Разрешаем установку драйверов обычным пользователям Windows

http://winitpro.ru/index.php/2014/05/19/razreshaem-ustanovku-drajverov-obychnym-polzovatelyam-windows/

По-умолчанию рядовые пользователи системы/домена не имеют прав для установки драйверов устройств на своих компьютерах. Это подход рационален с точки зрения обеспечения безопасности и стабильности работы ПК, но неудобен с точки зрения администрирования, ведь для установки любого нового драйвера в системе пользователю необходимо прибегать к помощи администратора или службы технической поддержки, которые обладают правами администратора на ПК пользователя.

В этой статье мы покажем, как разрешить обычным пользователям домена устанавливать драйвера в системе без прав администратора. Основное преимущество предлагаемого подхода – администратор домена сам формирует список доверенных драйверов, которые пользователи могут устанавливать в системе, тем самым риск установки «вредного» драйвера минимизирован.

Чтобы разрешить рядовым пользователям домена самим устанавливать драйвера устройств (без появления окна повышения привилегий UAC), нужно чтобы рабочая среда пользователей соответствовала следующим условиям:

- Устанавливаемый драйвер должен находиться в хранилище драйверов (Driver Store)
- Устанавливаемый класс драйвера должен быть разрешен для установки обычными пользователями
- Драйвер должен быть подписан валидной цифровой подписью доверенного издателя

Примечание. Ранее как частный случай этой методики мы рассматривали особенности установки принтеров в домене без прав администратора.

А теперь по порядку:

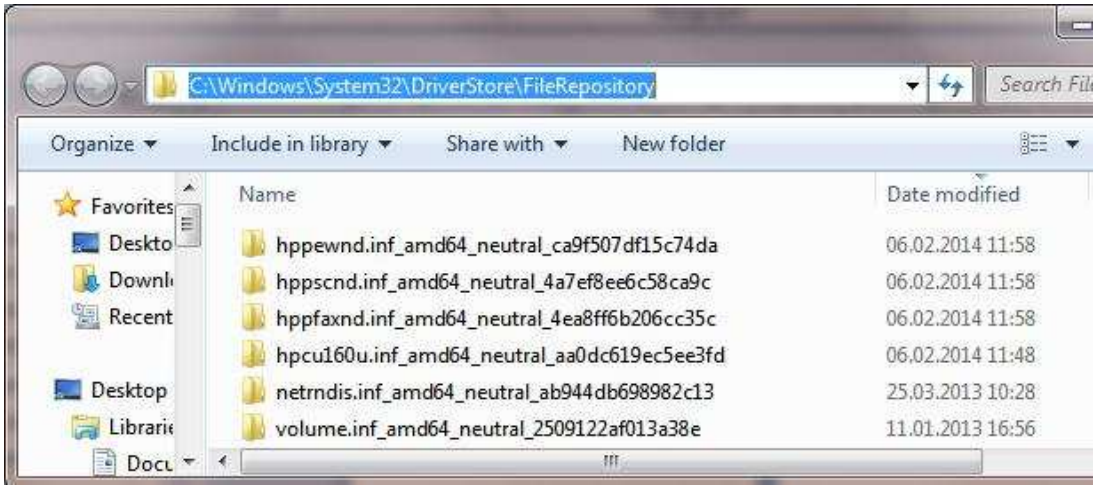
Contents

Получение каталога с драйвером устройства

Чтобы получить актуальную версию драйвера для конкретного устройства – лучше всего найти и скачать последнюю версию драйвера на сайте производителя. Скачанный архив с драйвером нужно распаковать в отдельный каталог.

НО! Не все драйвера предоставляются в формате, удобном для распространения. Допустим, некий драйвер устанавливается проприетарным инсталляционным пакетом. Каким же образом извлечь из системы каталог с файлами установленного драйвера?

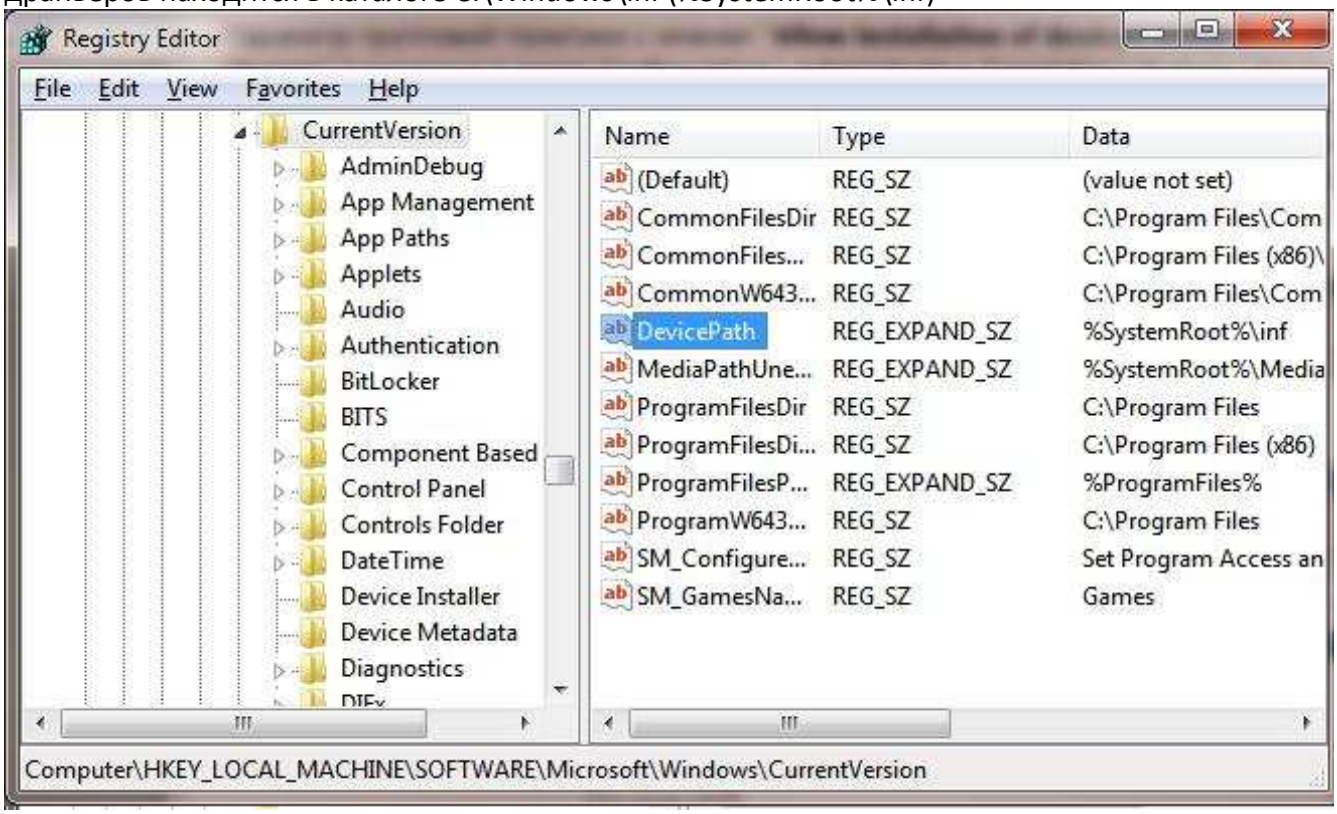
После установки все файлы драйвера хранятся централизованно, в каталоге **C:\Windows\System32\DriverStore\FileRepository**. Чтобы найти каталог с недавно установленным драйвером, просто отсортируйте содержимое этого каталог по дате создания/модификации. Вуаля! Осталось скопировать каталог с драйвером в сетевой каталог, который будет указан на клиентах в качестве сетевого Driver Store (об этом чуть ниже).



Централизованное хранилище драйверов

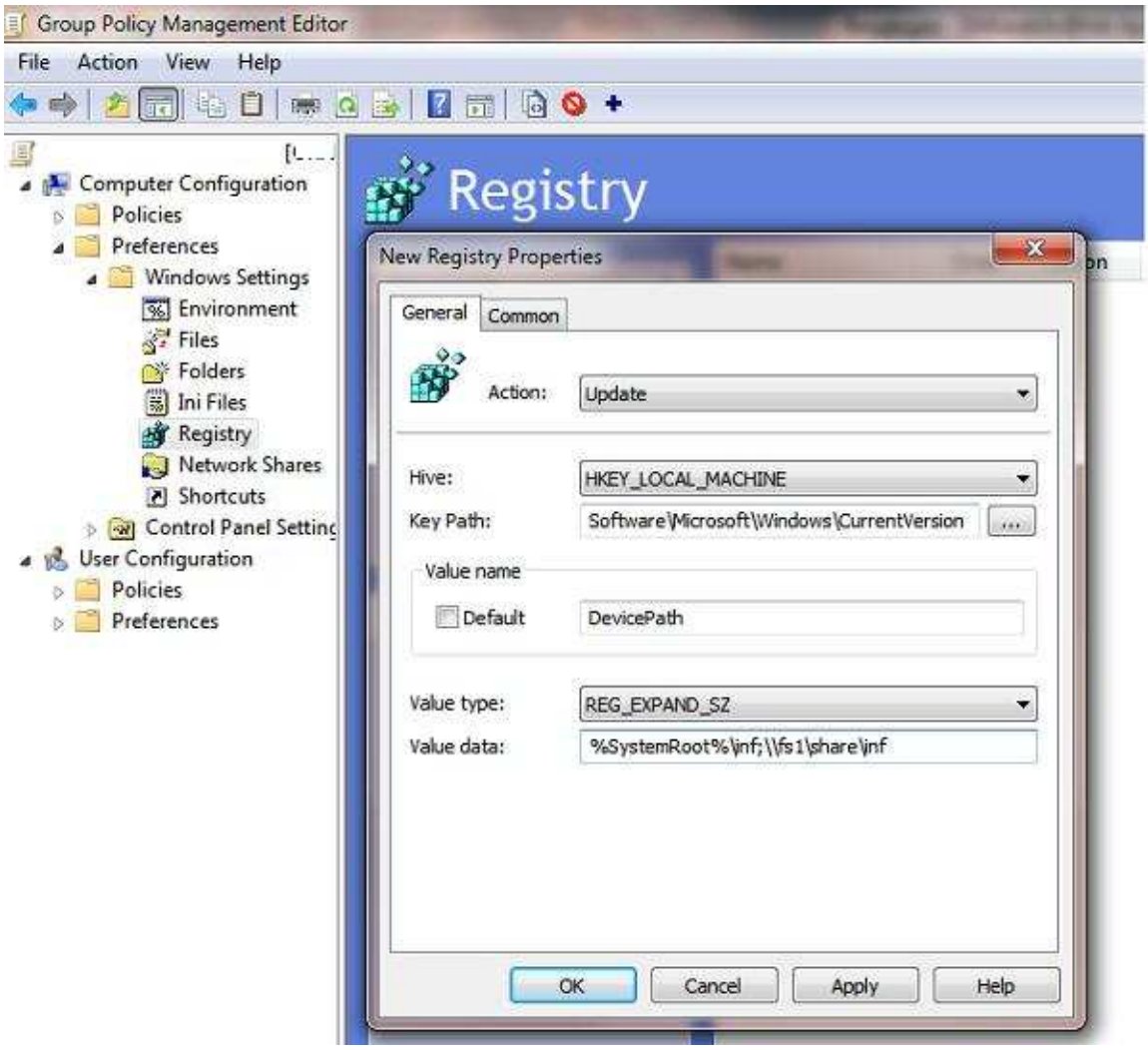
Понятие Driver Store или хранилища драйверов (подробнее о нем мы говорили в этой статье) впервые появилось в Windows Vista и представляет собой доверенную защищённую область компьютера, содержащую набор драйверов, которые разрешены для установки. Таким образом, пользователь может установить в системе только драйвер, который уже имеется в хранилище драйверов. Так при установке нового драйвера администратором, сначала он копируется и регистрируется в хранилище драйверов и только потом устанавливается в системе (файлы драйвера копируются из хранилища в системное расположение).

Путь к хранилищу драйверов Windows задается в реестре параметром **DevicePath** (**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion**). По умолчанию хранилище драйверов находится в каталоге C:\Windows\inf (%SystemRoot%\Inf)



Можно расширить область хранилища драйверов, по которому производится поиск при установке нового драйвера в системе, указав в этом реестра дополнительный каталог. В доменной среде проще всего это сделать с помощью расширения групповых политик — Group Policy Preferences. Для этого в разделе политики **Computer Configuration -> Preferences -> Registry** добавить новый элемент **Registry Item** с параметрами:

- **Action**: Update
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path**: Software\Microsoft\Windows\CurrentVersion
- **Value Name**: DevicePath
- **Value Type**: REG_SZ
- **Value Data**: %SystemRoot%\inf;\\fs1\share\inf



В качестве дополнительного доверенного каталога хранилища драйверов мы указали сетевую папку \\fs1\share\inf (не забудьте, что учетная запись компьютера должна обладать правами на чтение из этой папки). В качестве источника драйвером можно указать сразу несколько сетевых каталогов, например указав в качестве значения переменной: %SystemRoot%\inf;\\fs1\share\Printers;\\fs2\Drivers\USB;\\fs3\Drivers\VGA

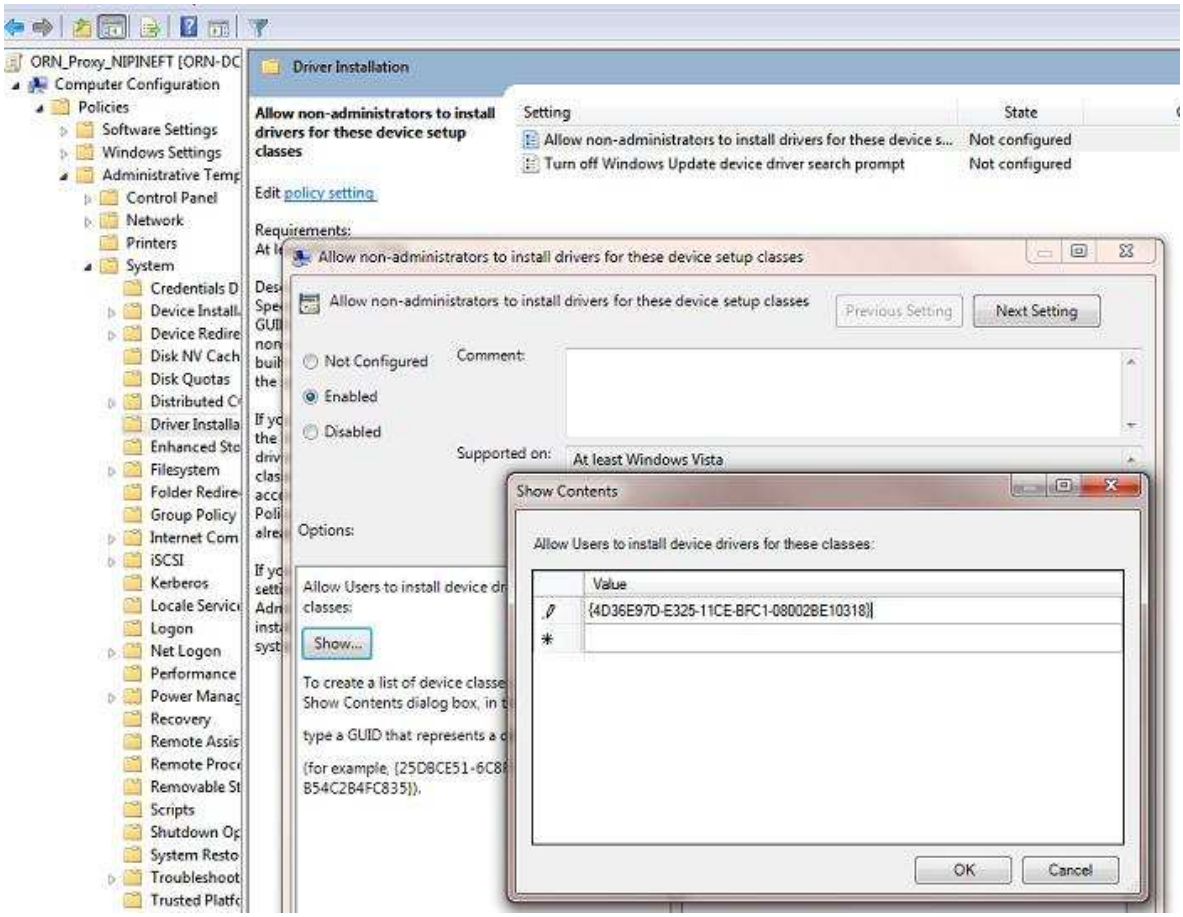
Список классов драйверов, разрешенных для установки

Чтобы определить код класса устройства, откройте каталог с файлами драйвером устройства. Откройте его inf файл и найдите строку с параметром **ClassGUID**. Код класса устройства в нашем примере выглядит так: {4D36E97D-E325-11CE-BFC1-08002BE10318}.

```
;
;
;--*/

[Version]
Signature="$WINDOWS NT$"
Class=SYSTEM
ClassGuid={4D36E97D-E325-11CE-BFC1-08002BE10318}
Provider=%DELL%
DriverVer=08/13/2013,7.4.0.453
CatalogFile=dcdbas64.cat
```

Чтобы разрешить данный класс устройств для самостоятельной установки пользователями, откройте действующую (или создайте новую) групповых политику и в ветке Computer Configuration -> Administrative Templates -> System -> Driver Installation найдите политику **Allow installation of devices using drivers that match these device setup classes**. Включите ее и в качестве значения укажите скопированный ранее код класса устройства.



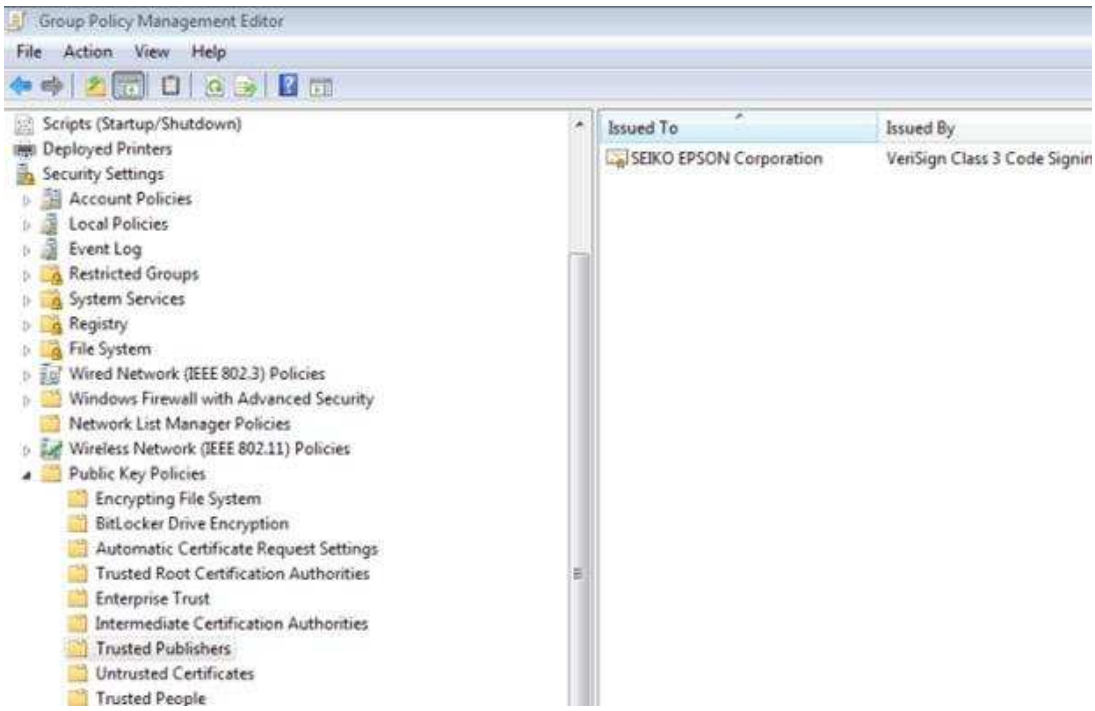
Цифровая подпись драйвера

Чтобы пользователь мог самостоятельно установить драйвер, он в обязательном порядке должны быть подписан, а сертификат издателя цифровой подписи должен находится в списке доверенных. Большинство драйверов крупных вендоров подписаны цифровыми подписями Microsoft и являются доверенными.

Но в этом правиле есть исключения. Чтобы получить сертификат издателя такого драйвера, установите его в системе с правами администратора. Во время установки драйвера появится предупреждения. Установите флажок «**Always trust software from …**» и нажмите **Install**. После установки драйвера откройте оснастку управления сертификатами (**certmgr.msc**), найдите сертификат издателя в разделе **Trusted Published-> Certificates**. Щелкните ПКМ по сертификату

нужного издателя и экспортируйте его в файл.

Далее этот сертификат с помощью групповой политики нужно распространить на всех компьютерах, на которых нужно разрешить установку этого драйвера пользователями. Для этого просто импортируйте сохраненный сертификат в раздел **GPO Computer Configuration -> Windows Settings -> Security Settings -> Public Key Polices -> Trusted Publishers**.



Совет. В том случае, если требуется установить драйвер, цифровая подпись которого отсутствует, можно попробовать самостоятельно подписать его самоподписанным сертификатом. Подробно процесс описан в **этой** статье.

Итак, если вы все сделали правильно, пользователи вашего домена могут самостоятельно (без прав администратора) устанавливать драйвера предопределенных устройств.