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 разрешать и запрещать доступ к определенным типам файлов и контролировать весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, параллельные и последовательные порты, WiFi и Bluetooth-адаптеры, ленточные накопители, КПК и смартфоны, сетевые и локальные принтеры, 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.

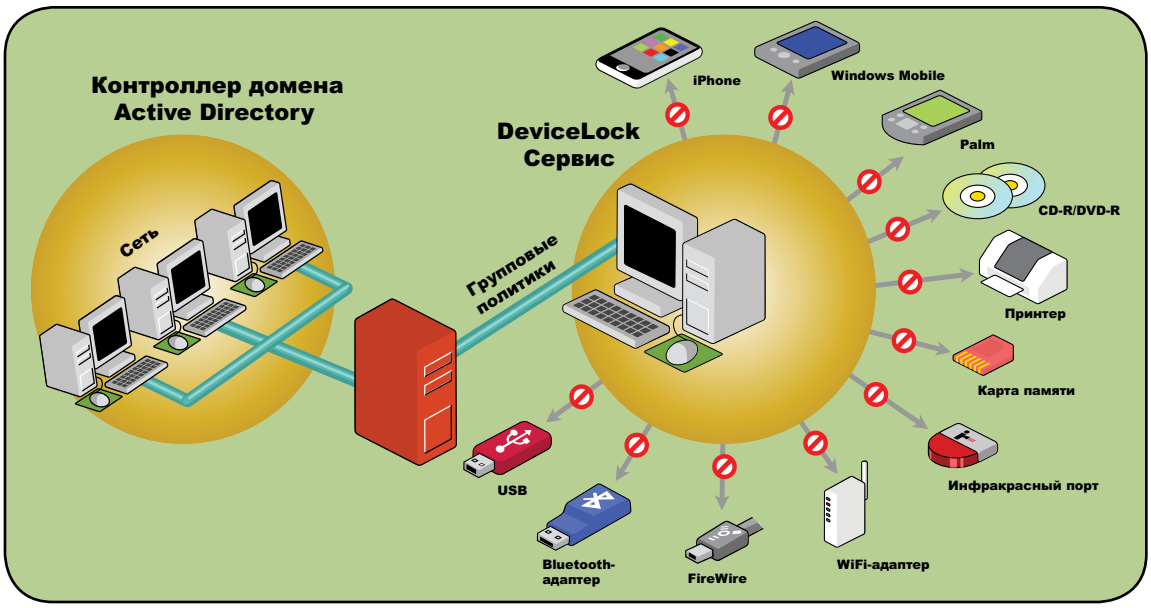
Как это работает

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.

Основные функции DeviceLock

Контроль доступа. Вы можете контролировать доступ пользователей и групп к устройствам (дисководы, CD/DVD-приводы, сменные накопители, КПК и смартфоны, жесткие диски, локальные и сетевые принтеры, WiFi, Bluetooth и т.п.) и портам ввода-вывода (USB, FireWire, COM, LPT, IrDA) в зависимости от времени и дня недели. Для сменных носителей, дисководов, жестких дисков, CD/DVD-приводов, КПК и ленточных накопителей можно устанавливать тип доступа «*только чтение*».

«Контентно-зависимые» правила. Для каждого пользователя или группы можно разрешать и запрещать доступ к определенным типам файлов вне зависимости от установленных на устройство разрешений. Вы также можете использовать контентно-зависимые правила для включения и отключения теневого копирования для заданных типов файлов. Определение типов файлов основано на сигнатурном методе и не зависит от расширения файла. Поддерживается более 3800 различных типов файлов.

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 сохраняются точные копии данных, копируемых на внешние устройства, передаваемых через последовательные и параллельные порты, а также печатаемых на локальных и сетевых принтерах. Точные копии всех файлов и данных сохраняются в SQL-базе данных на сервере.

«Оффлайн» политики. DeviceLock может применять один набор политик для ситуации когда компьютер подключен к сети, доступен контроллер домена или доступен DeviceLock Enterprise Server, и другой набор политик для ситуации, когда компьютер не подключен к сети, не доступен контроллер домена или не доступен DeviceLock Enterprise Server.

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.

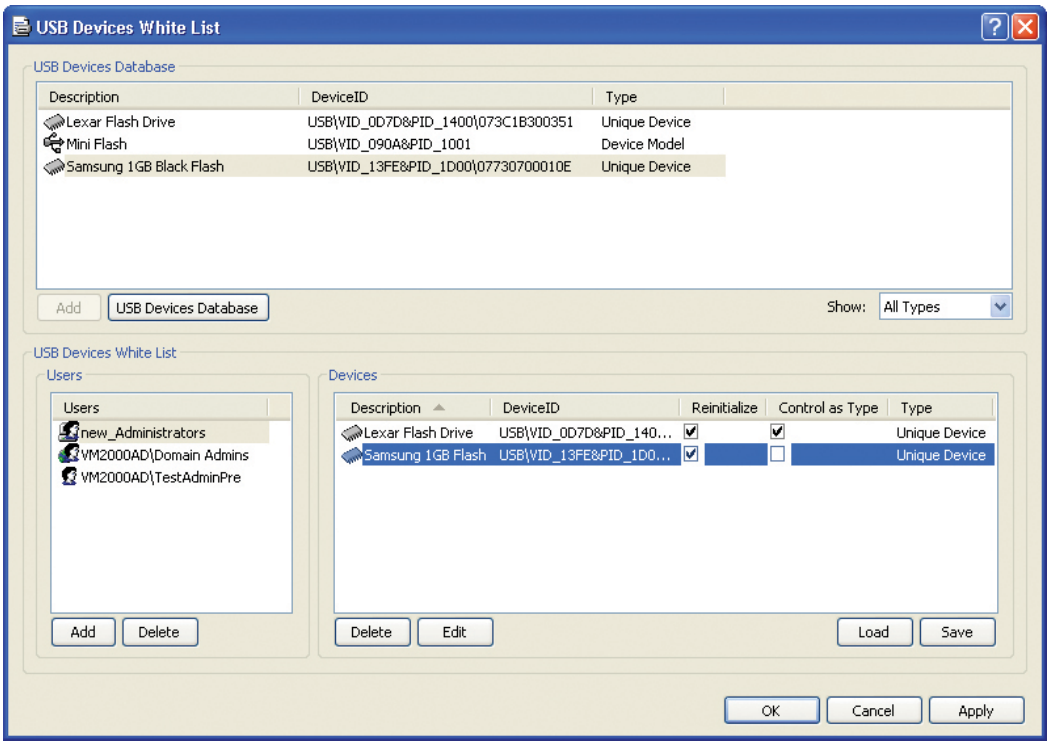
Централизованное управление. DeviceLock имеет систему удаленного управления, позволяющую обеспечивать доступ ко всем возможным функциям программы с рабочего места администратора системы. DeviceLock Management Console представляет из себя оснастку (*snap-in*) для *Microsoft Management Console*, со стандартным 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.

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

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.

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. Вы можете формировать графические отчеты на основе данных из журналов аудита и теневого копирования, хранимых на DeviceLock Enterprise Server'e. Эти отчеты могут быть автоматически высланы по электронной почте на указанный адрес. Также DeviceLock позволяет формировать отчеты по установленным настройкам и по устройствам (USB, FireWire и PCMCIA), которые используют пользователи на своих локальных компьютерах.



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.

Расширенные функции DeviceLock

Интеграция с внешними средствами шифрования. DeviceLock обнаруживает диски, зашифрованные при помощи продуктов ViPNet SafeDisk (продукт российской компании Инфотекс, сертифицирован ФСБ России как СКЗИ), PGP Whole Disk Encryption и TrueCrypt, а также распознает флеш-диски Lexar SAFE PSD, поддерживающие аппаратное шифрование данных, и применяет специальные «политики шифрования» к ним. Используя такие политики, вы можете, например, разрешить запись только зашифрованных данных на съемные устройства и запретить запись незашифрованных данных.

Контроль, аудит и теневое копирование для КПК. DeviceLock позволяет контролировать, осуществлять аудит и теневое копирование для КПК, работающих под управлением ОС Windows Mobile и Palm OS. Вы можете задавать разрешения для различных объектов (файлы, контакты, почта и т.д.), передаваемых с/на КПК. Также возможно включить аудит и теневое копирование для файлов и других объектов (контакты, почта и т.д.), копируемых с компьютера на КПК. Поддерживаются все интерфейсы (USB, COM, IrDA, Bluetooth, WiFi).

Обнаружение и блокирование аппаратных кейлогеров. DeviceLock обнаруживает USB-кейлогеры и блокирует клавиатуры, подсоединенные к ним. Также DeviceLock может предотвращать запись данных на PS/2-кейлогеры. DeviceLock искажает вводимые с PS/2-клавиатуры данные и вынуждает PS/2-кейлогеры записывать «мусор» вместо реально вводимых данных.

Централизованный мониторинг. DeviceLock Enterprise Server позволяет контролировать текущее состояние агентов на удаленных компьютерах путем периодического опроса, и сохраняет в журнал мониторинга текущее состояние, версию и сведения о настройках каждого агента. Кроме того, DeviceLock Enterprise Server периодически сравнивает текущие политики безопасности (настройки) агентов на указанных администратором компьютерах с эталонными политиками, сохраненными в XML-файл, и записывает информацию о выявленных отклонениях в журнал мониторинга. При этом возможна автоматическая замена текущих политик безопасности на эталонные.

Обновление настроек на отключенных от сети компьютерах. Вы можете создавать файлы с настройками агентов и передавать их пользователям, чьи компьютеры не подключены к сети и находятся вне досягаемости консолей управления DeviceLock. Для предотвращения неавторизованных изменений в настройках эти файлы могут быть подписаны при помощи электронной цифровой подписи.

Установка агентов с предопределенными настройками. Агенты могут быть установлены на удаленные компьютеры с уже определенными политиками безопасности (настройками) путем развертывания специально созданного установочного пакета Microsoft Installer (MSI). Такой MSI-пакет создается администратором при помощи стандартной консоли управления DeviceLock.

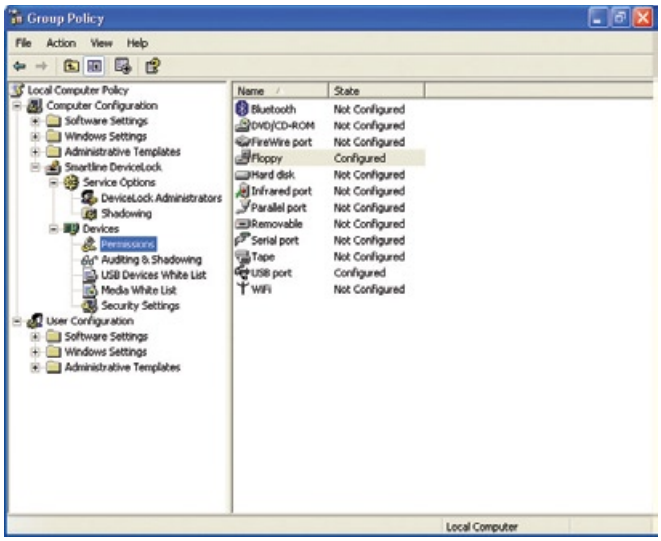
Компрессия данных при передаче по сети. Включив опцию потокового сжатия для данных аудита и теневого копирования, пересылаемых с удаленных агентов на DeviceLock Enterprise Server, вы можете уменьшить объем передаваемой по сети информации и тем самым снизить нагрузку на сеть.

Контроль пропускной способности сети. DeviceLock может определять баланс своего сетевого трафика, позволяя вам ограничивать пропускную способность сети для данных аудита и теневого копирования идущих от агентов на DeviceLock Enterprise Server.

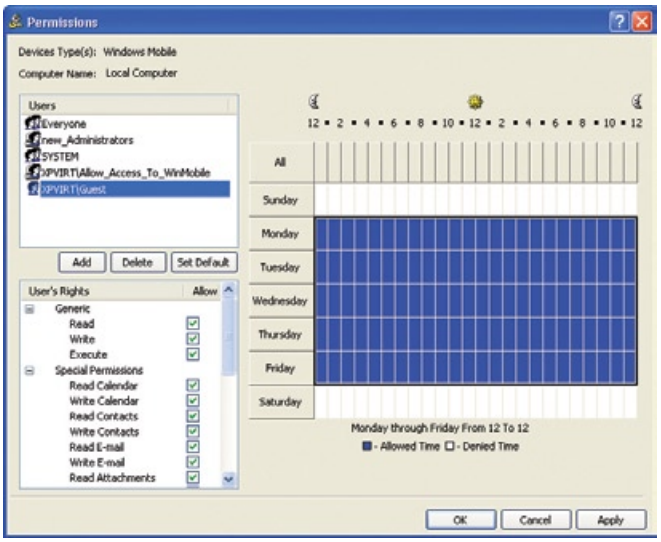
Автоматический выбор оптимального сервера. Для передачи данных аудита и теневого копирования, агенты могут выбирать из своих списков наиболее быстрые из доступных серверов.

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

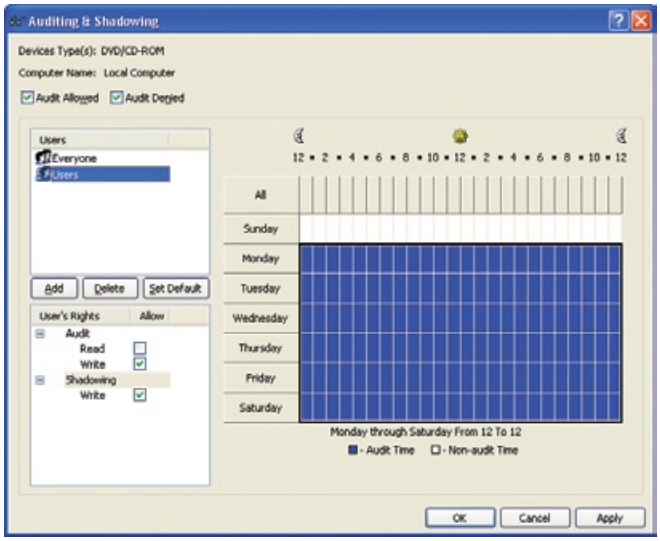
Каждый раз, когда пользователь пытается получить доступ к устройству, DeviceLock перехватывает запрос на уровне ядра ОС.



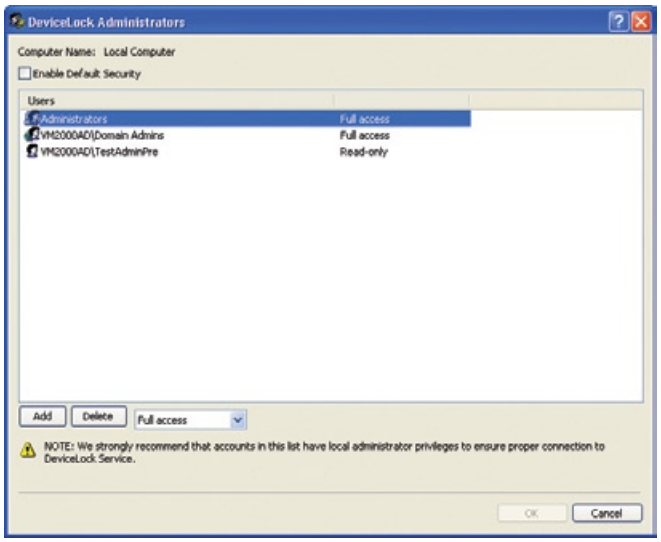
- **DeviceLock Group Policy Manager интегрируется в редактор политик Windows и позволяет управлять настройками DeviceLock через групповые политики.**



- **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]

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 55 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:

«*Решение использовать DeviceLock было принято как одна из мер по снижению рисков утечки информации и вирусного заражения при использовании внешних носителей информации сотрудниками Банка. Важным критерием, повлиявшим на окончательный выбор продукта, является его функциональность и надежность. Предполагаем, что использование DeviceLock позволит уменьшить риски информационной безопасности Банка при использовании периферийных устройств и внешних носителей информации*». (Шабунин В.В., начальник ОИБ УБиЗИ Среднерусского банка Сбербанка России).

«*Руководство Компании удовлетворено результатами внедрения DeviceLock на 700 рабочих станциях. По результатам анализа аналогичных продуктов мы пришли в выводу, что DeviceLock может быть успешно использован совместно со штатными средствами ОС Windows и ПО других производителей, а также характеризуется оптимальным соотношением цена/качество. К тому же программный продукт очень легок в установке*». (Холодов А., руководитель отдела сетевых технологий ОАО «КапиталЪ Страхование»).

«*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*». (Шипкова Г., главный специалист отдела информационных технологий ФГУП «Атомэнергопроект»).

«*Установить DeviceLock было легко. Администраторы и отдел ИБ Банка остались довольны результатами внедрения программы DeviceLock. С внедрением данного программного решения политика информационной безопасности Банка не была изменена, DeviceLock позволил взять на контроль выполнение правил, закрепленных в политике информационной безопасности, а также оптимизировать процесс управления*». (Брагин А.Ю., начальник отдела информационной безопасности ВТБ 24).

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

SmartLine
Proactive Network Security

ЗАО «Смарт Лайн Инк»

Москва, Б. Семеновская ул., д. 40, офис 301

Тел. (495) 967-99-60
(495) 366-21-93
Факс (495) 366-29-45

support@smartline.ru