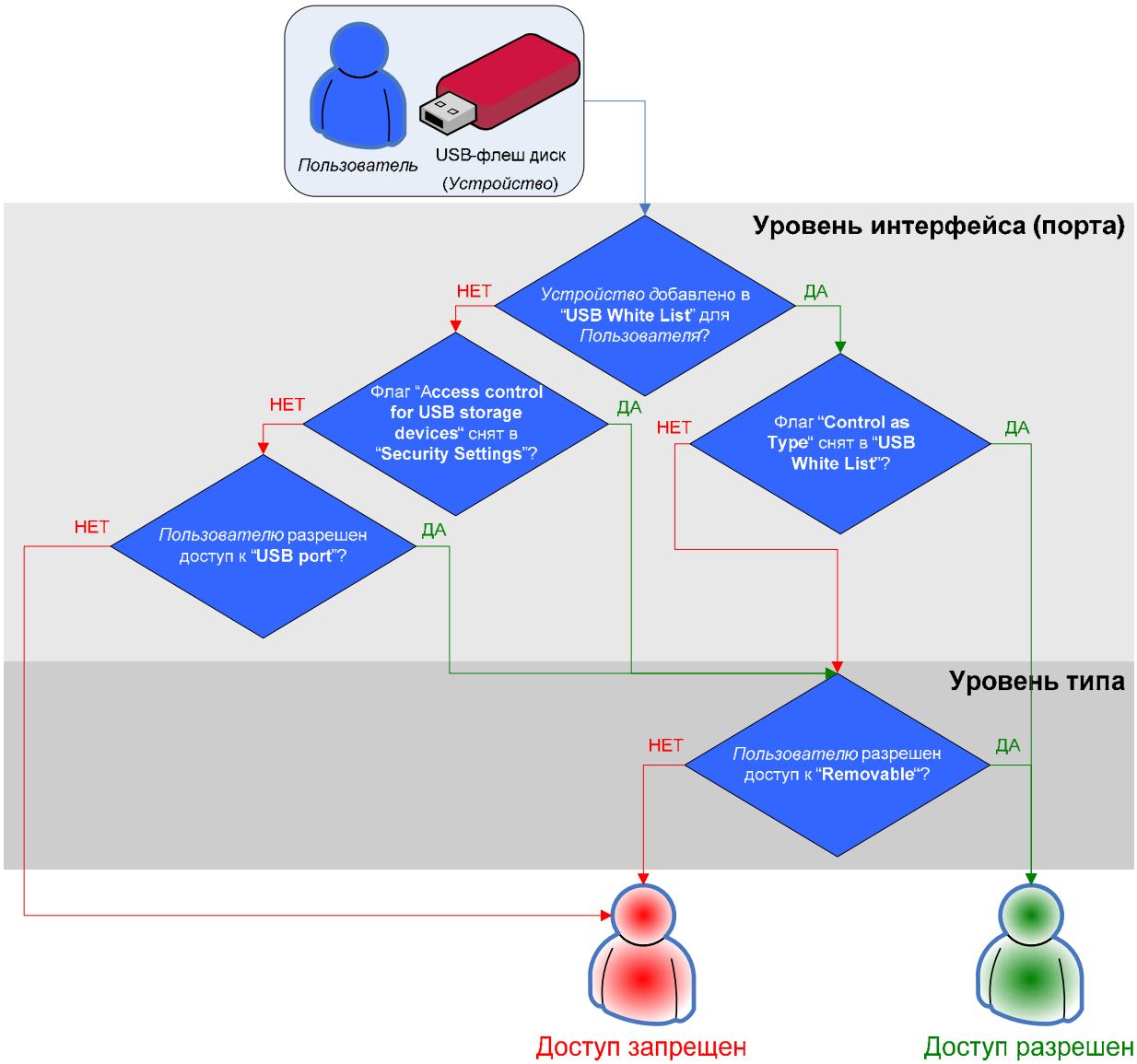


1.2 Управляемый контроль доступа

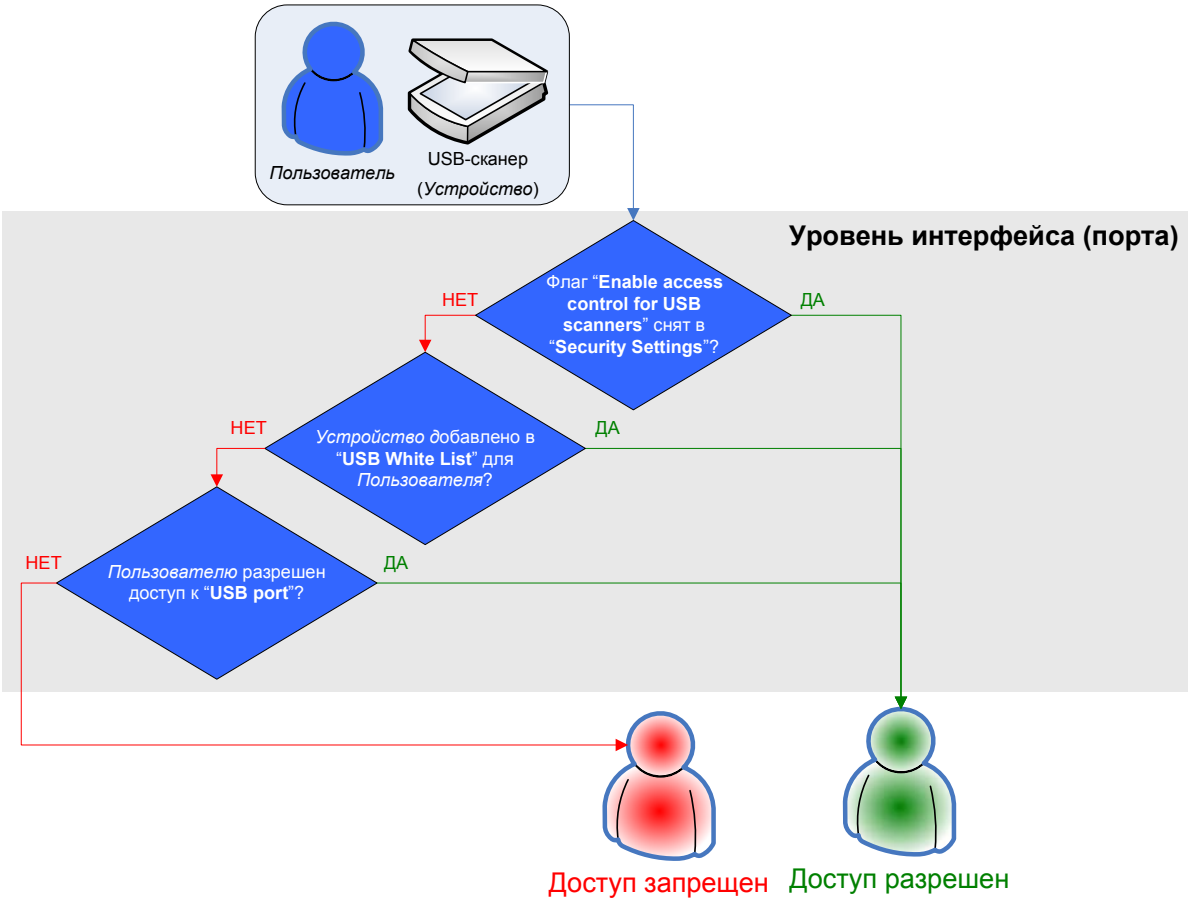
Каждый раз, когда пользователь пытается получить доступ к устройству, DeviceLock перехватывает запрос на уровне ядра ОС.

В зависимости от типа устройства и интерфейса подключения (напр., USB), DeviceLock проверяет права пользователя в соответствующем списке управления доступом (ACL). Если у пользователя отсутствуют права доступа к данному устройству, будет возвращено сообщение об ошибке "*доступ запрещен*".

Контроль доступа может выполняться на двух уровнях: уровне интерфейса (порта) и уровне типа. Некоторые устройства проверяются на обоих уровнях, в то время как другие – только на одном: либо на уровне интерфейса (порта), либо на уровне типа.



Рассмотрим случай доступа пользователя к USB-флеш через USB-порт. В данном случае DeviceLock в первую очередь проверит на уровне интерфейса (USB-порта), открыт или нет доступ к USB-порту. Затем, поскольку Windows определяет USB-флеш как съемное устройство, DeviceLock также проверит ограничения на уровне типа устройства (Removable). В случае использования USB-сканера доступ будет проверяться только на уровне интерфейса (USB-порта), поскольку DeviceLock не имеет отдельного типа устройств для сканеров.



Существуют дополнительные настройки безопасности, которые могут выключать контроль доступа для классов устройств (напр., для всех USB-клавиатур и мышей), в то время как остальные устройства остаются под контролем. В этом случае, если устройство принадлежит к классу, для которого контроль отключен, DeviceLock пропускает все запросы на соединение с этим устройством на уровне интерфейса (порта).

DeviceLock также поддерживает белый список определенных устройств; иными словами, вы можете отключить контроль доступа только для определенных устройств (например, некоторых USB-принтеров).

ПРИМЕЧАНИЕ: если доступ к устройству запрещен на уровне интерфейса (порта), DeviceLock не будет проверять разрешения на уровне типа. Однако, если доступ разрешен на уровне интерфейса (порта), DeviceLock будет проверять ограничение доступа в том числе и на уровне типа; и лишь в том случае, если права предоставлены на обоих уровнях, пользователь сможет подключиться к этому устройству.

1.3 Рекомендуемые меры по обеспечению безопасности

Ниже приведен ряд основополагающих правил обеспечения безопасности, которые должны соблюдаться для компьютеров, подключаемых к корпоративной сети:

а. **Измените последовательность загрузки.** Жесткий диск должен быть первым загрузочным устройством. Измените последовательность загрузки в BIOS таким образом, чтобы компьютер не мог загружаться с дискеты, USB-устройства или DVD/CD-ROM. Если жесткий диск не является первым загрузочным устройством, кто угодно сможет использовать загрузочный CD или флеш-диск, подключаемый к USB, чтобы получить доступ к жесткому диску.

б. **Защитите BIOS паролем.** Пароль должен быть установлен для доступа к BIOS, чтобы только человек, знающий его, мог вносить изменения в конфигурацию. Если BIOS не защищен паролем, кто угодно может изменить последовательность загрузки и использовать загрузочный CD, дискету или флеш-диск (см. выше).

в. **Опечатайте корпус компьютера и шасси.** Существует возможность подключить внешнее загрузочное устройство непосредственно к компьютеру и получить доступ к жесткому диску. Более того, если кто-то получит физический доступ к материнской плате, ему будет очень просто найти переключатель очистки CMOS и затем стереть пароль для доступа к BIOS (см. выше).

г. **Не предоставляйте административные привилегии обычному пользователю.** Обычный пользователь не должен быть членом локальной группы *Администраторы*.

   Однако, даже если пользователи вашей сети имеют административные привилегии на локальных компьютерах, DeviceLock способен обеспечить необходимый уровень защиты. Никто, за исключением авторизированного администратора программы DeviceLock, не может подключиться, остановить или удалить DeviceLock Service. Даже члены локальной группы *Администраторы* не могут отключить DeviceLock, если они не являются администраторами DeviceLock.

д. **Удалите консоль восстановления системы.** Если консоль восстановления системы установлена на локальном компьютере, кто угодно может загрузиться в режиме восстановления и отключить DeviceLock Service (конечно, для этого требуется пароль локального администратора). По этой причине мы рекомендуем удалить консоль восстановления. Для получения более подробной информации о том, как установить, удалить или использовать консоль восстановления, обратитесь к документу Microsoft: http://support.microsoft.com/default.aspx?scid=kb;ru;307654.

2. Установка

2.1 Системные требования

DeviceLock работает на любом компьютере с операционными системами Windows NT 4.0 SP6/2000/XP/Vista и Windows Server 2003/2008. Поддерживаются 32-х и 64-х битные платформы.

Для установки и использования DeviceLock вы ДОЛЖНЫ иметь права администратора. Если вы собираетесь использовать DeviceLock только на локальном компьютере, вы должны иметь права локального администратора. Если вы собираетесь использовать DeviceLock в сети, вы должны иметь права администратора домена.

Если вы хотите использовать DeviceLock в сети, у вас должен быть установлен сетевой протокол TCP/IP. Однако DeviceLock может работать и на отдельных компьютерах. Сеть нужна только в том случае, если вы хотите контролировать DeviceLock Service с удаленного компьютера.

2.2 Развертывание DeviceLock Service

Агент (DeviceLock Service) должен быть установлен на каждый компьютер, где необходимо контролировать доступ пользователей к устройствам. Существует несколько способов установить DeviceLock Service на клиентские системы.

2.2.1 Интерактивная установка

Запустите программу установки (*setup.exe*) и следуйте инструкциям на экране.

Вам необходимо запускать *setup.exe* на каждом компьютере, где должен быть установлен DeviceLock Service.

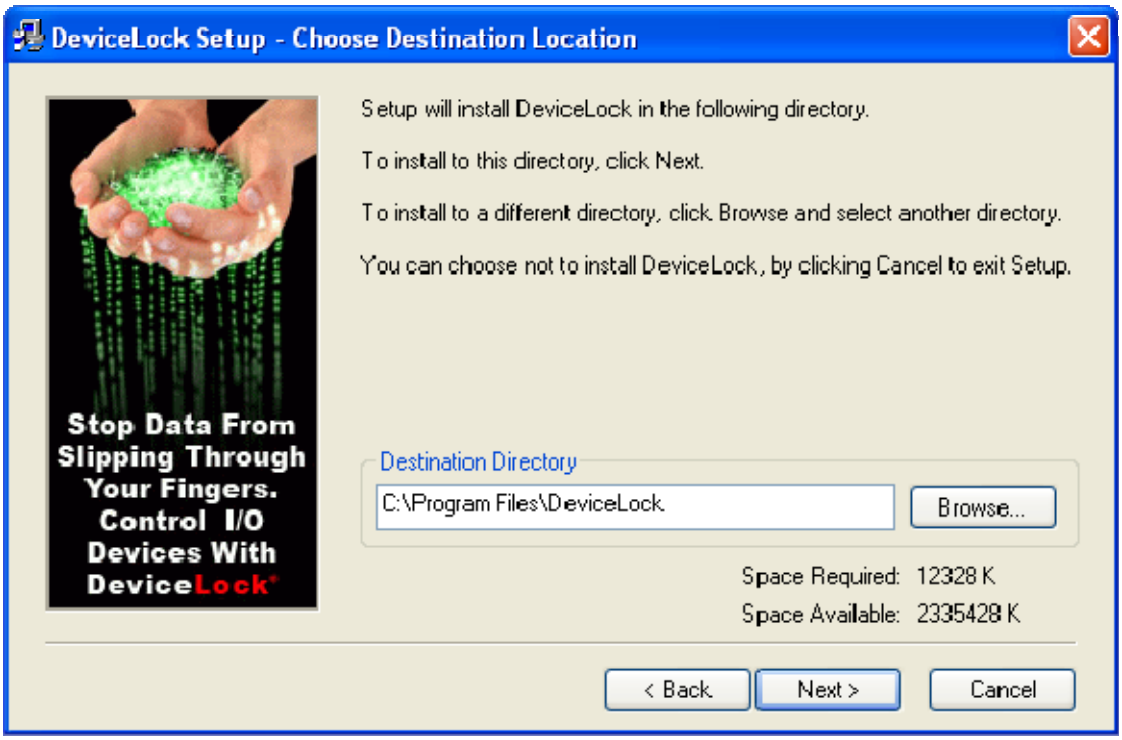
Если вы устанавливаете DeviceLock Service поверх уже существующей предыдущей версии, убедитесь, что у вас есть административные права доступа к DeviceLock Service, в противном случае вы не сможете продолжить установку.

Вы должны принять лицензию на использование программы перед тем, как продолжить установку.

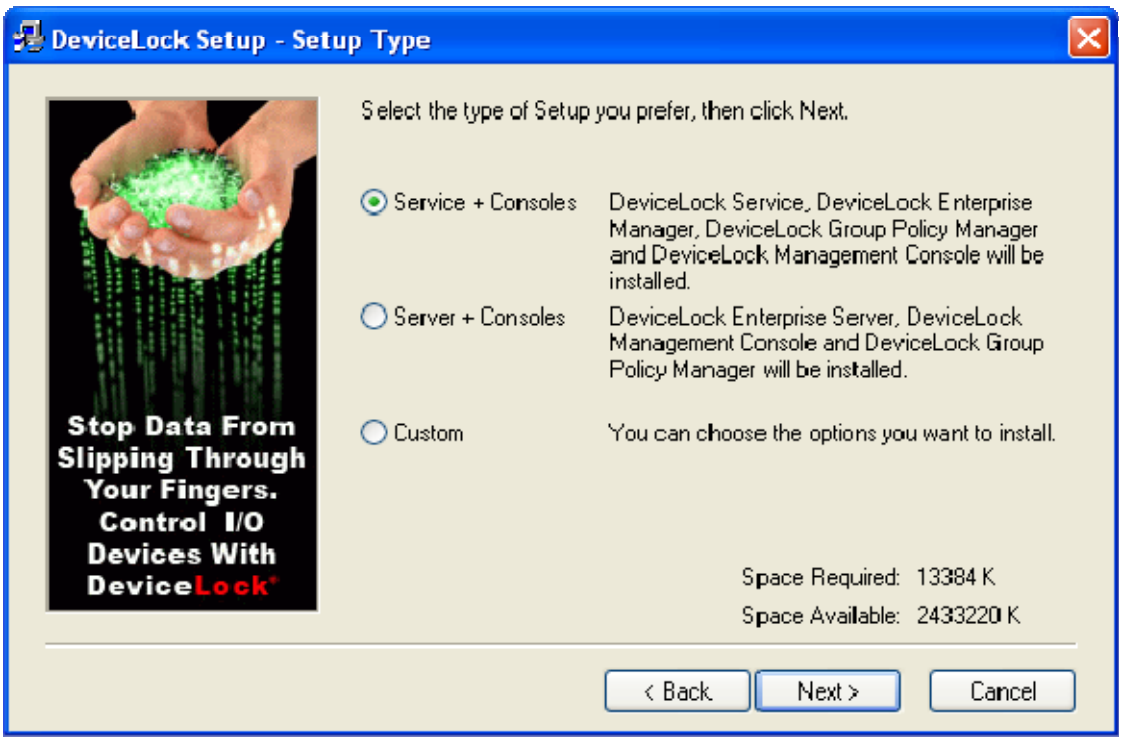
DeviceLock устанавливается в каталог, выбранный вами. Сначала программа установки попытается найти предыдущую версию DeviceLock и, если она существует, программа предложит вам установить DeviceLock в тот же каталог.

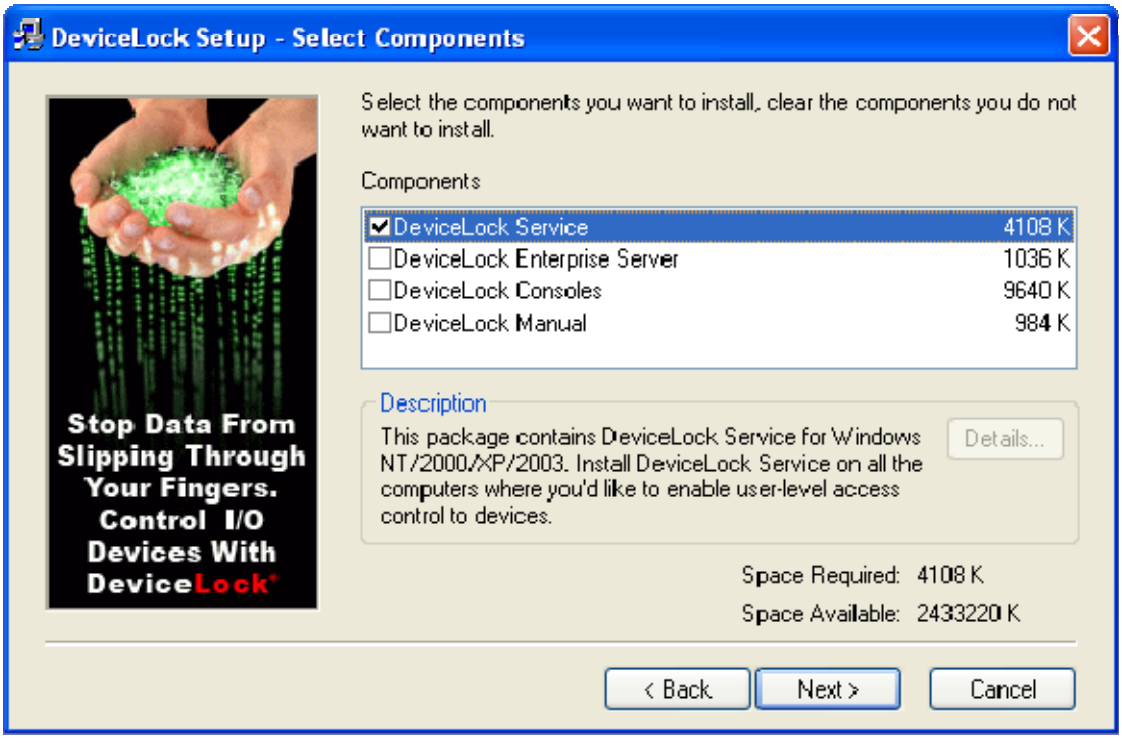
Если предыдущей установки найдено не было, программа предложит вам установить DeviceLock в каталог Program Files системного диска (например, *C:\Program Files\DeviceLock*).

В любом случае, вы можете сами выбрать любой каталог для установки.



У вас есть два варианта выбора: установить DeviceLock Service и консоли управления DeviceLock, выбрав опцию *Service + Consoles* или установить только DeviceLock Service, выбрав опцию *Custom* и потом отметив компонент *DeviceLock Service*.

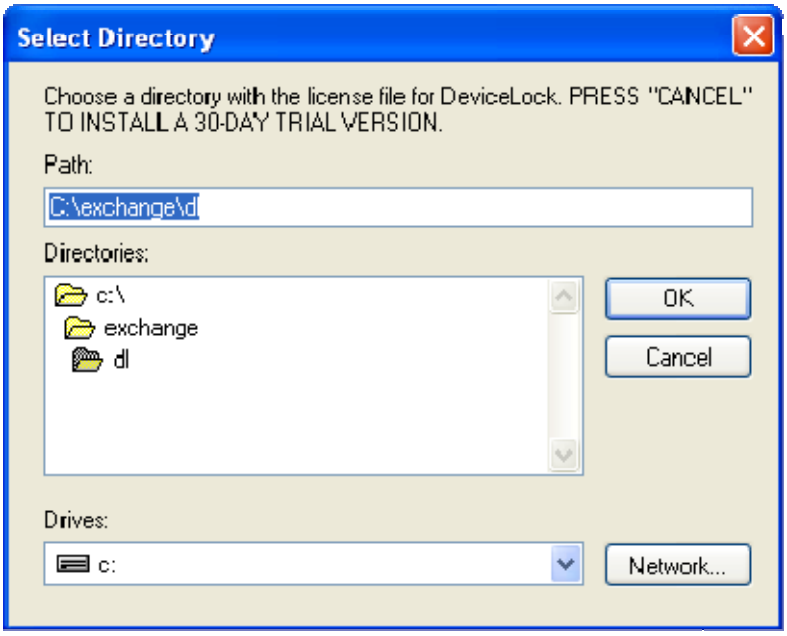




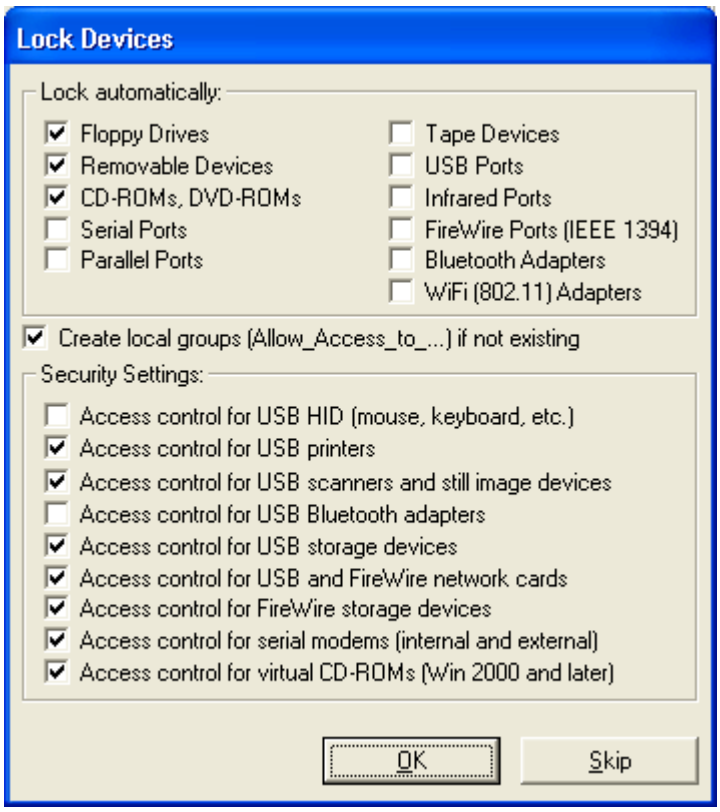
Если вы выбрали установку консолей управления DeviceLock, программа может предложить вам создать новый сертификат (DeviceLock Certificate).

Вы всегда можете создать новый сертификат позже, используя специальную программу Certificate Generation Tool, устанавливаемую вместе с консолями управления DeviceLock. Поэтому, если на этом шаге установки вы не уверены в том, нужен вам новый сертификат или нет, просто нажмите кнопку *No* и продолжайте установку.

Также, если вы выбрали опцию *Service* + *Consoles*, программа установки может предложить вам указать лицензионный файл. Если у вас нет лицензионного файла, нажмите кнопку *Cancel,* чтобы установить DeviceLock в ознакомительном 30-ти дневном режиме.



В процессе установки вы можете задать разрешения для локальных устройств.



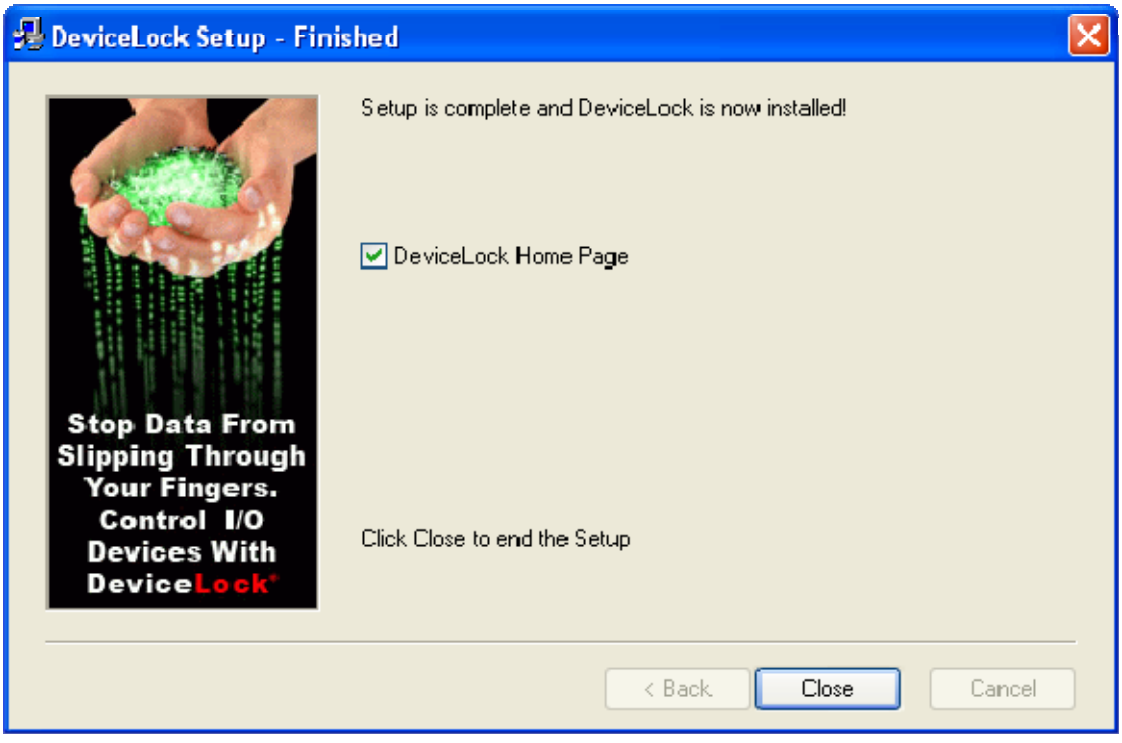
Отметьте устройства, для которых вы хотите установить разрешения. Отметьте *Create local groups if not existing,* и программа создаст специальные локальные группы пользователей *Allow_Access_To_* для каждого типа устройств (например, *Allow_Access_To_Floppy* для дисководов), если они не существовали на локальном компьютере.

Программа назначит права **Read**, **Write**, **Format** и **Eject,** членам группы *Администраторы* и учетной записи *СИСТЕМА*. Члены группы *Allow_Access_To_* будут иметь права **Read**, **Write** и **Eject**.

Также вы можете определить дополнительные настройки безопасности, чтобы исключить определенные типы устройств из контроля доступа. Установите флаги *Access control for USB HID*, *Access control for USB printers*, *Access control for USB scanners and still image devices*, *Access control for USB Bluetooth adapters* или *Access control for USB storage devices*, чтобы разрешить агенту контролировать доступ к устройствам ввода (мышь, клавиатура и т.д.), принтерам, сканерам и фотоаппаратам, Bluetooth-адаптерам или устройствам хранения информации (таким как флеш-диски), подключаемым к USB-портам. Чтобы разрешить контроль доступа для USB и FireWire-сетевых карт, установите флаг *Access control for USB and FireWire network cards*. В противном случае, даже если порты (USB и/или FireWire) заблокированы, эти устройства будут продолжать работать как обычно. Чтобы разрешить контроль доступа для модемов *(*внутренних или внешних*)*, установите флаг *Access control for serial modems*. Чтобы отключить блокирование виртуальных DVD/CD-ROM'ов на системах Windows 2000 и выше, снимите галочку с *Access control for virtual CD-ROMs*. Чтобы отключить блокирование виртуальных принтеров на системах Windows 2000 и выше, снимите галочку с *Access control for virtual printers*.

Нажмите кнопку *OK,* чтобы применить установки. Нажмите кнопку *Skip,* если вы предпочитаете устанавливать разрешения, используя консоли управления DeviceLock.

В конце установки программа предложит вам открыть сайт DeviceLock.



Снимите галочку с *DeviceLock Home Page*, если вы не хотите открывать сайт DeviceLock в данный момент.

Нажмите кнопку *Close,* чтобы завершить процесс установки.

2.2.2 Установка без вмешательства пользователя

DeviceLock также поддерживает так называемую “тихую” установку, которая позволяет установить DeviceLock Service без вмешательства пользователя с помощью специального конфигурационного файла *devicelock.ini.* Для установки DeviceLock без вмешательства пользователя запустите программу установки с параметром */s* (например, *c:\setup.exe /s*). *Devicelock.ini* должен находиться в одном каталоге с *setup.exe*. При помощи этого файла вы можете задать параметры установки.

Вы можете открывать и редактировать файл *devicelock.ini* в любом текстовом редакторе (например, Notepad). Удалите точку с запятой (;) перед параметром, чтобы присвоить новое значение этому параметру, либо оставьте точку с запятой, чтобы присвоить значение по умолчанию.

В этом конфигурационном файле есть две секции (*[Install]* и *[Misc]*) и каждая секция имеет свой собственный набор параметров:

1. *[Install]*

Чтобы установить DeviceLock Service, установите параметр *Service* в единицу:

Service = 1

Аналогично вы можете установить консоли управления DeviceLock и документацию, используя параметры *Manager* и *Documents*.

Если вы хотите только обновить DeviceLock Service и не хотите менять существующие настройки, используйте параметр *OnlyUpgradeService*:

OnlyUpgradeService = 1

В этом случае программа установки игнорирует все заданные параметры и только копирует новый файл DeviceLock Service (*dlservice.exe* или *dlservice_x64.exe*) поверх существующего.

Вы также можете указать путь для установки DeviceLock:

InstallDir = C:\Program Files\DeviceLock

Программа использует этот параметр, если не может найти существующую установку DeviceLock.

Если вы купили лицензию для DeviceLock, вы также можете указать расположение файла лицензии:

RegFileDir = C:\Directory

где *C:\Directory* – каталог, в котором находится файл лицензии.

Вам не нужно указывать лицензию, если вы устанавливаете только DeviceLock Service. Лицензия требуется для консолей управления DeviceLock.

Для использования DeviceLock Service фиксированного TCP-порта укажите значение параметра *FixedPort*:

FixedPort = [*номер порта*]

где *номер порта* – номер TCP-порта, который вы будете использовать для установления связи между консолью управления и DeviceLock Service. Для использования динамической привязки к портам в качестве номера укажите 0. По умолчанию DeviceLock Service использует порт 9132.

Если параметр *CreateGroups* установлен в “1”, программа установки создаст специальную локальную группу пользователей *Allow_Access_To_* для каждого типа устройств (например, *Allow_Access_To_Floppy* для дисководов), если такой группы еще не существует на локальном компьютере.

Чтобы установить разрешения, правила аудита и настройки DeviceLock Service, в параметре *SettingsFile* укажите полный путь к предварительно сохраненному XML-файлу:

SettingsFile = C:\settings.dls

Этот файл с настройками может быть создан с помощью DeviceLock Management Console, DeviceLock Group Policy Manager’a и/или DeviceLock Service Settings Editor’a.

2. [Misc]

Если вы хотите запустить какую-либо программу после успешной установки DeviceLock, вы можете задать параметр *Run*:

Run = C:\mybatchfile.bat

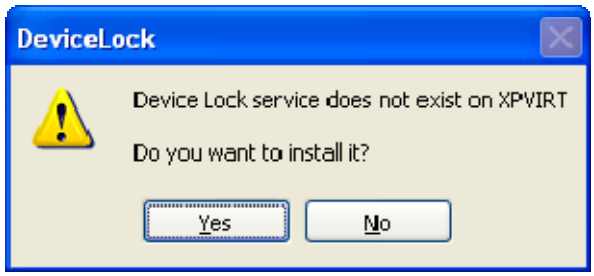
Для запрета автоматической перезагрузки компьютера после завершения установки, даже если программа установки требует этого, установите параметр *DisableRestart* в “1”.

2.2.3 Установка с помощью Systems Management Server

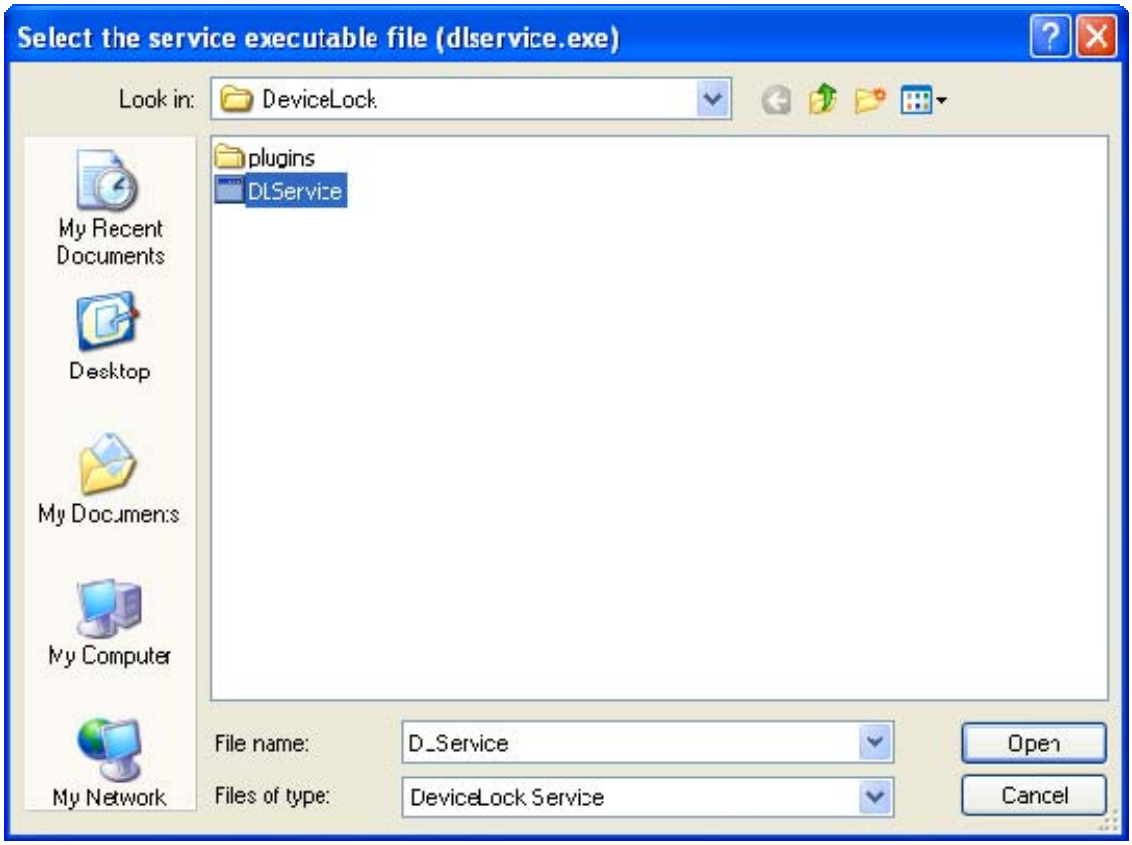
Используя "тихую" установку, вы можете также развернуть DeviceLock Service в сети при помощи Microsoft Systems Management Server (SMS). Используйте файлы *DevLock.pdf* для SMS версии 1.x и *DevLock.sms* для SMS версий 2.0 и выше. Эти файлы входят в состав поставки DeviceLock и находятся в файле *sms.zip*.

2.2.4 Установка в DeviceLock Management Console

DeviceLock Management Console (оснастка для MMC) поддерживает удаленную установку агентов. Когда вы пытаетесь подключиться к компьютеру, где DeviceLock Service не установлен либо установлена старая версия, консоль управления предложит соответственно установить либо обновить DeviceLock Service.



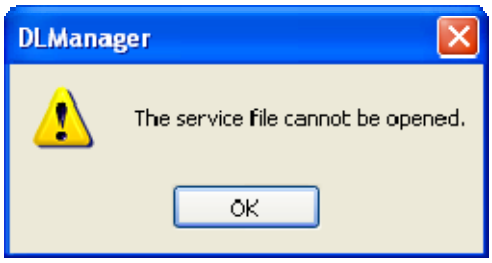
Выберите исполняемый файл DeviceLock Service'а (*dlservice.exe* или *dlservice_x64.exe*), и консоль управления скопирует его на удаленный компьютер.



Исполняемый файл DeviceLock Service будет скопирован в системный каталог Windows (например, *c:\winnt\system32*), если до этого DeviceLock Service не был установлен на данном компьютере. Если же предыдущая версия DeviceLock

Service уже установлена, то консоль управления скопирует новый файл в директорию с существующей версией и старый файл будет перезаписан новым.

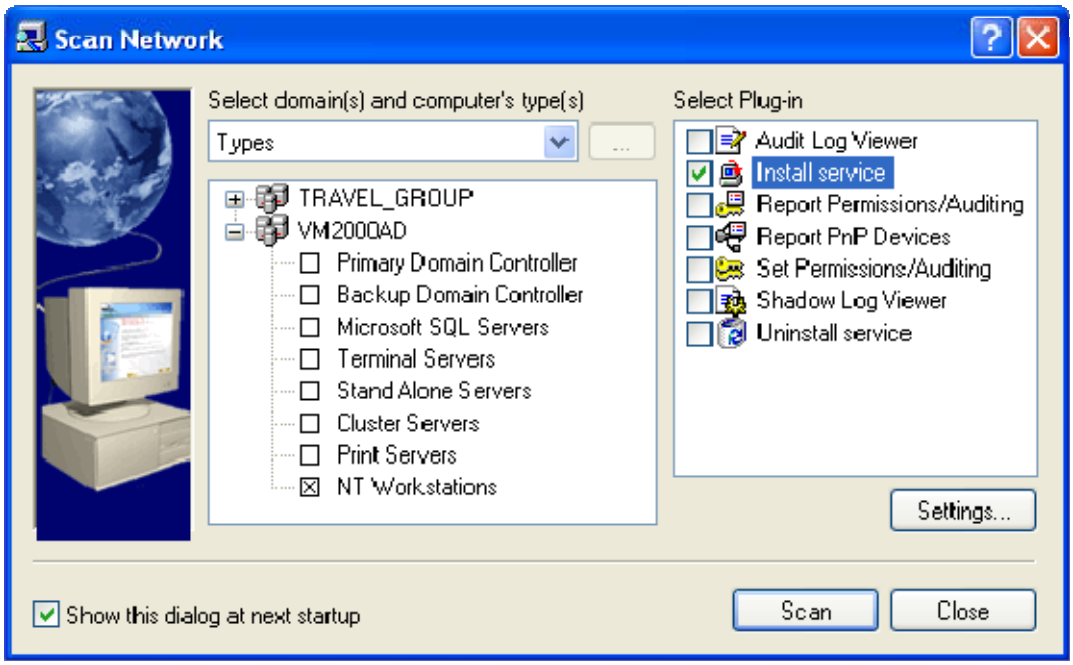
Имейте в виду, что если DeviceLock Service работает на том же самом компьютере, где вы используете консоль управления и при этом включена защита DeviceLock Service от пользователей с правами локального администратора (снят флаг *Enable Default Security* в DeviceLock Administrators), то консоль управления (как и любое иное приложение) не сможет получить доступ к исполняемому файлу DeviceLock Service.



Чтобы обойти это ограничение, вы можете скопировать исполняемый файл в другую директорию перед включением защиты и использовать эту копию для удаленной установки.

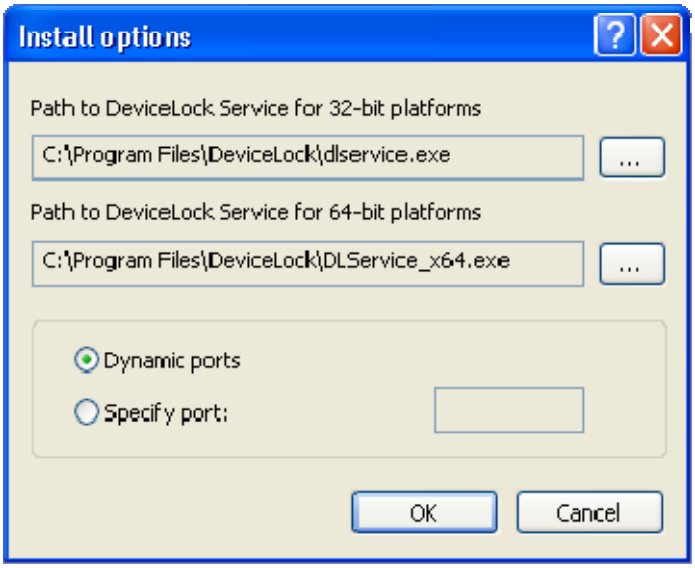
2.2.5 Установка в DeviceLock Enterprise Manager

DeviceLock Enterprise Manager содержит специальный модуль *Install service*, который позволяет автоматически устанавливать DeviceLock Service на все компьютеры в сети.



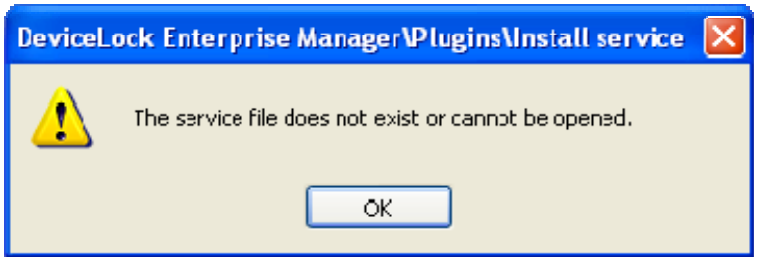
Сперва выберите компьютеры, на которые DeviceLock Service должен быть установлен. DeviceLock Enterprise Manager позволяет выбирать компьютеры по типам и именам. Вы также можете загрузить список компьютеров из внешнего файла или выбрать из любого LDAP-дерева (Active Directory, Novell eDirectory, OpenLDAP и т.п.).

Затем выберите модуль *Install service* и нажмите кнопку *Settings*, чтобы указать местонахождение исполняемого файла DeviceLock Service. Вы также можете настроить DeviceLock Service на использование фиксированного TCP-порта при установлении связи с консолью управления (опция *Specify port*). Для использования динамической привязки к портам выберите опцию *Dynamic ports*. По умолчанию DeviceLock Service использует порт 9132.



Исполняемый файл DeviceLock Service будет скопирован в системный каталог Windows (например, *c:\winnt\system32*), если до этого DeviceLock Service не был установлен на данном компьютере. Если же предыдущая версия DeviceLock Service уже установлена, то модуль *Install service* скопирует новый файл в директорию с существующей версией и старый файл будет перезаписан новым.

Имейте в виду, что если DeviceLock Service работает на том же самом компьютере, где вы используете DeviceLock Enterprise Manager и при этом включена защита DeviceLock Service от пользователей с правами локального администратора (снят флаг *Enable Default Security* в DeviceLock Administrators), то DeviceLock Enterprise Manager (как и любое иное приложение) не сможет получить доступ к исполняемому файлу DeviceLock Service.



Чтобы обойти это ограничение, вы можете скопировать исполняемый файл в другую директорию перед включением защиты и использовать путь к этой копии в настройках модуля *Install service*.

2.2.6 Установка через групповые политики Active Directory

Эта пошаговая инструкция описывает, как использовать групповую политику Active Directory для автоматической установки DeviceLock Service на компьютеры

в домене. DeviceLock Service может быть развернут в домене Active Directory с использованием пакета (*DeviceLock Service.msi* и *DeviceLock Service x64.msi*) для Microsoft Software Installer (MSI).

ПРИМЕЧАНИЕ: Программа автоматической установки Microsoft Windows требует, чтобы на клиентских компьютерах была установлена Windows 2000 или более поздняя версия ОС.

Вы можете использовать групповую политику для установки DeviceLock Service следующим образом:

- Создание точки распространения

  Чтобы установить DeviceLock Service, вы должны создать точку распространения на сервере:

  1. Войти на сервер в качестве администратора.

  2. Создать общедоступную сетевую папку.
  3. Установить права на данную папку, разрешающие доступ к дистрибутиву.

  4. Скопировать MSI-пакет (*DeviceLock Service.msi* и/или *DeviceLock Service x64.msi*) в созданную общую сетевую папку.

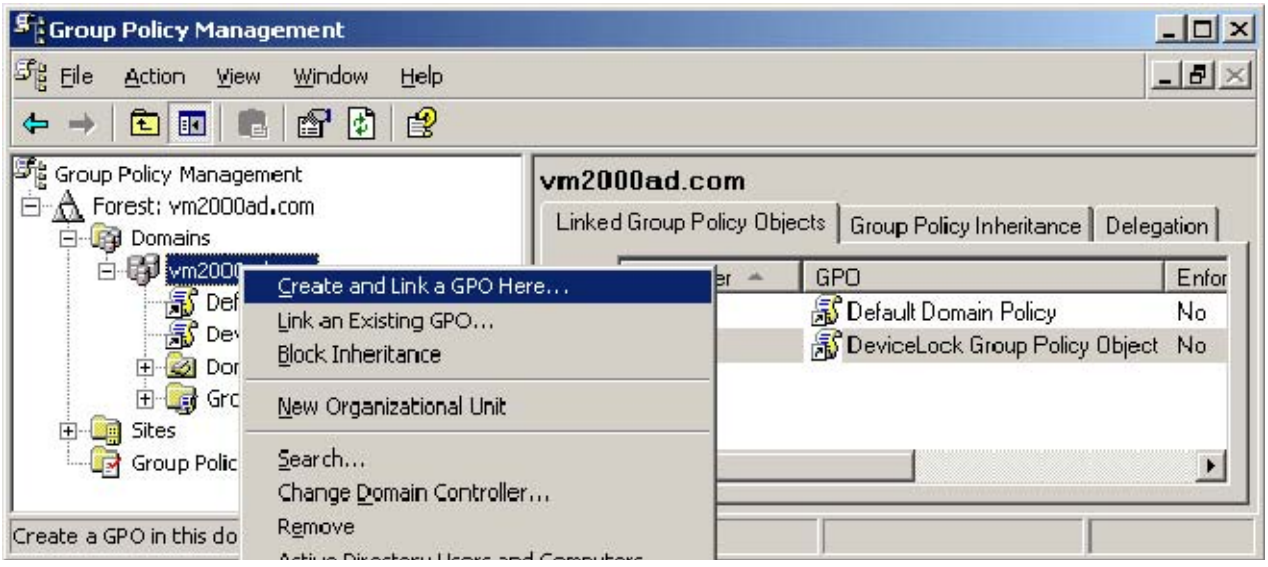
- Создание объекта групповой политики

  Для создания объекта групповой политики (GPO), с помощью которого будет устанавливаться DeviceLock Service:

  1. Запустите оснастку *Group Policy Management*.

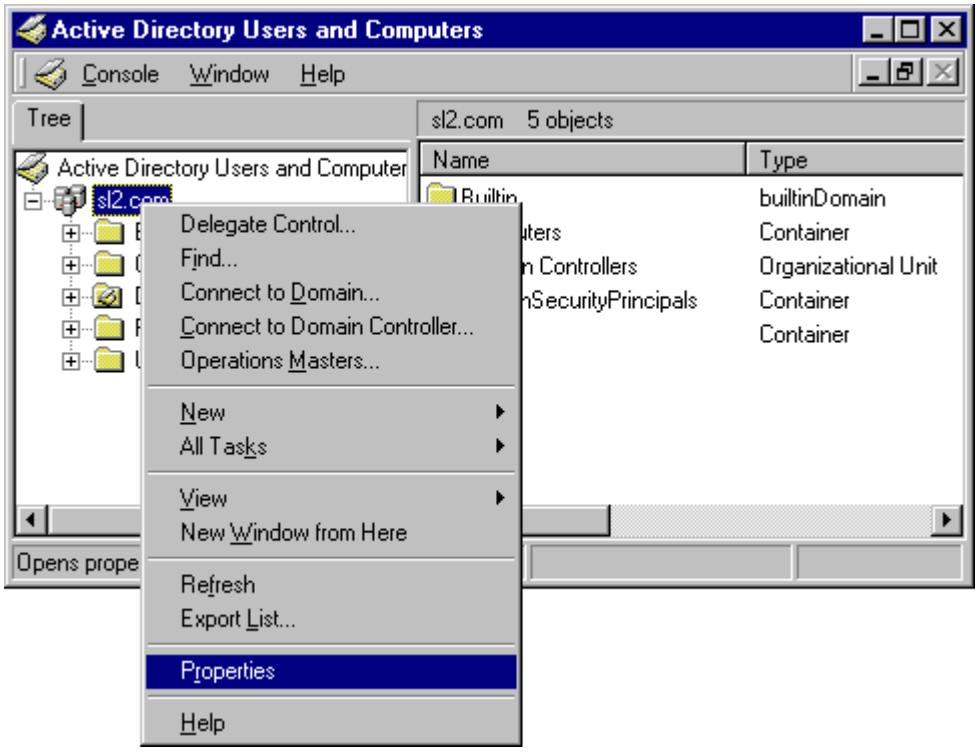
     Если оснастка *Group Policy Management* не установлена на вашем компьютере, вы можете использовать оснастку *Active Directory Users and Computers*.

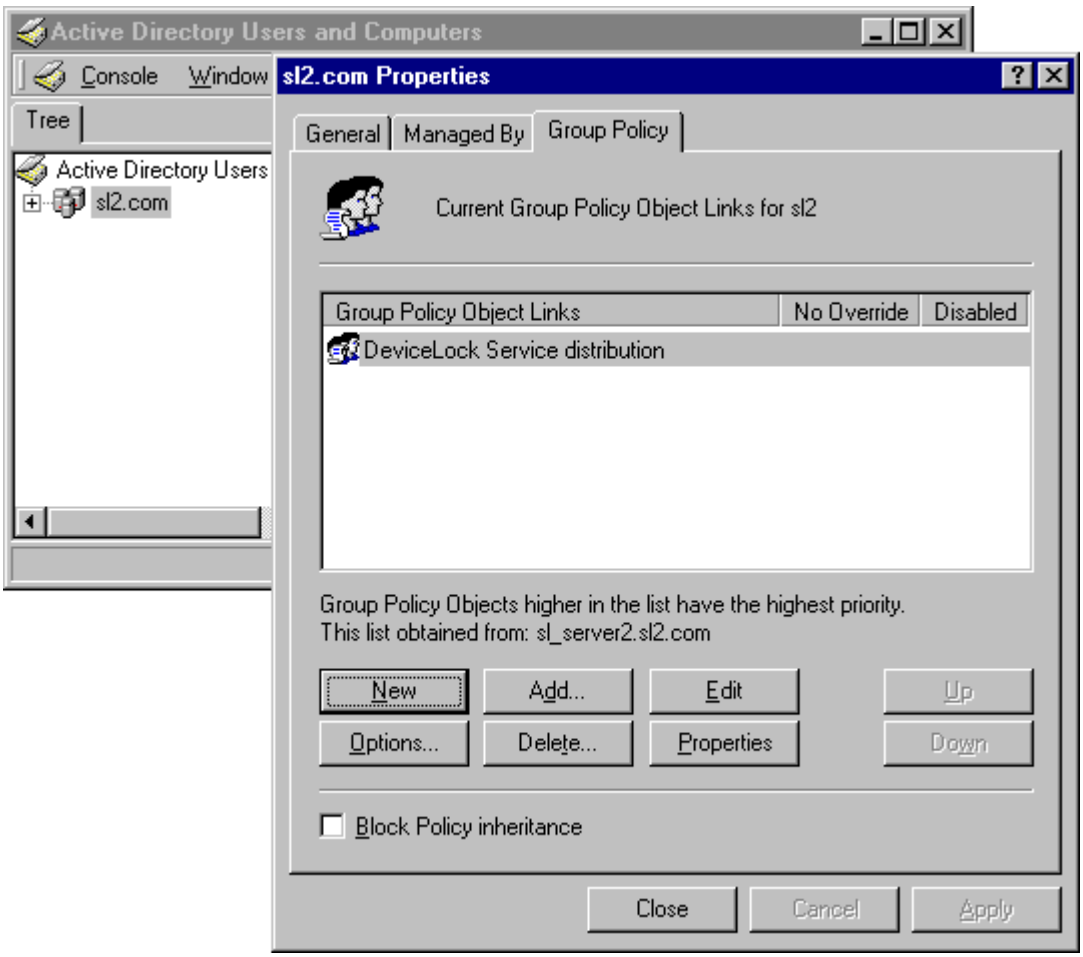
  2. Выберите необходимый домен в дереве консоли.



3. Кликните *Create and Link a GPO Here* в контекстном меню, доступном по нажатию правой кнопки мыши на домене.

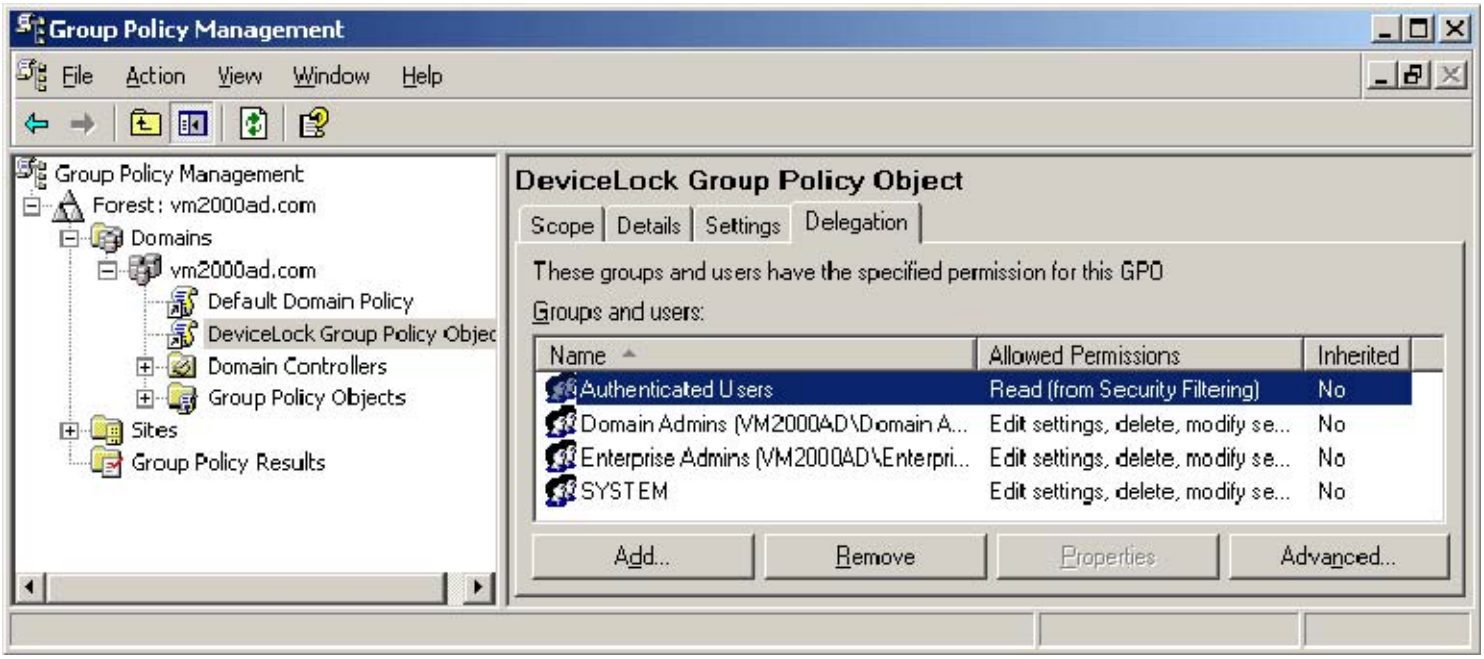
   Если вы используете оснастку *Active Directory Users and Computers*, то в дереве консоли кликните правой кнопкой на домене, кликните на *Properties*, кликните на вкладке *Group Policy* и затем нажмите на кнопку *New.*



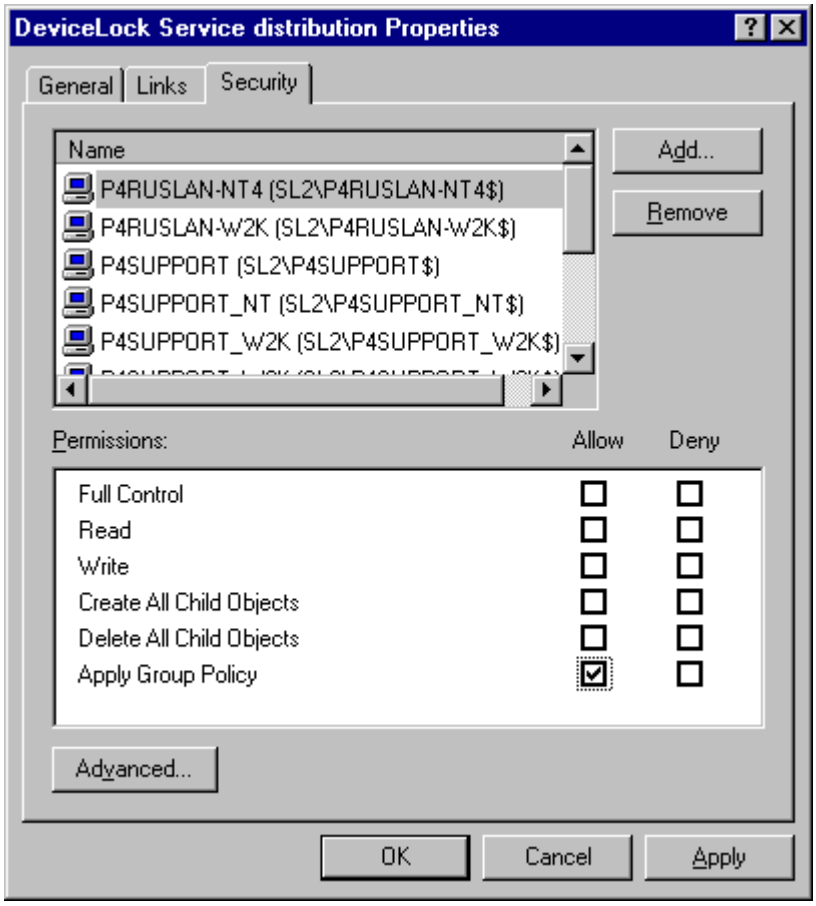


4. Введите название, которое вы хотите назначить для этого объекта групповой политики и нажмите клавишу *ENTER*.

5. Выберите объект групповой политики в дереве консоли, кликните на вкладку *Delegation* и затем нажмите на кнопку *Advanced*.



Если вы используете оснастку *Active Directory Users and Computers*, то нажмите на кнопку *Properties* на вкладке *Group Policy* и затем кликните на вкладку *Security*.



Установите флаг *Deny,* соответствующий праву *Apply Group Policy,* для тех групп, для которых вы хотите запретить применение данной политики. Установите флаг *Allow* для тех групп, к которым будет применяться данная политика. После завершения нажмите *OK*.

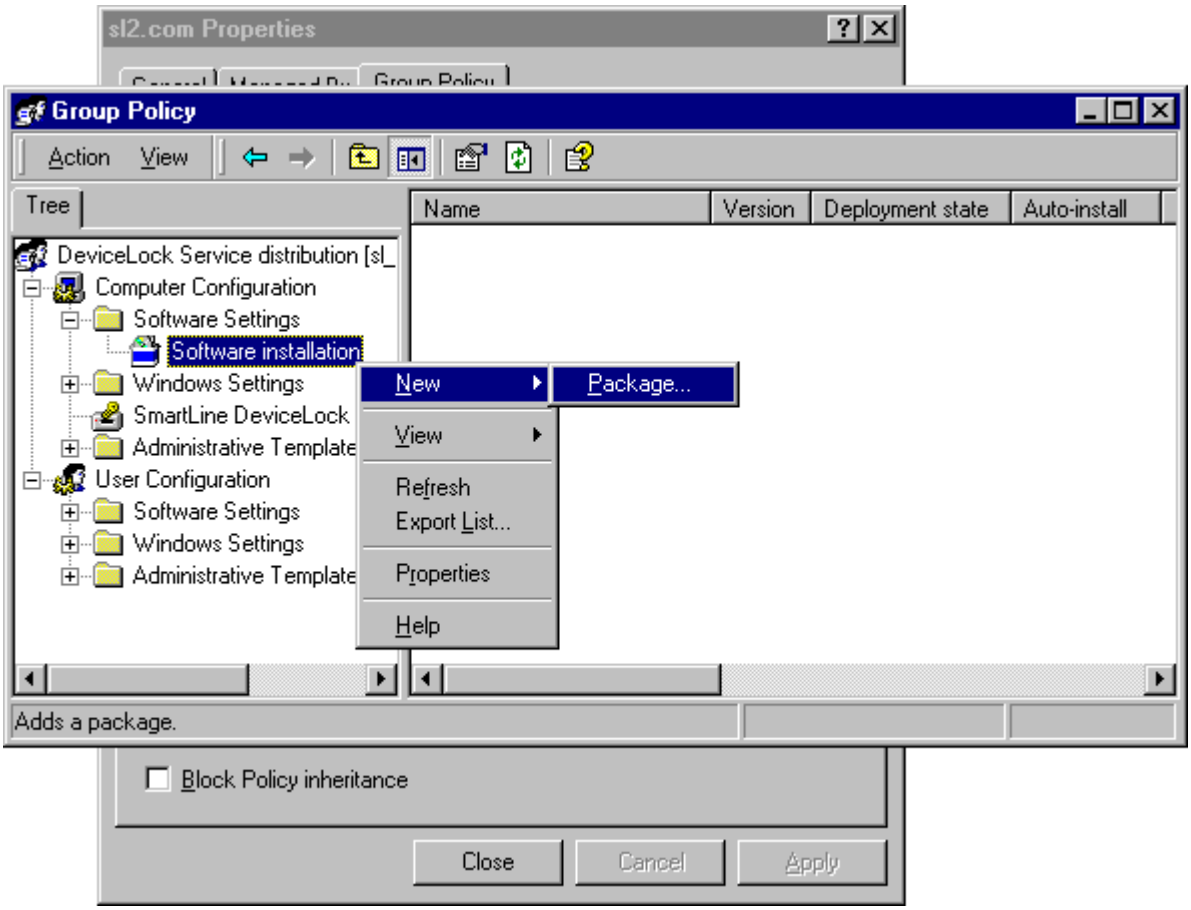
- Установка пакета

Для установки DeviceLock Service на компьютеры, которые работают под управлением Windows 2000 или более поздними ОС:

1. Откройте необходимый объект групповой политики в редакторе политик Windows Group Policy Object (используйте оснастку *Group Policy Management* или *Active Directory Users and Computers*).

2. В разделе *Computer Configuration* раскройте пункт *Software Settings*.

3. Нажмите правой кнопкой мыши на *Software installation*, выберите *New* и затем кликните на *Package*.

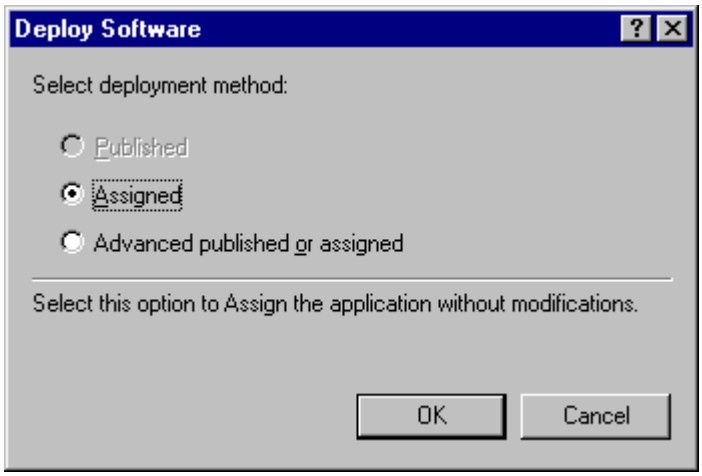


4. В диалоге *Open* введите полный сетевой путь (UNC) к общей сетевой папке, содержащей MSI-пакет. Например: *\\file server\share\DeviceLock Service.msi*.

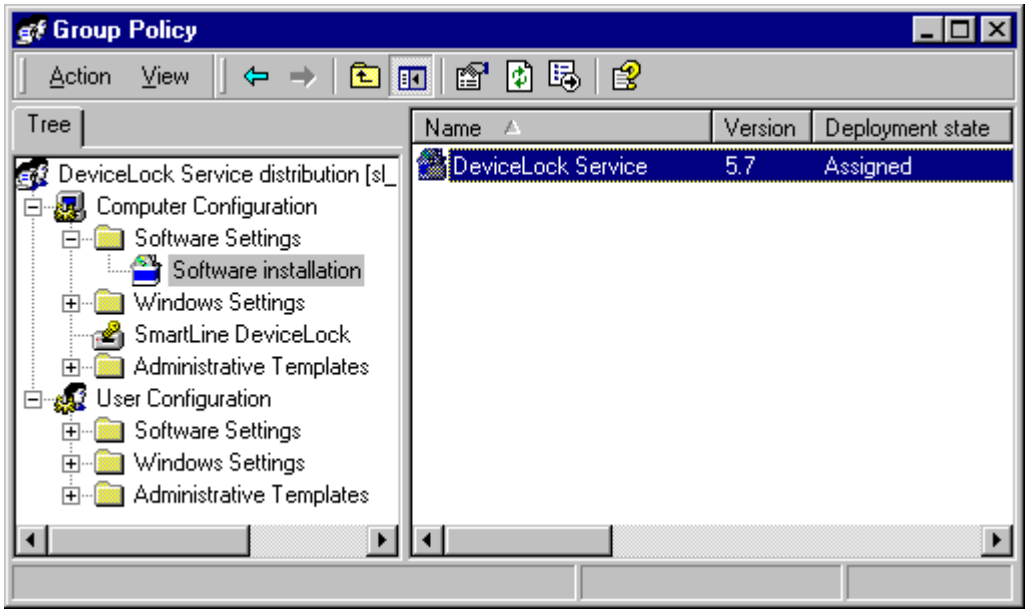
ВАЖНО: Убедитесь, что вы используете именно сетевой (а не локальный) путь к MSI-файлу!

5. Нажмите *Open*.

6. Выберите опцию *Assigned*, а затем нажмите *OK*. Пакет будет добавлен в правую часть окна *Group Policy*.



7. Закройте редактор политик. DeviceLock Service будет установлен на компьютеры при их следующем включении.



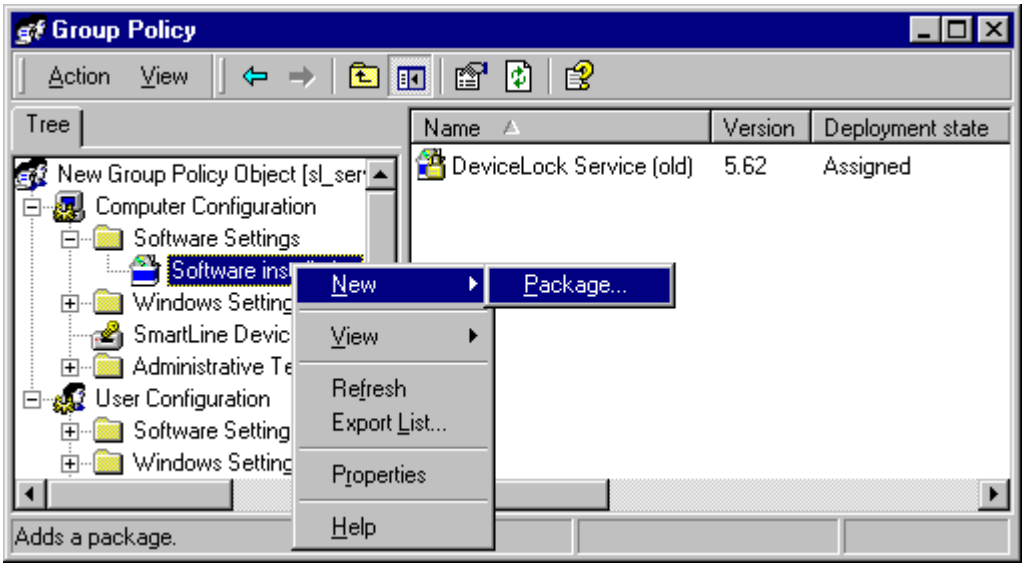
- Обновление пакета

  Если предыдущая версия DeviceLock Service уже была установлена и вы хотите обновить ее на новую версию:

  1. Откройте объект групповой политики, содержащий старый DeviceLock Service, в редакторе политик Windows Group Policy Object (используйте оснастку *Group Policy Management* или *Active Directory Users and Computers*).

2. В разделе *Computer Configuration* раскройте пункт *Software Settings*.

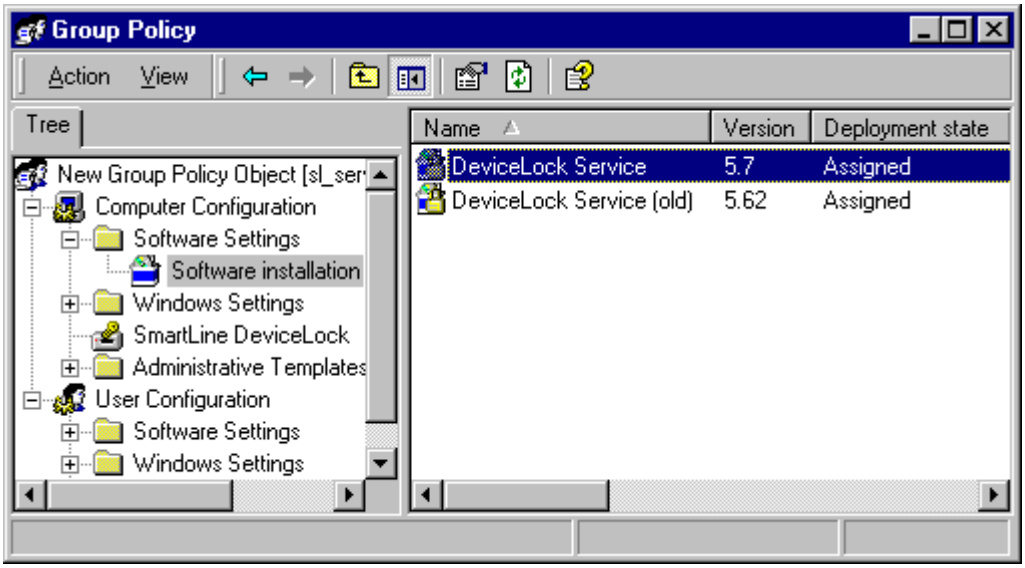
3. Нажмите правой кнопкой мыши на *Software installation*, выберите *New* и затем кликните на *Package*.



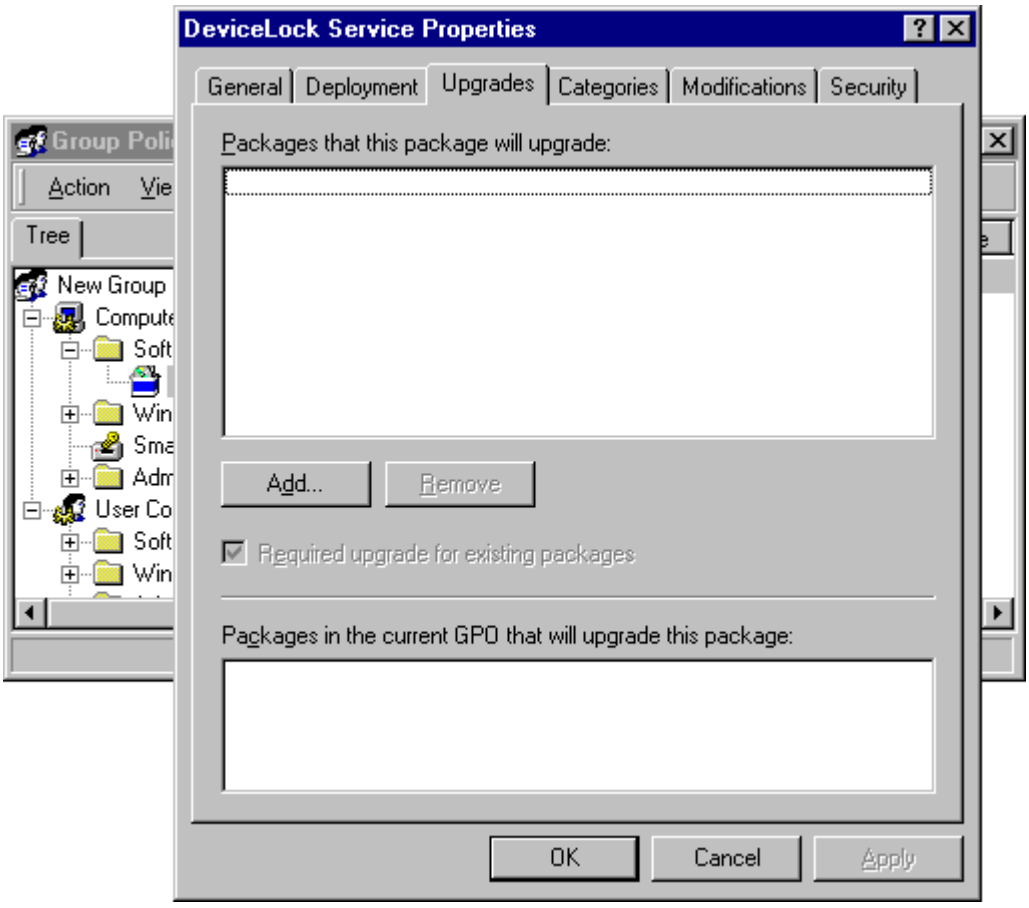
4. В диалоге *Open* введите полный сетевой путь (UNC) к общей сетевой папке, содержащей новый MSI-пакет. Например: *\\file server\share\DeviceLock Service.msi*.

5. Нажмите *Open*.

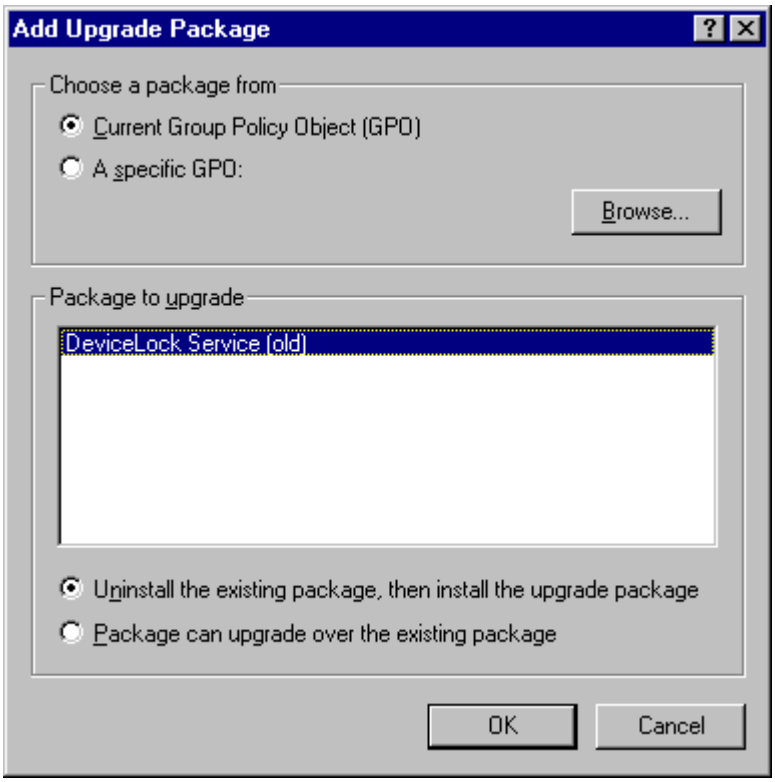
6. Выберите опцию *Assigned*, а затем нажмите *OK*. Новый пакет будет добавлен в правую часть окна *Group Policy*.



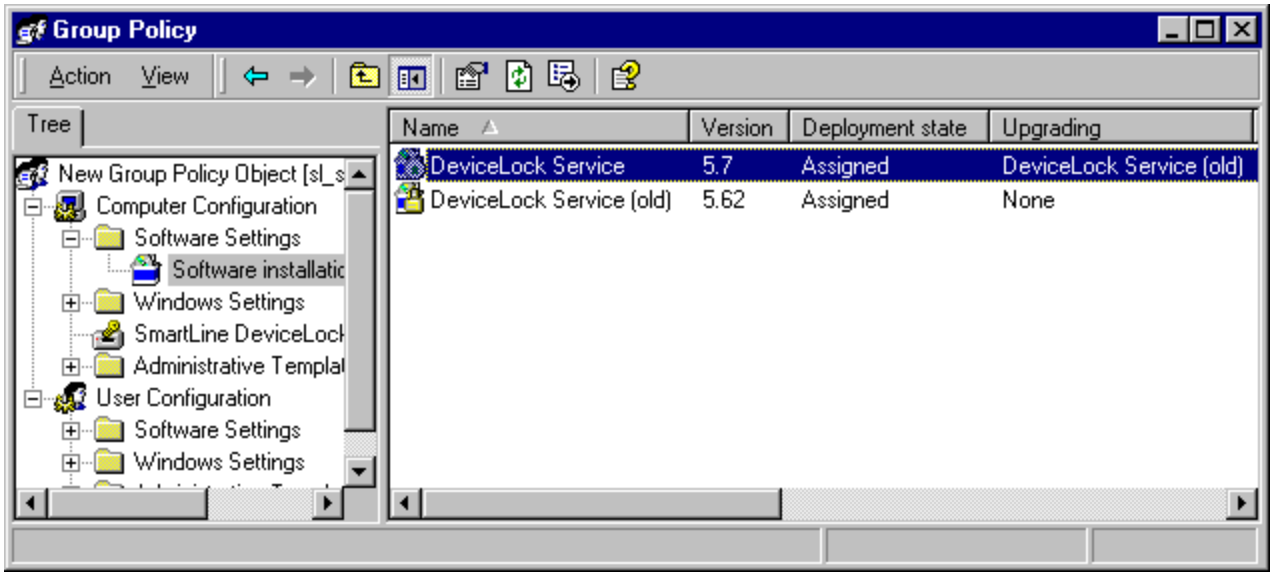
7. Нажмите правой кнопкой мыши на новом пакете, выберите *Properties*, а затем кликните на вкладке *Upgrades*.



8. Нажмите на кнопку *Add*, выберите старый пакет DeviceLock Service, который вы хотите обновить, выберите опцию *Uninstall the existing package, then install the upgrade package* и затем нажмите на *OK*.



9. Нажмите *OK,* чтобы закрыть окно *Properties*, закройте редактор политик. DeviceLock Service будет обновлен на компьютерах при их следующем включении.



ПРИМЕЧАНИЕ: Обычно когда вы обновляете DeviceLock Service, новый MSI-пакет сам обнаруживает предыдущую установку в объекте групповых политик и автоматически совершает все действия, описанные в пунктах 7 и 8.

- Переустановка пакета

  В некоторых случаях вам может потребоваться переустановить текущую версию DeviceLock Service. Для переустановки пакета:

  1. Откройте объект групповой политики, содержащий установленный DeviceLock Service, в редакторе политик Windows Group Policy Object (используйте оснастку *Group Policy Management* или *Active Directory Users and Computers*).

  2. В разделе *Computer Configuration* раскройте пункт *Software Settings*.

  3. Выберите запись, которая соответствует установленному пакету.

  4. В правой части окна *Group Policy* нажмите правой кнопкой мыши на запись пакета, выберите *All Tasks*, затем кликните *Redeploy application*. Будет показано сообщение: “*Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?*”

  5. Нажмите *Yes*.

  6. Закройте редактор политик.

- Удаление пакета

  Чтобы удалить DeviceLock Service:

  1. Откройте объект групповой политики, содержащий установленный DeviceLock Service, в редакторе политик Windows Group Policy Object (используйте оснастку *Group Policy Management* или *Active Directory Users and Computers*).

  2. В разделе *Computer Configuration* раскройте пункт *Software Settings*.

  3. Выберите запись, которая соответствует установленному пакету.

  4. В правой части окна *Group Policy* нажмите правой кнопкой мыши на запись пакета, выберите *All Tasks* и затем кликните *Remove*.

  5. Выберите *Immediately uninstall the software from users and computers*, затем кнопку *OK*.

  6. Закройте редактор политик.

Пожалуйста, имейте в виду:

- Установка и удаление происходит только при включении компьютера. Это предохраняет от нежелательных результатов, таких как удаление или обновление приложения, используемого в данный момент пользователями.

- DeviceLock Service будет скопирован в системную папку Windows (например, *c:\winnt\system32*), если он еще не установлен в системе. Если старая версия DeviceLock Service уже была установлена, то DeviceLock Service будет скопирован в папку, где установлена эта предыдущая версия и заменит ее.

Дополнительную информацию об использовании оснастки *Group Policy Management* можно получить в статье “*New ways to do familiar tasks using GPMC*”, расположенной на сайте Microsoft:
http://technet2.microsoft.com/WindowsServer/en/library/7c73c060-3c97-4aad-95d3-2182d4692ded1033.mspx?mfr=true

Если вы не используете оснастку *Group Policy Management*, вам может быть интересна другая статья – “*New ways to do familiar Group Policy tasks (pre-GPMC)*”:
http://technet2.microsoft.com/WindowsServer/en/library/f5860815-522a-4159-906b-bc606335948e1033.mspx?mfr=true

Также прочитайте статью “*Deploying and upgrading software*”:
http://technet2.microsoft.com/WindowsServer/en/library/fdbf74c6-2b98-4a79-815b-d831d8d757b51033.mspx?mfr=true

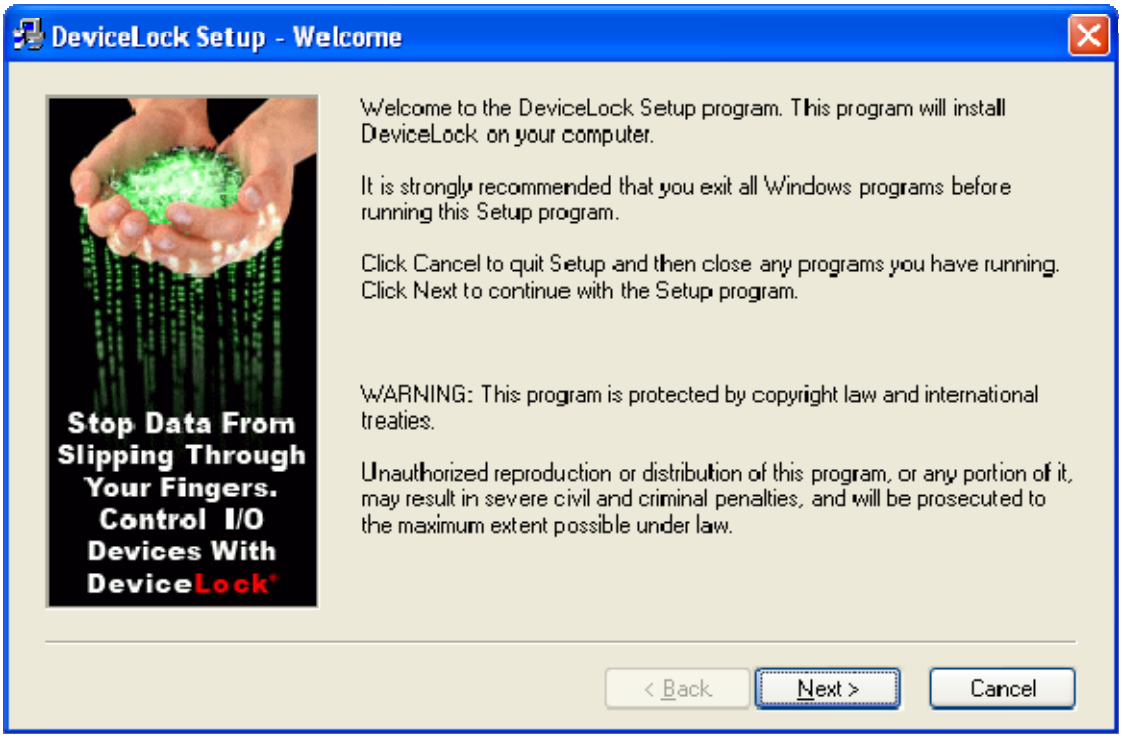
2.3 Установка консолей управления

Консоли управления – это интерфейсы контроля, которые системный администратор использует для удаленного управления DeviceLock Service и DeviceLock Enterprise Server'ом.

Консоли управления DeviceLock должны быть установлены на компьютер, с которого администратор планирует управлять установками DeviceLock'а. Нет необходимости устанавливать консоли управления на сервер (контроллер домена или любой другой). Даже если вы планируете использовать консоль DeviceLock Group Policy Manager для управления настройками через групповые политики Active Directory, вы можете делать это со своего рабочего компьютера (для этого, разумеется, требуются соответствующие доменные привилегии).

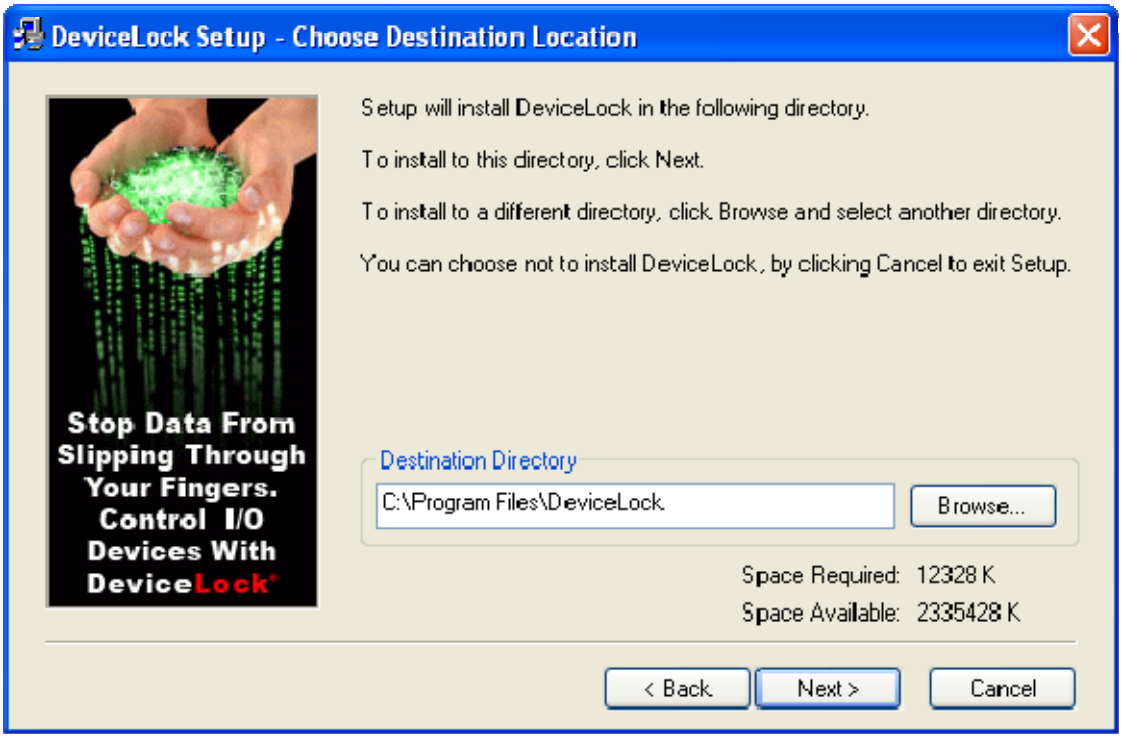
ПРИМЕЧАНИЕ: Чтобы использовать DeviceLock Management Console (оснастка для MMC) и DeviceLock Service Settings Editor на компьютерах с Windows NT 4.0, вы должны установить Microsoft Management Console. Вы можете скачать это обновление совершенно бесплатно с сайта Microsoft: http://www.microsoft.com/downloads/details.aspx?familyid=3F620A07-C996-4A81-AAD8-30134A43EC46&displaylang=en.

Запустите программу установки (*setup.exe*) и следуйте инструкциям на экране.

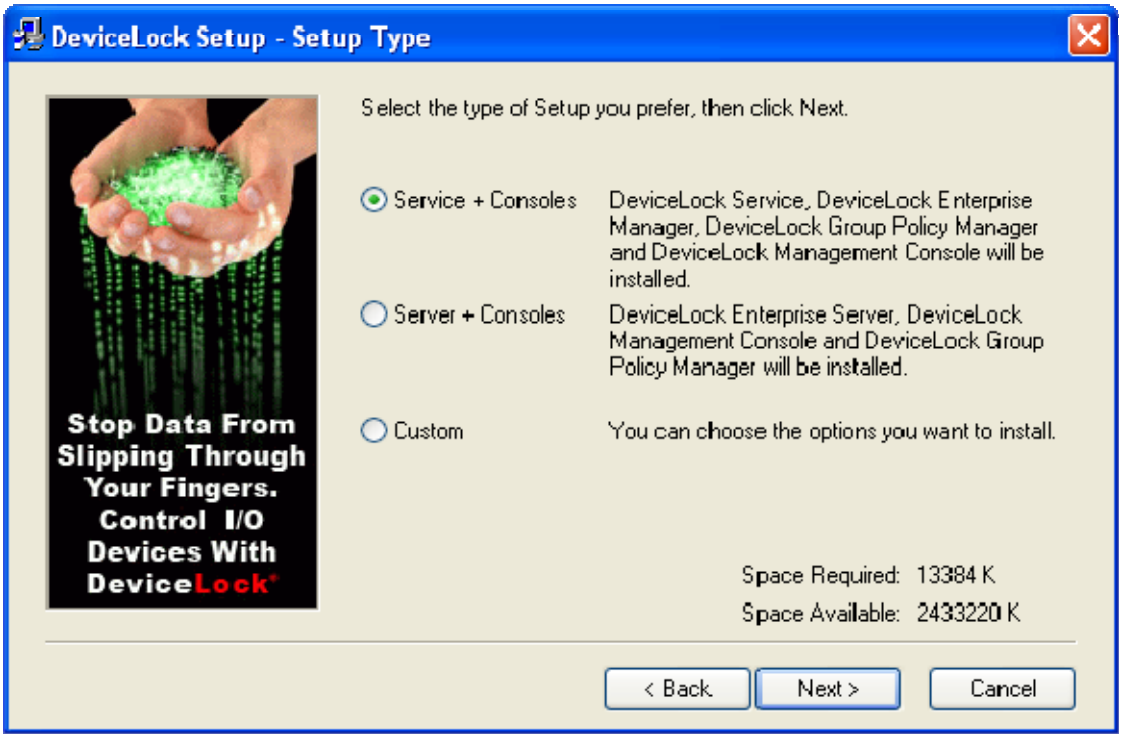


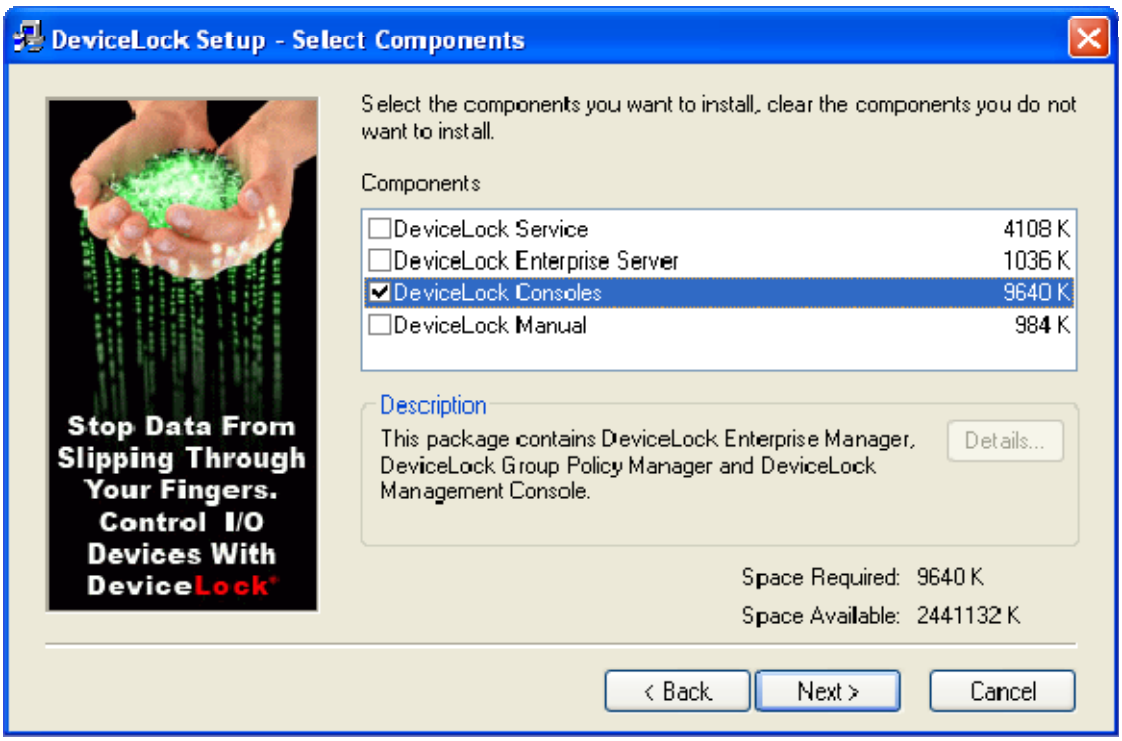
Вы должны принять лицензию на использование программы перед тем как продолжить установку.

DeviceLock устанавливается в каталог, выбранный вами. Сначала программа установки попытается найти предыдущую версию DeviceLock и, если она существует, то вам будет предложен тот же каталог. Если предыдущей установки найдено не было, программа предложит вам установить DeviceLock в каталог Program Files системного диска (например, *C:\Program Files\DeviceLock*). В любом случае вы можете сами выбрать любой другой каталог.



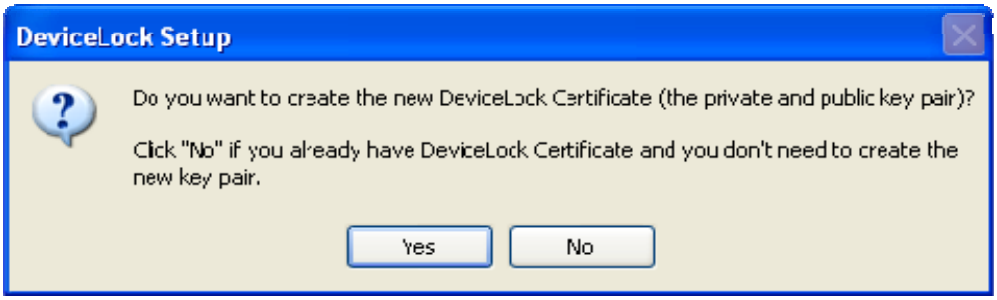
У вас есть три варианта выбора: установить DeviceLock Service и консоли управления DeviceLock, выбрав опцию *Service + Consoles*; установить DeviceLock Enterprise Server и консоли управления, выбрав опцию *Server + Consoles*; или установить только консоли управления, выбрав опцию *Custom* и затем отметив компонент *DeviceLock Consoles*.





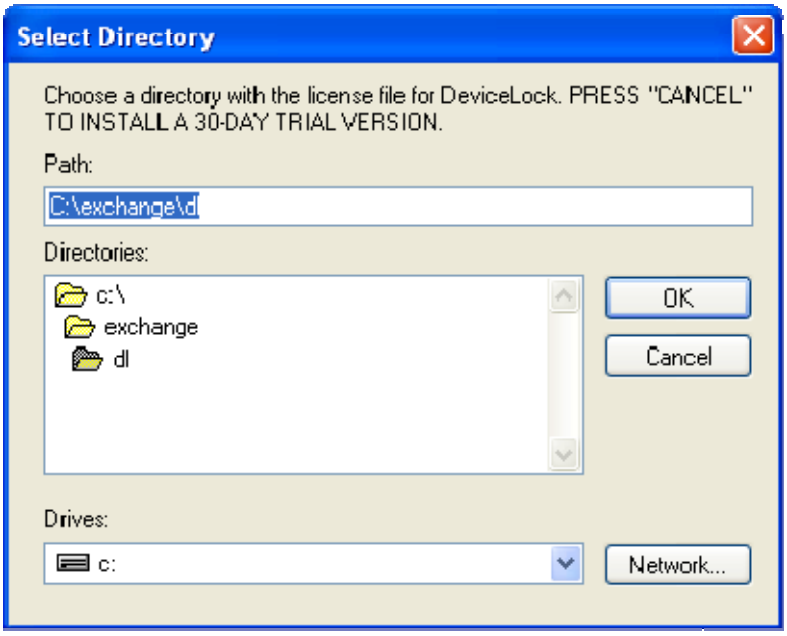
DeviceLock поставляется с тремя различными консолями управления: DeviceLock Management Console (оснастка для MMC), DeviceLock Enterprise Manager и DeviceLock Group Policy Manager (интегрируется в редактор групповых политик Windows). Также вместе с остальными консолями управления устанавливается и DeviceLock Service Settings Editor, который служит для создания и редактирования внешних XML-файлов с разрешениями, правилами аудита и настройками DeviceLock Service.

Программа установки может предложить вам создать новый сертификат (DeviceLock Certificate).

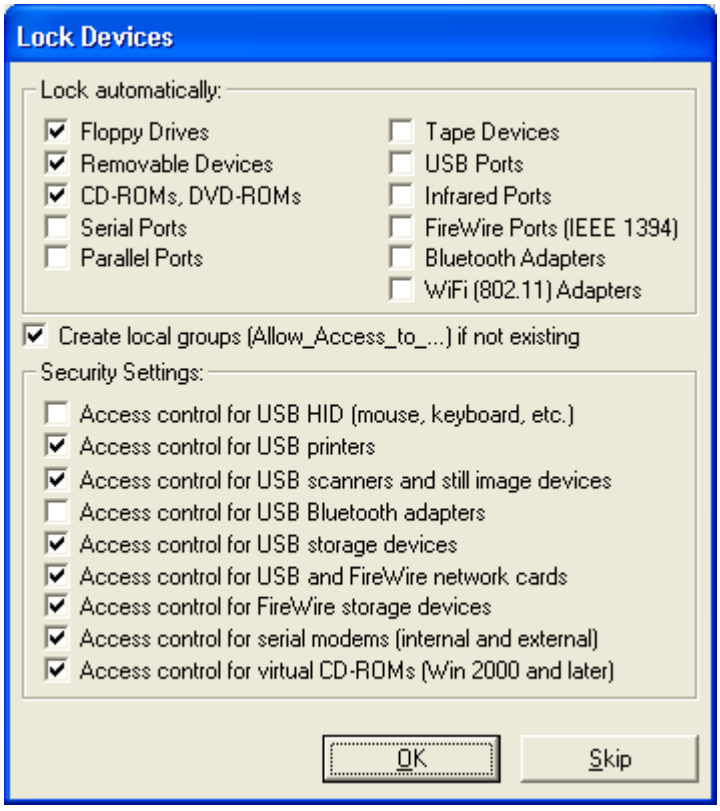


Вы всегда можете создать новый сертификат позже, используя специальную программу Certificate Generation Tool, устанавливаемую вместе с консолями управления DeviceLock. Поэтому, если на этом шаге установки вы не уверены в том, нужен вам новый сертификат или нет, просто нажмите кнопку *No* и продолжайте установку.

Также программа установки может предложить вам указать лицензионный файл. Если у вас нет лицензионного файла, нажмите кнопку *Cancel,* чтобы установить DeviceLock в ознакомительном 30-ти дневном режиме.

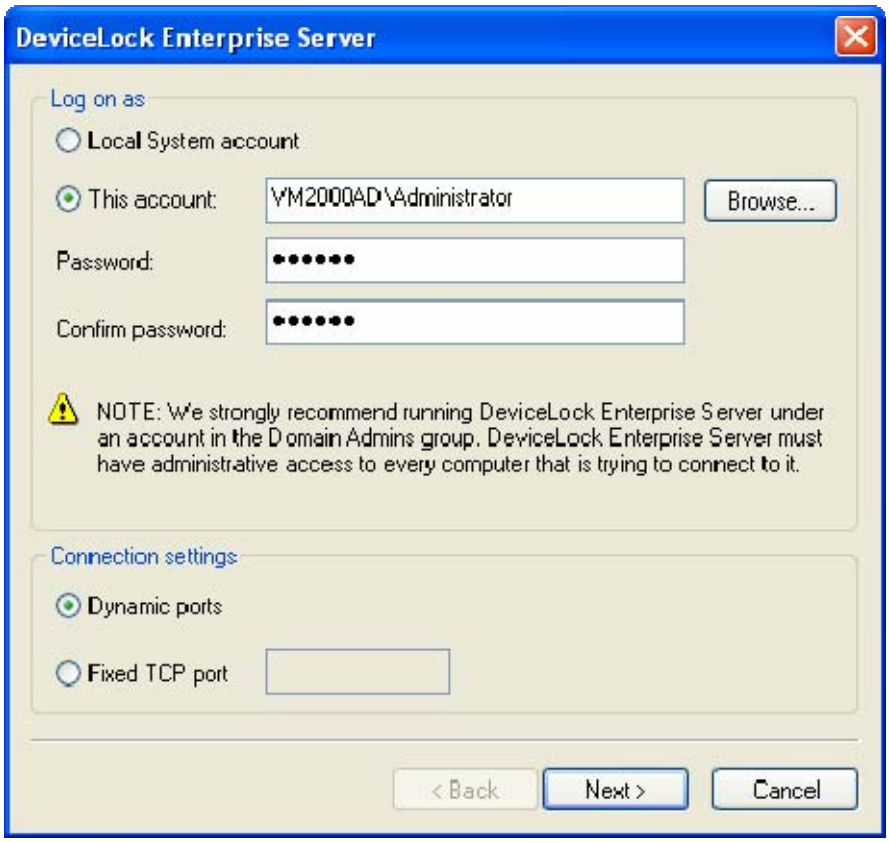


Если вы выбрали установку DeviceLock Service, вам будет предложено задать разрешения для локальных устройств.



Нажмите кнопку *Skip,* если вы предпочитаете устанавливать разрешения используя консоли управления DeviceLock. Дополнительную информацию относительно этих установок вы можете найти в главе **Развертывание DeviceLock Service** данного руководства.

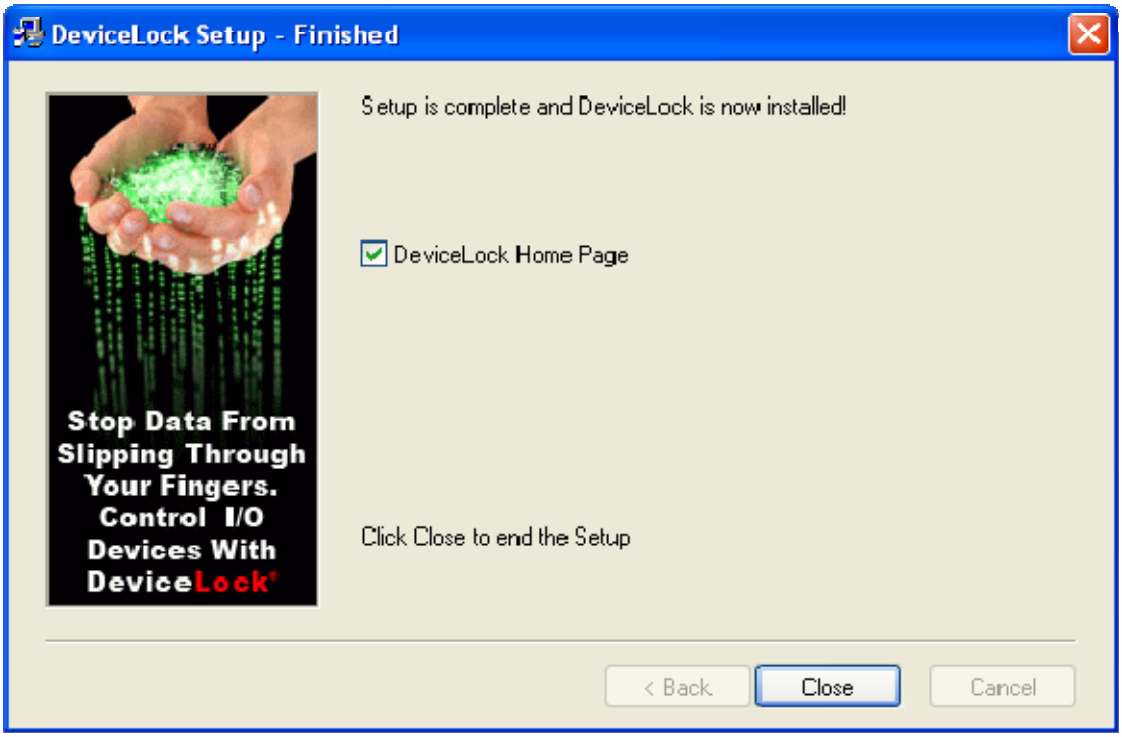
Если вы также выбрали установку DeviceLock Enterprise Server'а, программа установки предложит вам настроить его, используя специальный мастер настроек.



Дополнительную информацию относительно этих настроек вы можете найти в главе **Установка DeviceLock Enterprise Server** данного руководства.

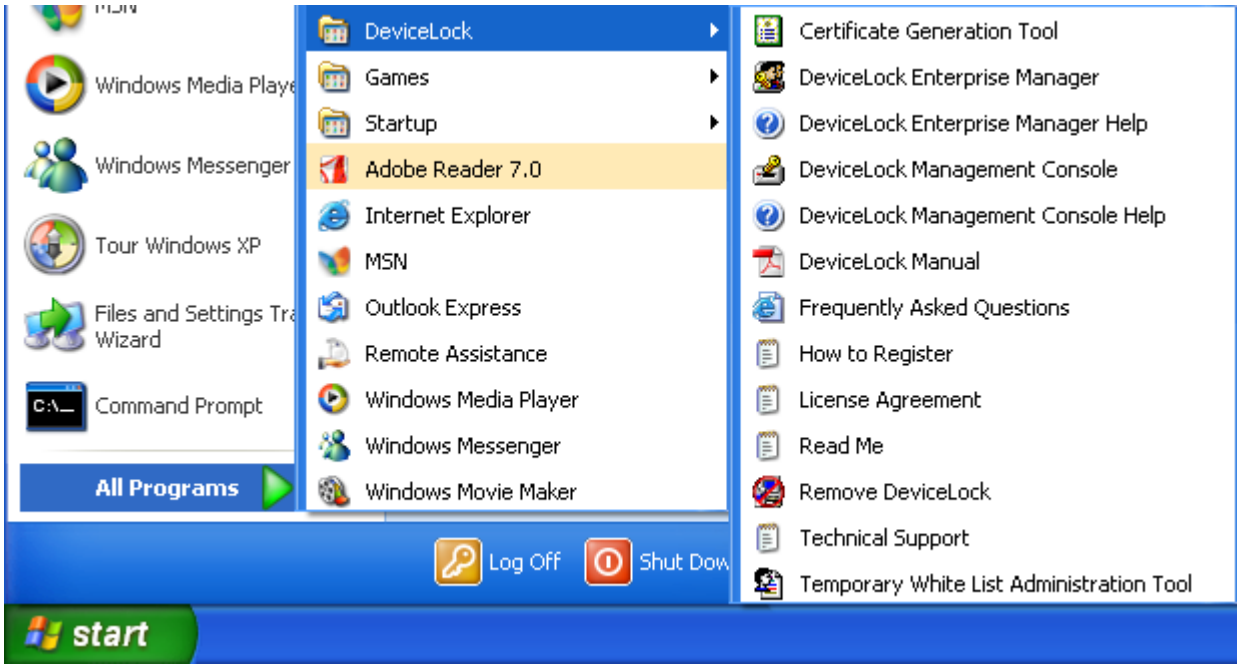
Вы можете добавить ярлыки быстрого запуска для DeviceLock Management Console, DeviceLock Enterprise Manager'а и для DeviceLock Service Settings Editor'а на ваш текущий рабочий стол.

В конце установки программа предложит вам открыть сайт DeviceLock.



Снимите галочку с *DeviceLock Home Page*, если вы не хотите открывать сайт DeviceLock в данный момент. Нажмите кнопку *Close,* чтобы завершить процесс установки.

Консоли управления DeviceLock доступны в меню *Programs*, появляющемся при нажатии на кнопку *Start*.



ПРИМЕЧАНИЕ: DeviceLock Group Policy Manager интегрируется в редактор групповых политик Windows и недоступен как отдельное приложение. Чтобы использовать DeviceLock Group Policy Manager, вы должны запустить стандартный Windows Group Policy Editor.

2.4 Установка DeviceLock Enterprise Server

DeviceLock Enterprise Server – это дополнительный необязательный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита. DeviceLock Enterprise Server также поддерживает централизованный мониторинг, позволяющий контролировать текущее состояние агентов на удаленных компьютерах путем периодического опроса.

Чтобы использовать DeviceLock Enterprise Server на компьютерах с Windows NT 4.0 SP6 и Windows 2000, вам необходимо установить на эти компьютеры Microsoft Data Access Components (MDAC) версии 2.8 или более поздней. MDAC доступен для свободного скачивания с сайта Microsoft: http://www.microsoft.com/downloads/details.aspx?familyid=78cac895-efc2-4f8e-a9e0-3a1afbd5922e&displaylang=ru.

2.4.1 Планирование инфраструктуры

Вы можете установить несколько экземпляров DeviceLock Enterprise Server в вашей сети, чтобы равномерно распределить нагрузку на каждый из них и на всю сеть в целом.

DeviceLock Enterprise Server использует MS SQL Server для хранения своих данных. Следовательно, необходимо установить и запустить MS SQL Server в вашей сети до того, как вы будете устанавливать DeviceLock Enterprise Server. Если у вас нет MS SQL Server'а, вы может установить и использовать бесплатную версию под названием SQL Server Express Edition, которая доступна для свободного скачивания с сайта Microsoft: http://msdn.microsoft.com/vstudio/express/sql/download/.

Нет необходимости устанавливать MS SQL Server и DeviceLock Enterprise Server на один и тот же компьютер. Более того, чтобы повысить производительность и надежность всей системы, рекомендуется устанавливать DeviceLock Enterprise Server на отдельный компьютер.

Есть три варианта использования "связки" DeviceLock Enterprise Server и MS SQL Server. Вы должны выбрать наиболее подходящий для вас вариант перед установкой DeviceLock Enterprise Server'а:

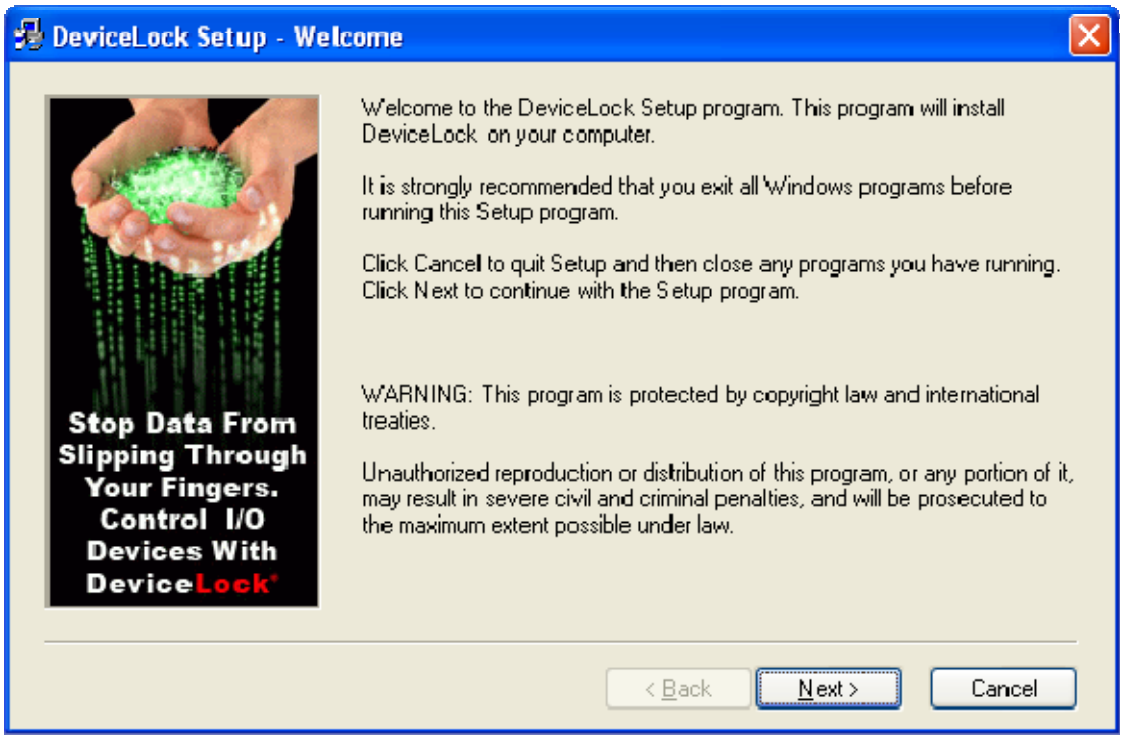
1. ОДИН К ОДНОМУ: вы устанавливаете один DeviceLock Enterprise Server и соединяете его с одним MS SQL Server'ом. Этот вариант больше всего подходит для маленьких сетей (несколько сотен компьютеров).

2. МНОГО КО МНОГО: вы устанавливаете несколько DeviceLock Enterprise Servers'ов и каждый соединяете с отдельным MS SQL Server'ом. Этот вариант подходит для средних и больших сетей, разделенных на несколько сегментов и имеющих медленные соединения между этими сегментами.

3. МНОГО К ОДНОМУ: вы устанавливаете несколько DeviceLock Enterprise Server'ов и все их соединяете с одним MS SQL Server'ом. Этот вариант подходит для средних и больших сетей, где имеется отдельный мощный компьютер (с большим объемом оперативной памяти и дискового пространства), выделенный под MS SQL Server.

2.4.2 Интерактивная установка

Запустите программу установки (*setup.exe*) и следуйте инструкциям на экране. Вам необходимо запускать *setup.exe* на каждом компьютере, где должен быть установлен DeviceLock Enterprise Server.

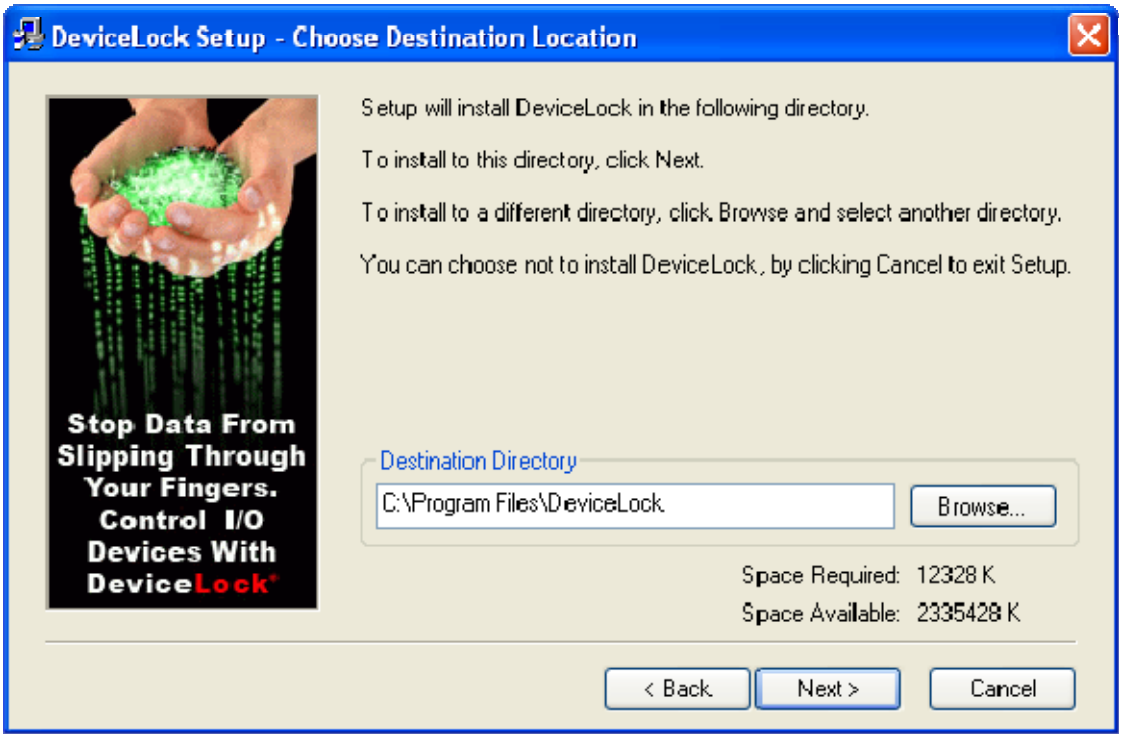


Вы должны принять лицензию на использование программы перед тем как продолжить установку.

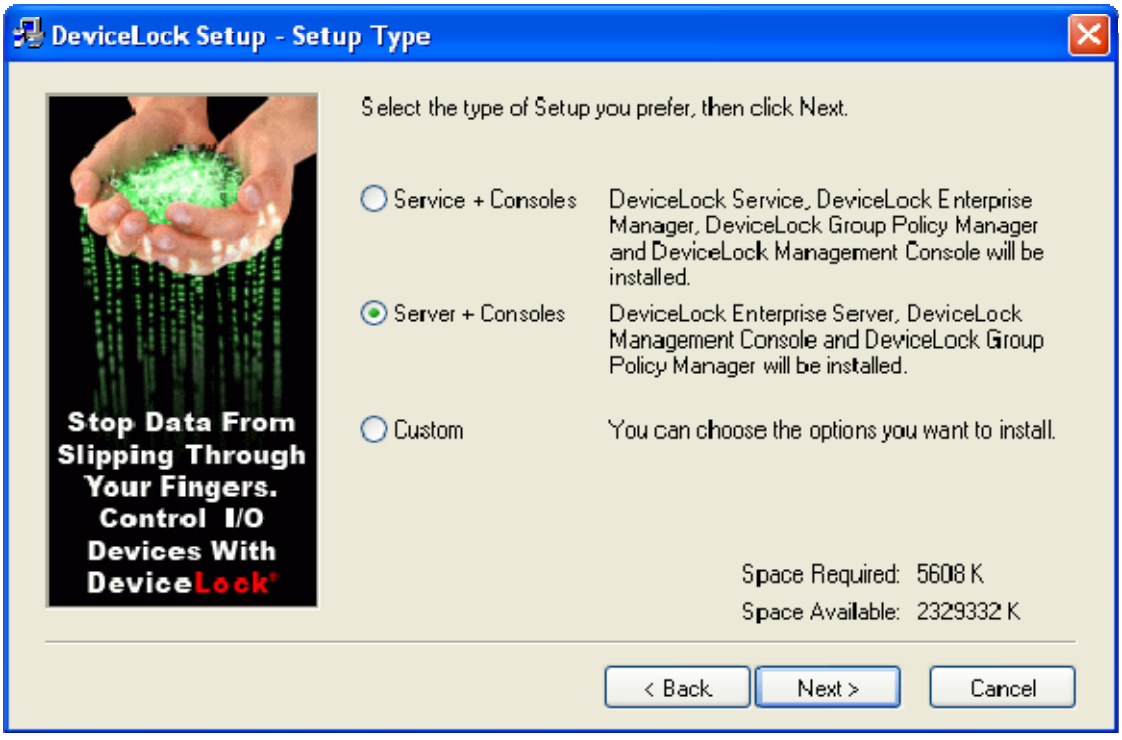
DeviceLock устанавливается в каталог, выбранный вами. Сначала программа установки попытается найти предыдущую версию DeviceLock и, если она существует, то вам будет предложен тот же каталог.

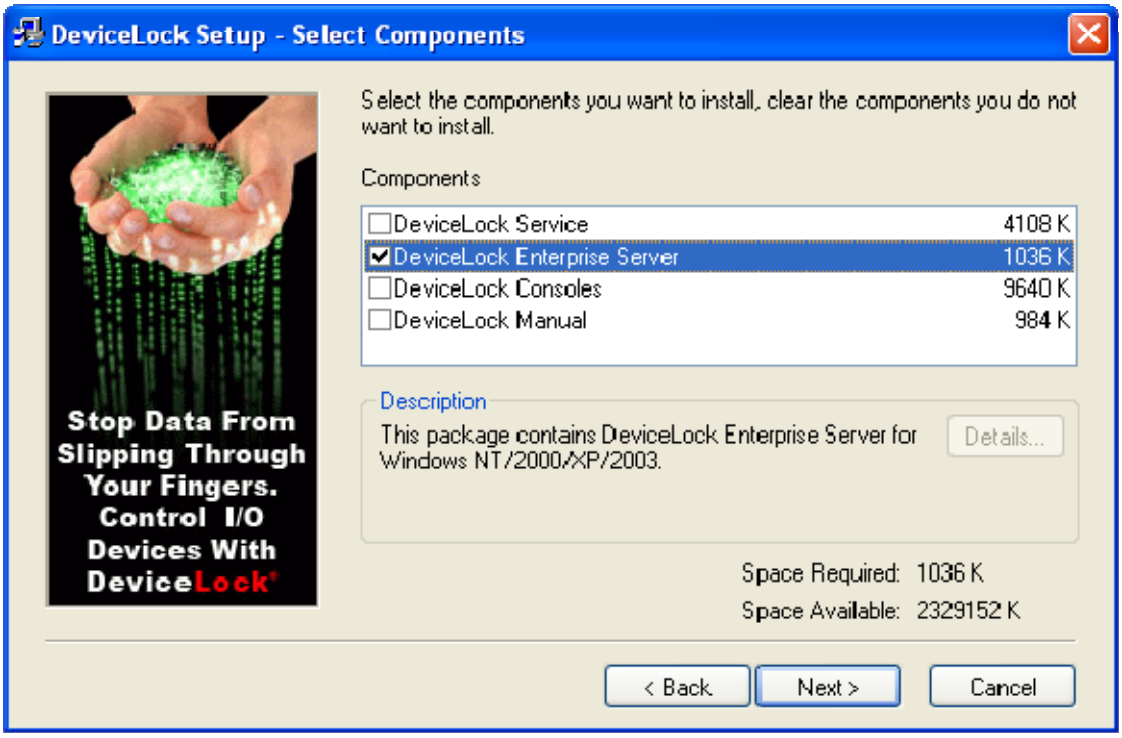
Если предыдущей установки найдено не было, программа предложит вам установить DeviceLock в каталог Program Files системного диска (например, *C:\Program Files\DeviceLock*).

В любом случае, вы можете сами выбрать любой другой каталог.

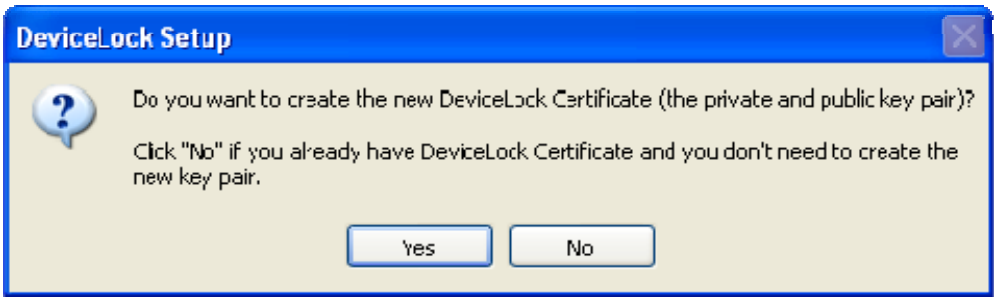


У вас есть два варианта выбора: установить DeviceLock Enterprise Server и консоли управления DeviceLock, выбрав опцию *Server + Consoles* или установить только DeviceLock Enterprise Server, выбрав опцию *Custom* и затем отметив компонент *DeviceLock Enterprise Server*.





Если вы выбрали установку консолей управления DeviceLock, программа может предложить вам создать новый сертификат (DeviceLock Certificate).



Вы всегда можете создать новый сертификат позже, используя специальную программу Certificate Generation Tool, устанавливаемую вместе с консолями управления DeviceLock. Поэтому, если на этом шаге установки вы не уверены в том, нужен вам новый сертификат или нет, просто нажмите кнопку *No* и продолжайте установку.

Если программа установки обнаруживает что MS SQL Server не запущен на локальном компьютере и при этом его дистрибутив доступен, программа предложит вам запустить процесс установки MS SQL Server'а.

Если вы не хотите устанавливать MS SQL Server на локальный компьютер или он уже установлен, но не запущен – нажмите кнопку *No* и продолжайте установку.

В процессе установки вам необходимо сконфигурировать DeviceLock Enterprise Server и задать его основные параметры, используя специальный мастер настроек.

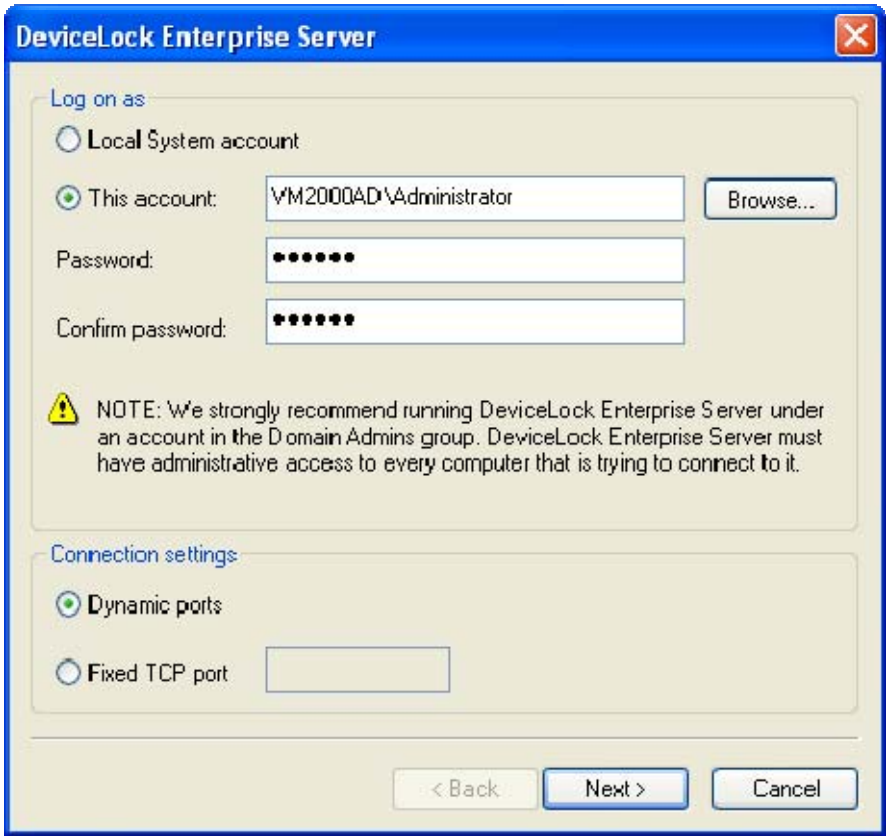
Если вы устанавливаете обновление DeviceLock Enterprise Server'а или просто переустанавливаете его и при этом не хотите ничего менять в текущих настройках, вы можете нажать кнопку *Cancel,* чтобы закрыть мастер настроек и сохранить текущую конфигурацию.

В случае, если вам все же надо изменить какой-либо параметр, но сохранить все остальные настройки – отредактируйте только этот нужный параметр и пройдите через все страницы мастера настроек и нажмите кнопку *Finish* на последней странице.

ПРИМЕЧАНИЕ: Если вы устанавливаете DeviceLock Enterprise Server в первый раз на данный компьютер и при этом закрываете мастер настроек, не задав все необходимые параметры, программа установки не сможет установить и запустить службу DeviceLock Enterprise Server'а и вам будет предложено запустить мастер настроек снова.

Если вы нажмете No для продолжения без установки службы DeviceLock Enterprise Server'а, то вам будет нужно запустить программу установки позже и установить эту службу в любом случае.

На первой странице мастера настроек вы можете задать параметры запуска службы DeviceLock Enterprise Server'а.



1.1. Log on as

Прежде всего вы должны выбрать учетную запись, которая будет использоваться для запуска службы DeviceLock Enterprise Server'а. Как и многие другие службы Windows, служба DeviceLock Enterprise Server'а может запускаться как под учетной записью системы (*СИСТЕМА*), так и от имени любого другого пользователя с соответствующими правами.

Чтобы запустить службу под учетной записью *СИСТЕМА*, выберите опцию *Local System account*. Имейте в виду, что программы, работающие под пользователем *СИСТЕМА,* не могут иметь доступ к общим сетевым ресурсам и авторизуются на удаленных компьютерах под анонимным непривилегированным пользователем. Таким образом, DeviceLock Enterprise Server, запущенный под учетной записью *СИСТЕМА*, не может хранить файлы теневого копирования на удаленных компьютерах (например, на файловых серверах) и должен использовать сертификат (DeviceLock Certificate) для авторизации на DeviceLock Service'ах, работающих на удаленных компьютерах.

Дополнительную информацию о методах авторизации можно прочитать в описании параметра Certificate Name.

Чтобы запустить службу от имени пользователя, выберите опцию *This account*, введите имя пользователя и его пароль. Рекомендуется использовать учетную запись пользователя, которая имеет административные привилегии на всех компьютерах, где работает DeviceLock Service. В противном случае вам будет необходимо использовать авторизацию, основанную на сертификате (DeviceLock Certificate).

Если вы устанавливаете DeviceLock Enterprise Server в домене, то мы рекомендуем вам использовать учетную запись пользователя, входящую в группу доменных администраторов (*Domain Admins*). Поскольку группа доменных администраторов входит в локальную группу *Администраторы* на каждом компьютере-члене домена, то члены группы доменных администраторов будут иметь полный доступ к DeviceLock Service на каждом компьютере этого домена.

Также не стоит забывать, что если включена защита DeviceLock Service от пользователей с правами локального администратора (снят флаг *Enable Default Security* в DeviceLock Administrators), то учетная запись, указанная в параметре *This account,* должна быть в списке администраторов DeviceLock с правом **Full access**. В противном случае вам будет необходимо использовать авторизацию, основанную на сертификате (DeviceLock Certificate).

1.2. Connection settings

Вы можете настроить DeviceLock Enterprise Server на использование фиксированного TCP-порта при установлении связи с консолью управления. Укажите номер порта в параметре *Fixed TCP port*. Для использования динамической привязки к портам выберите опцию *Dynamic ports*. По умолчанию DeviceLock Enterprise Server использует порт 9133.

Нажмите на кнопку *Next*, чтобы запустить службу DeviceLock Enterprise Server'а и перейти ко второй странице мастера настроек.

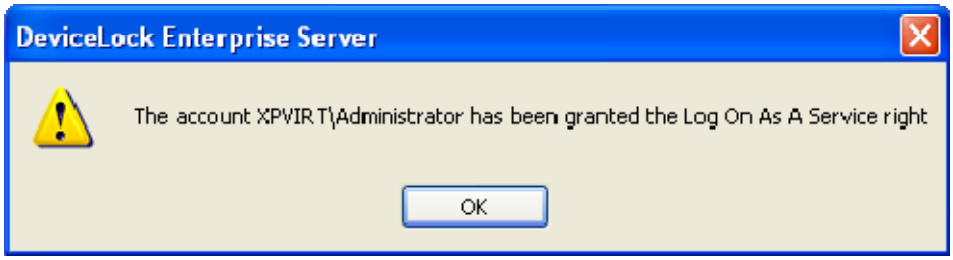
Если текущий пользователь, использующий мастер настроек, не имеет полного административного доступа к DeviceLock Enterprise Server'у (в случае, когда вы устанавливаете обновление поверх уже настроенного сервера), мастер настроек не сможет применить новые параметры. Подобная ошибка также возникает, когда текущий пользователь не имеет привилегий локального администратора на компьютере, где устанавливается DeviceLock Enterprise Server.

Если вы указали неверное имя учетной записи в *This account* или неверный пароль для нее, то DeviceLock Enterprise Server не сможет запуститься.

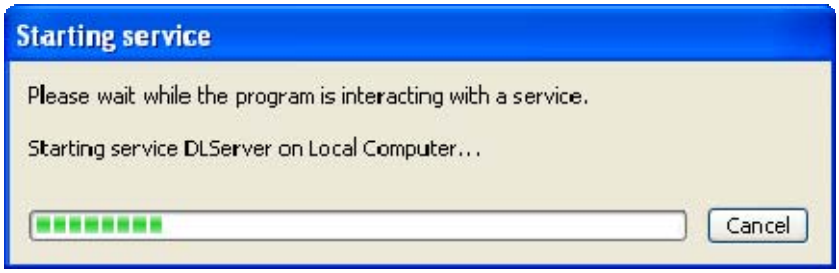
Вы будете предупреждены, если учетная запись, указанная в *This account*, не является членом группы доменных администраторов (*Domain Admins)*.

Вы можете продолжить, нажав на кнопку *Yes*. Тем не менее, имейте в виду, что в этом случае указанная учетная запись пользователя должна иметь полный административный доступ ко всем удаленным компьютерам с запущенными DeviceLock Service'ами, либо *открытый* ключ сертификата (DeviceLock Certificate) должен быть установлен на каждом компьютере с DeviceLock Service.

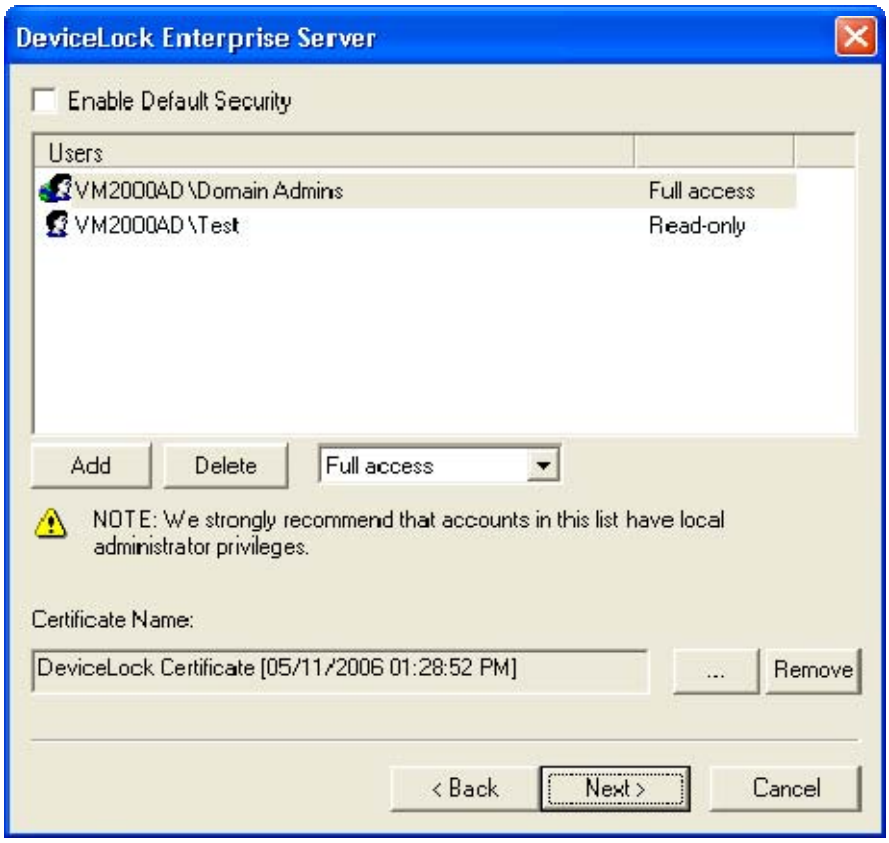
Если учетная запись пользователя, указанная в *This account*, не имеет системной привилегии *Log On As A Service*, то мастер настроек автоматически присвоит ей эту привилегию. Данная привилегия необходима, чтобы запускать службы от имени пользователя.



Если все параметры запуска службы были указаны корректно, то мастер настроек запустит DeviceLock Enterprise Server.



На второй странице мастера настроек вы можете задать список учетных записей, которые будут иметь административный доступ к DeviceLock Enterprise Server'у, а также установить *секретный* ключ сертификата (DeviceLock Certificate).



2.1. Enable Default Security

При контроле доступа к DeviceLock Enterprise Server'у по умолчанию все пользователи с привилегиями локальных администраторов могут подключаться к DeviceLock Enterprise Server'у с помощью консоли управления, изменять его настройки и смотреть отчеты.

Чтобы включить контроль доступа по умолчанию, установите флаг *Enable Default Security*.

Если же вам необходим более гибкий контроль доступа к DeviceLock Enterprise Server'у, отключите контроль по умолчанию, сняв флаг *Enable Default Security*.

Затем вам будет нужно задать список авторизованных учетных записей (пользователи и/или группы), которые смогут подключаться к DeviceLock Enterprise Server'у. Чтобы добавить новую учетную запись, нажмите на кнопку *Add*. Вы можете добавить несколько записей одновременно.

Чтобы удалить запись из списка, нажмите на кнопку *Delete*. Для удаления нескольких записей одновременно используйте клавиши *Ctrl* и/или *Shift*.

Чтобы определить, какие действия разрешены для пользователя или группы, установите соответствующие права:

- **Full access** – предоставляется полный доступ к DeviceLock Enterprise Server'у. Пользователи могут менять настройки и смотреть отчеты.

- **Change** – предоставляется доступ для изменения настроек, установки и удаления DeviceLock Enterprise Server'а, а также для просмотра отчетов. Пользователи не могут добавлять новые учетные записи в список администраторов сервера и изменять права доступа для уже существующих в этом списке учетных записей.

- **Read-only** – предоставляется доступ только для просмотра настроек DeviceLock Enterprise Server'а и отчетов. Пользователи не могут ничего изменять в конфигурации.

ПРИМЕЧАНИЕ: Мы настоятельно рекомендуем вам, чтобы учетные записи, включенные в этот список, имели привилегии локального администратора, поскольку в некоторых ситуациях (установка, обновление и деинсталляция службы DeviceLock Enterprise Server'а) может потребоваться доступ к Windows Service Control Manager (SCM) и общим сетевым ресурсам.

2.2. Certificate Name

Вам может понадобится установить *секретный* ключ на DeviceLock Enterprise Server, чтобы включить авторизацию, основанную на сертификате (DeviceLock Certificate). Существует два метода авторизации DeviceLock Enterprise Server'а на удаленных компьютерах с работающими DeviceLock Service'ами:

а. *Авторизация по пользователю* – служба DeviceLock Enterprise Server'а запущена и работает от имени пользователя, который имеет полный административный доступ к DeviceLock Service на удаленном компьютере. За информацией о том, как запустить DeviceLock Enterprise Server от имени пользователя обращайтесь к описанию параметра Log on as.

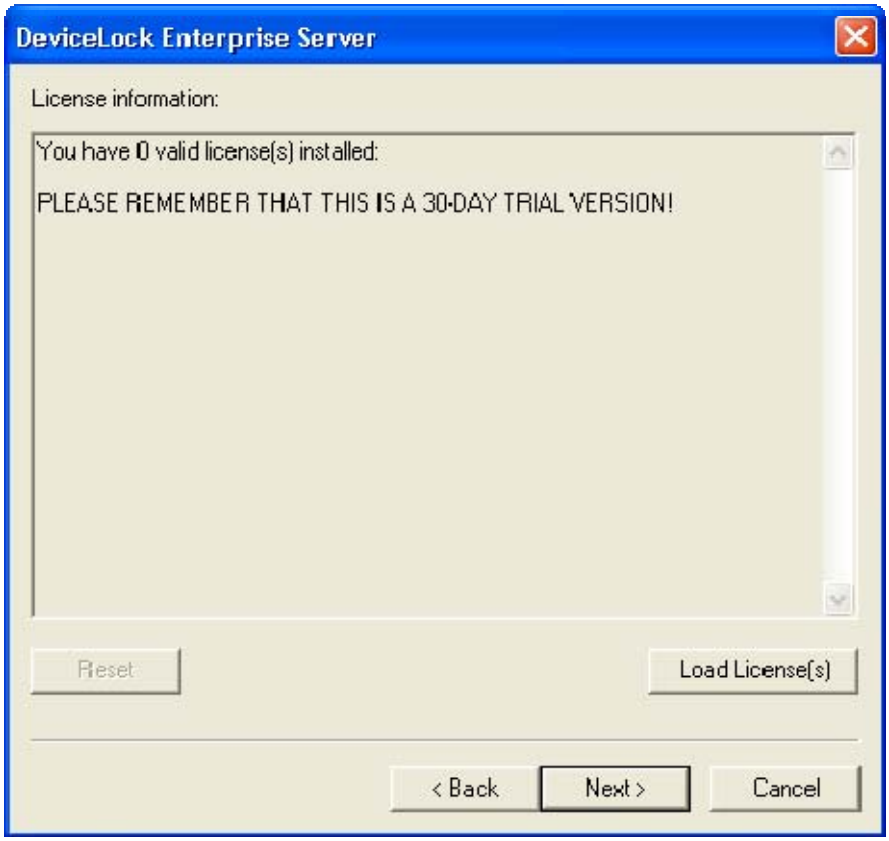
б. *Авторизация по сертификату* – в ситуации, когда учетная запись пользователя, под которой запущен DeviceLock Enterprise Server, не может получить полный доступ к DeviceLock Service, работающему на уделенном компьютере, вы должны использовать авторизацию, основанную на сертификате (DeviceLock Certificate).

   Открытый ключ должен быть установлен на DeviceLock Service и соответствующий ему *секретный* ключ должен быть установлен на DeviceLock Enterprise Server'е.

Чтобы установить сертификат, нажмите на кнопку **…** и выберите файл с *секретным* ключом. Чтобы удалить сертификат, нажмите на кнопку *Remove*.

Чтобы получить дополнительную информацию о сертификате, обратитесь к разделу **DeviceLock Certificate** данного руководства.

Нажмите на кнопку *Next*, чтобы применить настройки и перейти к третьей странице мастера настроек. На этой странице вы можете установить лицензии на DeviceLock.



3.1. License information

Если вы приобрели лицензию на DeviceLock, вы должны установить эту лицензию на DeviceLock Enterprise Server.

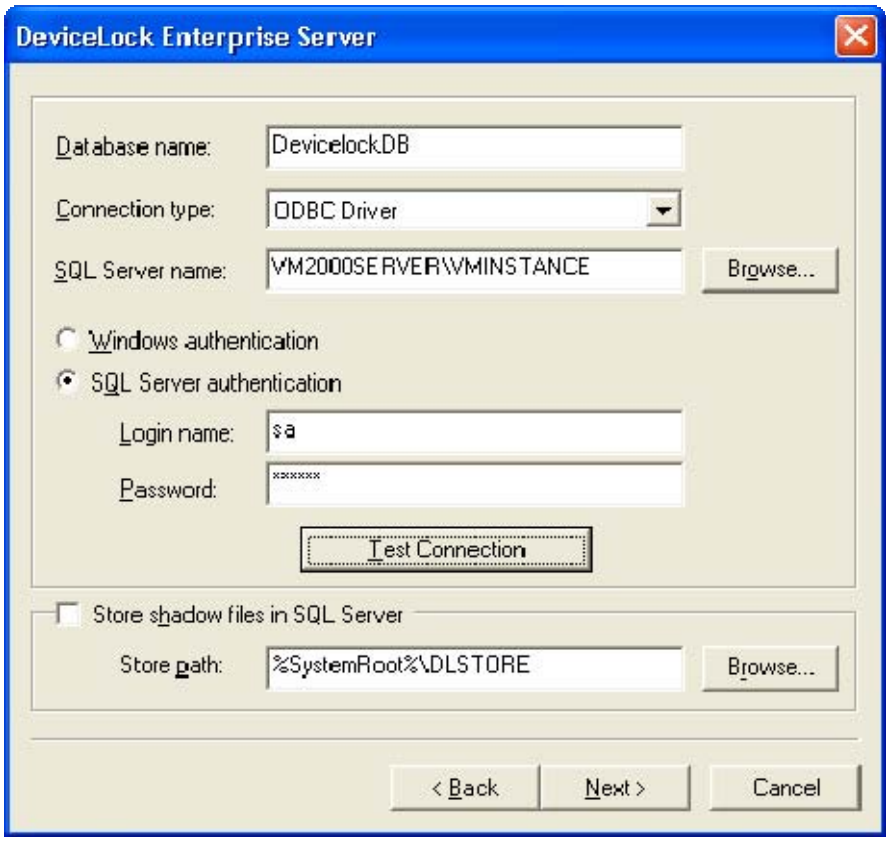
DeviceLock Enterprise Server работает только с тем количеством компьютеров с установленными DeviceLock Service'ами, которое было лицензировано. Например, если у вас есть лицензия на 100 компьютеров, но при этом в вашей сети работает 101 компьютер с DeviceLock Service'ами, то DeviceLock Enterprise Server будет работать только с первыми 100 компьютерами, а последний не лицензированный компьютер будет игнорироваться.

Чтобы установить лицензию, нажмите на кнопку *Load License(s)* и выберите файл с лицензией. Вы можете загрузить несколько файлов подряд – один за другим.

Если не установлено ни одной действительной лицензии, то DeviceLock Enterprise Server работает в ознакомительном режиме и может обслуживать только два компьютера с установленными DeviceLock Service'ами.

Нажмите на кнопку *Next*, чтобы установить лицензии и перейти к четвертой странице мастера настроек.

На четвертой странице вы можете определить настройки, относящиеся к базе данных и к соединению с SQL Server'ом.



4.1. Database name

Вы должны указать имя базы данных в SQL Server'е, которое будет использоваться DeviceLock Enterprise Server'ом для хранения данных. Мастер настроек по умолчанию предлагает имя *DeviceLockDB*.

4.2. Connection type

Есть два способа задать настройки соединения с SQL Server'ом:

a. *ODBC Driver* – вы задаете имя SQL Server'а в параметре *SQL Server name* и выбираете метод авторизации (*Windows* или *SQL Server*).

   Параметр *SQL Server name* должен содержать не просто имя компьютера, на котором запущен SQL Server, а именно полное имя самого SQL Server'а. Обычно имя SQL Server'а состоит из двух частей: имя компьютера и имя экземпляра, разделенные обратным слешем (например, *computer\instance*). Иногда имя экземпляра отсутствует (при настройках SQL Server'а по умолчанию), и вы можете использовать имя компьютера в качестве имени SQL Server'а. Чтобы получить список имен SQL Server'ов доступных в вашей сети, нажмите кнопку *Browse* (вы должны иметь доступ к удаленному реестру компьютера с SQL Server'ом, чтобы получить имя экземпляра).

Если параметр *SQL Server name* пуст, то это означает, что SQL Server работает на том же компьютере что и DeviceLock Enterprise Server и при этом имя его экземпляра не задано (настройка SQL Server'а по умолчанию).

Чтобы установить соединение с SQL Server'ом, вы должны настроить параметры авторизации.

Выберите опцию *Windows authentication* для авторизации на SQL Server'е от имени учетной записи, под которой работает служба DeviceLock Enterprise Server'а.

Если служба работает под учетной записью *СИСТЕМА* и SQL Server находится на удаленном компьютере, DeviceLock Enterprise Server не сможет подсоединиться к SQL Server'у, т.к. учетная запись *СИСТЕМА* не имеет права на доступ к сетевым ресурсам. Дополнительную информацию о том, как запустить DeviceLock Enterprise Server от имени пользователя можно прочитать в описании параметра Log on as.

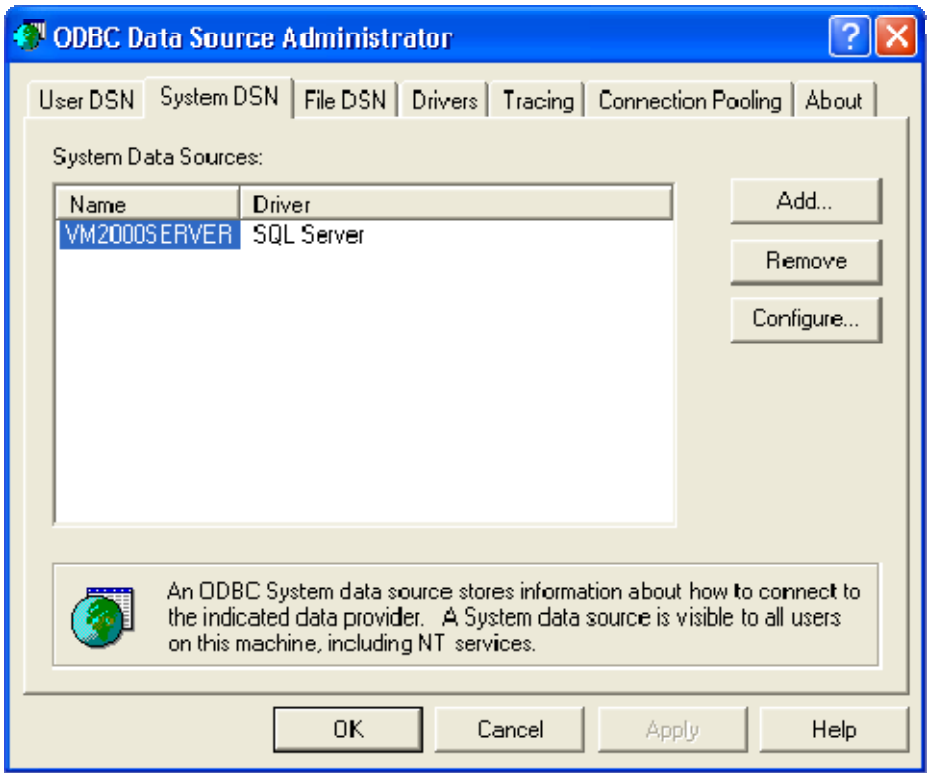
Выберите опцию *SQL Server authentication,* чтобы разрешить SQL Server'у выполнять свою собственную авторизацию, основанную на заранее заданных имени и пароле. Перед тем как включить опцию *SQL Server authentication* убедитесь, что SQL Server был настроен для работы в смешанном режиме авторизации.

Укажите имя пользователя SQL в параметре *Login name* и соответствующий ему пароль в параметре *Password*.

ПРИМЕЧАНИЕ: Режим авторизации Windows намного более надежный и безопасный, чем режим авторизации SQL Server'а. Всегда, когда это возможно, используйте режим авторизации Windows.

б. *System Data Source* – вы выбираете заранее созданный системный источник данных из списка *Data Source Name*.

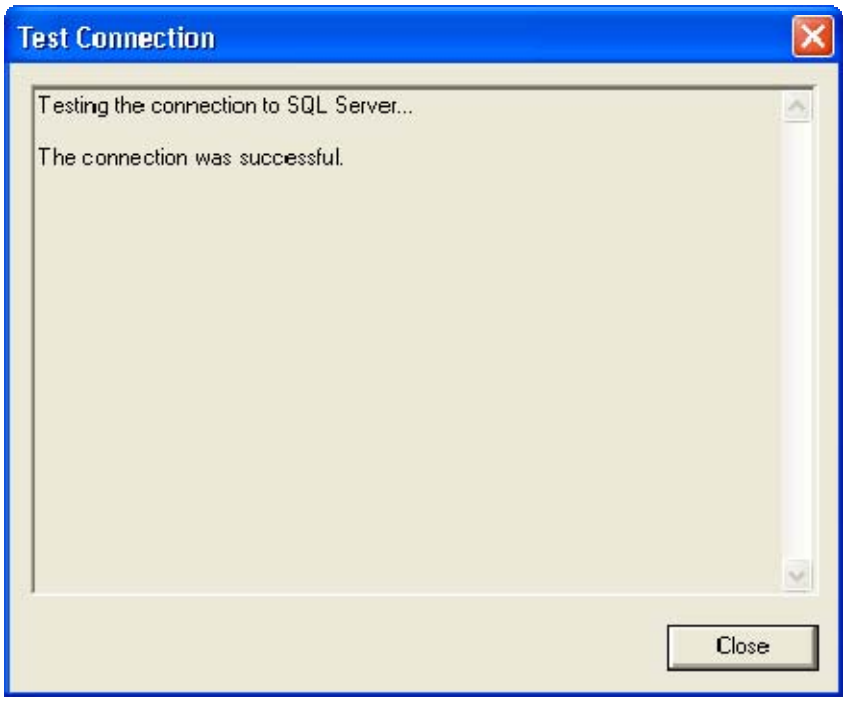
Чтобы задать источник данных, используйте компонент *Data Sources (ODBC)* в *Control Panel -> Administrative Tools*.



Если при конфигурации системного источника данных был выбран режим авторизации SQL Server'а, то вам необходимо указать имя пользователя SQL в параметре *Login name* и его пароль в параметре *Password*. Если был выбран режим авторизации Windows, то вы должны оставить оба эти параметра пустыми.

Чтобы обновить список *Data Source Name*, нажмите на кнопку *Refresh*.

Когда все параметры соединения с SQL Server'ом заданы, вы можете протестировать само соединение. Нажмите кнопку *Test Connection*, чтобы проверить настройки соединения.



Имейте в виду, что данная функция проверяет только само соединение с SQL Server'ом. Если существуют какие-либо проблемы с базой данных или с доступом к базе данных, вы не увидите никаких ошибок в диалоге *Test Connection*.

Если какие-либо параметры соединения были указаны неправильно, то вы можете увидеть одну из этих ошибок:

- *SQL Server does not exist or access denied* – вы указали неправильное имя SQL Server'а в параметре *SQL Server name*, либо удаленный компьютер на котором работает SQL Server недоступен. Возможно, вы указали имя компьютера, но не указали имя экземпляра SQL Server'а через обратный слеш.

- *Login failed for user 'COMPUTER_NAME$'* – вы выбрали режим авторизации Windows, но учетная запись, под которой работает служба DeviceLock Enterprise Server'а не может получить доступ к SQL Server'у. Это может происходить, когда служба работает под учетной записью *СИСТЕМА*, либо под учетной записью пользователя, который не имеет привилегий администратора на компьютере с SQL Server'ом.

- *Login failed for user 'user_name'* – вы выбрали режим авторизации SQL Server'а и указали либо неверное имя пользователя SQL, либо неверный пароль для него. Имейте в виду, что пользователи SQL это не то же самое, что пользователи Windows. Вы не можете использовать учетную запись пользователя Windows в параметре *Login name*. Пользователи SQL существуют только для SQL Server'а и для управления ими необходимо использовать средства администрирования SQL Server'а (такие как Microsoft SQL Server Management Studio).

- *Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection* – вы выбрали режим авторизации SQL Server'а, но SQL Server не поддерживает данный режим. Необходимо либо использовать режим авторизации Windows, либо настроить SQL Server для работы в смешанном режиме авторизации.

- *Login failed for user ''. The user is not associated with a trusted SQL Server connection* – источник данных, указанный в параметре *Data Source Name* был настроен для работы в режиме авторизации SQL Server'а, но параметр *Login name* пуст.

- *Data source name not found and no default driver specified* – указан неверный (например, пустая строка) источник данных в параметре *Data Source Name*.

4.3. Store shadow files in SQL Server

Есть два режима хранения данных теневого копирования: данные хранятся в SQL Server'е или данные хранятся в виде файлов на диске.

Чтобы хранить все данные в SQL Server'е, установите флаг *Store shadow files in SQL Server*.

Если вы выбрали режим хранения всех данных в SQL Server'е, мы рекомендуем вам значительно увеличить максимальный размер файла с журналом транзакций для базы данных, указанной в параметре *Database name*. В противном случае, SQL Server может некорректно обрабатывать большие объемы данных (сотни мегабайт и больше) в одной транзакции. Также рекомендуется увеличить размер оперативной памяти доступной для SQL Server'а и включить режим PAE (Physical Address Extension).

Дополнительную информацию о том, как настроить SQL Server для хранения больших объемов данных, можно прочитать в статье, расположенной на сайте Microsoft:
http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/rdbmspft.mspx.

Чтобы хранить данные в виде файлов на диске, снимите флаг *Store shadow files in SQL Server*. В этом режиме в базе данных SQL Server'а хранятся только указатели на файлы и некоторая другая дополнительная информация небольшого объема.

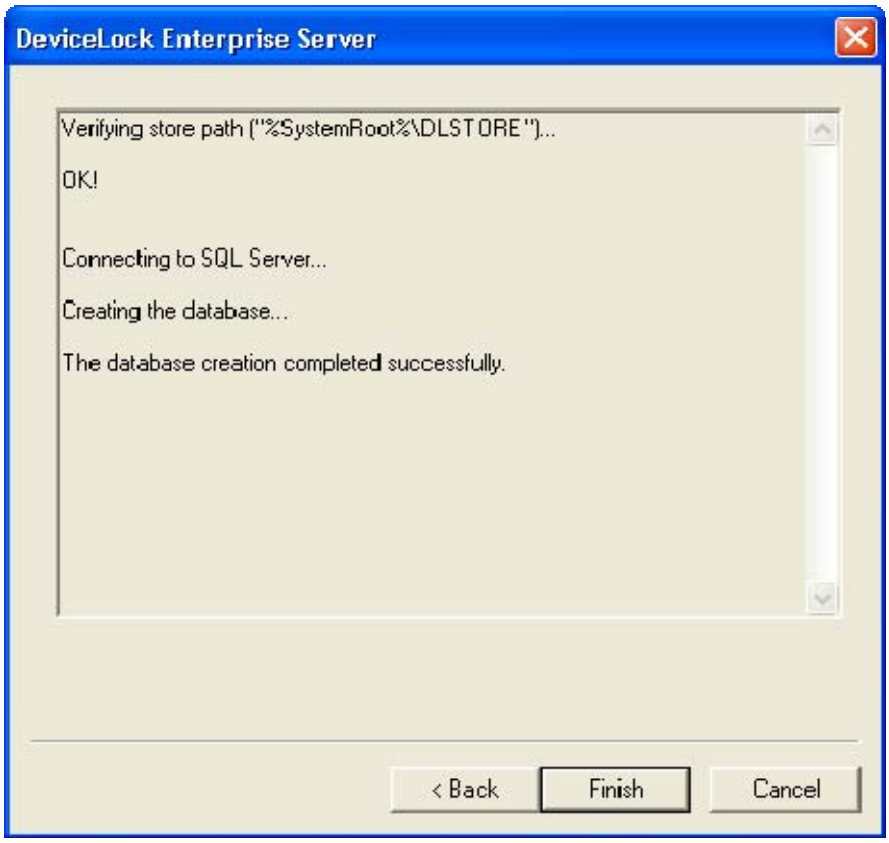
Когда данные хранятся на диске в виде файлов, сами файлы при этом находятся в директории, указанной в параметре *Store path*. Чтобы выбрать другую папку, используйте кнопку *Browse*.

Вы также можете указать сетевой путь к общему ресурсу (например, *\\server\dlstore*), который будет использоваться в качестве хранилища файлов с данными.

Убедитесь, что учетная запись, под которой запущена служба DeviceLock Enterprise Server'а, имеет полный доступ к этому сетевому ресурсу.

ПРИМЕЧАНИЕ: Мы рекомендуем хранить данные на диске в виде файлов.

Нажмите на кнопку *Next*, чтобы применить настройки и перейти к последней странице.



Вам придется подождать какое-то время, пока создается база данных, указанная в параметре *Database name*. Если база данных уже существует и у нее правильный формат (она была создана DeviceLock Enterprise Server'ом), то DeviceLock Enterprise Server будет использовать эту существующую базу данных.

Если какие-либо параметры на предыдущей странице мастера настроек были указаны неправильно, то вы можете увидеть одну из этих ошибок:

- *[2] The system cannot find the file specified* – вы указали DeviceLock Enterprise Server'у хранить данные на диске, но путь, заданный в параметре *Store path,* неверен. Если вы указали общий сетевой ресурс, то возможно, что этот ресурс недоступен.

- *Failed to verify store path. [5] Access is denied* – путь, указанный в параметре *Store path* верен, но учетная запись пользователя, под которой работает служба DeviceLock Enterprise Server'а, не имеет полного доступа к файлам и директориям по этому пути.

- *CREATE DATABASE permission denied in database 'name'* – пользователь, который используется для подключения к SQL Server'у не имеет достаточно привилегий, чтобы создать базу данных. Пользователь должен иметь как минимум серверную роль *dbcreator* (см. *Server Roles* в *Login Properties* у Microsoft SQL Server Management Studio).

- *The server principal "user_name" is not able to access the database "name" under the current security context* – пользователь, который используется для подключения к SQL Server'у, не имеет доступа к существующей базе данных. Пользователь должен быть привязан к этой базе данных (см. *User Mapping* в *Login Properties* у Microsoft SQL Server Management Studio).

- *SELECT permission denied on object 'name', database 'name', schema 'name'* – пользователь, который используется для подключения к SQL Server'у, не имеет доступа на чтение/запись к существующей базе данных. Пользователь должен иметь как минимум роли базы данных *db_datareader* и *db_datawriter* (см. *User Mapping* в *Login Properties* у Microsoft SQL Server Management Studio).

- *Invalid object name 'name'* – база данных, указанная в параметре *Database name* уже существует, но имеет неверный формат. Это случается, когда вы пытаетесь использовать базу данных, которая не была создана DeviceLock Enterprise Server'ом или была повреждена.

- *DeviceLock Database has an unsupported format* – база данных, указанная в параметре *Database name,* уже существует, но имеет устаревший формат и не может быть обновлена до новой версии. Вы должны использовать другую базу данных или создать новую.

- *DeviceLock Database has a format that is not supported by the current server version* – база данных, указанная в параметре *Database name,* уже существует, но была создана более новой версией DeviceLock Enterprise Server'а. Вы должны использовать новую версию DeviceLock Enterprise Server'а или использовать другую базу данных (например, создать новую).

Кроме того, здесь могут отображаться и некоторые ошибки соединения, описанные выше.

Используйте кнопку *Back*, чтобы вернуться на предыдущую страницу и внести необходимые изменения в настройки.

Если никаких ошибок не возникло, нажмите на кнопку *Finish*, чтобы закрыть мастер настроек и продолжить процесс установки.

В конце установки программа предложит вам открыть сайт DeviceLock.

Снимите галочку с *DeviceLock Home Page*, если вы не хотите открывать сайт DeviceLock в данный момент. Нажмите кнопку *Close,* чтобы завершить процесс установки.

3. DeviceLock Certificate

3.1 Общая информация

Сертификат состоит из двух ключей (ключевой пары): *секретного* и *открытого*:

- *Секретный* ключ должен храниться на компьютере администратора, и только администратор должен иметь доступ к нему. *Секретный* ключ также может быть установлен на DeviceLock Enterprise Server'е. ***ПРИМЕЧАНИЕ: Убедитесь, что обычные пользователи не могут получить доступ к секретному ключу.***

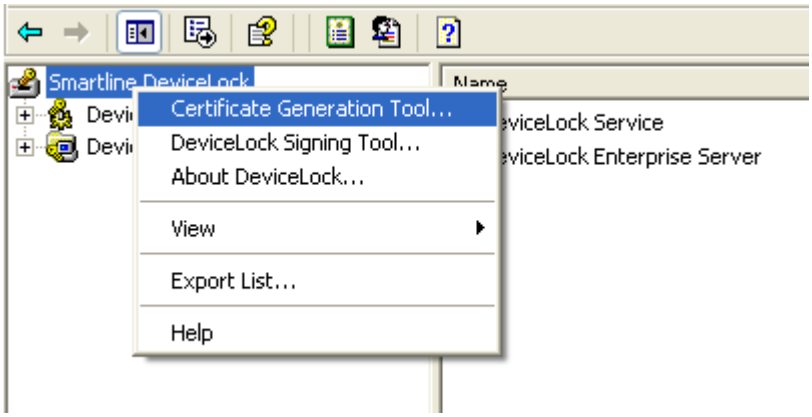
- *Открытый* ключ устанавливается на компьютеры, где работают DeviceLock Service'ы. Если о*ткрытый* ключ не установлен на компьютере пользователя, то невозможно использовать функцию временного белого списка и авторизацию по сертификату для DeviceLock Enterprise Server'а.

3.2 Создание сертификата

Прежде всего надо создать сертификат, используя специальную программу Certificate Generation Tool, устанавливаемую вместе с консолями управления DeviceLock.

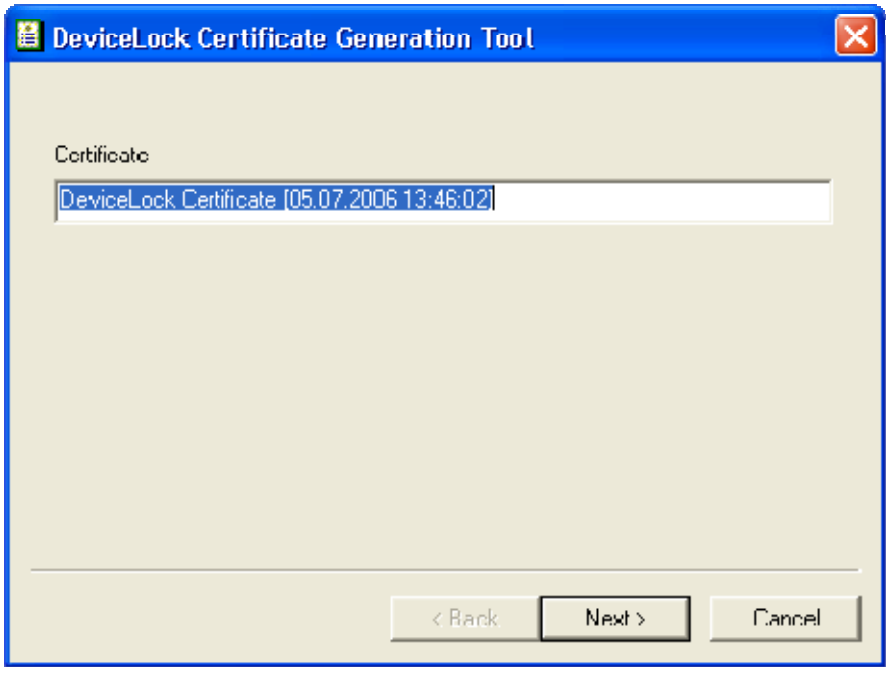
Мы рекомендуем создать только один сертификат и установить его *открытый* ключ на все пользовательские компьютеры. Генерация и установка нового сертификата необходима только в случае компрометации *секретного* ключа или его утере.

Чтобы запустить программу Certificate Generation Tool, выберите *Certificate Generation Tool* из меню *File* в DeviceLock Enterprise Manager. Чтобы запустить Certificate Generation Tool из DeviceLock Management Console (оснастка для MMC) и DeviceLock Group Policy Manager, используйте контекстное меню, доступное по нажатию правой кнопки мыши.



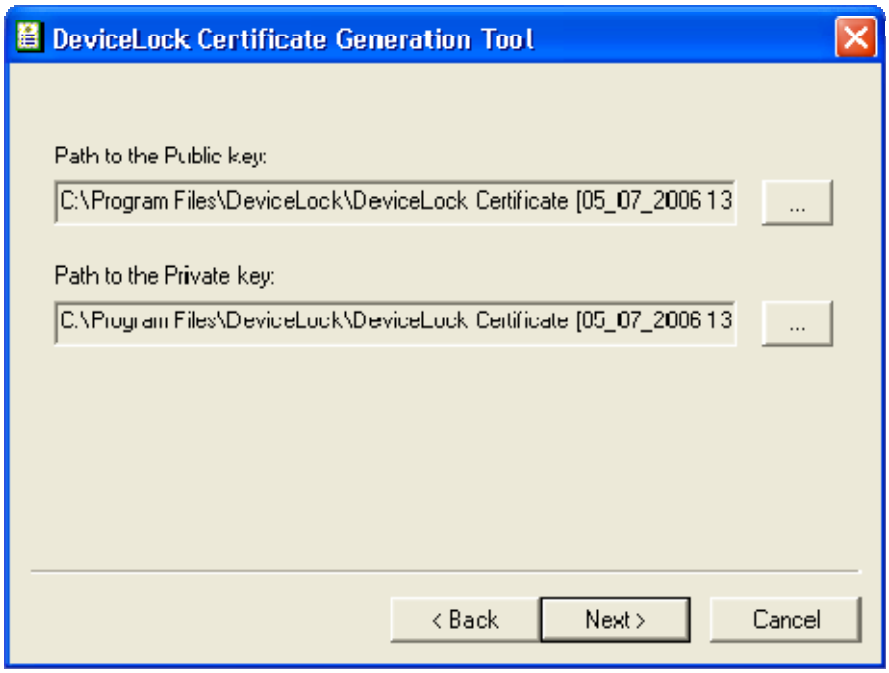
Необходимо выполнить всего два простых шага для создания ключевой пары:

1. Задайте имя сертификата.



Программа Certificate Generation Tool автоматически создает имя, основанное на текущей дате и времени, но вы можете ввести любое иное имя.

2. Задайте путь и имена файлов для *секретного* и *открытого* ключей.



Как только сертификат будет создан, вы можете приступить к установке *открытого* ключа на пользовательские компьютеры.

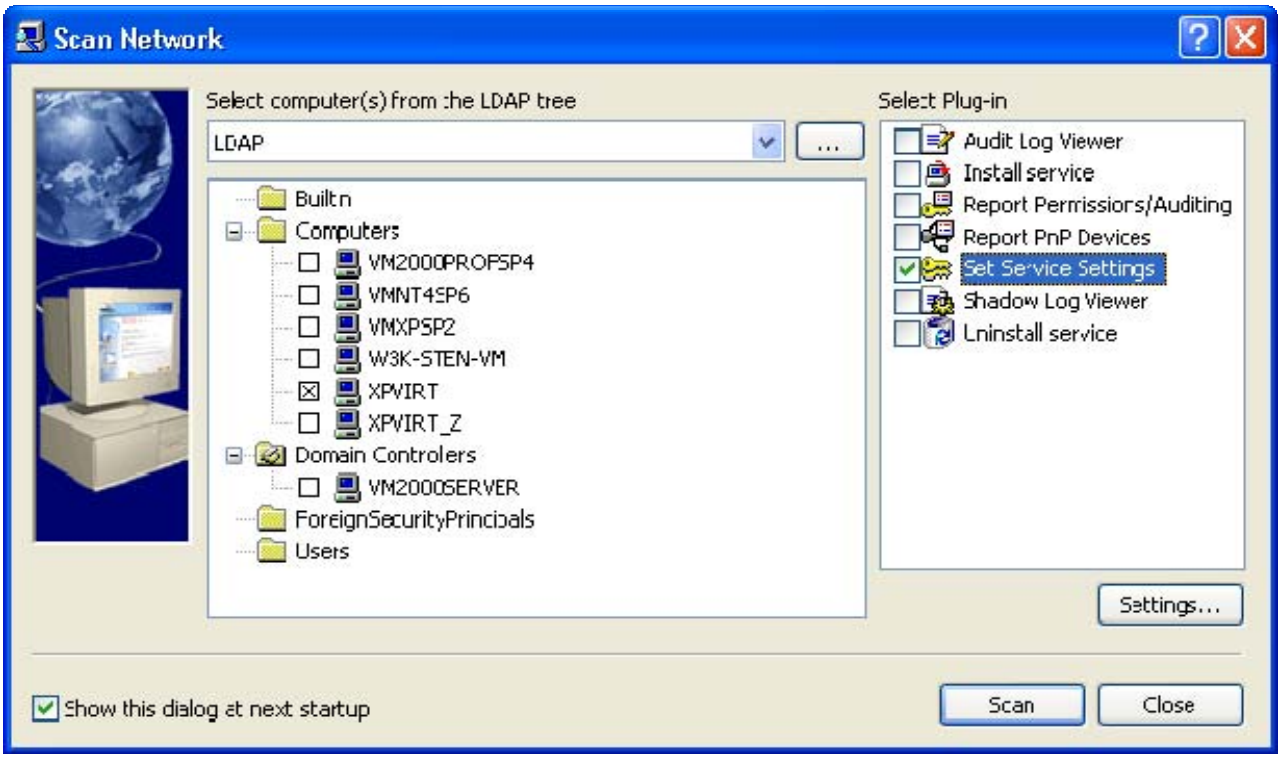
ПРИМЕЧАНИЕ: Вновь созданный сертификат не устанавливается автоматически на компьютеры с помощью программы Certificate Generation Tool. Вы должны установить его вручную из консоли управления DeviceLock.

3.3 Установка и удаление сертификата

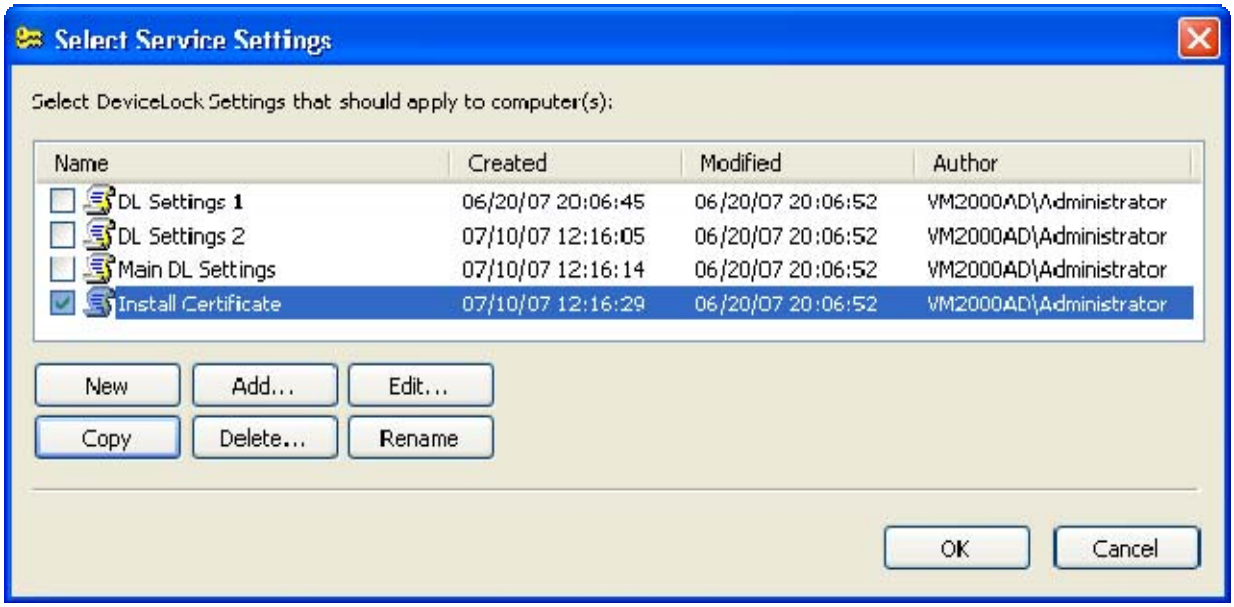
Чтобы установить или удалить *открытый* ключ с пользовательских компьютеров, вы можете использовать любую консоль управления DeviceLock:

a. DeviceLock Enterprise Manager

В диалоге *Scan Network* выберите компьютеры для установки или удаления *открытого* ключа, затем выберите модуль *Set Service Settings*.



Нажмите на кнопку *Settings*, чтобы открыть диалог с настройками.

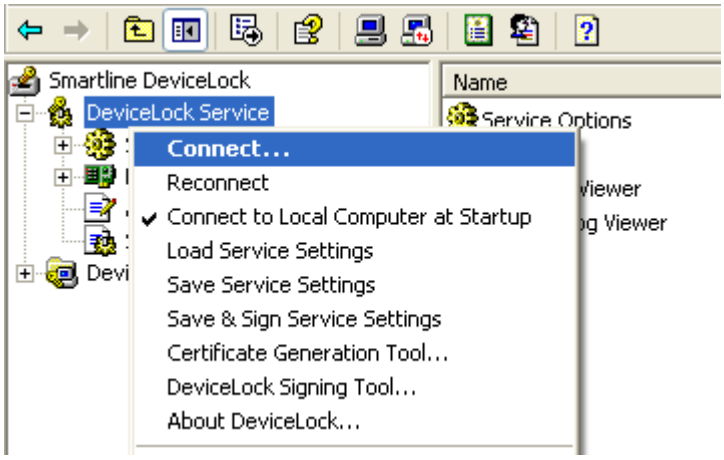


Чтобы задать политику, в которой будет устанавливаться или удаляться сертификат, создайте новый XML-файл или используйте один из существующих. Выделите файл в списке и затем нажмите на кнопку *Edit* для редактирования политики, как это описано ниже. Когда вы закончите редактирование политики, отметьте файл в списке путем установки флага рядом с его именем.

Нажмите *OK*, чтобы закрыть диалог с настройками и затем нажмите кнопку *Scan* на диалоге *Scan Network*, чтобы начать процесс установки или удаления ключа.

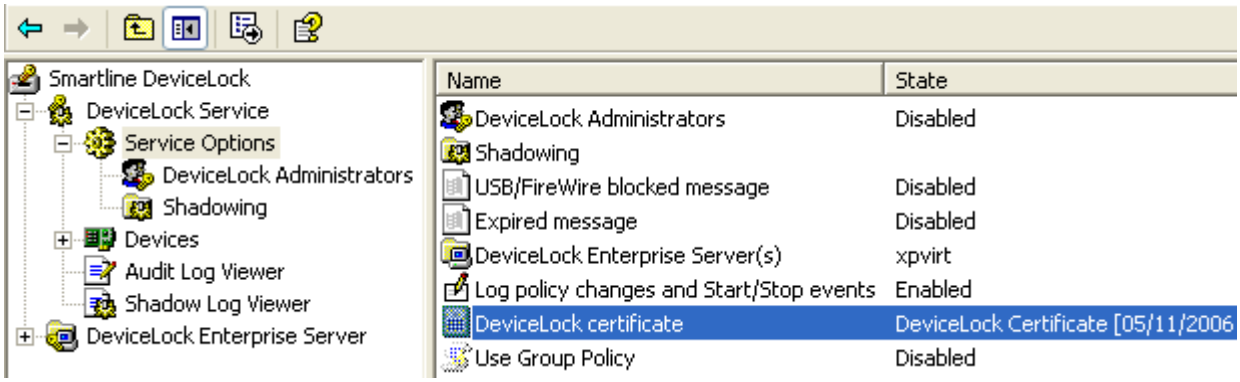
б. DeviceLock Management Console, DeviceLock Group Policy Manager и DeviceLock Service Settings Editor

Если вы используете DeviceLock Management Console (оснастка для MMC), сначала вам надо подключиться к компьютеру с запущенным DeviceLock Service. Используйте контекстное меню, доступное по нажатию правой кнопки мыши.

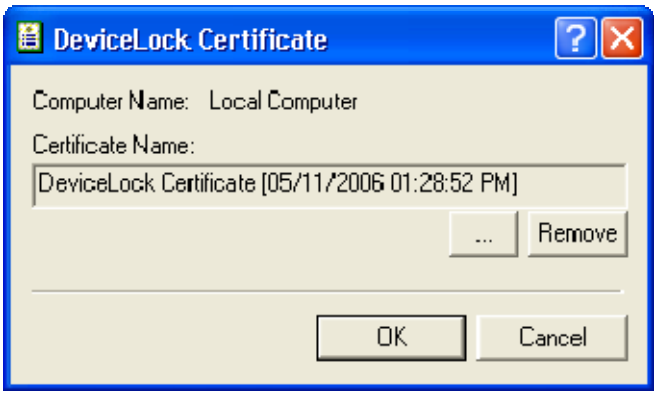


Когда используется DeviceLock Group Policy Manager, то вам не требуется подключаться к клиентским компьютерам, т.к. эта консоль работает с объектом групповой политики, а не с отдельным компьютером. Вам также не требуется подключаться к клиентским компьютерам, когда с помощью DeviceLock Service Settings Editor'а редактируется политика во внешнем XML-файле.

Выберите раздел *Service Options* из дерева консоли.



Два раза кликните мышкой на параметре *DeviceLock certificate*, чтобы открыть диалог с настройками.



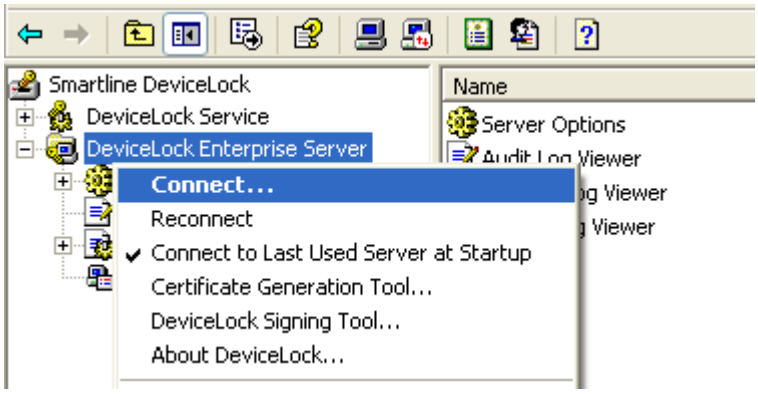
Укажите путь к файлу с *открытым* ключом в параметре *Certificate Name*, если вы хотите установить сертификат. Вы можете использовать кнопку **...**, чтобы открыть диалог выбора файлов.

Для удаления *открытого* ключа, используйте кнопку *Remove*.

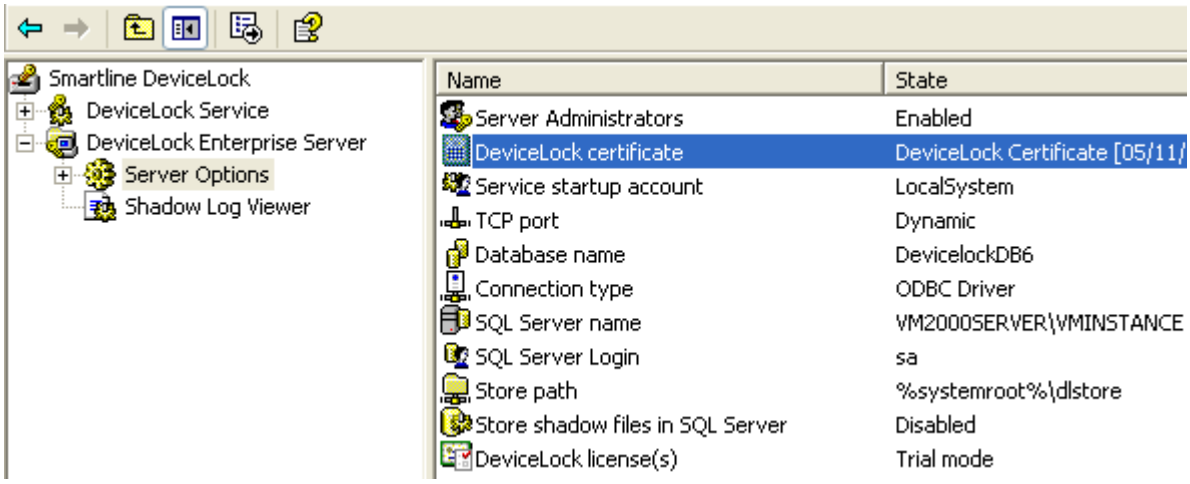
Нажмите *OK*, чтобы закрыть диалог и применить настройки.

Чтобы установить или удалить *секретный* ключ с DeviceLock Enterprise Server'а, вы должны использовать DeviceLock Management Console (оснастка для MMC).

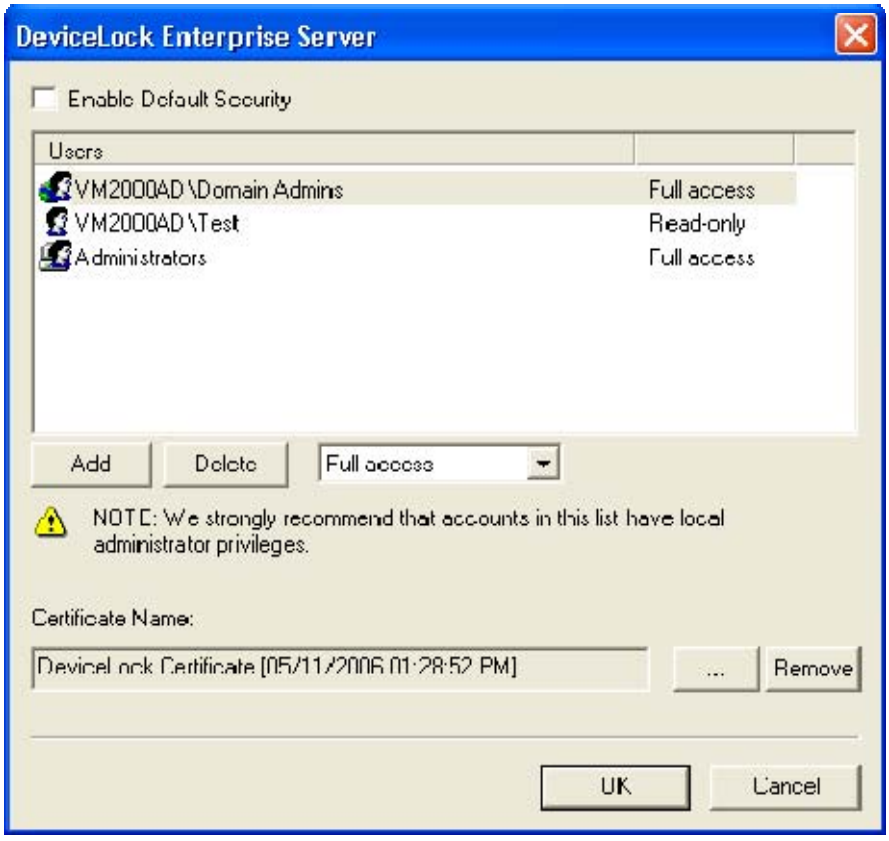
Сначала вам надо подключиться к компьютеру с запущенным DeviceLock Enterprise Server'ом. Используйте контекстное меню, доступное по нажатию правой кнопки мыши.



Выберите раздел *Server Options* из дерева консоли.



Два раза кликните мышкой на параметре *DeviceLock certificate*, чтобы открыть диалог с настройками.



Укажите путь к файлу с *секретным* ключом в параметре *Certificate Name*, если вы хотите установить сертификат. Вы можете использовать кнопку **...**, чтобы открыть диалог выбора файлов. Для удаления *секретного* ключа используйте кнопку *Remove*.

Нажмите *OK*, чтобы закрыть диалог и применить настройки.

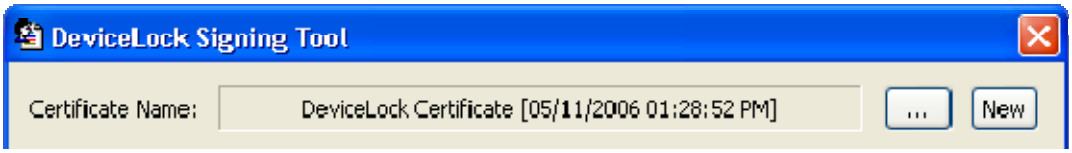
Чтобы получить дополнительную информацию относительно процесса установки *секретного* ключа, обратитесь к разделу **Установка DeviceLock Enterprise Server** данного руководства.

4. DeviceLock Signing Tool

4.1 Общая информация

DeviceLock Signing Tool - это инструмент, с помощью которого вы можете предоставлять пользователям временный доступ к запрошенным устройствам и подписывать XML-файлы с настройками DeviceLock Service'a, созданные при помощи DeviceLock Management Console или DeviceLock Group Policy Manager'a.

Чтобы запустить DeviceLock Signing Tool, выберите *DeviceLock Signing Tool* из меню *File* в DeviceLock Enterprise Manager или из контекстного меню в DeviceLock Management Console (оснастка для MMC) или DeviceLock Service Settings Editor'a.



Прежде всего вы должны загрузить необходимый сертификат (*секретный* ключ).

DeviceLock Signing Tool должен использовать *секретный* ключ, который принадлежит тому же сертификату, что и *открытый* ключ, установленный на пользовательском компьютере.

По умолчанию, DeviceLock Signing Tool автоматически загружает последний использованный сертификат. Вы можете загрузить другой сертификат, нажав на кнопку **...** и выбрав файл с *секретным* ключом.

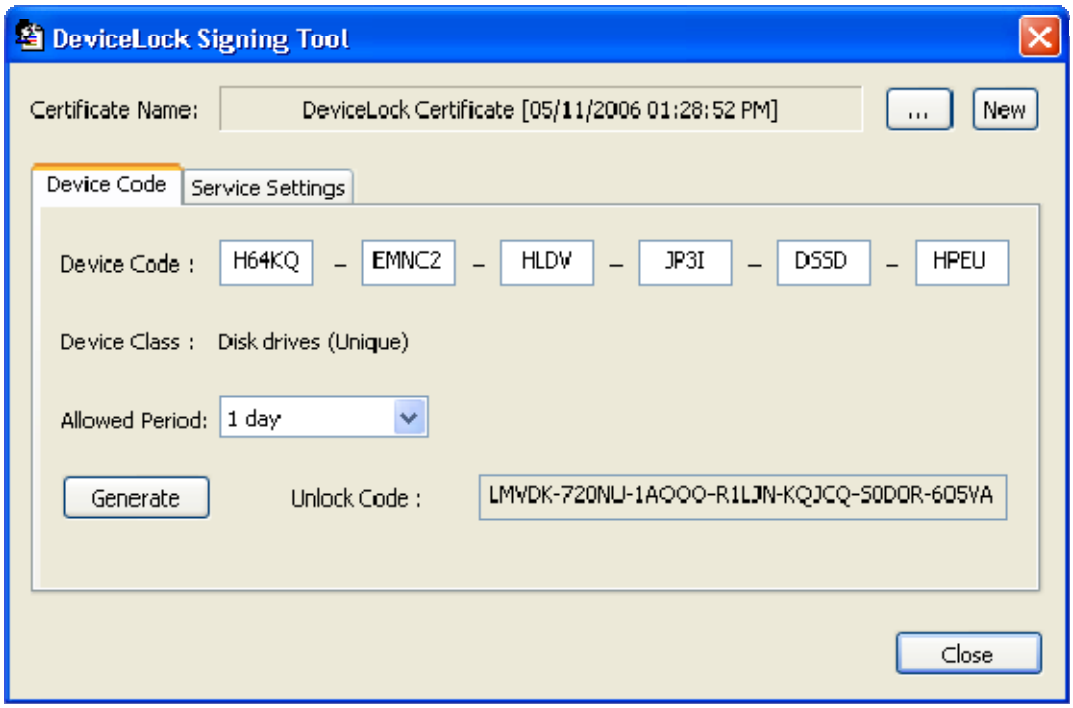
Для создания нового сертификата вы можете запустить программу Certificate Generation Tool непосредственно из DeviceLock Signing Tool. Чтобы это сделать, нажмите на кнопку *New*. Однако имейте в виду, что если вы создаете новый сертификат и предполагаете использовать его новый *секретный* ключ в DeviceLock Signing Tool, вы должны также установить соответствующий ему *открытый* ключ на пользовательских компьютерах.

Затем вы должны решить, какое действие вам необходимо выполнить: создать **Разблокирующий Код** или подписать XML-файл, содержащий настройки DeviceLock Service'a.

4.2 Device Code

Чтобы предоставить пользователю временный доступ к запрошенному устройству, вы должны создать **Разблокирующий Код** в ответ на присланный вам **Код Устройства**.

За более подробной информацией относительно **Кода Устройства** обратитесь, пожалуйста, к разделу **Временный белый список** данного руководства.



Создание **Разблокирующего Кода** осуществляется в четыре простых шага:

1. Загрузите необходимый сертификат (*см. выше*).

2. Введите **Код Устройства**, который пользователь прислал вам.

   Как только будет введен корректный **Код Устройства**, вы сможете увидеть в поле *Device Class* класс устройства, к которому пользователь хочет получить доступ. Информация о классе устройства поможет вам проконтролировать, какой тип устройства пользователь намерен использовать. Если, к примеру, пользователь сообщает администратору, что он намерен использовать USB-сканер, а на самом деле пытается получить доступ к флеш-диску, администратор сможет увидеть это несоответствие.

   Рядом с классом устройства также есть параметр (в круглых скобках), указывающий, может ли запрашиваемое устройство быть авторизовано как уникальное устройство с серийным номером либо оно может быть авторизовано лишь как модель. Если вы авторизуете устройство как модель, то пользователь получит доступ ко всем устройствам этой модели. Для более подробной информации обратитесь, пожалуйста, к разделу **USB Devices White List** данного руководства.

3. Выберите период, в течение которого запрашиваемое устройство будет доступно пользователю. В поле *Allowed Period* вы можете выбрать один из нескольких предопределенных периодов: 5, 15, 30, 60 минут, 5 часов, 1 или два дня, 1 или 2 недели, 1 месяц, пока устройство не будет отключено или пока текущий пользователь не завершит свою сессию (не выйдет из системы).

   Когда вы выбираете фиксированное время (например, 10 минут), пользователь получает право доступа к устройству только на этот период. Как только разрешенное время истечет, доступ к устройству снова будет запрещен. При этом не имеет значения, что пользователь делает с этим устройством – даже

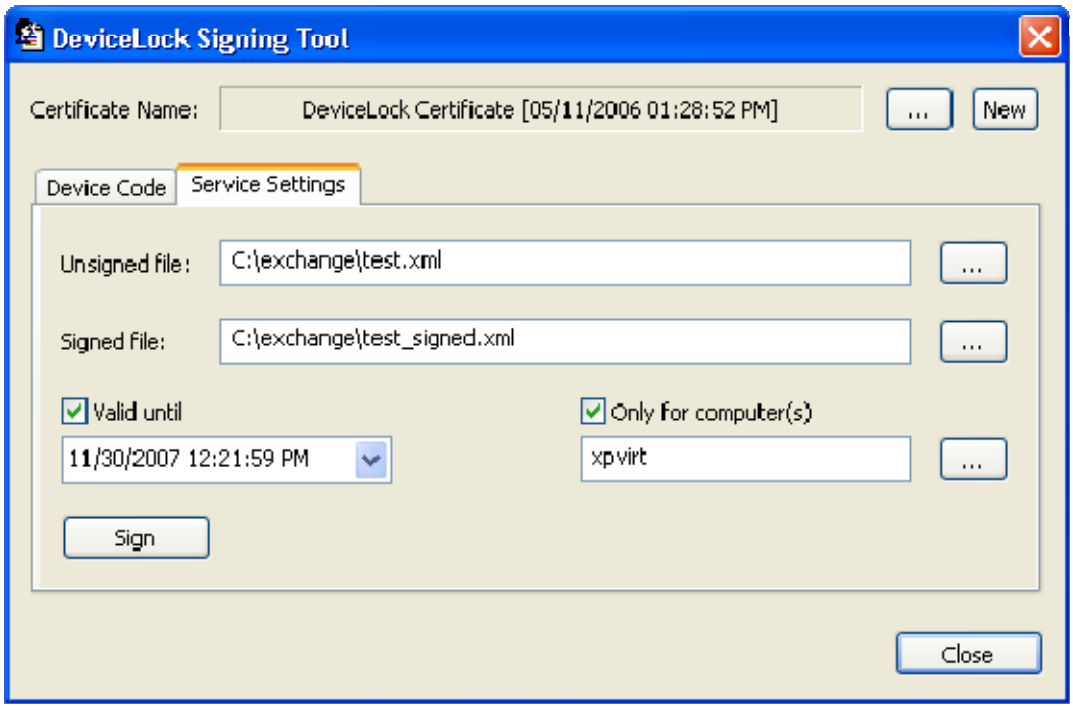
если он все еще копирует файлы на USB-диск или печатает документ на USB-принтере, все операции будут прерваны.

Для того чтобы разрешить пользователю использовать устройство без ограничения времени, выберите опцию *until unplug* в *Allowed Period*. Пользователь получит доступ к устройству до тех пор, пока оно будет подключено к порту. Как только пользователь отключит это устройство, доступ к нему снова будет запрещен.

4. Нажмите на кнопку *Generate* для создания **Разблокирующего Кода**. Передайте этот код пользователю по телефону или любым другим способом. Процесс формирования **Разблокирующего Кода** – это ресурсоемкая операция. Время создания кода зависит от мощности процессора, установленного на вашем компьютере и может составить несколько секунд.

4.3 Service Settings

Для предотвращения неавторизованных изменений вы можете подписать XML-файл, содержащий настройки DeviceLock Service'а при помощи цифровой подписи. Позже этот файл может быть послан пользователям, чьи компьютеры не подключены к сети и находятся вне досягаемости консолей управления.



Подписывание XML-файла осуществляется в шесть простых шагов:

1. Загрузите необходимый сертификат (*см. выше*).

2. Загрузите файл с настройками, который вы хотите подписать.

   Полный путь к файлу должен быть введен в поле *Unsigned file*. Вы можете использовать кнопку **...**, чтобы открыть диалог выбора файлов.

XML-файл с настройками DeviceLock Service'а может быть создан при помощи *Save Service Settings* из контекстного меню DeviceLock Management Console, DeviceLock Group Policy Manager'а или DeviceLock Service Settings Editor'а.

3. В поле *Signed file* укажите путь к результирующему файлу с подписью. Вы можете использовать кнопку **…**, чтобы выбрать директорию, где этот файл будет создан.

4. Решите, должен ли результирующий файл содержать информацию о сроке годности.

   Если вы хотите позволить пользователям импортировать настройки из этого файла без каких-либо ограничений по времени, снимите флаг *Valid until*.

   Если вы установите флаг *Valid until* и зададите дату/время, то информация о сроке годности файла будет записана в результирующий файл и пользователи смогут импортировать настройки из этого файла только до указанной даты/времени.

   Имейте в виду, что данный флаг имеет силу только когда пользователи импортируют настройки DeviceLock Service'а через приложение *DeviceLock* из панели управления Windows. Когда XML-файл с настройками загружается при помощи *Load Service Settings* из контекстного меню DeviceLock Management Console или DeviceLock Group Policy Manager'а, информация о сроке годности файла игнорируется.

5. Решите, должен ли результирующий файл быть привязан к определенному компьютеру, или он может использоваться на любом компьютере.

   Если вы хотите позволить пользователям импортировать настройки из этого файла на любых компьютерах, снимите флаг *Only for computer(s)*.

   Если вы установите флаг *Only for computer(s)* и зададите имя компьютера, то пользователи смогут импортировать настройки из этого файла только на этом компьютере. Используя точку с запятой (;) в качестве разделителя, вы можете указать несколько имен компьютеров, что позволит пользователям использовать результирующий файл на любом из этих компьютеров.

   ПРИМЕЧАНИЕ: Вы не можете использовать IP-адрес компьютера в этом параметре. Вы должны указывать именно имя компьютера, в точности как оно отображается в программе System из панели управления Windows.

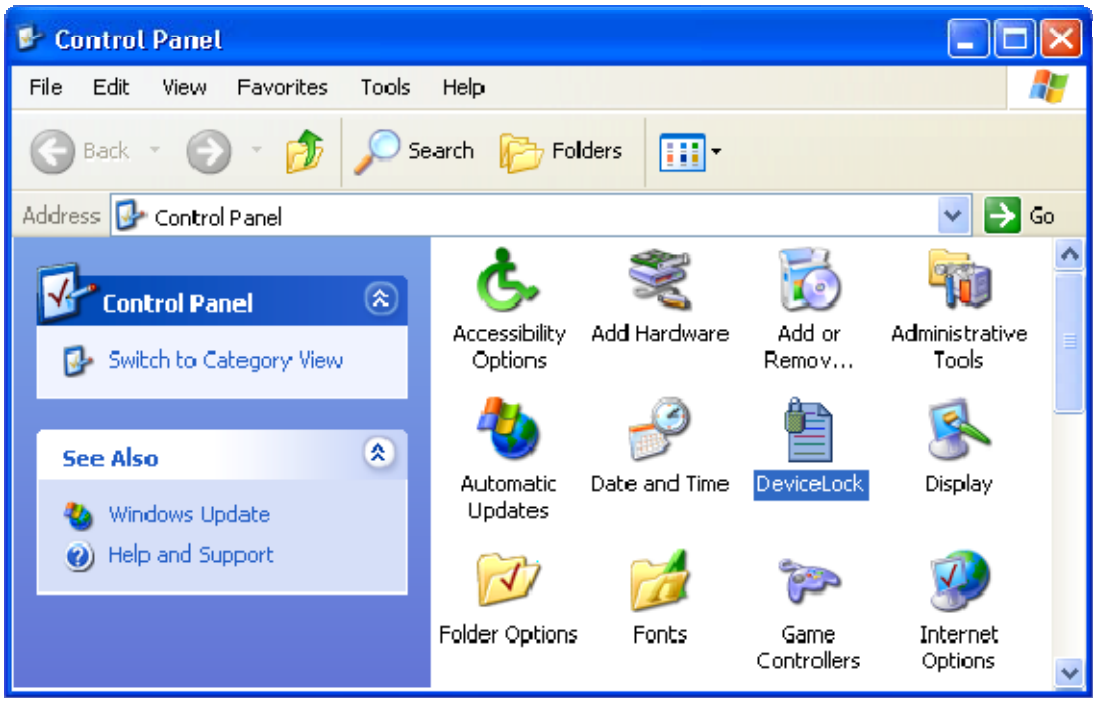
   Вы можете загрузить заранее подготовленный список компьютеров из внешнего текстового файла. Чтобы открыть внешний файл, нажмите на кнопку **…**. Текстовый файл должен содержать имена компьютеров, каждое из которых должно быть записано на отдельной строке.

   Имейте в виду, что данный флаг имеет силу только когда пользователи импортируют настройки DeviceLock Service'а через приложение *DeviceLock* из панели управления Windows. Когда XML-файл с настройками загружается при помощи *Load Service Settings* из контекстного меню DeviceLock Management

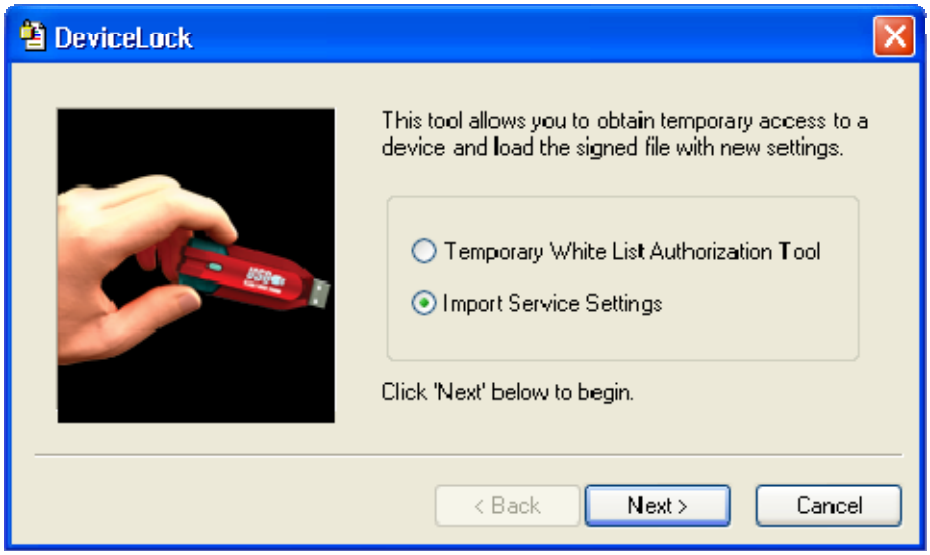
Console или DeviceLock Group Policy Manager'а, информация о привязке к компьютеру игнорируется.

Нажмите на кнопку *Sign* для создания подписанного файла с настройками DeviceLock Service'а. Передайте этот файл пользователю любым удобным способом. Процесс создания цифровой подписи – это ресурсоемкая операция. Время создания подписи зависит от мощности процессора, установленного на вашем компьютере и может составить несколько секунд.

Когда пользователю потребуется загрузить настройки DeviceLock Service'а из этого подписанного XML-файла, он должен запустить приложение *DeviceLock* из панели управления Windows и выбрать опцию *Import Service Settings*.

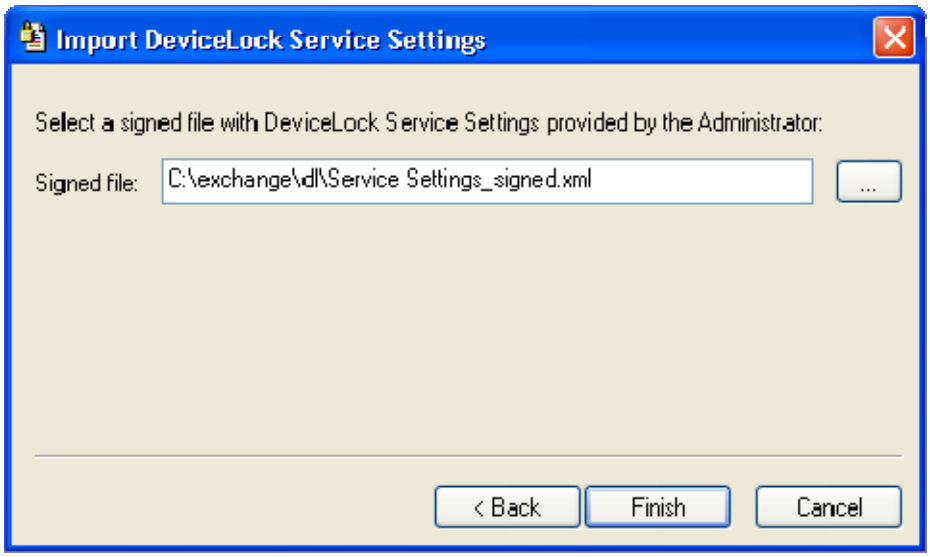


ПРИМЕЧАНИЕ: В Windows XP и более поздних версиях ОС пользователь должен переключить отображение панели управления в стандартный режим для получения доступа ко всем возможным приложениям.



Импорт настроек из подписанного файла выполняется в два простых шага:

1. Полный путь к подписанному файлу должен быть введен в поле *Signed file*. Вы можете использовать кнопку **…**, чтобы открыть диалог выбора файлов.



2. Нажмите на кнопку *Finish*. Если цифровая подпись файла верна, то новые настройки будут немедленно загружены в DeviceLock Service.

Пользователь может также загрузить настройки DeviceLock Service'а из подписанного XML-файла используя командную строку:

DLTempAccess.cpl -s <путь к подписанному файлу>

где *<путь к подписанному файлу>* – полный путь к подписанному XML-файлу с настройками DeviceLock Service'а. Например:

DLTempAccess.cpl -s "C:\Program Files\DeviceLock\settings_signed.dls"

Все успешные попытки загрузить настройки из файла протоколируются, если протоколирование изменений в настройках DeviceLock Service включено в Service Options.

5 DeviceLock Management Console

5.1 Общая информация

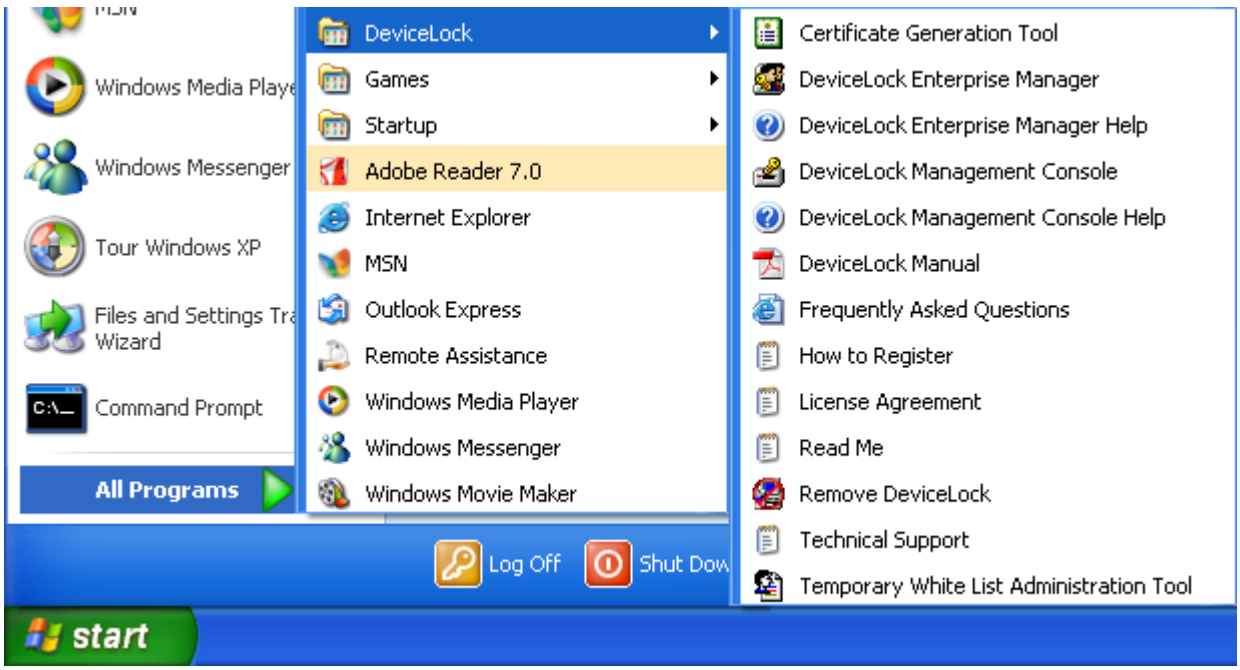
DeviceLock Management Console – это оснастка для Microsoft Management Console (MMC).

Используя DeviceLock Management Console, вы можете просматривать и изменять разрешения и правила аудита, устанавливать DeviceLock Service, а также просматривать журналы аудита и теневого копирования для отдельных компьютеров.

DeviceLock Management Console также используется для управления DeviceLock Enterprise Server'ом.

Чтобы получить информацию относительно процесса установки DeviceLock Management Console, обратитесь к разделу **Установка консолей управления** данного руководства.

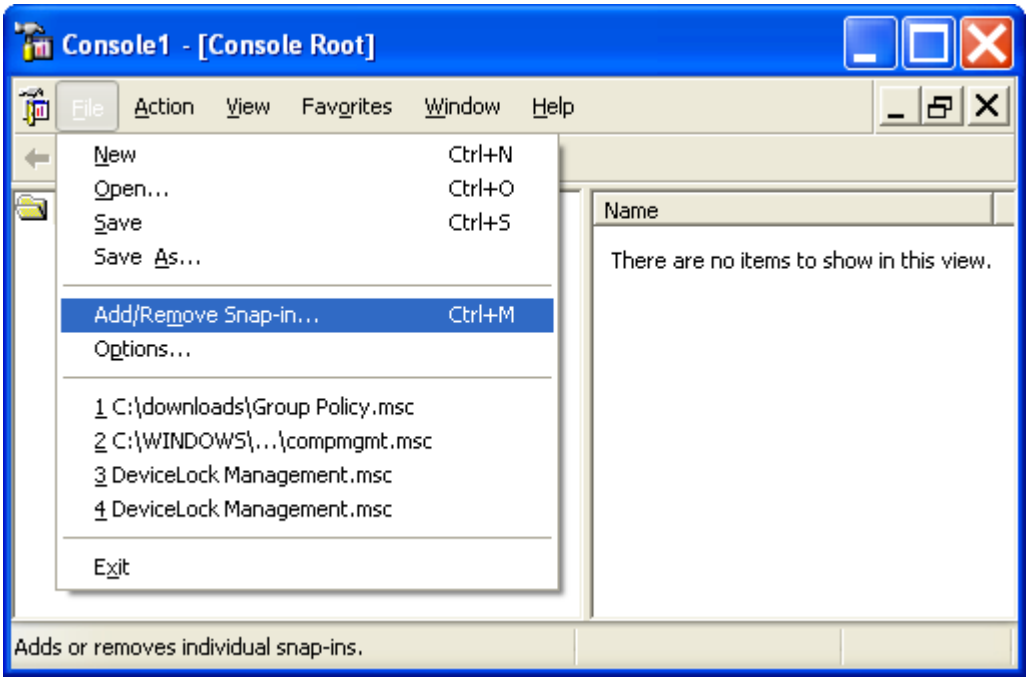
Чтобы запустить DeviceLock Management Console, выберите соответствующий ярлык из меню *Programs*, появляющегося при нажатии на кнопку *Start*.



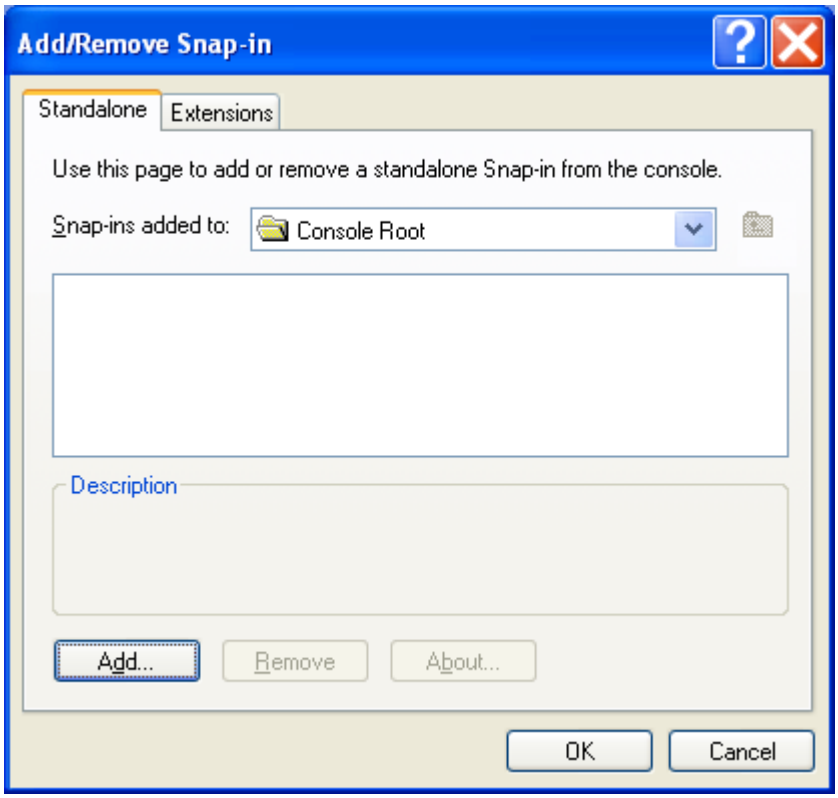
Кроме того, вы можете запустить MMC и добавить оснастку *DeviceLock Management Console* вручную:

1. Запустите *mmc* из командной строки или используйте меню *Run* для выполнения этой команды.

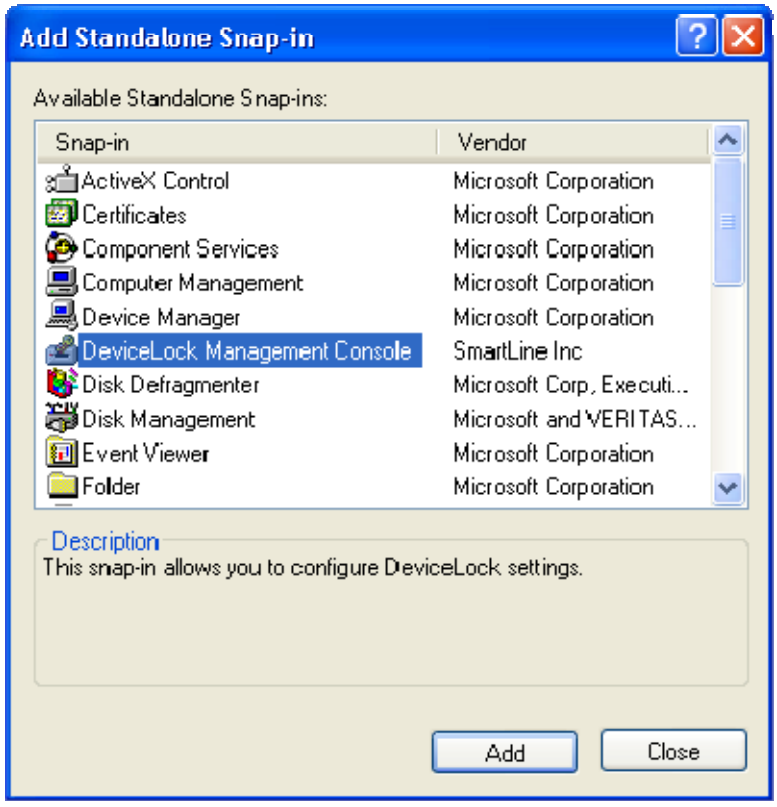
2. Откройте меню *File*, затем кликните *Add/Remove snap-in*.



3. Кликните на вкладку *Standalone*, затем нажмите *Add*.

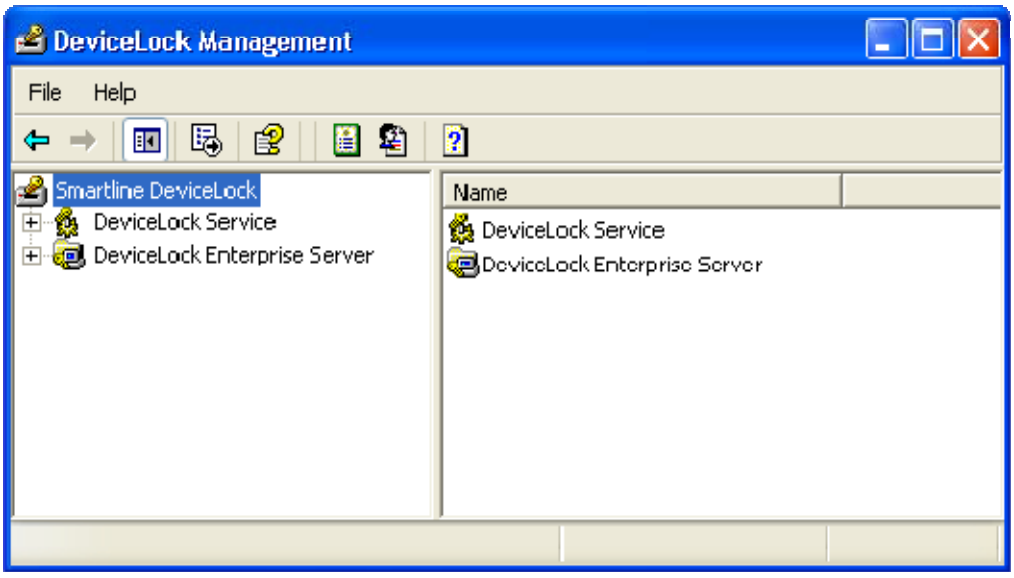


4. Выберите из списка оснастку *DeviceLock Management Console* и нажмите *Add*.



5.2 Интерфейс

DeviceLock Management Console имеет дружественный, удобный в использовании интерфейс, предоставляемый Microsoft Management Console (MMC). В любом окне программы вы можете получить помощь, нажав клавишу *F1*.



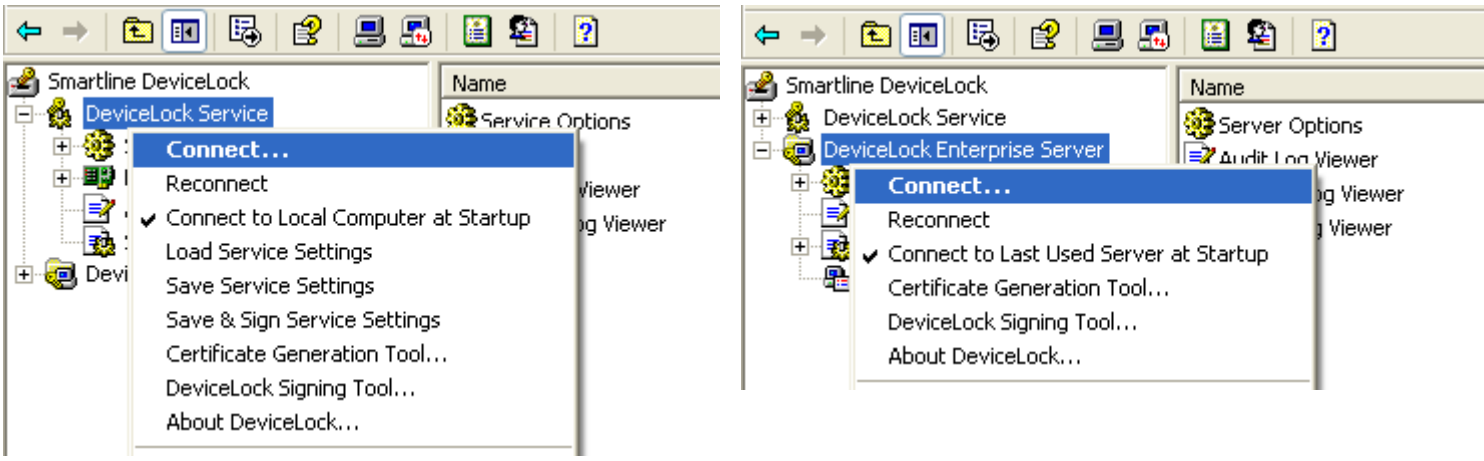
Есть два независимых раздела в DeviceLock Management Console:

3. *DeviceLock Service* – позволяет управлять DeviceLock Service'ами, работающими на локальном и удаленных компьютерах.

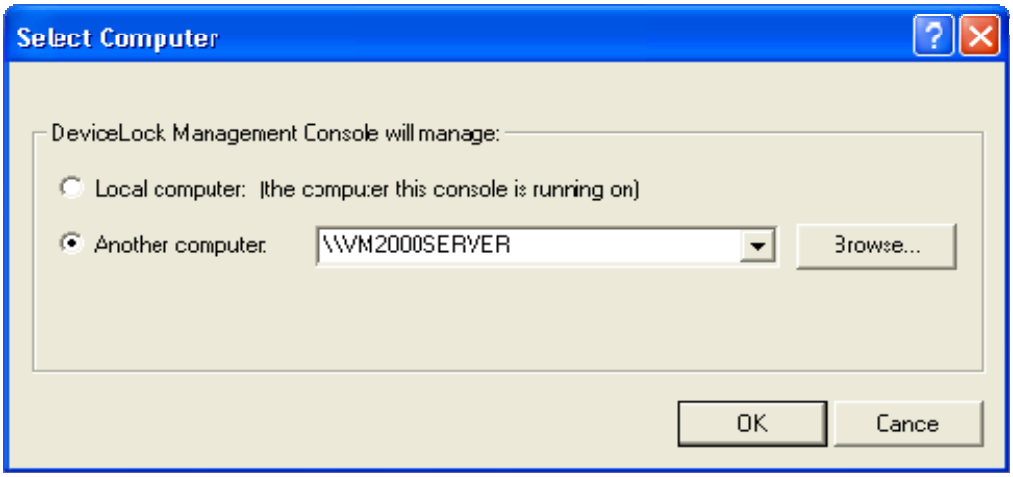
4. *DeviceLock Enterprise Server* – позволяет управлять DeviceLock Enterprise Server'ами, работающими на локальном и удаленных компьютерах.

5.3 Подключение к компьютеру

Прежде всего вам необходимо подключиться к компьютеру, где работает DeviceLock Service или DeviceLock Enterprise Server. Используйте *Connect* из контекстного меню или соответствующую кнопку на инструментальной панели.



Вы можете подключиться одновременно и к DeviceLock Service и к DeviceLock Enterprise Server'у, даже если они работают на разных компьютерах.



Укажите имя удаленного компьютера или его IP-адрес в параметре *Another computer*. Чтобы просмотреть список компьютеров в локальной сети, используйте кнопку *Browse*. Для подключения к локальному компьютеру используйте опцию *Local computer*.

Для соединения консоли управления с компьютером, на котором DeviceLock Service или DeviceLock Enterprise Server настроен на использование фиксированного TCP-порта, вы должны указать номер порта в квадратных скобках сразу после имени компьютера, например, *имя_компьютера[номер_порта]*.

Нажмите *OK*, чтобы подключиться к выбранному компьютеру.

ПРИМЕЧАНИЕ: Убедитесь в том, что удаленный компьютер, к которому вы пытаетесь подключиться, доступен с компьютера, где запущена консоль управления. Удаленный компьютер должен работать под управлением ОС, совместимой с DeviceLock (Windows NT 4.0 SP6 и новее). Сетевой протокол TCP/IP должен быть настроен и функционировать корректно. В случае если используется какой-либо файрвол (включая встроенный файрвол Windows), он также должен быть правильно настроен, т.е. разрешать соединения с DeviceLock Service и/или DeviceLock Enterprise Server'ом.

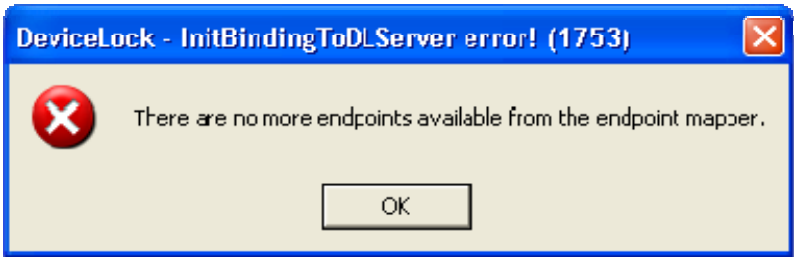
DeviceLock Service автоматически добавляет себя в список исключений встроенного файрвола Windows.

Когда вы пытаетесь подключиться к компьютеру, на котором DeviceLock Service не установлен или установлена старая его версия, консоль управления предлагает вам установить новую версию DeviceLock Service. Чтобы получить информацию относительно процесса удаленной установки в DeviceLock Management Console, обратитесь к разделу **Установка в DeviceLock Management Console** данного руководства.

При подключении к DeviceLock Service, работающему в режиме групповых политик, вы увидите предупреждающее сообщение.

Все изменения в настройках DeviceLock Service, которые вы внесете при помощи DeviceLock Management Console, будут отменены и все параметры получат свои изначальные значения (заданные в объекте групповой политики) при следующем обновлении групповой политики. За дополнительной информацией обращайтесь к разделу **Service Options** данного руководства.

При попытке подключения к компьютеру, где DeviceLock Enterprise Server не установлен или не запущен, вы получите сообщение об ошибке соединения.



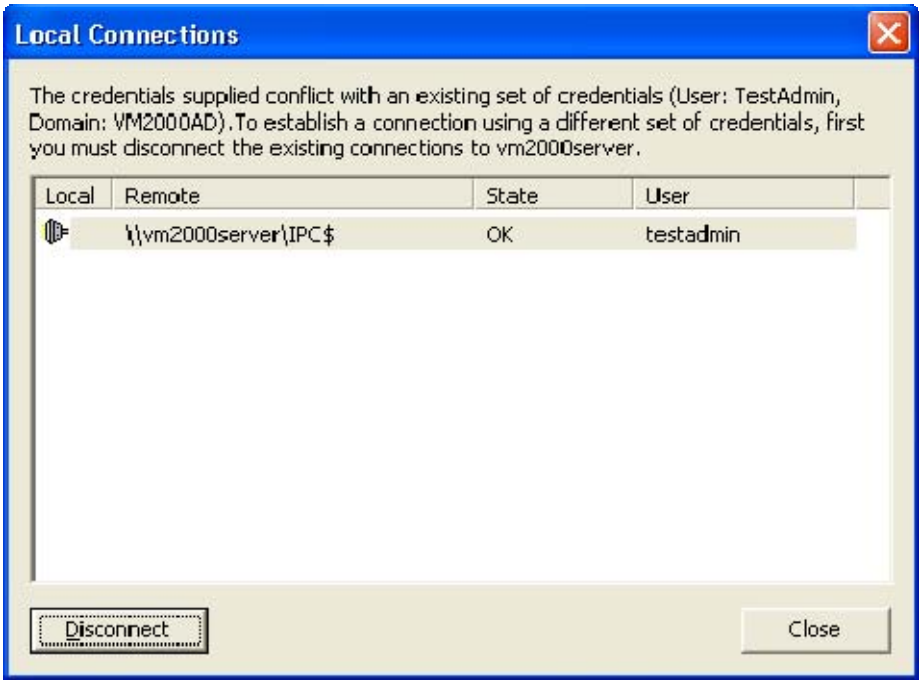
DeviceLock Enterprise Server должен быть установлен и запущен до того как консоль управления может быть подключена к нему. Дополнительную информацию относительно установки сервера вы можете найти в главе **Установка DeviceLock Enterprise Server** данного руководства.

Если у вас нет административных привилегий на выбранном компьютере, то консоль управления предложит вам подключиться к этому компьютеру, используя учетную запись другого пользователя.

В параметре *Connect As* вы должны указать учетную запись пользователя с административными привилегиями. Эта учетная запись также должна быть в списке администраторов DeviceLock, если контроль доступа по умолчанию отключен для DeviceLock Service или DeviceLock Enterprise Server'a.

При подключении к удаленному компьютеру под учетной записью другого пользователя возможен т.н. "конфликт учетных записей". Это происходит по причине того, что ваш локальный компьютер уже подключен к удаленному компьютеру под другим (текущим) пользователем – например, у вас подключен сетевой диск, открыт общий сетевой ресурс и т.п. Чтобы избежать подобного конфликта, вы должны удалить все конкурентные соединения с удаленным компьютером.

Когда DeviceLock Management Console обнаруживает "конфликт учетных записей", то на экран выводится диалог со списком всех соединений локального компьютера и вам предлагается удалить некоторые из них.



Выделите в списке все соединения с удаленным компьютером, к которому вы хотите подключиться, и нажмите на кнопку *Disconnect*.

Нажмите кнопку *Close* и попробуйте подключиться к этому компьютеру еще раз.

ПРИМЕЧАНИЕ: В некоторых случаях существующее соединение не может быть удалено, что препятствует подключению консоли управления к удаленному компьютеру под учетной записью другого пользователя. В этом случае вам нужно запустить DeviceLock Management Console либо под учетной записью пользователя с административным доступом к DeviceLock Service или DeviceLock Enterprise Server, либо под учетной записью пользователя, который вообще не имеет никаких соединений с удаленным компьютером. Вы можете воспользоваться функцией Run As (выполните RUNAS из командной строки), доступной в ОС начиная с Windows 2000, чтобы запустить DeviceLock Management Console под учетной записью другого пользователя.

5.3.1 Возможные ошибки подключения

Когда вы пытаетесь подключить консоль управления к компьютеру с DeviceLock Service или DeviceLock Enterprise Server, возможно возникновение некоторых из этих ошибок:

- *(1722) The RPC server is unavailable* – вы пытаетесь подключиться к компьютеру, который либо не существует (неправильное имя или IP-адрес), либо недоступен. Убедитесь в том, что имя компьютера введено правильно. Попробуйте выполнить комманду *ping* для этого имени или IP-адреса. Попробуйте подключиться к этому комьютеру, используя стандартные средства администрирования Windows (такие как *Computer Management*, *Services* и т.п.). Убедитесь, что компьютер работает под управлением ОС, совместимой с DeviceLock (Windows NT 4.0 SP6 и новее).

  Также возможно, что файрвол блокирует доступ к компьютеру. Вам необходимо сконфигурировать файрвол таким образом, чтобы открыть некоторые порты для DeviceLock. Вы также можете настроить DeviceLock для работы по фиксированному TCP-порту, что упростит задачу по конфигурированию файрвола. По умолчанию DeviceLock Service и DeviceLock Enterprise Server используют порты 9132 и 9133 соответственно. За дополнительной информацией обращайтесь, пожалуйста, к разделу Вопросы и Ответы на нашем сайте. Также имейте в виду, что DeviceLock Service автоматически добавляет себя в список исключений встроенного файрвола Windows.

- *(1753) There are no more endpoints available from the endpoint mapper* – вы пытаетесь подключиться к компьютеру, где DeviceLock Service или DeviceLock Enterprise Server недоступны. Прежде всего убедитесь в том, что DeviceLock Service или DeviceLock Enterprise Server установлены и запущены на этом компьютере.

  Существует вероятность того, что данный компьютер был только что запущен и Windows в настоящий момент находится в стадии инициализации. Возможно, еще не успела стартовать служба *Remote Procedure Call (RPC)* .

Также возможно, что файрвол блокирует доступ к DeviceLock Service или DeviceLock Enterprise Server. Дополнительную информацию можно получить в описании ошибки 1722 (см. выше). Для решения проблем с RPC Endpoint Mapper, обратитесь к этой статье на сайте Microsoft: http://support.microsoft.com/?kbid=839880#XSLTH3267121125120121120120

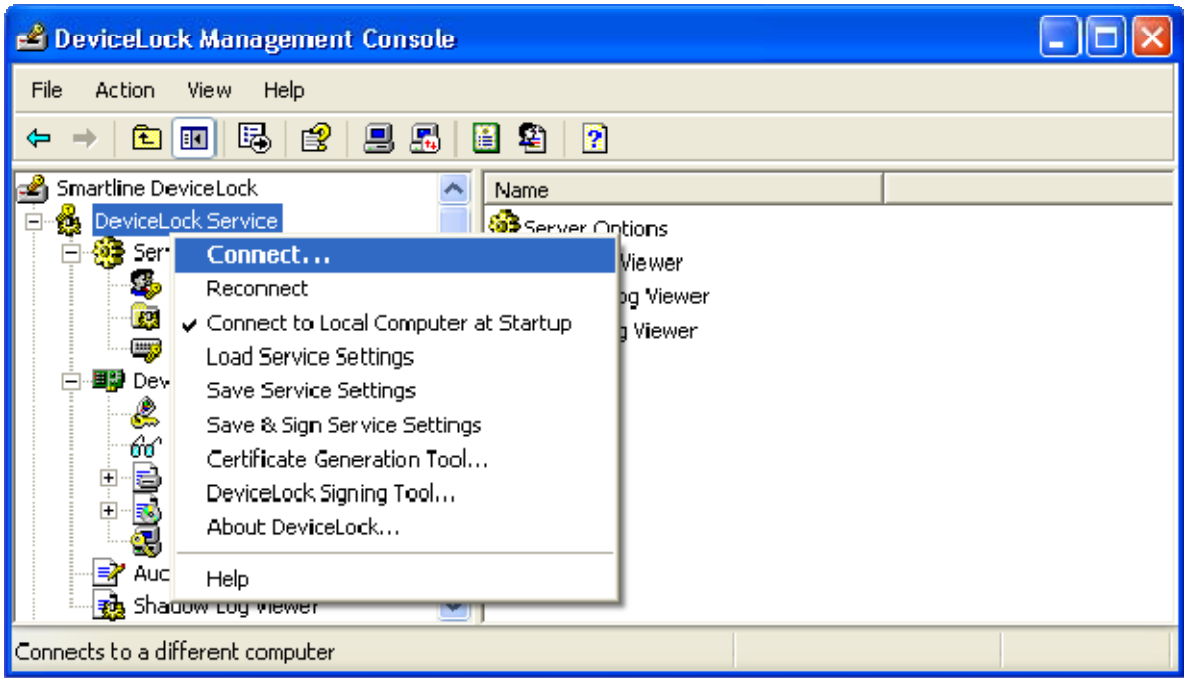
- *(5) Access is denied* – у вас недостаточно привилегий для подключения к удаленному компьютеру. Убедитесь, что консоль управления пытается подключиться к удаленному компьютеру под учетной записью пользователя с привилегиями локального администратора этого компьютера.

  Возможно, вам потребуется запустить консоль управления под учетной записью другого пользователя, который обладает необходимыми привилегиями на удаленном компьютере.

- *(7045) You must have administrative privileges to perform this operation* – у вас недостаточно привилегий для подключения к DeviceLock Service или DeviceLock Enterprise Server. Консоль управления пытается подключиться к удаленному компьютеру под пользователем, который не входит в список администраторов DeviceLock.

5.4 Администрирование DeviceLock Service

Раскройте раздел *DeviceLock Service*, чтобы получить доступ ко всем функциям и настройкам агента.



По нажатию правой кнопки мыши на элементе *DeviceLock Service* появляется контекстное меню:

- *Connect* – для подключения к удаленному или локальному компьютеру. За дополнительной информацией обращайтесь к разделу **Подключение к компьютеру** данного руководства.

- *Reconnect* – подключается к текущему компьютеру повторно.

- *Connect to Local Computer at Startup* – установите этот флаг для того, чтобы при каждом запуске консоль управления автоматически подключалась к локальному компьютеру.

- *Load Service Settings* – загружает настройки из внешнего XML-файла и передает их подключенному в данный момент DeviceLock Service'у. Вам нужно выбрать файл, созданный в DeviceLock Service Settings Editor'е, DeviceLock Management Console или в DeviceLock Group Policy Manager'е. Поскольку на данном шаге цифровая подпись не проверяется, этот файл может быть как подписанным, так и неподписанным.

- *Save Service Settings* – сохраняет все настройки из подключенного в данный момент DeviceLock Service'а во внешний XML-файл. Позже этот файл может быть отредактирован DeviceLock Service Settings Editor'ом и загружен с помощью DeviceLock Management Console и/или DeviceLock Group Policy Manager'а. Также файл с настройками может быть послан пользователям, чьи компьютеры не подключены к сети и находятся вне досягаемости консолей управления. Для предотвращения неавторизованных изменений вы должны подписать этот XML-файл при помощи цифровой подписи, используя программу DeviceLock Signing Tool и сертификат (*секретный* ключ).

- *Save & Sign Service Settings* – сохраняет все настройки из подключенного в данный момент DeviceLock Service'а во внешний XML-файл и автоматически подписывает его, используя последний использованный сертификат (*секретный* ключ). Этот пункт меню недоступен, если в программе DeviceLock Signing Tool никогда не использовался *секретный* ключ.

- *Certificate Generation Tool* – запускает специальную программу для создания сертификатов (DeviceLock Certificate). За дополнительной информацией обращайтесь к разделу **Создание сертификата** данного руководства.

- *Create MSI Package* – создает установочный пакет Microsoft Software Installer (MSI) с предопределенными настройками, полученными из подключенного в данный момент DeviceLock Service'а.

  На первом шаге вам необходимо выбрать исходный MSI-пакет с DeviceLock Service'ом. Вы можете использовать MSI-пакеты, которые поставляются вместе с DeviceLock (*DeviceLock Service.msi* и *DeviceLock Service x64.msi*).

  Затем вам надо указать имя результирующего MSI-пакета, который будет создан на основе исходного MSI-пакета, заданного на первом шаге, и настроек, полученных из подключенного в данный момент DeviceLock Service'а

С помощью такого специально созданного установочного MSI-пакета агенты DeviceLock могут быть установлены на удаленные компьютеры с уже определенными политиками безопасности (настройками). За дополнительной информацией относительно установки с помощью MSI-пакета обращайтесь к разделу **Установка через групповые политики Active Directory** данного руководства.

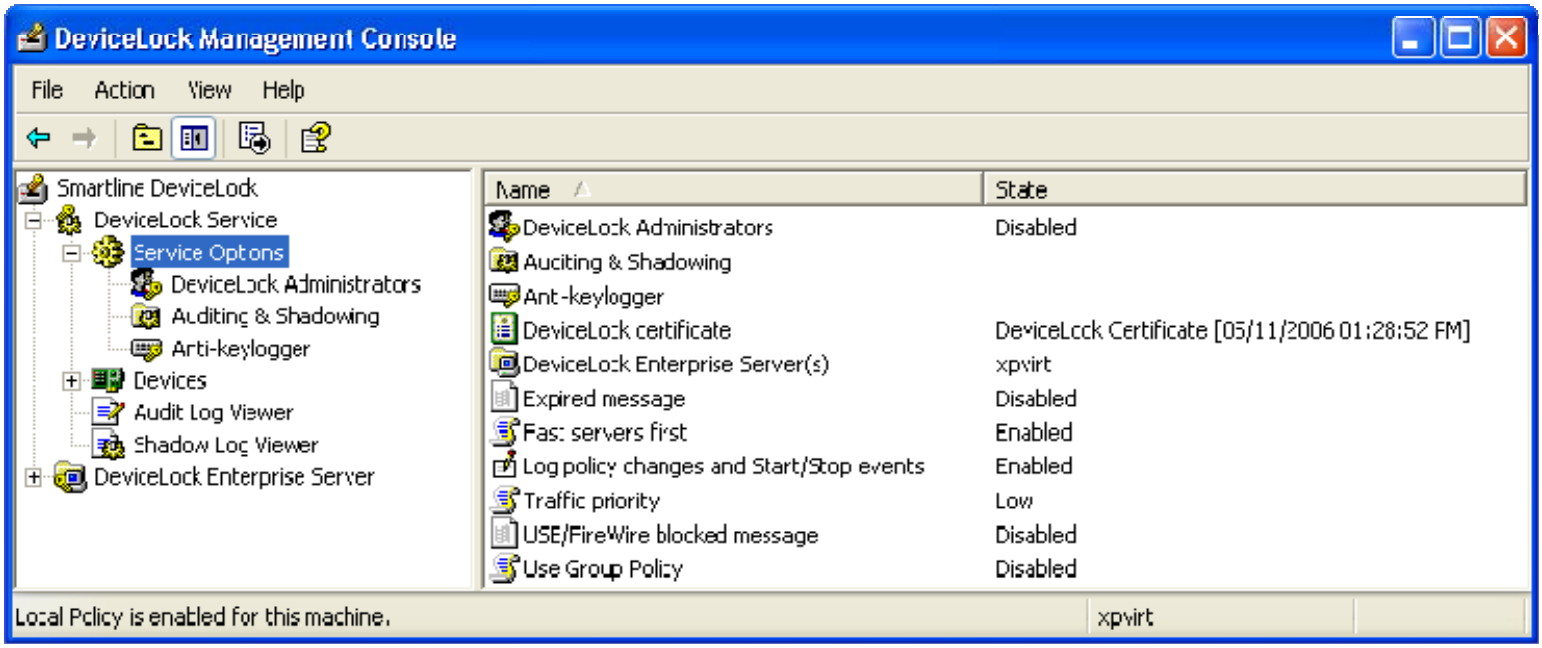
Имейте ввиду, что пункт контекстного меню *Create MSI Package* недоступен, если Microsoft Windows Installer (версии 1.0 или более поздней) не установлен на локальном компьютере.

- *DeviceLock Signing Tool* – запускает специальную программу для авторизации устройств во временном белом списке и подписывания XML-файлов с настройками DeviceLock Service'а. За дополнительной информацией обращайтесь к разделу **DeviceLock Signing Tool** данного руководства.

- *About DeviceLock* – показывает диалог с информацией о версии и установленных лицензиях на DeviceLock.

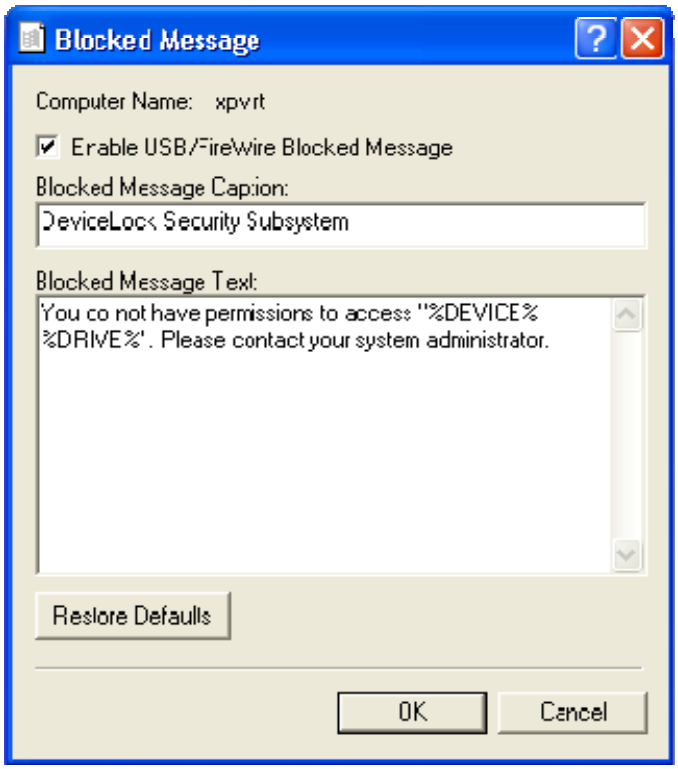
5.4.1 Service Options

Эти дополнительные параметры позволяют вам настроить DeviceLock Service. Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши на каждом параметре.



a. USB/FireWire blocked message

Вы можете определить собственное сообщение, которое будет показываться пользователю при попытке подключения запрещенных USB или FireWire-устройств.



Для разрешения показа этого пользовательского сообщения установите флаг *Enable USB/FireWire Blocked Message*.

ПРИМЕЧАНИЕ: Сообщение будет отображено только в том случае, если была попытка подключения устройства, заблокированного на уровне интерфейса (USB или FireWire). Если какое-либо устройство заблокировано только на уровне типа (например, Removable), DeviceLock не будет отображать пользовательское сообщение.

Также вы можете установить дополнительные параметры, такие как:

- *Blocked Message Caption* – текст, который будет отображаться в заголовке. Вы можете совместно с текстом использовать три предопределенных макроса:

  1. *%TYPE%* – добавляет имя порта (*USB port*, *FireWire port*), к которому подключено заблокированное устройство.

  2. *%DEVICE%* – добавляет имя устройства (например, *USB Mass Storage Device*), полученное из системы.

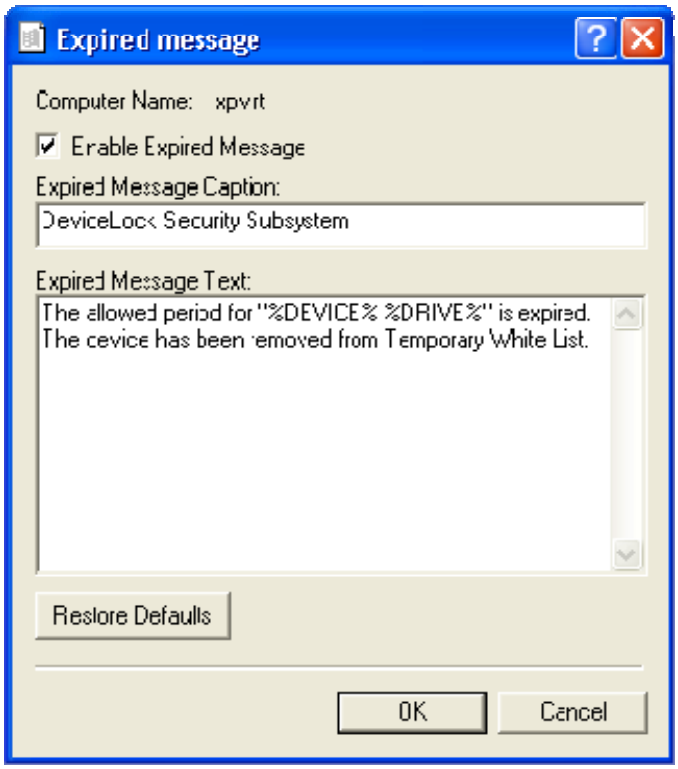
  3. *%DRIVE%* – добавляет букву диска устройства (например, *F:*). Если буква к устройству не привязана, макрос вставит пустую строку.

  Используя эти макросы, вы можете создавать более информативные сообщения для пользователя.

- *Blocked Message Text* – основной текст сообщения. Вы можете использовать предопределенные макросы аналогично тому, как описано выше.

б. Expired message

Вы можете определить пользовательское сообщение, которое будет показываться по истечении разрешенного периода использования устройств, авторизованных через функцию временного белого списка.



Для разрешения показа этого пользовательского сообщения установите флаг *Enable Expired Message*.

Также вы можете установить дополнительные параметры, такие как:

- *Expired Message Caption* – текст, который будет отображаться в заголовке. Вы можете совместно с текстом использовать два предопределенных макроса:

  1. *%DEVICE%* – добавляет имя устройства (например, *USB Mass Storage Device*), полученное из системы.

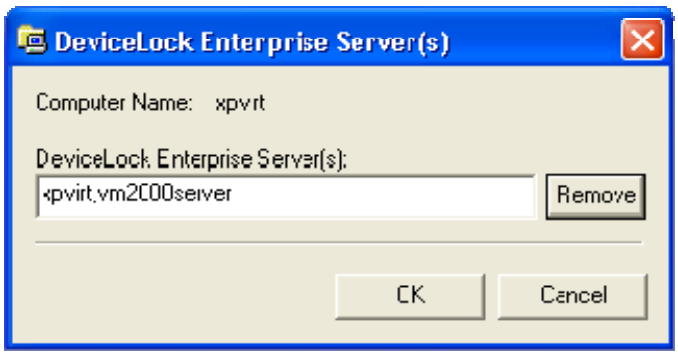
  2. *%DRIVE%* – добавляет букву диска устройства (например, *F:*). Если буква к устройству не привязана, макрос вставит пустую строку.

  Используя эти макросы, вы можете создавать более информативные сообщения для пользователя.

- *Expired Message Text* – основной текст сообщения. Вы можете использовать предопределенные макросы аналогично тому, как описано выше.

в. DeviceLock Enterprise Server(s)

Чтобы разрешить DeviceLock Service посылать свои данные на DeviceLock Enterprise Server, укажите имя или IP-адрес этого сервера.



Используя точку с запятой (;) в качестве разделителя, вы можете указать несколько DeviceLock Enterprise Server'ов, чтобы равномерно распределить нагрузку на каждый из них и на всю сеть в целом. На старте DeviceLock Service выбирает один сервер и использует его для посылки данных. Если выбранный сервер недоступен, DeviceLock Service выбирает следующий из списка.

Убедитесь в том, что DeviceLock Enterprise Server правильно установлен и сконфигурирован, в противном случае данные не будут собираться и храниться централизованно. Дополнительную информацию относительно установки сервера вы можете найти в главе **Установка DeviceLock Enterprise Server** данного руководства.

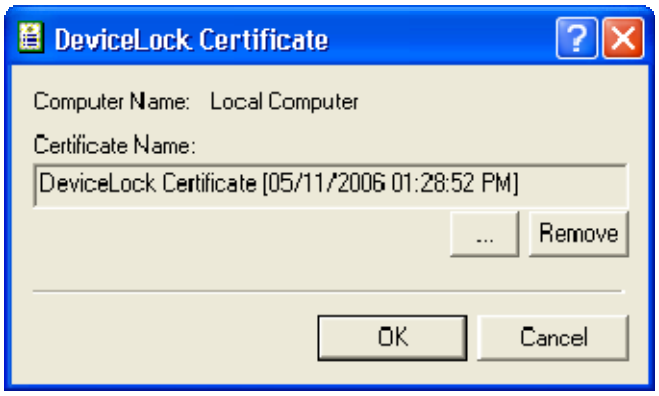
г. Log Policy changes and Start/Stop events

Вы можете разрешить протоколирование изменений в настройках DeviceLock Service и зафиксировать время старта и остановки агента. Имеется возможность ведения протокола изменений разрешений, правил аудита, белых списков и всех остальных настроек.

Для включения такого протоколирования установите флаг *Log Policy changes and Start/Stop events*.

д. DeviceLock certificate

Используйте этот параметр для установки и удаления сертификата (DeviceLock Certificate).



Укажите путь к файлу с *открытым* ключом в параметре *Certificate Name*, если вы хотите установить сертификат. Вы можете использовать кнопку **…**, чтобы открыть диалог выбора файлов.

Для удаления *открытого* ключа используйте кнопку *Remove*.

Чтобы получить дополнительную информацию, обратитесь к разделу **DeviceLock Certificate** данного руководства.

e. Use Group Policy

Если DeviceLock Service настроен для работы с групповой политикой Active Directory, вы можете осуществлять контроль за режимом эффективной политики (групповая или локальная).

Чтобы включить режим групповой политики для данного DeviceLock Service, установите флаг *Use Group Policy.* В этом режиме все изменения в настройках DeviceLock Service, которые вы внесете при помощи DeviceLock Management Console и DeviceLock Enterprise Manager, будут отменены и все параметры получат свои изначальные значения (заданные в объекте групповой политики) при следующем обновлении групповой политики.

Чтобы включить режим локальной политики для данного экземпляра DeviceLock Service, снимите флаг *Use Group Policy.* В этом режиме все изменения в настройках DeviceLock Service, которые вы внесете при помощи DeviceLock Management Console и DeviceLock Enterprise Manager, будут иметь приоритет над настройками из объекта групповой политики.

Если DeviceLock Service не был настроен для работы с групповой политикой Active Directory, флаг *Use Group Policy* снят и недоступен для изменения.

Если флаг *Use Group Policy* установлен, но недоступен для изменения, это означает, что режим групповой политики всегда имеет приоритет (установлен флаг *Override Local Policy* в DeviceLock Group Policy Manager) и режим локальной политики для данного экземпляра DeviceLock Service не может быть установлен. Дополнительную информацию вы можете найти в главе **Использование DeviceLock Group Policy Manager** данного руководства.

ж. Fast servers first

DeviceLock Service может выбирать из списка наиболее быстрый из доступных серверов.

Установите “0, чтобы DeviceLock Service выбирал сервер из списка случайным образом. Установите “1”, чтобы DeviceLock Service выбирал из списка наиболее быстрый сервер.

Если флаг *Fast servers first* установлен, то все сервера, указанные в параметре *DeviceLock Enterprise Server(s),* разделяются на три группы в зависимости от их сетевой скорости. Вначале предпочтение отдается одному из доступных серверов из самой быстрой группы. Если все сервера из быстрой группы недоступны, DeviceLock Service пытается выбрать сервер из следующей группы и так далее.

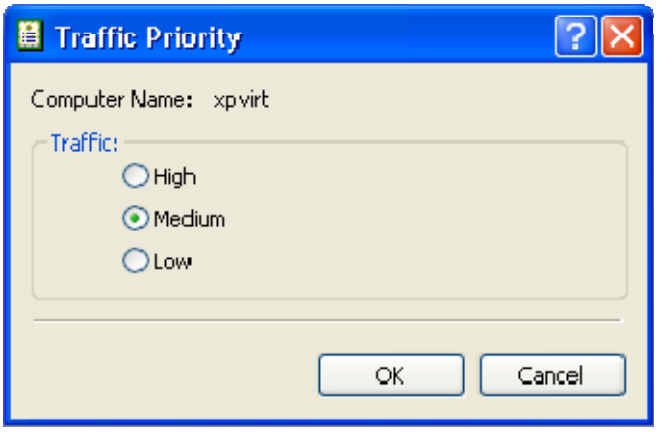
Если этот флаг не установлен, то DeviceLock Service выбирает сервер из списка случайным образом.

Данный параметр имеет силу только если в параметре *DeviceLock Enterprise Server(s)* задано больше одного сервера.

з. Traffic priority

Вы можете ограничивать пропускную способность сети для данных аудита и теневого копирования, идущих от DeviceLock Service'а на DeviceLock Enterprise Server.

Можно выбрать один из трех приоритетов: высокий, средний или низкий. Средний и низкий приоритеты снижают нагрузку на сеть.

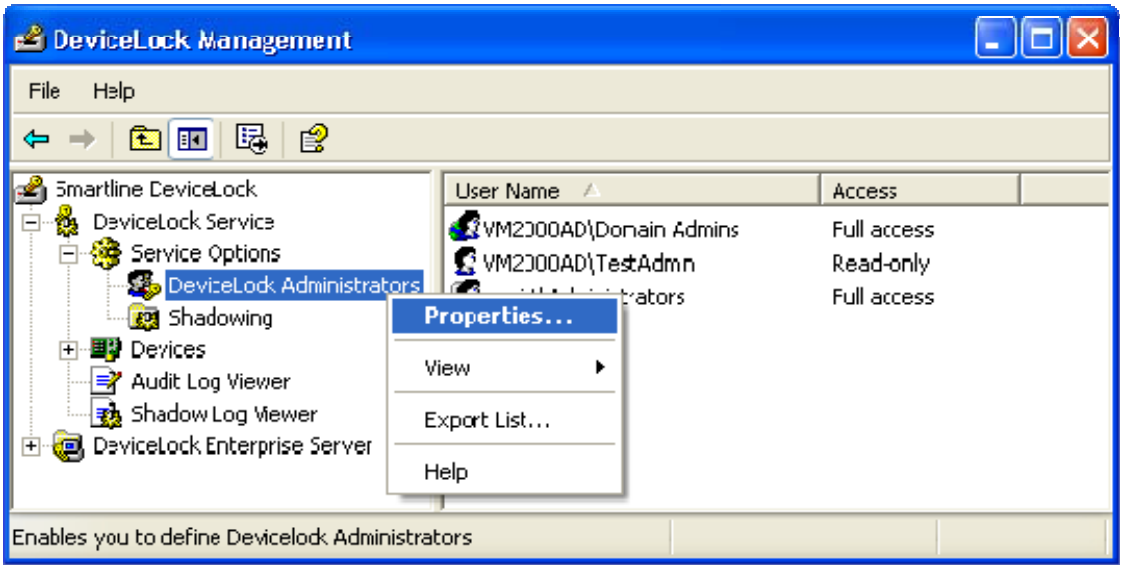


Когда выбрано *High* это означает, что может использоваться до 100% канала. Чтобы разрешить использование до 50% канала, выберите *Medium*. Выберите *Low,* чтобы задать самый низкий приоритет, при котором может использоваться до 10% канала.

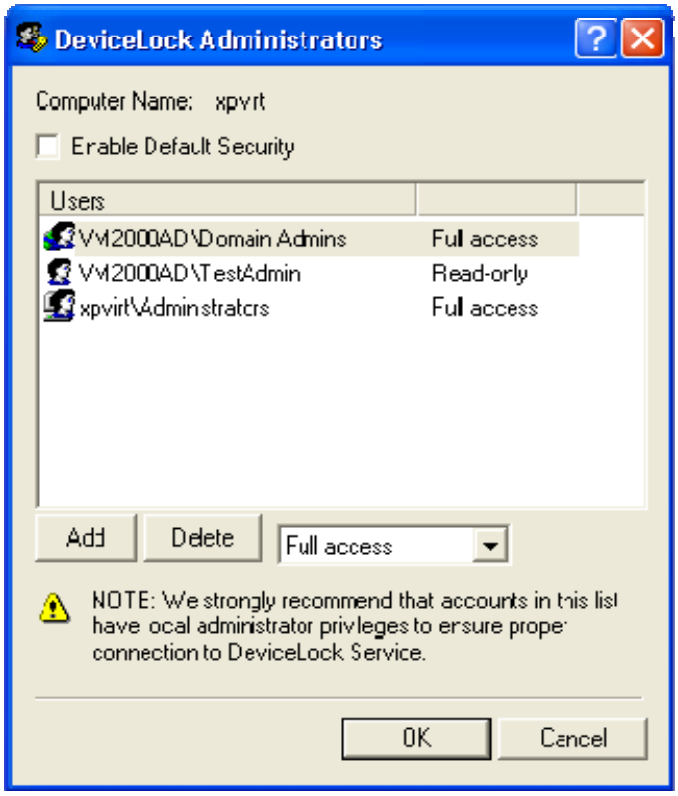
Средний и низкий приоритеты могут быть заданы, только если на компьютере с работающим DeviceLock Service'ом установлен сетевой компонент Quality of Service Packet Scheduler (QoS Packet Scheduler). В противном случае параметр *Traffic priority* недоступен для изменения и всегда используется до 100% канала. Для получения более подробной информации о QoS, обратитесь к документу Microsoft: http://www.microsoft.com/technet/network/qos/default.mspx.

5.4.1.1 DeviceLock Administrators

Эти настройки позволяют определить список учетных записей с административными правами доступа к DeviceLock Service.



Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши на элементе *DeviceLock Administrators*, чтобы открыть диалог с настройками.



Стандартная защита основана на списке управления доступом (ACL) Windows. Пользователь без локальных административных привилегий не может подключиться к DeviceLock Service, изменить его настройки или удалить его. Все это контролируется подсистемой безопасности Windows.

Для включения стандартной защиты, основанной на ACL, установите флаг *Enable Default Security*.

ПРИМЕЧАНИЕ: Как указано в разделе Рекомендуемые меры по обеспечению безопасности данного руководства, не рекомендуется наделять обычных пользователей административными привилегиями.

Пользователи с правами локального администратора (члены локальной группы *Администраторы*) могут подключаться к DeviceLock Service, используя консоль управления и изменять настройки разрешений, аудита и другие параметры. Более того, такие пользователи могут удалить DeviceLock со своих компьютеров, отключить или остановить DeviceLock Service, изменить значения ключей реестра агента, удалить исполняемый файл агента и так далее. Другими словами, пользователи с правами локального администратора могут обойти стандартную систему защиты, основанную на ACL.

Однако, даже если пользователи вашей сети имеют административные привилегии на локальных компьютерах, DeviceLock способен обеспечить необходимый уровень защиты. Когда защита DeviceLock включена, никто, исключая авторизованных администраторов, не может подключаться к DeviceLock Service, останавливать или удалять его. Даже члены локальной группы *Администраторы* (если они не входят в список авторизованных администраторов DeviceLock) не могут обойти защиту DeviceLock.

Для включения защиты DeviceLock снимите флаг *Enable Default Security*.

Затем вам необходимо определить авторизованные учетные записи (пользователей и/или группы), которые могут администрировать DeviceLock Service. Для того чтобы добавить нового пользователя или группу в список авторизованных учетных записей, нажмите кнопку *Add*. Одновременно можно добавить несколько учетных записей.

Для удаления записи из списка, используйте кнопку *Delete*. Используя клавиши *Ctrl* и/или *Shift,* вы сможете выделить и удалить несколько записей одновременно.

Чтобы определить, какие действия разрешены администратору DeviceLock, установите соответствующие права:

- **Full access** – предоставляет полный доступ к DeviceLock Service. Администраторы могут изменять ограничения, аудит и другие параметры, удалять или обновлять DeviceLock Service.

- **Change** – разрешает доступ только для изменения конфигурации. Администраторы могут изменять настройки, устанавливать и удалять DeviceLock Service, но они не могут добавлять новые учетные записи в список администраторов DeviceLock и изменять права для существующих в этом списке учетных записей.

- **Read-only** – разрешает доступ только для чтения ограничений, аудита и иных параметров. Администраторы могут просматривать отчеты, установленные параметры, но не могут ничего изменять или удалять/обновлять DeviceLock Service.

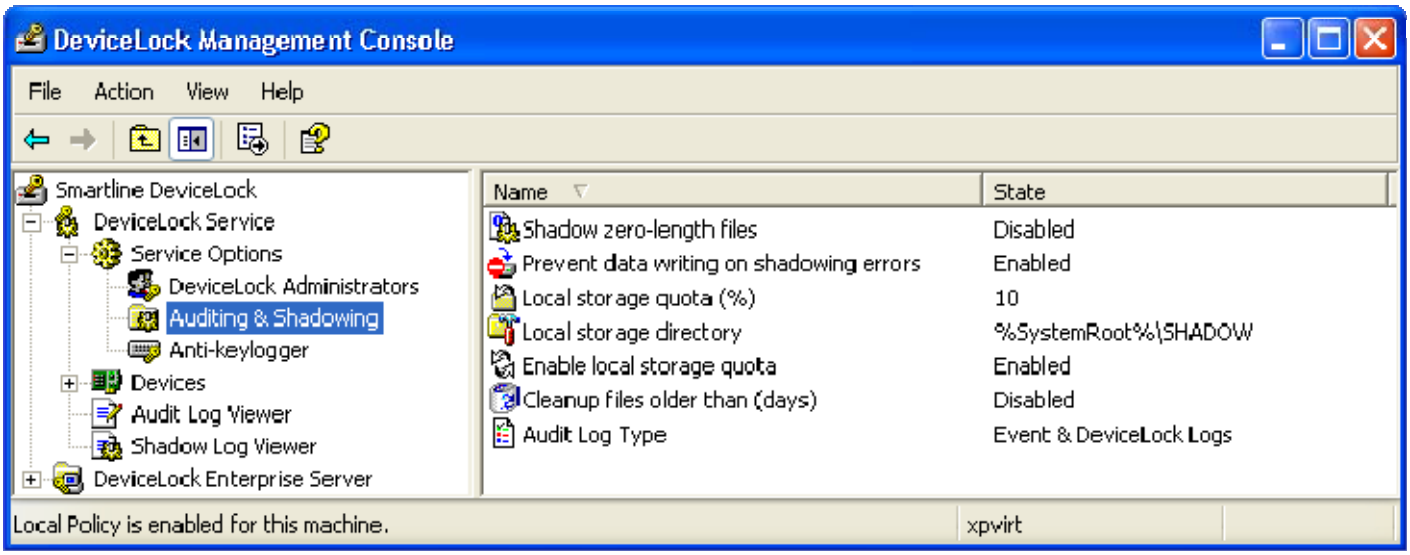
ПРИМЕЧАНИЕ: Мы настоятельно рекомендуем, чтобы учетные записи, включенные в этот список, имели привилегии локального администратора, поскольку в некоторых ситуациях (установка, обновление и деинсталляция DeviceLock Service) может потребоваться доступ к Windows Service Control Manager (SCM) и общим сетевым ресурсам.

Вот один пример того, как правильно определить список администраторов DeviceLock: добавьте группу *Domain Admins* с правами **Full access**. Группа *Domain Admins* является членом локальной группы *Администраторы* на каждом компьютере домена, все члены группы *Domain Admins* будут иметь полные права доступа к DeviceLock Service на каждом компьютере. Однако остальные члены локальной группы *Администраторы* не будут иметь возможности администрировать DeviceLock Service или останавливать его.

Помните, если DeviceLock Service установлен и работает на одном компьютере вместе с консолью управления DeviceLock и включена защита DeviceLock, ни консоль управления, ни любое иное приложение не будут иметь доступа к исполняемому файлу DeviceLock Service (*dlservice.exe* или *dlservice_x64.exe)*. Это происходит вследствие того, что DeviceLock Service защищает свой исполняемый файл от изменения пользователем с правами локального администратора. Может оказаться необходимым получить доступ к файлам *dlservice.exe* и/или *dlservice_x64.exe*, когда вы хотите установить DeviceLock Service на удаленных компьютерах со своей машины. Для этого вы можете скопировать эти исполняемые файлы в другую директорию перед включением защиты DeviceLock и использовать данные копии для удаленной установки.

5.4.1.2 Auditing & Shadowing

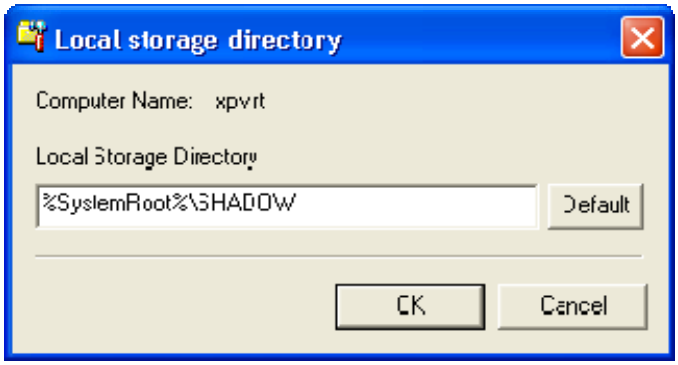
Эти настройки позволяют задать дополнительные параметры теневого копирования и аудита в DeviceLock Service.



Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши на каждом параметре.

а. Local storage directory

Используйте этот параметр, чтобы определить, где на локальном жестком диске будут сохраняться данные теневого копирования



По умолчанию DeviceLock Service использует директорию *%SystemRoot%\SHADOW* для хранения данных теневого копирования на локальном компьютере. *%SystemRoot%* – это стандартная переменная среды, которая определяет путь до корневой директории Windows (например, *C:\Windows*). Вы можете указать любую другую директорию на локальном жестком диске. DeviceLock Service защищает эту директорию, чтобы пользователи не могли получить доступ к файлам внутри нее.

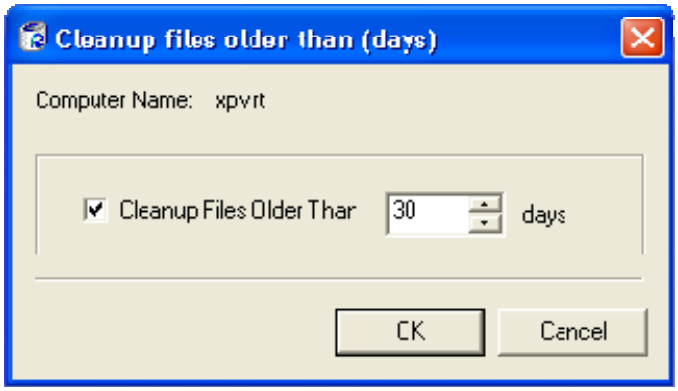
Убедитесь, что на диске есть достаточно свободного места (если пользователь может скопировать 1 Гб данных на флеш-диск, то вам необходимо примерно 2 Гб на локальном диске). Минимально необходимый размер свободного места на диске – примерно 150 Мб.

б. Enable local storage quota

Используйте этот флаг, чтобы включить или отключить автоматическую очистку локально сохраненных данных теневого копирования. Когда этот флаг установлен, вы также можете задавать параметры *Cleanup files older than (days)* и *Local storage quota (%)* parameters (см. ниже).

в. Cleanup files older than (days)

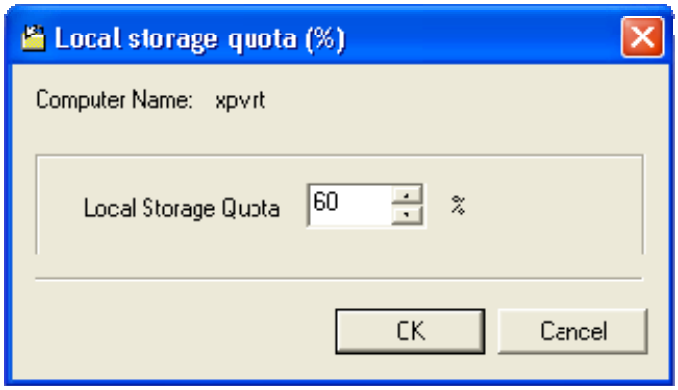
Вы можете задать количество дней, которое должно пройти, прежде чем данные теневого копирования могут быть автоматически удалены из локального хранилища, заданного в параметре *Local storage directory*.



Установите флаг *Cleanup Files Older Than* и задайте количество дней.

г. Local storage quota (%)

Вы можете задать дисковую квоту для данных теневого копирования.



В параметре *Local Storage Quota* задайте максимальный размер в процентах (от 5 до 100) свободного места на локальном диске, которое может быть занято под данные теневого копирования.

Если квота не установлена (флаг *Enable local storage quota* снят), то DeviceLock Service использует все доступное место на диске, на котором находится локальное хранилище, указанное в параметре *Local storage directory*.

Когда размер локального хранилища, указанного в параметре *Local storage directory,* превышает заданную квоту, DeviceLock Service либо начинает удалять старые данные (если задан параметр *Cleanup files older than (days)*), либо останавливает теневое копирование (если параметр *Cleanup files older than (days)* не задан либо нет сохраненных данных для удаления).

д. Shadow zero-length files

Установите этот флаг, если вы хотите включить теневое копирование для файлов нулевой длины.

Протоколирование файлов нулевой длины может понадобиться, поскольку даже если файл не содержит данных, существует возможность передать информацию (размером до нескольких килобайт) в его имени и пути.

е. Prevent data writing on shadowing errors

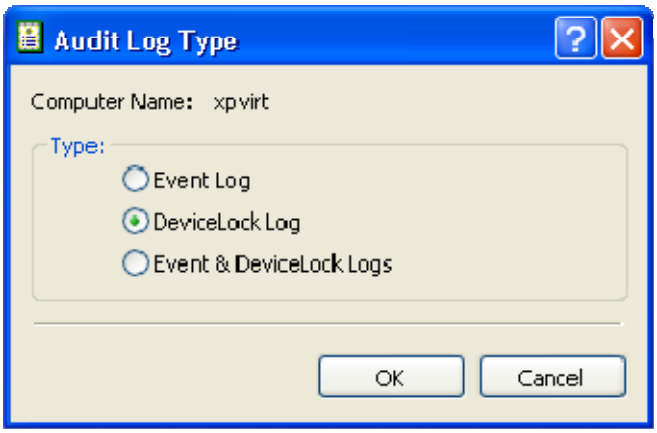
Установите этот флаг, если вы хотите запретить пользователям копировать данные, когда теневое копирование не может нормально функционировать.

Пользователи смогут передавать данные только тогда, когда функция теневого копирования нормально работает (свободное дисковое пространство достаточно для сохранения данных теневого копирования).

Если стоит флаг *Prevent data writing on shadowing errors*, превышена квота, заданная в параметре *Local storage quota (%)* и при этом нет данных, которые могут быть удалены, то DeviceLock Service останавливает теневое копирование и блокирует любые попытки пользователя передать данные.

ж. Audit log type

Используя этот параметр вы можете определить, в какой из двух журналов следует сохранять данные аудита



Есть три возможных варианта:

1. *Event Log* – данные аудита записываются только в стандартный журнал Windows (Event Log), хранящийся на локальном компьютере.

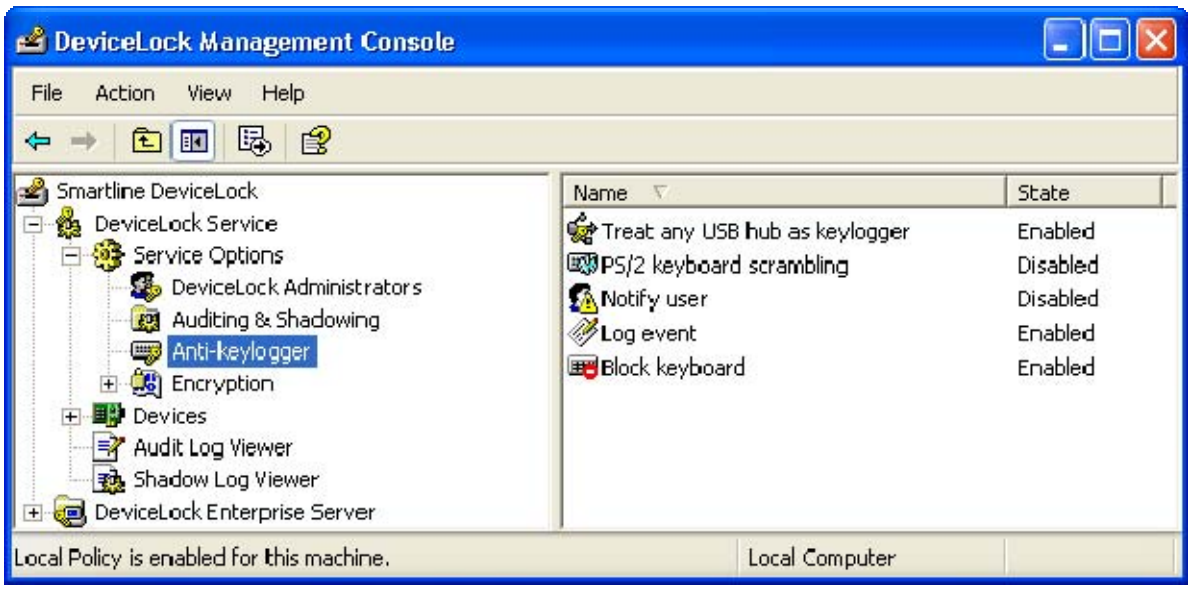
2. *DeviceLock Log* – данные аудита записываются только в собственный защищенный журнал, отсылаемый на DeviceLock Enterprise Server для централизованного хранения.

3. *Event & DeviceLock Logs* – данные аудита записываются в оба журнала.

5.4.1.3 Anti-keylogger

Эти настройки позволяют задать параметры обнаружения аппаратных кейлогеров (клавиатурных шпионов) и действия, которые DeviceLock Service должен предпринять, когда кейлогер обнаружен.

Кейлогеры - это устройства, которые перехватывают и записывают в собственную память все нажатия клавиш на клавиатуре. DeviceLock Service обнаруживает USB-кейлогеры и блокирует клавиатуры, подсоединенные к ним. Также DeviceLock Service может блокировать PS/2-кейлогеры.



Используйте контекстное меню, которое появляется по нажатию правой кнопки мыши на каждом параметре.

а. Treat any USB hub as keylogger

Установите этот флаг, если вы хотите, чтобы DeviceLock Service считал кейлогером любой USB-хаб с подключенной к нему клавиатурой.

В противном случае DeviceLock Service считает кейлогерами только те USB-хабы, которые занесены в его внутренний список.

б. PS/2 keyboard scrambling

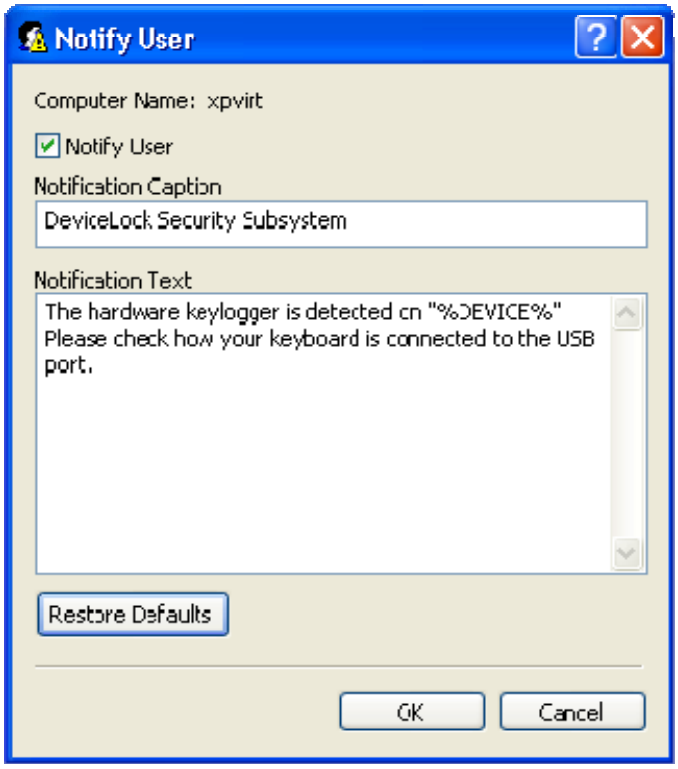
Установив этот флаг, вы можете предотвратить запись данных на PS/2-кейлогеры. DeviceLock Service не способен обнаруживать PS/2-кейлогеры и информировать пользователей об их возможном присутствии в системе. Однако DeviceLock Service искажает вводимые с PS/2-клавиатуры данные и вынуждает PS/2-кейлогеры записывать “мусор” вместо реально вводимых данных.

ПРИМЕЧАНИЕ: Когда флаг PS/2 keyboard scrambling установлен во время работы с KBM-переключателем, то переключение между компьютерами при помощи клавиатуры работать не будет.

в. Notify user

Вы можете определить пользовательское сообщение, которое будет показываться при обнаружении аппаратных USB-кейлогеров.

Поскольку DeviceLock Service запускается раньше того момента, когда пользователь вводит пароль входа в Windows, это сообщение может предупредить и предостеречь этого пользователя от набора пароля на клавиатуре подключенной к кейлогеру.



Для разрешения показа этого пользовательского сообщения установите флаг *Notify User*.

Также вы можете установить дополнительные параметры, такие как:

Notification Caption – текст, который будет отображаться в заголовке. Вы можете совместно с текстом использовать предопределенный макрос: *%DEVICE%* – добавляет имя клавиатуры (например, *USB Keyboard*), полученное из системы. Используя этот макрос, вы можете создавать более информативные сообщения для пользователя.

- *Notification Text* – основной текст сообщения. Вы можете использовать предопределенный макрос аналогично тому, как описано выше.

г. Log event

Установите этот флаг, чтобы протоколировать факты обнаружения кейлогеров в журнал аудита.

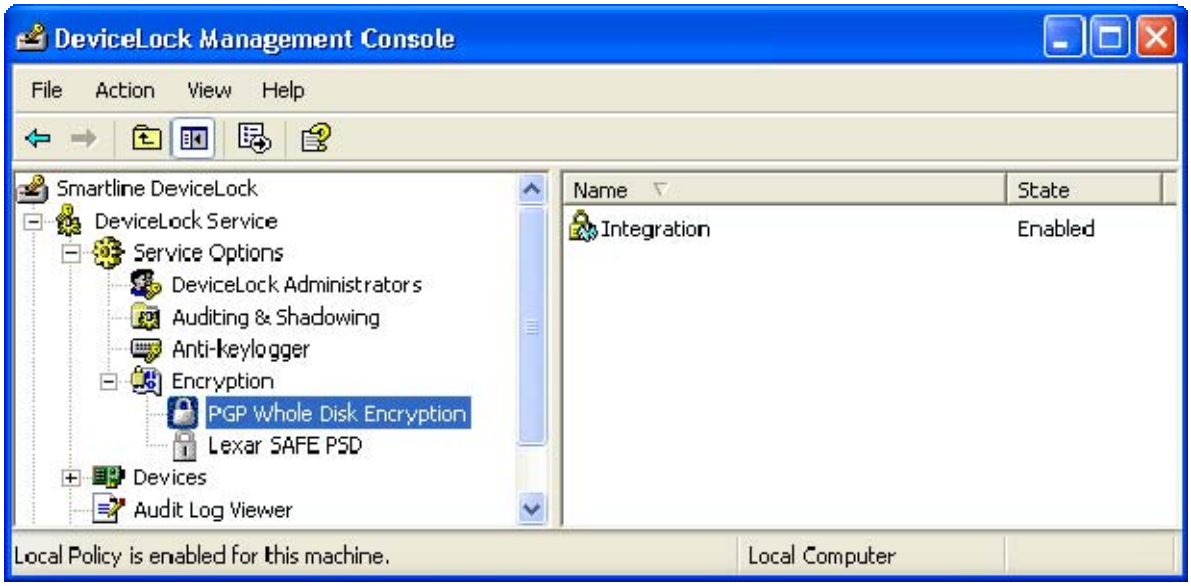
д. Block keyboard

Установите этот флаг, чтобы блокировать клавиатуру, подключенную к USB-кейлогеру в момент его обнаружения. Поскольку DeviceLock Service запускается раньше того момента, когда пользователь вводит пароль входа в Windows, блокировка клавиатуры позволит предотвратить набор пароля на клавиатуре подключенной к кейлогеру.

ПРИМЕЧАНИЕ: Некоторые аппаратные кейлогеры продолжают записывать нажатия клавиш даже на заблокированной клавиатуре, которая не функционирует в Windows. Это происходит из-за того, что такие кейлогеры являются самодостаточными устройствами и не требуют наличия драйверов и ОС.

5.4.1.4 Encryption

DeviceLock Service может обнаруживать диски (USB-флешки и другие съемные устройства), зашифрованные сторонними продуктами и применять к ним специальные “политики шифрования”. Например, вы можете разрешить запись данных только на зашифрованные устройства и запретить запись на незашифрованные.



В настоящий момент DeviceLock поддерживает следующие сторонние продукты, которые осуществляют шифрование внешних носителей:

- *PGP Whole Disk Encryption* – DeviceLock Service может обнаруживать диски, зашифрованные PGP и применять к ним специальные “политики шифрования” когда продукт PGP® Whole Disk Encryption установлен на компьютере, где запущен DeviceLock Service и установлен флаг *Integration*. Подробную пошаговую инструкцию о том, как устанавливать и использовать PGP® Whole Disk Encryption совместно с DeviceLock, можно найти в документе **PGP/DeviceLock Integration Guide** (на английском языке), созданном компанией PGP. Для получения более подробной информации о PGP® Whole Disk Encryption посетите сайт компании PGP: www.pgp.com/products/wholediskencryption/index.html.

- *Lexar SAFE PSD* – DeviceLock Service может обнаруживать USB-диски Lexar™ SAFE PSD S1100 и применять к ним специальные “политики шифрования” когда пользователи подключают эти диски к компьютерам, где работает DeviceLock Service и установлен флаг *Integration*. Для получения более подробной информации о Lexar™ SAFE PSD S1100 посетите сайт компании Lexar: www.lexar.com/enterprise/safe_psd_S1100.html.

- *TrueCrypt* – DeviceLock Service может обнаруживать диски, зашифрованные TrueCrypt и применять к ним специальные “политики шифрования” когда продукт TrueCrypt установлен на компьютере, где запущен DeviceLock Service и установлен флаг *Integration*. Для получения более подробной информации о TrueCrypt, посетите сайт: www.truecrypt.org. ***ПРИМЕЧАНИЕ: Чтобы DeviceLock Service мог определить раздел TrueCrypt’а как шифрованный, этот раздел***

должен быть создан как "Partition/device-hosted". Если раздел создан как "File-hosted (container)", DeviceLock всегда будет распознавать его как нешифрованный.

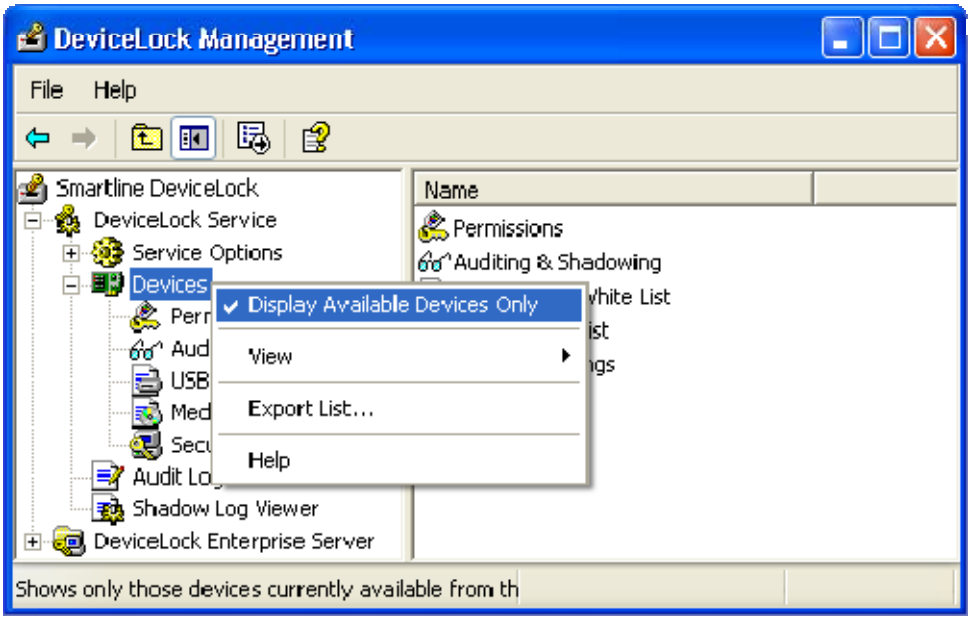
Если вы не хотите, чтобы DeviceLock Service обнаруживал диски, зашифрованные каким-либо сторонним продуктом (из списка продуктов перечисленных выше) и применял к ним специальные "политики шифрования", то снимите флаг *Integration* в разделе соответствующем этому продукту.

За дополнительной информацией относительно "политик шифрования", обратитесь к разделу **Permissions** данного руководства.

ПРИМЕЧАНИЕ: DeviceLock не поставляется вместе со сторонними продуктами шифрования и не требует их наличия для своего функционирования. Сторонний продукт шифрования должен быть правильно установлен, настроен и запущен на том же самом компьютере, где работает DeviceLock Service, только когда вы хотите использовать интеграцию DeviceLock'а с этим сторонним продуктом.

5.4.2 Devices

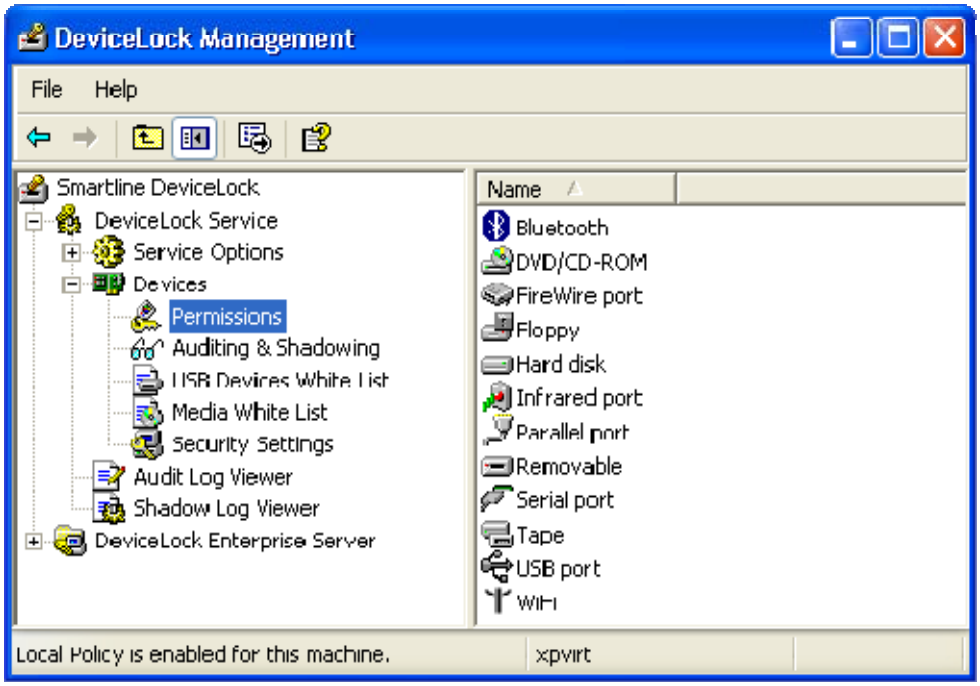
Эти настройки предоставляют доступ к основным функциям DeviceLock – установка разрешений, правил аудита и теневого копирования, белым спискам и т.д.



Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши на элементе *Devices*, чтобы получить доступ к флагу *Display Available Devices Only*. Если этот флаг установлен, то DeviceLock Management Console показывает только те типы устройств, которые доступны в данный момент на подключенном компьютере. В противном случае вы увидите список всех типов устройств, поддерживаемых DeviceLock. Такой вариант полезен, когда вы хотите установить ограничения на те устройства, которые в данный момент к компьютеру не подключены.

5.4.2.1 Permissions

В этом списке показывается список типов устройств, для которых вы можете установить разрешения.



ПРИМЕЧАНИЕ: При установке разрешений на тип устройств они устанавливаются одновременно для всех устройств, принадлежащих к данному типу. Невозможно установить разные разрешения на устройства одного типа, например, на два дисковода. Чтобы задать разные права доступа для пользователей к USB-устройствам одного типа, вы можете воспользоваться функцией [белый список устройств](#).

Контроль доступа может выполняться на двух уровнях: уровне интерфейса (порта) и уровне типа. Некоторые устройства проверяются на обоих уровнях, в то время как другие – только на одном: либо на уровне интерфейса (порта), либо на уровне типа.

Чтобы получить дополнительную информацию о том, как работает контроль доступа к устройствам в DeviceLock, обратитесь к разделу **Управляемый контроль доступа** данного руководства.

DeviceLock поддерживает следующие типы устройств:

1. *Bluetooth* (уровень типа) – включает все внешние и внутренние Bluetooth-адаптеры, с любым интерфейсом подключения к компьютеру (USB, PCMCIA и т.д.).

2. *DVD/CD-ROM* (уровень типа) – включает все внешние и внутренние CD/DVD-приводы (включая пишущие) с любым интерфейсом подключения к компьютеру (IDE, SATA, USB, FireWire, PCMCIA и т.д.).

3. *FireWire port* (уровень интерфейса) – включает все устройства, которые могут быть подключены к FireWire-порту (IEEE 1394), исключая хабы.

4. *Floppy* (уровень типа) – включает все внешние и внутренние дисководы, с любым интерфейсом подключения к компьютеру (IDE, USB, PCMCIA и т.д.). Существуют некоторые модели нестандартных дисководов, которые распознаются Windows как сменные накопители, в этом случае DeviceLock также относит такие дисководы к типу *Removable*.

5. *Hard disk* (уровень типа) – включает все внешние и внутренние жесткие диски, с любым интерфейсом подключения к компьютеру (IDE, SATA, SCSI и т.д.). DeviceLock относит все жесткие диски, подключаемые через интерфейсы USB, FireWire и PCMCIA к типу *Removable*. Также DeviceLock относит к типу *Removable* некоторые жесткие диски (обычно с интерфейсом подключения SATA и SCSI), если они поддерживают функцию “горячего” подключения и при этом на них не установлена используемая ОС Windows.

   ПРИМЕЧАНИЕ: Даже если вы полностью запретили доступ к жесткому диску, пользователи с правами локального администратора и сама ОС смогут получить доступ к разделу этого диска, на котором установлена текущая ОС Windows.

6. *Infrared port* (уровень интерфейса) – включает все устройства, которые могут быть подключены к компьютеру через инфракрасный порт (IrDA).

7. *Palm* (уровень типа) – включает все устройства, работающие под управлением ОС Palm OS, с любым интерфейсом подключения к компьютеру (USB, COM, IrDA, Bluetooth, WiFi). DeviceLock контролирует те Palm-устройства, которые работают с компьютером через приложение HotSync.

8. *Parallel port* (уровень интерфейса) – включает все устройства, которые могут быть подключены к компьютеру через параллельный порт (LPT).

9. *Printer* (уровень типа) – включает все локальные и сетевые принтеры, с любым интерфейсом подключения к компьютеру (USB, LPT, Bluetooth и т.д.). DeviceLock может также контролировать виртуальные принтеры, т.е. принтеры, которые печатают не на реальном физическом устройстве, а, например, перенаправляют печать в файл.

10. *Removable* (уровень типа) – включает все устройства с любым интерфейсом подключения к компьютеру (USB, FireWire, PCMCIA, IDE, SATA, SCS и т.д.), которые распознаются Windows как сменные накопители (например, USB-флешки, карт-ридеры, магнитооптические приводы и т.п.). DeviceLock относит все жесткие диски, подключаемые через интерфейсы USB, FireWire и PCMCIA к типу *Removable*. Также DeviceLock относит к типу *Removable* некоторые жесткие диски (обычно с интерфейсом подключения SATA и SCSI), если они поддерживают функцию “горячего” подключения и при этом на них не установлена используемая ОС Windows.

11. *Serial port* (уровень интерфейса) – включает все устройства, которые могут быть подключены к компьютеру через последовательный порт (COM), включая внутренние модемы.

12. *Tape* (уровень типа) – включает все внешние и внутренние ленточные накопители с любым интерфейсом подключения к компьютеру (SCSI, USB, IDE и т.д.).

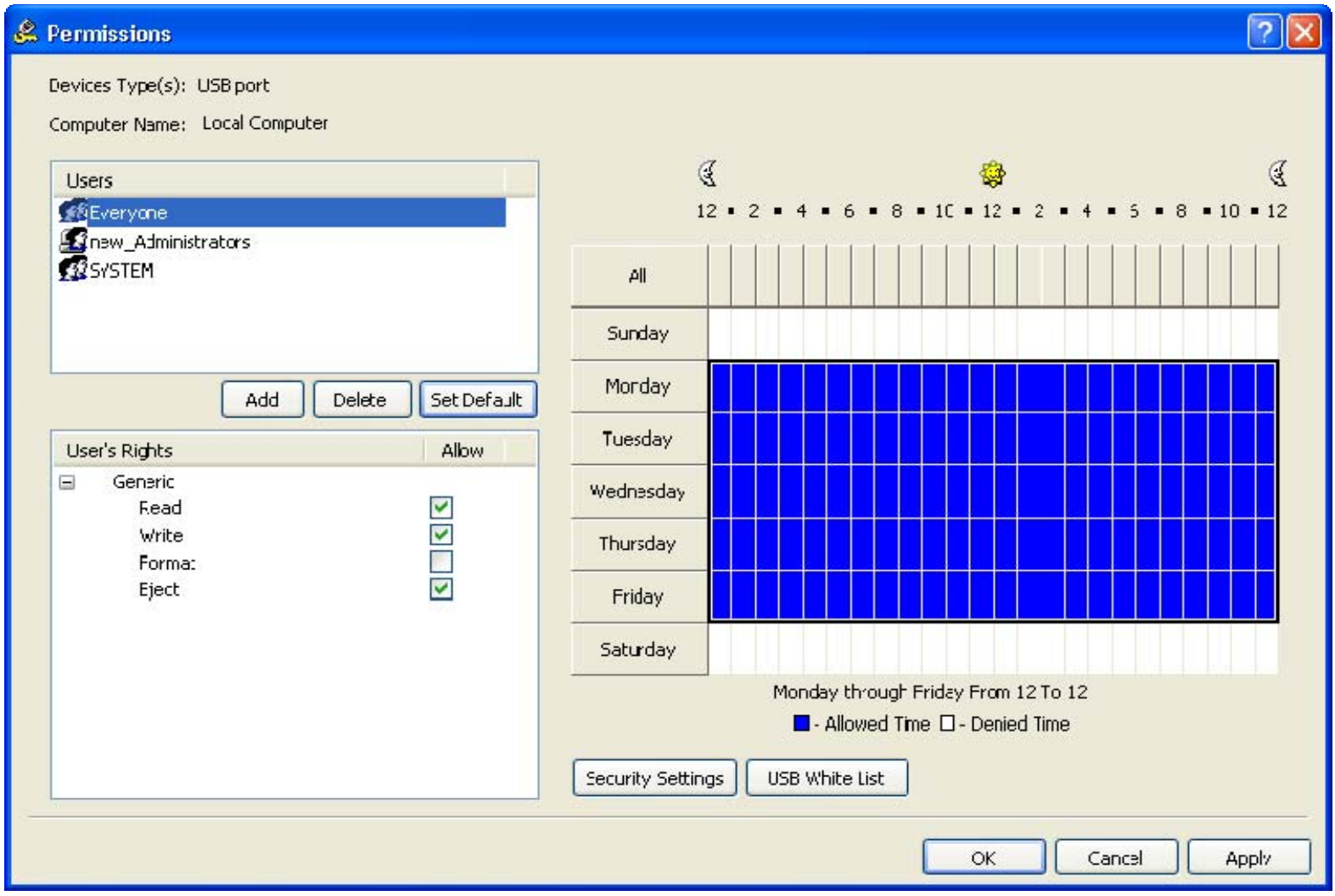
13. *USB port* (уровень интерфейса) – включает все устройства, которые могут быть подключены к USB-порту, исключая хабы.

14. *WiFi* (уровень типа) – включает все внешние и внутренние WiFi-адаптеры, с любым интерфейсом подключения к компьютеру (USB, PCMCIA и т.д.).

    ПРИМЕЧАНИЕ: Используя тип WiFi, вы можете контролировать доступ пользователей к самим устройствам этого типа, но не к сетям.

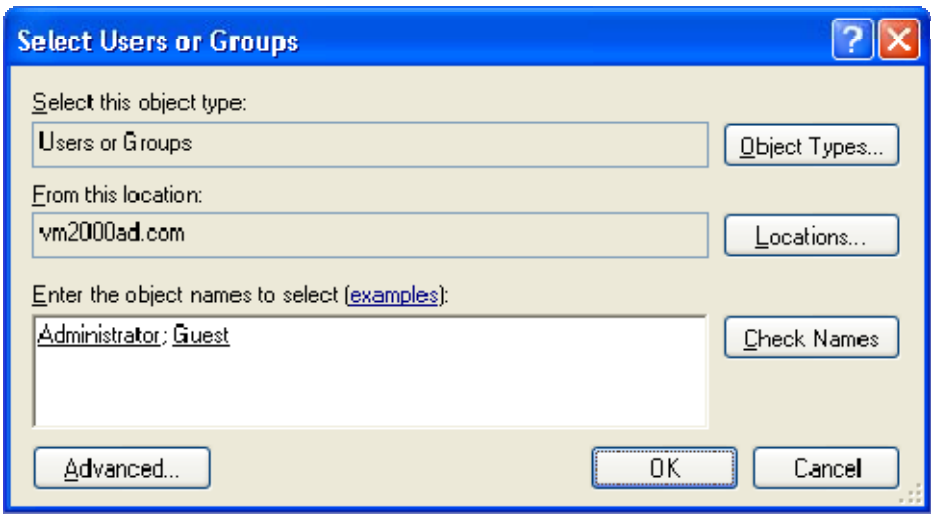
15. *Windows Mobile* (уровень типа) – включает все устройства, работающие под управлением ОС Windows Mobile, с любым интерфейсом подключения к компьютеру (USB, COM, IrDA, Bluetooth, WiFi). DeviceLock контролирует те Windows Mobile-устройства, которые работают с компьютером через приложения Windows Mobile Device Center (WMDC) и Microsoft ActiveSync или их программный интерфейс (API).

Чтобы установить разрешения на тип устройства, выделите его (для одновременного выделения нескольких типов устройств используйте клавиши *Ctrl* и/или *Shift*) и выберите пункт *Set Permissions* из контекстного меню, либо используйте соответствующую кнопку на инструментальной панели.



Имена пользователей и групп пользователей, назначенных данному типу, отображаются в списке учетных записей в левой верхней части диалога *Permissions*.

Чтобы добавить нового пользователя или группу пользователей в список учетных записей, нажмите на кнопку *Add*. Вы можете добавить несколько учетных записей одновременно.



Для удаления учетных записей из списка используйте кнопку *Delete*. Используя клавиши *Ctrl* и/или *Shift*, вы можете выбирать и удалять несколько записей одновременно.

Чтобы установить для устройства разрешения по умолчанию, необходимо использовать кнопку *Set Default*. Разрешения по умолчанию заданы следующим образом:

Учетная запись / Тип устройства	Все	Администраторы	СИСТЕМА
Bluetooth	*Generic*: Read, Write	*Generic*: Read, Write	*Generic*: Read, Write
DVD/CD-ROM	*Generic*: Read, Write, Eject	*Generic*: Read, Write, Eject	*Generic*: Read, Write, Eject
FireWire port	*Generic*: Read, Write, Eject	*Generic*: Read, Write, Format, Eject	*Generic*: Read, Write, Format, Eject
Floppy	*Generic*: Read, Write, Eject	*Generic*: Read, Write, Format, Eject	*Generic*: Read, Write, Format, Eject
Hard disk	*Generic*: Read, Write	*Generic*: Read, Write, Format	*Generic*: Read, Write, Format
Infrared port	*Generic*: Read, Write	*Generic*: Read, Write	*Generic*: Read, Write
Palm	*Generic*: Read, Write	*Generic*: Read, Write	*Generic*: Read, Write
Parallel port	*Generic*: Read, Write	*Generic*: Read, Write	*Generic*: Read, Write

Учетная запись / Тип устройства	Все	Администраторы	СИСТЕМА
Printer	*Generic*: Print	*Generic*: Print	*Generic*: Print
Removable	*Generic*: Read, Write, Eject *Encrypted*: Read, Write, Format	*Generic*: Read, Write, Format, Eject *Encrypted*: Read, Write, Format	*Generic*: Read, Write, Format, Eject *Encrypted*: Read, Write, Format
Serial port	*Generic*: Read, Write	*Generic*: Read, Write	*Generic*: Read, Write
Tape	*Generic*: Read, Write	*Generic*: Read, Write	*Generic*: Read, Write
USB port	*Generic*: Read, Write, Eject	*Generic*: Read, Write, Format, Eject	*Generic*: Read, Write, Format, Eject
WiFi	*Generic*: Read, Write	*Generic*: Read, Write	*Generic*: Read, Write
Windows Mobile	*Generic*: Read, Write, Execute	*Generic*: Read, Write, Execute	*Generic*: Read, Write, Execute

Используя контроль по времени, вы можете задать период, когда выбранный пользователь или группа будут иметь (или не иметь) доступ к устройствам. Специальный элемент управления для выбора времени расположен в правом верхнем углу диалога Permissions. Используйте левую кнопку мыши для выбора разрешенного времени. Для выбора времени, когда доступ запрещен, используйте правую кнопку мыши. Для задания разрешенных или запрещенных периодов вы также можете использовать клавиатуру: стрелки для навигации и пробел для переключения между разрешенным/запрещенным временем.

Для определения действий, доступных или недоступных пользователю или группе, необходимо установить соответствующие права. Все права в DeviceLock'е разделены на три группы: *Generic*, *Encrypted* и *Special Permissions*. Каждая группа имеет свой собственный набор прав:

- **Generic** – группа "Generic" не применяется к устройствам, которые распознаются DeviceLock Service'ом как шифрованные. За дополнительной информацией относительно интеграции со сторонними продуктами шифрования обращайтесь к разделу **Encryption** данного руководства.

  - **Read** – разрешает чтение данных с устройства. Данное право применимо ко всем типам устройств.

  - **Write** – разрешает запись данных на устройство. Для всех типов устройств, кроме *Windows Mobile* вы можете установить это право, только если установлено право **Read** из группы *Generic*. Данное право не может быть отключено для следующих типов устройств: *Bluetooth*, *Infrared port*, *Parallel port*, *Serial port* и *WiFi*. Если право **Write** отключено для USB и FireWire-портов, то это означает следующее: устройства хранения данных (такие как дисководы, CD/DVD-приводы, флеш-диски и т.п.) могут быть доступны для чтения; устройства, не предназначенные для хранения данных (такие как принтеры, сканеры и т.п.), становятся недоступны.

- **Format** – разрешает форматирование и другие действия, для которых необходим прямой доступ к устройству. Вы можете установить это право только в том случае, если установлено право **Read** из группы *Generic*. Данное право применимо только к следующим типам устройств: *FireWire port*, *Floppy*, *Hard disk*, *Removable* и *USB port*. Если это право установлено для USB и FireWire-портов, то оно влияет только на устройства хранения данных, подключаемые к этим портам.

- **Eject** – разрешает извлечение сменного носителя из устройства. Вы можете установить это право только в том случае, если установлено право **Read** из группы *Generic*. Это право контролирует только программное извлечение носителя. Физическое извлечение путем нажатия на кнопку на передней панели устройства не может быть предотвращено. Данное право применимо только к следующим типам устройств: *DVD/CD-ROM*, *FireWire port*, *Floppy*, *Removable* и *USB port*. Если это право установлено для USB и FireWire-портов, то оно влияет только на устройства хранения данных, подключаемые к этим портам.

- **Execute** – разрешает удаленное выполнение кода на стороне устройства. Данное право применимо только к типу *Windows Mobile*.

- **Print** – разрешает печать документов. Данное право применимо только к типу *Printer*.

- **Encrypted** – группа "Encrypted" применяется только к устройствам, которые распознаются DeviceLock Service'ом как шифрованные. За дополнительной информацией относительно интеграции со сторонними продуктами шифрования обращайтесь к разделу **Encryption** данного руководства.

  - **Read** – разрешает чтение данных с шифрованного устройства. Данное право применимо только к типу *Removable*.

  - **Write** – разрешает запись данных на шифрованное устройство. Вы можете установить это право, только если установлено право **Read** из группы *Encrypted*. Данное право применимо только к типу *Removable*.

  - **Format** – разрешает форматирование и другие действия, для которых необходим прямой доступ к шифрованному устройству. Вы можете установить это право, только если установлено право **Read** из группы *Encrypted*. Данное право применимо только к типу *Removable*.

- **Special Permissions** – эти права применимы только к типам *Windows Mobile* и *Palm*. Типы данных (*Calendar*, *Contacts*, *Tasks*, и т.д.), которые контролируются данными правами, представляют те же типы данных, что и их аналоги в приложениях HotSync, Microsoft ActiveSync и WMDC. Для Palm-устройств вы можете включить любое Write-право, только если включено соответствующее ему Read-право.

  - **Read Calendar** – разрешает чтение данных календаря с мобильного устройства.

- **Write Calendar** – разрешает запись данных календаря на мобильное устройство.
- **Read Contacts** – разрешает чтение контактов с мобильного устройства.
- **Write Contacts** – разрешает запись контактов на мобильное устройство.
- **Read E-mail** – разрешает чтение электронной почты с мобильного устройства.
- **Write E-mail** – разрешает запись электронной почты на мобильное устройство.
- **Read Attachments** – разрешает чтение вложений электронной почты с Windows Mobile-устройства. Вы можете установить это право, только если установлено право **Read E-mail** из группы *Special Permissions*.
- **Write Attachments** – разрешает запись вложений электронной почты на Windows Mobile-устройство. Вы можете установить это право, только если установлено право **Write E-mail** из группы *Special Permissions*.
- **Read Favorites** – разрешает чтение избранного (закладок) с Windows Mobile-устройства.
- **Write Favorites** – разрешает запись избранного (закладок) на Windows Mobile-устройство.
- **Read Files** – разрешает чтение файлов с мобильного устройства.
- **Write Files** – разрешает запись файлов на мобильное устройство. Для Palm-устройства данное право также включает право **Write Document** из группы *Special Permissions*.
- **Read Media** – разрешает чтение медиа-данных с Windows Mobile-устройства при помощи Windows Media Player и чтение медиа-файлов с Palm-устройства. Вы можете установить это право, только если установлено право **Read Files** из группы *Special Permissions*. Для Windows Mobile-устройства это право также требует установки **Execute** из группы *Generic*.
- **Write Media** – разрешает запись медиа-данных на Windows Mobile-устройство при помощи Windows Media Player и запись медиа-файлов на Palm-устройство. Вы можете установить это право, только если установлено право **Write Files** из группы *Special Permissions*. Для Windows Mobile-устройства это право также требует установки **Execute** из группы *Generic*.
- **Read Notes** – разрешает чтение заметок с мобильного устройства. Для Palm-устройства это право контролирует типы данных *Memos* и *Note Pad*.
- **Write Notes** – разрешает запись заметок на мобильное устройство. Для Palm-устройства это право контролирует типы данных *Memos* и *Note Pad*.

- **Read Pocket Access** – разрешает чтение баз данных Pocket Access с Windows Mobile-устройства.
- **Write Pocket Access** – разрешает запись баз данных Pocket Access на Windows Mobile-устройство.
- **Read Tasks** – разрешает чтение задач с мобильного устройства.
- **Write Tasks** – разрешает запись задач на мобильное устройство.
- **Read Expense** – разрешает чтение данных приложения Palm Expense с Palm-устройства.
- **Write Expense** – разрешает запись данных приложения Palm Expense на Palm-устройство.
- **Read Document** – разрешает чтение документов с Palm-устройства. Вы можете установить это право, только если установлено право **Read Files** из группы *Special Permissions*.
- **Write Document** – разрешает запись документов на Palm-устройство. Вы можете установить это право, только если установлено право **Write Files** из группы *Special Permissions*.
- **Read Unknown Content** – разрешает чтение некатегоризированных данных с Windows Mobile-устройства.
- **Write Unknown Content** – разрешает запись некатегоризированных данных на Windows Mobile-устройство.

Если все права включены для учетной записи, это означает, что данная учетная запись имеет полный доступ к устройству – “full access”. Если все права отключены для учетной записи, то это означает, что данная учетная запись вообще не имеет доступа к устройству – “no access”.

ПРИМЕЧАНИЕ: Право “no access” имеет приоритет над всеми остальными правами. Это означает, что если группе, к которой принадлежит пользователь, назначить право “no access”, а самому пользователю назначить ‘full access”, то пользователь все равно не получит доступа к устройству. Если вы хотите запретить доступ для какого-либо пользователя (или группы), просто удалите его из списка учетных записей, вместо того, чтобы ставить ему право “no access”.

Кроме того, учетная запись Все имеет приоритет над всеми остальными учетными записями. Это означает, что если учетной записи Все установлено право “no access”, то никто вообще не сможет получить доступ к устройству.

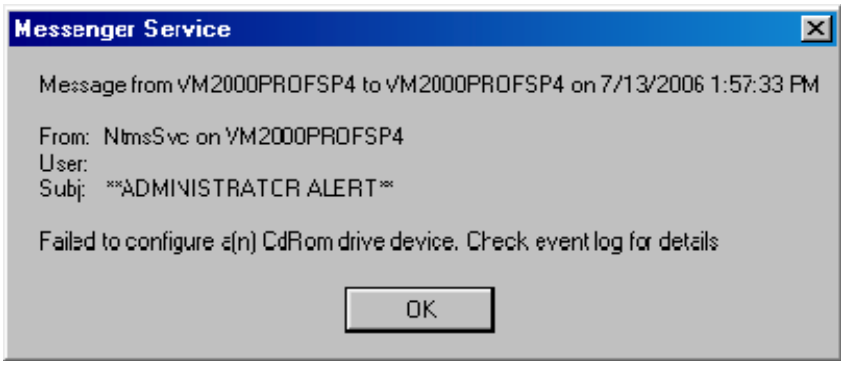
Даже если вы полностью запретили доступ к жесткому диску, члены локальной группы *Администраторы* и учетная запись *СИСТЕМА* смогут получить доступ к разделу этого диска, на котором установлена используемая ОС Windows.

Мы рекомендуем добавлять в список учетных записей только тех пользователей, которые должны иметь доступ к устройству.

Если список учетных записей пуст, это означает, что никто не имеет доступ к устройству.

Также настоятельно рекомендуется добавить учетную запись *СИСТЕМА* с правом “full access” для жестких дисков и CD/DVD-приводов.

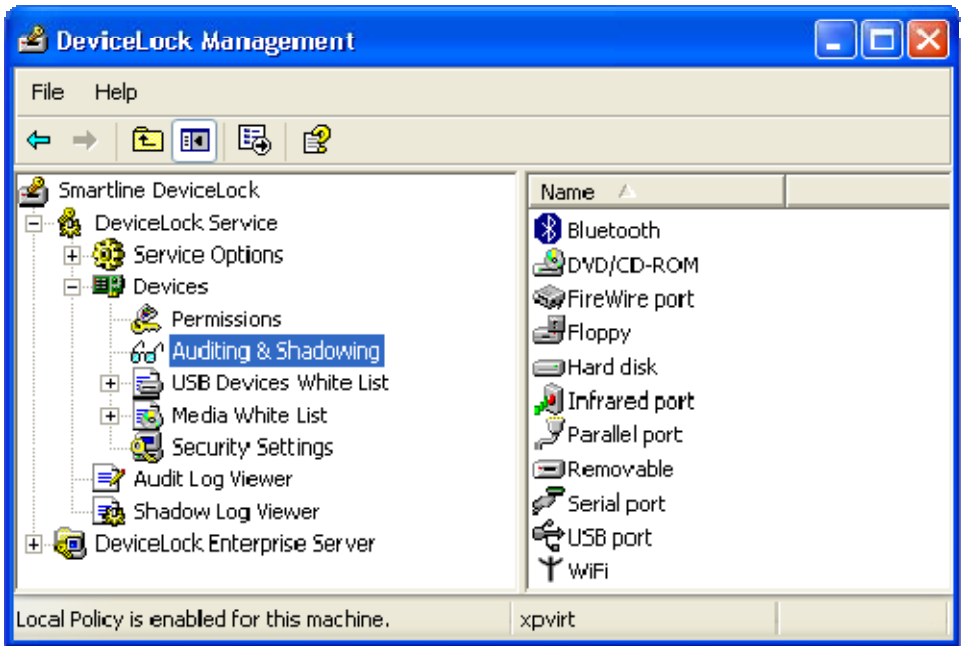
На некоторых компьютерах пользователи могут видеть подобное сообщение при входе в систему.



Это значит, что учетная запись *СИСТЕМА* не может получить доступ к CD/DVD-приводу. Чтобы избежать такой ситуации, установите право “full access” на доступ к CD/DVD-приводу для учетной записи *СИСТЕМА*.

5.4.2.2 Auditing & Shadowing

В этом списке показывается список типов устройств, для которых вы можете настроить правила аудита и теневого копирования.



Между назначением прав доступа и правил аудита нет значительной разницы, поэтому мы рекомендуем вам прочитать раздел **Permissions** данного руководства до того, как вы будете задавать правила аудита.

DeviceLock Service может использовать стандартную подсистему ведения протоколов событий (Windows Event Log) для регистрации информации об устройствах. Это особенно важно для системных администраторов, поскольку они могут использовать любое программное обеспечение для просмотра стандартных журналов Windows. Вы можете, к примеру, использовать стандартную программу *Event Viewer*. Также DeviceLock Service может использовать собственный защищенный журнал. Данные из этого журнала передаются на DeviceLock Enterprise Server для централизованного хранения в базе данных. Чтобы указать, в какой из двух журналов следует сохранять данные аудита, используйте параметр *Audit log type* из Service Options.

DeviceLock Management Console имеет встроенный просмотрщик событий, который предлагает более удобную форму представления информации из стандартного журнала Windows. Чтобы получить дополнительную информацию, обратитесь к разделу **Audit Log Viewer (для компьютера)** данного руководства.

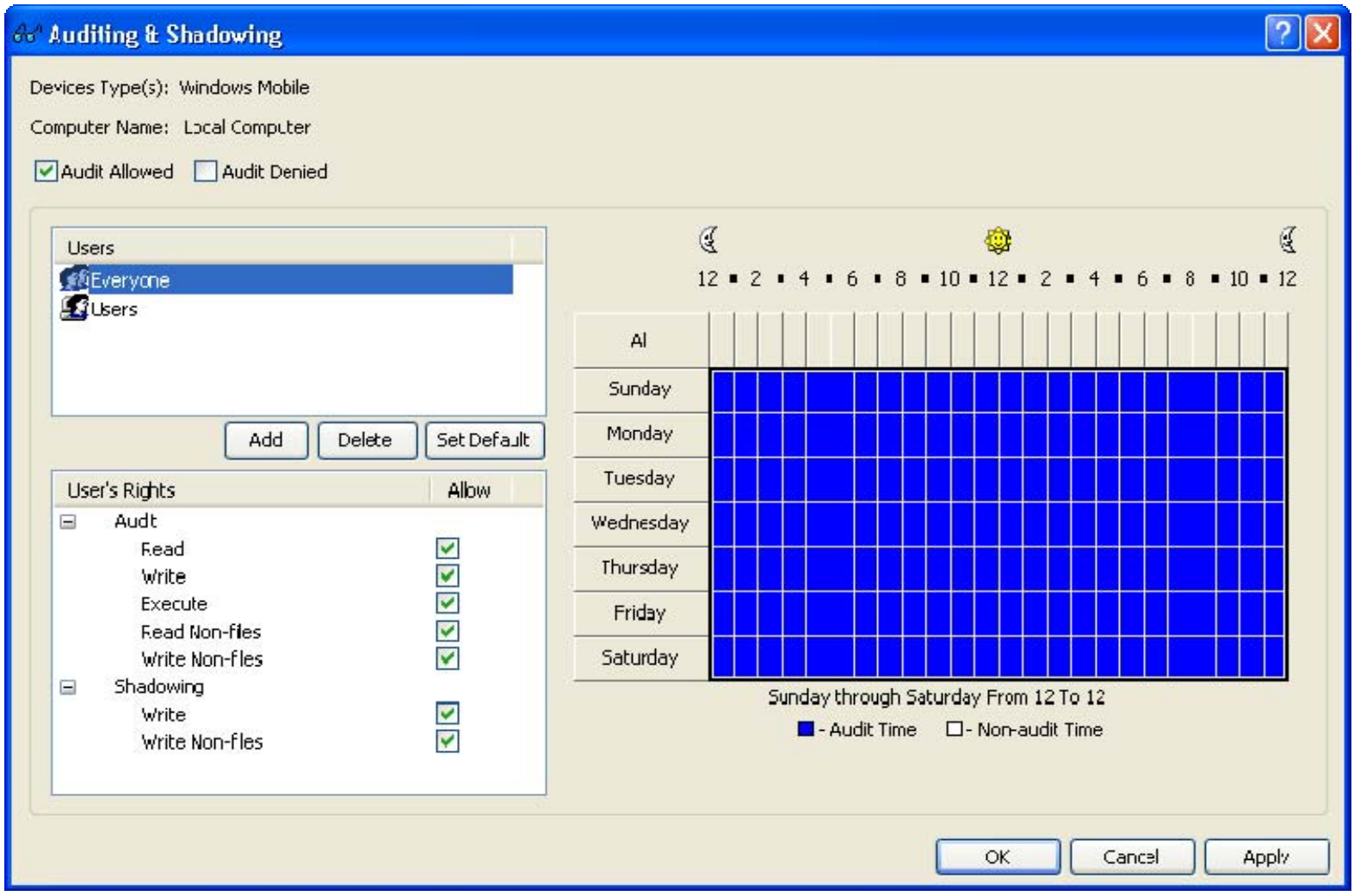
Для просмотра данных аудита, хранимых на DeviceLock Enterprise Server'е, используйте серверный просмотрщик.

Кроме того, существует расширение стандартной функции аудита, называемое теневым копированием – возможность сохранять точную копию данных, копируемых пользователем, на внешние устройства хранения информации и передаваемых через COM и LPT-порты. Сохраняются точные копии всех файлов и данных. Данные теневого копирования сохраняются локально в специальную директорию (см. Service Options) и затем могут быть переданы на DeviceLock Enterprise Server, указанный в настройках Service Options для хранения в SQL-базе данных.

Для просмотра локально сохраненных данных теневого копирования используйте встроенный в DeviceLock Management Console просмотрщик. Чтобы получить дополнительную информацию, обратитесь к разделу **Shadow Log Viewer (для компьютера)** данного руководства.

Для просмотра данных теневого копирования, хранимых на DeviceLock Enterprise Server'е, используйте серверный просмотрщик.

Чтобы задать правила аудита и теневого копирования для типа устройства, выделите его (для одновременного выделения нескольких типов устройств используйте клавиши *Ctrl* и/или *Shift*) и выберите пункт *Set Auditing & Shadowing* из контекстного меню, либо используйте соответствующую кнопку на инструментальной панели.



Для каждого устройства можно протоколировать два типа попыток доступа:

- *Разрешенные* – все попытки доступа, которые были разрешены DeviceLock Service'ом, т.е. пользователю был предоставлен доступ к устройству.

- *Запрещенные* – все попытки доступа, которые были заблокированы DeviceLock Service'ом, т.е. пользователю был запрещен доступ к устройству.

Для того чтобы включить протоколирование одного или обоих типов доступа, установите флаги *Audit Allowed* и/или *Audit Denied*. Эти флаги не имеют логической привязки к отдельным учетным записям пользователей или групп, они влияют на весь тип устройства.

Имена пользователей и групп пользователей, назначенных данному типу устройства, отображаются в списке учетных записей в левой верхней части диалога *Auditing & Shadowing*.

Чтобы добавить нового пользователя или группу пользователей в список учетных записей, нажмите на кнопку *Add*. Вы можете добавить несколько учетных записей одновременно.

Для удаления учетных записей из списка используйте кнопку *Delete*. Используя клавиши *Ctrl* и/или *Shift*, вы можете выбирать и удалять несколько записей одновременно.

Чтобы установить для устройства правила аудита и теневого копирования по умолчанию, необходимо использовать кнопку *Set Default*. Правила по умолчанию заданы следующим образом: права аудита **Read** и **Write** включены для локальной группы *Пользователи* и учетной записи *Все*, а теневое копирование для них отключено.

Используя специальный элемент управления для выбора времени, вы можете задать период, когда правило аудита для выбранного пользователя или группы будет (или не будет) активно. Элемент управления для выбора времени расположен в правом верхнем углу диалога *Auditing & Shadowing*. Используйте левую кнопку мыши для выбора времени, когда правило аудита активно. Для выбора времени, когда правило аудита неактивно, используйте правую кнопку мыши. Вы также можете использовать клавиатуру: стрелки для навигации и пробел для переключения между активным/неактивным состоянием.

Чтобы определить, какие действия пользователя должны быть запротоколированы, установите соответствующие права аудита. Все права разделены на две группы: *Audit* и *Shadowing*. Каждая группа имеет свой собственный набор прав:

- **Audit** – права принадлежащие этой группе отвечают за запись действий пользователей в журнал аудита.

  - **Read** – протоколируются попытки пользователя читать данные. Для типов устройств *Bluetooth*, *FireWire port*, *Infrared port*, *Parallel port*, *Serial port*, *USB port* и *WiFi* вы можете установить это право только в том случае, если установлено право **Write** из группы *Audit*.

  - **Write** – протоколируются попытки пользователя записывать данные. Для типов устройств *Bluetooth*, *FireWire port*, *Infrared port*, *Parallel port*, *Serial port*, *USB port* и *WiFi* вы можете установить это право только в том случае, если установлено право **Read** из группы *Audit*.

  - **Print** – протоколируются попытки пользователя посылать документы на принтеры. Данное право применимо только к типу *Printer*.

  - **Execute** – протоколируются попытки пользователя удаленно выполнить код на стороне устройства. Данное право применимо только к типу *Windows Mobile*.

  - **Read Non-files** – протоколируются попытки пользователя читать не файловые объекты (календарь, контакты, задачи и т.п.). Данное право применимо только к типам *Windows Mobile* и *Palm*.

- **Write Non-files** – протоколируются попытки пользователя записывать не файловые объекты (календарь, контакты, задачи и т.п.). Данное право применимо только к типам *Windows Mobile* и *Palm*.

- **Shadowing** – права принадлежащие этой группе отвечают за запись действий пользователей в журнал теневого копирования.

  - **Write** – включается теневое копирование для всех данных, записываемых пользователетелем. Данное право применимо только к типам устройств *DVD/CD-ROM*, *Floppy*, *Parallel port*, *Removable*, *Serial port*, *Windows Mobile* и *Palm*.

  - **Print** – включается теневое копирование для всех документов посылаемых на принтеры. Позже теневые копии этих документов могут быть просмотрены с помощью DeviceLock Printer Viewer. Данное право применимо только к типу *Printer*.

  - **Write Non-files** – включается теневое копирование для всех не файловых объектов (календарь, контакты, задачи и т.п.), записываемых пользователетелем. Данное право применимо только к типам *Windows Mobile* и *Palm*.

В нижеследующей таблице вы можете увидеть, какие права аудита могут быть назначены тому или иному типу устройств и что при этом будет записано в журнал. DeviceLock Service для всех событий записывает в журнал тип события, дату и время, тип устройства, имя пользователя, информацию о приложении и некоторую другую специфичную для события информацию (описанную в таблице).

Тип Аудита / Тип Устройства	Audit: Read	Audit: Write/Print	Audit: Execute	Audit: Read Non-files	Audit: Write Non-files	Shadowing: Write/Print	Shadowing: Write Non-files
Bluetooth	Событие *Device Access* записывается в журнал аудита	Событие *Device Access* записывается в журнал аудита	-	-	-	-	-
DVD/CD-ROM	События *Open*, *Device Access* и *Direct Access*, имена файлов и флаги (*Read*, *DirectRead*, *Eject*, *DirList*) записываются в журнал аудита	События *Open*, *Device Access* и *Direct Access* и флаги (*Write*, *Del*, *DirectWrite*) записываются в журнал аудита	-	-	-	Образы CD/DVD в формате CUE и/или файлы записываются в журнал теневого копирования	-

Тип Аудита / Тип Устройства	Audit: Read	Audit: Write/Print	Audit: Execute	Audit: Read Non-files	Audit: Write Non-files	Shadowing: Write/Print	Shadowing: Write Non-files
FireWire port	События *Insert*, *Remove* и *Device Access* и имена устройств записываются в журнал аудита	События *Insert*, *Remove* и *Device Access* и имена устройств записываются в журнал аудита	-	-	-	-	-
Floppy	События *Open*, *Mount*, *Unmount* и *Direct Access*, имена файлов и флаги (*Read*, *DirectRead, Eject*, *DirList*) записываются в журнал аудита	События *Direct Access*, *Delete*, *Rename* и *Create new*, имена файлов и флаги (*Write*, *DirectWrite*, *Format*, *Del*, *DirCreate*) записываются в журнал аудита	-	-	-	Файлы записываются в журнал теневого копирования	-
Hard disk	События *Open*, *Mount*, *Unmount* и *Direct Access*, имена файлов и флаги (*Read*, *DirectRead, Eject*, *DirList*) записываются в журнал аудита	События *Direct Access*, *Delete*, *Rename* и *Create new*, имена файлов и флаги (*Write*, *DirectWrite*, *Format*, *Del*, *DirCreate*) записываются в журнал аудита	-	-	-	-	-
Infrared port	Событие *Device Access* записывается в журнал аудита	Событие *Device Access* записывается в журнал аудита	-	-	-	-	-

Тип Аудита / Тип Устройства	Audit: Read	Audit: Write/Print	Audit: Execute	Audit: Read Non-files	Audit: Write Non-files	Shadowing: Write/Print	Shadowing: Write Non-files
Palm	Событие *Read File*, имена файлов и флаг *Sync* записываются в журнал аудита	Событие *Write File*, имена файлов и флаг *Sync* записываются в журнал аудита	-	События *Read Calendar*, *Read Contact*, *Read Expense*, *Read E-mail*, *Read Document*, *Read Memo*, *Read Notepad*, *Read Task* и *Read Media* и имена объектов записываются в журнал аудита	События *Write Calendar*, *Write Contact*, *Write Expense*, *Write E-mail*, *Write Document*, *Write Memo*, *Write Notepad*, *Write Task*, *Write Media* и *Install* и имена объектов записываются в журнал аудита	Файлы записываются в журнал теневого копирования	Все не файловые объекты (календарь, контакты, задачи и т.п.) записываются в журнал теневого копирования
Parallel port	Событие *Device Access* записывается в журнал аудита	Событие *Device Access* записывается в журнал аудита	-	-	-	Все данные, посылаемые в порт, записываются в журнал теневого копирования	-
Printer	-	Событие *Print*, имена документов и принтера записываются в журнал аудита	-	-	-	Все данные, посылаемые на принтер, записываются в журнал теневого копирования в формате спуллера	-
Removable	События *Open*, *Mount*, *Unmount* и *Direct Access*, имена файлов и флаги (*Read*, *DirectRead, Eject*, *DirList*) записываются в журнал аудита	События *Direct Access*, *Delete*, *Rename* и *Create new*, имена файлов и флаги (*Write*, *DirectWrite*, *Format*, *Del*, *DirCreate*) записываются в журнал аудита	-	-	-	Файлы записываются в журнал теневого копирования	-

Тип Аудита / Тип Устройства	Audit: Read	Audit: Write/Print	Audit: Execute	Audit: Read Non-files	Audit: Write Non-files	Shadowing: Write/Print	Shadowing: Write Non-files
Serial port	События *Mount*, *Unmount*, *Insert*, *Remove* и *Device Access* записываются в журнал аудита	События *Mount*, *Unmount*, *Insert*, *Remove* и *Device Access* записываются в журнал аудита	-	-	-	Все данные, посылаемые в порт, записываются в журнал теневого копирования	-
Tape	События *Open*, *Device Access* и *Direct Access* и флаги (*Read*, *DirectRead*) записываются в журнал аудита	События *Open*, *Device Access* и *Direct Access* и флаги (*Write*, *DirectWrite*) записываются в журнал аудита	-	-	-	-	-
USB port	События *Insert*, *Remove* и *Device Access* и имена устройств записываются в журнал аудита	События *Insert*, *Remove* и *Device Access* и имена устройств записываются в журнал аудита	-	-	-	-	-
WiFi	Событие *Device Access* записывается в журнал аудита	Событие *Device Access* записывается в журнал аудита	-	-	-	-	-

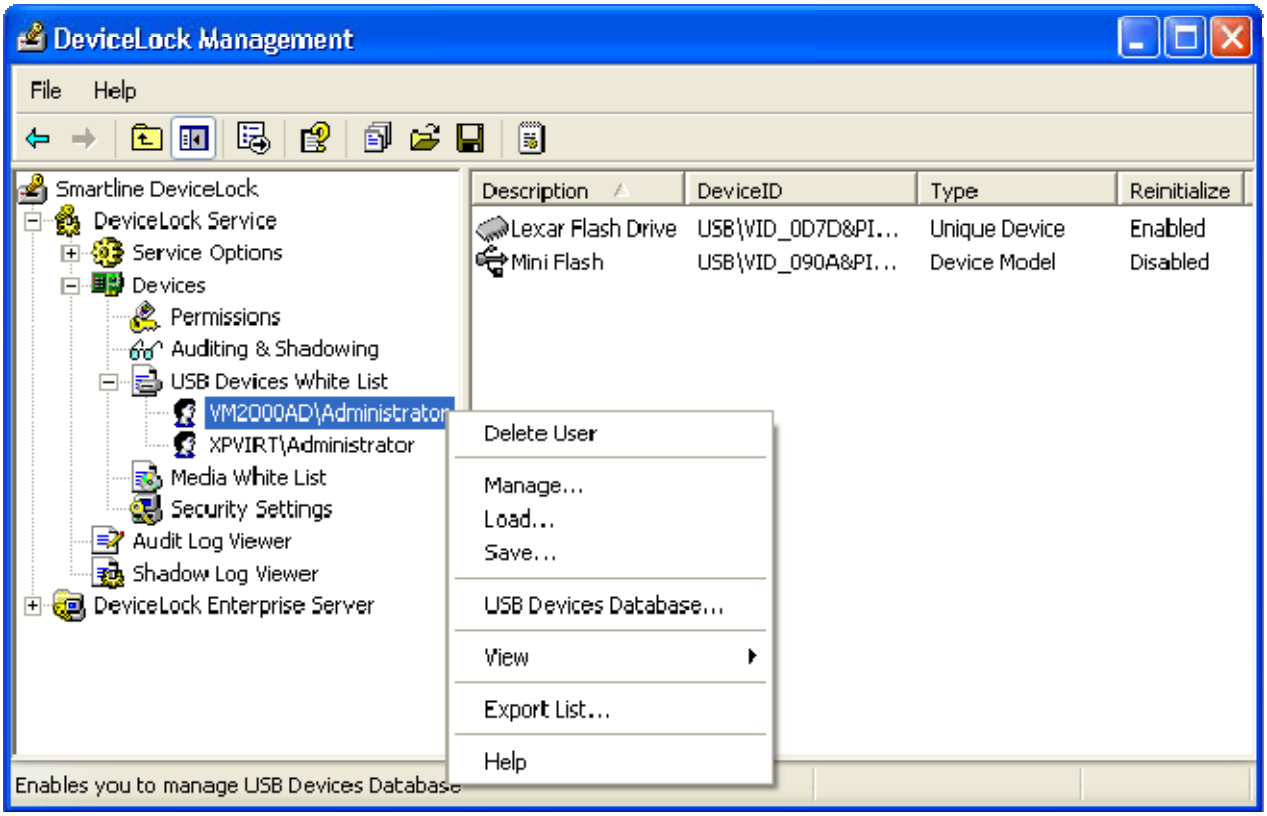
Тип Аудита / Тип Устройства	Audit: Read	Audit: Write/Print	Audit: Execute	Audit: Read Non-files	Audit: Write Non-files	Shadowing: Write/Print	Shadowing: Write Non-files
Windows Mobile	События *Read File*, *Get File Attributes*, *Create New File*, *Overwrite/Create File*, *Open File* и *Open/Create File*, имена файлов и флаги записываются в журнал аудита	События *Write File*, *Delete File*, *Rename File*, *Create File*, *Create New File*, *Overwrite/ Create File*, *Open File*, *Open/Create File*, *Overwrite*, *Set File Attributes*, *Create Shortcut* и *Copy File*, имена файлов и флаги записываются в журнал аудита	События *Invoke* и *Execute*, имена файлов и названия функций (процедур) записываются в журнал аудита	События *Read Calendar*, *Read Contact*, *Read Favorite*, *Read E-mail*, *Read Attachment*, *Read Note*, *Read Task*, *Read Media*, *Read Pocket Access* и *Read Unknown* и имена объектов записываются в журнал аудита	События *Write Calendar*, *Delete Calendar*, *Write Contact*, *Delete Contact*, *Write Favorite*, *Delete Favorite*, *Write E-mail*, *Delete E-Mail*, *Write Attachment*, *Delete Attachment*, *Write Note*, *Delete Note*, *Write Task*, *Delete Task*, *Write Media*, *Delete Media*, *Write Pocket Access*, *Delete Pocket Access*, *Write Unknown* и *Delete Unknown* и имена объектов записываются в журнал аудита	Файлы записываются в журнал теневого копирования	Все не файловые объекты (календарь, контакты, задачи и т.п.) записываются в журнал теневого копирования

ПРИМЕЧАНИЕ: Пока не установлен флаг Audit Allowed или Audit Denied, протоколирование для данного типа устройств в журнал аудита выполняться не будет, несмотря на наличие правил аудита.

Протоколирование в журнал аудита также отключается для устройств, которые находятся в белом списке, а также для целого класса устройств, если контроль доступа к устройствам этого класса выключен в дополнительных настройках безопасности.

5.4.2.3 USB Devices White List

Белый список устройств позволяет разрешать использовать только конкретные устройства, которые не будут заблокированы вне зависимости от остальных установок. Это сделано для того, чтобы разрешить использование отдельных устройств при блокировании всех остальных.



Устройства в белом списке могут быть заданы индивидуально для каждого пользователя и группы.

Чтобы получить дополнительную информацию о том, как работает белый список устройств в DeviceLock, обратитесь к разделу **Управляемый контроль доступа** данного руководства.

Имеется два варианта идентификации устройств в белом списке:

1. **Device Model** – описывает все устройства одной и той же модели. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID) и продукта (PID).

   Комбинация VID и PID описывает конкретную модель, но не конкретное устройство. Это значит, что все устройства данной модели данного производителя будут распознаны как одно устройство.

2. **Unique Device** – описывает конкретное уникальное устройство. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера.

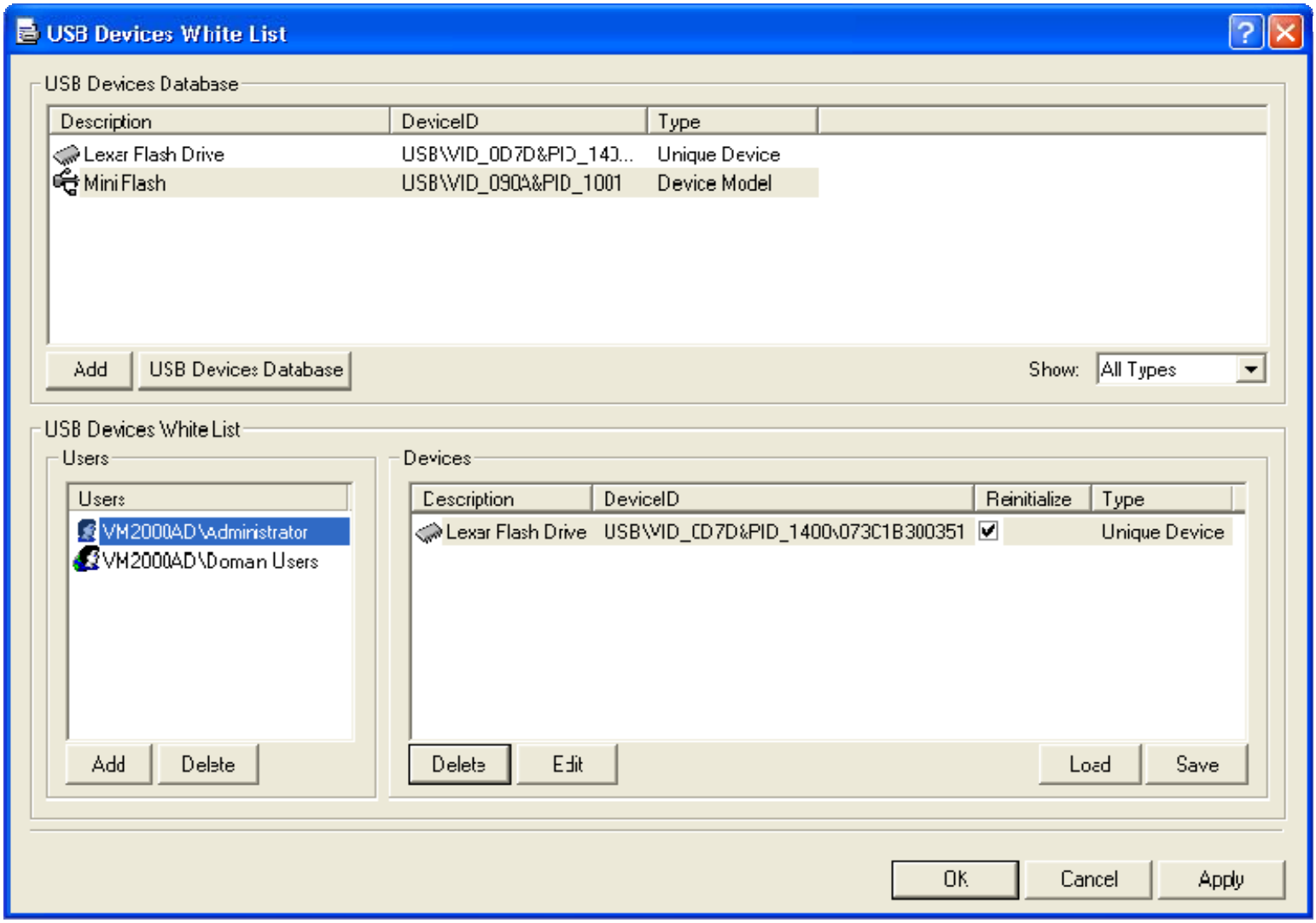
   Не каждое устройство имеет собственный серийный номер. Устройство может быть добавлено в белый список как уникальное устройство только в том случае, если производитель присвоил ему серийный номер на этапе изготовления.

Авторизация устройств в белом списке проходит в два этапа:

1. Добавление устройства в базу данных устройств для того, чтобы сделать возможным его добавление в белый список.

2. Добавление в белый список. В результате устройство становится авторизованным и для него отключается контроль доступа на уровне интерфейса (USB).

Чтобы задать белый список, выберите пункт *Manage* из контекстного меню, либо используйте соответствующую кнопку на инструментальной панели.



В верхней части диалога в списке *USB Devices Database* вы можете видеть устройства, добавленные в базу данных.

Как только устройства добавляются из базы данных в белый список определенного пользователя или группы, они становятся разрешенными и ограничение доступа на них не распространяется, когда этот пользователь входит в систему.

Чтобы добавить устройство в список *USB Devices White List*:

1. Выберите соответствующего пользователя (или группу), для которого это устройство должно быть разрешено.

   Нажмите кнопку *Add* под списком *Users*, чтобы добавить учетную запись. Чтобы удалить учетную запись из списка *Users*, нажмите на *Delete*.

2. Выберите соответствующее устройство в списке *USB Devices Database* и нажмите кнопку *Add*.

   Если устройство имеет серийный номер, оно может быть добавлено в белый список двояко: как модель устройства (**Device Mode**) и как уникальное устройство (**Unique Device**). В этом случае модель устройства имеет приоритет над уникальным устройством.

Когда флаг *Control as Type* включен, контроль доступа к устройствам, добавленным в белый список, отключается только на уровне интерфейса (USB). Если же находящееся в белом списке устройство (например, USB флеш-диск) принадлежит к обоим уровням: интерфейсу (USB) и типу (Removable), то ограничения (если они есть) на уровне типа устройства будут применяться в любом случае.

В противном случае, если флаг *Control as Type* выключен, то контроль доступа к устройствам на уровне типа также отключен. Например, отключив флаг *Control as Type* для USB-диска, вы можете избежать проверки прав доступа на уровне типа Removable.

Если есть необходимость переинициализировать (переподключить) устройство в момент входа пользователя в систему, установите флаг *Reinitialize*.

Некоторые USB-устройства (такие как мышь) не будут работать без переинициализации, поэтому рекомендуется оставить этот флаг включенным для устройств без файловой системы.

Мы рекомендуем снимать флаг *Reinitialize* для устройств с файловой системой (такие как дисководы, CD/DVD-приводы, флеш-диски и т.п.).

Некоторые устройства вообще не могут быть переинициализированы из DeviceLock Service. Это означает, что драйвера этих устройств не поддерживают программное переподключение. Если такое устройство было добавлено в белый список, но доступ к нему не предоставляется, пользователь должен вручную переподключить его.

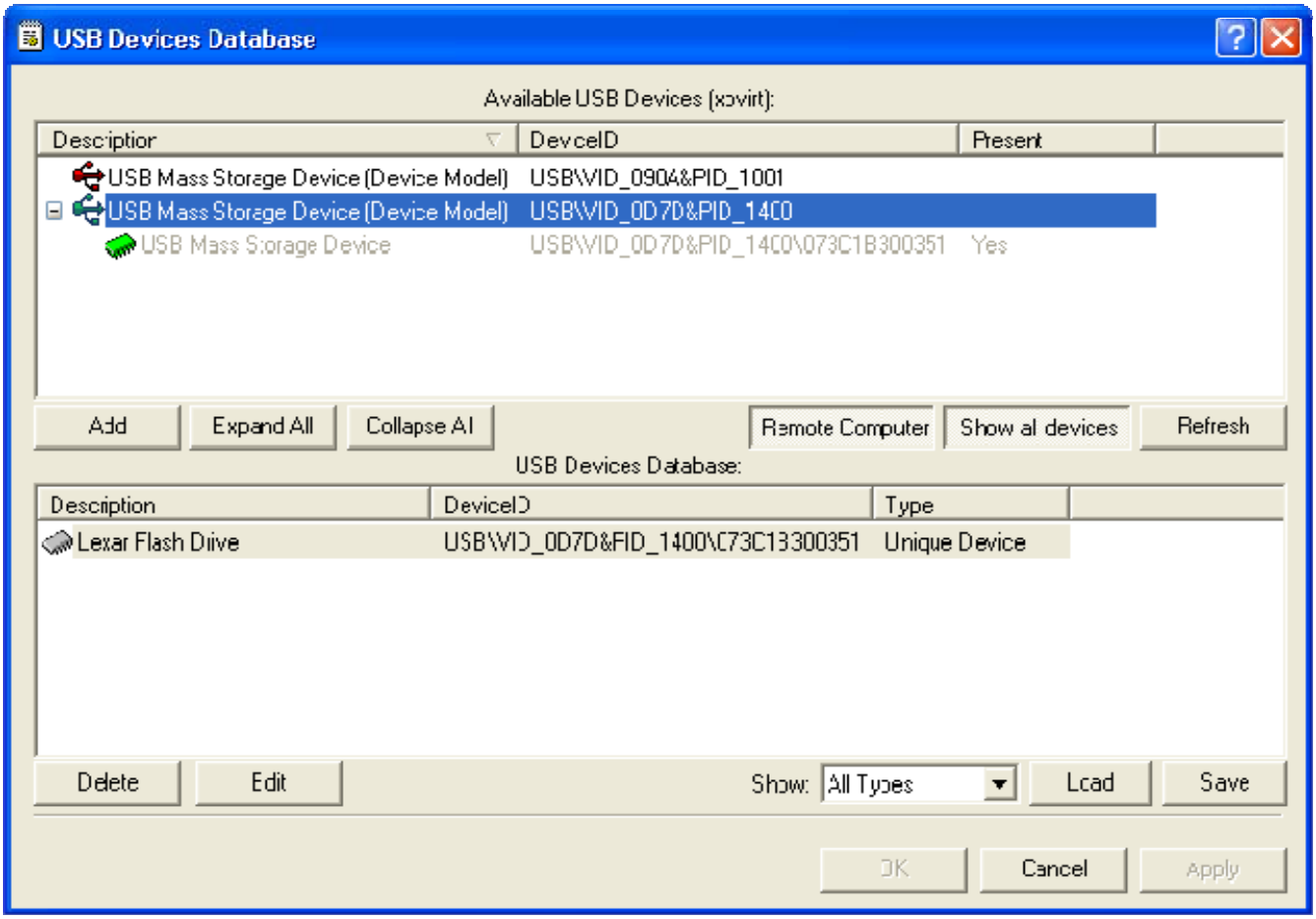
Для редактирования описания устройства выберите соответствующую запись в списке *USB Devices White List* и нажмите кнопку *Edit*. Для удаления записей используйте кнопку *Delete* (для одновременного выбора нескольких записей можно использовать клавиши *Ctrl* и/или *Shift*).

Чтобы сохранить белый список в виде файла, нажмите кнопку *Save* и выберите имя файла. Чтобы загрузить ранее сохраненный белый список, нажмите *Load* и выберите файл со списком устройств.

Для управления базой данных устройств нажмите кнопку *USB Devices Database*.

5.4.2.3.1 База данных устройств

В диалоге *USB Devices Database* вы можете добавлять новые устройства и редактировать записи существующих устройств.



Перед тем как устройство может быть авторизовано через белый список, оно должно быть добавлено в базу данных.

Вверху диалога находится список *Available USB Devices.* В нем отображаются все устройства, доступные на компьютере.

Устройства отображаются в виде простого дерева, в котором родительская запись представляет модель устройства (**Device Model**), а потомок – уникальное устройство (**Unique Device**). Если запись для уникального устройства отсутствует, то это устройство не имеет серийного номера.

Данный список показывает как подключенные на данный момент устройства (если не нажата кнопка *Show all devices),* так и те, которые когда-либо были подключены (если кнопка *Show all devices* нажата).

Консоль управления автоматически обновляет список доступных устройств и показывает новые устройства при их подключении. Чтобы обновить список вручную, нажмите кнопку *Refresh*.

Чтобы получить список устройств с удаленного компьютера, нажмите кнопку *Remote Computer*. Это кнопка недоступна, когда вы подключены к локальному компьютеру.

В списке *USB Devices Database,* расположенном внизу диалога, вы можете видеть устройства, которые уже имеются в базе данных.

Вы можете добавлять устройства в этот список, выбирая соответствующие записи в списке *Available USB Devices* и нажимая кнопку *Add*. Повторное добавление одного и того же устройства невозможно.

Для редактирования описания устройства выберите соответствующую запись в списке *USB Devices Database* и нажмите кнопку *Edit*.

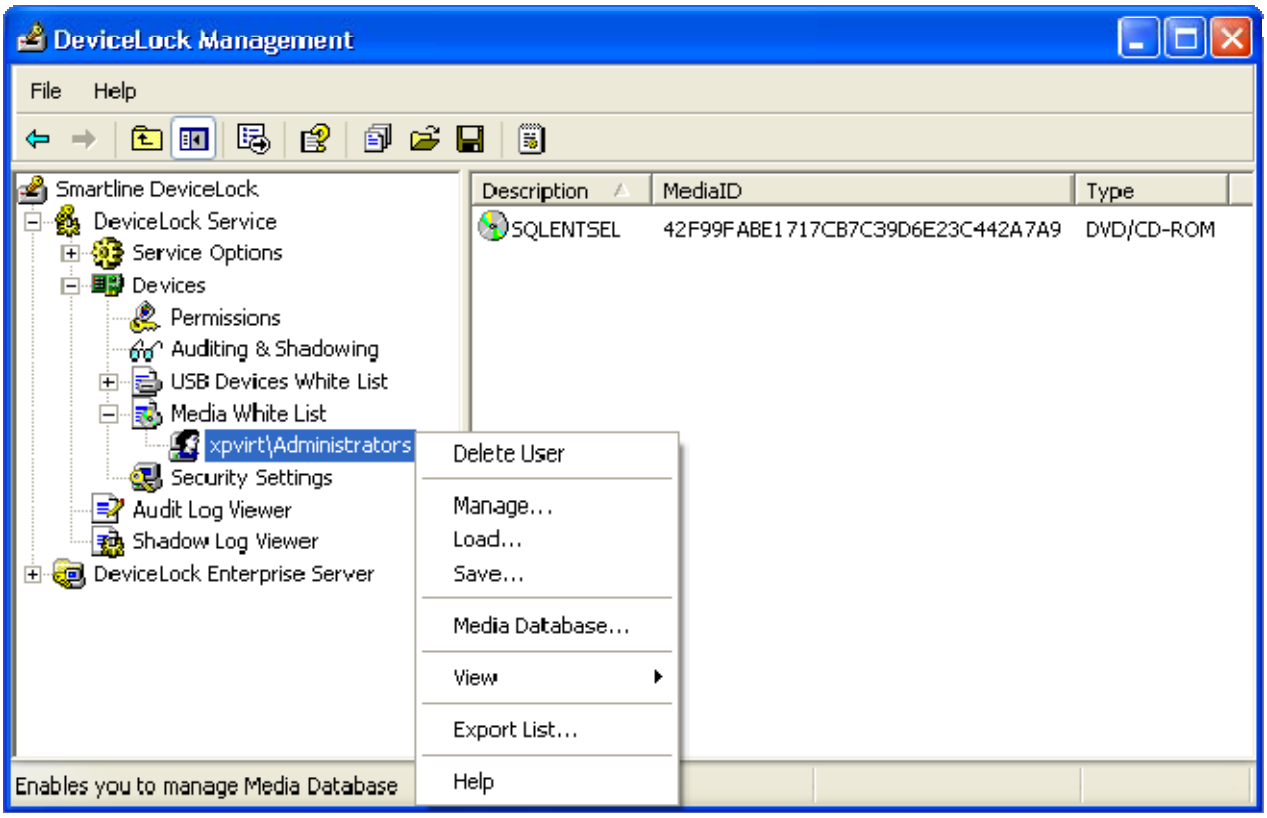
Для удаления записей используйте кнопку *Delete* (для одновременного выбора нескольких записей можно использовать клавиши *Ctrl* и/или *Shift*).

База данных устройств может быть сохранена в виде файла. Для этого нажмите кнопку *Save* и выберите формат файла – .txt или .csv .

Чтобы загрузить ранее сохраненную базу данных, нажмите кнопку *Load* и выберите файл со списком устройств.

5.4.2.4 Media White List

Белый список носителей позволяет идентифицировать определенный CD/DVD-диск на основе записанных на него данных и разрешить его использование, даже если сам CD/DVD-привод заблокирован.



Любое изменение в авторизованных данных приведет к изменению уникального идентификатора носителя, и носитель перестанет распознаваться как авторизованный.

Если авторизованный носитель был скопирован без изменений (побайтовое копирование), то копия также будет авторизованной.

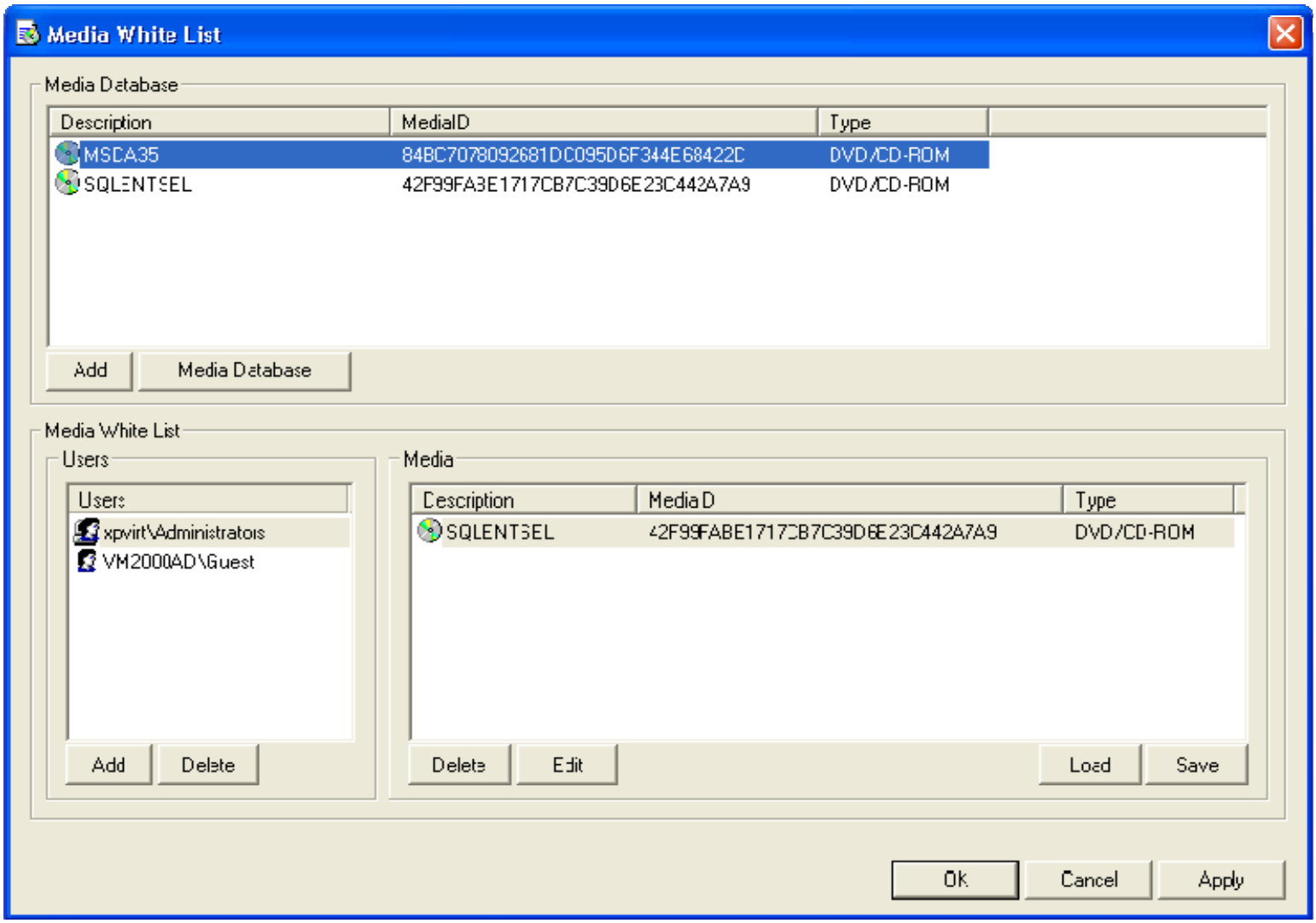
ПРИМЕЧАНИЕ: Доступ к носителям, включенным в белый список, может быть открыт только на уровне типа (DVD/CD-ROM). Если же CD/DVD-привод подключается к порту (USB или FireWire) и доступ к этому порту заблокирован, доступ к носителю будет также заблокирован.

Чтобы авторизовать носитель надо:

1. Добавить носитель в базу данных носителей для того, чтобы сделать возможным его добавление в белый список.

2. Добавить носитель в белый список, после чего этот носитель становится авторизованным и к нему предоставляется доступ на чтение на уровне типа (DVD/CD-ROM).

Чтобы задать белый список, выберите пункт *Manage* из контекстного меню, либо используйте соответствующую кнопку на инструментальной панели.



В верхней части диалога в списке *Media Database* вы можете видеть носители, добавленные в базу данных.

Как только носители добавляются из базы данных в белый список определенного пользователя или группы, они становятся разрешенными и ограничение доступа на них не распространяется, когда этот пользователь входит в систему.

Чтобы добавить носитель в список *Media White List*:

1. Выберите соответствующего пользователя (или группу), для которого этот носитель должен быть разрешен.

   Нажмите кнопку *Add* под списком *Users*, чтобы добавить учетную запись. Чтобы удалить учетную запись из списка *Users*, нажмите на *Delete*.

2. Выберите соответствующий носитель в списке *Media Database* и нажмите кнопку *Add*.

Для редактирования описания носителя выберите соответствующую запись в списке *Media White List* и нажмите кнопку *Edit*.

Для удаления записей используйте кнопку *Delete* (для одновременного выбора нескольких записей можно использовать клавиши *Ctrl* и/или *Shift*).

Чтобы сохранить белый список в виде файла, нажмите кнопку *Save* и выберите имя файла.

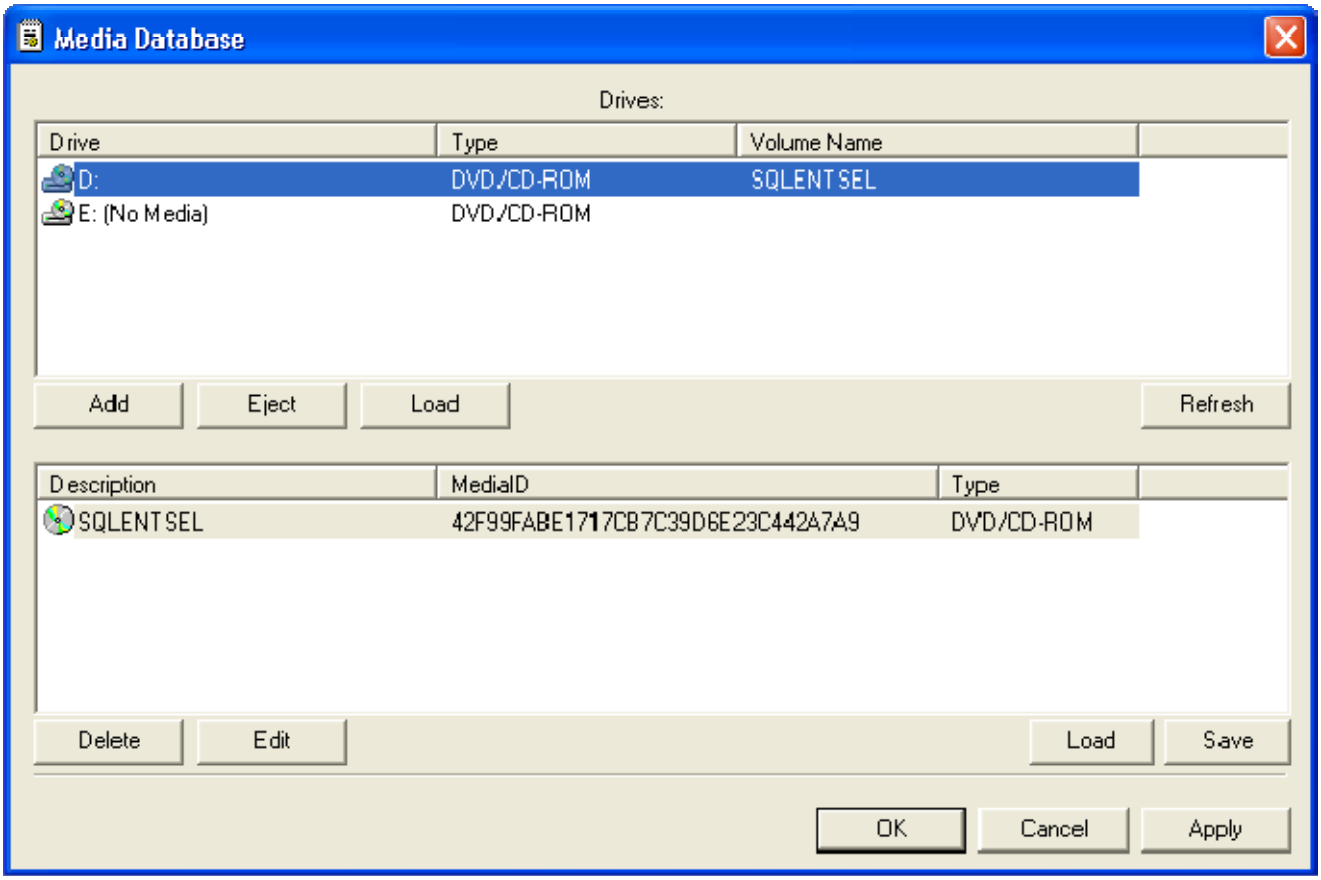
Чтобы загрузить ранее сохраненный белый список, нажмите *Load* и выберите файл со списком носителей.

Для управления базой данных носителей нажмите кнопку *Media Database*.

ПРИМЕЧАНИЕ: Используя белый список носителей, пользователю возможно предоставить доступ только на чтение данных. Невозможно авторизовать носитель для записи.

5.4.2.4.1 База данных носителей

В диалоге *Media Database* вы можете добавлять новые носители и редактировать записи существующих носителей.



Перед тем как носитель может быть авторизован через белый список, он должен быть добавлен в базу данных.

В верхней части диалога находится список *Drives.* В нем отображены все устройства локального компьютера, которые могут содержать носители.

Консоль управления автоматически обновляет список доступных носителей и показывает новые носители по мере их появления в устройствах. Чтобы обновить список вручную, нажмите кнопку *Refresh*.

В списке, расположенном в нижней части диалога, отображаются носители, которые уже имеются в базе данных.

Вы можете добавлять носители в этот список, выбирая соответствующие записи в списке *Drives* и нажимая кнопку *Add*. Авторизация носителя занимает некоторое время, в зависимости от объема данных, записанных на нем. Повторное добавление одного и того же носителя невозможно.

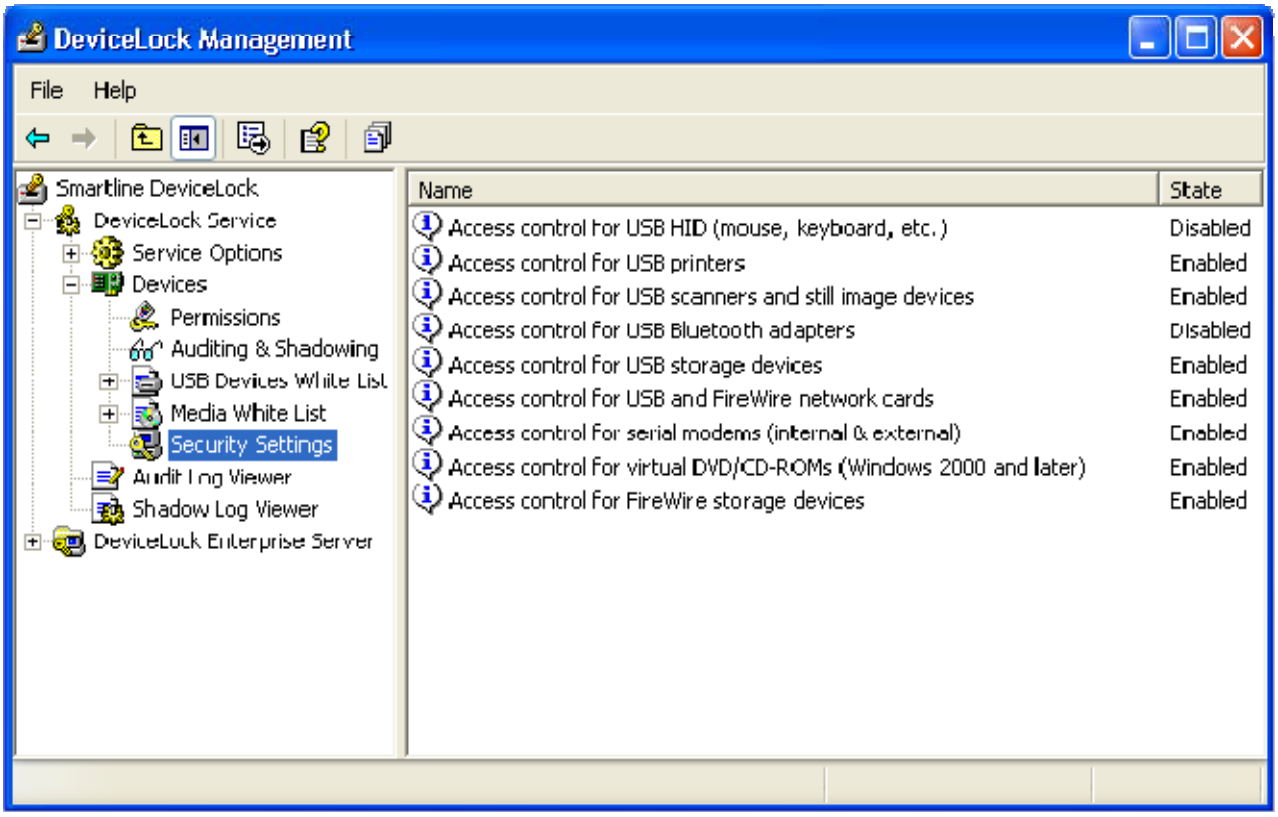
Для редактирования описания носителя выберите соответствующую запись в списке и нажмите кнопку *Edit*.

Для удаления записей используйте кнопку *Delete* (для одновременного выбора нескольких записей можно использовать клавиши *Ctrl* и/или *Shift*).

База данных носителей может быть сохранена в виде файла. Для этого нажмите кнопку *Save* и выберите формат файла – .txt или .csv . Чтобы загрузить ранее сохраненную базу данных, нажмите кнопку *Load* и выберите файл со списком носителей.

5.4.2.5 Security Settings

Эти дополнительные настройки безопасности влияют на установленные разрешения и правила аудита для некоторых типов устройств.



Дополнительные настройки безопасности дают возможность полностью блокировать определенные типы устройств, но разрешить использование отдельных классов устройств.

Например, вы можете полностью закрыть доступ к USB-порту, но разрешить использование любых мышей и клавиатур с USB-интерфейсом.

DeviceLock поддерживает заранее предопределенные классы устройств для дополнительных настроек безопасности:

- *Access control for USB HID* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к устройствам ввода (клавиатура, мышь), подключенным к USB-портам. Если флаг снят, то эти устройства продолжат работу в обычном режиме и аудит для них также будет отключен.

- *Access control for USB printers* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к принтерам, подключенным к USB-портам. Если флаг снят, то даже при заблокированном USB-порте принтеры будут работать в обычном режиме и аудит для них также будет отключен.

- *Access control for USB scanners and still image devices* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к сканерам и цифровым фотоаппаратам, подключенным к USB-портам. Если флаг снят, то даже при заблокированном USB-порте эти устройства будут работать в обычном режиме и аудит для них также будет отключен.

- *Access control for USB Bluetooth adapters* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к Bluetooth-адаптерам, подключенным к USB-портам. Если флаг снят, то даже при заблокированном USB-порте Bluetooth-адаптеры будут работать в обычном режиме и аудит для них также будет отключен.

  Этот флаг влияет только на контроль доступа и аудит на уровне интерфейса (USB). Если устройство принадлежит к обоим уровням, контроль доступа и аудит для уровня типа (Bluetooth) будут выполняться в любом случае.

- *Access control for USB storage devices* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к устройствам хранения данных (таким как флеш-диски), подключенным к USB-портам. Если флаг снят, то даже при заблокированном USB-порте эти устройства будут работать в обычном режиме и аудит для них также будет отключен.

  Этот флаг влияет только на контроль доступа и аудит на уровне интерфейса (USB). Если устройство принадлежит к обоим уровням, контроль доступа и аудит для уровня типа (Removable, Floppy, DVD/CD-ROM или Hard disk) будут выполняться в любом случае.

- *Access control for USB and FireWire network cards* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к сетевым картам, подключенным к USB или FireWire-портам. Если флаг снят, то даже при заблокированном USB/FireWire-порте эти устройства будут работать в обычном режиме и аудит для них также будет отключен.

- *Access control for FireWire storage devices* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к устройствам хранения данных, подключенным к FireWire-портам. Если флаг снят, то даже при заблокированном FireWire-порте эти устройства будут работать в обычном режиме и аудит для них также будет отключен.

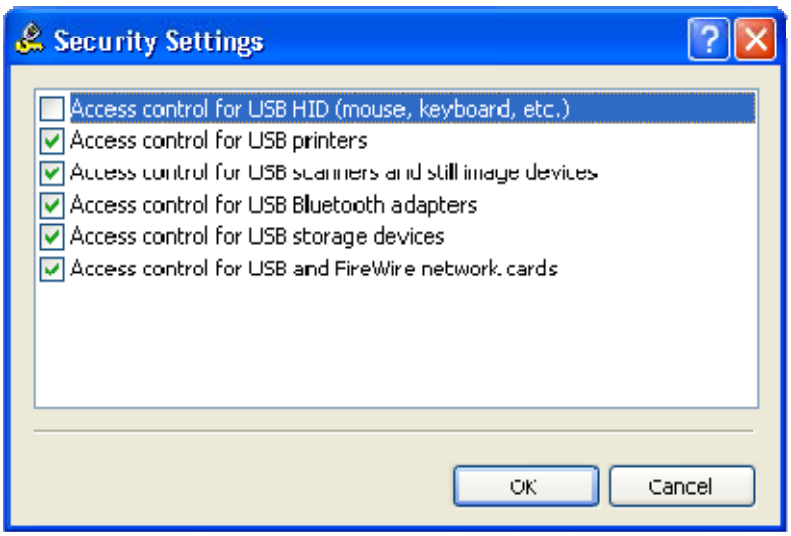
  Этот флаг влияет только на контроль доступа и аудит на уровне интерфейса (FireWire). Если устройство принадлежит к обоим уровням, контроль доступа и аудит для уровня типа (Removable, Floppy, DVD/CD-ROM или Hard disk) будут выполняться в любом случае.

- *Access control for serial modems (internal & external)* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к модемам, подключенным к COM-портам. Если флаг снят, то даже при заблокированном COM-порте эти устройства будут работать в обычном режиме и аудит для них также будет отключен.

- *Access control for virtual CD-ROMs* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать доступ к виртуальным CD/DVD-приводам. Если флаг снят, то даже при заблокированном DVD/CD-ROM виртуальные диски будут работать в обычном режиме и аудит для них также будет отключен. Этот флаг имеет силу только для ОС начиная с Windows 2000.

- *Access control for virtual printers* – если флаг установлен, то DeviceLock Service может контролировать и протоколировать отправку документов на виртуальные принтеры, т.е. принтеры, которые печатают не на реальном физическом устройстве, а, например, перенаправляют печать в файл. Если флаг снят, то даже при заблокированном физическом принтере виртуальные принтеры будут печатать как обычно, и аудит для них также будет отключен. Этот флаг имеет силу только для ОС начиная с Windows 2000.

Чтобы установить или снять один из этих флагов, два раза кликните мышкой на соответствующей записи. Также вы можете выбрать пункт *Manage* из контекстного меню или нажать на соответствующую кнопку на инструментальной панели.



Дополнительные настройки безопасности подобны белому списку устройств, но имеют три важных отличия:

1. Используя настройки безопасности, вы можете разрешить использование целого класса устройств; но вы не можете разрешить использование только одной конкретной модели, пока все остальные устройства этого же класса являются заблокированными.

2. Используя настройки безопасности, вы можете выбрать устройство только из списка предопределенных классов. Если устройство не принадлежит ни одному из предопределенных классов, оно не может быть разрешено через настройки безопасности.

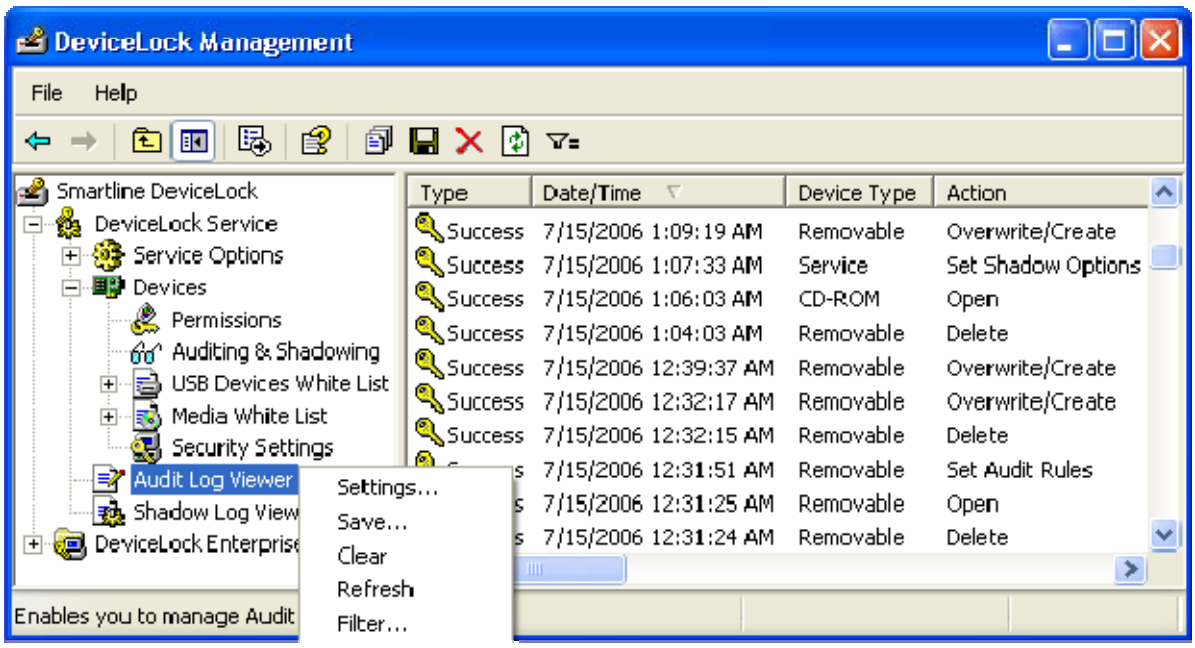
3. Используя настройки безопасности, вы не можете контролировать доступ к устройствам для пользователей или групп. Настройки безопасности влияют сразу на всех пользователей локального компьютера.

ПРИМЕЧАНИЕ: Дополнительные настройки безопасности гарантированно работают только для устройств, управляемых стандартными драйверами Windows. Некоторые устройства, использующие драйвера сторонних производителей, не могут быть отнесены DeviceLock Service к тому или иному классу. Такие устройства рекомендуется авторизовывать индивидуально с помощью белого списка.

5.4.3 Audit Log Viewer (для компьютера)

Консоль управления содержит встроенный просмотрщик записей аудита, который позволяет просматривать данные аудита из стандартного журнала Windows подключенного компьютера.

Стандартный журнал Windows используется для хранения записей аудита, только если параметр *Audit log type* в Service Options установлен в значение *Event Log* или *Event & DeviceLock Logs*. В противном случае, записи аудита хранятся в специальном журнале и могут быть просмотрены с помощью серверного просмотрщика.



Журнал аудита используется для хранения записей протокола доступа (событий) пользователей к устройствам, подпавшим под заданные правила аудита. Чтобы получить дополнительную информацию, обратитесь к разделу **Auditing & Shadowing** данного руководства.

В журнал аудита также записываются все изменения в настройках DeviceLock Service, если соответствующий флаг установлен в Service Options.

Информация из журнала аудита отображается в виде таблицы, столбцы которой определены следующим образом:

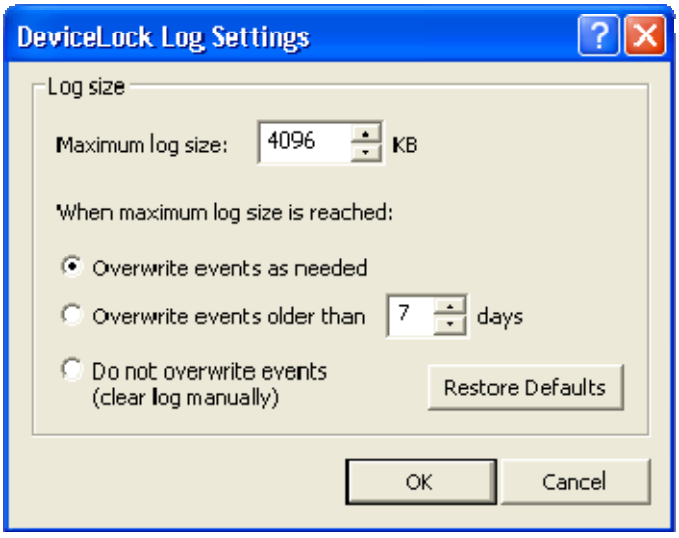
- *Type* – тип попытки доступа (*Success* для разрешенной попытки, либо *Failure* для запрещенной попытки).
- *Date/Time* – дата и время, когда событие было получено DeviceLock Service.
- *Device Type* – тип устройства.
- *Action* – тип действия пользователя.
- *Name* – название объекта (файла, устройства и т.п.).
- *Information* – иная, специфичная для данного устройства информация о событии, такая как флаги доступа и т.п.
- *User* – имя пользователя, связанное с событием.
- *PID* – идентификатор процесса приложения, связанного с событием.
- *Process* – полный путь к исполняемому файлу приложения. В некоторых случаях вместо полного пути может быть показано только имя процесса.

Чтобы обновить список событий, используйте *Refresh* из контекстного меню или соответствующую кнопку на инструментальной панели.

Чтобы полностью очистить журнал аудита, используйте *Clear* из контекстного меню или соответствующую кнопку на инструментальной панели.

5.4.3.1 Настройки журнала аудита (для компьютера)

Чтобы определить максимальный размер журнала аудита и действия Windows в случае его заполнения, используйте *Settings* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Audit Log Viewer* или соответствующую кнопку на инструментальной панели.



В параметре *Maximum log size* вы можете указать максимальный размер журнала (в килобайтах). Файл журнала находится в директории *%SystemRoot%\system32\config* и имеет имя *DeviceLo.evt*.

Чтобы определить действия Windows в случае заполнения журнала аудита, выберите одну из этих опций:

- *Overwrite events as needed* – ОС перезаписывает старые записи новыми, когда превышается размер, заданный в параметре *Maximum log size*.

- *Overwrite events older than* – ОС перезаписывает только те записи, которые старше заданного количества дней.

- *Do not overwrite events (clear log manually)* – ОС вообще не перезаписывает записи, когда превышается размер, заданный в параметре *Maximum log size,* и в таком случае вам необходимо очищать журнал вручную.

ПРИМЕЧАНИЕ: Когда журнал аудита заполнен и в нем нет записей, которые можно было бы удалить, DeviceLock Service не может писать новые записи в такой журнал.

Если вы хотите сбросить текущие настройки, используйте кнопку *Restore Defaults*. Настройки по умолчанию выглядят следующим образом:

- Параметр *Maximum log size* равен 512-ти килобайтам.

- Выбрана опция *Overwrite events older than* и для нее установлено значение 7 дней.

5.4.3.2 Фильтр журнала аудита (для компьютера)

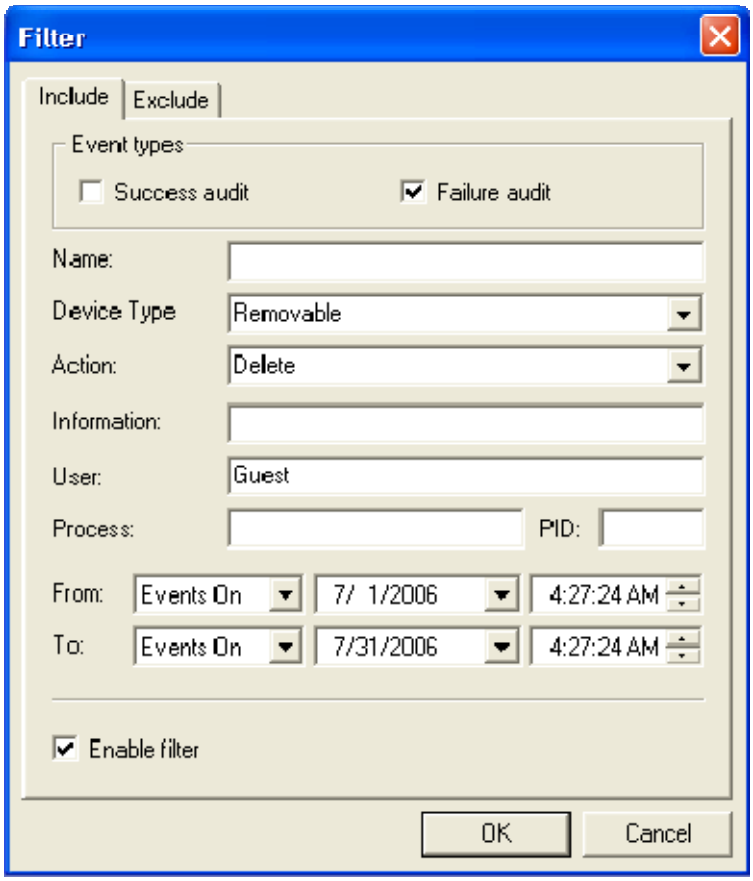
Вы можете фильтровать данные в Audit Log Viewer так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список.

Чтобы открыть диалог *Filter*, используйте *Filter* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Audit Log Viewer* или соответствующую кнопку на инструментальной панели.

Существует два типа фильтров:

- **Включающие** – в списке отображаются только записи, удовлетворяющие условиям, заданным на вкладке *Include*.

- **Исключающие** – в списке не отображаются записи, удовлетворяющие условиям, заданным на вкладке *Exclude*.



Чтобы использовать любой тип фильтра, вы должны сначала включить его.

Установите флаг *Enable filter*, чтобы включить фильтр.

Чтобы временно выключить фильтр, снимите флаг *Enable filter*.

Когда фильтр включен, вы можете определить условия фильтрации, задав необходимые значения в следующих полях:

- *Success audit* – флаг, определяющий нужно ли фильтровать записи по успешным попыткам доступа.

- *Failure audit* – флаг, определяющий нужно ли фильтровать записи по запрещенным попыткам доступа.

- *Name* – текст, соответствующий значению столбца *Name* в Audit Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Device Type* – текст, соответствующий значению столбца *Device Type* в Audit Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Action* – текст, соответствующий значению столбца *Action* в Audit Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Information* – текст, соответствующий значению столбца *Information* в Audit Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *User* – текст, соответствующий значению столбца *User* в Audit Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Process* – текст, соответствующий значению столбца *Process* в Audit Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *PID* – число, соответствующее значению столбца *PID* в Audit Log Viewer.

- *From* – определяет начало временного интервала событий, которые вы хотите фильтровать. Выберите *First Event,* чтобы фильтровать события, начиная с самого первого в журнале. Выберите *Events On*, чтобы фильтровать события, начиная с определенной даты и времени.

- *To* – определяет конец временного интервала событий, которые вы хотите фильтровать. Выберите *Last Event*, чтобы фильтровать события, заканчивая самым последним событием в журнале. Выберите *Events On,* чтобы фильтровать события, заканчивая событием с определенной датой и временем.

Логика “И” применяется для всех заданных полей и между активными фильтрами. Это означает, что результатом фильтрации станут только те записи, которые соответствуют всем заданным условиям.

Если вы не хотите включать какое-либо поле в результат фильтрации, просто оставьте это поле пустым.

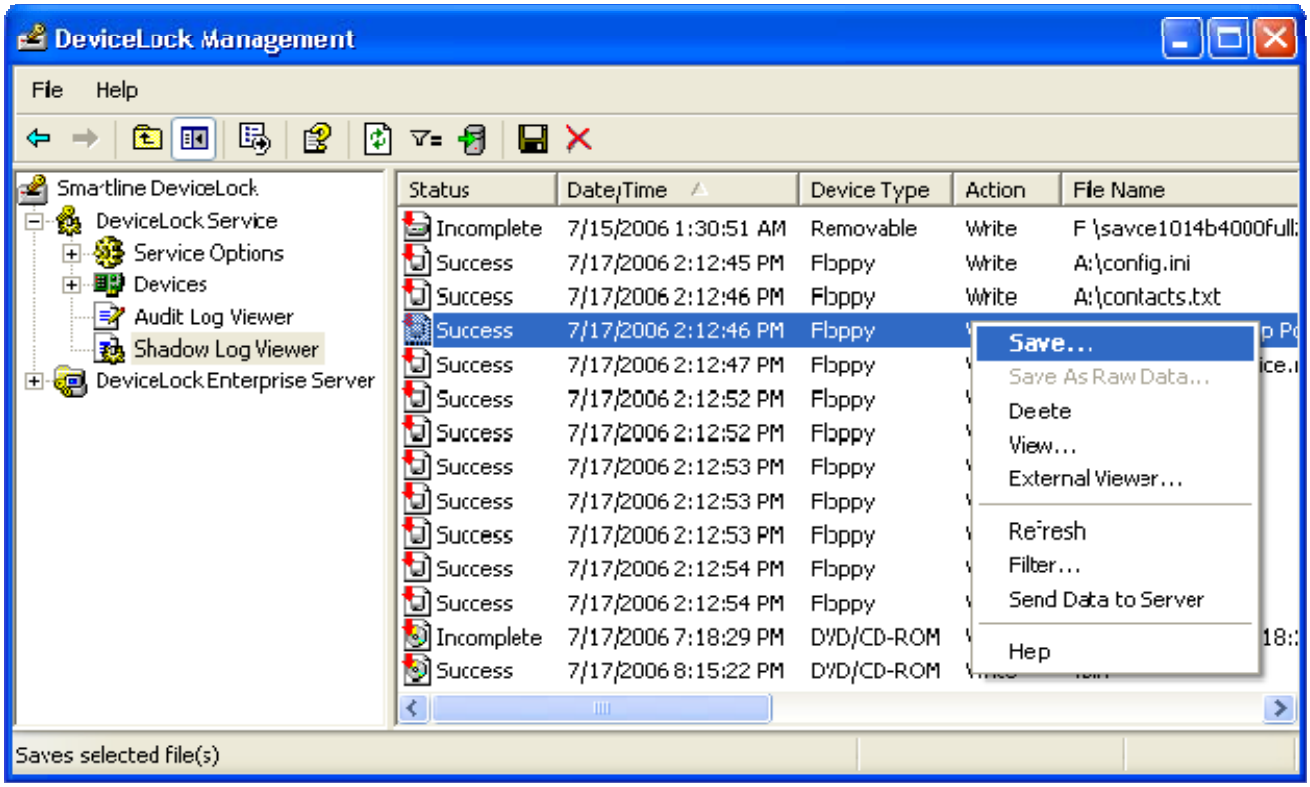
Для некоторых полей вы можете использовать маски. Маска представляет из себя набор специальных символов, таких как звездочка (*) и вопросительный знак (?), и частей слов. Специальные символы используются для обозначения одного или нескольких неизвестных символов.

Используйте звездочку как замену нескольким неизвестным символам. Например, если вы ищете все слова, начинающиеся на "*win*", но вы не знаете остальную часть слова, используйте маску *win**. Под эту маску попадут все слова, начинающиеся с "*win*", включая *Windows*, *Winner* и *Wind*.

Используйте вопросительный знак как замену одному неизвестному символу. Например, если вы используйте маску *win?*, то под нее попадет только слово *Wind*, но не слова *Windows* или *Winner*.

5.4.4 Shadow Log Viewer (для компьютера)

Консоль управления содержит встроенный просмотрщик локально сохраненных данных теневого копирования, который позволяет просматривать данные для подключенного компьютера.



Типичная конфигурация DeviceLock подразумевает, что данные теневого копирования хранятся на DeviceLock Enterprise Server. В этом случае данные теневого копирования, которые изначально были получены и закэшированы DeviceLock Service на локальном компьютере, периодически перемещаются на сервер. При этом локальная копия данных теневого копирования удаляется, как только перемещение на сервер успешно завершается. Поэтому для просмотра данных теневого копирования хранимых на DeviceLock Enterprise Server, используйте серверный просмотрщик.

Тем не менее, в некоторых случаях вам может быть необходимо просмотреть данные теневого копирования, хранящиеся на конкретном компьютере. Например, если вы не используете DeviceLock Enterprise Server вообще или используете его, но по каким-то причинам некоторые данные все еще не были перемещены на сервер с компьютеров пользователей.

Столбцы просмотрщика определены следующим образом:

- *Status* – состояние данных (*Success* для успешно запротоколированных данных, либо *Incomplete* для данных, которые возможно были запротоколированы не полностью).
- *Date/Time* – дата и время, когда данные были переданы.
- *Device Type* – тип устройства.
- *Action* – действие пользователя.
- *File Name* – оригинальное имя файла либо автоматически созданное имя для данных, которые изначально не были представлены в виде файла (такие как CD/DVD-образ, данные записанные напрямую на носитель или переданные через COM или LPT-порт)
- *File Size* – размер данных.
- *User* – имя пользователя, передавшего данные.
- *PID* – идентификатор процесса приложения, использовавшегося для передачи данных.
- *Process* – полный путь к исполняемому файлу приложения. В некоторых случаях вместо полного пути может быть показано только имя процесса.

Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши на каждой записи.

a. Open

Чтобы открыть файл из выбранной записи в проассоциированном приложении, используйте *Open* из контекстного меню. Если для этого типа файлов нет проассоциированного приложения, то откроется диалог 'Открыть с помощью'. В случае, когда запись не имеет данных (размер данных равен 0 или данные не были запротоколированы), *Open* не доступно.

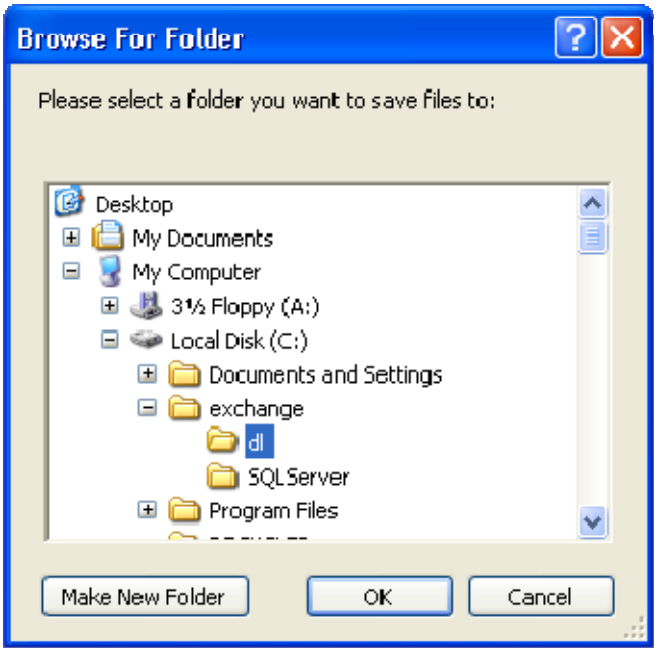
Если вы используете *Open* для данных теневого копирования, полученных от типов устройств *Printer* или *Parallel port*, то проассоциированным приложением всегда будет встроенный просмотрщик, называющийся DeviceLock Printer Viewer.

DeviceLock Printer Viewer может отображать данные теневого копирования принтеров в формате спулера, распечатывать их опять или сохранять во внешний файл (формата BMP, GIF, JPEG, PNG, EMF или TIFF). Для отображения

поддерживаются следующие форматы спулера: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, GDI printing (ZjStream) и EMF Spooled Files.

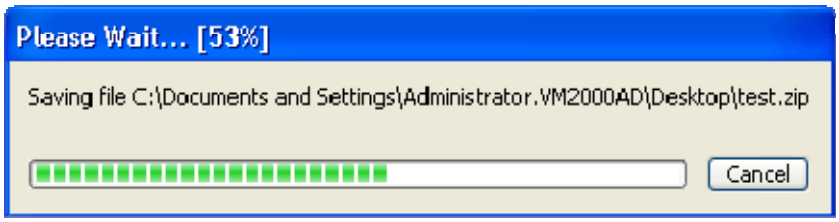
б. Save

Если вам необходимо сохранить данные из выбранной записи на локальный компьютер, используйте *Save* из контекстного меню или соответствующую кнопку на инструментальной панели. Используя клавиши *Ctrl* и/или *Shift,* вы можете сохранить данные из нескольких записей одновременно.



В случае, когда запись не имеет данных (размер данных равен 0 или данные не были запротоколированы), *Save* не доступно ни в контекстном меню, ни на инструментальной панели.

Индикатор выполнения появляется, когда вы сохраняете большой файл.



Вы можете нажать на кнопку *Cancel*, чтобы прервать сохранение. В этом случае результирующий файл, который вы получите на локальном компьютере, будет неполным, он будет содержать только те данные, которые были получены до того момента, как вы прервали процесс сохранения.

Данные, которые были переданы пользователем в виде файла, сохраняются в журнале теневого копирования как файл и могут быть сохранены на локальный компьютер тоже как файл.

Когда пользователь записывает данные на CD/DVD-диск, все данные сохраняются в журнале теневого копирования в виде одного образа (один образ на каждый записанный CD/DVD-диск или сессию) в формате CUE.

CD/DVD-образы, а также другие данные, которые изначально не были представлены в виде файлов, показываются в журнале теневого копирования с автоматически созданными именами. Такие имена создаются на основе действия пользователя, имени диска или устройства и даты/времени (например, *direct_write(E:) 19:18:29 17.07.2006.bin*).

Каждый CD/DVD-образ сохраняется на локальном компьютере в виде двух файлов: файла данных (например, *direct_write(E_) 19_18_29 17_07_2006.bin*) и файла с расширением *.cue*, который имеет то же имя, что и файл данных (например, *direct_write(E_) 19_18_29 17_07_2006_bin.cue*). Оба этих файла необходимы для открытия CD/DVD-образа в программах, которые поддерживают формат CUE (такие как Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO и т.п.)

в. Save As Raw Data

Когда вы выбираете запись, которая содержит данные, записанные как дополнительная сессия к уже существующему CD/DVD-диску, в контекстном меню доступен пункт *Save As Raw Data*. Эта функция позволяет сохранить данные на локальный компьютер “как есть”, без внесения в них каких-либо изменений в процессе сохранения.

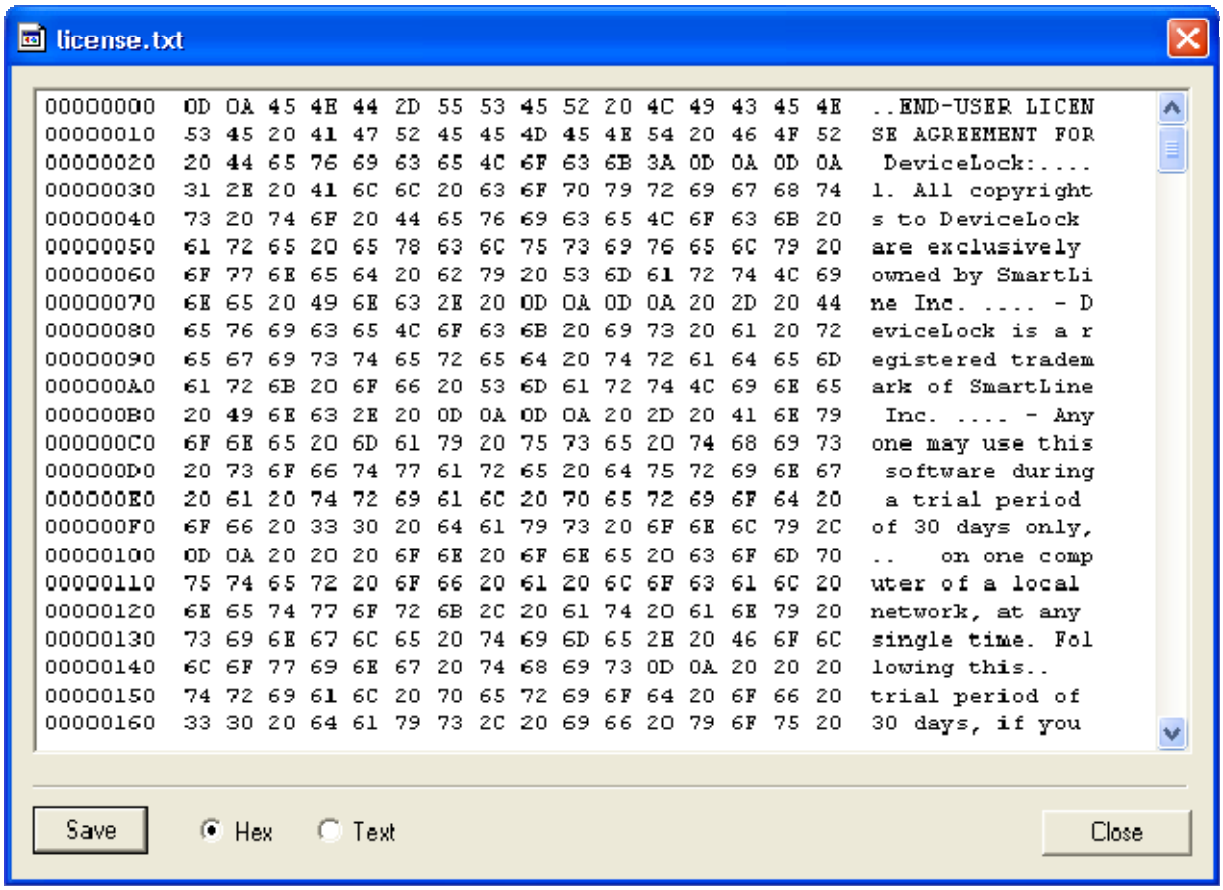
Если вы используете обычную функцию сохранения (см. выше), консоль управления может обнаружить, что CD/DVD-образ содержит ссылки на данные из другой (предыдущей) сессии. Поскольку эта предыдущая сессия недоступна (она могла быть записана на диск задолго до того, как DeviceLock Service был установлен), то консоль управления находит и исправляет все ссылки на эти несуществующие данные, чтобы сделать результирующий файл образа пригодным для чтения в приложениях, поддерживающих формат CUE.

Тем не менее, если вам необходимо получить данные без изменений, то используйте *Save As Raw Data*. В этом случае результирующий файл образа может быть не пригодным для чтения в приложениях, поддерживающих формат CUE.

Когда вы сохраняете большой файл, вы можете нажать на кнопку *Cancel* на индикаторе выполнения, чтобы прервать сохранение. В этом случае, результирующий файл, который вы получите на локальном компьютере, будет неполным, он будет содержать только те данные, которые были получены до того момента, как вы прервали процесс сохранения.

г. View

Чтобы открыть данные во встроенном просмотрщике, используйте *View* из контекстного меню.

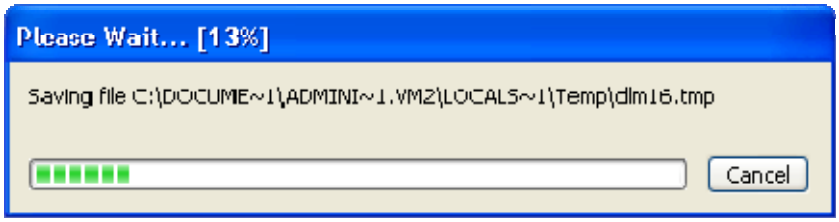


Этот простой просмотрщик поддерживает два режима отображения данных:

1. **Шестнадцатирично-текстовый** – выберите опцию *Hex*, чтобы отобразить данные в смешанном режиме, как показано на картинке выше.

2. **Текстовый** – выберите опцию *Text*, чтобы отобразить данные в текстовом режиме.

Когда вы открываете большой файл, вы можете нажать на кнопку *Cancel* на индикаторе выполнения, чтобы прервать процесс.



В этом случае, просмотрщик покажет только те данные, которые были получены до того момента, как вы прервали процесс открытия.

Нажмите на кнопку *Save*, чтобы сохранить данные из просмотрщика во внешний файл.

д. External Viewer

Также вы можете открыть данные во внешней программе. Если такая внешняя программа определена, то пункт *External Viewer* доступен в контекстном меню.

Чтобы задать внешнюю программу просмотра данных, используйте редактор реестра Regedit и внесите следующие изменения в реестр компьютера, на котором запущена консоль управления:

- Ключ: *HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager*
- Имя: *ExternalShadowViewer*
- Тип: *REG_SZ*
- Значение: *<полный_путь_к_программе> %1*

где *<полный_путь_к_программе>* должен сдержать полный путь к исполняемому файлу программы. Если путь содержит пробелы, то его необходимо заключить в кавычки. Например, *"C:\Program Files\Microsoft Office\OFFICE11\winword.exe" %1*.

Когда вы открываете большой файл, вы можете нажать на кнопку *Cancel* на индикаторе выполнения, чтобы прервать процесс. В этом случае, внешнее приложение отобразит только те данные, которые были получены до того момента, как вы прервали процесс открытия.

е. Delete

Чтобы удалить запись, используйте *Delete* из контекстного меню или соответствующую кнопку на инструментальной панели. Используя клавиши *Ctrl* и/или *Shift,* вы можете выделить и удалить несколько записей одновременно.

ж. Refresh

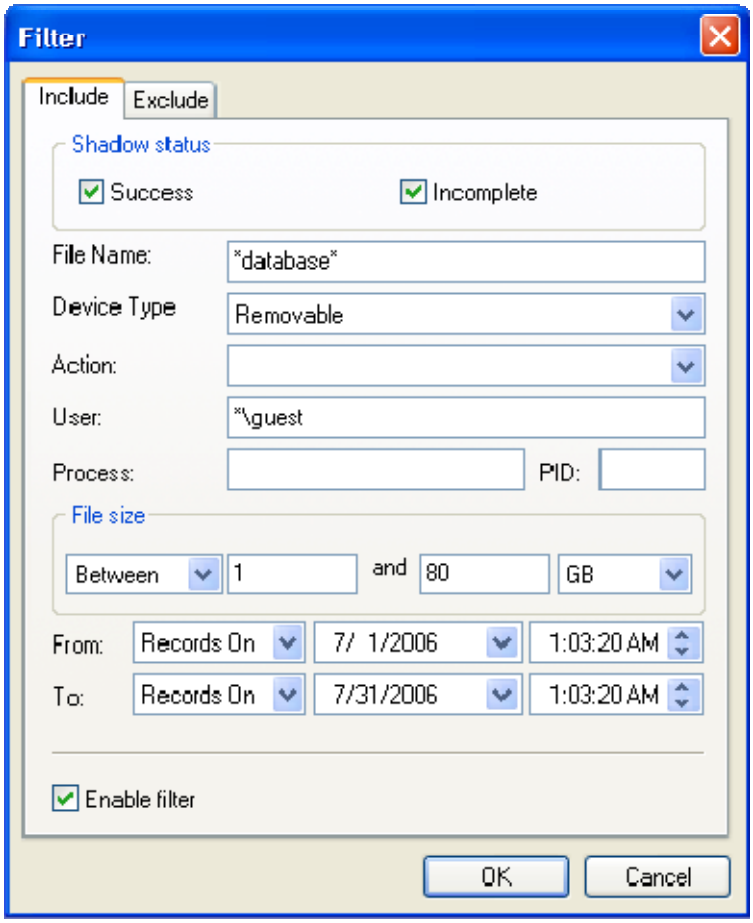
Чтобы обновить список, используйте *Refresh* из контекстного меню или соответствующую кнопку на инструментальной панели.

з. Send Data to Server

Когда список DeviceLock Enterprise Server'ов определен в Service Options и вам необходимо форсировать передачу данных с текущего подключенного компьютера на сервер, используйте *Send Data to Server* из контекстного меню или соответствующую кнопку на инструментальной панели.

5.4.4.1 Фильтр журнала теневого копирования (для компьютера)

Вы можете фильтровать данные в Shadow Log Viewer так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список.



Чтобы открыть диалог *Filter*, используйте *Filter* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Shadow Log Viewer* или соответствующую кнопку на инструментальной панели.

Разница между заданием фильтра для журнала аудита и журнала теневого копирования незначительна, поэтому рекомендуем прочитать раздел **Фильтр журнала аудита (для компьютера)** данного руководства.

Когда фильтр включен, вы можете определить условия фильтрации, задав необходимые значения в следующих полях:

- *Success* – флаг, определяющий нужно ли фильтровать успешно запротоколированные данные.

- *Incomplete* – флаг, определяющий нужно ли фильтровать данные, которые возможно были запротоколированы не полностью.

- *File Name* – текст, соответствующий значению столбца *File Name* в Shadow Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Device Type* – выбираемый параметр, соответствующий значению *Device Type* в Shadow Log Viewer.

- *Action* – выбираемый параметр, соответствующий значению *Action* в Shadow Log Viewer.

- *User* – текст, соответствующий значению столбца *User* в Shadow Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Process* – текст, соответствующий значению столбца *Process* в Shadow Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *PID* – число, соответствующее значению столбца *PID* в Shadow Log Viewer.

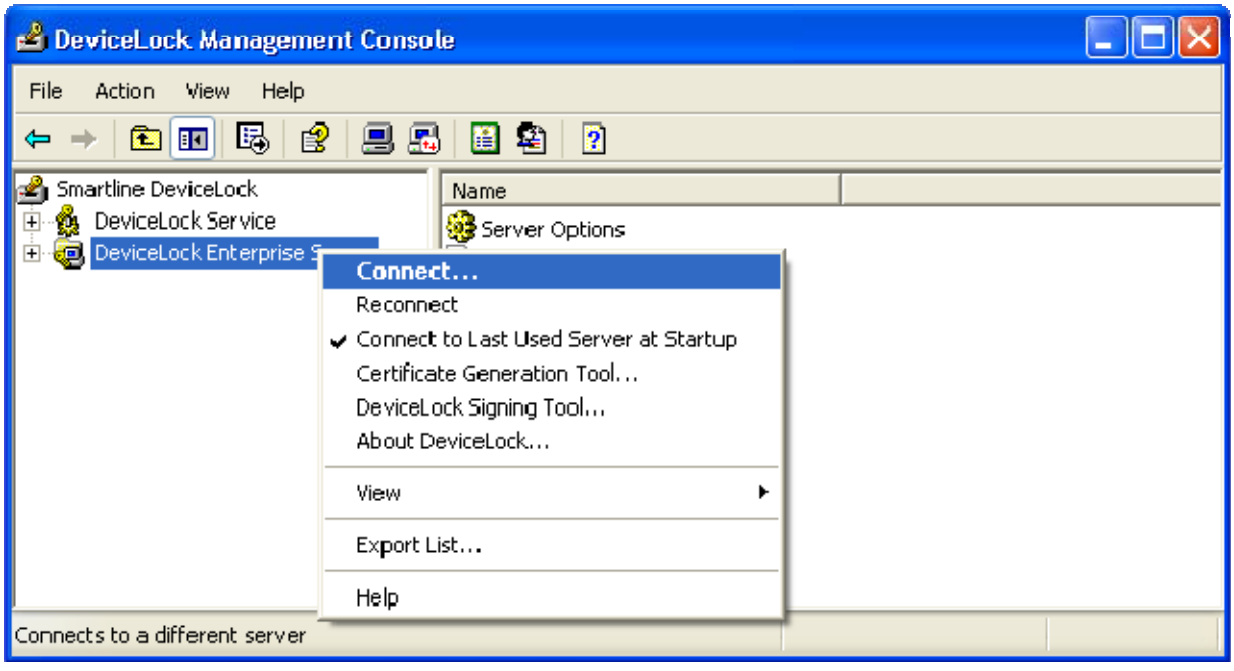
- *File size* – число или регион чисел, соответствующих значению столбца *File Size* в Shadow Log Viewer.

- *From* – определяет начало временного интервала записей, которые вы хотите фильтровать. Выберите *First Record,* чтобы фильтровать записи, начиная с самой первой в журнале. Выберите *Records On*, чтобы фильтровать записи, начиная с определенной даты и времени.

- *To* – определяет конец временного интервала записей, которые вы хотите фильтровать. Выберите *Last Record*, чтобы фильтровать записи, заканчивая самой последней в журнале. Выберите *Records On,* чтобы фильтровать записи, заканчивая записью с определенной датой и временем.

5.5 Администрирование DeviceLock Enterprise Server

Раскройте раздел *DeviceLock Enterprise Server*, чтобы получить доступ ко всем функциям и настройкам сервера.



По нажатию правой кнопки мыши на элементе *DeviceLock Enterprise Server* появляется контекстное меню:

- *Connect* – для подключения к удаленному или локальному компьютеру. За дополнительной информацией обращайтесь к разделу **Подключение к компьютеру** данного руководства.

  Когда вы подключаетесь к компьютеру, на котором установлена предыдущая версия DeviceLock Enterprise Sever, то консоль управления показывает следующее сообщение:

  В этом случае вам надо установить новую версию DeviceLock Enterprise Server на этот компьютер. Информацию относительно установки сервера вы можете найти в главе **Установка DeviceLock Enterprise Server** данного руководства.

- *Reconnect* – подключается к текущему компьютеру повторно.

- *Connect to Last Used Server at Startup* – установите этот флаг для того, чтобы при каждом запуске консоль управления автоматически подключалась к серверу, который использовался в предыдущий раз.

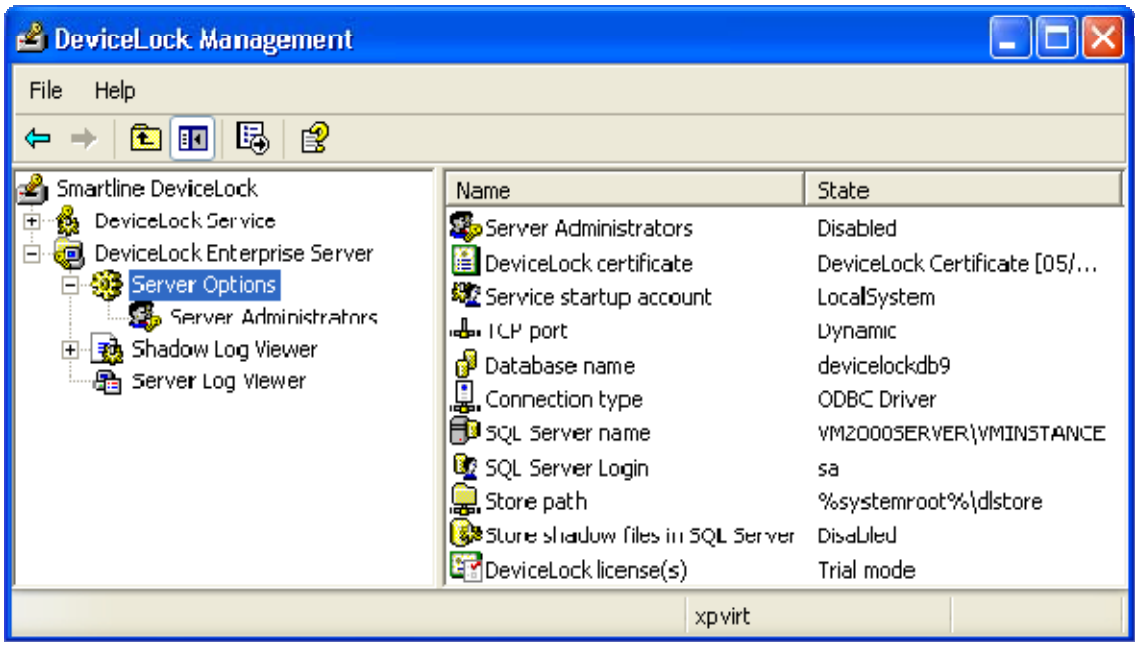
- *Certificate Generation Tool* – запускает специальную программу для создания сертификатов (DeviceLock Certificate). За дополнительной информацией обращайтесь к разделу **Создание сертификата** данного руководства.

- *DeviceLock Signing Tool* – запускает специальную программу для авторизации устройств во временном белом списке и подписывания XML-файлов с настройками DeviceLock Service'а. За дополнительной информацией обращайтесь к разделу **DeviceLock Signing Tool** данного руководства.

- *About DeviceLock* – показывает диалог с информацией о версии и установленных лицензиях на DeviceLock.

5.5.1 Server Options

Эти дополнительные параметры позволяют настроить DeviceLock Enterprise Server.



Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши, или кликните два раза на параметре *Stream compression*, чтобы включить или выключить его. Когда параметр *Stream compression* включен, DeviceLock сжимает данные аудита и теневого копирования, передаваемые с DeviceLock Service'ов на DeviceLock Enterprise Server. Это позволяет уменьшить размер передаваемых данных и соответственно снизить нагрузку на сеть.

DeviceLock Enterprise Server может автоматически извлекать файлы из CD/DVD-образов в журнале теневого копирования. Когда включен параметр *Unpack ISO*, все файлы из CD/DVD-образов извлекаются по мере поступления образов на сервер и сохраняются в базе данных по отдельности (одна запись на один файл). Если параметр *Unpack ISO* выключен, то в базе данных сохраняются целиком сами CD/DVD-образы.

Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши на остальных параметрах. Также вы можете два раза кликнуть мышкой на параметре, чтобы открыть диалог с его настройками.

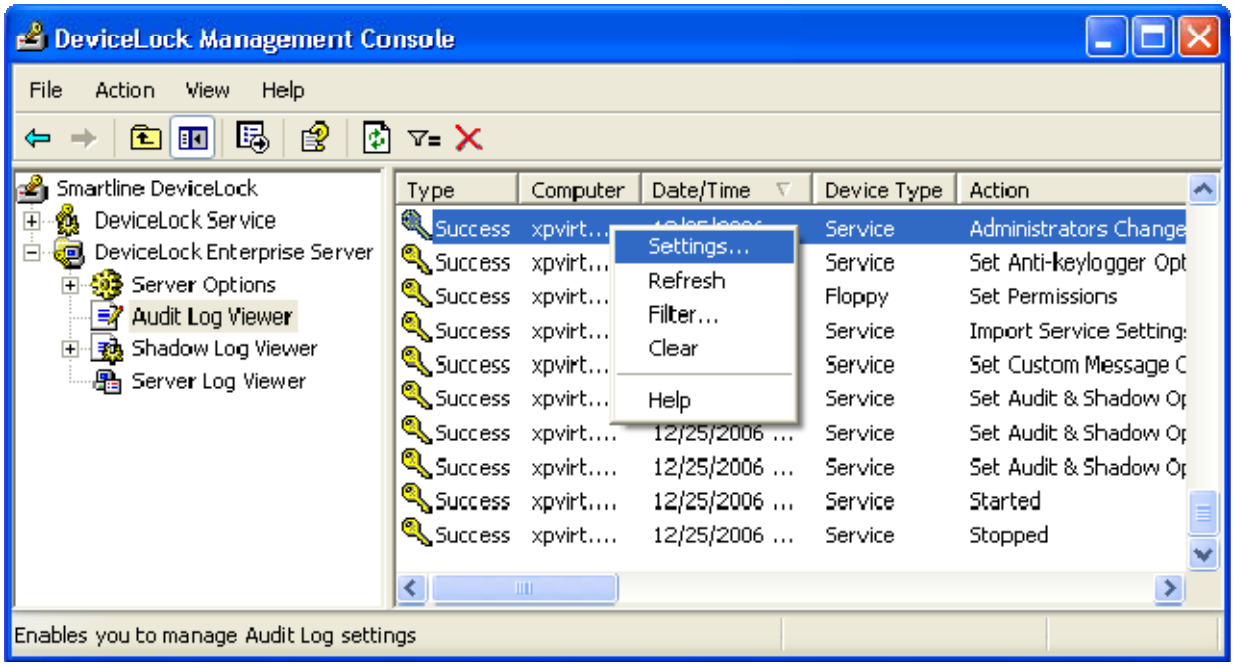
Все эти параметры и их настройки подробно описаны в разделе **Установка DeviceLock Enterprise Server** данного руководства.

Чтобы открыть мастер настроек для установки или просмотра параметров сервера, используйте пункт *Properies* из контекстного меню, появляющегося при нажатии правой кнопки мыши на элементе *Server Options*. Мастер настроек также подробно описан в разделе **Установка DeviceLock Enterprise Server** данного руководства.

5.5.2 Audit Log Viewer (для сервера)

Консоль управления содержит встроенный просмотрщик записей аудита, хранимых на DeviceLock Enterprise Server'е.

DeviceLock Enterprise Server собирает записи аудита с удаленного компьютера, только если параметр *Audit log type* в Service Options установлен в значение *DeviceLock Log* или *Event & DeviceLock Logs*. В противном случае, записи аудита хранятся в стандартном журнале Windows на локальном компьютере и могут быть просмотрены с помощью просмотрщика аудита для компьютера.



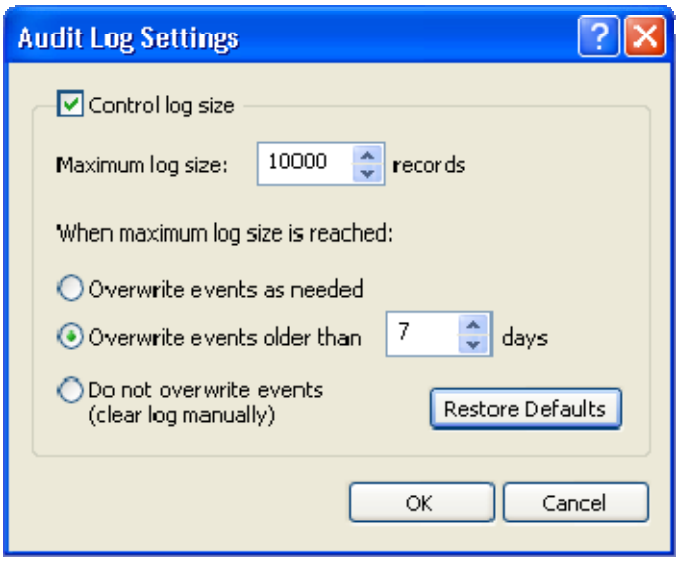
Разница между просмотрщиком журнала аудита для сервера и для отдельных компьютеров незначительна, поэтому рекомендуем прочитать раздел **Audit Log Viewer (для компьютера)** данного руководства.

По сравнению с просмотрщиком журнала аудита для отдельных компьютеров, серверный просмотрщик имеет два дополнительных столбца:

- *Computer* – имя компьютера, с которого были получены данные аудита.
- *Event* – номер, идентифицирующий событие.

5.5.2.1 Настройки журнала аудита (для сервера)

Чтобы определить максимальный размер журнала аудита и действия DeviceLock Enterprise Server'а в случае его заполнения, используйте *Settings* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Audit Log Viewer*.



ПРИМЕЧАНИЕ: Данные настройки хранятся в базе данных, и они специфичны для журнала, а не для DeviceLock Enterprise Server'а. Это означает, что если несколько DeviceLock Enterprise Server'ов используют одну и туже базу данных, то для них всех настройки журнала будут идентичны.

Установите флаг *Control log size,* чтобы разрешить DeviceLock Enterprise Server'у контролировать количество записей в журнале и удалять устаревшие записи по необходимости для освобождения места под новые записи. В противном случае, если флаг *Control log size* не установлен, DeviceLock Enterprise Server использует все доступное для базы данных пространство для хранения журнала.

В параметре *Maximum log size* вы можете указать максимальное количество записей, которое данный журнал может содержать. Имейте в виду, что если более чем один DeviceLock Enterprise Server использует эту базу данных, то количество записей в журнале может незначительно превышать заданное значение.

Чтобы определить действия DeviceLock Enterprise Server'а в случае заполнения журнала, выберите одну из этих опций:

- *Overwrite events as needed* – сервер перезаписывает старые записи новыми, когда превышается размер, заданный в параметре *Maximum log size*.

- *Overwrite events older than* – сервер перезаписывает только те записи, которые старше заданного количества дней.

- *Do not overwrite events (clear log manually)* – сервер вообще не перезаписывает записи, когда превышается размер, заданный в параметре *Maximum log size,* и в таком случае вам необходимо очищать журнал вручную.

Если вы хотите сбросить текущие настройки, используйте кнопку *Restore Defaults*. Настройки по умолчанию выглядят следующим образом:

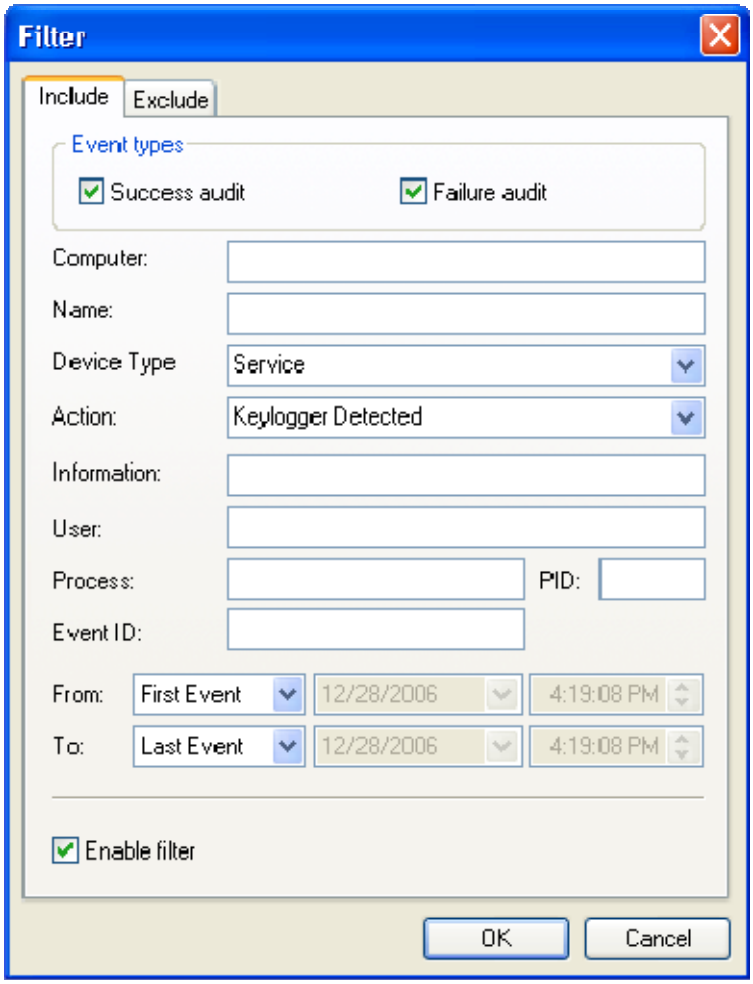
- Параметр *Maximum log size* равен 10000 записей.

- Выбрана опция *Overwrite events older than* и для нее установлено значение 7 дней.

Если в журнале аудита нет места для новых записей и нечего удалять, то DeviceLock Enterprise Server не будет удалять данные аудита с компьютеров пользователей. Это предотвращает потерю данных аудита по причине отсутствия места на сервере. Когда в журнале появляется свободное место, DeviceLock Enterprise Server перемещает оставшиеся данные аудита с компьютеров пользователей в этот журнал.

5.5.2.2 Фильтр журнала аудита (для сервера)

Вы можете фильтровать данные в Audit Log Viewer так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список.



Чтобы открыть диалог *Filter*, используйте *Filter* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Audit Log Viewer* или соответствующую кнопку на инструментальной панели.

Разница между заданием фильтра журнала аудита для сервера и для отдельных компьютеров незначительна, поэтому рекомендуем прочитать раздел **Фильтр журнала аудита (для компьютера)** данного руководства.

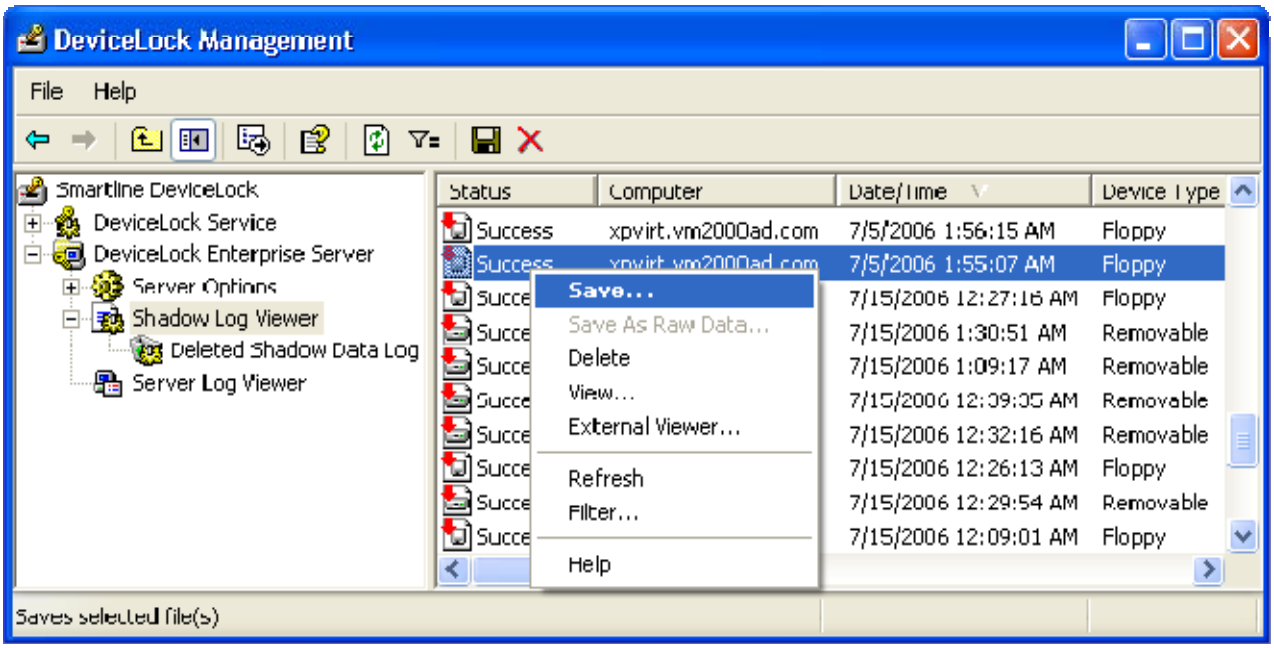
По сравнению с фильтром журнала аудита для отдельных компьютеров этот серверный фильтр имеет только два дополнительных поля:

- *Computer* – текст, соответствующий значению столбца *Computer* в Audit Log Viewer. Это поле нечувствительно к регистру, и вы можете использовать маски.

- *Event ID* – число, соответствующее значению столбца *Event* в Audit Log Viewer.

5.5.3 Shadow Log Viewer (для сервера)

Консоль управления содержит встроенный просмотрщик данных теневого копирования, хранимых на DeviceLock Enterprise Server'е.



Разница между просмотрщиком журнала теневого копирования для сервера и для отдельных компьютеров незначительна, поэтому рекомендуем прочитать раздел **Shadow Log Viewer (для компьютера)** данного руководства.

По сравнению с просмотрщиком журнала теневого копирования для отдельных компьютеров, серверный просмотрщик имеет только один дополнительный столбец:

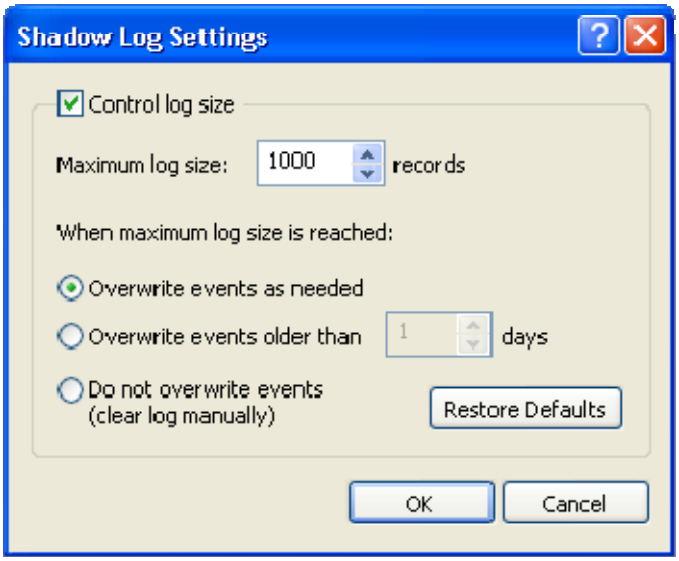
- *Computer* – имя компьютера, с которого были получены данные теневого копирования.

Кроме того, в отличие от просмотрщика журнала теневого копирования для отдельных компьютеров, в серверном просмотрщике при удалении записи из списка, сами данные также удаляются из базы данных или с диска (в зависимости от флага *Store shadow files in SQL Server*), но остальная информация (такая как имя файла и его размер, пользователь, дата/время и т.п.) переносится в специальный журнал Deleted Shadow Data Log.

Этот специальный журнал удаленных данных используется в тех случаях, когда вам больше не нужны сами данные (содержимое файлов), которые пользователи передавали и вы хотите очистить хранилище (SQL Server или диск), но в то же самое время вам необходимо сохранить информацию о самом факте передачи данных.

5.5.3.1 Настройки журнала теневого копирования (для сервера)

Чтобы определить максимальный размер журнала теневого копирования и действия DeviceLock Enterprise Server'а в случае его заполнения, используйте *Settings* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Shadow Log Viewer*.



Все эти настройки подробно описаны в разделе **Настройки журнала аудита (для сервера)** данного руководства.

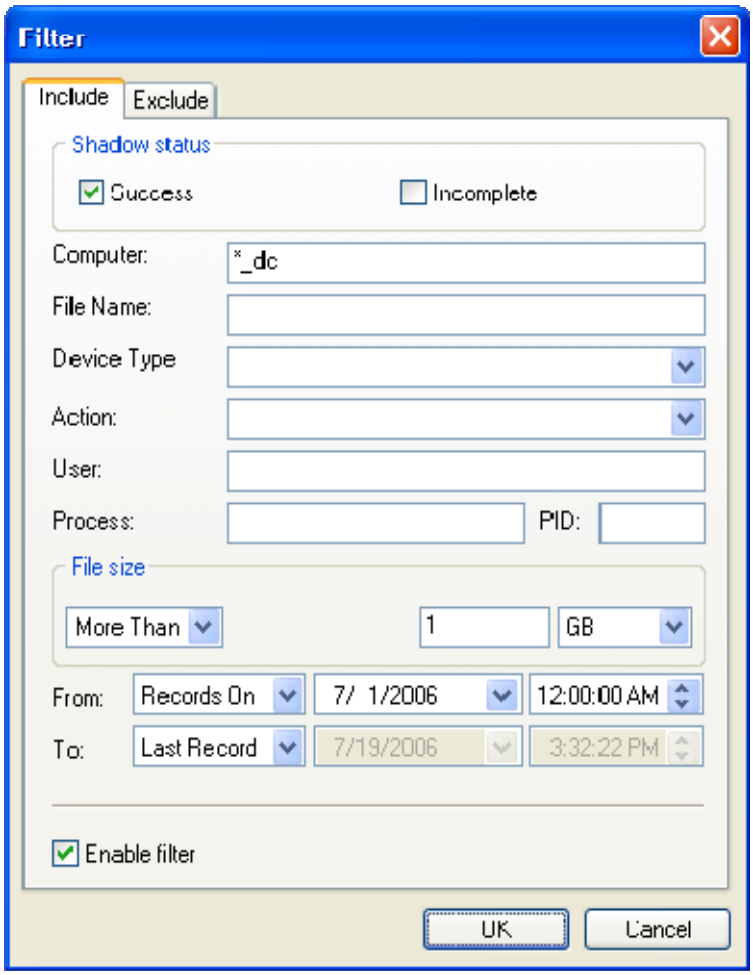
Когда в соответствии с заданными настройками (*Overwrite events as needed* и *Overwrite events older than*) DeviceLock Enterprise Server'у необходимо удалить некоторые старые записи из журнала теневого копирования, эти записи переносятся в специальный журнал Deleted Shadow Data Log.

Если в журнале теневого копирования нет места для новых записей и нечего удалять, то DeviceLock Enterprise Server не будет удалять данные теневого копирования с компьютеров пользователей. Это предотвращает потерю данных теневого копирования по причине отсутствия места на сервере. Когда в журнале появляется свободное место, DeviceLock Enterprise Server перемещает оставшиеся данные теневого копирования с компьютеров пользователей в этот журнал.

Мы настоятельно рекомендуем не допускать ситуации, когда данные сетевого копирования накапливаются на компьютерах пользователей. Необходимо регулярно проверять предупреждающие записи в журнале DeviceLock Enterprise Server'а.

5.5.3.2 Фильтр журнала теневого копирования (для сервера)

Вы можете фильтровать данные в Shadow Log Viewer так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список.



Чтобы открыть диалог *Filter*, используйте *Filter* из контекстного меню доступного по нажатию правой кнопки мыши на элементе *Shadow Log Viewer* или соответствующую кнопку на инструментальной панели.

Разница между заданием фильтра журнала теневого копирования для сервера и для отдельных компьютеров незначительна, поэтому рекомендуем прочитать раздел **Фильтр журнала теневого копирования (для компьютера)** данного руководства.

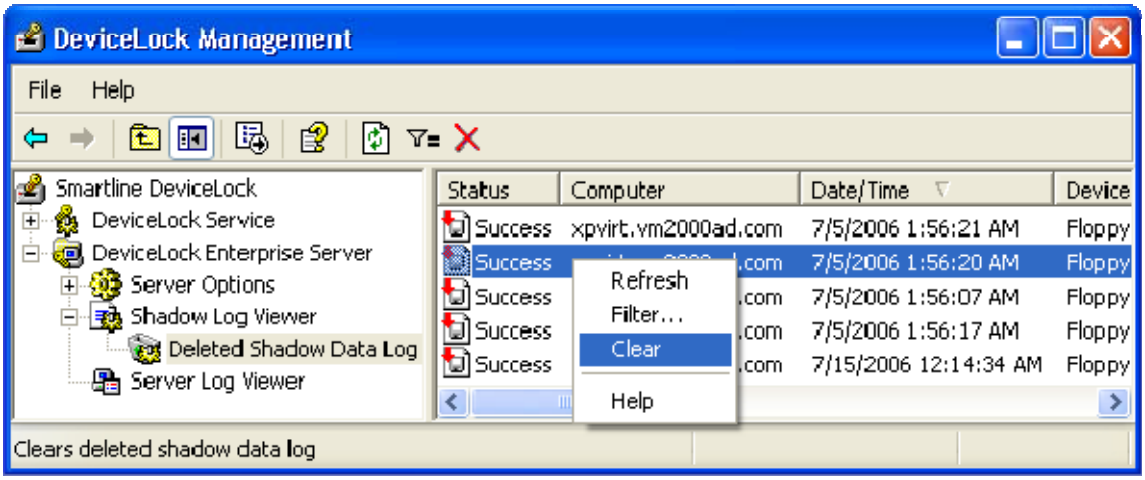
По сравнению с фильтром журнала теневого копирования для отдельных компьютеров, этот серверный фильтр имеет только одно дополнительное поле:

- *Computer* – текст, соответствующий значению столбца *Computer* в Shadow Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

5.5.3.3 Deleted Shadow Data Log

Этот встроенный просмотрщик позволяет получить список записей, удаленных из журнала теневого копирования.

Когда в Shadow Log Viewer запись удаляется из журнала теневого копирования, то сами данные удаляются из базы данных или с диска (в зависимости от флага *Store shadow files in SQL Server*), но остальная информация (такая как имя файла и его размер, пользователь, дата/время и т.п.) переносится в этот специальный журнал.



Этот журнал используется в тех случаях, когда вам больше не нужны сами данные (содержимое файлов), которые пользователи передавали и вы хотите очистить хранилище (SQL Server или диск), но в то же самое время вам необходимо сохранить информацию о самом факте передачи данных.

Чтобы определить максимальный размер журнала и действия DeviceLock Enterprise Server'а в случае его заполнения, используйте *Settings* из контекстного меню, доступного по нажатию правой кнопки мыши. Все эти настройки подробно описаны в разделе **Настройки журнала аудита (для сервера)** данного руководства.

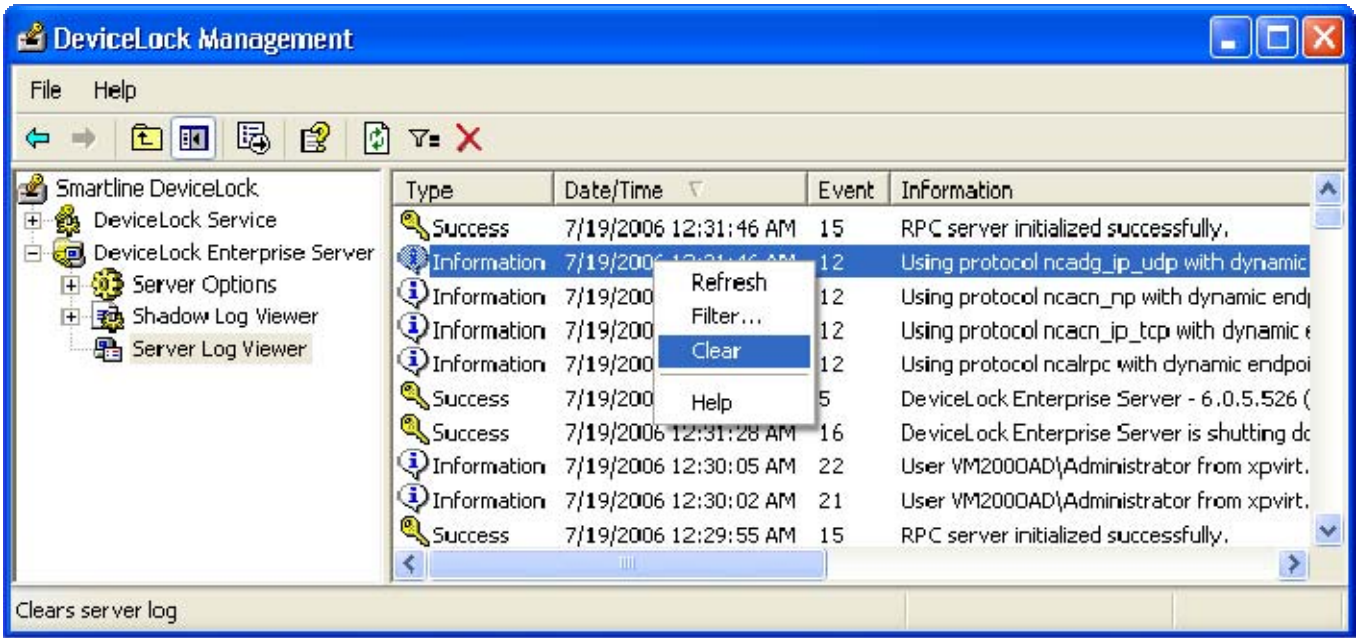
Если в журнале нет места для новых записей и нечего удалять, то DeviceLock Enterprise Server будет терять эти новые записи. Чтобы предотвратить потерю данных по причине отсутствия места на сервере, необходимо регулярно проверять предупреждающие записи в журнале DeviceLock Enterprise Server'a.

Чтобы обновить список, используйте *Refresh* из контекстного меню или соответствующую кнопку на инструментальной панели.

Чтобы отфильтровать записи в этом списке, используйте *Filter* из контекстного меню, доступного по нажатию правой кнопки мыши или соответствующую кнопку на инструментальной панели. Здесь используется тот же самый фильтр, что и в просмотрщике журнала теневого копирования, поэтому прочитайте раздел **Фильтр журнала теневого копирования (для сервера)** данного руководства. Чтобы полностью очистить этот журнал, используйте *Clear* из контекстного меню или соответствующую кнопку на инструментальной панели.

5.5.4 Server Log Viewer

Этот встроенный просмотрщик позволяет получить список записей из внутреннего журнала DeviceLock Enterprise Server. Сервер использует этот журнал, чтобы протоколировать свои собственные события, ошибки и любую другую важную информацию (например, изменения в настройках, запуск и остановку, номер версии и т.п.).



Вы можете использовать информацию из этого журнала для диагностики и выявления проблем в работе сервера, мониторинга изменений в его настройках и действий по очистке журналов.

Столбцы просмотрщика определены следующим образом:

- *Type* – класс события: *Success*, *Information*, *Warning* или *Error*.
- *Date/Time* – дата и время, когда событие произошло.
- *Event* – номер идентифицирующий событие.
- *Information* – иная, специфичная для данного события информация, такая как описание ошибки, название и значение измененного параметра и т.п.
- *Server* – имя сервера, где событие произошло.
- *Record N* – номер записи.

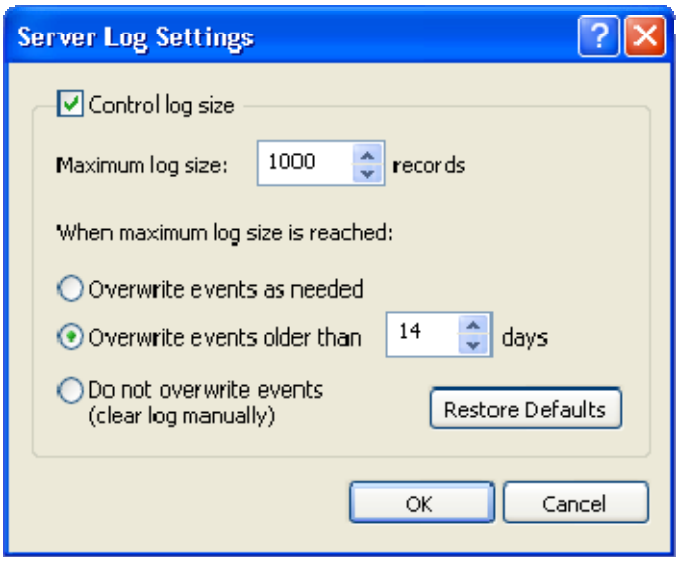
Чтобы обновить список, используйте *Refresh* из контекстного меню или соответствующую кнопку на инструментальной панели.

Чтобы полностью очистить этот журнал, используйте *Clear* из контекстного меню или соответствующую кнопку на инструментальной панели.

После очистки этого журнала в него автоматически добавляется одно событие, говорящее о самом факте очистки (например, “*The Server Log (100 record(s)) was cleared by VM2000AD\Administrator from xpvirt.vm2000ad.com*”).

5.5.4.1 Настройки журнала сервера

Чтобы определить максимальный размер журнала сервера и действия DeviceLock Enterprise Server’а в случае его заполнения, используйте *Settings* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Server Log Viewer*.

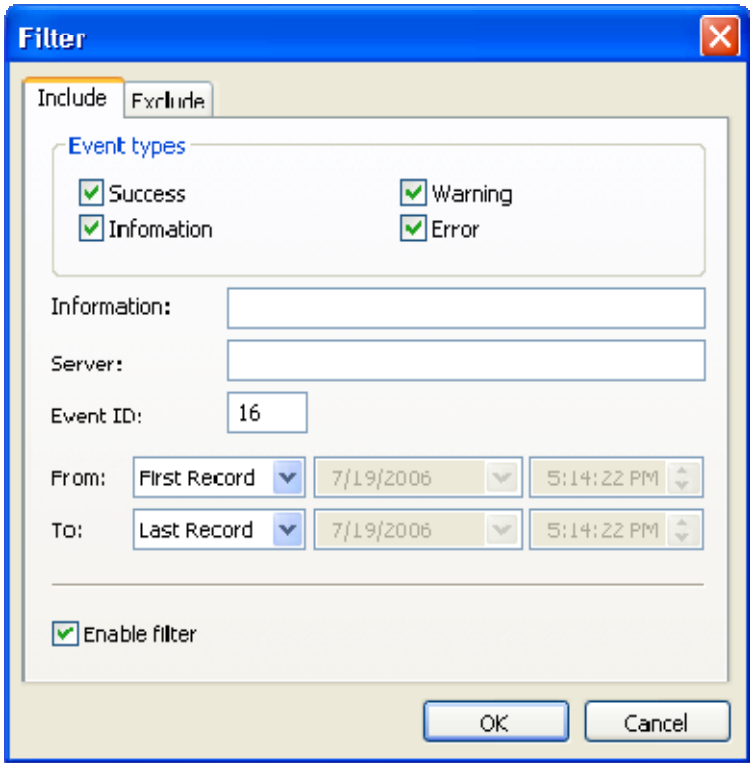


Все эти настройки подробно описаны в разделе **Настройки журнала аудита (для сервера)** данного руководства.

Если в журнале сервера нет места для новых записей и нечего удалять, то DeviceLock Enterprise Server будет терять эти новые записи.

5.5.4.2 Фильтр журнала сервера

Вы можете фильтровать данные в Server Log Viewer так чтобы только записи, удовлетворяющие заданным условиям, выводились в список.



Чтобы открыть диалог *Filter*, используйте *Filter* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Server Log Viewer* или соответствующую кнопку на инструментальной панели.

Разница между заданием фильтра для журнала аудита и журнала сервера незначительна, поэтому рекомендуем прочитать раздел **Фильтр журнала аудита** данного руководства.

Когда фильтр включен, вы можете определить условия фильтрации, задав необходимые значения в следующих полях:

- *Success* – флаг, определяющий нужно ли фильтровать записи по классу *Success*.
- *Information* – флаг, определяющий нужно ли фильтровать записи по классу *Information*.
- *Warning* – флаг, определяющий нужно ли фильтровать записи по классу *Warning*.
- *Error* – флаг, определяющий нужно ли фильтровать записи по классу *Error*.
- *Information* – текст, соответствующий значению столбца *Information* в Server Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.
- *Server* – текст, соответствующий значению столбца *Server* в Server Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Event ID* – число, соответствующее значению столбца *Event* в Server Log Viewer.

- *From* – определяет начало временного интервала событий, которые вы хотите фильтровать. Выберите *First Event,* чтобы фильтровать события, начиная с самого первого в журнале. Выберите *Events On*, чтобы фильтровать события, начиная с определенной даты и времени.

- *To* – определяет конец временного интервала событий, которые вы хотите фильтровать. Выберите *Last Event*, чтобы фильтровать события, заканчивая самым последним событием в журнале. Выберите *Events On,* чтобы фильтровать события, заканчивая событием с определенной датой и временем.

5.5.5 Мониторинг

Централизованный мониторинг – функция DeviceLock Enterprise Server'а, позволяющая контролировать текущее состояние агентов на удаленных компьютерах путем периодического опроса. Результат мониторинга отображается в консоли управления в режиме реального времени, а также сохраняется в специальном журнале и позже может быть проанализирован при помощи встроенного просмотрщика журнала мониторинга.

Кроме того, DeviceLock Enterprise Server периодически сравнивает текущие политики безопасности (настройки) агентов на указанных администратором компьютерах с эталонными политиками, и фиксирует информацию о выявленных отклонениях. При этом возможно автоматическое восстановление измененных политик безопасности.

5.5.5.1 Обзор архитектуры

Все действия (опрос компьютеров и DeviceLock Service'ов, проверка целостности политики и т.п.) в мониторинге выполняются задачами.

На одном DeviceLock Enterprise Server'е вы можете создать любое количество задач. Максимальное количество задач на сервере ограничено только количеством свободной памяти, скоростью процессора и пропускной способностью сети. Имейте в виду, что сервер должен иметь достаточно ресурсов, чтобы одновременно подключаться как минимум к 10 удаленным компьютерам.

По умолчанию DeviceLock Enterprise Server может выполнять одновременно до 30 задач. Это означает, что если у вас, например, 40 задач, и все они запускаются в одно и то же время, то сначала будут запущены первые 30 задач, а затем, по мере их окончания, по одной будут запускаться оставшиеся 10 задач.

Тем не менее, вы можете изменить максимальное количество одновременно запускаемых задач. Чтобы поменять это значение, используйте редактор реестра Regedit и внесите следующие изменения в реестр компьютера, на котором запущен DeviceLock Enterprise Server:

- Ключ: *HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer*

- Имя: *ConcurrentJobs*

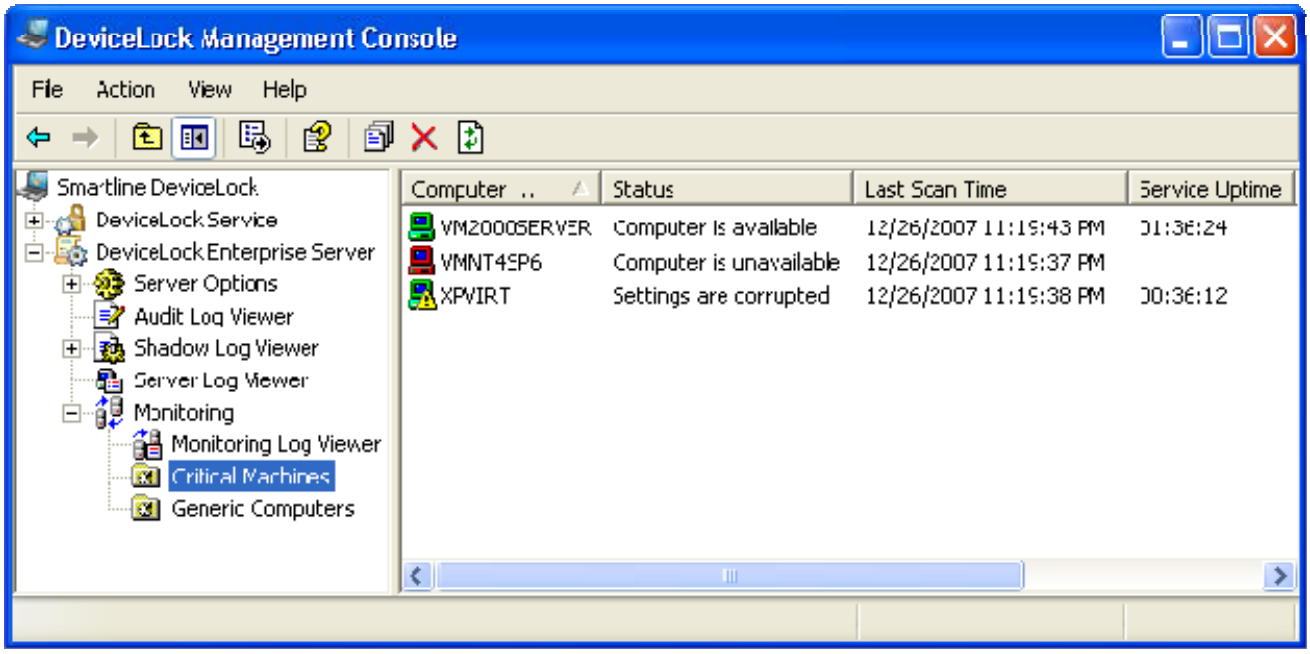
- Тип: *DWORD*

- Значение: *<количество_потоков>*

где *<количество_потоков>* должно сдержать число от 1 до 1000.

Во время своего выполнения задачи пишут полезную информацию в журнал мониторинга. Эта информация включает в себя текущие состояния компьютеров и DeviceLock Service'ов, а также возможные ошибки, которые возникают в процессе сканирования компьютеров и подключения к DeviceLock Service'ам.

Также задачи отображают списки компьютеров и их текущие состояния в консоли управления. Это позволяет анализировать ситуацию в режиме реального времени.



Чтобы просмотреть список компьютеров для определенной задачи, выделите эту задачу в левом дереве.

Чтобы обновить информацию в списке компьютеров, используйте *Refresh* из контекстного меню или соответствующую кнопку на инструментальной панели.

- *Computer Name* – имя компьютера.

- *Status* – текущее состояние (статус) компьютера и DeviceLock Service'а.

  Статус также влияет на картинку (иконку) отображаемую слева от параметра *Computer Name*. Общее правило для отображения иконки компьютера такое:

  - *Зеленый компьютер* – означает, что компьютер и DeviceLock Service работают.

  - *Красный компьютер* – означает, что компьютер не работает (либо не найден) или работает, но DeviceLock Service не запущен.

  - *Компьютер с восклицательным знаком* – означает, что обнаружены проблемы либо с компьютером, либо с DeviceLock Service'ом.

  Выделяется семь различных состояний (статусов):

  1. *Computer is available* – этот статус означает, что компьютер работает и DeviceLock Service на нем запущен. Также если эта задача проверят целостность политики, то данная проверка прошла без ошибок. Иконка компьютера будет – "*зеленый компьютер*".

  2. *Computer is unavailable* – этот статус означает, что DeviceLock Enterprise Server не может просканировать компьютер. Это происходит, когда компьютер выключен или соединения блокируются файрволом, но при этом имя компьютера или его IP-адрес могут быть получены через DNS. Иконка компьютера будет – "*красный компьютер*".

  3. *Service is unavailable* – этот статус означает, что DeviceLock Enterprise Server не может подсоединиться к DeviceLock Service'у. Это происходит, когда компьютер работает, но DeviceLock Service не запущен на нем. Также это может происходить из-за того, что DeviceLock Service запущен не на том TCP-порту, который указан в настройках задачи, или соединения блокируются файрволом. Иконка компьютера будет – "*красный компьютер с восклицательным знаком*". За дополнительной информацией относительно проблем соединения, обращайтесь к описанию параметра *Service connection settings*.

  4. *Settings are corrupted* – этот статус означает, что компьютер работает и DeviceLock Service на нем запущен, но процедура проверки целостности политики вернула ошибку. Это происходит, когда эталонная политика, присвоенная данной задаче, отличается от политики, установленной на DeviceLock Service. Иконка компьютера будет – "*зеленый компьютер с восклицательным знаком*".

  5. *Unresolved computer address* – этот статус означает, что DeviceLock Enterprise Server не может получить имя/адрес компьютера. Это происходит, когда задано имя компьютера не существующее в DNS. Также это может происходить из-за того, что компьютер в данный момент не включен, а в сети нет DNS-сервера. В таком случае статус *Unresolved computer address* должен трактоваться вами как *Computer*

is unavailable. Иконка компьютера будет – "*красный компьютер с восклицательным знаком*".

6. *Unsupported service version* – этот статус означает, что DeviceLock Enterprise Server пытается получить политику (настройки) из DeviceLock Service'а версии 6.2 и ниже. Проверка целостности политик поддерживается только для версий 6.2.1 и выше. Иконка компьютера будет – "*зеленый компьютер с восклицательным знаком*".

7. *Access is denied* – этот статус означает, что DeviceLock Enterprise Server не может подсоединиться к DeviceLock Service'у из-за недостатка привилегий. Это происходит, когда учетная запись, под которой запущена служба DeviceLock Enterprise Server'а, не имеет прав доступа для подключения к DeviceLock Service'у. Иконка компьютера будет – "*зеленый компьютер с восклицательным знаком*". За дополнительной информацией относительно проблем соединения обращайтесь к описанию параметра *Service connection settings*.

Также, все те же самые статусы (за исключением *Computer is available*) записываются в журнал мониторинга и могут быть проанализированы позже.

- *Last Scan Time* – дата и время последней попытки сканирования.

- *Service Uptime* – время работы DeviceLock Service'а.

- *Computer Uptime* – время работы компьютера.

- *Service Version* – версия DeviceLock Service'а. Последние пять цифр определяют номер сборки.

5.5.5.2 Алгоритм мониторинга

Алгоритм, используемый в мониторинге, прост, но эффективен:

1. Прежде всего DeviceLock Enterprise Server пытается просканировать компьютер и определить, работает он или нет. Если сканирование удалось, то компьютер получает статус *доступен* и мониторинг компьютера продолжается. В противном случае компьютер получает статус *недоступен* и мониторинг компьютера прекращается (происходит запись в журнал).

2. Затем DeviceLock Enterprise Server пытается подключиться к DeviceLock Service'у. Если подключение удалось, то DeviceLock Service получает статус *доступен* и мониторинг компьютера продолжается. В противном случае DeviceLock Service получает статус *недоступен* и мониторинг компьютера прекращается (происходит запись в журнал).

3. Если данная задача должна проверять целостность политики, то мониторинг компьютера продолжается. В противном случае мониторинг компьютера прекращается (в журнал ничего не пишется).

4. DeviceLock Enterprise Server получает политику из DeviceLock Service'а и сравнивает ее с эталонной политикой, присвоенной данной задаче. Если расхождений в политиках не обнаружено, то мониторинг компьютера прекращается (в журнал ничего не пишется). Если обнаружены различия в двух политиках, то мониторинг компьютера продолжается (происходит запись в журнал).

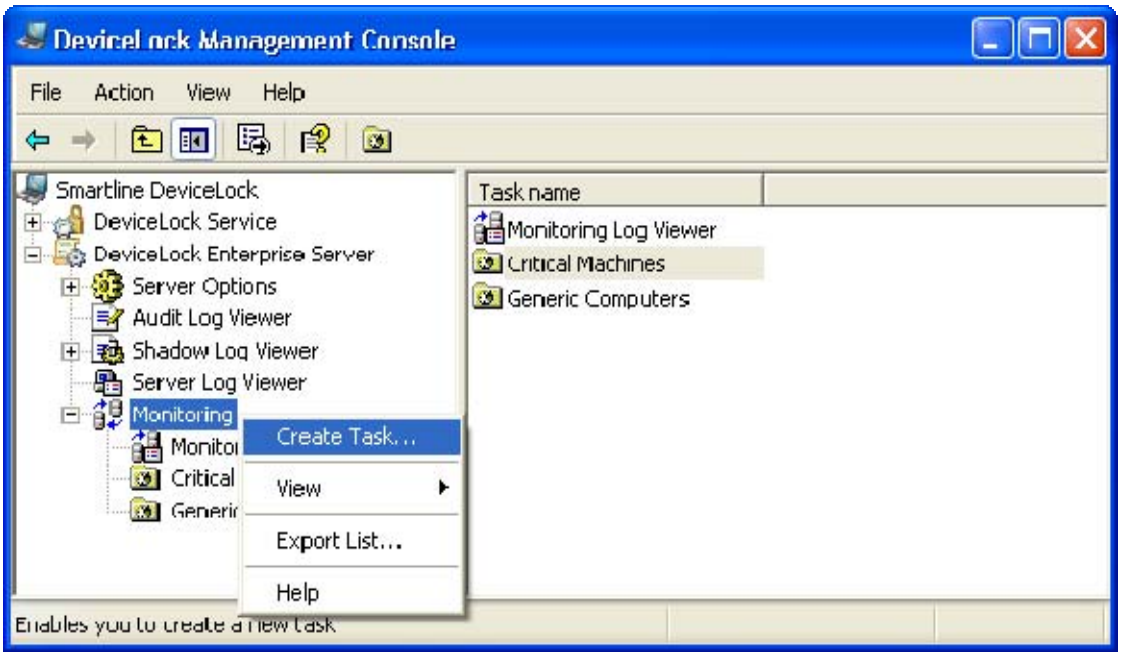
5. Если данная задача должна восстанавливать измененную политику, то DeviceLock Enterprise Server заменяет политику на DeviceLock Service на эталонную и мониторинг компьютера прекращается (происходит запись в журнал). В противном случае мониторинг компьютера просто прекращается (в журнал ничего не пишется).

Если на каком либо из шагов, описанных выше, происходит ошибка, то в журнал записывается сообщение об этой ошибке. Если ошибка не критичная, то мониторинг компьютера продолжится. Если же ошибка критичная, то мониторинг компьютера прекратится.

Также, некоторые очень критичные ошибки (такие как нехватка памяти) могут вызвать остановку исполнения всей задачи.

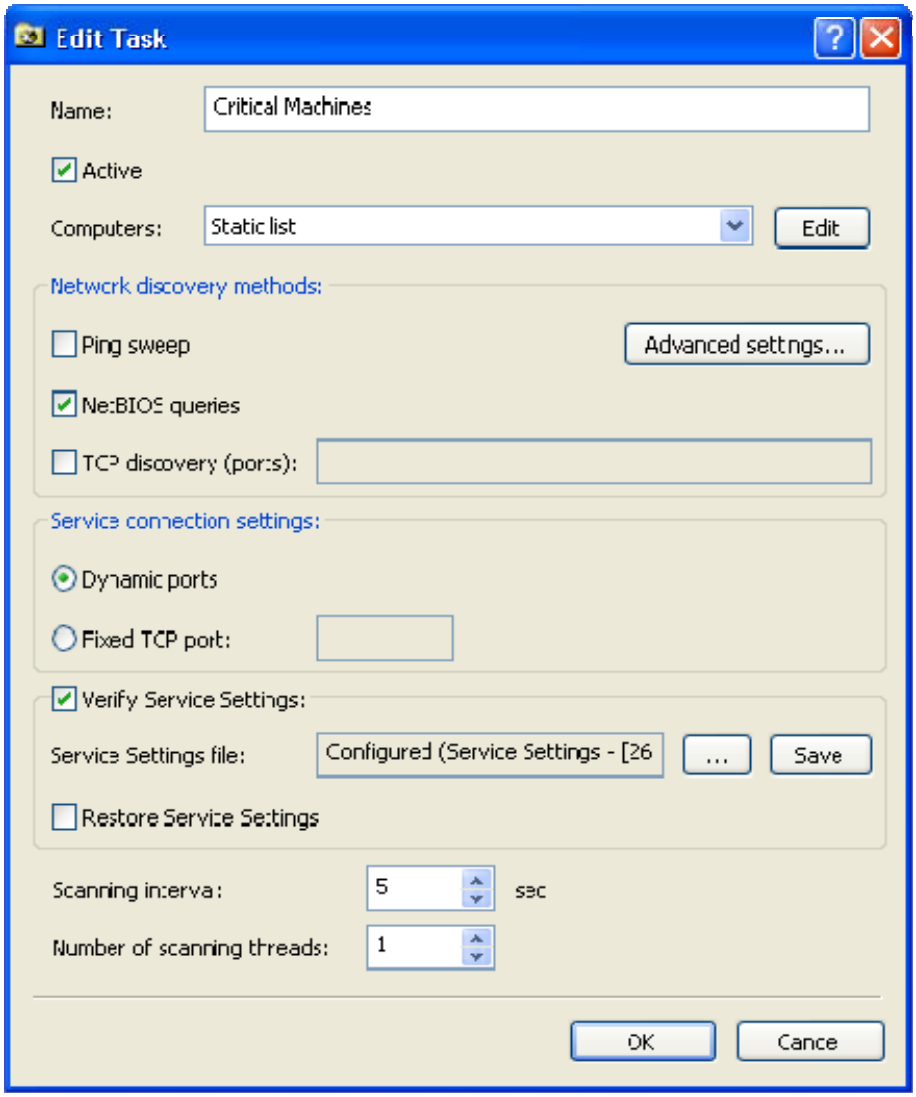
5.5.5.3 Создание / Редактирование задачи

Каждая задача содержит свой собственный список компьютеров и набор настроек.



Чтобы создать новую задачу, используйте *Create Task* из контекстного меню доступного для пункта *Monitoring*. Чтобы отредактировать существующую задачу, используйте *Edit Task* из контекстного меню.

Если вы хотите навсегда удалить задачу, выделите эту задачу в левом дереве и используйте *Delete Task* из контекстного меню.



а. *Name* – название задачи, которое используется для ее идентификации в списке задач и в журнале мониторинга.

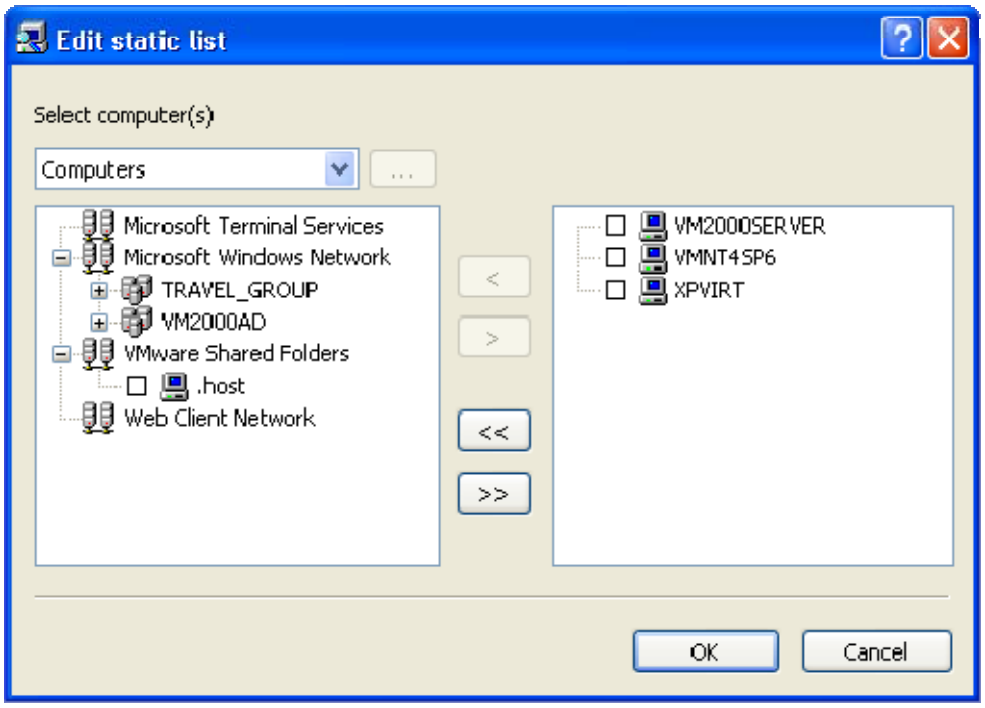
б. *Active* – если флаг установлен, то DeviceLock Enterprise Server будет выполнять задачу. Снимите этот флаг, если вы хотите отключить выполнение данной задачи, но не хотите ее удалять.

в. *Computers* – тип списка компьютеров, используемый для задания компьютеров, которые будут контролироваться данной задачей.

Нажмите на кнопку *Edit*, чтобы сконфигурировать список, выбранный в *Computers*.

Поддерживаются два типа списков компьютеров:

1. *Static list* – все компьютеры задаются в списке по именам и/или IP-адресам. Поскольку этот список статический, то даже если какой-либо компьютер больше не существует в сети, он будет контролироваться задачей, пока запись о нем не будет вручную удалена из этого списка.



Контролируемые компьютеры задаются в правом списке. Вы должны выбрать необходимые компьютеры в левом списке и затем переместить их в правый список путем нажатия на кнопку **>**.

Если вам необходимо исключить некоторые компьютеры из процесса мониторинга, то выделите их в правом списке и нажмите на кнопку **<**.

Используя кнопки **>>** и **<<**, вы можете добавлять и удалять все доступные компьютеры за один раз (не нужно по отдельности выделять компьютеры в списках).

Есть несколько вариантов выбора компьютеров в левом списке:

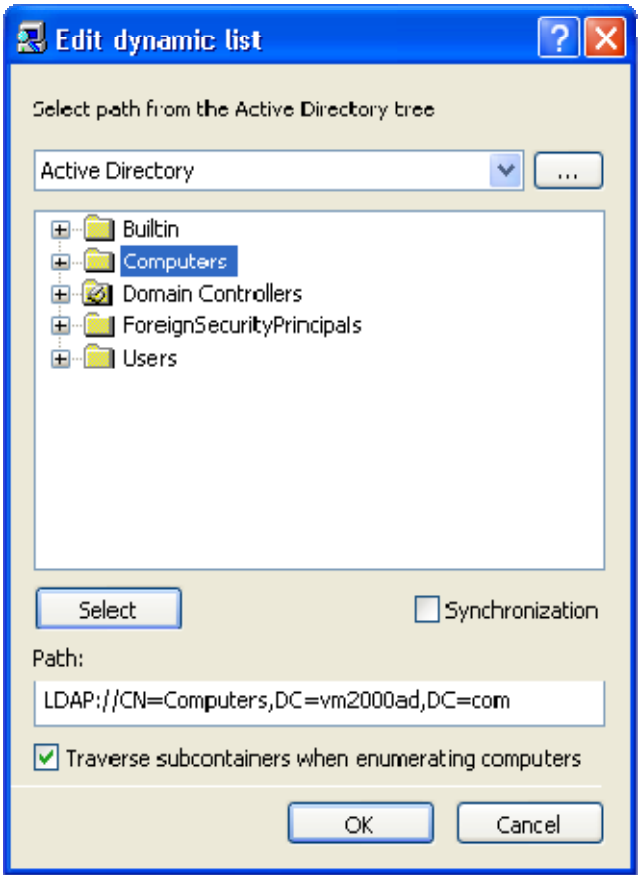
- *Computers* – вы просматриваете дерево сети и выбираете компьютеры.

- *From File* – вы загружаете заранее подготовленный список компьютеров из внешнего текстового файла, а затем выбираете компьютеры. Чтобы открыть внешний файл, нажмите на кнопку **...**. Текстовый файл может содержать имена компьютеров и/или IP-адреса, каждый из которых должен быть записан на отдельной строке, и может быть как в уникод, так и в не уникод кодировке.

- *Manual* – вы вручную вводите компьютеры и затем выбираете их. Имена компьютеров и/или IP-адреса должны быть на отдельных строках.

2. *Dynamic list* – вместо имен компьютеров или IP-адресов, динамический список содержит путь к контейнеру (например, подразделение) в дереве службы каталогов (такой как Active Directory, Novell eDirectory, OpenLDAP и т.п.). Каждый раз в момент выполнения задачи DeviceLock Enterprise Server получает все компьютеры, которые в настоящий момент времени существуют в контейнере. Таким образом, если некоторый компьютер был удален из службы каталогов или был перемещен в другой контейнер, то он не будет более контролироваться задачей. И наоборот, если появился новый компьютер, который не существовал в контейнере на момент создания/редактирования задачи, а был добавлен туда позже, то этот новый компьютер будет контролироваться в момент выполнения задачи.

   ПРИМЕЧАНИЕ: Если DeviceLock Enterprise Server работает на Windows NT4, то для использования динамического списка должен быть установлен компонент "Расширение Active Directory для Windows NT 4.0". Вы можете бесплатно скачать этот компонент с сайта Microsoft: www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=7c219dcc-ec00-4c98-ba61-fd98467952a8



   Путь к контейнеру, из которого DeviceLock Enterprise Server будет получать все компьютеры в момент выполнения задачи, должен быть указан в поле *Path*. Вы должны использовать строку в LDAP-формате.

Вы можете просматривать дерево службы каталогов и выбирать контейнер путем нажатия на кнопку *Select*. В этом случае путь к этому контейнеру будет подставлен в поле *Path* автоматически.

Установите флаг *Traverse subcontainers when enumerating computers*, чтобы разрешить DeviceLock Enterprise Server'у получать компьютеры из всех вложенных контейнеров, находящихся внутри выбранного контейнера. В противном случае, если флаг *Traverse subcontainers when enumerating computers* выключен, то все вложенные контейнеры игнорируются и компьютеры получаются непосредственно только из выбранного контейнера.

Есть два режима работы со службой каталогов:

- *Active Directory* – вы просматриваете дерево Active Directory и выбираете нужный контейнер.

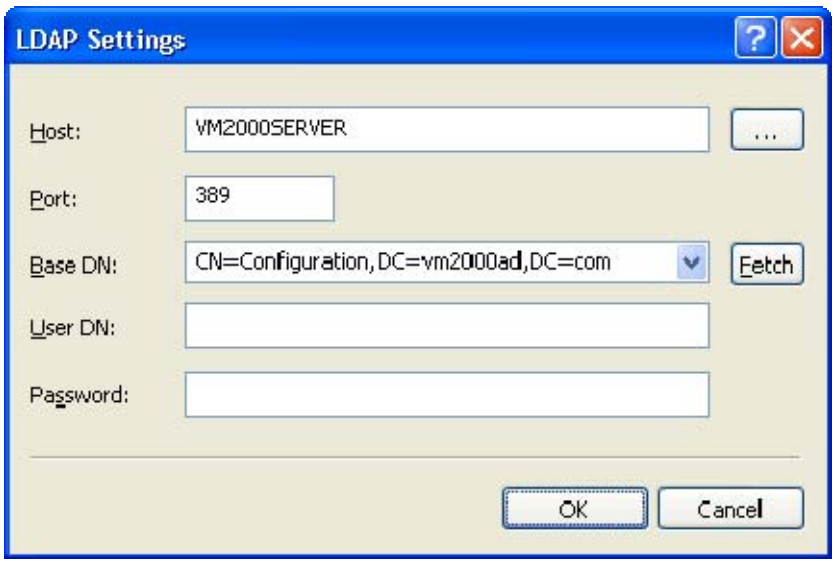
  Несмотря на то, что дерево Active Directory может отображаться и в режиме *LDAP* (см. ниже), мы рекомендуем вам использовать этот специальный режим *Active Directory*, т.к. в этом случае DeviceLock Enterprise Server работает со службой каталогов более эффективно и потребляет меньше ресурсов.

  Если для доступа к Active Directory вам требуется задать данные (пользователь и пароль) альтернативной учетной записи, то нажмите на кнопку **…** и укажите в открывшемся диалоге *Credentials* необходимое имя пользователя и соответствующий ему пароль. ***ПРИМЕЧАНИЕ: Если альтернативная учетная запись не задана, то для доступа к Active Directory используется учетная запись, от имени которой запущена служба DeviceLock Enterprise Server'а. За дополнительной информацией обращайтесь к описанию параметра Log on as.***

  Установите флаг *Synchonization*, чтобы разрешить DeviceLock Enterprise Server'у использовать внутренний механизм синхронизации, предоставляемый Active Directory. Использование данного механизма позволяет значительно снизить нагрузку на контроллер домена и быстрее получать компьютеры в момент выполнения задачи. ***ПРИМЕЧАНИЕ: Чтобы использовать механизм синхронизации, требуется доступ к Active Directory с правами администратора.***

- *LDAP* – вы просматриваете LDAP-дерево (*Lightweight Directory Access Protocol*) и выбираете нужный контейнер.

  Чтобы настроить подключение к LDAP-серверу, нажмите на кнопку **…** и откройте диалог *LDAP Settings*.



- *Host* – имя или IP-адрес LDAP-сервера, к которому выполняется подключение.

- *Port* – номер порта, по котором LDAP-сервер принимает подключения. По умолчанию это порт 389.

- *Base DN* – начальная точка для просмотра дерева каталога. Вы должны использовать строку в LDAP-формате (например, *cn=qa,o=SMARTLINE,c=US*). Оставьте поле *Base DN* пустым для просмотра с корня дерева.

  При нажатии на кнопку *Fetch* вы можете получить все доступные контексты.

- *User DN* – имя пользователя, под которым выполняется подключение к каталогу. Вы должны использовать строку в LDAP-формате (например, *cn=admin,o=SMARTLINE,c=US*).
  ПРИМЕЧАНИЕ: Если имя пользователя не задано, то для доступа к LDAP-серверу используется учетная запись, от имени которой запущена служба DeviceLock Enterprise Server'а. За дополнительной информацией обращайтесь к описанию параметра Log on as.

- *Password* – пароль пользователя.

г. *Network discovery methods* – различные методы сетевого сканирования используемые для определения статусов (*доступен* или *недоступен*) проверяемых компьютеров.

В момент выполнения задачи DeviceLock Enterprise Server использует все выбранные методы сканирования в перечисленном порядке, пока один из них не вернет статус *доступен* для компьютера. Если ни один из методов не вернул статус *доступен*, то данный компьютер получает статус *недоступен*.

Поддерживается три метода сетевого сканирования:

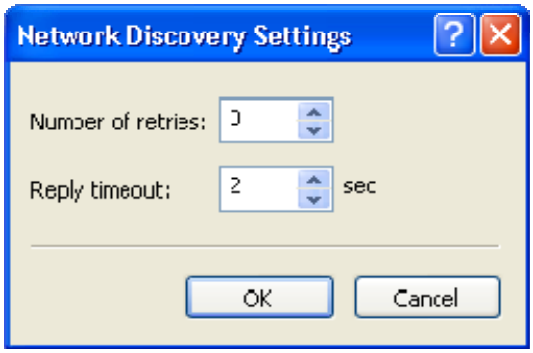
1. *Ping sweep* – DeviceLock Enterprise Server посылает обычный ICMP-пакет (“пинг”) к компьютеру и ждет от него ответа.

2. *NetBIOS queries* – если компонент “*Клиент для сетей Microsoft*” установлен на компьютере, то этот компьютер ответит на NetBIOS-запрос, посланный DeviceLock Enterprise Server’ом.

3. *TCP discovery (ports)* – DeviceLock Enterprise Server проверяет перечисленные TCP-порты на компьютере и ищет первый открытый порт. Используя запятую (,) или точку с запятой (;) в качестве разделителя, вы можете указать несколько портов одновременно.

ПРИМЕЧАНИЕ: Если на компьютере используется какой-либо файрвол, то он может блокировать отсылку некоторых или всех сетевых пакетов. В таком случае данный компьютер получит статус недоступен, даже если он на самом деле включен и работает.

Чтобы задать дополнительные параметры сканирования, нажмите на кнопку *Advanced settings* и откройте диалог *Network Discovery Settings*.



- *Number of retries* – определяет, какое количество раз DeviceLock Enterprise Server будет повторно выполнять каждый метод сканирования, когда он возвращает статус *недоступен*. 0 – означает, что повторных попыток сканирования этим же методом предприниматься не будет (для данного компьютера в данный момент выполнения задачи).

- *Reply timeout* – время в секундах, в течении которого DeviceLock Enterprise Server ожидает ответ от компьютера для каждого метода сканирования. Если DeviceLock Enterprise Server работает в медленной или в загруженной сети, то вам, возможно, будет нужно увеличить это значение.

д. *Service connection settings* – эти параметры определяют как DeviceLock Enterprise Server должен подключаться к DeviceLock Service’ам, работающим на контролируемых компьютерах для получения номера версии, настроек и т.п. Если параметры соединения заданы неправильно, то DeviceLock Enterprise Server не сможет подключиться к сервисам и компьютеры, на которых они работают не получат статус *доступен*.

DeviceLock Service может быть настроен на использование либо фиксированного порта, либо динамических портов. За дополнительной информацией обращайтесь к разделам **Установка без вмешательства пользователя** и **Установка в DeviceLock Enterprise Manager** данного руководства.

Есть два способа подключения:

- *Dynamic ports* – для использования DeviceLock Enterprise Server'ом динамических портов при подключении к DeviceLock Service'ам выберите эту опцию.

- *Fixed TCP port* – если DeviceLock Service'ы настроены на использование фиксированного TCP-порта, то вы должны выбрать эту опцию и указать номер порта.

ПРИМЕЧАНИЕ: Чтобы успешно подключаться к контролируемым сервисам и получать необходимую информацию от них, DeviceLock Enterprise Server должен обладать как минимум правом доступа только на чтение (Read-only) к этим сервисам. Если данная задача также должна перезаписывать настройки (политики) на контролируемых сервисах, то DeviceLock Enterprise Server должен обладать правом полного доступа (Full access) к этим сервисам.

Для подключения к контролируемым DeviceLock Service'ам используется учетная запись, от имени которой запущена служба DeviceLock Enterprise Server'а. Если секретный ключ установлен, то DeviceLock Enterprise Server может использовать авторизацию по сертификату. За дополнительной информацией обращайтесь к описанию параметров Log on as и Certificate Name.

e. *Verify Service Settings* – установите этот флаг, если вы хотите проверять целостность политик DeviceLock Service'ов на контролируемых компьютерах.

- *Service Settings file* – чтобы назначить задаче эталонную политику, вы должны загрузить настройки сервиса из внешнего XML-файла (файл эталонной политики). Этот файл эталонной политики может быть создан в DeviceLock Service Settings Editor'е, DeviceLock Management Console или в DeviceLock Group Policy Manager'е.

  В процессе проверки целостности DeviceLock Enterprise Server получает политики из контролируемых DeviceLock Service'ов и сравнивает их с эталонной политикой, присвоенной данной задаче.

  Все неопределенные параметры (те, у которых состояние "не определен") в эталонной политике игнорируются в процессе проверки целостности. Используя эту особенность, вы можете контролировать целостность только отдельных настроек (самых важных) и при этом позволить изменять остальные параметры без записи уведомления в журнал мониторинга.

  Чтобы загрузить файл эталонной политики, нажмите на кнопку **…**. Поскольку на данном шаге цифровая подпись не проверяется, этот файл

может быть как подписанным, так и неподписанным. Тем не менее, если вы загружаете подписанный файл, то его имя будет отображаться в поле *Service Settings file* в круглых скобках.

Если вы редактируете задачу и эталонная политика уже назначена ей, вы можете экспортировать эту политику во внешний XML-файл, путем нажатия на кнопку *Save*.

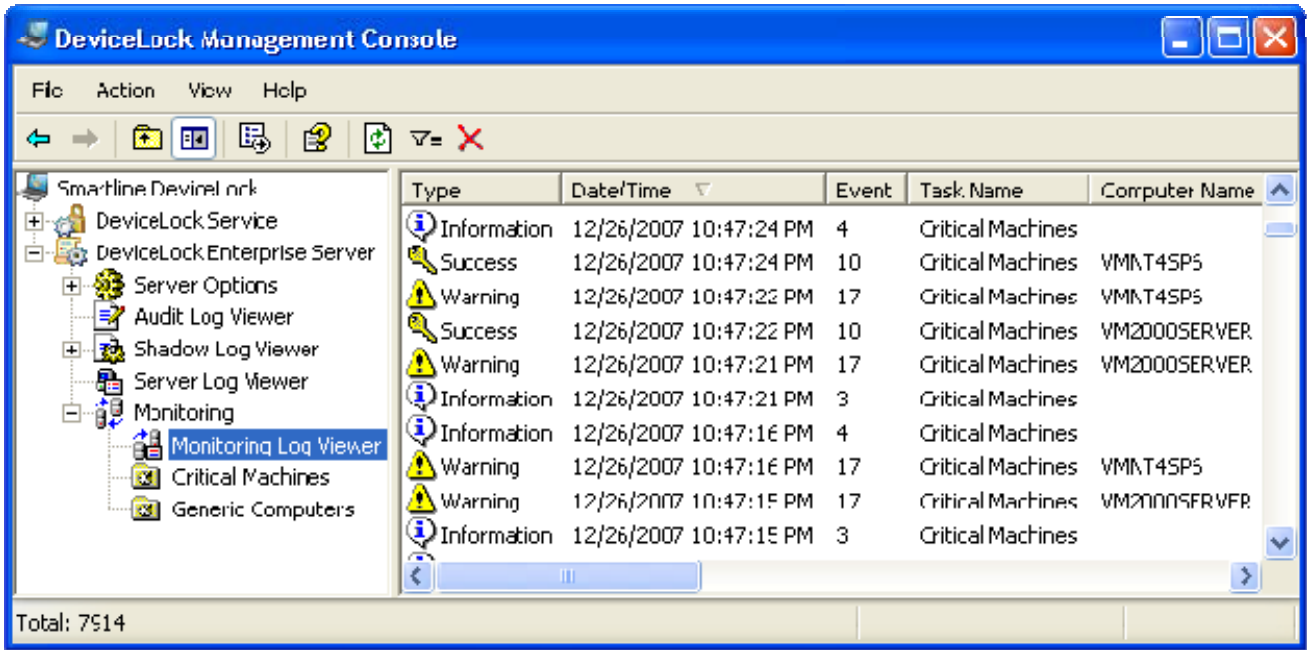
- *Restore Service Settings* – установите этот флаг, если вы хотите позволить DeviceLock Enterprise Server'у восстанавливать измененную политику на эталонную у контролируемых DeviceLock Service'ов для которых в процессе проверки целостности было выявлено расхождение политик. Используя эту функцию, вы можете не только пассивно мониторить целостность отдельных настроек, но и восстанавливать оригинальные значения настроек в случае их изменения.

ж. *Scanning interval* – время в секундах, которое должно пройти после окончания выполнения задачи и перед началом выполнения этой же задачи снова.

з. *Number of scanning threads* – максимальное количество потоков, которое может быть задействовано данной задачей в процессе своего выполнения. Вы можете увеличить это значение, чтобы распараллелить процесс сканирования компьютеров. Тем не менее, большее число потоков требует большего количества ресурсов (особенного памяти и сетевого трафика) для DeviceLock Enterprise Server'а.

5.5.5.4 Monitoring Log Viewer

Этот встроенный просмотрщик позволяет получить список записей из журнала мониторинга. Журнал мониторинга используется задачами для записи информации о контролируемых ими компьютерах и DeviceLock Service'ах.



Столбцы просмотрщика определены следующим образом:

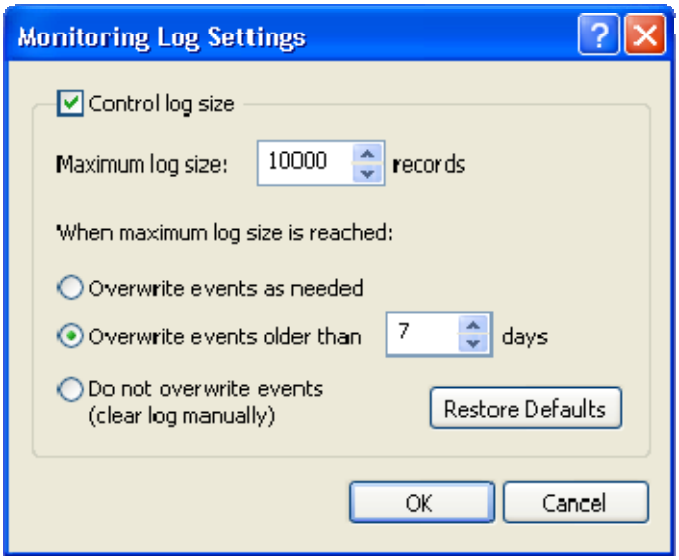
- *Type* – класс события: *Success*, *Information*, *Warning* или *Error*.
- *Date/Time* – дата и время, когда событие произошло.
- *Event* – номер идентифицирующий событие.
- *Task Name* – название задачи ответственной за это событие. Может быть пустым, если событие не связано с задачей.
- *Computer Name* – имя компьютера, принадлежащего задаче, которая ответственна за это событие. Может быть пустым, если событие не связано с компьютером.
- *Information* – иная, специфичная для данного события информация, такая как описание ошибки, предупреждение и т.п.
- *Server* – имя сервера, где событие произошло.
- *Record N* – номер записи.

Чтобы обновить список, используйте *Refresh* из контекстного меню или соответствующую кнопку на инструментальной панели.

Чтобы полностью очистить этот журнал, используйте *Clear* из контекстного меню или соответствующую кнопку на инструментальной панели.

5.5.5.2.1 Настройки журнала мониторинга

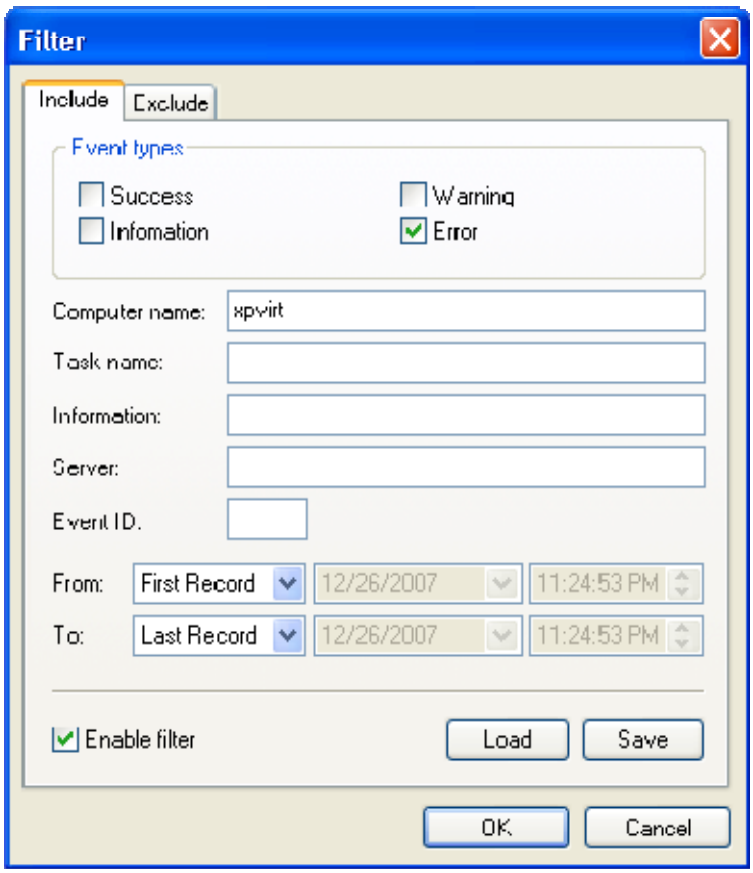
Чтобы определить максимальный размер журнала мониторинга и действия DeviceLock Enterprise Server'а в случае его заполнения, используйте *Settings* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе Monitoring Log Viewer.



Все эти настройки подробно описаны в разделе **Настройки журнала аудита (для сервера)** данного руководства.

5.5.5.2.2 Фильтр журнала мониторинга

Вы можете фильтровать данные в Monitoring Log Viewer так чтобы только записи, удовлетворяющие заданным условиям, выводились в список.



Чтобы открыть диалог *Filter*, используйте *Filter* из контекстного меню, доступного по нажатию правой кнопки мыши на элементе *Monitoring Log Viewer* или соответствующую кнопку на инструментальной панели.

Разница между заданием фильтра для журнала аудита и журнала мониторинга незначительна, поэтому рекомендуем прочитать раздел **Фильтр журнала аудита** данного руководства.

Когда фильтр включен, вы можете определить условия фильтрации, задав необходимые значения в следующих полях:

- *Success* – флаг, определяющий нужно ли фильтровать записи по классу *Success*.

- *Information* – флаг, определяющий нужно ли фильтровать записи по классу *Information*.

- *Warning* – флаг, определяющий нужно ли фильтровать записи по классу *Warning*.

- *Error* – флаг, определяющий нужно ли фильтровать записи по классу *Error*.

- *Computer Name* – текст, соответствующий значению столбца *Computer Name* в Monitoring Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Task Name* – текст, соответствующий значению столбца *Task Name* в Monitoring Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Information* – текст, соответствующий значению столбца *Information* в Monitoring Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Server* – текст, соответствующий значению столбца *Server* в Monitoring Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски.

- *Event ID* – число, соответствующее значению столбца *Event* в Monitoring Log Viewer.

- *From* – определяет начало временного интервала событий, которые вы хотите фильтровать. Выберите *First Event,* чтобы фильтровать события, начиная с самого первого в журнале. Выберите *Events On*, чтобы фильтровать события, начиная с определенной даты и времени.

- *To* – определяет конец временного интервала событий, которые вы хотите фильтровать. Выберите *Last Event*, чтобы фильтровать события, заканчивая самым последним событием в журнале. Выберите *Events On,* чтобы фильтровать события, заканчивая событием с определенной датой и временем.

6 DeviceLock Group Policy Manager

6.1 Общая информация

В дополнение к стандартным возможностям управления настройками через DeviceLock Management Console, DeviceLock обеспечивает вас и более мощным механизмом – разрешения, правила аудита и настройки могут быть изменены и применены с использованием групповых политик службы управления каталогами Active Directory.

Поддержка групповых политик в DeviceLock делает возможным администрирование на основе политик домена, используемых в Active Directory. Политики создаются с использованием оснастки *Group Policy* для MMC. Системные администраторы могут использовать политики для контроля настроек с единого рабочего места. Глубокая интеграция в Active Directory – важная особенность DeviceLock. Она упрощает развертывание в больших сетях и более удобна для системных администраторов.

Интеграция в Active Directory исключает необходимость установки дополнительных приложений для централизованного управления и развертывания. DeviceLock не требует своей собственной серверной версии для контроля всей сети, вместо этого используется стандартная функция, предоставляемая Active Directory.

Посредством групповой политики можно:

- Установить DeviceLock Service на всех компьютерах локальной сети, даже на те, которые в данный момент не работают или только подключаются к сети.

  Чтобы получить дополнительную информацию, обратитесь к разделу **Установка через групповые политики Active Directory** данного руководства.

- Контролировать и конфигурировать DeviceLock Service на большом количестве компьютеров в различных доменах/подразделениях одновременно.

  Даже если какие-то компьютеры в данный момент не работают или еще не подключены к сети, вы можете автоматически установить на них предопределенные настройки DeviceLock.

- Просматривать применяемую и результирующую политики.

  Чтобы получить дополнительную информацию, обратитесь к разделу **Использование Resultant Set of Policy (RSoP)** данного руководства.

ПРИМЕЧАНИЕ: Для управления DeviceLock посредством групповых политик вы должны предварительно установить и должным образом настроить Active Directory. Для более полной информации об установке и настройке Active Directory обращайтесь, пожалуйста, к соответствующей документации Microsoft.

6.2 Применение групповых политик

Политики обновляются при запуске компьютера. Когда пользователь включает компьютер, система применяет политику для DeviceLock.

Опционально политики могут обновляться на периодической основе. По умолчанию политика обновляется каждые 90 минут. Чтобы задать другой интервал, через который политика будет обновляться, используйте *Group Policy Object Editor*. Более подробно об этом читайте в базе знаний Microsoft: http://support.microsoft.com/default.aspx?scid=kb;en-us;203607

Политики также могут быть обновлены по требованию. Для немедленного обновления текущих политик на Windows XP или более поздних системах, администратор может вызвать утилиту командной строки: *gpupdate.exe /force,* предоставляемую Microsoft. В операционной системе Windows 2000 администратор может вызвать другую утилиту командной строки, предлагаемую Microsoft: *secedit /refreshpolicy machine_policy /enforce*.

При обновлении политики система запрашивает у Active Directory список объектов групповой политики (GPO). Каждый объект групповой политики связан с контейнером службы управления каталогами, которому принадлежит компьютер. Компьютер получает установки последнего обработанного контейнера службы управления каталогами Active Directory. Обрабатывая объекты групповой политики, система проверяет список управления доступом (ACL), связанный с каждым объектом. Если запись управления доступом (ACE) запрещает доступ компьютера к объекту групповой политики, система не применит политики, определенные в этом объекте. Если запись управления доступом дает доступ к объекту, система применяет политики этого объекта.

6.3 Стандартные правила наследования политик

Любые неопределенные (незаданные) настройки в объекте политики игнорируются, поскольку они не наследуются вниз по дереву. Только определенные (заданные) настройки наследуются. Есть три возможных сценария:

- Если объект политики содержит настройки, определенные (заданные) для родительской записи, и те же настройки не определены (не заданы) для записи потомка, то потомок наследует все настройки от родителя.
- Если объект политики содержит настройки, определенные (заданные) для родительской записи, и они не конфликтуют с настройками, определенными (заданными) для записи потомка, то потомок наследует эти настройки от родителя и также применяет свои собственные настройки.

- Если объект политики содержит настройки, определенные (заданные) для родительской записи, которые конфликтуют с настройками, определенными (заданными) для записи потомка, то потомок не наследует эти настройки от родителя, а применяет свои собственные настройки. Т.е. в этом случае настройки потомка имеют приоритет над настройками родителя.

6.4 Запуск DeviceLock Group Policy Manager

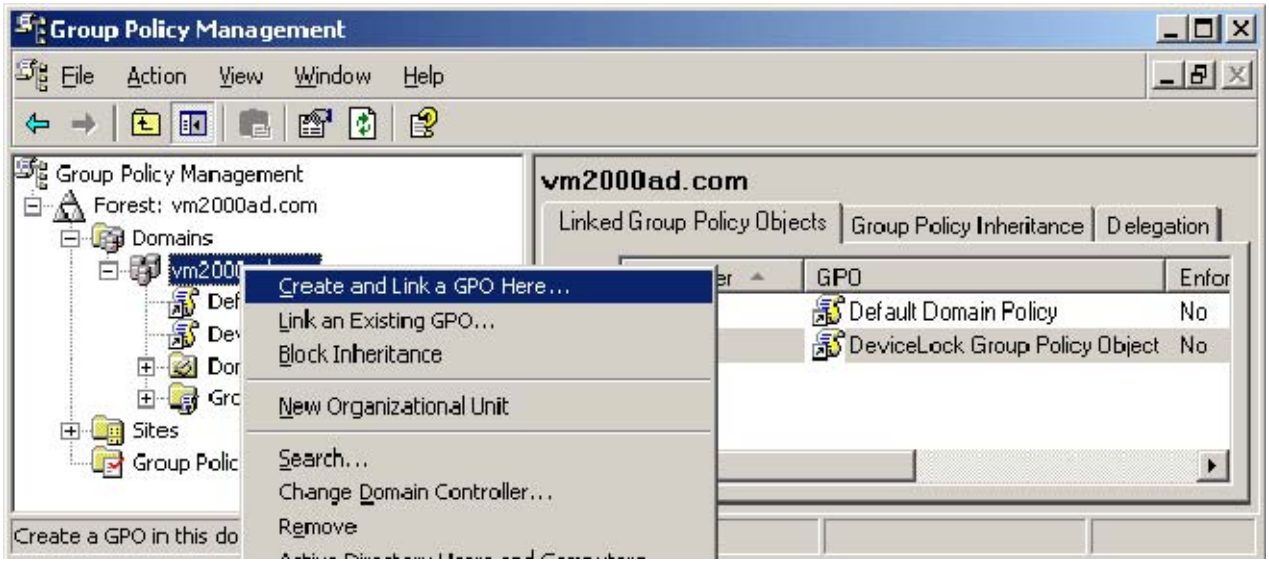
DeviceLock Group Policy Manager интегрируется в редактор групповых политик Windows и не доступен как отдельное приложение. Чтобы использовать DeviceLock Group Policy Manager на вашем локальном компьютере, а не на контроллере домена, на ваш компьютер необходимо установить редактор групповых политик. Для Windows XP/2003 мы рекомендуем использовать Group Policy Management Console (GPMC). GPMC доступен для свободного скачивания с сайта Microsoft: http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.

Чтобы использовать DeviceLock Group Policy Manager, сначала вы должны запустить стандартный редактор групповых политик:

1. Запустите оснастку *Group Policy Management*.

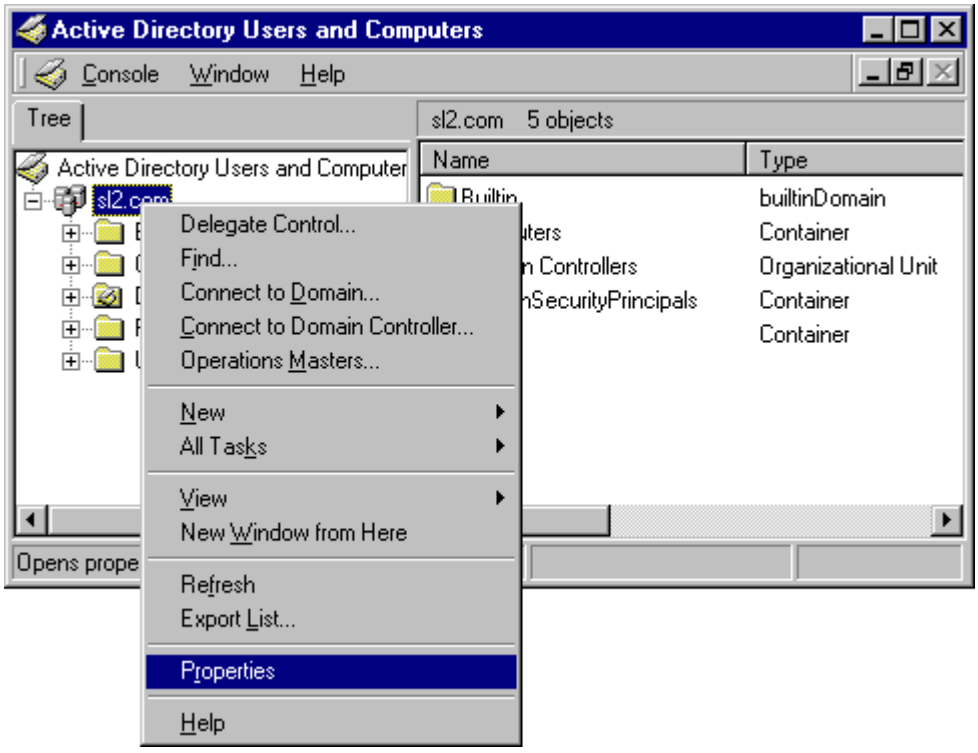
   Если оснастка *Group Policy Management* не установлена на вашем компьютере, вы можете использовать оснастку *Active Directory Users and Computers*.

2. Выберите необходимый домен в дереве консоли.

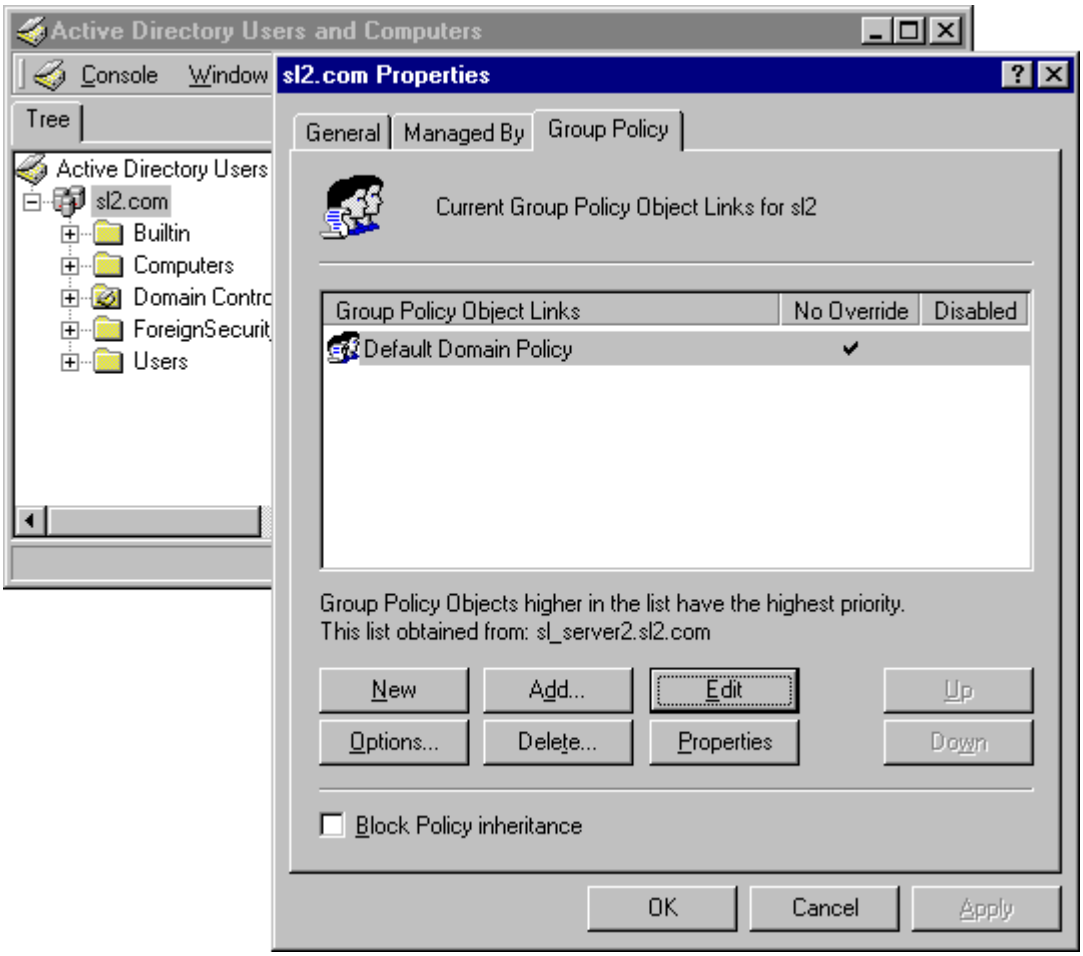


3. Выберите нужный объект групповой политики и затем кликните *Edit* в контекстном меню, доступном по нажатию правой кнопки мыши. Если вы хотите создать новый объект политики, кликните *Create and Link a GPO Here* в контекстном меню домена.

Если вы используете оснастку *Active Directory Users and Computers*, то в дереве консоли кликните правой кнопкой на домене и кликните на *Properties*.



Кликните на вкладке *Group Policy*, выберите нужный объект групповой политики и затем нажмите на кнопку *Edit*. Если вы хотите создать новый объект, нажмите на кнопку *New*.



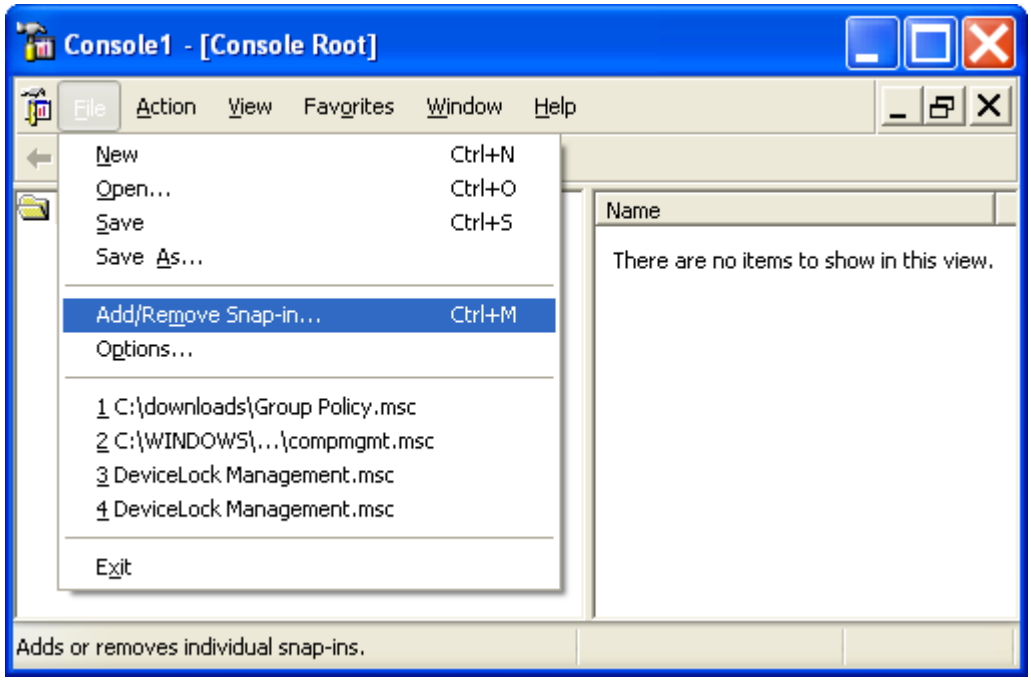
4. Подождите, пока редактор групповой политики запустится. Это может занять какое-то время.

5. В разделе *Computer Configuration* выберите пункт *DeviceLock*.

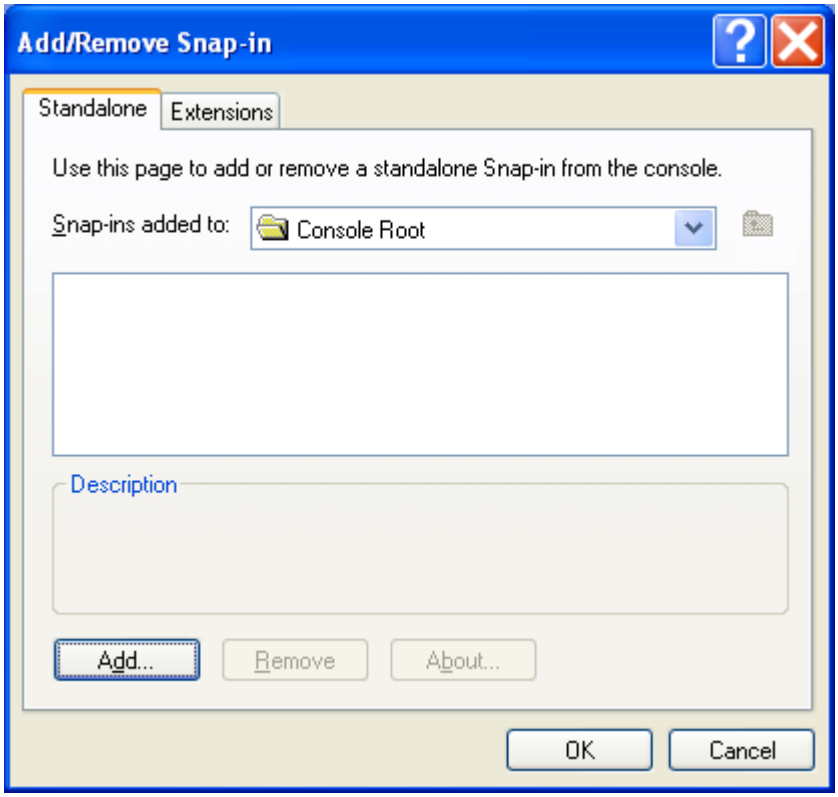
Кроме того, вы можете запустить MMC и добавить оснастку *Group Policy* вручную:

1. Запустите *mmc* из командной строки или используйте меню *Run* для выполнения этой команды.

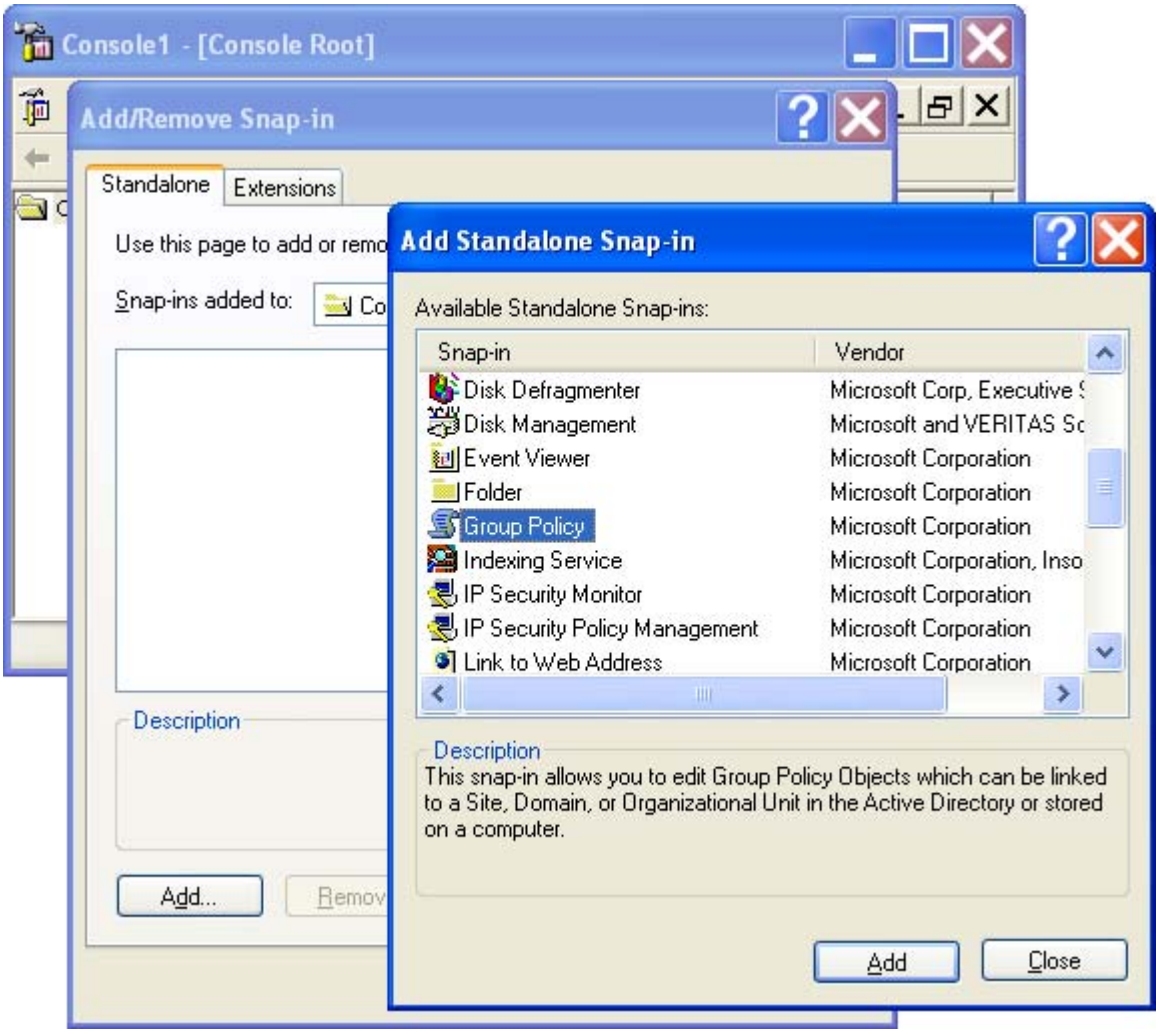
2. Откройте меню *File*, затем кликните *Add/Remove snap-in*.



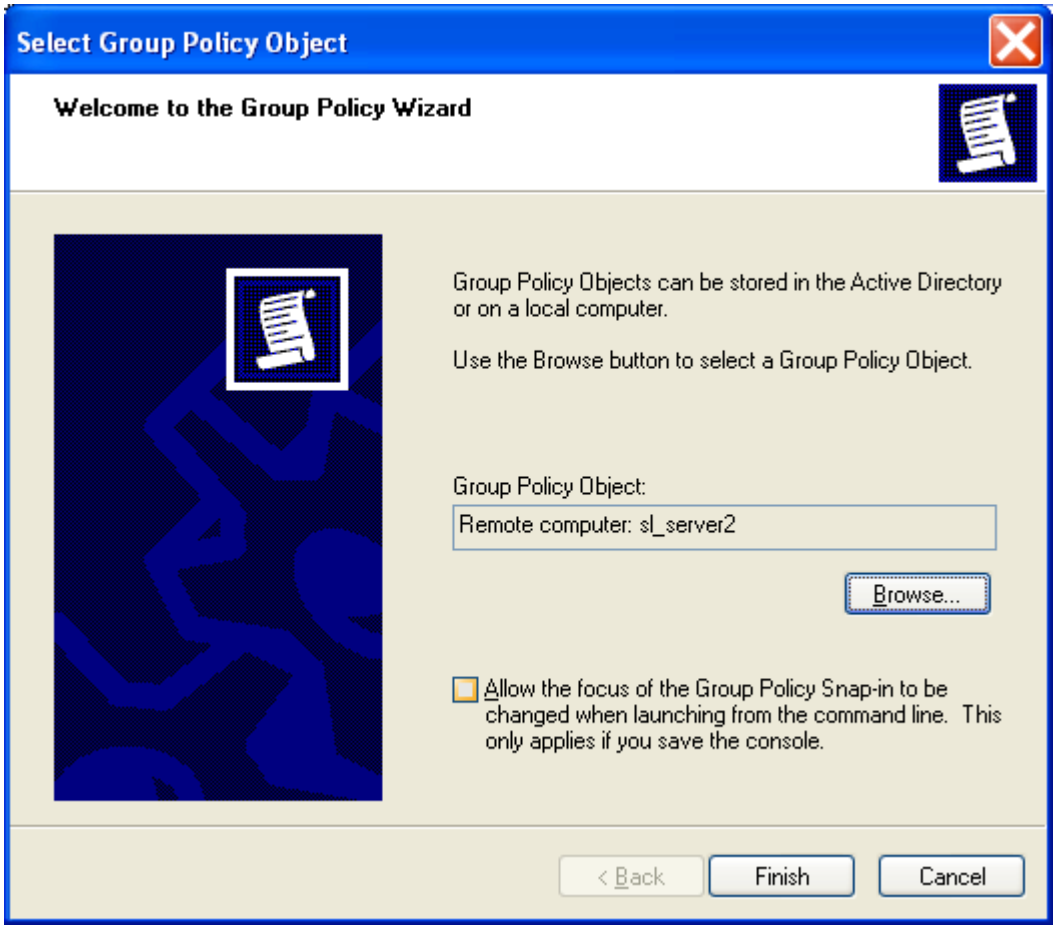
3. Кликните на вкладку *Standalone*, затем нажмите *Add*.



4. Выберите из списка оснастку *Group Policy* и нажмите *Add*.



5. Выберите объект групповой политики либо из Active Directory, либо из локального компьютера, затем нажмите на *Finish*.



6. Нажмите *Close*, чтобы закрыть окно *Add Standalone Snap-in*.

7. Кликните *OK*, чтобы добавить оснастку.

8. В разделе *Computer Configuration* выберите пункт *DeviceLock*.

6.5 Использование DeviceLock Group Policy Manager

Разница между администрированием через DeviceLock Management Console и DeviceLock Group Policy Manager незначительна, поэтому рекомендуем прочитать раздел **Администрирование DeviceLock Service** данного руководства.

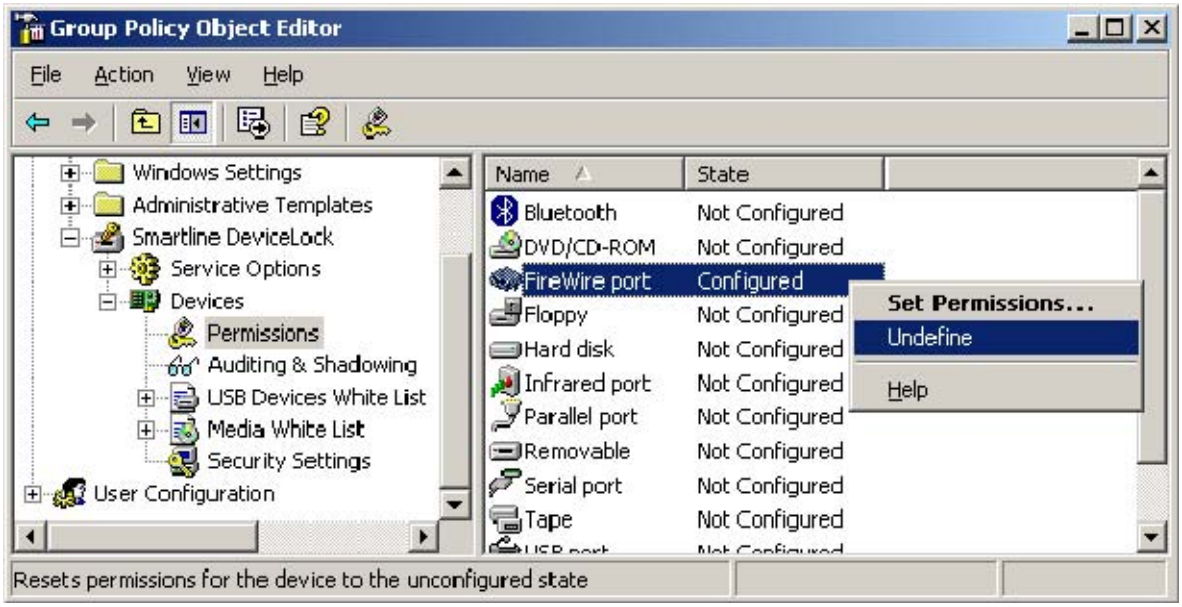
Используя DeviceLock Group Policy Manager, невозможно управлять DeviceLock Enterprise Server'ом и просматривать журналы. Для этих операций вы должны использовать DeviceLock Management Console.

По сравнению с DeviceLock Management Console, DeviceLock Group Policy Manager имеет три дополнительные функции:

a. **Override Local Policy** – если вы хотите запретить изменение настроек не через групповые политики, установите флаг *Override Local Policy* в разделе *Service Options*. Это принудительно включит режим групповой политики для всех компьютеров, входящих в объект групповой политики.

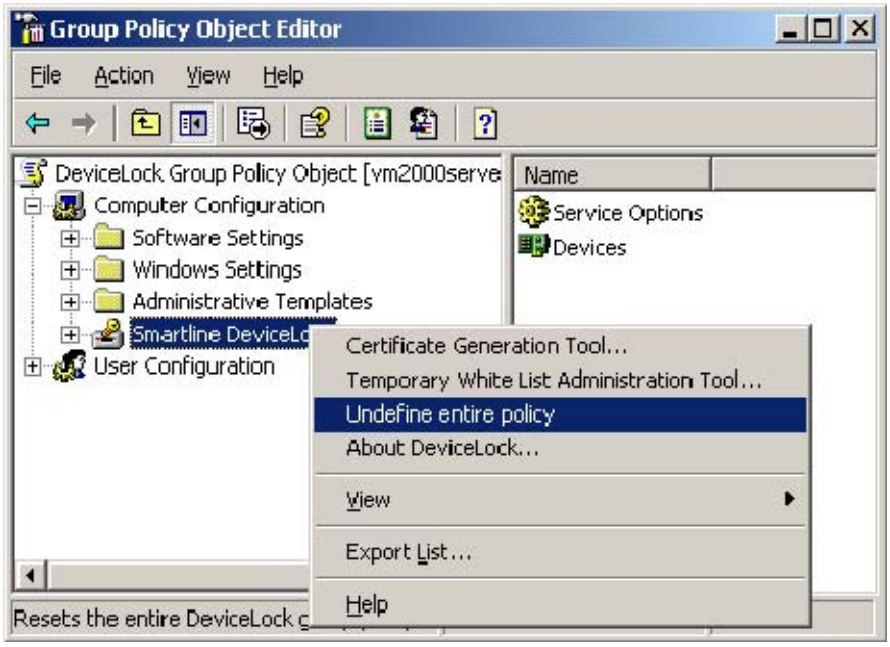
Если флаг *Override Local Policy* установлен, это означает, что флаг *Use Group Policy* в *Service Options* у DeviceLock Management Console и DeviceLock Enterprise Manager не может быть включен.

б. **Undefine** – вы можете установить любой параметр в состояние "не определен". Все неопределенные (незаданные) параметры игнорируются в объекте групповой политики. За дополнительной информацией, обращайтесь к разделу **Стандартные правила наследования политик** данного руководства.



Используйте *Undefine* из контекстного меню, доступного по нажатию правой кнопки мыши на любом параметре. Также в некоторых диалогах вы можете использовать промежуточное (серое) состояние флага, чтобы установить ему состояние “не определен”.

в. **Undefine entire policy** – вы можете установить все параметры в состояние “не определен” одним кликом мыши.



Используйте *Undefine entire policy* из контекстного меню, доступного по нажатию правой кнопки мыши на корневом элементе *DeviceLock*.

ПРИМЕЧАНИЕ: Для того, чтобы управлять настройками DeviceLock Service через групповые политики, сам DeviceLock Service должен быть установлен и запущен на всех компьютерах, входящих в объект групповой политики. Дополнительную информацию относительно установки агентов вы можете найти в разделе Развертывание DeviceLock Service данного руководства.

Также не забудьте, что групповая политика обновляется периодически (по умолчанию, каждые 90 минут), следовательно, ваши изменения не вступят в силу немедленно. Чтобы получить дополнительную информацию, обратитесь к разделу Применение групповых политик данного руководства.

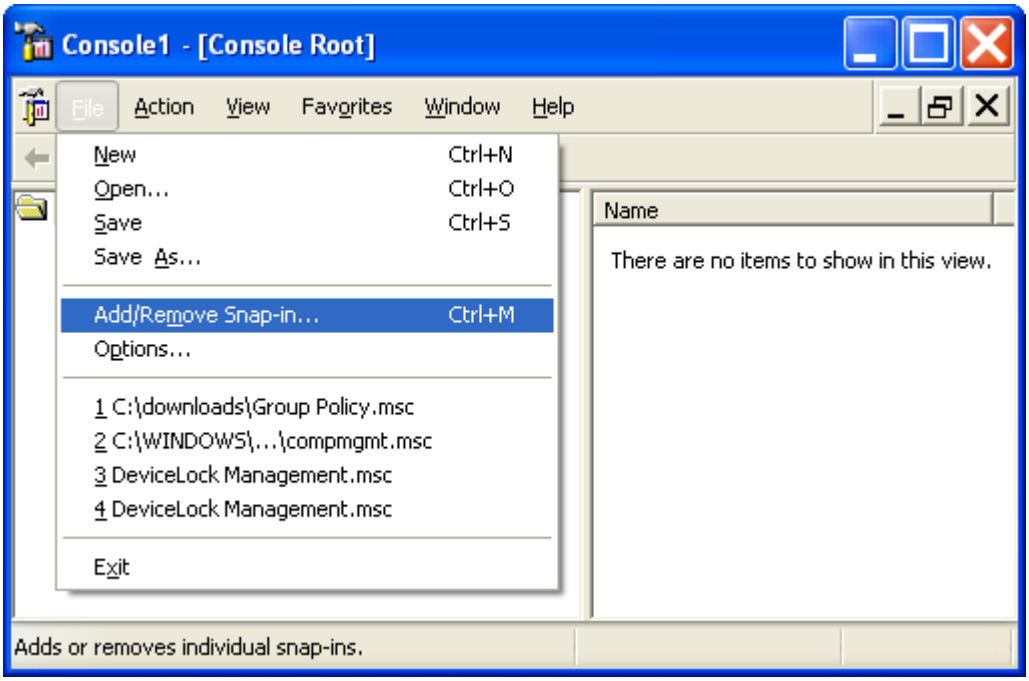
6.6 Использование Resultant Set of Policy (RSoP)

DeviceLock поддерживает Resultant Set of Policy (RSoP). Вы можете использовать стандартную оснастку Windows RSoP для просмотра актуально применяемой политики DeviceLock и для проверки результирующей политики, которая будет применена в заданной ситуации.

Чтобы использовать RSoP, вы должны запустить MMC и добавить оснастку *Resultant Set of Policy* вручную:

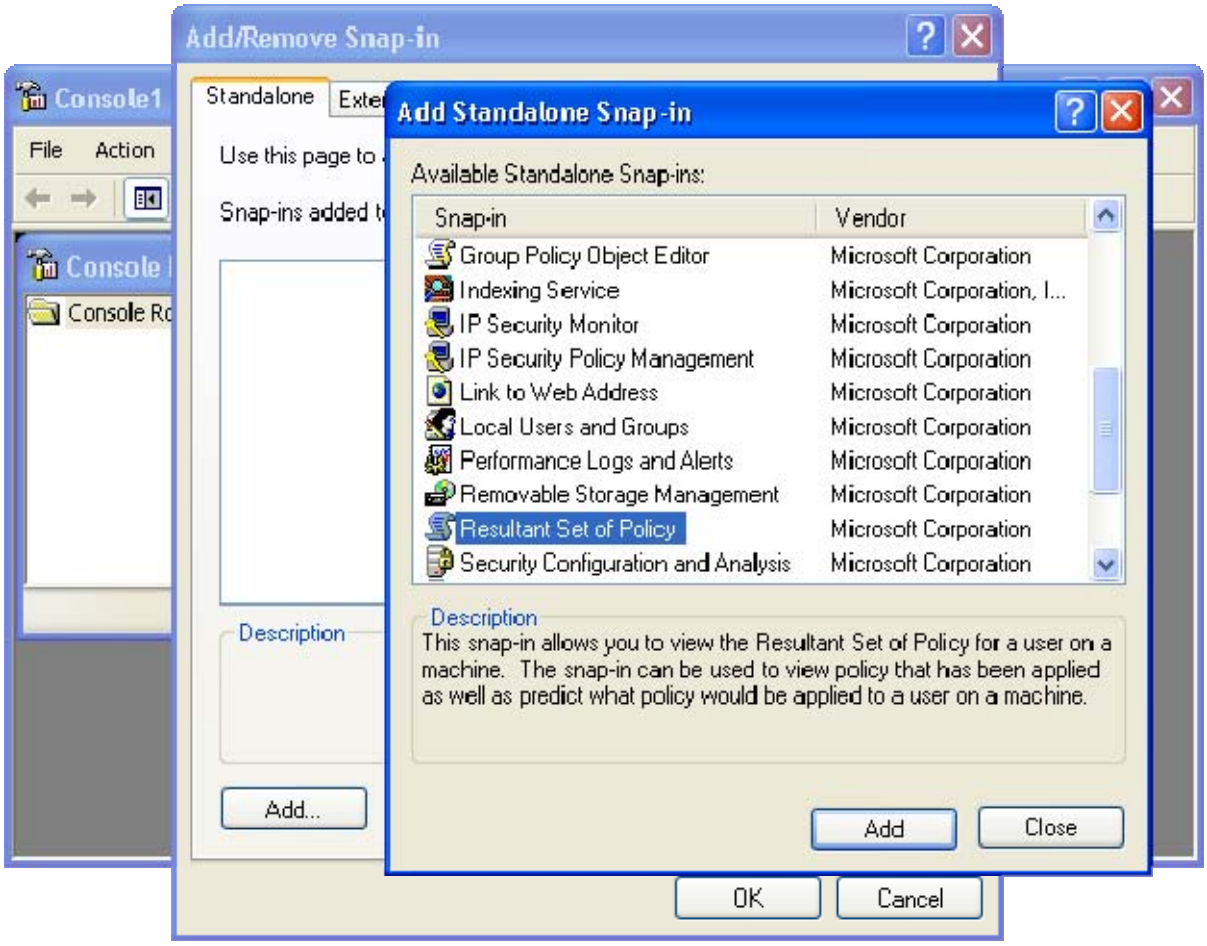
1. Запустите *mmc* из командной строки или используйте меню *Run* для выполнения этой команды.

2. Откройте меню *File*, затем кликните *Add/Remove snap-in*.



3. Кликните на вкладку *Standalone*, затем нажмите *Add*.

4. Выберите из списка оснастку *Resultant Set of Policy* и нажмите.



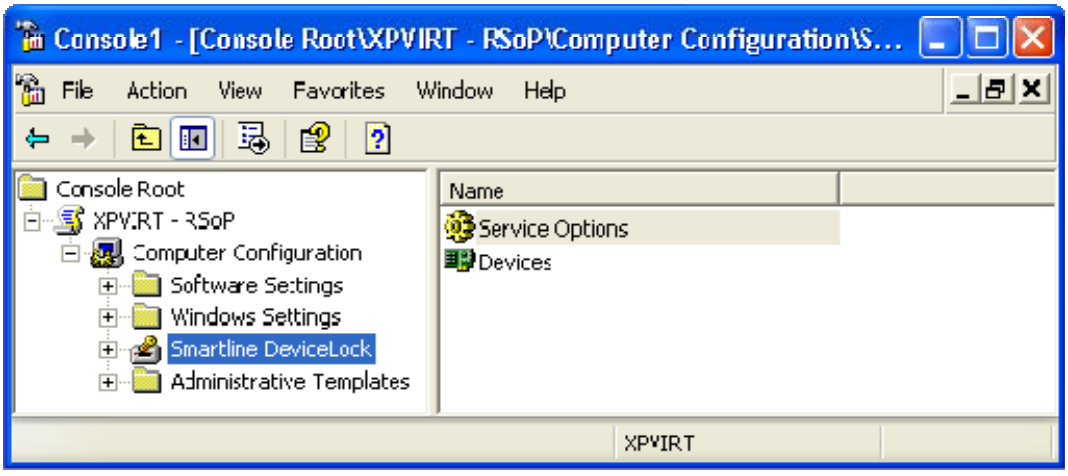
5. Нажмите *Close*, чтобы закрыть окно *Add Standalone Snap-in* и затем кликните *OK*, чтобы добавить оснастку.

6. В дереве консоли выберите *Resultant Set of Policy*.

7. Выберите пункт *Generate RSoP Data* из контекстного меню.

8. Пройдите через все страницы мастера *Resultant Set of Policy*, чтобы собрать информацию с выбранного компьютера.

9. В разделе *Computer Configuration* выберите пункт *DeviceLock*.



Пожалуйста, имейте в виду, что, используя RSoP, вы не можете изменять политики – все настройки доступны только для просмотра.

RSoP очень полезен для понимания того, какой конкретно объект групповой политики (GPO) применяется или будет применен для выбранного компьютера.

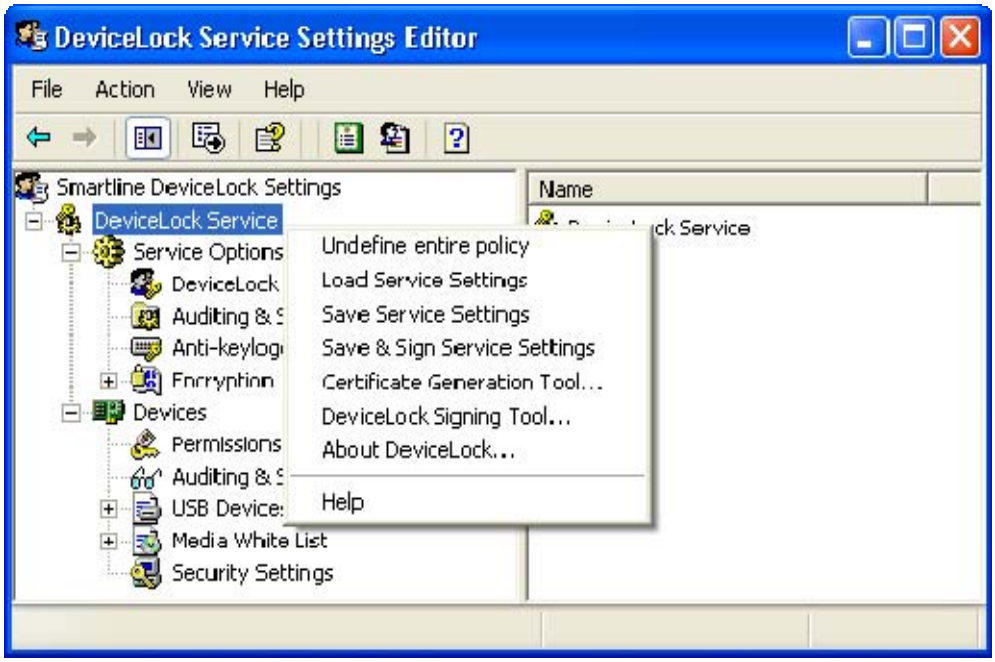
За дополнительной информацией относительно Resultant Set of Policy обратитесь к базе знаний Microsoft: http://technet2.microsoft.com/WindowsServer/en/library/1180b465-ea3b-4a73-8670-81fa5871a3c71033.mspx?mfr=true.

7 DeviceLock Service Settings Editor

7.1 Общая информация

Редактор настроек сервиса (DeviceLock Service Settings Editor) используется для создания и редактирования внешних XML-файлов с настройками, разрешениями, правилами аудита и теневого копирования.

DeviceLock Service Settings Editor устанавливается вместе с остальными консолями управления DeviceLock.



Разница между процедурой задания политик в DeviceLock Management Console и DeviceLock Service Settings Editor'е незначительна, поэтому рекомендуем прочитать раздел **Администрирование DeviceLock Service** данного руководства.

В DeviceLock Service Settings Editor'е по сравнению с DeviceLock Management Console:

- Не требуется подключаться к клиентским компьютерам, т.к. эта консоль работает с внешним XML-файлом, а не с отдельным компьютером. Все настройки редактируются и сохраняются непосредственно на локальном компьютере. Это похоже на то, как работает DeviceLock Group Policy Manager, но в отличие от объектов групповой политики используются XML-файлы.

- Вы можете установить любой параметр (или все параметры сразу) в состояние "не определен". Все неопределенные (незаданные) параметры игнорируются, когда политика применяется DeviceLock Service'ом.

Чтобы создать новую политику “с нуля”, запустите DeviceLock Service Settings Editor и вносите необходимые изменения в его чистую политику по умолчанию.

Если вы хотите отредактировать существующую политику, то загрузите XML-файл с этой политикой в редактор используя *Load Service Settings* из контекстного меню и вносите в нее необходимые изменения.

Чтобы сохранить изменения, которые вы внесли в редактируемую политику, вам в любом случае необходимо использовать *Save Service Settings* из контекстного меню. Вы также можете использовать *Save & Sign Service Settings* из контекстного меню для сохранения политики во внешний XML-файл и автоматического подписывания этого файла с использованием последнего использованного сертификата (*секретного* ключа). Пункт меню *Save & Sign Service Settings* недоступен, если в программе DeviceLock Signing Tool никогда не использовался *секретный* ключ.

Позже файлы с политиками, созданные в DeviceLock Service Settings Editor’е могут быть загружены с помощью DeviceLock Management Console и/или DeviceLock Group Policy Manager’а.

Также файлы с политиками могут быть посланы пользователям, чьи компьютеры не подключены к сети и находятся вне досягаемости консолей управления. Для предотвращения неавторизованных изменений вы должны подписывать такие XML-файлы при помощи цифровой подписи, используя программу DeviceLock Signing Tool и сертификат (*секретный* ключ). За дополнительной информацией обращайтесь к разделу **Service Settings** данного руководства.

DeviceLock Service Settings Editor также используется модулем *Set Service Settings* в DeviceLock Enterprise Manager'е. Этот модуль запускает DeviceLock Service Settings Editor как внешнее приложение и загружает в него XML-файл, выбранный в диалоге настройки модуля.

Если вы вносите изменения в XML-файл, открытый на редактирование модулем *Set Service Settings*, редактор автоматически сохраняет все ваши изменения в этот файл. Когда вы закончите редактировать политику, просто закройте DeviceLock Service Settings Editor и вернитесь в диалог настройки модуля.

За дополнительной информацией обращайтесь к разделу **Set Service Settings** данного руководства.

8 DeviceLock Enterprise Manager

8.1 Общая информация

С помощью DeviceLock Enterprise Manager вы можете устанавливать и просматривать разрешения и правила аудита, осуществлять установку, обновление и удаление агентов, а также просматривать журналы аудита и теневого копирования для всех компьютеров большой сети. Мы рекомендуем использовать DeviceLock Enterprise Manager в сети без Active Directory.

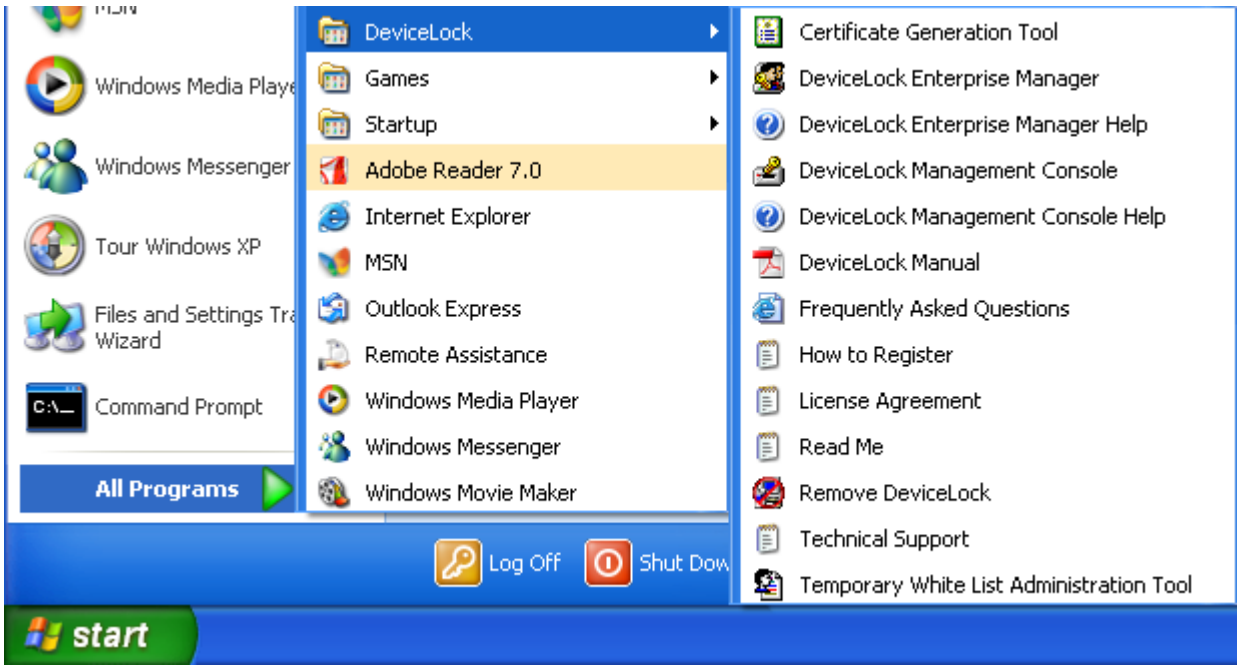
Основанный на многопоточном механизме, DeviceLock Enterprise Manager ускоряет выполнение всех действий для всех компьютеров в большой сети.

DeviceLock Enterprise Manager сохраняет, сравнивает и фильтрует данные, получаемые им со всех компьютеров. Администраторы могут делать "снимки" систем для последующего сравнения и записи изменений.

DeviceLock Enterprise Manager имеет гибкую архитектуру, позволяющую подключать модули (плагины) по мере необходимости. Каждый модуль отрабатывает свою задачу и отображает полученную информацию в своем собственном окне.

Чтобы получить информацию относительно процесса установки DeviceLock Enterprise Manager, обратитесь к разделу **Установка консолей управления** данного руководства.

Чтобы запустить DeviceLock Enterprise Manage, выберите соответствующий ярлык из меню *Programs*, появляющегося при нажатии на кнопку *Start*.



8.2 Интерфейс

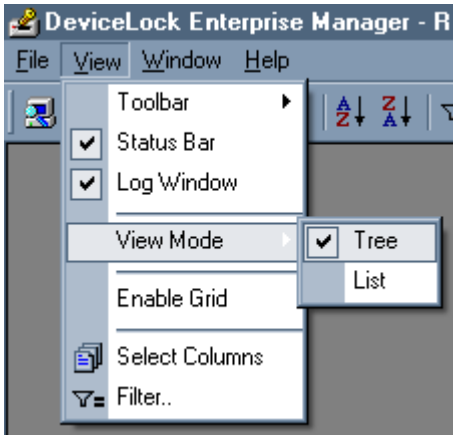
DeviceLock Enterprise Manager имеет многодокументный интерфейс (MDI), что позволяет использовать для каждой выполняемой задачи отдельное окно.

Размер основного окна можно изменять. DeviceLock Enterprise Manager сохраняет его размер и расположение и восстанавливает их при следующем запуске.

Многие функции программы доступны через главное меню основного окна.

Для изменения списка столбцов, отображаемых в окнах модулей, используйте пункт *Select Columns* в меню *View* или соответствующую кнопку на основной инструментальной панели.

По умолчанию DeviceLock Enterprise Manager отображает получаемую от модулей информацию в виде дерева, но вы можете выбрать вариант отображения в виде обычного списка. Для изменения режима отображения выберите пункт *View Mode* в меню *View* и затем выберите либо опцию *Tree*, либо *List*. Не забудьте, что этот режим устанавливается для каждого модуля индивидуально.



Вы можете скрыть панель статуса и/или окно протокола, выбрав соответствующие подпункты в меню *View*.

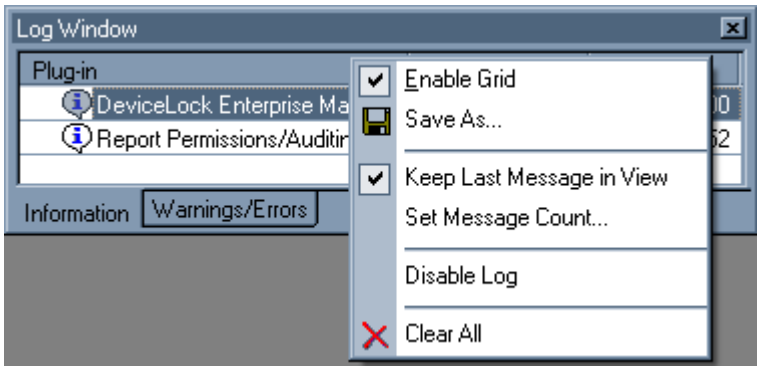
Для того чтобы в окне модулей значения были разделены сеткой, выберите подпункт *Enable Grid* в меню *View*. Этот режим устанавливается для каждого модуля индивидуально.

Чтобы отсортировать данные в окне какого-либо модуля, кликните по заголовку столбца. Для обратного порядка сортировки кликните по заголовку еще раз.

Если необходимо отсортировать данные верхнего уровня в дереве (такие, как домены или компьютеры), используйте соответствующую кнопку на основной инструментальной панели.

Окно протокола используется для отображения как полезной информации о текущей активности, так и диагностических сообщений и сообщений об ошибках.

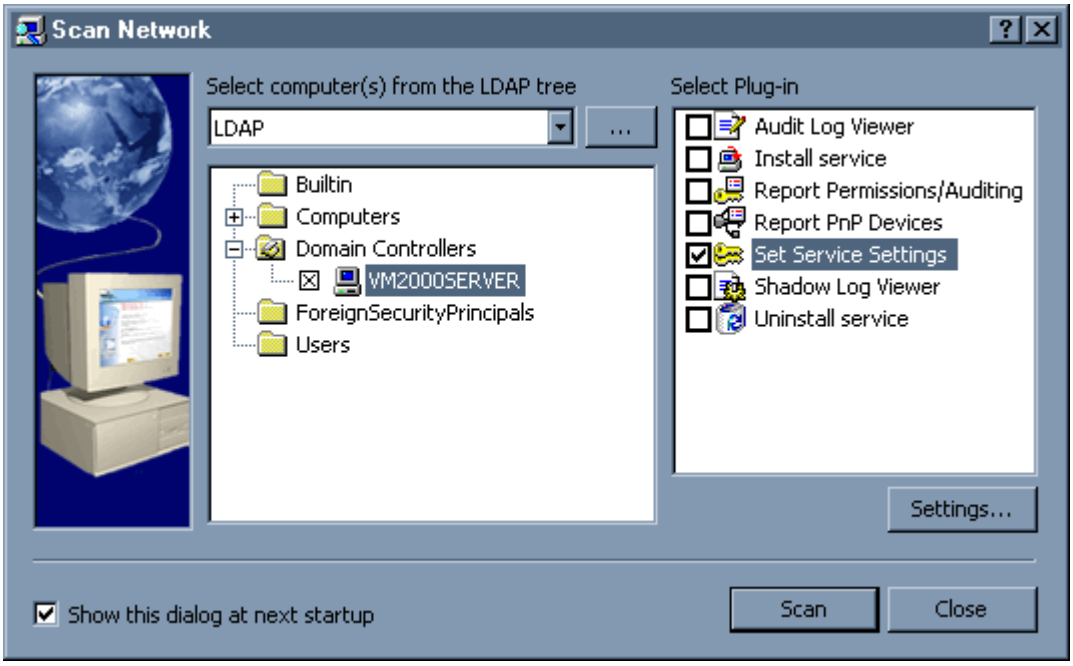
Имеется два типа протокола – *Information* и *Warnings/Errors*.



С помощью правой клавиши мыши в окне протокола вызывается контекстное меню.

8.3 Диалог Scan Network

Диалог *Scan Network* обеспечивает возможность выбора компьютеров в локальной сети и выполнения действий (установка или удаление агента, установка разрешений, правил аудита и т.п.), которые должны быть выполнены для этих компьютеров.



Чтобы открыть диалог *Scan Network*, выберите пункт *Scan Network* из меню *File* или используйте соответствующую кнопку на инструментальной панели. Если установлен флаг *Show this dialog at next startup*, то диалог *Scan Network* будет открываться автоматически при каждом запуске DeviceLock Enterprise Manager.

Ниже описаны три простых шага, которые позволят вам управлять DeviceLock Service'ами в локальной сети.

8.3.1 Выбор компьютеров

Первый шаг – выбор компьютеров.

Вы можете использовать контекстное меню, доступное по нажатию правой кнопки мыши, чтобы выбирать необходимые элементы (типы компьютеров, домены или компьютеры).

DeviceLock Enterprise Manager предоставляет несколько удобных способов для выбора компьютеров.

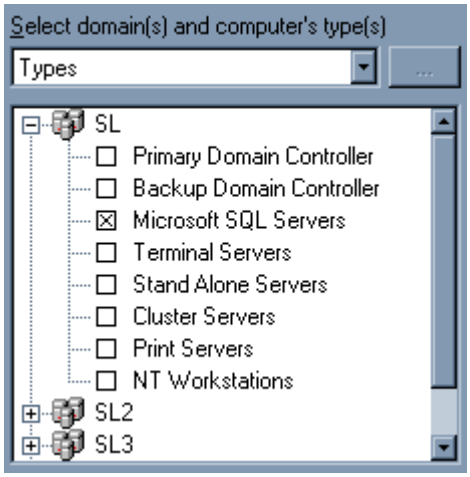
- Сетевые компьютеры могут быть выбраны по их типам.

  Каждый тип представляет все компьютеры, относящиеся к выбранной категории:

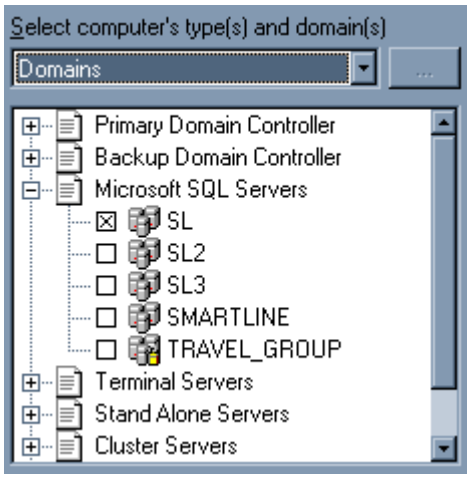
  - *Primary Domain Controller* – основной контроллер домена.
  - *Backup Domain Controller* – резервный контролер домена.
  - *Microsoft SQL Servers* – любой компьютер с запущенным сервером Microsoft SQL.
  - *Terminal Servers* – любой сервер, на котором запущены службы терминала.
  - *Stand Alone Servers* – любой сервер, не являющийся котроллером домена.
  - *Cluster Servers* – кластер серверов, доступный в домене.
  - *Print Servers* – любой компьютер, на котором имеется принтер общего доступа.
  - *NT Workstations* – любая рабочая станция под управлением Windows NT/2000/XP.

  Ниже представлены два способа выбора компьютеров по типам:

  1. *Types* – вы выбираете домен и затем тип компьютеров, с которыми вы собираетесь работать в этом домене.



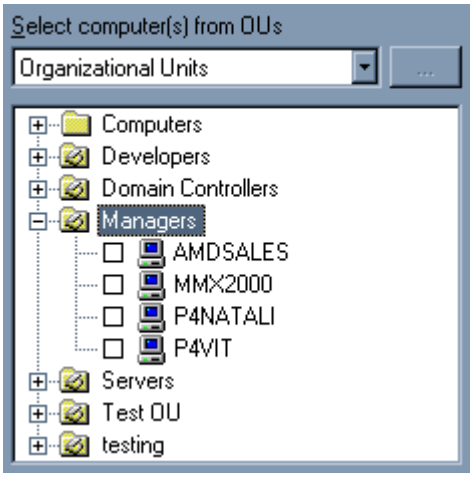
2. *Domains* – вы вначале выбираете тип компьютера и затем домен, с компьютерами которого вы собираетесь работать.



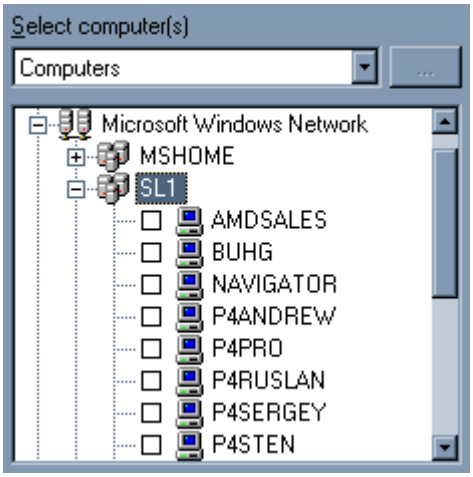
- Сетевые компьютеры также могут быть выбраны по их именам.

  Есть несколько вариантов выбора компьютеров по именам:

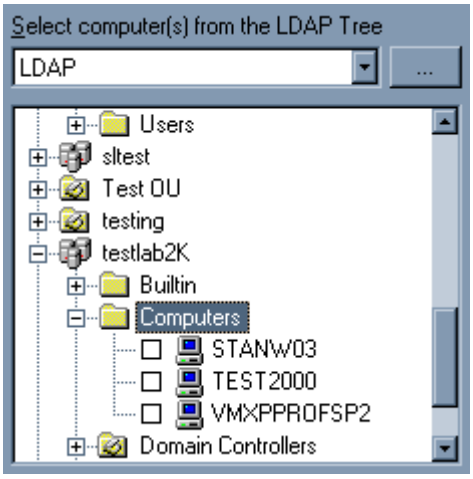
  1. *Organizational Units* – вы просматриваете подразделения в Active Directory и выбираете компьютеры, с которыми собираетесь работать.



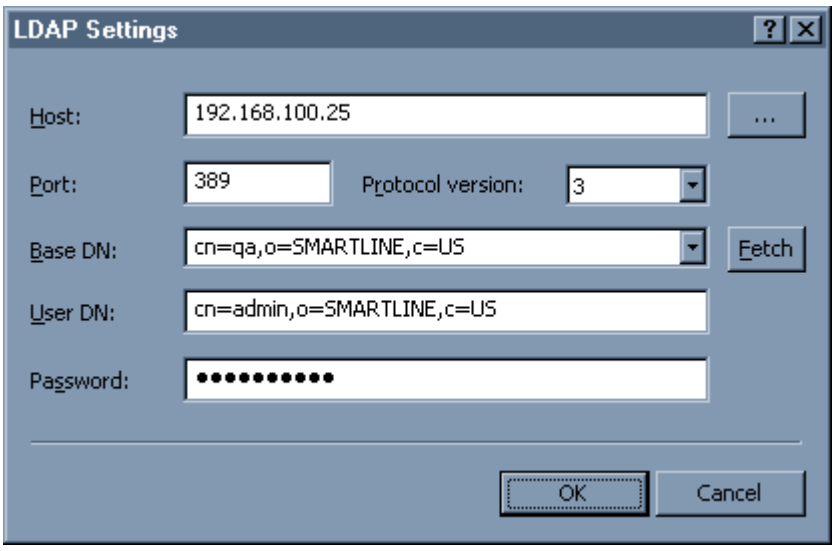
2. *Computers* – вы просматриваете дерево сети и выбираете компьютеры.



3. *LDAP* – вы просматриваете LDAP-дерево (*Lightweight Directory Access Protocol*) и выбираете компьютеры из службы каталогов.



Чтобы настроить подключение к LDAP-серверу, нажмите на кнопку **...**.



- *Host* – имя или IP-адрес LDAP-сервера, к которому выполняется подключение.

- *Port* – номер порта, по котором LDAP-сервер принимает подключения. По умолчанию это порт 389.

- *Protocol version* – версия LDAP-протокола. Некоторые реализации LDAP не полностью совместимы с LDAP-протоколом версии 3. Для таких случаев используйте при подключении протокол версии 2.

- *Base DN* – начальная точка для просмотра дерева каталога. Вы должны использовать строку в LDAP-формате (например, *cn=qa,o=SMARTLINE,c=US*). Оставьте поле *Base DN* пустым для просмотра с корня дерева.

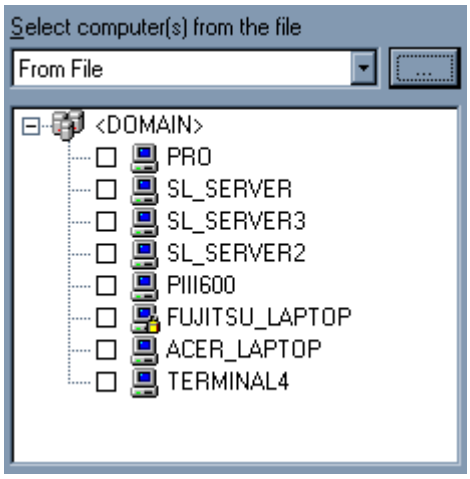
  При нажатии на кнопку *Fetch* вы можете получить все доступные контексты.

- *User DN* – имя пользователя, под которым выполняется подключение к каталогу. Вы должны использовать строку в LDAP-формате (например, *cn=admin,o=SMARTLINE,c=US*).

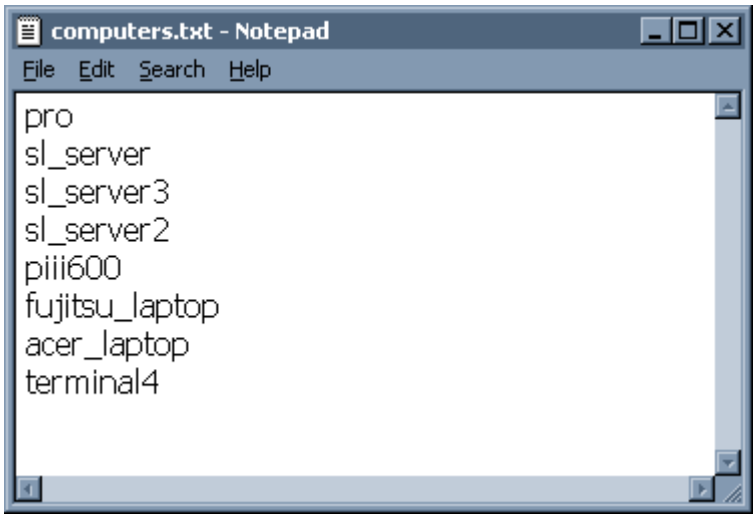
- *Password* – пароль пользователя.

4. *From File* – вы загружаете заранее подготовленный список компьютеров из внешнего текстового файла, а затем выбираете компьютеры.

   Чтобы открыть внешний файл, нажмите на кнопку **...**.

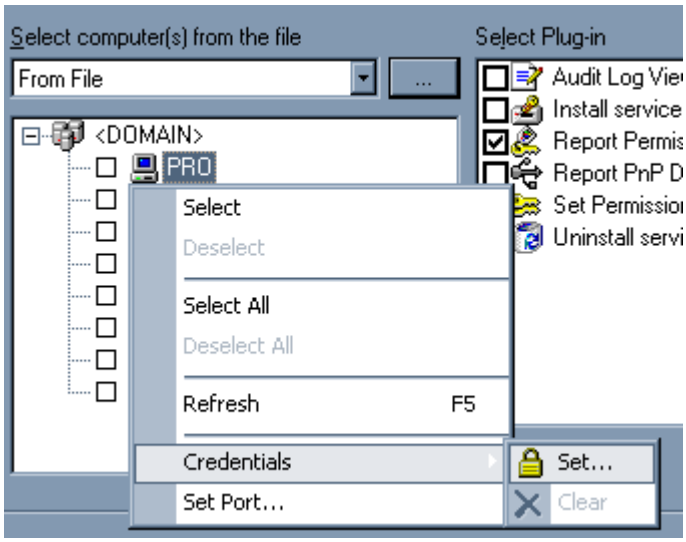


   Текстовый файл может содержать имена компьютеров и/или IP-адреса, каждый из которых должен быть записан на отдельной строке, и может быть как в уникод, так и в не уникод кодировке. Ниже приведен пример такого файла:



8.3.1.1 Задание альтернативных учетных записей

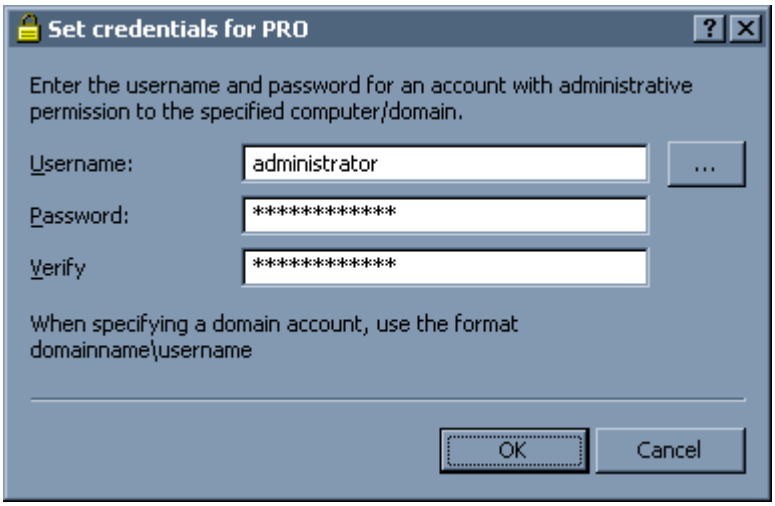
Если для подключения к удаленному компьютеру(-ам) вам требуются данные (пользователь и пароль) альтернативных учетных записей, выберите компьютер или домен из дерева и используйте подменю *Credentials* контекстного меню.



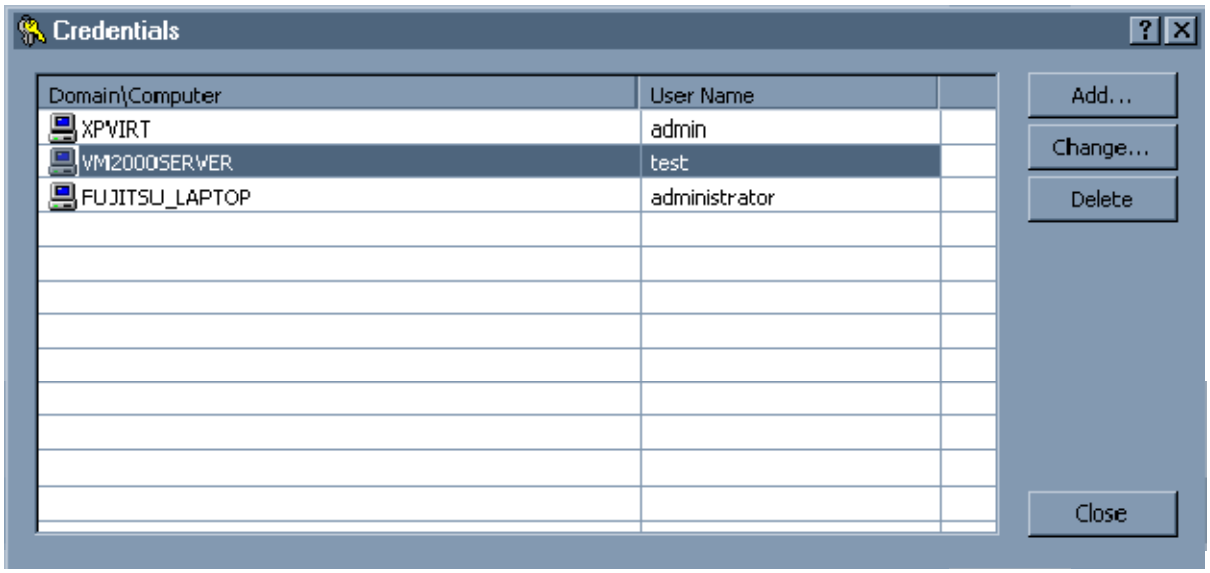
Вы можете задать альтернативные учетные записи как для отдельного компьютера, так и для всего домена. Для добавления альтернативных учетных записей используйте пункт *Set*, для удаления – *Clear*.

По умолчанию DeviceLock Enterprise Manager использует вашу текущую учетную запись для подключения и работы. Если текущая учетная запись не имеет административных привилегий на удаленных компьютерах, вам потребуется ввести альтернативные учетные записи. DeviceLock Enterprise Manager будет использовать альтернативные учетные записи при подключении к удаленным компьютерам.

Пароли для альтернативных учетных записей всегда сохраняются с использованием шифрования и недоступны никому, за исключением пользователя с правами администратора.



Альтернативные учетные записи также могут быть заданы с использование диалога *Credentials*. Для того, чтобы открыть диалог *Credentials*, выберите пункт *Credentials* из меню *File*.

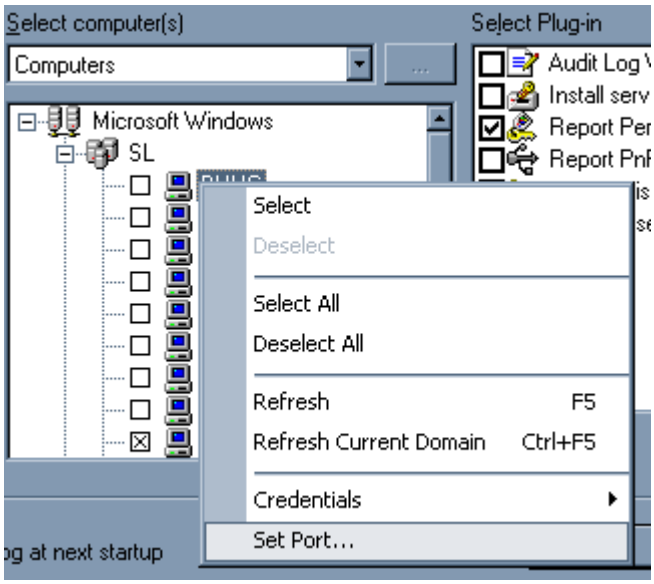


Нажмите на кнопку *Add*, чтобы задать новые учетные записи. Чтобы изменить существующую запись, выделите ее из списка и нажмите на кнопку *Change*.

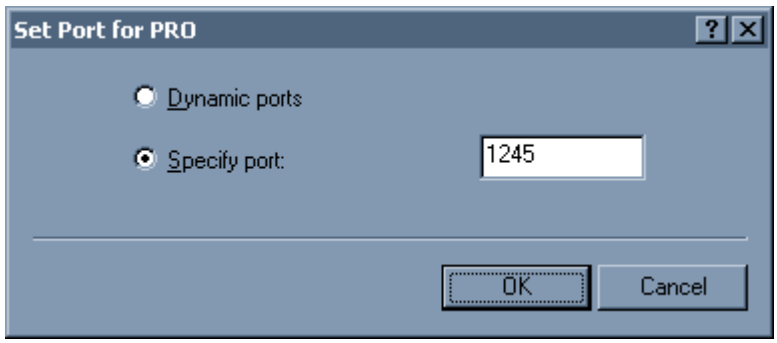
Чтобы удалить запись, выделите ее из списка и нажмите на кнопку *Delete*. Для одновременного удаления нескольких записей используйте клавиши *Ctrl* и/или *Shift*.

8.3.1.2 Установка порта

Вы можете установить использование фиксированного TCP-порта для DeviceLock Enterprise Manager. Для выполнения настройки используйте пункт *Set port* из контекстного меню.



По умолчанию DeviceLock Enterprise Manager использует динамические порты для подключения к DeviceLock Service. Однако, DeviceLock Service может также использовать и фиксированный порт. В этом случае, подключая DeviceLock Enterprise Manager к компьютеру, на котором DeviceLock Service настроен на использование фиксированного TCP-порта, вам следует выбрать опцию *Specify port* и задать порт.



Для использования динамических портов выберите опцию *Dynamic ports*.

DeviceLock Service может быть настроен на использование фиксированного порта или динамических портов в момент установки на компьютер. За дополнительной информацией обращайтесь к разделам **Установка без вмешательства пользователя** и **Установка в DeviceLock Enterprise Manager** данного руководства.

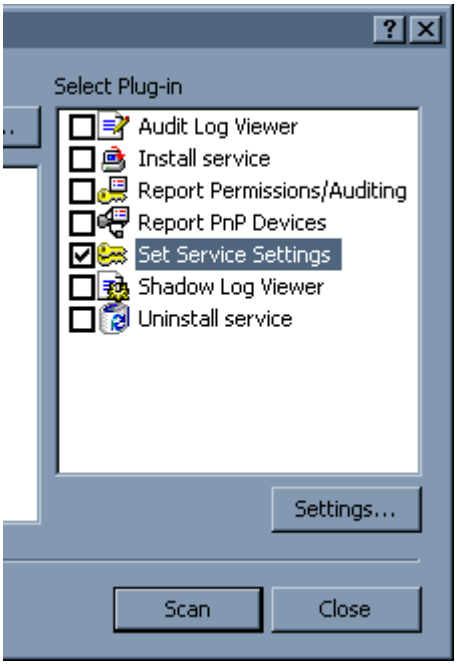
Если вам требуется изменить настройку порта, когда DeviceLock Service уже установлен на компьютере, используйте модуль *Install service*.

Информацию о том, какие порты должны быть открыты для того или иного действия, можно получить в разделе **Модули** данного руководства.

8.3.2 Выбор модуля

Второй шаг – выбор модуля для выполнения задания на компьютерах, которые были выбраны на первом шаге.

Для выбора модуля вы можете использовать контекстное меню, доступное по нажатию правой кнопки мыши.



Для задания настроек выбранного модуля используйте кнопку *Settings*, расположенную под списком модулей. Если модуль не имеет дополнительных настроек, кнопка *Settings* будет недоступна.

Задания поступают модулю от DeviceLock Enterprise Manager. Модуль выполняет задание и возвращает информацию в DeviceLock Enterprise Manager. Полученную от модулей информацию DeviceLock Enterprise Manager отображает в отдельных окнах.

8.3.3 Процесс сканирования

После выбора компьютеров и соответствующего модуля завершающим шагом будет являться процесс сканирования. Нажмите кнопку *Scan* для запуска процесса.

Сразу после того, как процесс сканирования запущен, вы можете приступить к просмотру информации, которая возвращается модулем.

Поскольку процесс сканирования запускается в отдельном потоке, вам нет необходимости ожидать окончания сканирования всех компьютеров. Также вы можете в это время выполнять иные действия в интерфейсе DeviceLock Enterprise Manager. Есть только несколько действий, которые вы не можете выполнять во время сканирования – вы не можете закрыть DeviceLock Enterprise Manager и вы не можете запустить другой процесс сканирования.

Если по каким-либо причинам вы хотите прервать активный процесс сканирования, вы можете использовать пункт *Stop Scan* из меню *File* или нажать соответствующую кнопку на инструментальной панели. Процесс сканирования будет прерван, как только модуль вернет управление в DeviceLock Enterprise Manager.

8.4 Модули

DeviceLock Enterprise Manager основан на архитектуре, позволяющей подключать модули по мере необходимости. DeviceLock Enterprise Manager загружает модули при запуске из директории *Plugins*, которая расположена в основной папке DeviceLock Enterprise Manager.

DeviceLock Enterprise Manager поставляется со стандартными модулями, которые требуют, чтобы некоторые сетевые порты были открыты, как описано в следующей таблице:

Необходимые порты	Модули
TCP 139 **UDP 137** – этот порт должен быть открыт только когда подключение происходит по имени компьютера. Если используется IP-адрес, то этот порт не нужен.	Audit Log Viewer, Report PnP Devices
TCP 139 **TCP 135** – этот порт должен быть открыт только когда используется подключение по динамическим портам. **TCP <*все порты выше 1024*>** – эти порты должны быть открыты только когда используется подключение по динамическим портам. **TCP <*порт*>** – этот порт должен быть открыт только когда используется подключение по фиксированному порту. **UDP 137** – этот порт должен быть открыт только когда подключение происходит по имени компьютера. Если используется IP-адрес, то этот порт не нужен.	Install Service, Uninstall Service

TCP 135 – этот порт должен быть открыт только когда используется подключение по динамическим портам. **TCP <*all ports above 1024*>** – эти порты должны быть открыты только когда используется подключение по динамическим портам. **TCP <*порт*>** – этот порт должен быть открыт только когда используется подключение по фиксированному порту **UDP 137** – этот порт должен быть открыт только когда подключение происходит по имени компьютера. Если используется IP-адрес, то этот порт не нужен.	Report Permissions/Auditing, Set Service Settings, Shadow Log Viewer

Чтобы получить информацию о том, как в DeviceLock Enterprise Manager настроить использование либо динамических портов, либо фиксированного порта, читайте раздел **Установка порта** данного руководства.

В момент подключения модуля к удаленному компьютеру возможно возникновение одной из этих ошибок:

- *The product version on the client and server machines does not match (7049)* – вы пытаетесь подключиться к компьютеру, на котором установлена и работает старая версия DeviceLock Service. Вы должны сначала обновить DeviceLock Service, используя модуль Install Service.

- *The network path was not found (53)* – вы пытаетесь подключиться к компьютеру, который либо не существует (неправильное имя или IP-адрес), либо недоступен. Убедитесь в том, что имя компьютера введено правильно. Попробуйте подключиться к этому комьютеру, используя стандартные средства администрирования Windows (такие как *Computer Management*, *Services* и т.п.).

  Данная ошибка возникает также когда стандартная служба *Server* не запущена на удаленном компьютере. Проверьте службу *Server* и запустите ее, если она остановлена.

Другие ошибки описаны в разделе **Возможные ошибки подключения** данного руководства.

8.4.1 Audit Log Viewer

Модуль *Audit Log Viewer* получает данные аудита из стандартного журнала Windows.

Чтобы определить максимальный размер журнала аудита и что Windows должна делать в случае его заполнения, используйте *Audit Log Settings* из контекстного меню доступного по нажатию правой кнопки мыши. Чтобы полностью очистить журнал аудита, используйте *Clear Audit Log* из контекстного меню.

За дополнительной информацией обращайтесь к разделу **Audit Log Viewer (для компьютера)** данного руководства.

8.4.2 Install Service

Модуль *Install Service* устанавливает и/или обновляет DeviceLock Service на компьютерах.

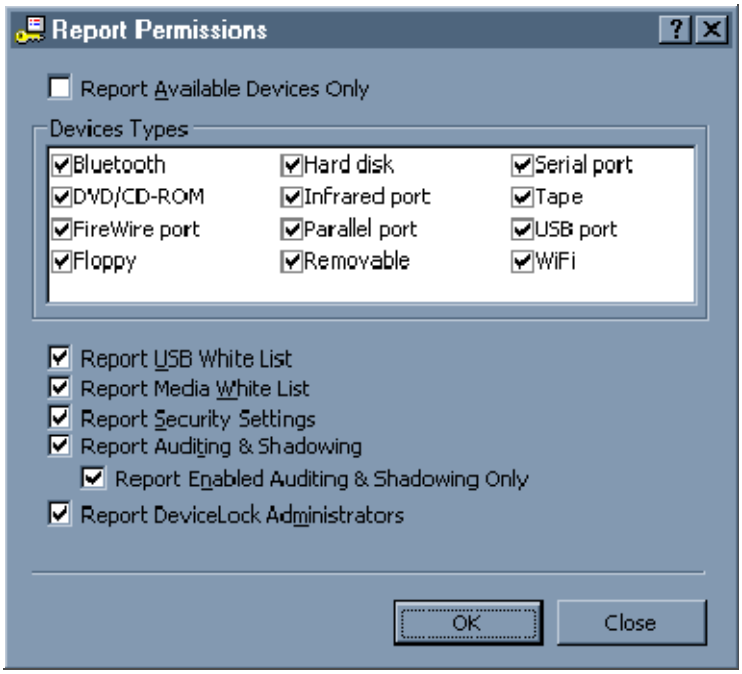
До того, как вы будете использовать этот модуль, вы должны указать путь к исполняемым файлам агента (*dlservice.exe* и *dlservice_x64.exe*). Вы можете сделать это, нажав на кнопку *Settings*, расположенную под списком модулей в окне диалога *Scan Network* (см. **Выбор модуля**).

За дополнительной информацией обращайтесь к разделу **Установка в DeviceLock Enterprise Manager** данного руководства.

8.4.3 Report Permissions/Auditing

Модуль *Report Permissions/Auditing* формирует отчет об установленных на компьютерах разрешениях, правилах аудита и других настройках DeviceLock Service.

Перед использованием этого модуля вы должны выбрать информацию, которую хотите включить в отчет. Вы можете сделать это, нажав на кнопку *Settings*, расположенную под списком модулей в окне диалога *Scan Network* (см. **Выбор модуля**).



- *Report Available Devices Only* – установите этот флаг, чтобы включить в отчет информацию об устройствах, подключенных в данный момент к компьютерам. В противном случае вы увидите информацию для всех поддерживаемых типов устройств.

- *Report USB White List* – установите этот флаг, чтобы включить в отчет информацию об устройствах, находящихся в белом списке (см. USB Devices White List).

- *Report Media White List* – установите этот флаг, чтобы включить в отчет информацию о носителях, находящихся в белом списке (см. Media White List).

- *Report Security Settings* – установите этот флаг, чтобы включить в отчет информацию об отключенных дополнительных параметрах безопасности (см. Security Settings).

- *Report Auditing & Shadowing* – установите этот флаг, чтобы включить в отчет информацию об установленных правилах аудита и теневого копирования.

  Также, когда этот флаг установлен, то в отчет попадает информация о состоянии флага *Log Policy changes and Start/Stop events* из Service Options.

- *Report Enabled Auditing & Shadowing Only* – установите этот флаг, чтобы исключить из отчета информацию об устройствах, для которых выключен аудит и теневое копирование.

  Этот флаг доступен только тогда, когда установлен флаг *Report Auditing & Shadowing*.

- *Report DeviceLock Administrators* – установите этот флаг, чтобы включить в отчет информацию об учетных записях, которые имеют доступ к DeviceLock Service.

В отчет всегда попадает информация об установленном сертификате (DeviceLock Certificate). Также, отчет содержит отдельную запись, если установлен флаг *Use Group Policy* в Service Options.

8.4.4 Report PnP Devices

Модуль *Report PnP Devices* формирует отчет, отображающий USB, FireWire и PCMCIA-устройства, которые в текущий момент подключены к компьютерам в локальной сети, и те, что были когда-либо подключены.

ПРИМЕЧАНИЕ: Для получения списка PnP-устройств с компьютеров, работающих под управлением Windows Vista/Server 2008, вы должны разрешить удаленный доступ к PnP-интерфейсу на этих компьютерах. Вы можете сделать это путем редактирования политики, как описано в статье: support.microsoft.com/kb/947040.

Столбцы отчета описаны ниже:

- *Description* – описание устройства, предоставляемое его изготовителем.

- *Device Information* – дополнительная информация об устройстве, предоставляемая его изготовителем.

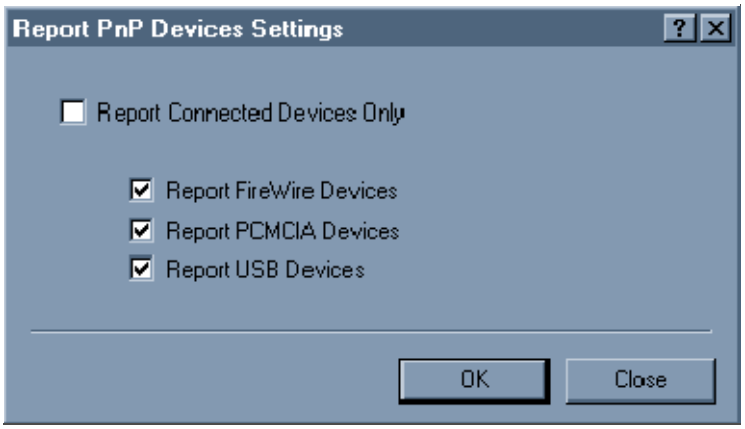
- *Connected to* – интерфейс, через который подключено устройство (*USB*, *FireWire* или *PCMCIA*).

- *Class* – класс устройства, определяемый Windows.

- *Class description* – описание класса устройства, определяемого Windows.
- *Present* – флаг, информирующий о том, подключено ли данное устройство в настоящий момент или нет (*Yes* или *No*).
- *DeviceID* – уникальный идентификатор устройства, установленный его изготовителем.
- *Driver* – название драйвера, который управляет данным устройством.

Вы можете добавить выбранное USB-устройство в базу данных устройств, используя контекстное меню, доступное по нажатию правой кнопки мыши.

Перед использованием этого модуля вы должны выбрать информацию, которую хотите включить в отчет. Вы можете сделать это, нажав на кнопку *Settings*, расположенную под списком модулей в окне диалога *Scan Network* (см. **Выбор модуля**).

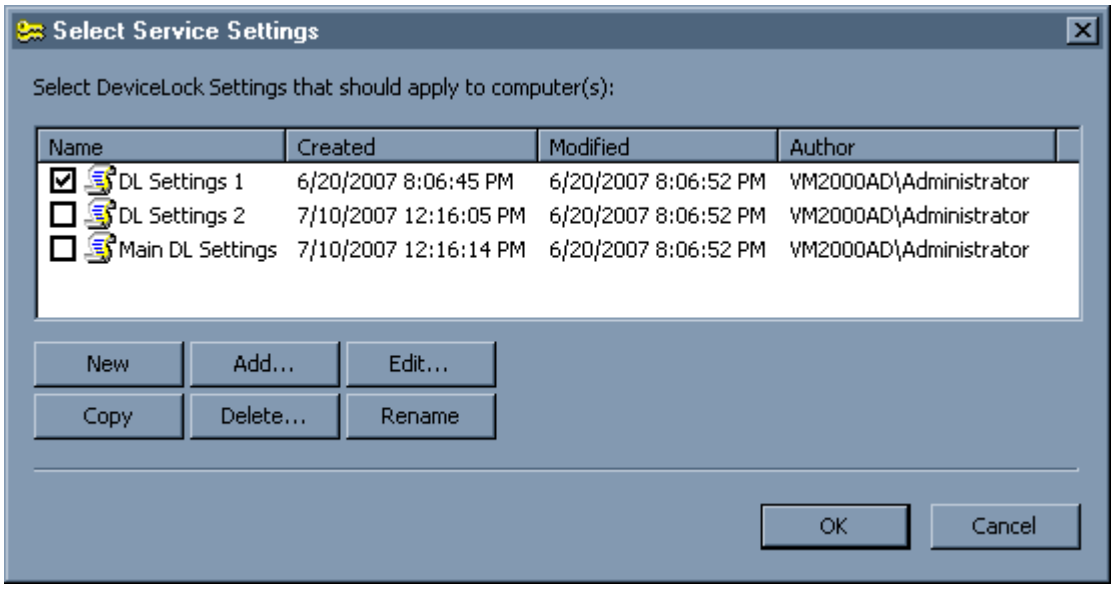


- *Report Connected Devices Only* – установите этот флаг, чтобы включить в отчет информацию об устройствах, подключенных в данный момент к компьютерам. В противном случае вы увидите информацию в том числе и для тех устройств, которые были когда-либо подключены.
- *Report FireWire Devices* – установите этот флаг, чтобы включить в отчет информацию об устройствах, подключенных к FireWire-порту.
- *Report PCMCIA Devices* – установите этот флаг, чтобы включить в отчет информацию об устройствах, подключенных через PCMCIA-интерфейс.
- *Report USB Devices* – установите этот флаг, чтобы включить в отчет информацию об устройствах, подключенных к USB-порту.

8.4.5 Set Service Settings

Модуль *Set Service Setting* считывает политику (настройки, разрешения, правила аудита и теневого копирования) из внешнего XML-файла и устанавливает ее для DeviceLock Service'ов в сети.

Перед использованием этого модуля вы должны задать настройки, разрешения и/или правила аудита, которые хотите установить. Вы можете сделать это, нажав на кнопку *Settings*, расположенную под списком модулей в окне диалога *Scan Network* (см. **Выбор модуля**).



Прежде всего, необходимо подготовить политику, которую вы хотите распространить по сети. Если в списке нет файлов, то вы можете, либо создать новый файл с чистой политикой, нажав на кнопку *New*, либо добавить уже существующий файл, нажав на кнопку *Add*.

Затем выделите файл в списке и нажмите на кнопку *Edit*, чтобы открыть редактор настроек сервиса. DeviceLock Service Settings Editor используется для создания и редактирования внешних XML-файлов с настройками, разрешениями, правилами аудита и теневого копирования. За дополнительной информацией обращайтесь к разделу **DeviceLock Service Settings Editor** данного руководства.

Когда вы завершите редактирование политики, отметьте ее файл, поставив флаг рядом с именем в списке. Затем нажмите кнопку *OK*, чтобы закрыть диалог настройки модуля *Set Service Setting*.

8.4.6 Shadow Log Viewer

Модуль *Shadow Log Viewer* получает записи журнала теневого копирования с компьютеров. Используйте контекстное меню, доступное по нажатию правой кнопки мыши, для доступа к основным функциям модуля.

За дополнительной информацией обращайтесь к разделу **Shadow Log Viewer (для компьютера)** данного руководства.

8.4.7 Uninstall Service

Модуль *Uninstall Service* удаляет DeviceLock Service, все его настройки и компоненты с компьютеров.

Если учетная запись, под которой этот модуль подключается к компьютеру, не имеет полного административного права на доступ к DeviceLock Service, то модуль не сможет выполнить операцию удаления. Похожая ошибка возникает, когда учетная запись не имеет привилегий локального администратора на компьютере, где запущен DeviceLock Service.

8.5 Загрузка / Сохранение / Экспорт

DeviceLock Enterprise Manager может сохранять всю информацию, полученную от модулей.

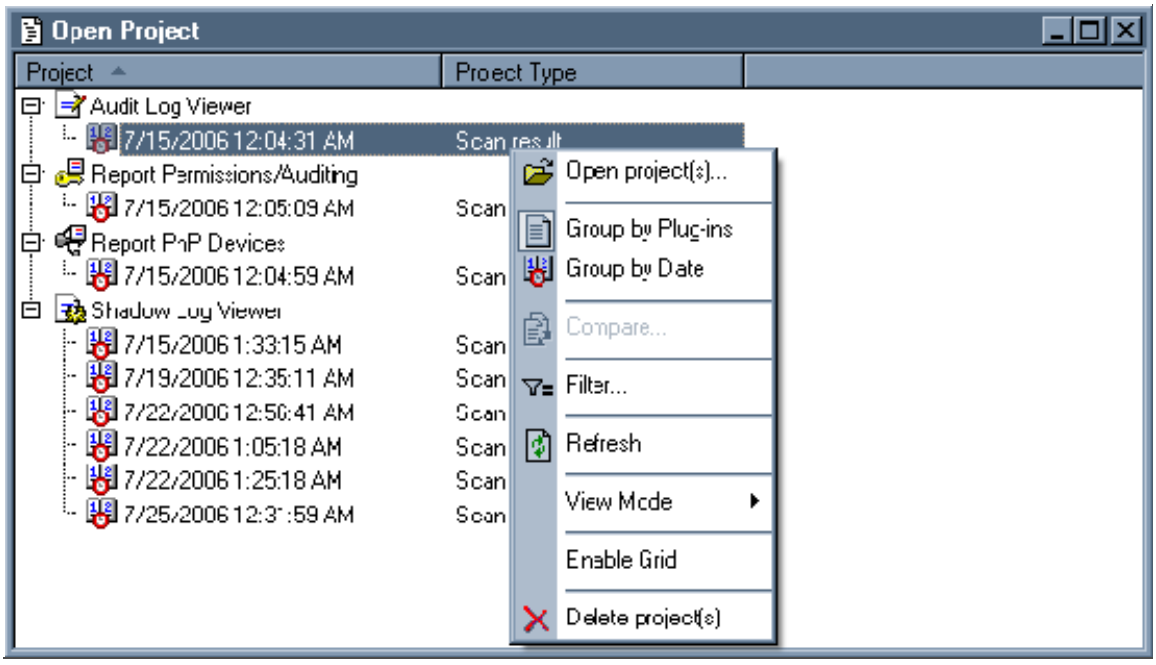
Данные сохраняются во внешних файлах и по запросу могут быть загружены в DeviceLock Enterprise Manager. Существует три варианта сохранения и загрузки данных:

1. Наиболее удобный способ хранения полученной информации – в виде проекта. DeviceLock Enterprise Manager сохраняет каждое окно с информацией в отдельном файле и помещает эти файлы в папку *Project*.

   Имена файлов проекта формируются автоматически и зависят от названия модуля, даты и времени начала сканирования.

   Чтобы сохранить данные в виде проекта, вы можете выбрать пункт *Save Project* из меню *File* или нажать на соответствующую кнопку на инструментальной панели.

   Для загрузки сохраненного проекта вы можете выбрать пункт *Open Project* из меню *File*.



   Окно *Open Project* имеет собственную инструментальную панель и контекстное меню.

Вы можете сгруппировать сохраненные проекты по датам, когда выполнялось сканирование, и по типу информации, содержащейся в них. Выберите пункт *Group by Plug-ins* или *Group by Date* из контекстного меню или нажмите соответствующую кнопку на инструментальной панели *Project*.

Чтобы открыть сохраненный проект, выберите его из списка и нажмите кнопку *Open Project* на инструментальной панели *Project*. Используя клавиши Ctrl и/или Shift, вы можете открыть одновременно несколько проектов.

2. Другой способ сохранения полученной информации в DeviceLock Enterprise Manager – выбор подпункта *Save As* из меню *File*. Этот способ позволяет вам сохранить файл в формате *ANM* в любом месте вашего диска или на любом ином устройстве и с любым именем.

   Для загрузки сохраненного файла выберите подпункт *Open* меню *File* или нажмите соответствующую кнопку на основной инструментальной панели. Вам будет необходимо указать файл, который вы хотите открыть. Загрузить можно будет лишь файлы в формате *ANM*.

3. Если вам необходимо передать полученную информацию во внешнее приложение, вы можете экспортировать данные во внешний файл и затем импортировать их в это приложение. Для экспорта данных во внешний файл выберите подпункт *Save As* меню *File* и затем выберите тип файла из списка *Save as type*. DeviceLock Enterprise Manager поддерживает экспорт в MS Excel (если он установлен на локальном компьютере) и в два текстовых формата – *Tab Delimited* (TXT) и *Comma Delimited* (CSV).

   Если вы экспортируете информацию во внешний файл, вы не сможете загрузить ее обратно, поскольку DeviceLock Enterprise Manager может открывать и загружать файлы только собственного формата (*ANM*). Однако возможность экспорта во внешний файл используется в том случае, если вы хотите обмениваться данными между DeviceLock Enterprise Manager и другими приложениями.

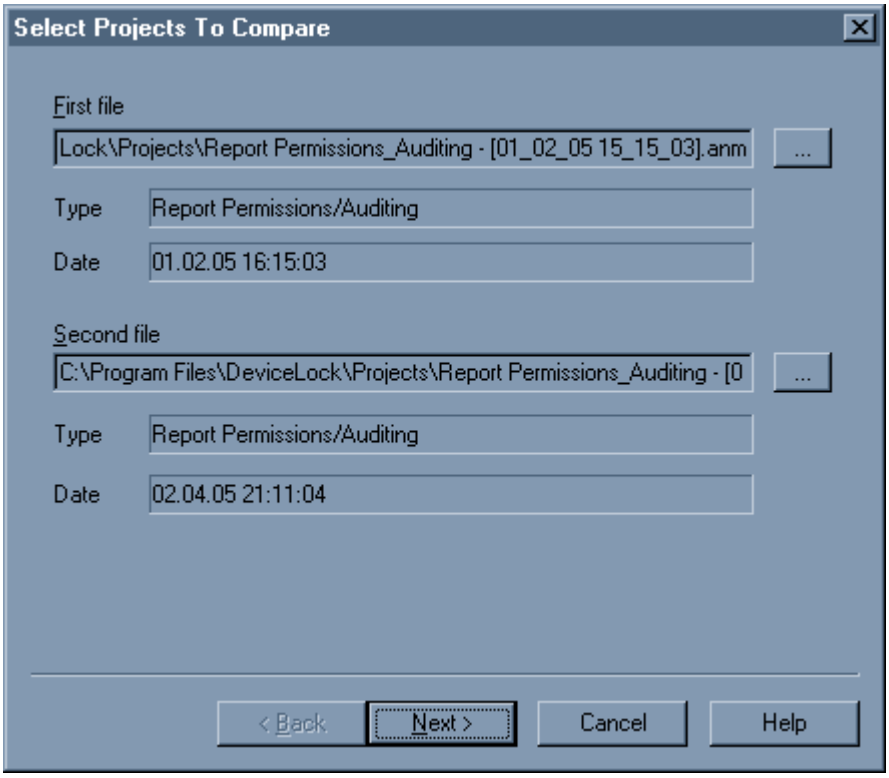
8.6 Сравнение данных

DeviceLock Enterprise Manager обеспечивает возможность отслеживать изменения на сетевых компьютерах, сравнивая два предварительно сохраненных проекта. Сравнение изменений очень важно, когда выполняется управление большим количеством компьютеров одной сети.

DeviceLock Enterprise Manager предоставляет удобный и простой в использовании мастер сравнения двух *ANM*-файлов. Чтобы открыть этот мастер сравнения, выберите подпункт *Compare* из меню *File*.

Ниже приведены три простых шага, которые позволят вам сравнить два файла, используя мастер сравнения:

1. Первый шаг – выбор файлов для сравнения.

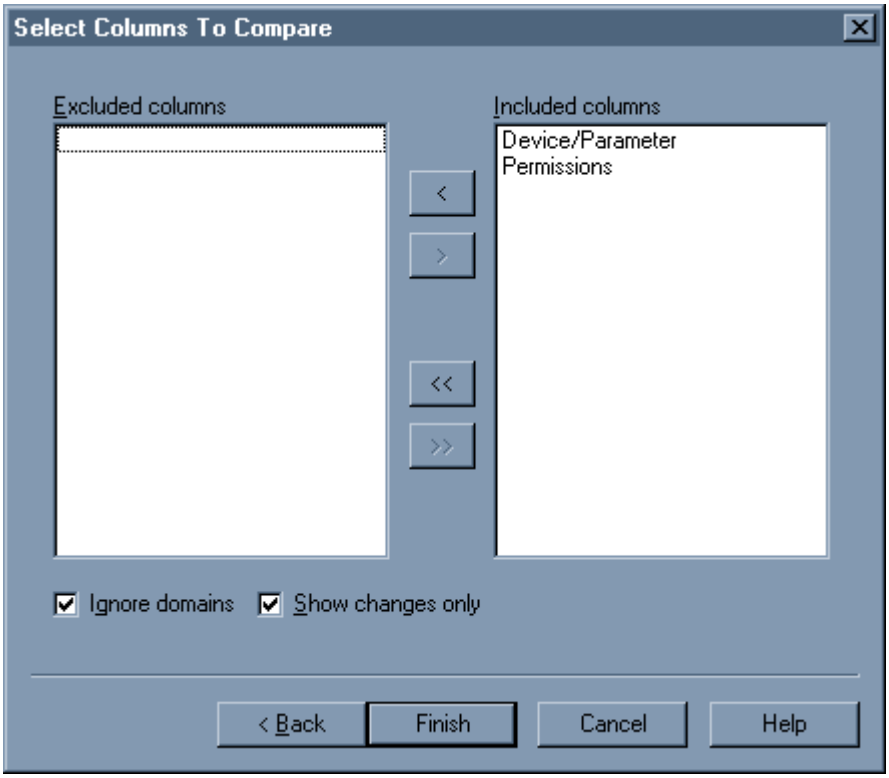


Выберите первый файл, затем второй нажатием соответствующих кнопок **...**.

Помните, что вы можете сравнивать файлы только одного и того же типа. Например, вы не можете сравнивать информацию, полученную от модуля *Report Permissions/Auditing* с информацией, полученной от модуля *Report PnP Devices*.

После выбора двух файлов, нажмите на кнопку *Next* для перехода к следующей странице мастера сравнения.

2. Второй шаг – выбор столбцов, по которым вы хотите выполнить сравнение.



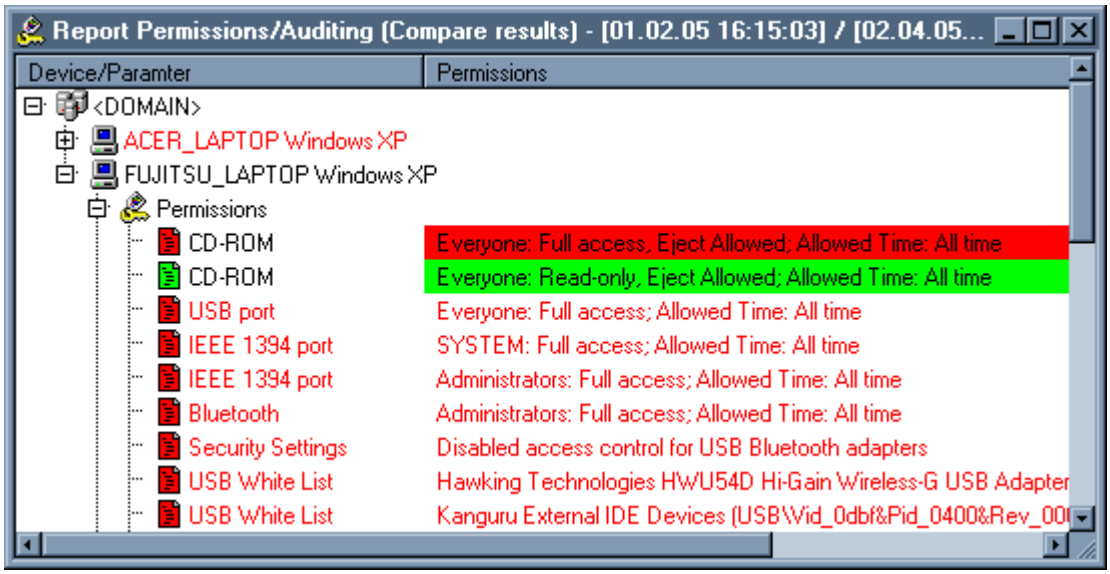
DeviceLock Enterprise Manager сравнивает только те столбцы, которые были выбраны на этом шаге. Если вам необходимо исключить один столбец из процесса сравнения, вам необходимо переместить его из списка *Included columns* в список *Excluded columns*. Исключенные столбцы будут видны в результате сравнения, но их значения игнорируются и не оказывают влияния на результат.

По умолчанию, результат сравнения будет содержать только те записи, которые имеют различия в выбранных для сравнения файлах. Если вы хотите увидеть все записи (включая одинаковые), вы можете снять флаг *Show changes only*.

Для включения имен доменов в процесс сравнения, снимите флаг *Ignore domains*. Когда флаг *Ignore domains* установлен, DeviceLock Enterprise Manager игнорирует домены и сравнивает только компьютеры и информацию, которую они содержат.

3. Третий и заключительный шаг – запуск процесса сравнения. Нажмите на кнопку *Finish* для выполнения сравнения двух выбранных файлов.

   DeviceLock Enterprise Manager отобразит результат сравнения в отдельном окне в виде дерева в точности, как отображается информация, полученная от модулей в процессе сканирования.



Алгоритм сравнения очень прост и эффективен:

1. Если флаг *Ignore domains* снят, программа определяет количество доменов в двух выбранных файлах и пытается найти каждый из них как в старом, так и в новом файле.

   Если домен имеется в старом файле, но отсутствует в новом, программа вставляет отсутствующий домен (включая все входящие в этот домен компьютеры и информацию, которая для них имеется) в результат сравнения и отображает все эти записи красным цветом.

Если домен отсутствует в старом файле, но имеется в новом, программа вставляет отсутствующий домен (включая все входящие в этот домен компьютеры и информацию, которая для них имеется) в результат сравнения и отображает все эти записи зеленым.

Если домен существует в обоих файлах, программа перебирает все входящие в этот домен компьютеры (см. ниже).

2. Если установлен флаг *Ignore domains*, программа будет игнорировать домены и переберет все компьютеры в обоих выбранных файлах, после чего попытается найти каждый компьютер, как в старом, так и в новом файле.

   Если компьютер имеется в старом файле, но отсутствует в новом, программа вставит отсутствующий компьютер вместе со всей его информацией в результат сравнения и отметит все записи красным.

   Если компьютер не существует в старом файле, но присутствует в новом, программа вставит отсутствующий компьютер вместе со всей его информацией в результат сравнения и отметит все записи зеленым цветом.

   Если компьютер имеется в обоих файлах, программа перебирает всю относящуюся к нему информацию (см. ниже).

3. Программа перебирает всю относящуюся к компьютеру информацию и пытается найти одинаковые записи в обоих файлах.

   Если запись имеется в старом файле и отсутствует в новом, программа вставит отсутствующую запись в результат сравнения и выделит ее красным цветом.

   Если запись отсутствует в старом файле, но присутствует в новом, программа вставит отсутствующую запись в результат сравнения и выделит ее зеленым цветом.

   Если запись имеется в обоих файлах, программа запустит процедуру сравнения каждого входящего в эту запись столбца:

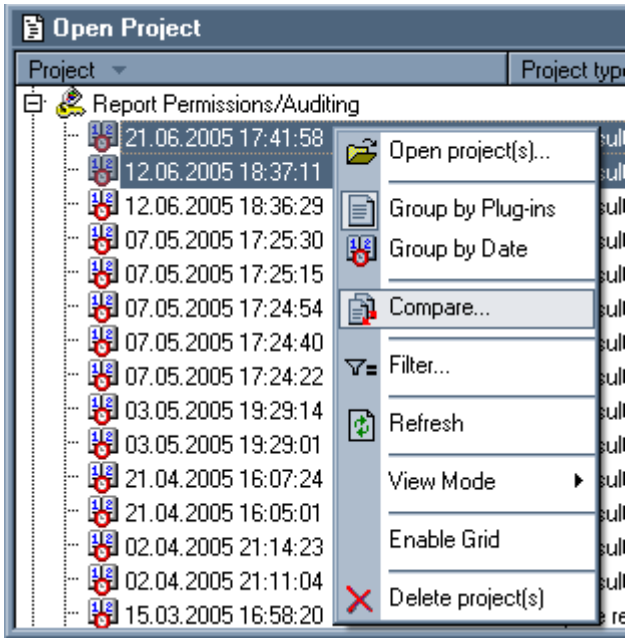
   - Если значение столбца для файлов различны, программа вставит обе записи в результат сравнения. Запись из нового файла будет размещена после записи из старого файла.

     Содержимое столбца, принадлежащее старой записи, будет выделено красным цветом. Содержимое столбца, принадлежащее новой записи, будет выделено зеленым.

     Содержимое всех, не включенных в процесс сравнения столбцов, выводится цветом по умолчанию.

- Если записи всех столбцов обоих файлов имеют одинаковые значения, программа либо пропустит эту запись (установлен флаг *Show changes only*), либо вставит запись в результат сравнения, используя цвет по умолчанию (флаг *Show changes only* снят).

Если вы хотите сравнить два файла, которые были сохранены как проекты, то удобно будет использовать специальную возможность окна *Open Project*.



Выберите пункт *Open Project* из меню *File*, выделите два проекта, которые вы хотите сравнить (используйте *Ctrl* и/или *Shift* для одновременного выделения двух проектов), а затем выберите пункт *Compare* из контекстного меню или нажмите на соответствующую кнопку на инструментальной панели *Project*. ***Пожалуйста, не забудьте, что вы можете выбрать только два проекта и оба проекта должны быть одного и того же типа.***

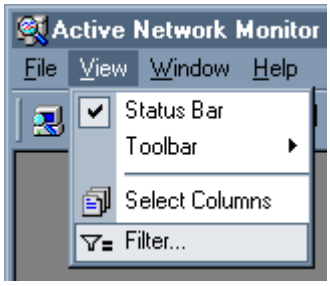
DeviceLock Enterprise Manager имеет две кнопки на инструментальной панели *Compare*, обеспечивающие удобную навигацию по результатам сравнения. Нажмите кнопку **<** для перехода к предыдущей записи результата, имеющей различия. Нажмите кнопку **>** для перехода на следующую запись, имеющую различия.

Результаты сравнения могут быть сохранены во внешнем файле формата *ANM* или экспортированы в MS Excel или текстовый файл (TXT и CSV). Выберите *Save As* из меню *File* или нажмите соответствующую кнопку на основной инструментальной панели для сохранения или экспорта результатов сравнения.

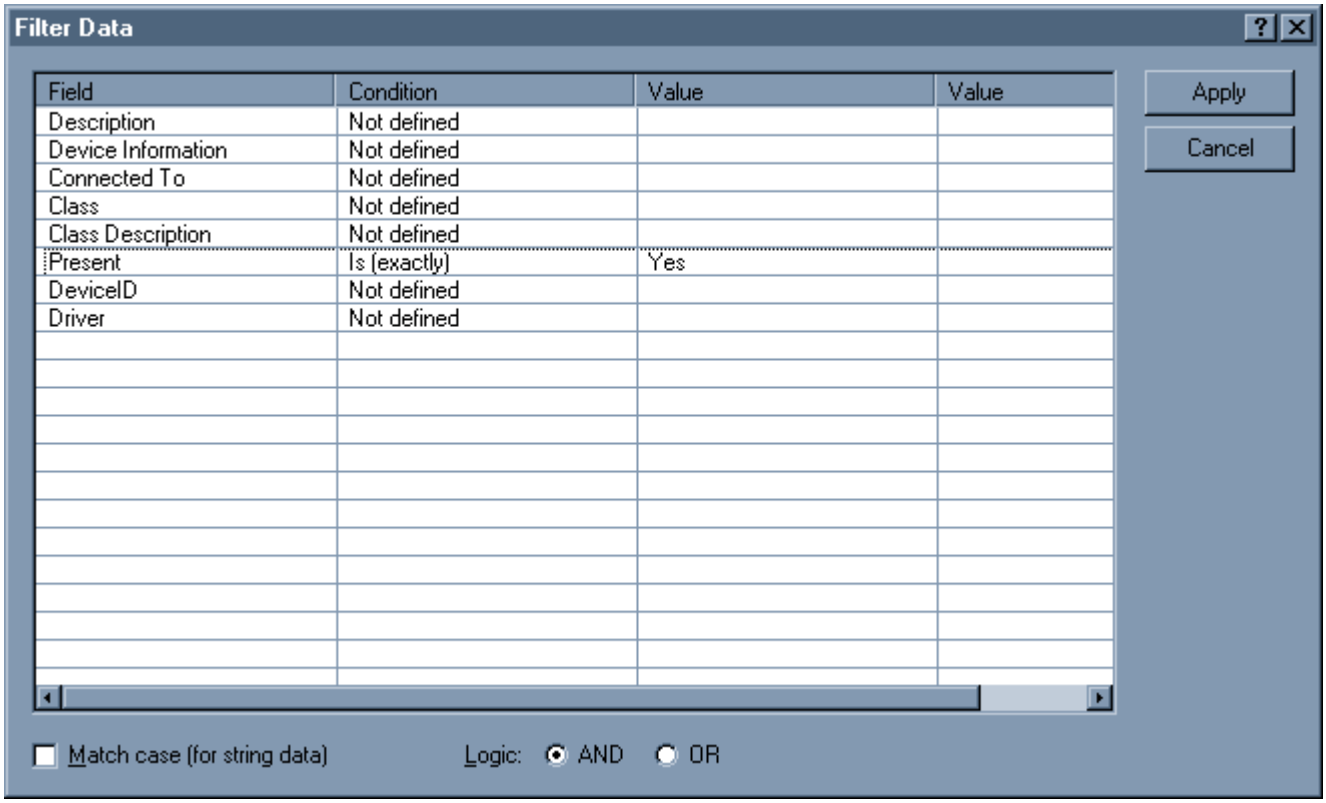
Как и любые другие файлы, сохраненные результаты могут быть открыты и загружены обратно в DeviceLock Enterprise Manager. Для того чтобы загрузить предварительно сохраненные результаты сравнения, вы можете выбрать пункт *Open* из меню *File* или нажать на соответствующую кнопку на основной инструментальной панели. Вам потребуется выбрать файл, который вы хотите открыть. Вы можете загрузить файлы только формата *ANM*.

8.7 Фильтрация данных

DeviceLock Enterprise Manager предоставляет очень мощную функцию фильтрации данных, позволяющую вам ограничить результаты сканирования и/или сравнения только теми данными, которые необходимы.



Чтобы открыть диалог *Filter Data*, вы можете выбрать пункт *Filter* из меню *View* или нажать на соответствующую кнопку на основной инструментальной панели.



- Столбец *Field* отображает все поля, доступные в результатах сканирования или сравнения, по значению которых можно задать фильтр. Вы можете использовать логику “*И-ИЛИ*” для всех полей:

  AND – включает в результат только те записи, которые полностью удовлетворяют всем заданными условиями. Например, *Process = “explorer.exe” AND PID = 3764* возвратит все данные, в которых значение *Process* соответствует “*explorer.exe*”, а *PID* равен *3764*. Результат не будет включать в себя данные, в которых значение поля *Process* равно “*explorer.exe*”, а *PID* не равен *3764,* или где *PID* равен *3764,* но *Process* не равен строке “*explorer.exe*”.

  OR – включает в результат записи, которые удовлетворяют хотя бы одному заданному условию. Например, *Process = “explorer.exe” OR PID = 3764* возвратит все данные, в которых верно одно или оба условия, где Process = “*explorer.exe*” (не важно, какое значение при этом имеет *PID*) или где *PID* равен *3764* (не важно, какое значение имеет *Process*).

- Столбец *Condition* содержит список логических операций, которые могут быть применены к выбранному полю. Вы можете выбрать только одну логическую операцию для каждого поля. DeviceLock Enterprise Manager поддерживает две группы логических операций, для *строковых* данных и для *не строковых* данных.

  Логические операции, которые могут быть выполнены над *строковыми* данными (сравниваемое значение (аргумент) также должно быть строковым, например “*Explorer.exe*”):

  - *Is (exactly)* – отбираются только те данные, значения полей которых полностью соответствуют сравниваемой строке.

  - *Includes* – отбираются только те данные, значения полей которых входят (содержатся) в сравниваемую строку.

  - *Is not* – отбираются только те данные, значения полей которых отличны от сравниваемой строки.

  - *Not includes* – отбираются только те данные, значения полей которых не входят (не содержатся) в сравниваемую строку.

  - *Empty* – отбираются только те данные, поля которых содержат пустую строку.

  - *Not Empty* – отбираются только те данные, поля которых не пустые.

  - *Regular expression* – отбираются только те данные, строки в полях которых удовлетворяют регулярному выражению. Регулярное выражение может содержать символы подстановки (например, “*expl*e?*”).

  Если вы хотите учитывать регистр букв в строке (например, чтобы "*Explorer.exe*" отличался от "e*xplorer.exe*"), установите флаг *Match case*. В противном случае регистр букв игнорируется (например, строки "*Explorer.exe*" и "*explorer.exe*" считаются одинаковыми).

  Логические операции, выполняемые над *не строковыми* данными:

  - *Equal to (=)* – отбираются данные, в которых значение сравниваемого поля равно заданному значению (например, *PID = 3764*).

  - *Greater than (>)* – отбираются данные, значение сравниваемого поля которых больше, чем заданное значение (например, *PID > 4*).

  - *Less than (<)* – отбираются данные, значение сравниваемого поля которых меньше, чем заданное значение (например, *PID < 4*).

  - *Not Equal to (!=)* – отбираются данные, значение сравниваемого поля которых не равно заданному значению (например, *PID != 0*).

- *Between (in)* – отбираются данные, значение сравниваемого поля которых находится между двумя заданными значениями (например, *PID in 3000-4000*).

- *Not Between (out)* – отбираются данные, значение сравниваемого поля которых находится вне региона двух заданных значений (например, *PID out 3000-4000*).

- *Regular expression* – отбираются только те данные, значение полей которых удовлетворяют регулярному выражению. Регулярное выражение может содержать символы подстановки (например, *3*1?9*).

Если вы не хотите выполнять логическую операцию для поля, выберите в списке логических операций пункт *Not defined*.

- Столбец *Value* содержит заданные пользователем аргументы. Второй столбец *Value* используется только для случаев, если выбраны логические операции *Between (in)* или *Not Between (out)*. Для всех остальных логических операций требуется только первый столбец *Value*.

После того, как выражение для фильтра определено, нажмите на кнопку *Apply*.

Вы можете сохранить результат фильтрации либо во внешнем файле *ANM,* либо экспортировать его в текстовый файл (TXT и CSV) или MS Excel.

Выберите пункт *Save As* в меню *File* или нажмите на соответствующую кнопку на основной инструментальной панели для сохранения или экспорта результатов.

Как и любые другие файлы, сохраненные результаты могут быть открыты и загружены обратно в DeviceLock Enterprise Manager.

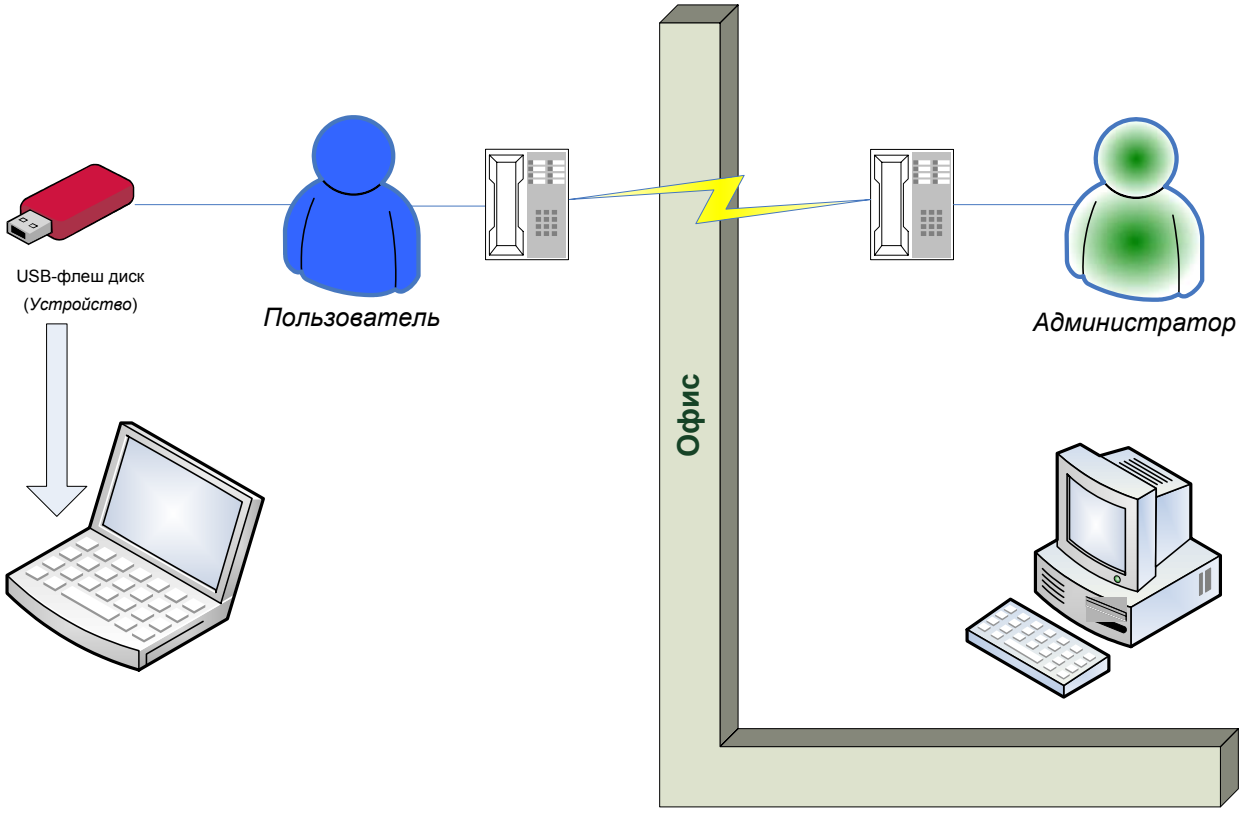
Для того чтобы загрузить предварительно сохраненные результаты фильтрации, вы можете выбрать пункт *Open* из меню *File* или нажать соответствующую кнопку на основной инструментальной панели. Вам потребуется выбрать файл, который вы хотите открыть.

Вы можете загрузить файлы только формата *ANM*.

9 Временный белый список

9.1 Общая информация

Функция «Временный белый список» позволяет предоставлять временный доступ к USB-устройствам при отсутствии сетевого подключения. Администратор сообщает пользователю специальный код по телефону, который временно разблокирует доступ к требуемому устройству.



Временный белый список работает аналогично белому списку устройств, но отличается тем, что не требуется сетевого подключения для добавления устройств и предоставления доступа к ним.

ПРИМЕЧАНИЕ: Использование временного белого списка – это возможность предоставления доступа к USB-устройствам, которые заблокированы на обоих уровнях: уровне интерфейса (USB) и уровне типа устройства. Если находящееся в белом списке устройство (например, USB флеш-диск) принадлежит к обоим уровням: интерфейсу (USB) и типу (Removable), ограничения (если они есть) на уровне типа устройства будут игнорироваться точно так же, как и на уровне USB.

Следующая пошаговая инструкция поможет вам создать и использовать временный белый список:

1. Администратор создает криптографический сертификат (DeviceLock Certificate), используя программу Certificate Generation Tool. Сертификат состоит из двух ключей – *секретного* и *открытого*.

2. Администратор устанавливает сертификат (*открытый* ключ) на компьютер пользователя.

3. Когда пользователю необходимо получить доступ к какому-либо USB-устройству, он запускает Temporary White List Authorization Tool, выбирает требуемое устройство из списка и формирует буквенно-цифровой код (**Код Устройства**). Затем пользователь должен передать этот код администратору по телефону или любым другим способом.

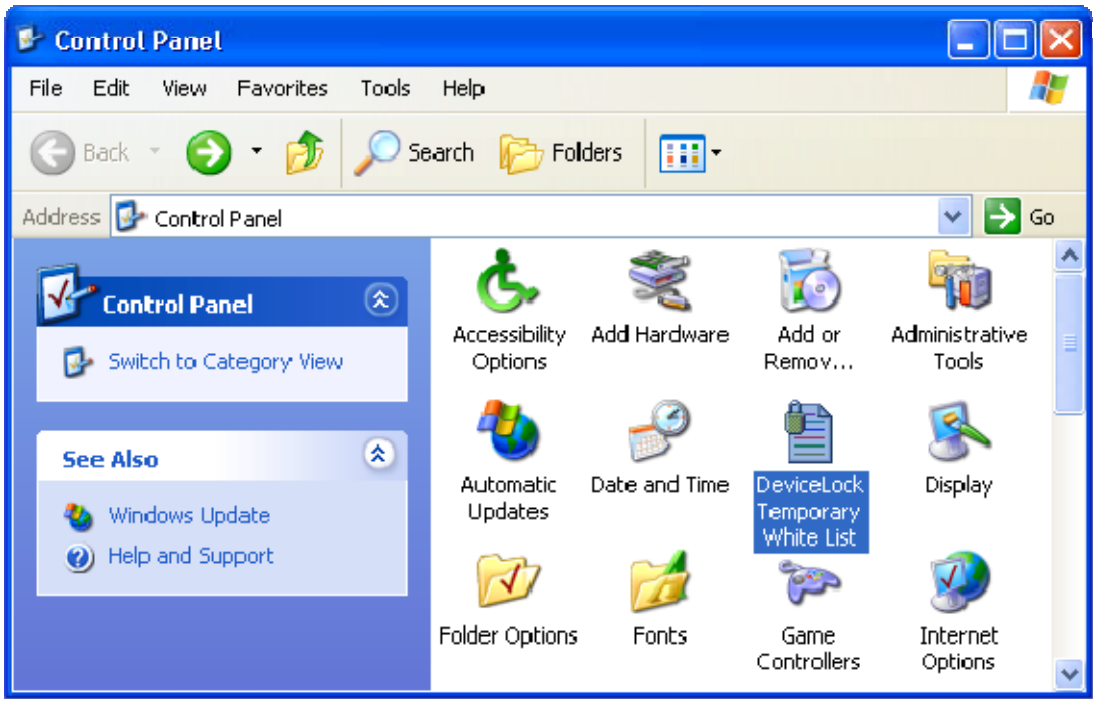
4. Администратор запускает программу DeviceLock Signing Tool, загружает соответствующий сертификат (*секретный* ключ), вводит переданный ему **Код Устройства**, задает необходимый период времени, формирует ответный код (**Разблокирующий Код)**, и передает этот код пользователю.

5. Пользователь вводит полученный от администратора **Разблокирующий Код** в Temporary White List Authorization Tool, после чего получает доступ к запрошенному устройству на заданный период времени.

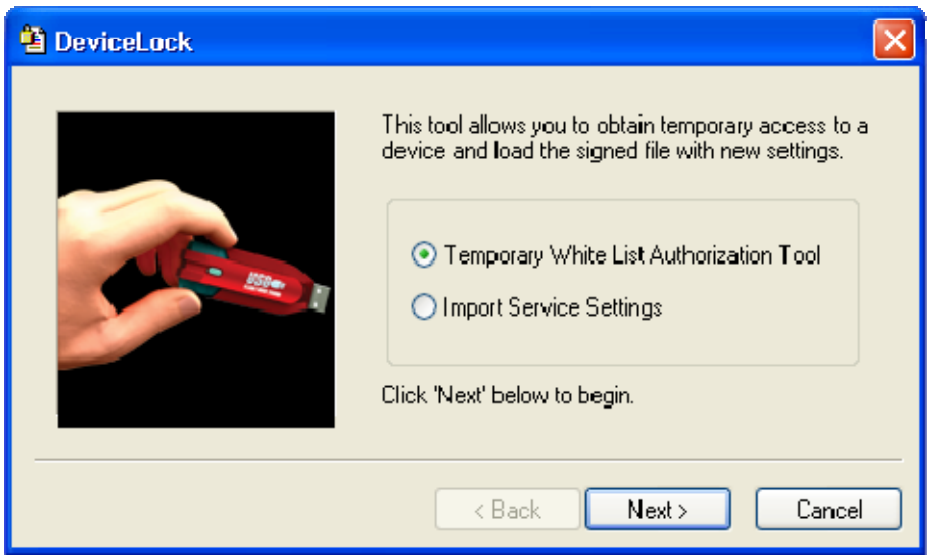
9.2 Temporary White List Authorization Tool

Пользователи используют Temporary White List Authorization Tool для получения временного доступа к устройствам.

Для открытия Temporary White List Authorization Tool пользователь должен запустить *DeviceLock* из панели управления Windows и выбрать опцию *Temporary White List Authorization Tool*.



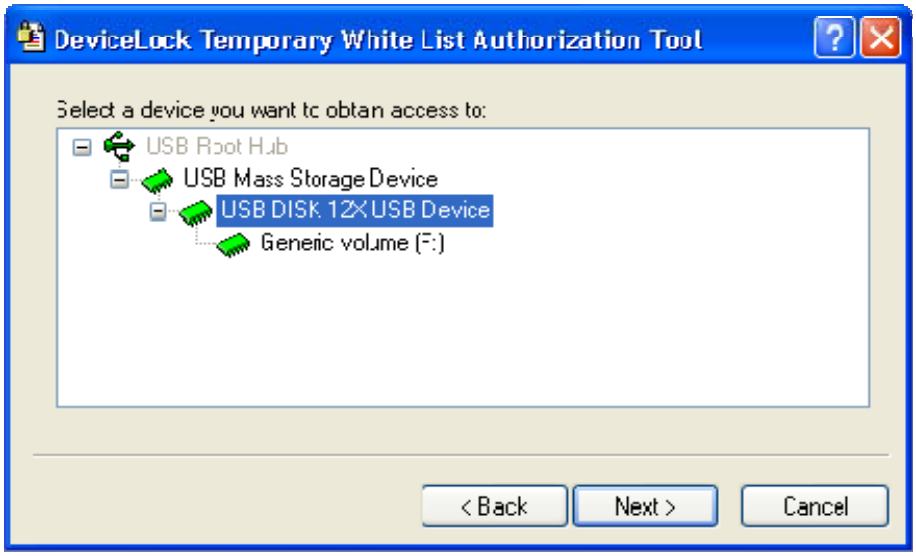
ПРИМЕЧАНИЕ: В Windows XP и более поздних версиях ОС пользователь должен переключить отображение панели управления в стандартный режим для получения доступа ко всем возможным приложениям.



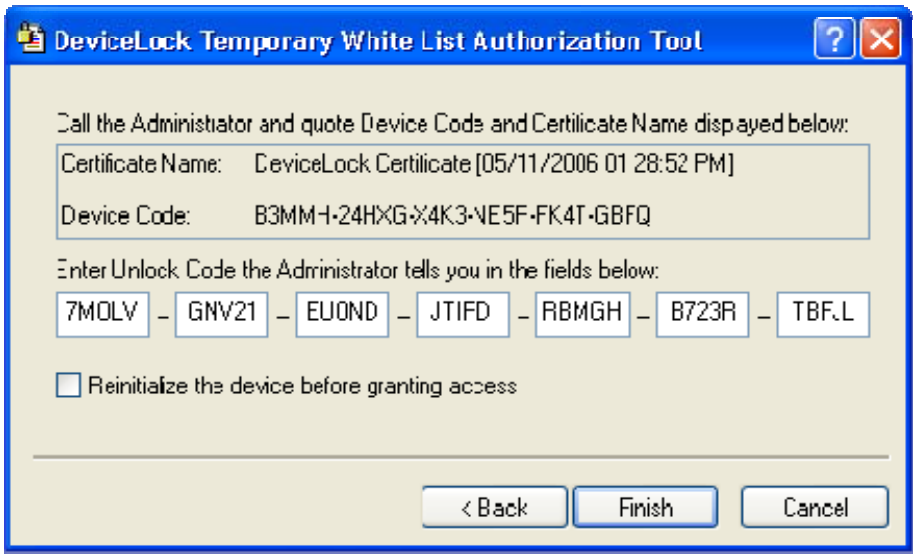
Получение временного доступа к устройству выполняется в пять простых шагов:

1. Подключите требуемое устройство к USB-порту.

2. Выберите устройство из списка доступных USB-устройств.



3. Свяжитесь с администратором и передайте ему имя сертификата и **Код Устройства**. Помните, что **Код Устройства** действителен только в течение 24 часов с момента его создания.



4. Введите **Разблокирующий Код**, полученный от администратора.

   Если есть необходимость переинициализировать (переподключить) устройство до того, как будет предоставлен к нему доступ, установите флаг *Reinitialize device before granting access*.

   Некоторые USB-устройства (такие как мышь) не будут работать без переинициализации, поэтому рекомендуется оставить этот флаг включенным для устройств без файловой системы.

   Мы рекомендуем снимать флаг *Reinitialize device before granting access* для устройств с файловой системой (такие как дисководы, CD/DVD-приводы, флеш-диски и т.п.).

   Некоторые устройства вообще не могут быть переинициализированы из DeviceLock Service. Это означает, что драйвера этих устройств не поддерживают программное переподключение. Если такое устройство было добавлено в белый список, но доступ к нему не предоставляется, пользователь должен вручную переподключить его.

5. Нажмите на кнопку *Finish*. Если **Разблокирующий Код** действителен, через несколько секунд доступ к устройству будет предоставлен.

Все успешные попытки добавить устройство во временный белый список протоколируются, если протоколирование изменений в настройках DeviceLock Service включено в Service Options.

10 Приложение

10.1 Примеры задания разрешений и правил аудита

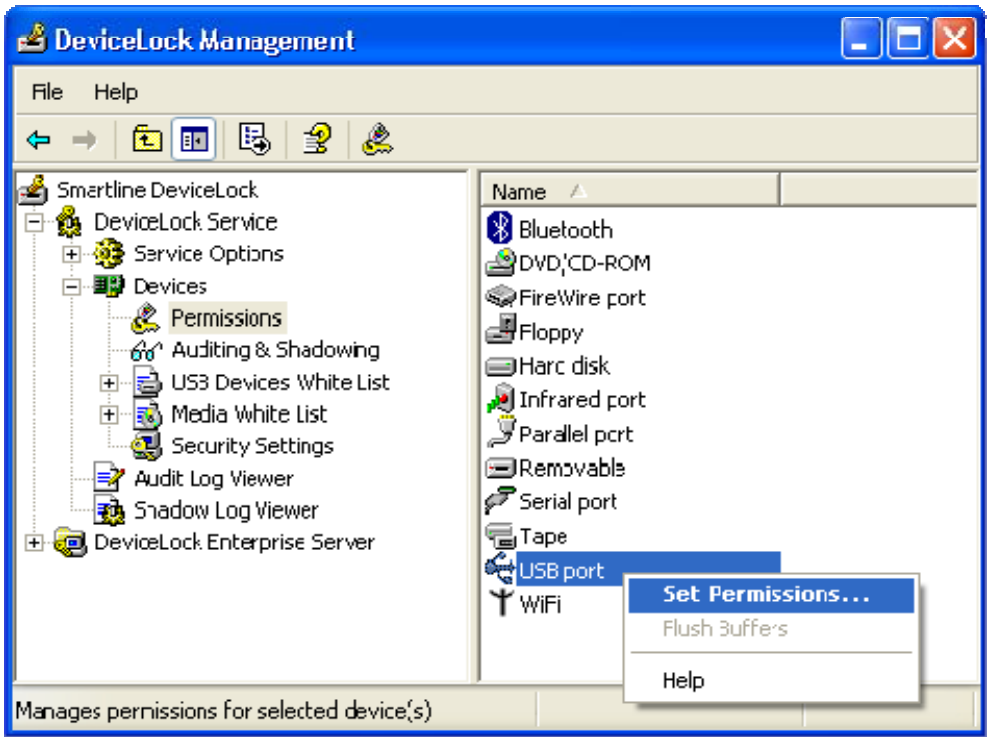
Используя следующие примеры, вы сможете лучше понять, как правильно устанавливать разрешения, правила аудита и теневого копирования в DeviceLock.

Все примеры подразумевают, что вы используете DeviceLock Management Console (оснастка для MMC) и эта консоль уже подключена к компьютеру, на котором запущен DeviceLock Service. Чтобы получить дополнительную информацию относительно использования DeviceLock Management Console, обратитесь к разделу **DeviceLock Management Console** данного руководства.

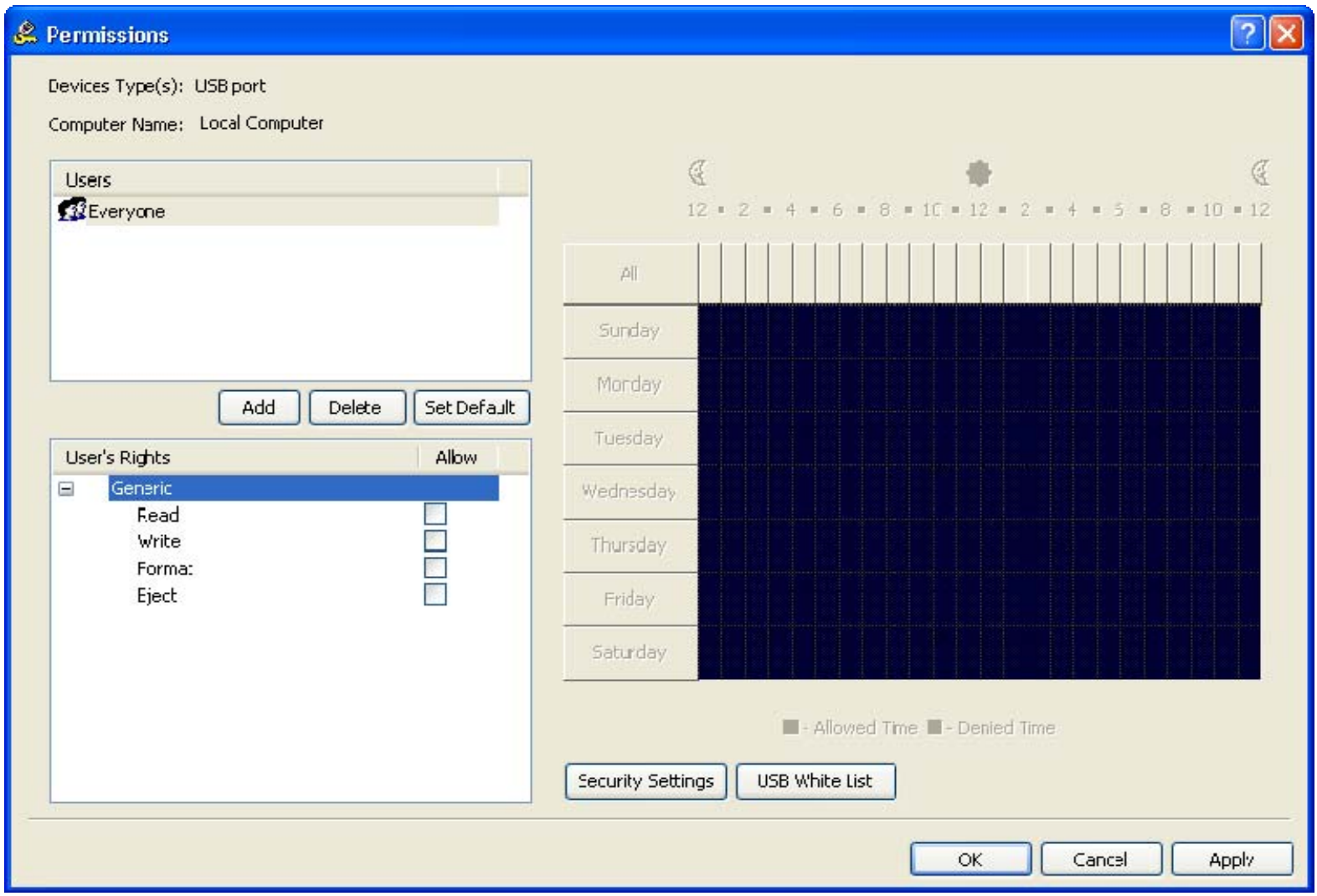
10.1.1 Примеры разрешений

- **Для всех пользователей запрещены все USB-устройства, исключая клавиатуры и мыши:**

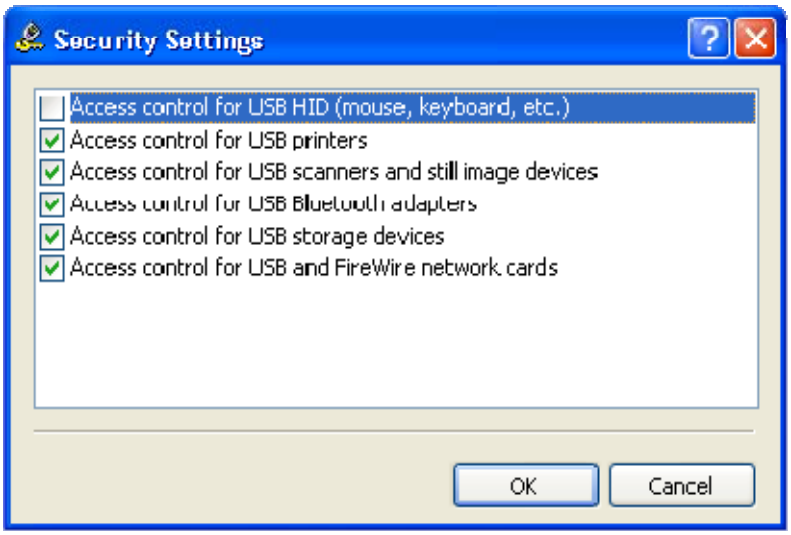
1. Выберите запись *USB port* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и отключите для нее все права в списке *User's Rights*.



3. Нажмите на кнопку *Security Settings* в диалоге *Permissions*, затем снимите флаг *Access control for USB HID (mouse, keyboard, etc.)* как показано на рисунке ниже.

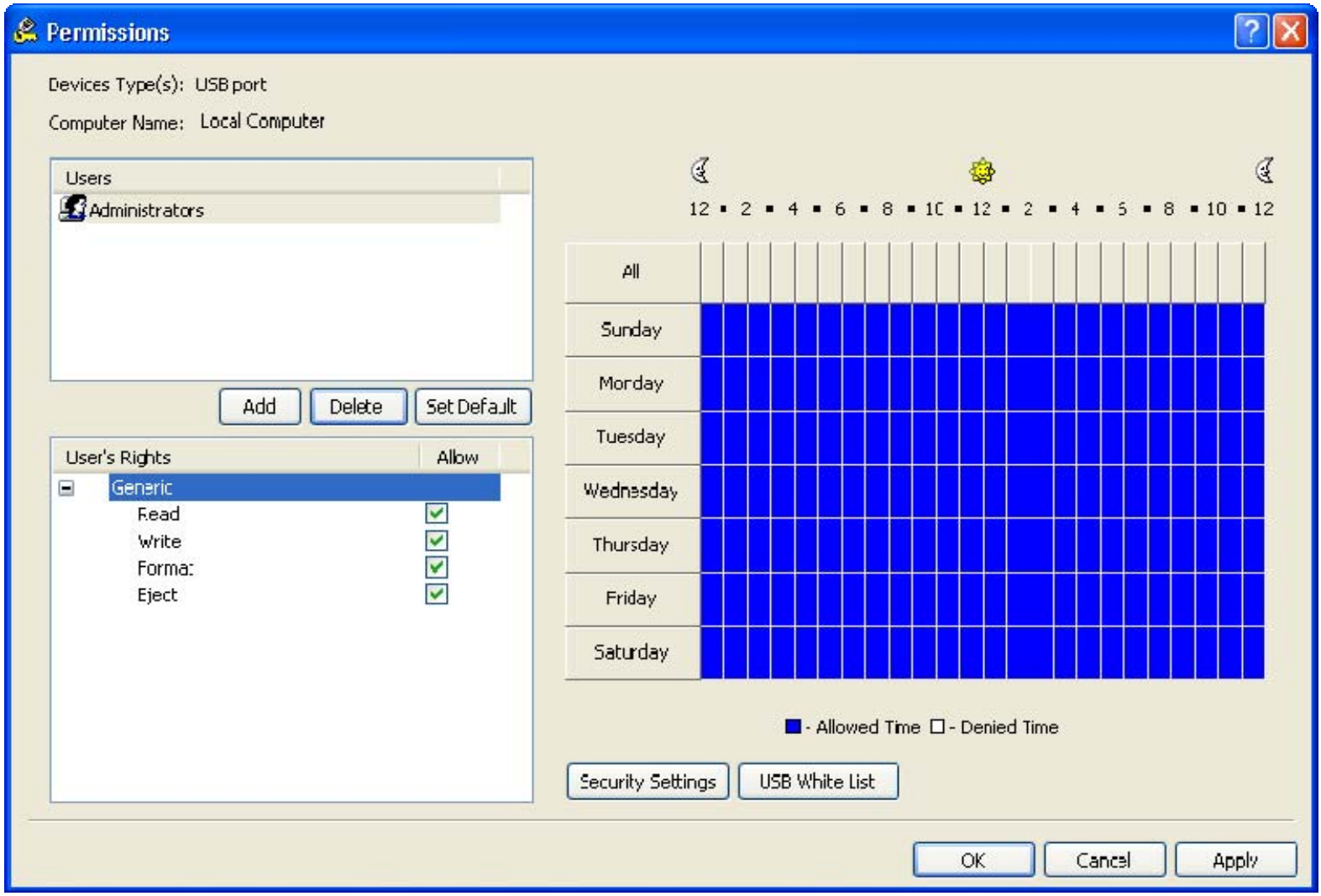


4. Нажмите *OK*, чтобы закрыть диалог *Security Settings*, нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*, затем нажмите *Yes*, чтобы подтвердить, что вы действительно хотите запретить доступ к USB для всех.

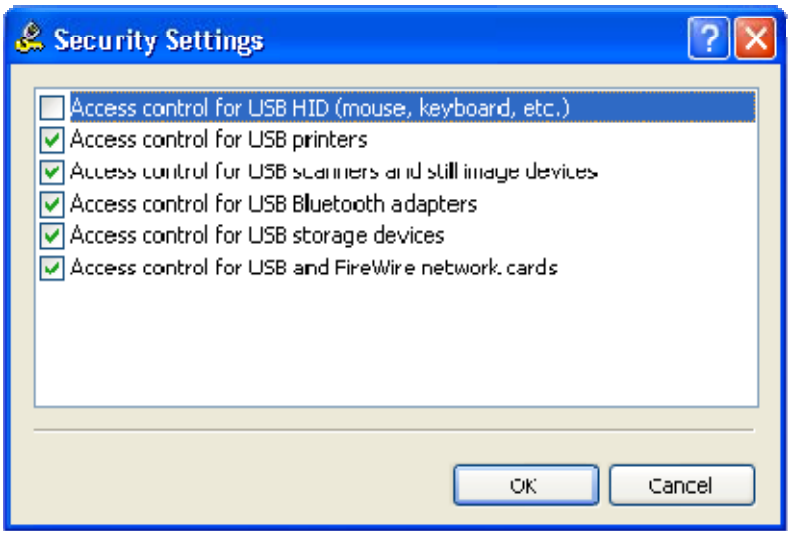
- **Для всех пользователей запрещены все USB-устройства, исключая клавиатуры и мыши, но члены группы *Администраторы* могут использовать любые USB-устройства:**

1. Выберите запись *USB port* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню доступного по нажатию правой кнопки мыши.

2. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте группу *Администраторы*, нажмите *OK*, чтобы закрыть диалог выбора группы, выделите запись *Администраторы* и включите для нее все права в списке *User's Rights*.



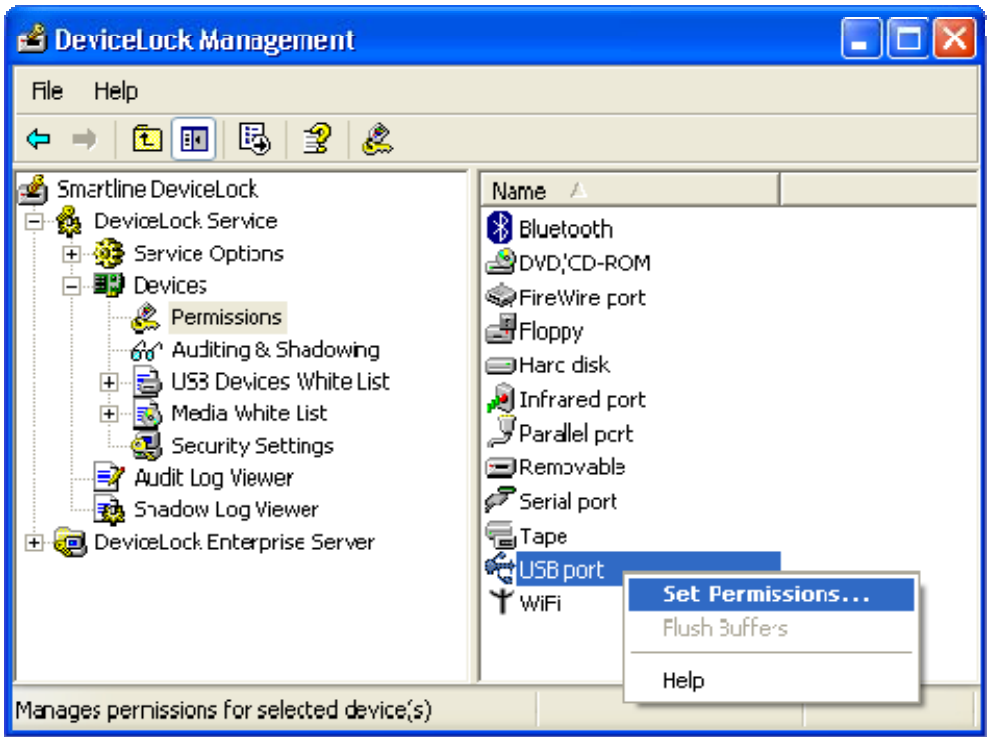
3. Нажмите на кнопку *Security Settings* в диалоге *Permissions*, затем снимите флаг *Access control for USB HID (mouse, keyboard, etc.)*.



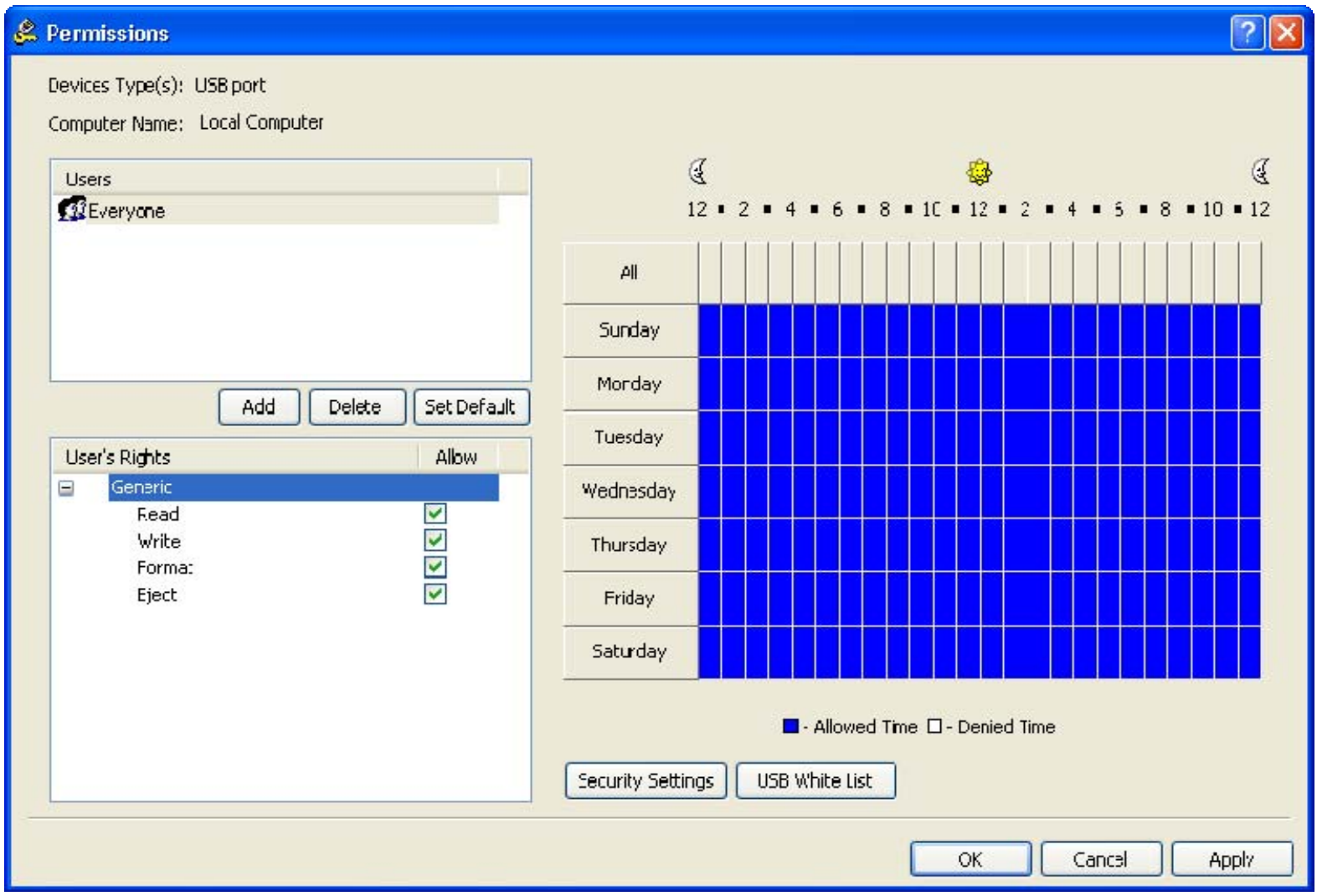
4. Нажмите *OK*, чтобы закрыть диалог *Security Settings*, затем нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*.

- **Для всех пользователей запрещены все устройства хранения данных, исключая внутренние жесткие диски, но все USB-устройства, не предназначенные для хранения данных – разрешены:**

1. Выберите запись *USB port* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню, доступного по нажатию правой кнопки мыши.

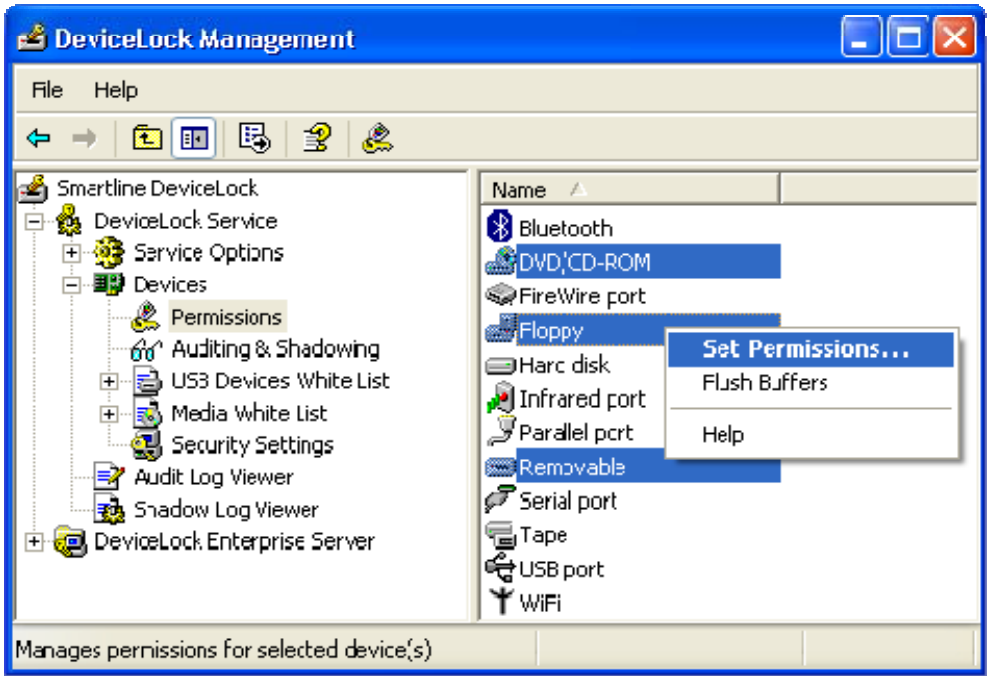


2. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и включите для нее все права в списке *User's Rights*.

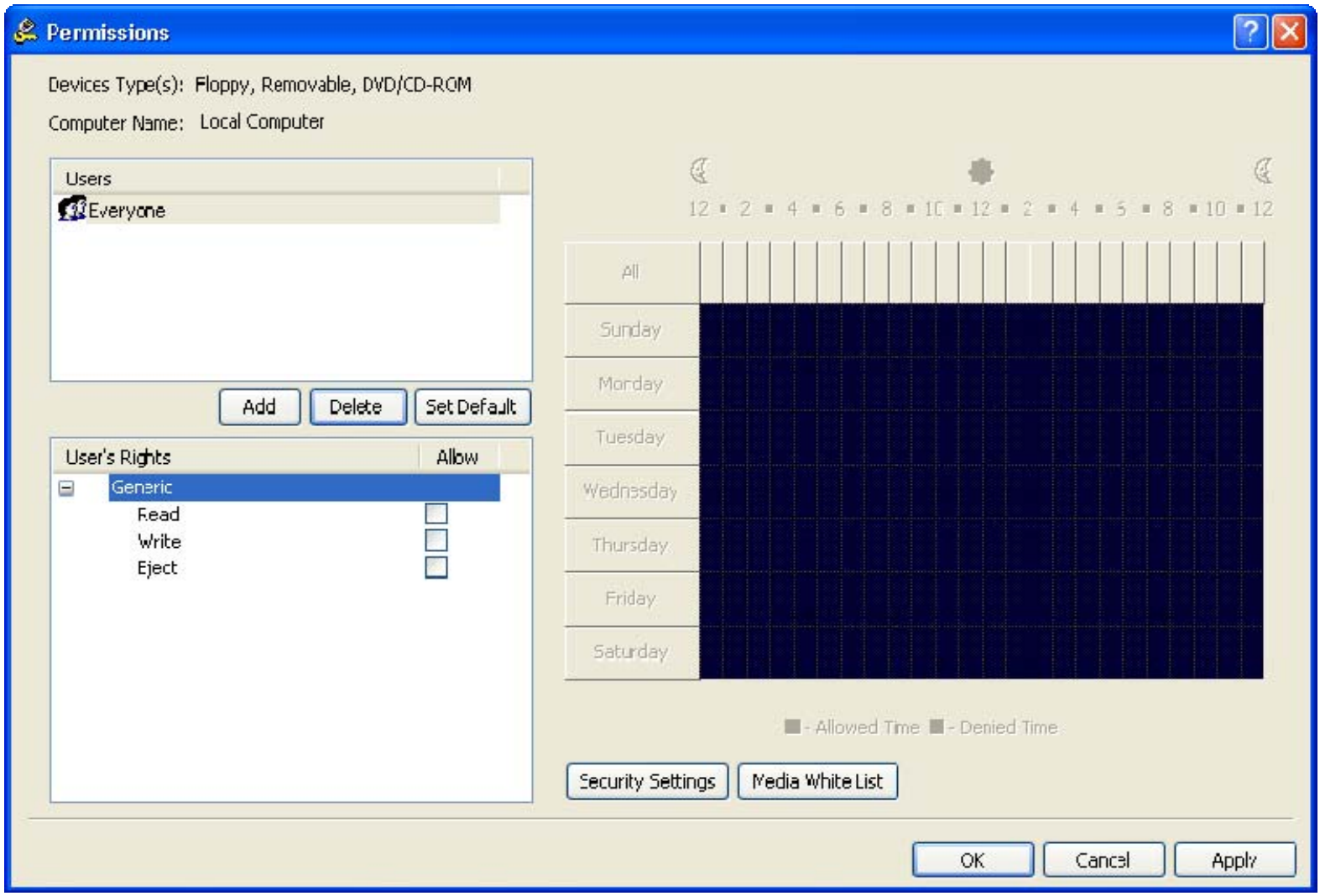


3. Нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*.

4. Выберите записи *DVD/CD-ROM*, *Floppy* и *Removable* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню, доступного по нажатию правой кнопки мыши.



5. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и отключите для нее все права в списке *User's Rights*.



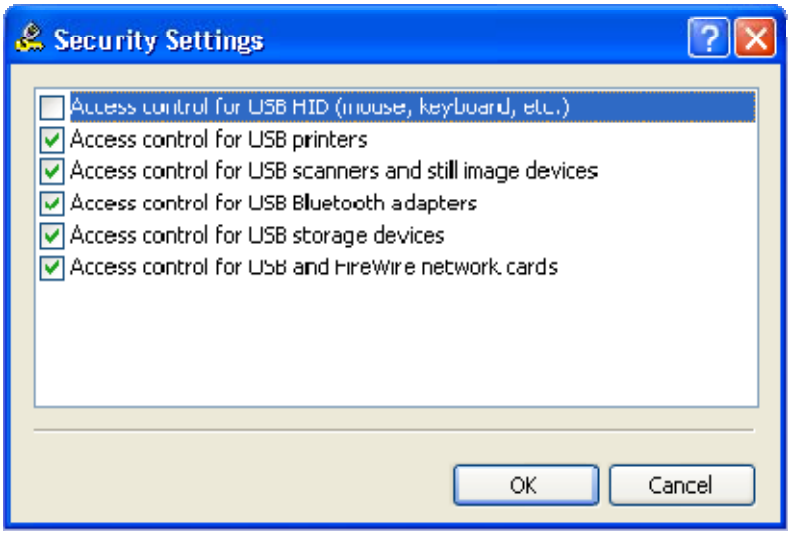
6. Нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*, затем нажмите *Yes*, чтобы подтвердить, что вы действительно хотите запретить доступ к этим устройствам для всех.

- **Для всех пользователей запрещены все USB-устройства, исключая клавиатуры и мыши, но члены группы *Администраторы* могут использовать определенную модель USB-флешки:**

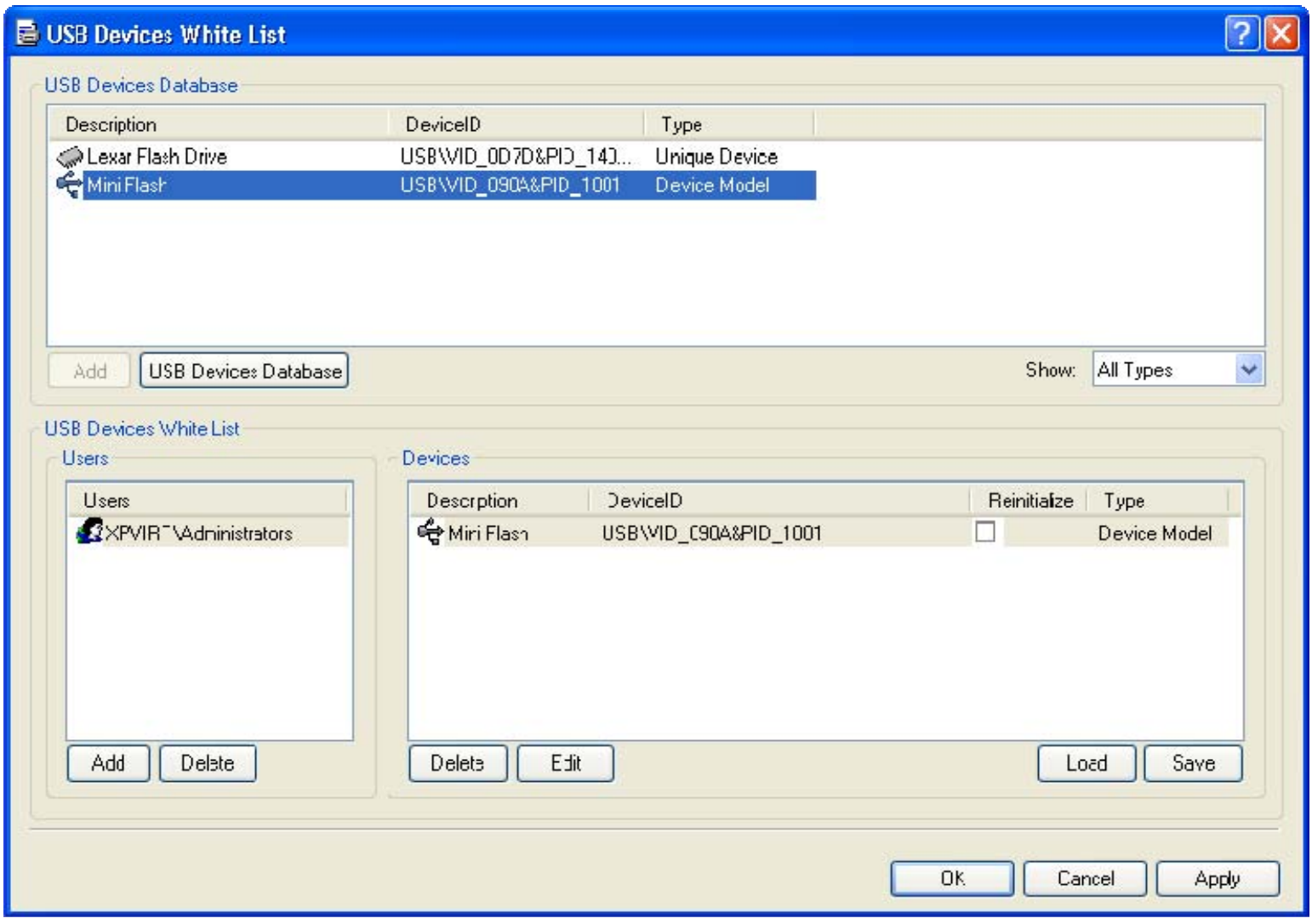
1. Выберите запись *USB port* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню, доступного по нажатию правой кнопки мыши.

2. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и отключите для нее все права в списке *User's Rights*.

3. Нажмите на кнопку *Security Settings* в диалоге *Permissions*, затем снимите флаг *Access control for USB HID (mouse, keyboard, etc.)* как показано на рисунке ниже.



4. Нажмите *OK*, чтобы закрыть диалог *Security Settings*, и затем нажмите на кнопку *USB White List* в диалоге *Permissions*.



5. Нажмите на кнопку *Add* под списком *Users*, добавьте группу *Администраторы*, нажмите *OK*, чтобы закрыть диалог выбора группы и выделите запись *Администраторы*.

6. Выделите нужную модель устройства в списке *USB Devices Database*, затем нажмите на кнопку *Add* под этим писком.

   Если в списке *USB Devices Database* нет записей, то нажмите на кнопку *USB Devices Database* под этим списком и затем добавьте устройства, как описано в разделе **База данных устройств** данного руководства. Когда вы закончите добавлять устройства в базу данных, нажмите *OK*, чтобы сохранить базу данных и закрыть диалог *USB Devices Database*.

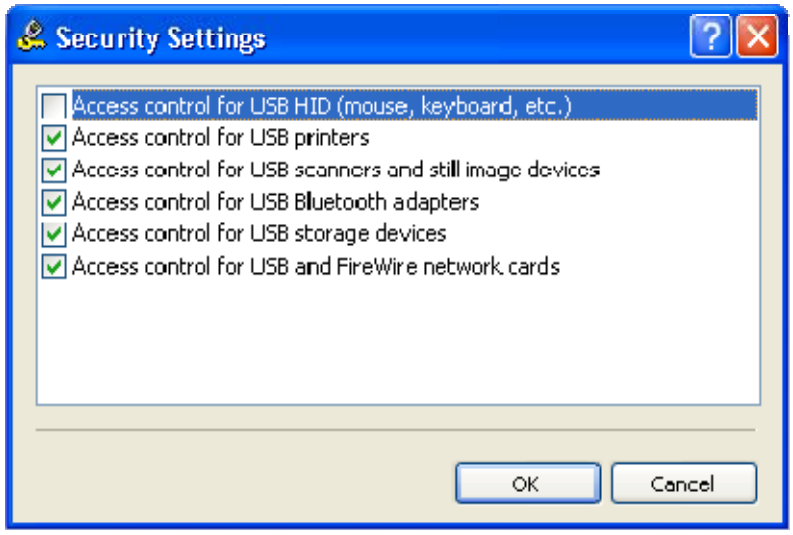
7. Нажмите *OK*, чтобы сохранить изменения в белом списке и закрыть диалог *USB Devices White List*, нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*, затем нажмите *Yes*, чтобы подтвердить, что вы действительно хотите запретить доступ к USB для всех.

- **Для всех пользователей запрещены все USB-устройства, исключая клавиатуры и мыши, но члены группы *Администраторы* могут использовать только определенный экземпляр USB-флешки:**

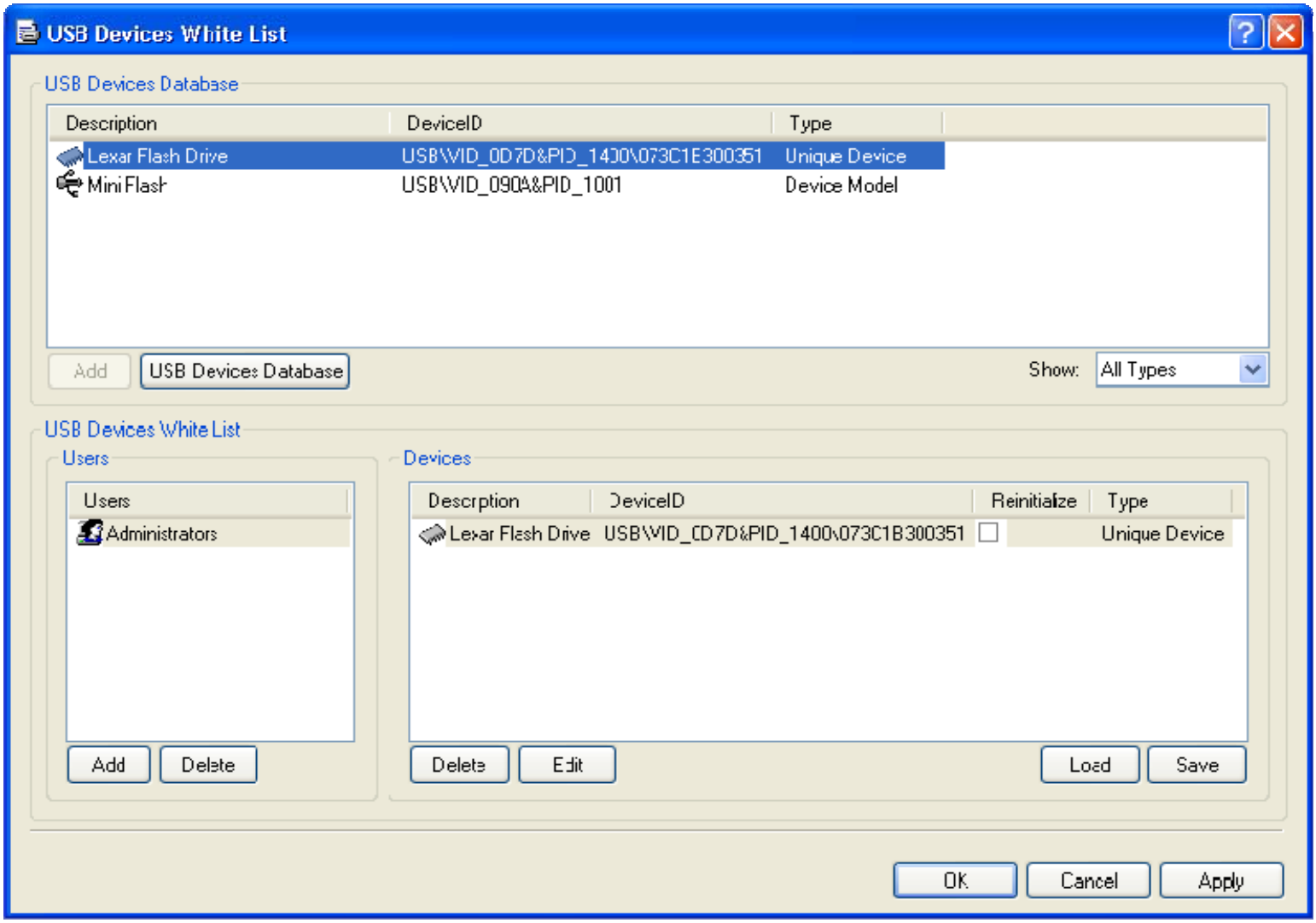
1. Выберите запись *USB port* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню, доступного по нажатию правой кнопки мыши.

2. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и отключите для нее все права в списке *User's Rights*.

3. Нажмите на кнопку *Security Settings* в диалоге *Permissions*, затем снимите флаг *Access control for USB HID (mouse, keyboard, etc.),* как показано на рисунке ниже.



4. Нажмите *OK*, чтобы закрыть диалог *Security Settings*, и затем нажмите на кнопку *USB White List* в диалоге *Permissions*.



5. Нажмите на кнопку *Add* под списком *Users*, добавьте группу *Администраторы*, нажмите *OK*, чтобы закрыть диалог выбора группы и выделите запись *Администраторы*.

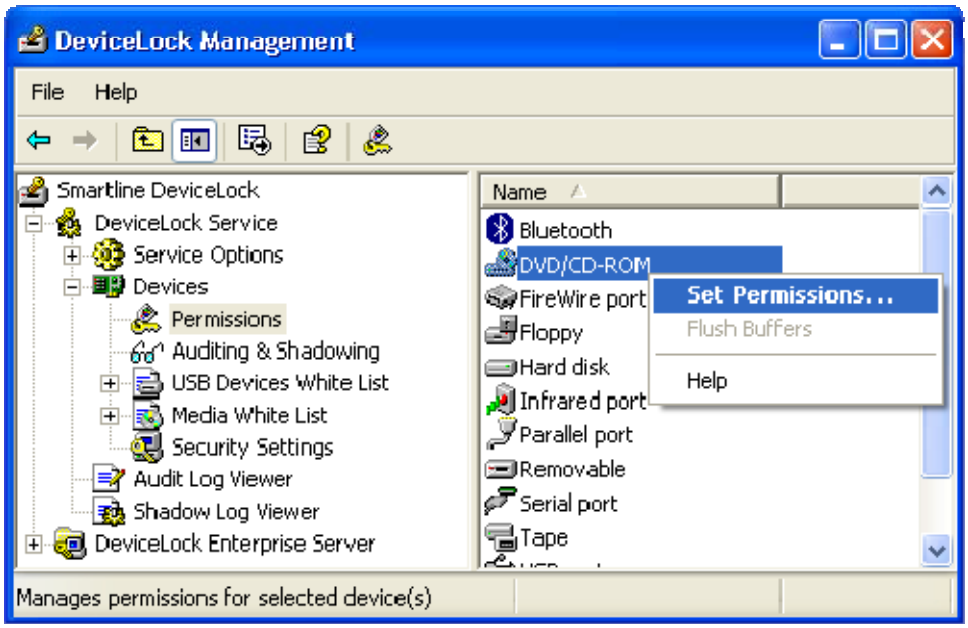
6. Выделите нужное уникальное устройство в списке *USB Devices Database*, затем нажмите на кнопку *Add* под этим писком.

   Если в списке *USB Devices Database* нет записей, то нажмите на кнопку *USB Devices Database* под этим списком и затем добавьте устройства как описано в разделе **База данных устройств** данного руководства. Когда вы закончите добавлять устройства в базу данных, нажмите *OK*, чтобы сохранить базу данных и закрыть диалог *USB Devices Database*.

7. Нажмите *OK*, чтобы сохранить изменения в белом списке и закрыть диалог *USB Devices White List*, нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*, затем нажмите *Yes*, чтобы подтвердить, что вы действительно хотите запретить доступ к USB для всех.

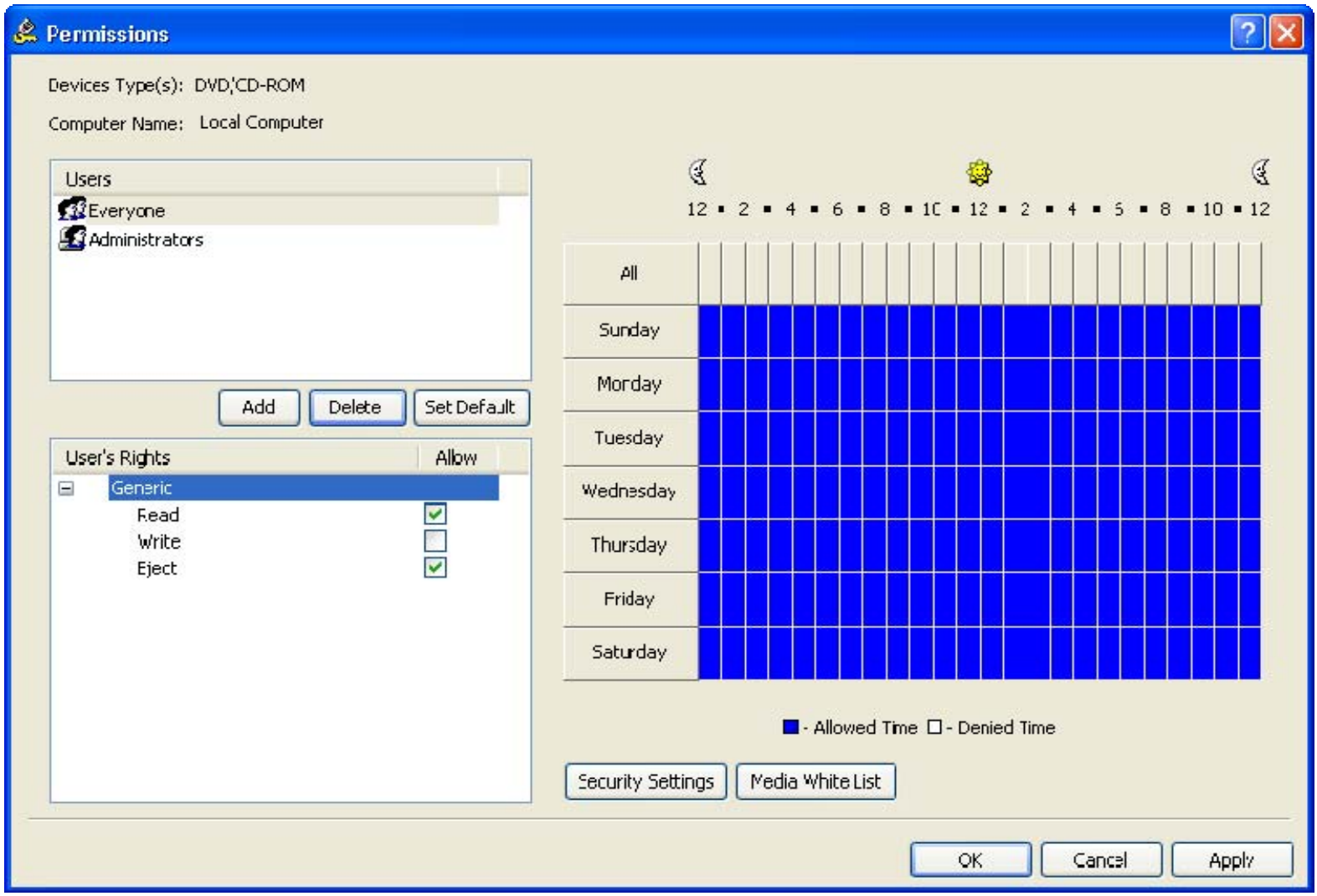
- **Для всех пользователей все приводы CD и DVD установлены в режим только для чтения, но члены группы *Администраторы* могут записывать CD и DVD-диски:**

1. Выберите запись *DVD/CD-ROM* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте группу *Администраторы*, нажмите *OK*, чтобы закрыть диалог выбора группы, выделите запись *Администраторы* и включите для нее все права в списке *User's Rights*.

3. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и отключите для нее право **Write** в списке *User's Rights*.



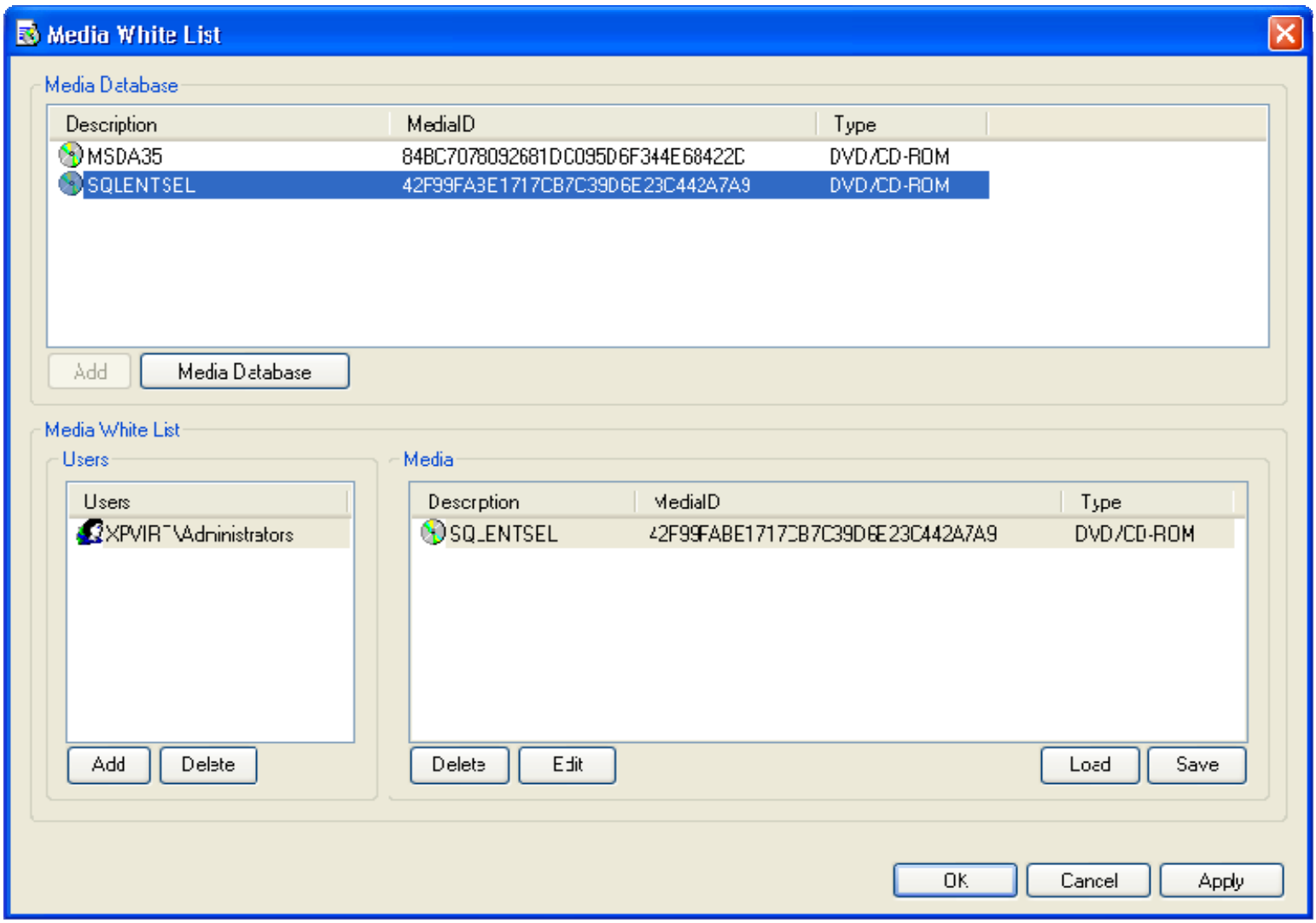
4. Нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*.

- **Для всех пользователей все приводы CD и DVD запрещены, но члены группы *Администраторы* могут читать определенный диск:**

1. Выберите запись *DVD/CD-ROM* из списка типов устройств в разделе *Permissions*, затем выберите *Set Permissions* из контекстного меню, доступного по нажатию правой кнопки мыши.

2. Нажмите на кнопку *Add* в диалоге *Permissions*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и отключите для нее все права в списке *User's Rights*.

3. Нажмите на кнопку *Media White List* в диалоге *Permissions*.



4. Нажмите на кнопку *Add* под списком *Users*, добавьте группу *Администраторы*, нажмите *OK*, чтобы закрыть диалог выбора группы и выделите запись *Администраторы*

5. Выделите нужный носитель в списке *Media Database*, затем нажмите на кнопку *Add* под этим списком

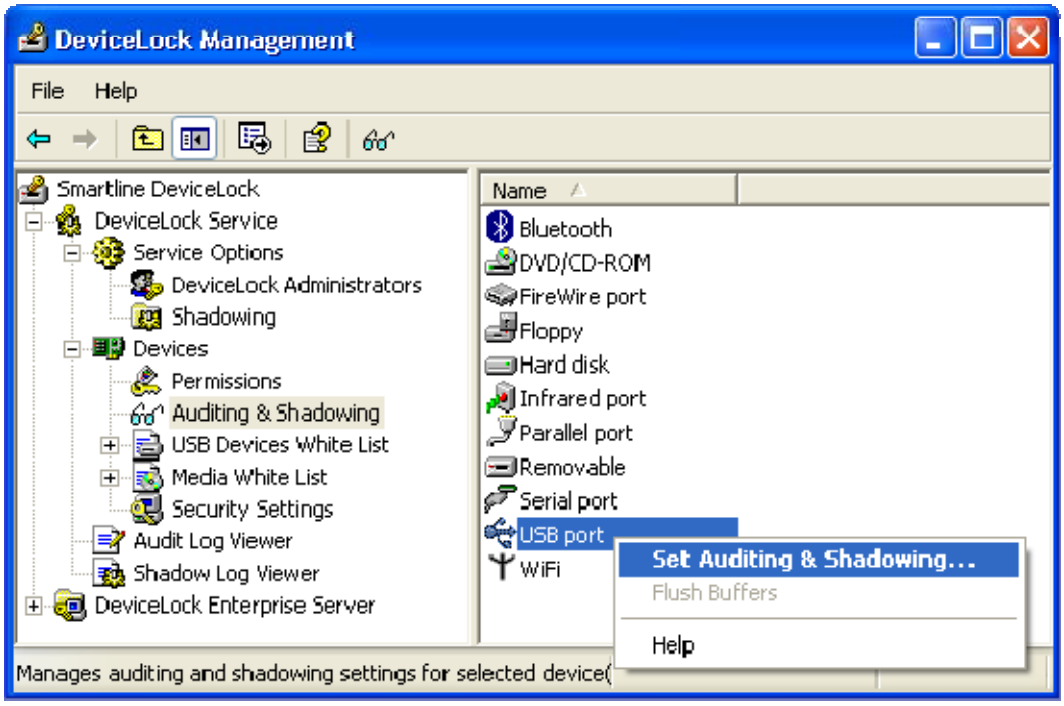
   Если в списке *Media Database* нет записей, то нажмите на кнопку *Media Database* под этим списком и затем добавьте носители, как описано в разделе **База данных носителей** данного руководства. Когда вы закончите добавлять носители в базу данных, нажмите *OK*, чтобы сохранить базу данных и закрыть диалог *Media Database*.

6. Нажмите *OK*, чтобы сохранить изменения в белом списке и закрыть диалог *Media White List*, нажмите *OK*, чтобы применить настройки и закрыть диалог *Permissions*, затем нажмите *Yes*, чтобы подтвердить, что вы действительно хотите запретить доступ к CD/DVD-приводам для всех.

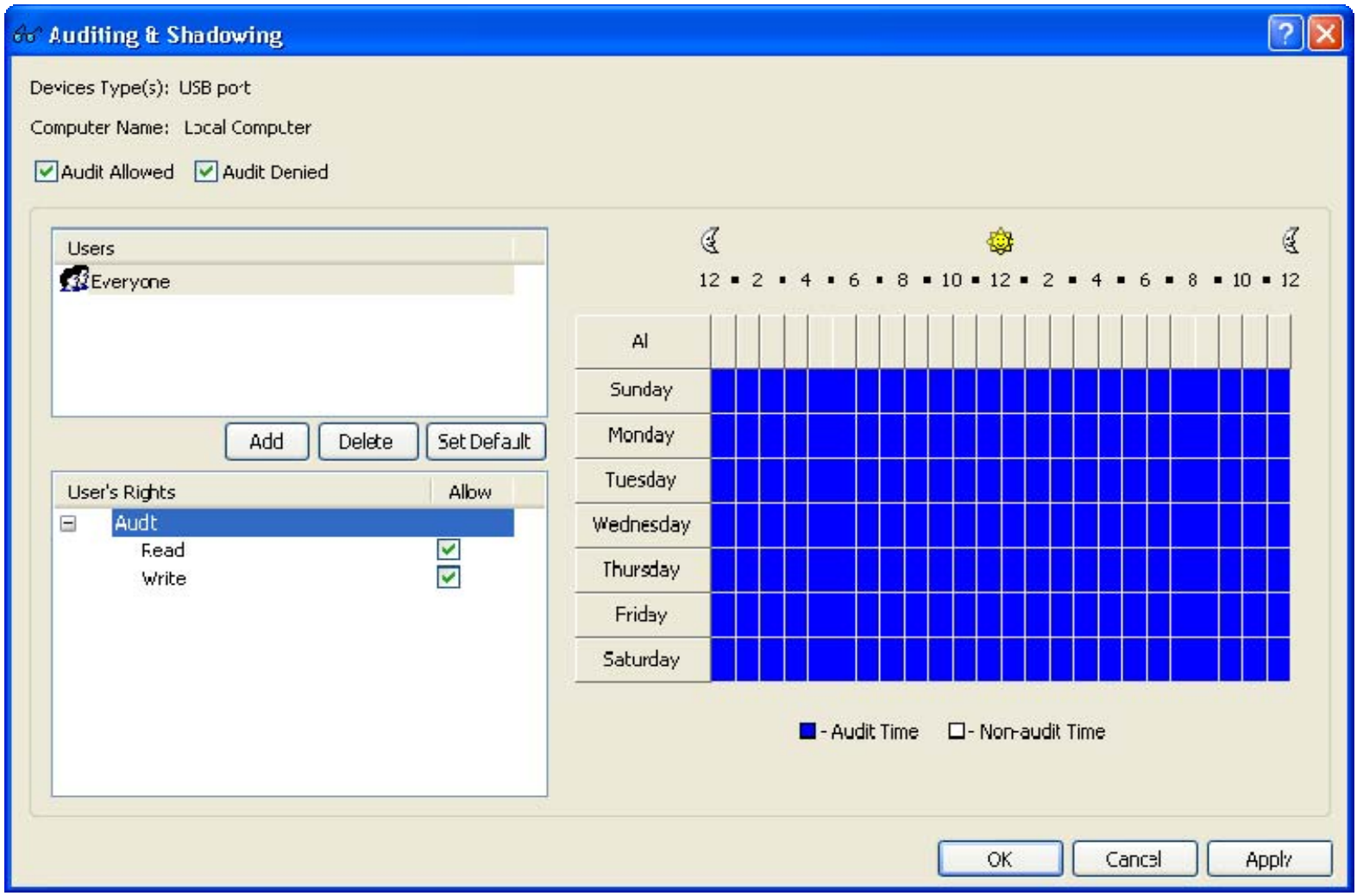
10.1.2 Примеры правил аудита и теневого копирования

- **Протоколируются события вставки, удаления и попытки доступа для всех USB-устройств для всех пользователей:**

1. Выберите запись *USB port* из списка типов устройств в разделе *Auditing & Shadowing*, затем выберите *Set Auditing & Shadowing* из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Нажмите на кнопку *Add* в диалоге *Audit*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*) и включите для нее права аудита **Read** и **Write** в списке *User's Rights*

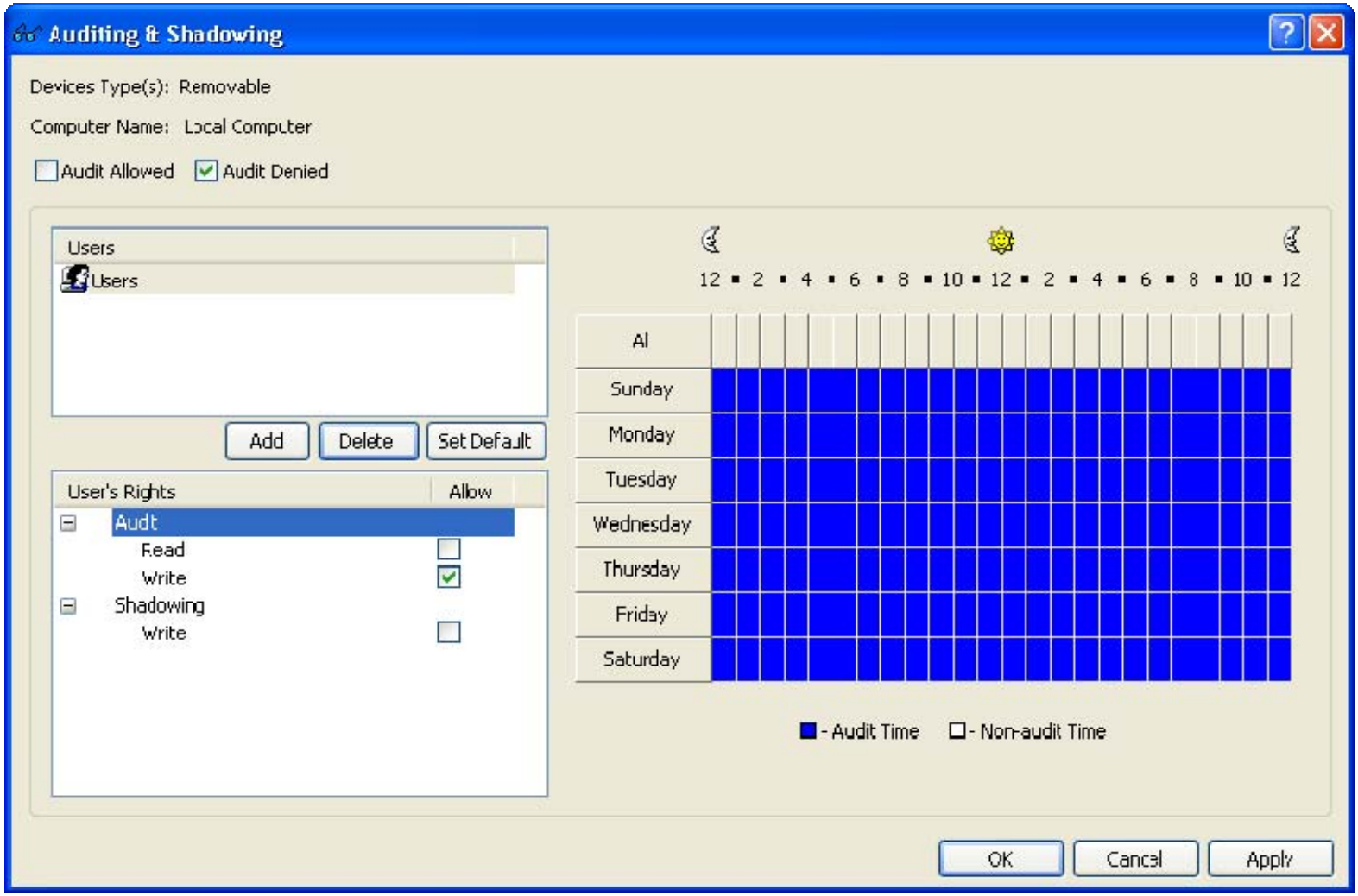


3. Установите флаги *Audit Allowed* и *Audit Denied,* находящиеся в верхней части диалога *Audit*, затем нажмите *OK*, чтобы применить настройки и закрыть диалог *Auditing & Shadowing*.

- **Протоколируются имена файлов и директорий только при запрещенных попытках записи на сменные накопители для членов группы *Пользователи*:**

1. Выберите запись *Removable* из списка типов устройств в разделе *Auditing & Shadowing*, затем выберите *Set Auditing & Shadowing* из контекстного меню, доступного по нажатию правой кнопки мыши.

2. Нажмите на кнопку *Add* в диалоге *Audit*, добавьте группу *Пользователи*, нажмите *OK*, чтобы закрыть диалог выбора группы, выделите запись *Пользователи* и включите для нее только право аудита **Write** в списке *User's Rights*.

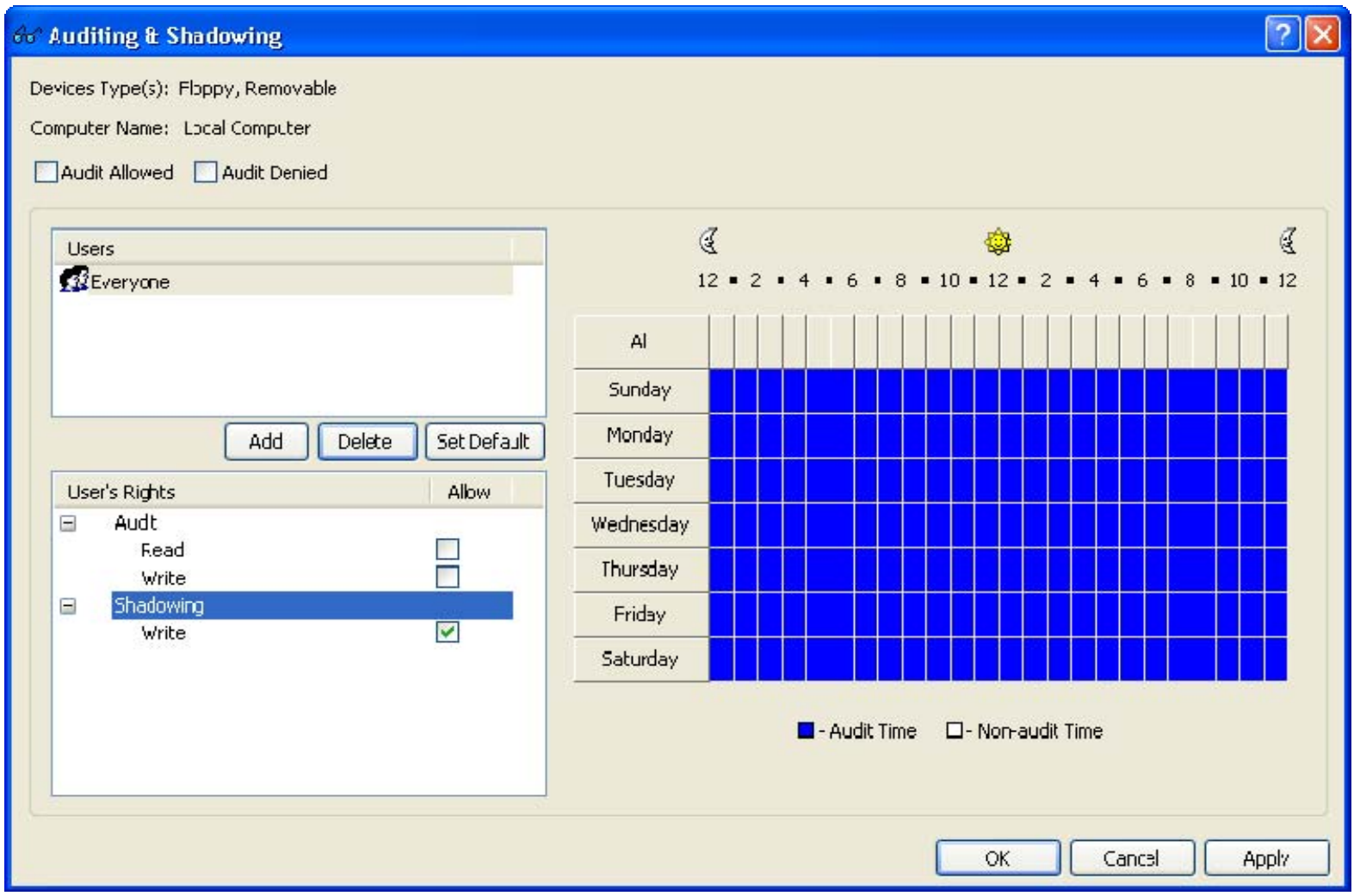


3. Установите только флаг *Audit Denied* находящийся вверху диалога *Audit*, затем нажмите *OK*, чтобы применить настройки и закрыть диалог *Auditing & Shadowing*.

- **Включено теневое копирование для всех данных, записываемых на сменные носители и дискеты любым пользователем:**

1. Выберите записи *Floppy* и *Removable* из списка типов устройств в разделе *Auditing & Shadowing*, затем выберите *Set Auditing & Shadowing* из контекстного меню.

2. Нажмите на кнопку *Add* в диалоге *Audit*, добавьте пользователя *Все* (*Everyone*), нажмите *OK*, чтобы закрыть диалог выбора пользователя, выделите запись *Все* (*Everyone*), отключите для нее все права аудита и включите только право теневого копирования **Write** в списке *User's Rights*.



3. Нажмите *OK*, чтобы применить настройки и закрыть диалог *Auditing & Shadowing*.

