
# McAfee Encryption
# Инструменты криптографической защиты

Владислав Радецкий
vr@bakotech.com

TM

# Пару слов о себе

Vladislav Radetskiy
Lead Technical Support Engineer
BAKOTECH GROUP
+380 95 880-7370
vr@bakotech.com

С 2011 года работаю в Группе компаний БАКОТЕК.

Занимаюсь технической поддержкой проектов по ИБ.

Отвечаю за такие направления McAfee:

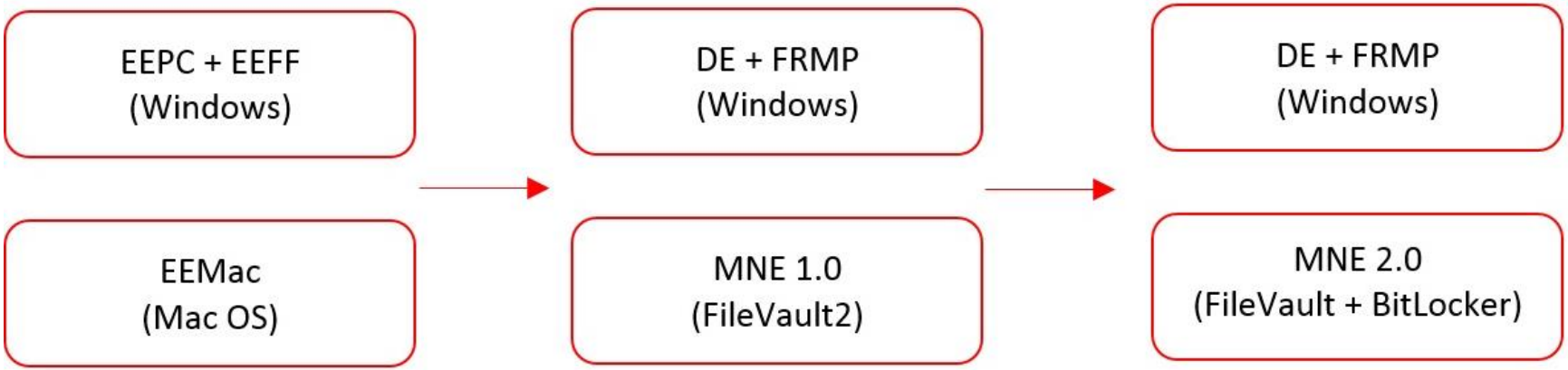
- Data Protection
- Email Security
- Endpoint Security
- Mobile Security
- One Time Password
- Security-as-a-Service
- Security Management

# О чем мы будем говорить

- Инструменты шифрования McAfee
- Основы работы с консолью McAfee ePO
- Детальный обзор решений
- Рассмотрение реальных проектов
- Q&A

# McAfee Encryption

## Процесс эволюции инструментов шифрования




**DE** = Drive Encryption, бывший Endpoint Encryption for PC (EEPC)

**FRMP** = File and Removable Media Protection, бывший Endpoint Encryption for Files & Folders (EEFF)

**MNE** = Management of Native Encryption (Apple FileVault + MS BitLocker)

**EEMac** = Endpoint Encryption for Mac (использовался до выхода Mavericks 10.9)

# Актуальные версии ПО

По состоянию на 1 марта 2015

**Управление**

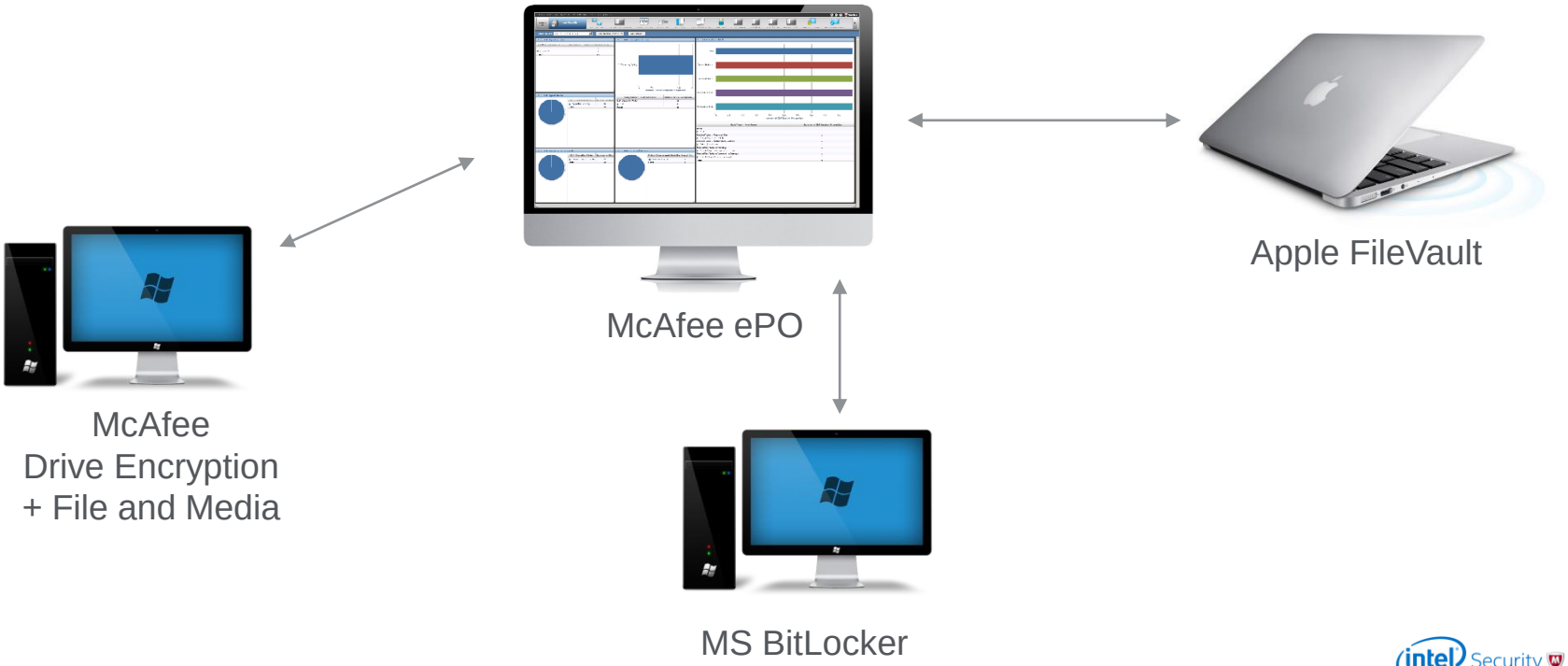
- ePO 4.6.8 &  ePO 5.1.1
- McAfee Agent 4.8 p3 & 5.0

**Шифрование**

- Drive Encryption **7.1.2**
- Management of Native Encryption **2.1.0**
- File and Removable Media Protection **4.3.1**

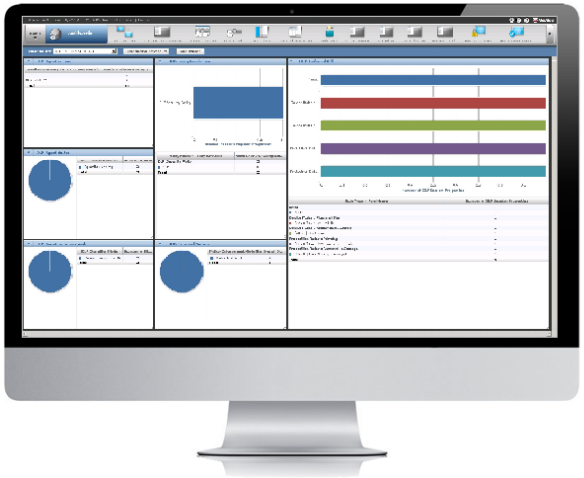
# ePO – единая консоль управления

## Контроль четырех систем шифрования из одной панели



# ePO – основы: агент

## Три основных порта, необходимых для коммуникации Агент-Сервер



443 TCP

80 TCP

8081 TCP

Encryption

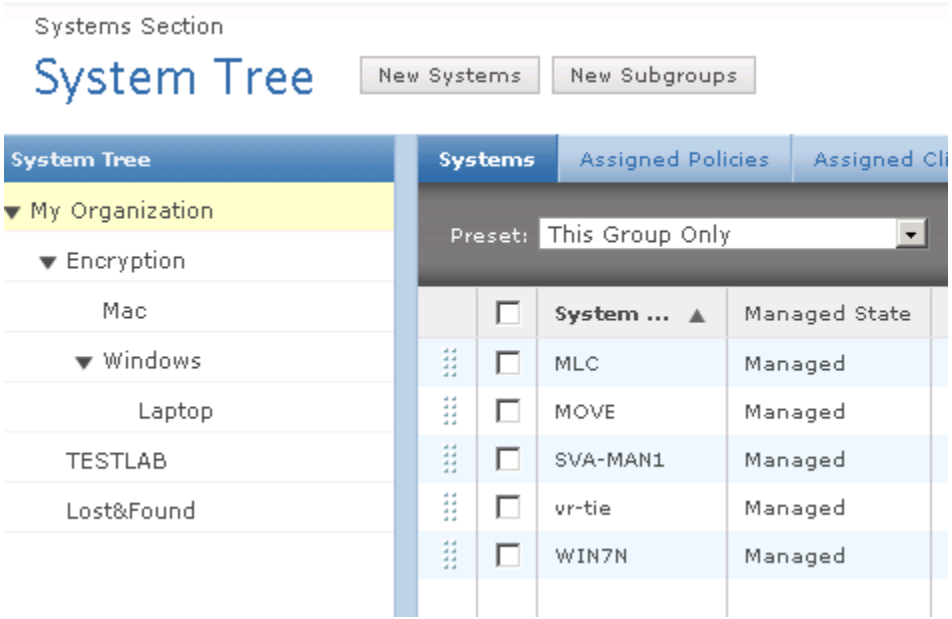
McAfee Agent

McAfee ePO

Endpoint

# ePO – основы: дерево систем

## Перечень систем




Формируется

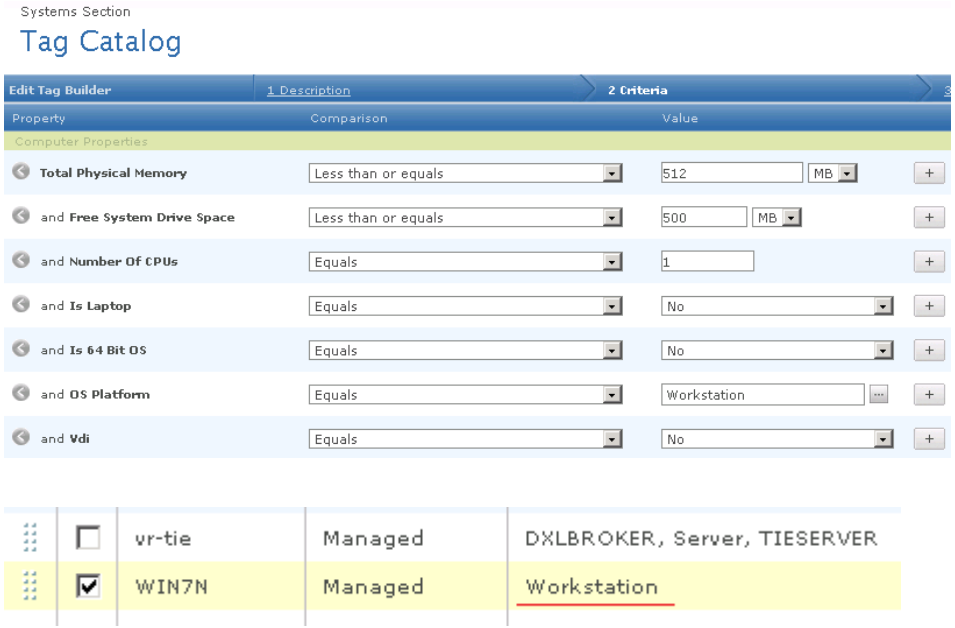
- Вручную
- Синхронизация с MS AD

Возможна сортировка систем по

- Тегам (меткам)
- IP адресам/подсетям

# ePO – основы: метки (теги)

## Разделяем системы между группами




Могут назначаться

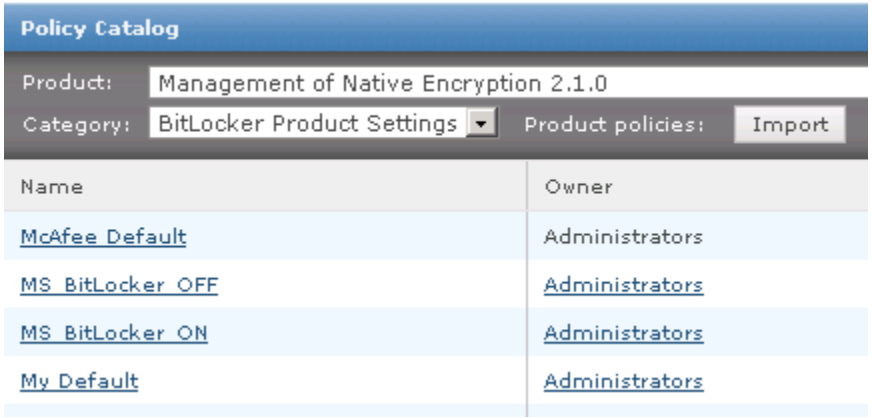
- По критериям
- Вручную (без критериев)

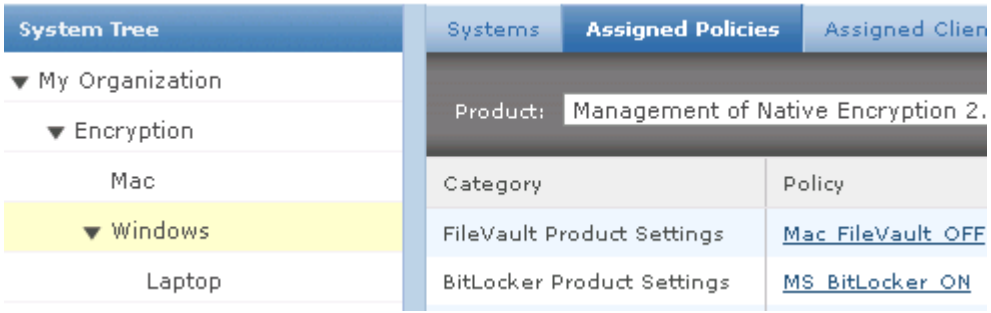
Используются для

- Сортировки систем
- Выборочного запуска задач
- Выбор. применения политик

# ePO – основы: политики

## Каждый модуль имеет свой набор политик




Политика **My Default** применяется сразу!

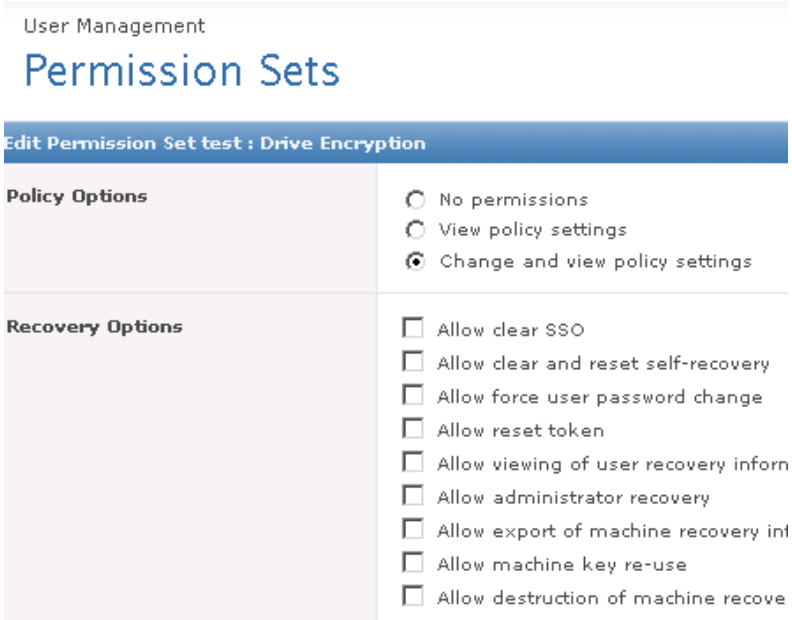
Принцип управления:

Создаем наборы политик и переключаем

- наследование
- по системам
- по группам

# ePO – основы: ролевая модель доступа

## Делегируем наборы разрешений




Операции могут быть распределены между:

- Администраторами (политики);
- Help-Desk`ом (сброс паролей);
- Инженерами (восстановление доступа);
- Аудиторами/руководством (отчетность)…

# Drive Encryption

## Короткая характеристика решения

- Система FDE с поддержкой HDD, Opal, SED и SSD дисков
- Широкий перечень поддерживаемых редакций Windows (XP – 8.1)
- Поддержка технологий: AES-NI, SSO, TPM, AMT, UEFI, GPT, Secure/Hybrid Boot…
- Возможность добавить  в pre-boot как доменных, так и недоменных пользователей
- Поддержка различных токенов (KB79787) и кард-ридеров (KB79788)
- Возможность сброса забытого пароля **6 разными** способами
- Симметричное шифрование секторов жесткого диска алгоритмом **AES-256-CBC**
- Для генерации случайных чисел DRBG использует **HMAC SHA256**
- Для аутентификации используется асимметричное шифрование **RSA 2048 bit**

# Drive Encryption

## Правильная последовательность внедрения

- **Выполнить резервное копирование важной информации с целевых систем**
- Настроить задачу синхронизации учетных записей из MS AD
- Определить политики по отношению к дереву систем, назначить пользователей
- Установить DEGO для проверки конфликтного ПО и SMART
- Установить модули шифрования при **неактивной политике** (Encryption_OFF)
- Активировать шифрование (Encryption_ON) с включенным Pre-Boot Smart Check
- По завершению процесса перезагрузить систему и пройти pre-boot

* Подробнее см. заметку в блоге

# Drive Encryption

## Методы сброса пароля/восстановления доступа к зашифрованной системе

- Self-recovery - **автономно**
- Admin recovery (challenge-response) - email, phone
- EETech boot USB/CD - локально
- DeepCommand on intel AMT systems - через Internet (IPsec)
- Endpoint Assistant (Android & iOS devices) - **автономно** / 7.1
- Self Service Portal (DPSSP) - через Internet / 7.2

**Итого**: 6 различных сценариев восстановления доступа

# Drive Encryption

## Полезные вещи, которые не включены по умолчанию

- SSO при использовании учетных записей из AD
- Использование TPM модуля для выгрузки ключа шифрования
- Add local domain users (EE:ALDU)
- Отключение pre-boot при отсутствии синхронизации
- Logon Hours на десктопах / серверах
- Процессы и каталоги DE должны быть в исключениях антивирусного ПО

# Management of Native Encryption

## Короткая характеристика решения

- Контроль Apple FileVault и MS BitLocker средствами ePO
- Два режима работы (report only & control)
- При использовании MNE нет необходимости в MBAM сервере
- Self Service Portal (DPSSP)
- Поддержка DEGO для Mac
- Периодическое пересоздание ключей восстановления
- Поддержка устройств Windows To Go, Microsoft Surface Tablets

# Management of Native Encryption

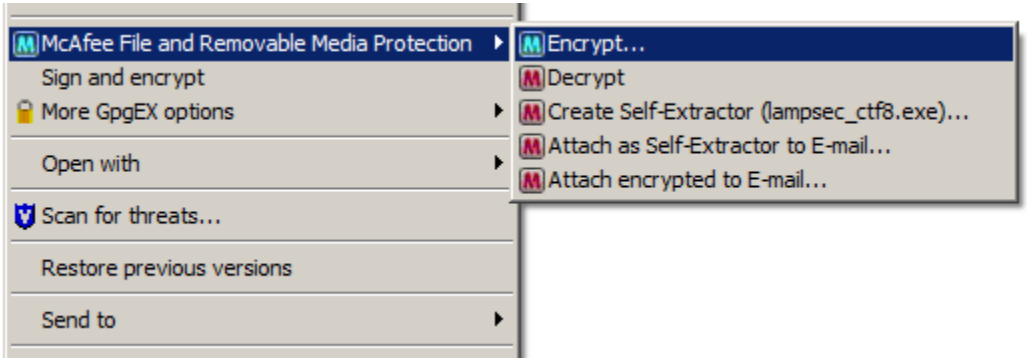
## Перечень поддерживаемых ОС

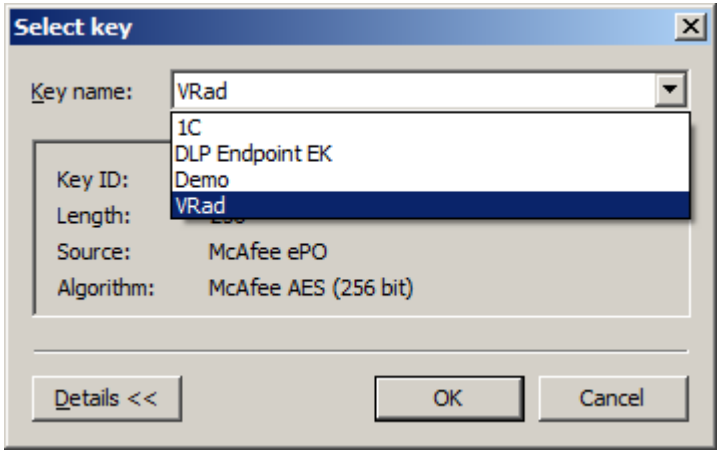
| Microsoft Versions | Apple OS X Versions |
| --- | --- |
| Windows Server 2012 R2 | OS X 10.8 (Mountain Lion) |
| Windows 7.0 (32-bit/64-bit) Enterprise and Ultimate | OS X 10.9 (Mavericks) |
| Windows 8.0 (32-bit/64-bit) | OS X 10.10.1 (Yosemite) |
| Windows 8.1 Update 2 (32-bit/64-bit)<br>Windows 8.1 Update 1 (32-bit/64-bit)<br>Windows 8.1 (32-bit/64-bit)<br>Windows 8 Enterprise and Professional | |
| Windows to Go | |

# File and Removable Media Protection

## Короткая характеристика решения

- Симметричное шифрование локальных/**сетевых** файлов/каталогов (AES 256)
- Шифрование внешних USB накопителей, CD/DVD, вложений электронной почты
- Гибкое делегирование ключей (User based / System based)

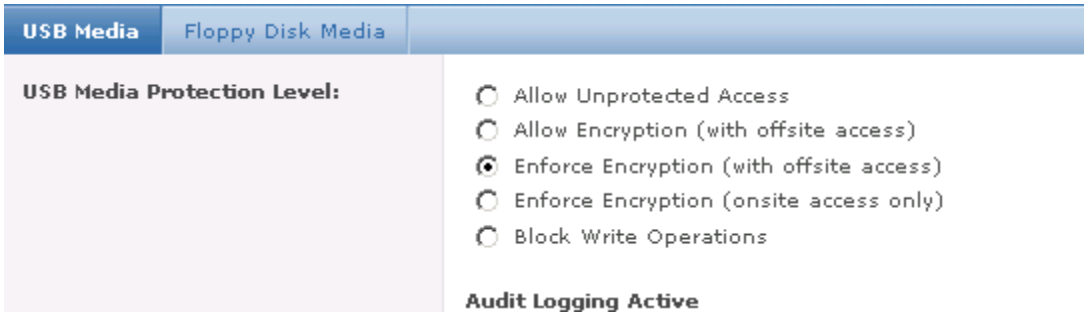


# File and Removable Media Protection

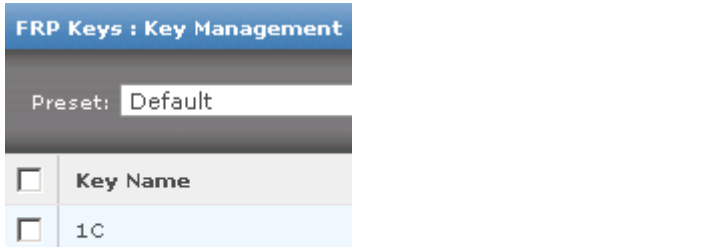
## Работа с CD/DVD и USB накопителями

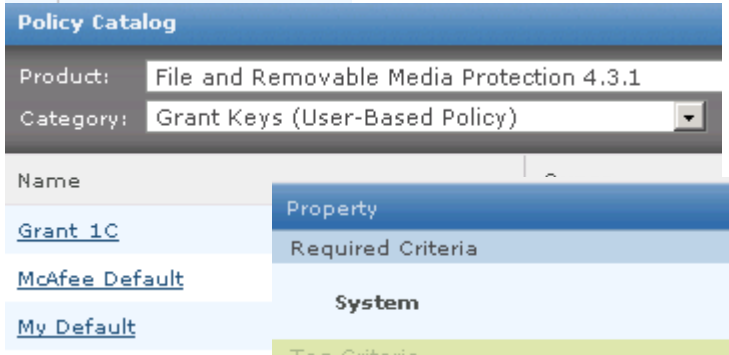
- Без шифрования/вручную/принудительно либо Read Only
- (USB) возможность привязки накопителя к конкретной системе
- (USB) возможность доступа на внешней системе (Windows & Mac)
- Доступ к зашифрованному без необходимости доп. ПО



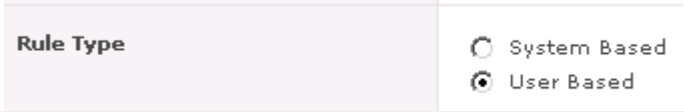

# File and Removable Media Protection

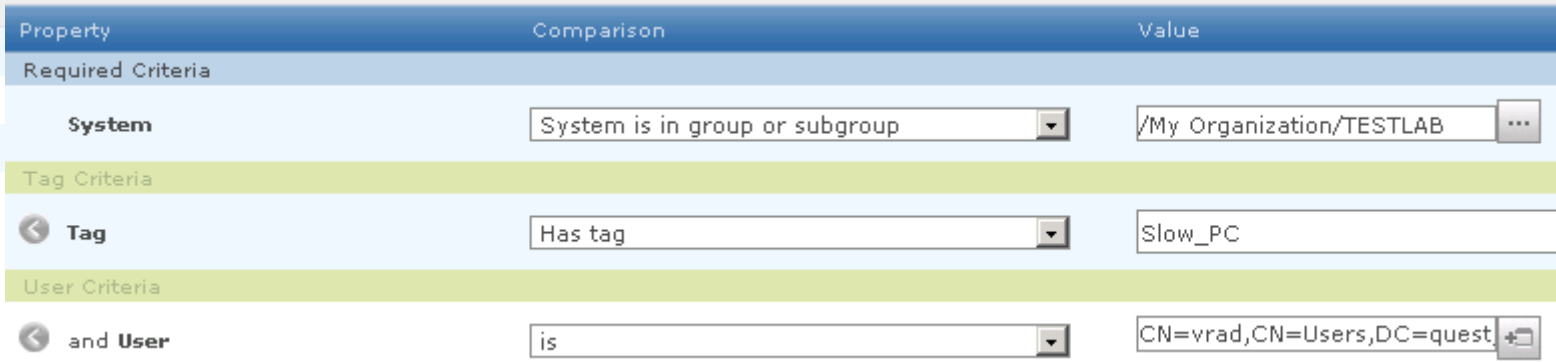
## Принцип назначения ключей




- Создаем необходимые ключи
- Создаем политику назначения ключа
- Выбираем к какому пользователю и на какой системе должна применяться политика, т.е.



# File and Removable Media Protection

## Особенности использования или о чем следует помнить

- Развертывается **только на клиентские** ОС Windows, тем не менее может шифровать документы на сетевых хранилищах
- Может интегрироваться с McAfee Device Control / DLP Endpoint
- Рекомендуется использовать для усиления с Drive Encryption
- При шифровании CD/DVD методом Onsite Access Only нужно использовать Windows Burner, Nero либо Roxio
- Отдельные накопители можно исключить из действия политики (KB75531)
- Процессы и каталоги ОС и ПО **не шифровать**

# Основные источники достоверной информации

- ✓ www.mcafee.com/expertcenter - каталог технических материалов
- ✓ https://kc.mcafee.com - база знаний
- ✓ https://radetskiy.wordpress.com - мой блог
- ✓ https://community.mcafee.com/community/business/data - анонсы, обсуждения
- ✓ https://www.youtube.com/user/McAfee - канал McAfee на YouTube

# Реальные внедрения шифрования

## Ключевые моменты для DE, F&RMP и MNE

- Ликбез или пилот для заказчика
- Разработка политик шифрования (на бумаге), планирование операций (по этапам)
- Формирование групп систем по общим признакам (сортировка + теги)
- Назначение пользователей/ключей/соотв. политик (выбор токенов / ридеров)
- Обучение/информирование персонала заказчика **(до запуска шифрования!)**
- Резервное копирование важных данных с целевых систем
- Развертывание и активация шифрования по отделам/департаментам
- Контроль работы (запросы/отчеты), автоматизация (задачи, метки, автоответы)
- Периодическая проверка восстановления доступа к зашифрованному

# Реальные внедрения шифрования

## Важные моменты

- Сайзинг сервера ePO, SQL Standard
- Организация коммуникации MA <-> ePO, смена портов
- Исключения антивируса
- Построение зеркал, обеспечение покрытия всех систем
- Отличия пилота от внедрения или процесс миграции/переноса
- Наличие загрузочного носителя EETech и инструкции для заказчика
- Наличие резервных копий (если что-то пойдет не так)

# Реальные внедрения шифрования

## Полезные советы

- (MA) C:\Program Files (x86)\McAfee\Common Framework**cmdAgent.exe /s**
- (DE) Используйте Autobooting для регламентных работ (обновление ОС, ПО)
- (DE) Всегда добавляйте в pre-boot сервисную учетную запись
- (DE) Pre-Boot Smart Check требует ~10 перезагрузок перед началом шифрования
- (DE) Automatic Repair Windows 8 off [ **bcdedit /set {current} recoveryenabled No** ]
- (MNE) Помните про исключения из парольной политики и DEGO для Mac
- (F&RMP) Ключи лучше деактивировать а не удалять, избегайте Local Keys
- (F&RMP) Если ключи не приходят по RDP – выполните logon локально
- (F&RMP) Шифрует файлы на уровне I/O, не сокетов(!) помнить о **blocking process**
- (F&RMP) При шифровании накопителя возможно два сценария

# Вопросы? Замечания? Пожелания?


radetskiy.wordpress.com
vr@bakotech.com
linkedin.com/pub/vladislav-radetskiy/47/405/809