**Настройка контроля USB-устройств в Блокхост-сеть 2.0. Практическое руководство.**

Данная статья применима к версии 2.2.16.1038 СЗИ Блокхост-сеть 2.0 (далее БХС)

1. **Описание механизма контроля портов**

Механизм контроля портов в БХС контролирует работу следующих устройств: все USB-устройства, CD и DVD приводы, COM и LPT порты. При этом для всех типов, кроме USB, реализовано только возможность отключения\подключения всех устройств в классе. Таким образом, основные возможности контроля портов в БХС сводятся к разграничению доступа к различным USB-устройствам для пользователей или групп пользователей.

Как видно из картинки ниже, все USB-устройства в контроле портов БХС разбиты на классы. Каждый класс соответствует определенному типу устройств, при этом все подклассы USB являются членами одного класса USB.



Каждый класс в контроле портов соответствует устройствам USB определённого типа. Если перечислять привязки устройств к классам сверху вниз согласно приведенному скрину, то последовательность будет следующей: в классе «USB устройства (0;0:0)» (самый верхний класс на скрине) попадут контроллеры шины USB, в классы c сокращением HID будут отображаться интерфейсные устройства, такие как USB-мышь и клавиатура станции, в классе «Запоминающиеся устройства» будут отображаться флэшки и отчуждаемые USB-диски. К классу «Неизвестные устройства» будут отнесены USB-устройства, которые не были классифицированы по ранее описанным классам. Например, сюда будут отнесены мобильные устройства, если их подключить к станции с помощью USB-кабеля. В последний класс (самый нижний на скрине) будут отнесены все отчуждаемые токены.

 В интерфейсе контроля USB отображаются все устройства, которые когда-либо подключались к системе и записи о подключении которых хранятся в специальном разделе реестра операционной системы. Контроль портов показывает все доступные записи о подключении USB-устройств, причем если у USB-устройства нет уникального идентификатора, то на каждое подключение такого устройства будет создана отдельная запись.

 Контроль USB-устройств в версии 1038 может работать в двух режимах: аудит и «белый» список. В режиме аудита подключение всех USB-устройств разрешено, при этом в журнале аудита БХС появляются сообщения о подключении новых устройств. Режим «белый» список может быть включен для класса USB-устройств. Для этого достаточно снять галку «разрешено» напротив названия класса. При этом все устройства в классе станут тоже запрещены. Устройства, возможность подключения которых необходимо сохранить, необходимо разрешать в отключенном классе отдельно. После включения для класса режима «белого» списка подключения всех новых устройств в этом классе будет также запрещено.

1. **Особенности отображения USB-устройств в механизме контроля портов.**

Для того, чтобы создать корректную политику контроля USB-устройств важно понимать, как именно подключенные устройства отображаются в интерфейсе механизма контроля портов, каким образом подключаются USB-устройства в операционной системе. Именно об этом мы поговорим в данном разделе.

Если посмотреть на скрин механизма контроля портов внимательней, то станет понятно, что он представляет собой большую таблицу, где записями являются USB-устройства, обнаруженные механизмом на данной станции. При этом USB-устройства, которые подключены в настоящее время, отмечены зеленным цветом. Первый столбец условной таблицы механизма контроля портов называется «Устройство». В нем отображается наименования типов устройства, которое контроль портов отыскал на машине и сумел определить. Если устройства определить не удалось, тип будет отображаться как «неизвестное устройство». Администратор безопасности может вручную отредактировать поле «Устройство» (два раза кликнув на него левой клавишей мыши), поменяв названия типа устройства на любую запись. Например, можно переименовать подключенную флэшку, которая ранее отображалась как “compatible USB storage device” в «sundisk 32 GB”. Для успешного переименования необходимо обязательно выполнить сохранение конфигурации БХС.



Также в этом поле можно оставить краткий комментарий по устройству USB, например, обозначить владельца устройства или причину разблокировки.

 Следующий столбец условной таблицы контроля портов называется «логический диск». В нем по замыслу разработчиков отображается буква логического диска, которую флэшка или USB-винчестер получает в системе при подключении. Очевидно, что этот столбец актуален только для класса запоминающих устройств, так как остальные USB-устройства как логические диски не подключаются. Если у вас одновременно подключено несколько флэшек или USB-дисков, то можно, сверив какая флэшка какой логический диск получила на конечной станции, идентифицировать устройства и выполнить их корректную настройку.

 Следующий столбец в таблице контроля портов называется “ID устройства». Это ключевой столбец в интерфейсе контроля портов, так как в нем отображается набор основных аппаратных идентификаторов устройства. Для примера разбора идентификатора возьмем его значений для нашей флэшки из последнего примера:

USB\VID\_0781&PID\_5580\AA010204131900340285

Как мы видим, идентификатор состоит из трех частей. Это VID устройства, PID устройства и собственно ID - идентификатор устройства. VID –это идентификатор, обозначающий цифровой код производителя устройства В нашем случае VID соответствует SanDisk Corporation, производителю нашей флэшки. PID – это номер продукта, цифровой код, который соответствует марке USB – устройства. По PID-коду флэшки из скрина марка устройства определяется как SDCZ80 Flash Drive. Последняя часть идентификатора обозначает код экземпляра устройства, который идентифицирует конечное устройство в серии. Производители некоторых устройств пренебрегают таким уникальным идентификатором для своей продукции. В этом случае значение этого идентификатора генерируется операционной системой при подключении устройства к шине USB. При такой генерации значения идентификатора будут различаться в зависимости от порта, к которому вы подключили флэшку или usb-диск. Понять, есть ли устройства уникальный идентификатор, можно посмотрев значение столбца «Уникальный ID». Если в этом столбце для устройства как раз отображается уникальный идентификатор, который устройству присваивает производитель при изготовлении. Если же там отображается слово «нет», значит ID данного устройства сгенерирован операционной системой. С помощью составного ID администратор безопасности может идентифицировать устройство пользователя, чтобы определить для него политику контроля.

1. **Особенности настройки механизма контроля USB-устройств.**

При настройке механизма контроля портов администратору безопасности следует учесть некоторые особенности интерфейса БХС:

* Если у USB-устройства нет уникального ID, то для каждого подключения такого устройства будет создана запись в интерфейсе контроля портов. При этом, при попытке отключить или разрешить использования такого устройства аналогичная настройка будет применена ко всем записям о этого устройства. Таким образом, создается ощущение что БХС при запрете одной записи запрещает несколько других записей ниже. На самом деле, БХС автоматически определяет, что все эти записи относятся к одному устройству и синхронизирует политику, которую вы выбрали для одной записи, на все записи о подключении данного устройства
* Если вы выполняете настройку класса USB, где на момент настройки есть только одна запись о подключении устройства, либо несколько записей о подключении одного и того же устройства без уникального ID, то простановка элемента «запрещено» на классе автоматически выставит значение «запрещено» на единственном устройстве в этом классе. На практике это означает, что вы не сможете настроить запрет класса и при этом разрешить работу USB-устройства, если оно единственное в своем классе. Если такую настройку произвести необходимо, то нужно добавить в данный класс еще одно уникальное устройство, после чего вы сможете настроить белый список для необходимой вам флэшки.
* Аудит контроля портов возможно отключить только для всех USB-устройств одновременно. Управление аудитом по классам устройств или по устройству в интерфейсе БХС 1038 невозможно
* При запрете класса USB интерфейс контроля портов автоматически проставляет запрет на все устройства в данном классе, разрешать устройство, если это необходимо, нужно вручную
* Для класса USB-устройств есть только два доступных состояния: класс разрешен и класс запрещен. Данное состояния определяет политику подключения новых устройств в классе, если класс запрещен - то новые подключенные устройства также по умолчанию запрещены, если разрешен – то разрешены. При этом в интерфейсе можно видеть, что галочки, определяющие политику на классе в интерфейсе, могут принимать три значения: полный запрет (галочка на «запрещено», «разрешено» пустое), частичный запрет (синий квадрат на «запрещено и «разрешено») и разрешение работы устройств в классе (галочка на «разрешено», «запрещено» пустое). Состояние частичного запрета по поведению класса полностью эквивалентно состоянию полного запрета, т. е. все новые устройства также будут запрещены. Интерфейс активирует состояние частичного запрета, если в классе есть хоть одно разрешенное устройство, по сути, это не более чем визуальная индикация такого состояния
1. **Пример практической настройки механизма контроля портов**

Рассмотрим практический пример настройки механизма контроля портов. В нашем примере мы будем настраивать контроль запоминающих устройств USB в режиме «белого» списка. В белом списке будет флэшка sundisk емкостью 32 GB, работа остальных запоминающих устройств в классе должна быть запрещена. Настройку контроля портов будем выполнять для пользователя RACK9\sky на клиенте w7x64. Перед началом настроек мягкий режим должен быть отключен!

Скрин начальных условий настройки ниже:



 Имеются две подключенных флэшки, одна из них с уникальным идентификатором - необходимая нам флэшка sundisk (можно определить по анализу ID устройства), вторая – неизвестная нам флэшка без уникального идентификатора. Настройки выполняются для пользователя sky на клиенте wks\_w7x64vp. Обратите внимание, что настройка, которую мы выполняем применится только пользователя rack9\sky на станции wks\_w7x64vp! Для всех остальных пользователей на этом клиенте контроль портов будет работать в режиме по умолчанию.

Начинаем выполнять настройки:

* Переименовываем разрешенную флэшку в sundsik32
* Запрещаем класс запоминающие устройства, тем самым включая режим «белого» списка
* Разрешаем sundsik32
* Выполняем сохранение настроек

В результате выполнения настроек наш скрин должен принять вот такой вид:



Далее необходимо проверить инициализировать настройки, а заодно проверить их работоспособность. Для этого завершаем сеанс пользователя, который был залогинен на wks\_w7x64vp и выполняем вход под RACK9\sky. Повторно подключаем к клиенту флэшку sundisk32.

Смотрим результат на клиенте. Флэшка sundisk32 подключилась, использование второй флэшки запрещено.

Проверить результаты работы механизма контроля портов можно в диспетчере устройств клиента:



Мы видим, что в диспетчере есть два запоминающих устройства USB, одно из которых запрещено. Запрет - результат действия механизма контроля портов БХС.