

Pointsec Protector: защита периферии вычислительных устройств

13 ноября 2007

Игорь Левен

Директор учебного центра

iloewen@ntc.ru

+7 (495) 580 9902

О чем пойдет речь...



Один USB flash drive в нехороших руках и ваш межсетевой экран бесполезен!

80 % инцидентов с безопасностью связаны с инсайдерами

USB flash drives легко потерять вследствие малых размеров

Но еще более серьезен риск принести на нем в корпоративную сеть злонамеренный код

О чем пойдет речь...



ОДИН 80 GB iPod позволяет
скопировать **2.500.000** документов Word
за **15 minutes...**

Вот почему UK MOD запретило Apple iPod's

Это слишком серьезная угроза
безопасности...

О чем пойдет речь...



Факты.....

Plug & Play

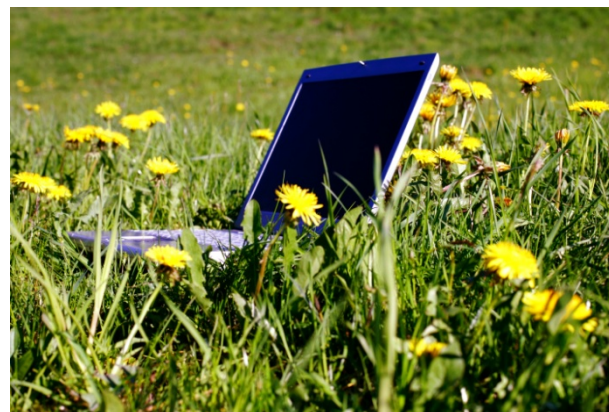


О чем пойдет речь...



Факты.....

Plug & Play
Wireless



О чем пойдет речь...



Факты.....

Plug & Play
Wireless
iPod



О чем пойдет речь...



Факты.....

По данным Samsung мировой рынок flash накопителей

€25 миллионов



О чем пойдет речь...



Факты.....



Динамика бизнеса, рост мобильности диктуют необходимость обмениваться большими объемами информации

О чем пойдет речь...



rip burn mix

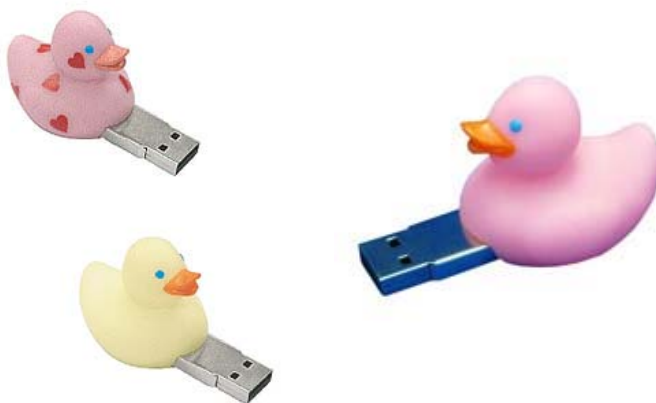


Сменные носители информации (USB flash, портативные жесткие диски и т.п.) становятся вездесущими. 85% сотрудников используют их для обмена данными между домом и офисом и потенциально переносят злонамеренное ПО.

О чем пойдет речь...



Конечно вы знаете о таких устройствах...



О чем пойдет речь...



Но знаете ли о таких ?



В чем проблема ?



Не требуется установка драйверов

Не требуется привилегий администратора

Нет групповых политик WiFi, Bluetooth, USB и FireWire!

Защита съемных носителей



Полная защита данных на внешних носителях



- Работает автоматически и прозрачно для пользователя
- Обеспечивает доступ к зашифрованному носителю и без предварительной установки ПО
- Возможна помощь для удаленного восстановления пароля

Зачем нужен Pointsec Device Protector?



- Чтобы защитить важные корпоративные данные от кражи и потери
- Чтобы внедрить в компании политику безопасности в части использования внешних носителей и устройств
- Чтобы понять, где понадобится такая политика в будущем
- Чтобы знать, что приходит и уходит из сети компании на неконтролируемых USB носителях
- Чтобы разрешить контролируемую работу мобильным сотрудникам



Pointsec Protector – Product Operation



Централизованное управление и аудит

*Отслеживание использования портов, подключения устройств,
планирование политики безопасности*

Контроль устройств и активности на портах

Wired

USB
Firewire
Serial
Printer
IDE

Wireless

Bluetooth
Infrared
WiFi

Devices

Memory cards
Digital cameras
Music players
Modems
Smart phones
Printers
Keyloggers



Возможности Pointsec Device Protector



1: Device Manager

Контролирует доступ как к известным, так и к неизвестным устройствам и портам, включая USB, Firewire и Bluetooth. Останавливает распространение как известных, так и новых злонамеренных программ (вирусов, червей, троянов, шпионского ПО).

2: Детальный аудит

Протоколирует все файловые операции на съемных носителях, все попытки сломать защиту и т. д. Предусматривает гибкие настройки фильтров, анализ данных аудита, хранящихся в базе MS SQL.

3: Управление съемными носителями

Проверка на вирусы, сканирование содержимого, контроль и авторизация устройств прежде, чем предоставить к ним доступ. Благодаря цифровой подписи можно отследить, когда носитель использовался вне организации.



4: Program Security Guard

Контроль за приложениями, предотвращение злонамеренного кода. Отслеживает и сообщает о файлах, которые могут использоваться, создаваться, удаляться, модифицироваться.

5: Encryption Policy Manager

Вынуждает данные быть зашифрованными прежде, чем будет скопировано на сменный носитель. Централизованное управление для пользователя, группы, подразделения. Offline доступ и доступ с доверенных сайтов. Присвоение носителя конкретному пользователю, группе, подразделению.

6: Deployment and Scalability

Поддерживается MS Windows NT/2000/2003/XP, прозрачная интеграция с NT Domain, Active Directory и Novell NDS. Online и Offline настройки позволяют раздельное управление постоянными и мобильными пользователями.

Управление устройствами

- Поддержка черных и белых списков
- Контроль внешних носителей на всех портах (USB, Firewire, IDE, etc.) как известных, так и неизвестных.
- Управление устройствами по типу, производителю, модели, индивидуальному устройству
- Предотвращает установку неизвестных устройств

Управление съемными носителями

- Цифровая подпись одобренных носителей
- Обнаружение изменений, созданных «извне». Принудительные проверки в этом случае
- Дополнительный уровень антивирусной защиты
- Настраиваемый контроль содержимого новых устройств

Прозрачное шифрование

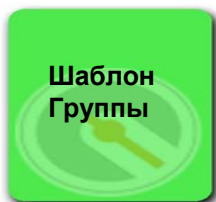
- Прозрачно защищает съемные носители, предотвращая хищение данных
- Обеспечивает безопасный доступ к зашифрованным устройствам без необходимости устанавливать ПО и не требует прав администратора
- Доступ к зашифрованным файлам для нескольких пользователей
- Отзыв зашифрованных устройств и восстановление ключей

Аудит

- Детальные отчеты о попытках проникновения
- Полный аудит использования устройств Complete (floppy, CD/DVD, USB flash media, diskOnKey, etc.)
- Фильтрация на клиенте
- Настраиваемые фильтры и отчеты для событий аудита
- Настраиваемые оповещения по электронной почте, отчеты в html

Шаблоны профилей

Шаблоны профилей задают политику безопасности для индивидуальных пользователей/групп/ПК








Контролируют типы файлов, представленных в сети, на жестких дисках и других подключенных устройствах;

Аудит передачи файлов на съемные носители и других событий безопасности

Будучи созданным, Профиль может обновляться и применяться к ПК в реальном времени

Черные и белые списки

Access to		Read/Write	Encrypt
Access to		Read/Write	
Access to		Read Only	
Access to		No	
Access to		Yes	

Централизованное управление



- **Pointsec Device Protector Enterprise Server обеспечивает удобное управление клиентами Pointsec Device Protector**
- **Политика задается из традиционной интерфейса Microsoft Management Console (MMC)**
- **Для доступа к серверу можно настроить несколько консолей (удаленное управление)**
- **Возможна иерархия доверительных отношений для разных уровней администрирования в разных подразделениях**
- **Шаблоны политики позволяют администратору распространять унифицированную политику внутри организации**
- **Эти шаблоны политик могут и должны отражать существующие политики безопасности**
- **Настраиваемые политики аудита; журналы могут экспортироваться для интеграции с внешними средствами анализа**

Детальное управление



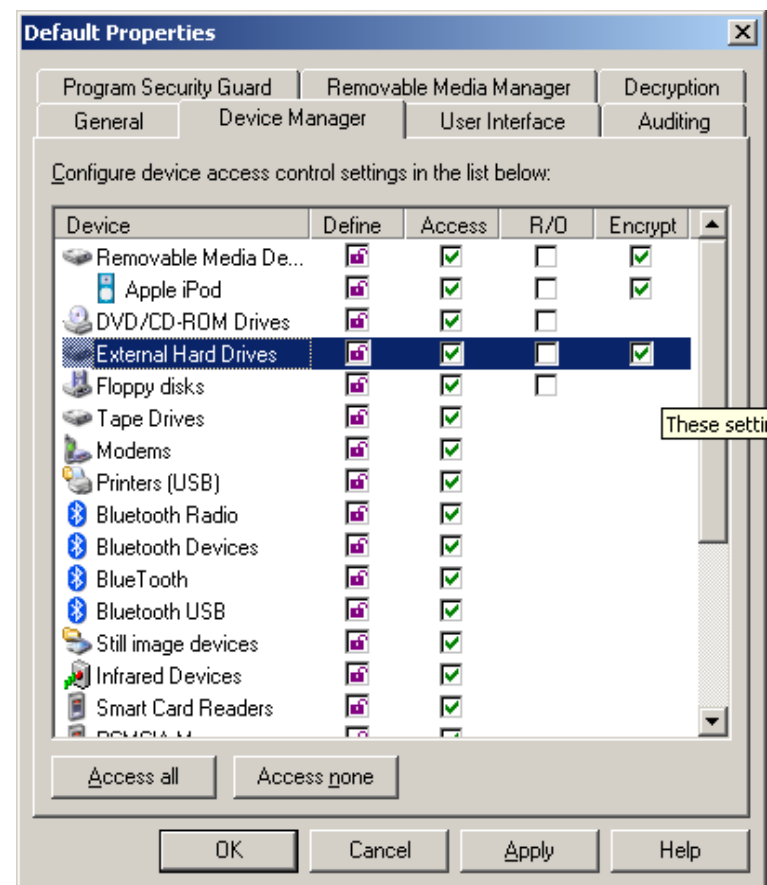
- Pointsec Device Protector предлагает гранулированное управление USB устройствами, модемами, подключениями к IrDA, Bluetooth, WiFi и т.д. глобально или конкретными устройствами
- Устройства могут разделяться по типу, полномочиям, предоставляемым в зависимости от имени/группы пользователя, рабочей станции
- Использование устройств может контролироваться как глобально, так и в зависимости от типа, производителя, конкретной модели
- Профиль предопределяет политики использования устройств и управление содержимым

Удобство использования

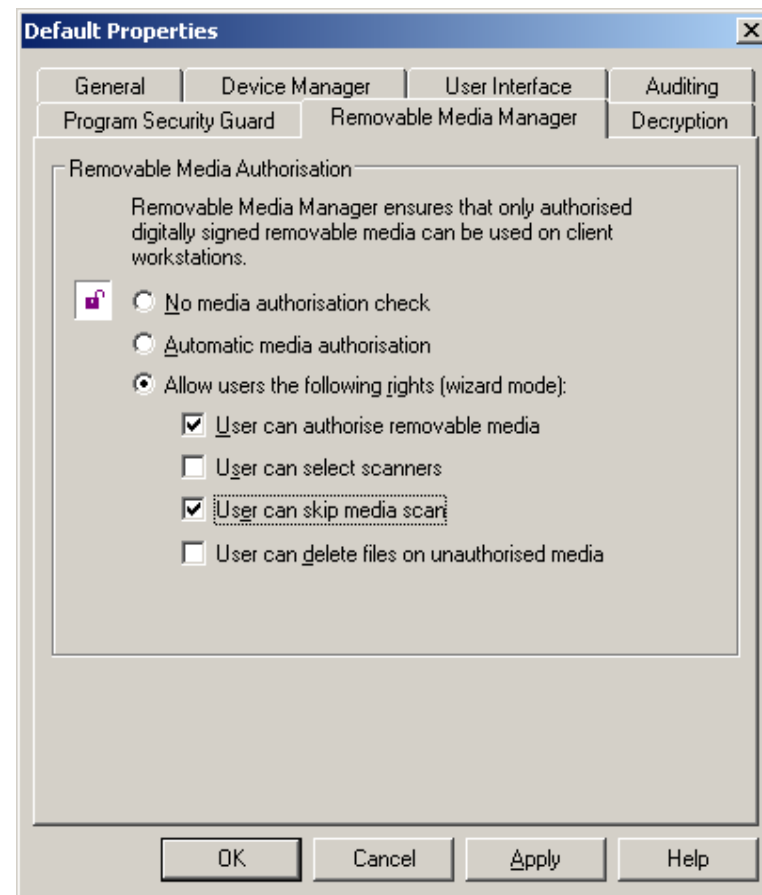


- Пользователи не участвуют в установке и узнают о наличии ПО только при попытке нарушить политику безопасности
- Сообщения для пользователей настраиваются и предоставляют исчерпывающую информацию о происходящем
- Политики могут распространяться на подписанных носителях
- Обычно политики включают принудительную проверку на вирусы и допустимость содержимого
- Цифровой идентификатор позволяет использование только разрешенных (подписанных) носителей и блокировать чужие даже если они того же производителя и модели
- При использовании в защищенном окружении зашифрованные носители выглядят как любое другое устройство, поскольку аутентификация и дешифрование осуществляются прозрачно
- Может быть (по решению администратора) предоставлен доступ к зашифрованным носителям Offline (вне компании)
- Offline access безопасен и не требует установки ПО на чужие компьютеры

- Доступ ко всем устройствам может задаваться гранулировано (full, read only or no access)
- Специфические настройки устройств могут применяться исходя из модели/производителя устройства
- Поддержка черных и белых списков
- Еще больший контроль достигается комбинацией с шифрованием



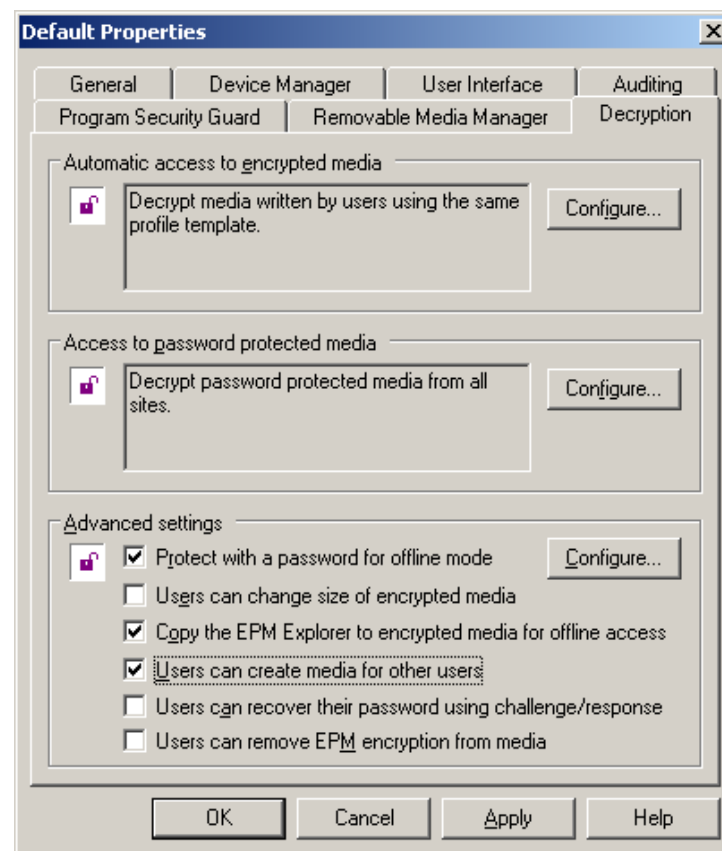
- Эта закладка используется для разрешения подключения только авторизованных устройств
- Разрешит доступ только к подписанным носителям
- Интеграция с антивирусными сканерами



Шифрование съемных носителей



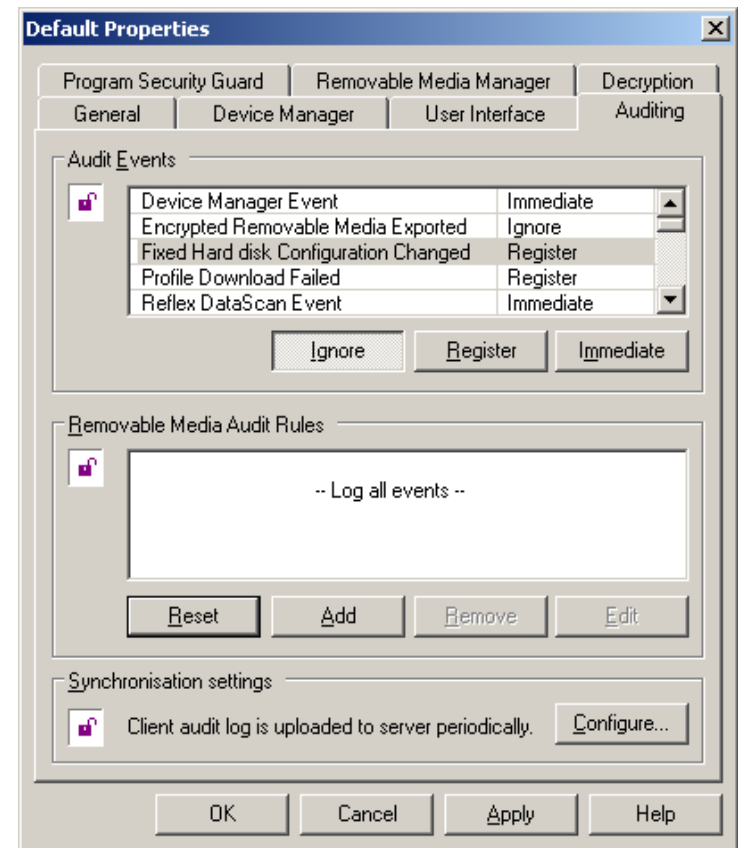
- Можно принудительно установить доступ к съемным носителям только при условии их шифрования
- Пользователям можно предоставить право доступа к таким носителям offline для защищенной передачи данных
- Offline доступ не требует инсталляции, прав администратора...



Детальный аудит



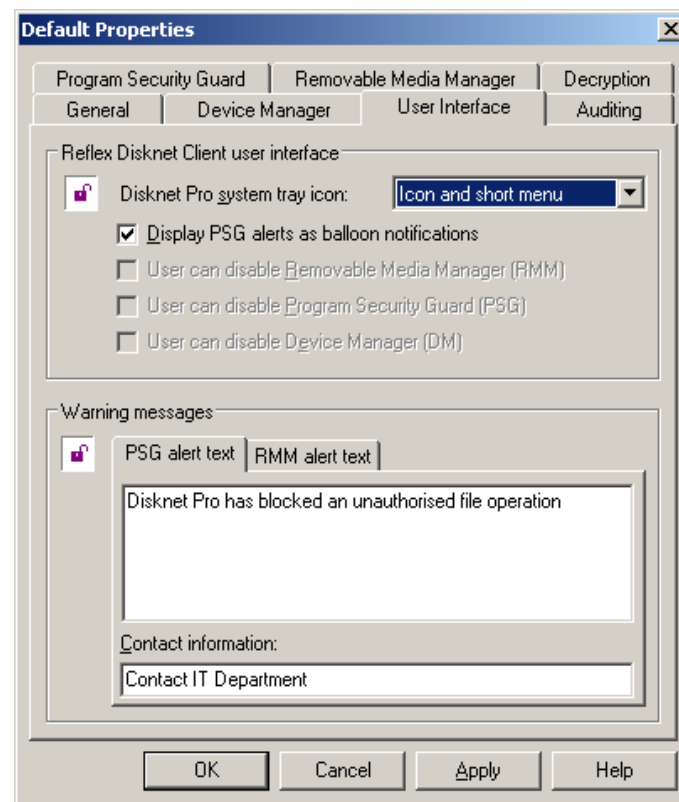
- Настраивается реакция/протоколирование на события
- Аудит попыток нарушения политики
- Аудит файловых операций на съемных носителях
- Разные методы оповещения сервера (настраиваемая синхронизация)



Пользовательские сообщения

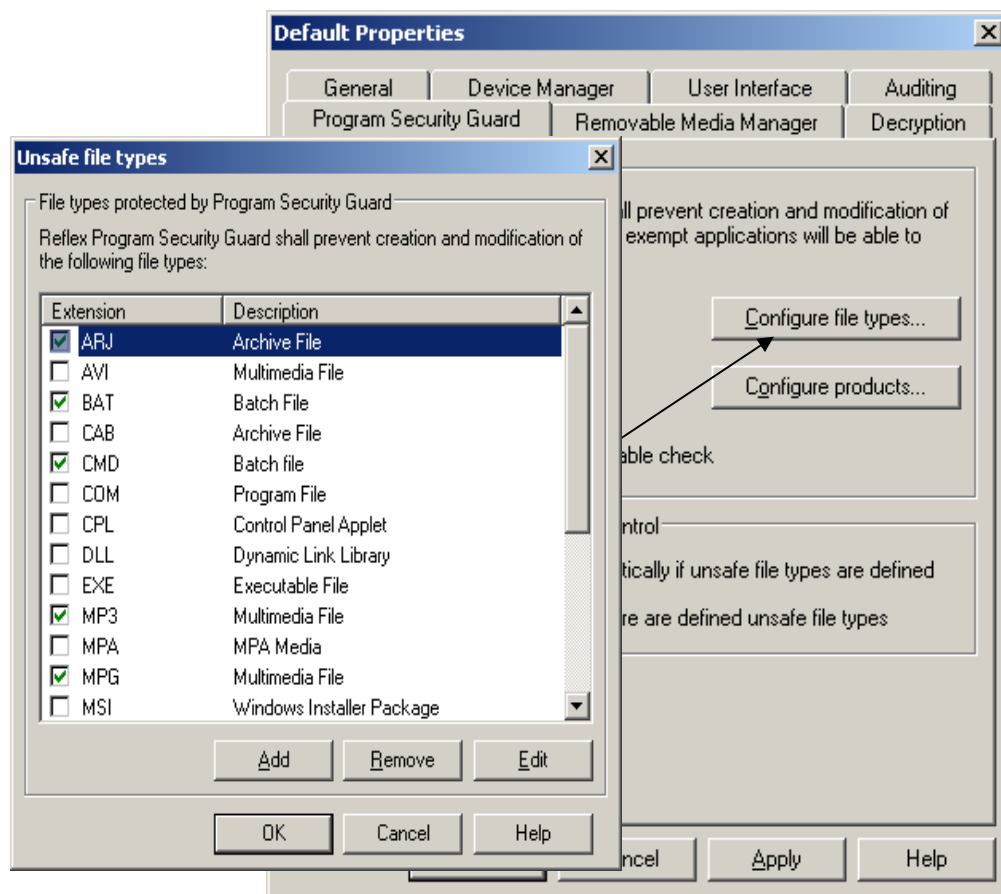


- Можно создавать собственные сообщения для пользователей при нарушении политики использования устройств
- 4 опции:
 - 1) Без иконки
 - 2) Только иконка
 - 3) Иконка и краткое меню
 - 4) Иконка и полное меню



Program Security Guard - PSG

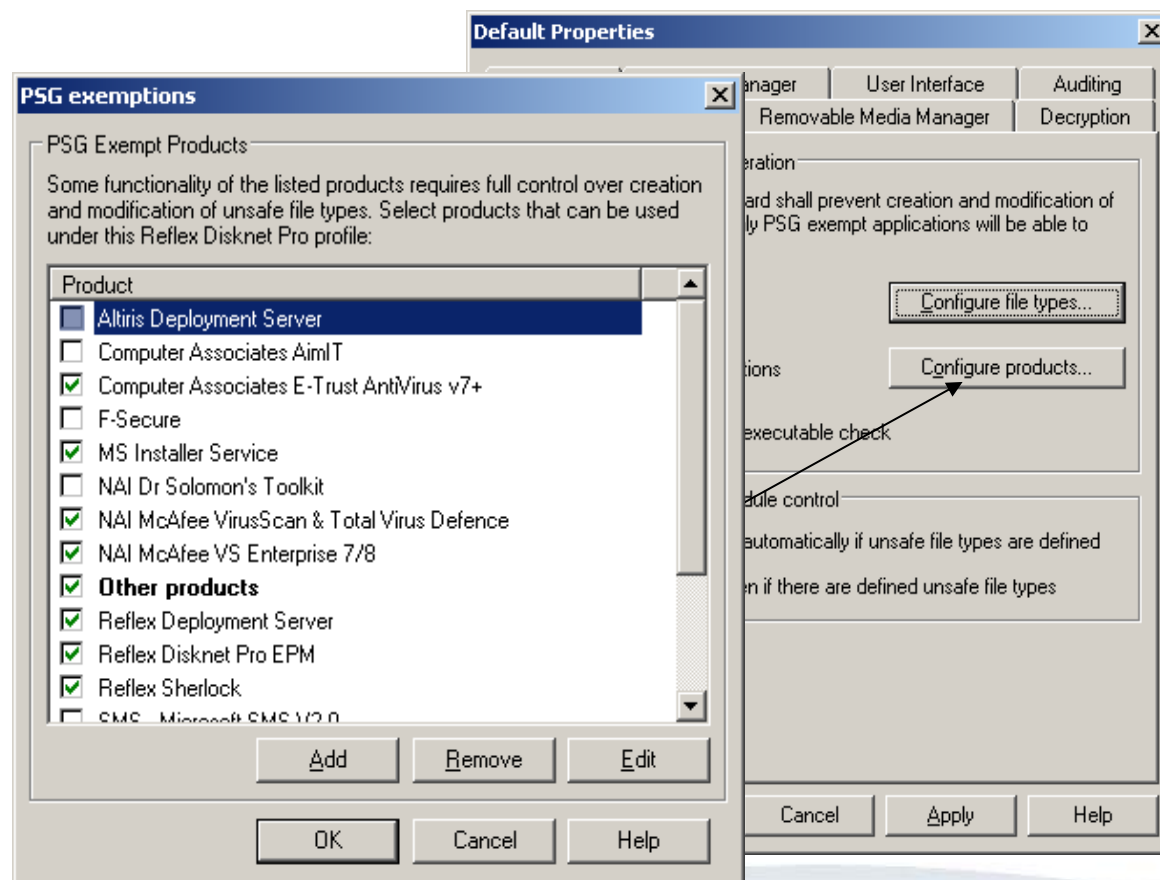
- **PSG предотвращает внедрение злонамеренного кода и неавторизованных файлов (MP3, MPG, AVI...);**
- **Дополнительный уровень помимо традиционной защиты от вирусов/червей**
- **PSG может блокировать удаление или изменение определенных типов файлов**



Program Security Guard



**PSG однако
позволяет
доверенным
приложениям,
определенным
администратором,
устанавливать,
модифицировать
новые пакеты**

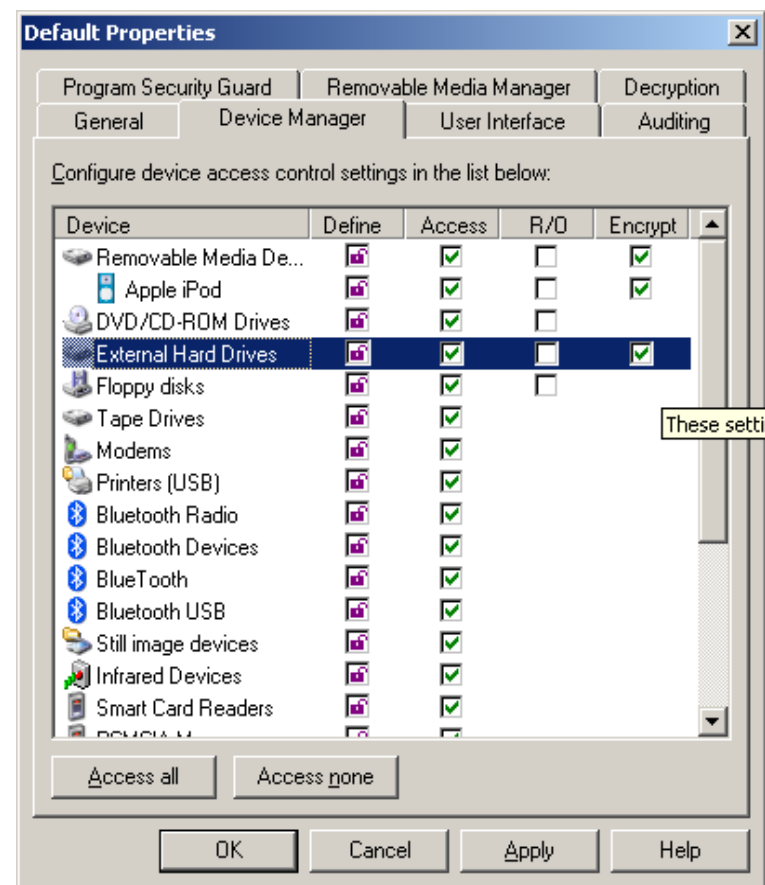


Device Management

Управление устройствами



- Доступ ко всем устройствам ввода/вывода управляются предоставлением прав полных, только на чтение...
- Специфические настройки могут задаваться на основе модели/производителя
- Поддержка черных и белых списков
- Дополнительные настройки для съемных носителей через Removable Media Manager & Encryption Policy Manager.



Client Base



Military



Government



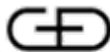
Law Enforcement





Client Base (continued...)

Corporate



Giesecke & Devrient
security at work.



ALLEN & OVERY



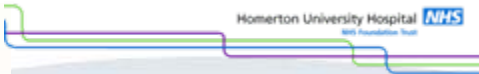
Technology



Financial



Health & Education



Резюме



Принудительная безопасность

Автоматическое, полное
шифрование диска

Простой сброс паролей

Удаленный challenge / response

Check Point Data Security

Полный набор решений

Ноутбуки, ПК, Linux, управление
портами, съемными носителями,
Symbian, Smartphone,
Pocket PC & Palm

Снижена стоимость уничтожения устройств

Не требуется дорогостоящее
уничтожение информации

Легкое и удобное администрирование

Нет излишней нагрузки

Устранены проблемы при потере устройства

Только стоимость замены устройства

Спасибо!