# DeviceLock®

**Защита Вашей Конфиденциальной Информации**

## Зачем **контролировать** устройства

Информация, которую вы стремитесь закрыть и спрятать за файрволами, в пределах периметра, словно протекает сквозь ваши пальцы. Представьте, сколько утечек данных происходит по вине инсайдеров или даже лояльных сотрудников, просто копирующих конфиденциальные файлы со своих рабочих компьютеров на мобильные телефоны, КПК, MP3-плееры, цифровые фотоаппараты или на любые другие современные мобильные устройства. Информация становится текучей и неконтролируемой. Вы не знаете, в чьи руки она в конце концов попадет.

SmartLine
Proactive Network Security

Использование неавторизованных USB-устройств представляет угрозу корпоративным сетям и данным. Причем не только конфиденциальная информация может «уйти» из корпоративной сети через USB-порт, но и вирусы или троянские программы могут быть занесены внутрь корпоративной сети, минуя серверные файрволы и антивирусы. Точно так же дело обстоит с записывающими CD/DVD-приводами и с FireWire-устройствами. Современные MP3-плееры имеют объемные встроенные жесткие диски и быстрые интерфейсы для подключения к компьютеру.

Тут как раз и приходит на помощь программное решение DeviceLock, которое с 1996 года разрабатывает российская компания «Смарт Лайн Инк». Механизм аутентификации портов и устройств, встроенный в DeviceLock, является незаменимым и подчас безальтернативным решением проблем внутренней корпоративной безопасности.

Обеспечивая контроль над пользователями, имеющими доступ к портам и устройствам локального компьютера, DeviceLock закрывает потенциальную гигантскую брешь в защите простым и экономичным способом. DeviceLock полностью интегрируется в подсистему безопасности Windows, функционируя на уровне ядра системы, и обеспечивает прозрачную для пользователя защиту.

DeviceLock®

**Утечки данных происходят, когда информация копируется на мобильные устройства**

DeviceLock позволяет контролировать весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, параллельные и последовательные порты, WiFi и Bluetooth-адаптеры, любые внутренние и внешние сменные накопители и жесткие диски. DeviceLock осуществляет детальный аудит действий пользователей с устройствами и данными.

DeviceLock может управляться через групповые политики Windows в домене Active Directory, благодаря чему легко интегрируется в существующую инфраструктуру организации любого масштаба.

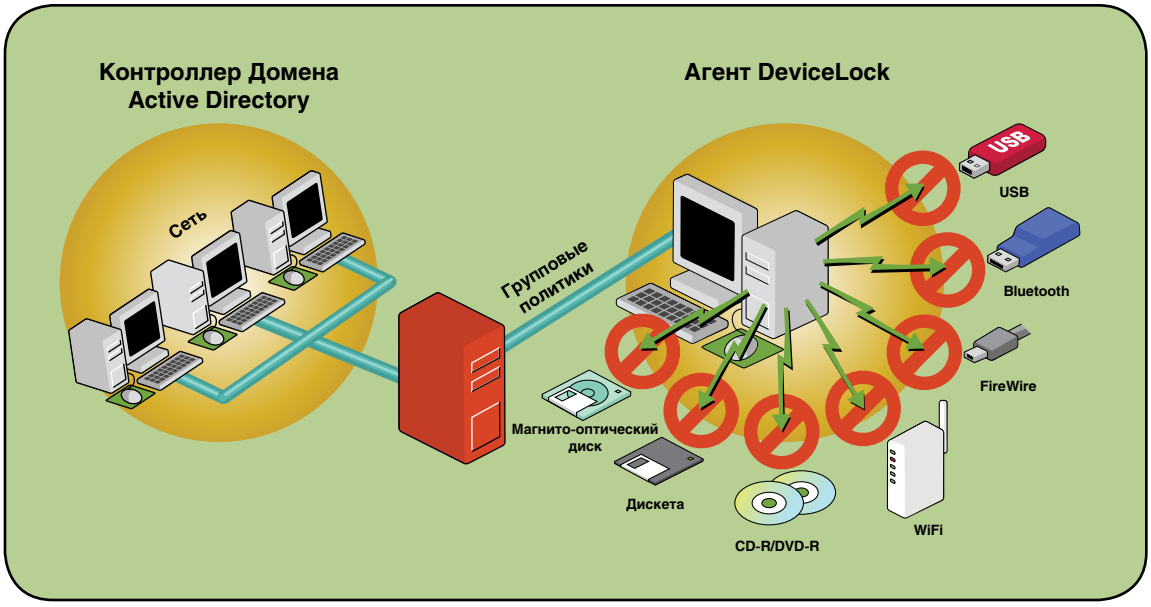
# Как это работает

***DeviceLock состоит из трех частей:***

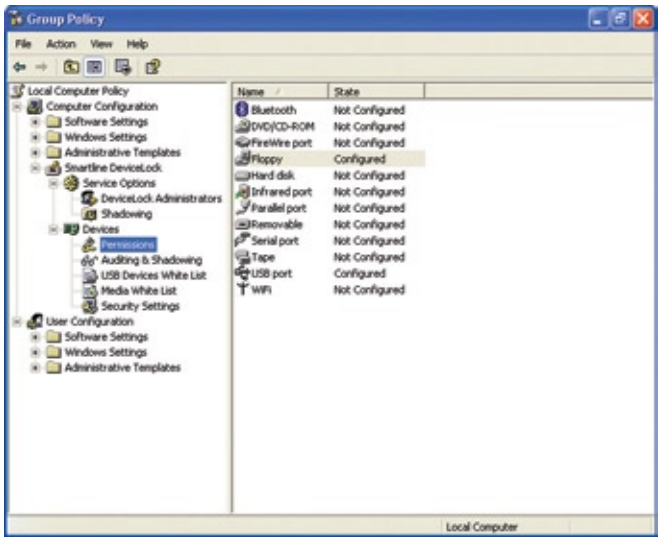
DeviceLock Service – это агент, устанавливаемый на каждый компьютер, который автоматически запускается и обеспечивает защиту устройств на машине-клиенте, в то же время оставаясь невидимым для локального пользователя.

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.

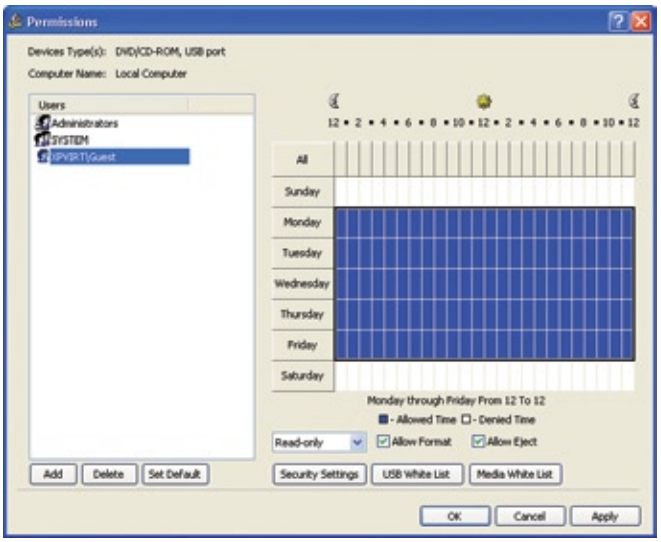
Консоль управления – это интерфейс контроля, который администратор использует для управления системой, на которой установлен агент. DeviceLock поставляется с тремя консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.



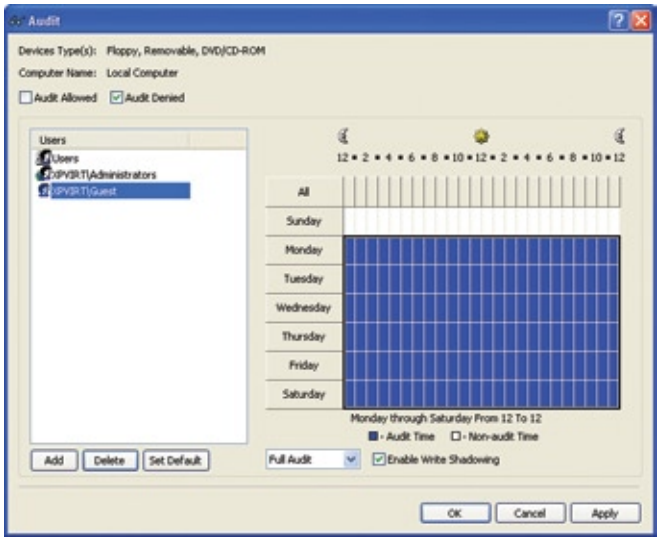

**Предприятия могут легко защищать десятки и сотни тысяч удаленных компьютеров при помощи DeviceLock, используя управление через групповые политики Active Directory.**



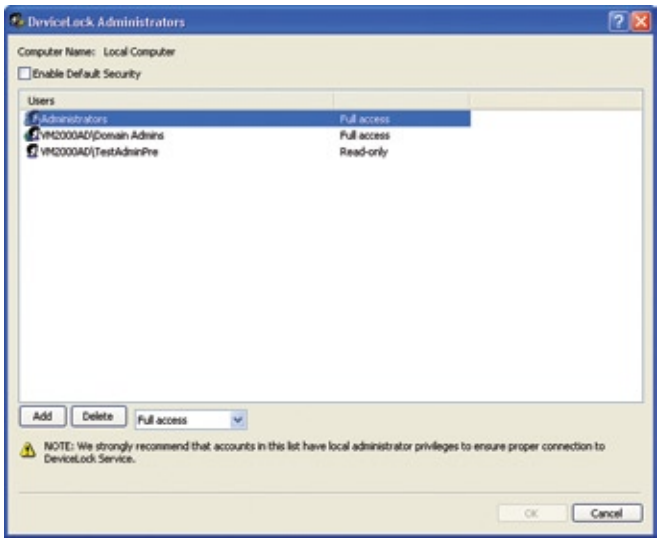

- **DeviceLock Group Policy Manager интегрируется в редактор политик Windows и позволяет управлять настройками DeviceLock через групповые политики.**




- **Администраторы DeviceLock могут назначать пользователей и группы для выбранных устройств, устанавливать тип и время доступа для них.**




- **Администраторы DeviceLock могут настроить протоколирование действий пользователей с устройствами и файлами, а также включить теневое копирование для определенного пользователя или группы.**




- **Когда включена защита агента DeviceLock, никто, исключая авторизованных администраторов, не может подключаться к агенту, останавливать или удалять его.**

# DeviceLock® является элегантным, простым и масштабируемым решением для контроля устройств и портов

[ www.smartline.ru ]

# Основные функции DeviceLock

**Контроль доступа.** Вы можете контролировать доступ пользователей и групп к устройствам и портам ввода-вывода в зависимости от времени и дня недели. Для сменных носителей, дисководов, жестких дисков и CD/DVD-приводов можно устанавливать тип доступа «*только чтение*».

**Белый список устройств.** Для каждого пользователя или группы можно задать свой список устройств, доступ к которым будет всегда разрешен. Устройства можно идентифицировать по модели и по уникальному серийному номеру.

**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. Для каждого пользователя или группы можно задать свой список носителей.

**Временный белый список.** Позволяет предоставлять временный доступ к устройствам при отсутствии сетевого подключения к агенту. Администратор сообщает пользователю специальный короткий буквенно-цифровой код по телефону, который временно разблокирует доступ только к требуемому устройству.

**Аудит.** Вы можете протоколировать все действия пользователей с устройствами и файлами (копирование, чтение, удаление и т.п.). Также можно протоколировать изменения в настройках DeviceLock, время старта и остановки агента.

**Теневое копирование.** Для каждого пользователя или группы можно сохранять точную копию данных, копируемых на внешние устройства и передаваемых через последовательные и параллельные порты. Точные копии всех файлов и данных сохраняются в SQL-базе данных на сервере.

**Защита от локального администратора.** Даже если пользователи в 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 агенту, останавливать или удалять его. Даже члены локальной группы *Администраторы* (если они не входят в список авторизованных администраторов) не могут обойти защиту.

**Централизованное управление.** DeviceLock имеет систему удаленного управления, позволяющую обеспечивать доступ ко всем возможным функциям программы с рабочего места администратора системы. DeviceLock Management Console представляет из себя оснастку (*snap-in*) для *Microsoft Management Console*, со стандартным интерфейсом, интуитивно понятным любому администратору Windows. Кроме того, для управления DeviceLock в сетях, где не используется Active Directory, предусмотрена дополнительная консоль с собственным интерфейсом – DeviceLock Enterprise Manager.

**Управление через групповые политики Actvie Directory.** DeviceLock может управляться через групповые политики Windows в домене Active Directory посредством стандартной оснастки *Group Policy*, которая входит в состав Windows 2000 и более поздних операционных систем. Полная интеграция в групповые политики Windows позволяет автоматически устанавливать DeviceLock на новые компьютеры, подключаемые к корпоративной сети, и осуществлять настройку для новых компьютеров в автоматическом режиме.

**Поддержка LDAP.** Вы можете выбирать компьютеры напрямую из служб каталогов LDAP (таких как Novell eDirectory, Open LDAP и т.п.).

**Централизованное хранение журналов аудита и теневого копирования.** Для централизованного сбора и хранения данных теневого копирования и журналов аудита используется дополнительный компонент – DeviceLock Enterprise Server. Вы можете установить несколько экземпляров DeviceLock Enterprise Server в вашей сети, чтобы равномерно распределить нагрузку. DeviceLock Enterprise Server использует SQL-сервер для хранения данных.

**Отчеты.** DeviceLock позволяет формировать отчеты по установленным настройкам и по устройствам (USB, FireWire и PCMCIA), которые используют пользователи на своих локальных компьютерах.

**DeviceLock работает вне зависимости от наличия подключения к локальной сети, что обеспечивает защиту для мобильных пользователей**

# Кому необходим DeviceLock

Быстро растущее число пользователей DeviceLock включает государственные органы, работающие с конфиденциальной информацией, и другие средние и крупные компании, нуждающиеся в контроле доступа к устройствам для приема, передачи или обработки данных. Качество и надежность программы подтверждают более 50 тысяч клиентов «Смарт Лайн Инк» во всем мире – банки, страховые компании, военные и государственные организации, крупные корпорации (нефтегазовая отрасль, машиностроение, энергетика) и другие коммерческие организации, медицинские, учебные и научно-исследовательские учреждения.

За время выхода на российский рынок программа завоевала авторитет крупнейших российских компаний, а также компаний малого и среднего бизнеса. Вот что говорят о программе российские клиенты:

«*DeviceLock – это наиболее простое и эффективное программное решение. У нас не возникло никаких проблем с его установкой. Системный администратор и пользователи остались довольны результатами внедрения программы DeviceLock*». (Еськин В.В., начальник отдела информационной безопасности Ханты-Мансийского банка).

«*ПО DeviceLock позволило не только ограничить время и виды используемых сотрудниками Банка внешних носителей информации, но и вести контроль их использования с протоколированием времени и названия модифицируемого файла. Тем самым с внедрением программы был закрыт потенциальный канал утечки информации в информационной системе Банка. Нас также устроило соотношение цены и качества программного продукта DeviceLock*». (Андрей Широков, начальник отдела информационной безопасности Банка «КОЛЬЦО УРАЛА»).

«*Мы пришли к выводу, что DeviceLock – это простое в использовании и относительно недорогое программное решение. Руководство института и системный администратор остались довольны результатами внедрения программы DeviceLock*». (Галина Шипкова, главный специалист отдела информационных технологий ФГУП «Атомэнергопроект»).

«*Использовать программное решение DeviceLock нам рекомендовали в московском представительстве Microsoft. Установить DeviceLock было очень легко. Администрация библиотеки осталась довольна внедрением DeviceLock, так как была устранена основная проблема, связанная с несанкционированным копированием материалов*». (Корытин А.А., заведующий центром информационных технологий, «Российская государственная библиотека»).

**Один из наших клиентов контролирует в своей сети более 68000 агентов DeviceLock с помощью групповых политик**

SmartLine
Proactive Network Security

[ www.smartline.ru ]