Управляемый USB over IP концентратор

DistKontrolUSB

(**Устройство подключения USB по сети**)

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Версия 3.18.2

Москва 2021 г.

Оглавление

ВНИМАНИЕ !!!

1. Работа над аппаратной и программной частями оборудования ведется непрерывно. Могут иметь место расхождения между описанием и существующим функционалом. Описываемые в руководстве опции и функции присутствуют в различных модификациях устройств, и не обязательно присутствуют в ВАШЕЙ модели устройства.

2. Устройство корректно работает с основной массой наиболее распространенных электронных ключей защиты, флеш носителей, USB камер и прочих USB устройств, но не гарантируется подключение по сети абсолютно всех USB устройств.

3. Настоящее «Руководство пользователя» предназначено для изучения устройства, порядка и правил эксплуатации, выполнения установки, настройки управляемого USB over IP концентратора. Для использования USB over IP концентратора рекомендуется изучить настоящее Руководство. При установке управляемого USB over IP концентратора следует руководствоваться положениями «Правил техники безопасности при эксплуатации электроустановок потребителей» и «Правил техники эксплуатации электроустановок потребителей». Для настройки управляемого USB over IP концентратора необходимо иметь навыки уверенного пользователя персональным компьютером.

4. «Руководство пользователя» актуально для концентратора с текущей версией ПО. Для ПО до указанной версии см. «Руководство пользователя» на устройстве. Историю версий ПО см.: http://distkontrol.ru/index.php/history-dk

1 ОБЩАЯ ИНФОРМАЦИЯ

Управляемый USB over IP концентратор (далее концентратор) входит в серию оборудования обеспечения безопасности и удобства использования USB устройств DistKontrolUSB:

- Управляемые USB over IP концентраторы - для удаленного подключения и аппаратного отключения и включения USB устройств по сети;
- USB over IP хабы - для удаленного подключения USB устройств по сети;
- Управляемые USB хабы – для аппаратного отключения и включения USB устройств, подключенных по интерфейсу USB;

1.1НАЗНАЧЕНИЕ ПРИБОРА

Управляемый USB over IP концентратор предназначен для подключения USB устройств (в том числе ключей электронной защиты, например, серии eToken, ruToken и других аналогов, ключей для программных продуктов 1С, сканеров, принтеров, МФУ, сенсоров и т.д.) к компьютерной сети и позволяет всем пользователям сети удаленно подключать USB устройства к своему компьютеру или ноутбуку, пользоваться ими и удаленно управлять физическим включением и подключением этих USB устройств.

Управляемый USB over IP концентратор обеспечивает двухступенчатую защиту USB устройств при совместном использовании USB по сети:

1. Удаленное физическое включение и выключение USB устройств;

2. Авторизацию для подключения USB устройств по логину, паролю и IP адресу.

В журнале управляемого USB over IP концентратора хранится вся информация о подключениях и отключениях как USB входов (портов) DistKontrolUSB, так и любого из USB устройств, а также попытки не правильного ввода пароля и прочая дополнительная информация.

1.2 МОДЕЛЬНЫЙ РЯД УПРАВЛЯЕМЫХ USB OVER IP КОНЦЕНТРАТОРОВ

Управляемый USB over IP концентратор
на 16 портов USB

Управляемый USB over IP концентратор
на 32 порта USB

Управляемый USB over IP концентратор
на 48 портов USB

Управляемый USB over IP концентратор
на 64 порта USB

1.3 ОБЛАСТЬ ПРИМЕНЕНИЯ УПРАВЛЯЕМЫХ USB OVER IP КОНЦЕНТРАТОРОВ

Возможность управления USB over IP портами позволяет удаленно, через WEB интерфейс отключать и включать USB устройства физически. Управляемый USB over IP концентратор поддерживает веб-управление, включающее в себя удаленное управление и систему оповещений. Исполнение – настольное (с возможностью установки в 19" стойку). Управляемый USB over IP концентратор позволяет аппаратно отключать и включать USB устройства, подключенные по сети. В WEB интерфейсе USB over IP концентратора, есть страницы для управления портами USB, добавления пользователей и управления правами доступа. Для пользователей в WEB интерфейсе доступно только управление разрешенными портами USB, изменение пароля и адреса электронной почты для отправки уведомлений.

Управляемый USB over IP концентратор (устройство подключения USB по сети DistKontrolUSB) - это аппаратно-программное решение, позволяющее устройствам USB использоваться удаленно посредством сети и работать с ним напрямую так же, как если бы они были подключены локально! Это даёт возможность использовать удаленные устройства USB на своем компьютере, так и делиться своими USB устройствами с другими пользователями или ресурсами по сети (по сути удлиняя USB кабель через линию интернета).

Устройство DistKontrolUSB имеет встроенный Wi-Fi-модуль и сетевой адаптер Ethernet (RJ-45), работающий со скоростью 100 Мбит/с. Это позволяет подключать устройство к сети, как по проводным, так и по беспроводным (Wi-Fi) каналам связи. Устройство выпускается в металлическом корпусе. Дальность действия беспроводной сети при исполнении устройства в металлическом корпусе – ограничена.

Подключение USB устройств по сети для их совместного использования позволяет более эффективно использовать компьютерные ресурсы и, главное, экономит время и деньги, несмотря на стоимость самого устройства подключения USB по сети. Наличие беспроводного канала связи в устройстве аппаратного подключения USB по сети, позволяет дополнительно обеспечить безопасность и физическую недоступность совместно используемых USB устройств.

Возможность удаленного подключения USB устройств по сети с помощью управляемого USB over IP концентратора позволит Вашей компании поднять на новый качественный уровень безопасность информации, безопасность совместного использования различных USB устройств. Все Ваши носители электронных цифровых подписей будут храниться в недоступном для свободного доступа (удаленном) месте и подключаться при необходимости тоже удаленно.

Отсутствие возможности потерять, вывести из строя какой-то ключ принесет существенную экономию материальных средств.

Устройство подключения USB по сети DistKontrolUSB идеально подходит для совместного использования USB устройств между несколькими пользователями в сети, через Интернет или в облаке без устройства USB, которое необходимо физически подключить к каждому пользовательскому компьютеру. На компьютере пользователя USB устройство выглядит так, как если бы оно было подключено напрямую, даже если оно подключено к удаленному серверу, поэтому существующие драйверы и программное обеспечение работают без каких-либо изменений.

Используя устройство аппаратного подключения USB по сети, вы сможете обеспечит беспрецедентную гибкость использования USB устройств и поднять на качественно новый уровень безопасность их использования. Возможность подключения, управляемого USB over IP концентратора к нескольким USB хостам одновременно позволит Вам легко продолжить использование USB устройств в кластерных системах.

Устройство подключения USB по сети DistKontrolUSB тестировалось и совместимо с платформами виртуализации VMware и Microsoft Hyper-V.

1.4 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ УПРАВЛЯЕМЫХ USB OVER IP КОНЦЕНТРАТОРОВ

Модель	**DistKontrolUSB-4**	**DistKontrolUSB-16**	**DistKontrolUSB-32**	**DistKontrolUSB-48**	**DistKontrolUSB-64**
Сетевые интерфейсы	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless
Порт Ethernet	1 x 10/100 Mb (опционально: 1 x 10/100/1000 Mb)	1 x 10/100 Mb (опционально: 1 x 10/100/1000 Mb) (опционально: 2 x 10/100/1000 Mb)	1 x 10/100 Mb (опционально: 1 x 10/100/1000 Mb) (опционально: 2 x 10/100/1000 Mb)	1 x 10/100 Mb (опционально: 1 x 10/100/1000 Mb) (опционально: 2 x 10/100/1000 Mb)	1 x 10/100 Mb (опционально: 1 x 10/100/1000 Mb) (опционально: 2 x 10/100/1000 Mb)
Количество не управляемых USB портов (входов)	4	-	-	-	-
Количество управляемых USB портов (входов)	-	16	32	48	64
IP адреса	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)
Индикация LEDs	Питание, LAN порт статус	Питание, LAN порт статус, наличие питания порта USB-устройства	Питание, LAN порт статус, наличие питания порта USB-устройства	Питание, LAN порт статус, наличие питания порта USB-устройства	Питание, LAN порт статус, наличие питания порта USB-устройства
Питание	Встроенный блок питания 220В 50 Гц, 100 Вт	Встроенный блок питания 220В 50 Гц, 150 Вт (опционально: Второй блок питания в режиме резервирования питания)	Встроенный блок питания 220В 50 Гц,200 Вт (опционально: Второй блок питания в режиме резервирования питания)	Два встроенных блока питания 220В 50 Гц, 200 Вт (опционально: Второй блок питания в режиме резервирования питания)	Встроенный блок питания 220В 50 Гц, 200 Вт (опционально: Второй блок питания в режиме резервирования питания)
Поддержка USB	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0
Защита USB портов	-	Ограничение USB портов по току, выключение USB порта при перегреве, схема плавного запуска USB портов	Ограничение USB портов по току, выключение USB порта при перегреве, схема плавного запуска USB портов	Ограничение USB портов по току, выключение USB порта при перегреве, схема плавного запуска USB портов	Ограничение USB портов по току, выключение USB порта при перегреве, схема плавного запуска USB портов
Номинальный ток нагрузки на порт USB	-	0,5 А	0,5 А	0,5 А	0,5 А

Предельный ток нагрузки на порт USB	-	0,9 А	0,9 А	0,9 А	0,9 А
Температура окружающей среды	0°C до +50°C	0°C до +50°C	0°C до +50°C	0°C до +50°C	0°C до +50°C
Относительная влажность воздуха	не более 80% (при температуре +35°C и ниже)	не более 80% (при температуре +35°C и ниже)	не более 80% (при температуре +35°C и ниже)	не более 80% (при температуре +35°C и ниже)	не более 80% (при температуре +35°C и ниже)
Поддержка операционных систем	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Linux, OSX 10.9.5-10.13	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Linux, OSX 10.9.5-10.13	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Linux, OSX 10.9.5-10.13	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Linux, OSX 10.9.5-10.13	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Linux, OSX 10.9.5-10.13
Габаритные размеры (высота/ширина/глубина)	35 / 140 / 110	44 / 440 / 285	85 / 440 / 205	130 / 440 / 205	130 / 440 / 205
Крепление в 19” стойку	нет	есть	есть	есть	есть
Размеры в Unit	-	1	2	3	3
Безопасность	https, ssl	https, ssl	https, ssl	https, ssl	https, ssl
Шифрование трафика USB	есть	есть	есть	есть	есть
Встроенный брандмауэр	есть	есть	есть	есть	есть
Ограничение по IP для подключения USB устройства	нет	есть	есть	есть	есть
Ограничение по IP для подключения USB порта	нет	есть	есть	есть	есть
Авторизация для подключения USB устройства	нет	есть	есть	есть	есть
Авторизация для подключения USB порта	нет	есть	есть	есть	есть
Модуль защиты подключаемых USB устройств	нет	(опционально: есть)	(опционально: есть)	(опционально: есть)	(опционально: есть)

Управляемый USB over IP концентратор обеспечивает ограничение USB портов по току и схему выключения при перегреве, которые защищают нагрузку от нештатных ситуаций. При возникновении перегрева выход блокируется до устранения неисправности. Удаление нагрузки перезагрузит USB вход. Также, концентратор имеют схему плавного запуска USB портов, которая минимизирует броски пускового тока в тех случаях, когда присутствует высокая емкостная нагрузка.

Управляемый USB over IP концентратор обеспечивает номинальный ток нагрузки 0,5 А на порт и ограничивает потребляемый нагрузкой ток (предельный ток нагрузки - 0,9 А).

1.5 КОМПЛЕКТ ПОСТАВКИ УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА

№	Наименование	Кол-во
1	Управляемый USB over IP концентратор	1
2	Паспорт	1
3	Шнур питания	1
4	Крепление в стойку 19"	2
5	Винты крепления	8
6	Ножка для настольной установки	4

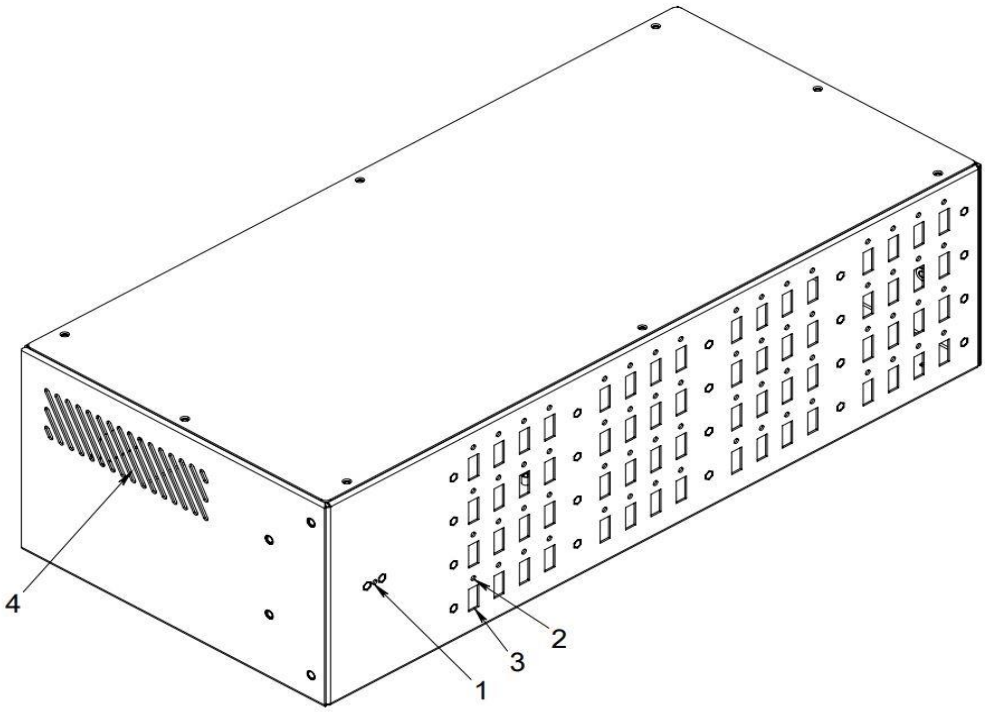
1.6 УСТРОЙСТВО И РАБОТА УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА

1.6.1 ГАБАРИТНЫЕ РАЗМЕРЫ УПРАВЛЯЕМЫХ USB OVER IP КОНЦЕНТРАТОРОВ (В 19” СТОЙКУ)

Наименование изделия	высота в U	габариты изделия в мм.			габариты упаковки в мм.		
		высота	ширина	глубина	высота	ширина	глубина
Управляемый USB over IP концентратор на 16 портов USB	1	44	440	285	50	500	320
Управляемый USB over IP концентратор на 32 порта USB	2	85	440	205	128	500	240
Управляемый USB over IP концентратор на 48 портов USB	3	130	440	205	128	500	240
Управляемый USB over IP концентратор на 64 порта USB	3	130	440	205	171	500	240

1.6.2 УСТРОЙСТВО ПРИБОРА

Концентратор выполнен в металлическом корпусе, допускающем его установку на стол или монтаж в стойку форм-фактора 19".



На передней панели расположены:

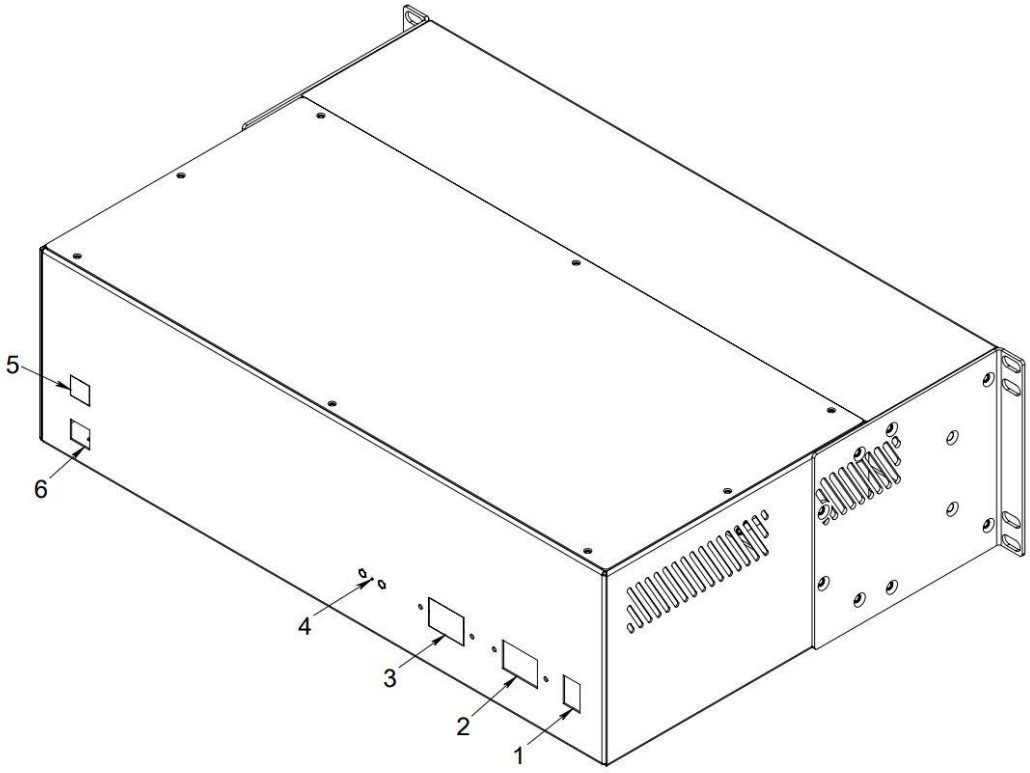
1 - индикатор включения питания;

2 - индикатор активности USB-порта.

3 - разъемы типа USB-A нисходящих портов для подключения устройств, поддерживающих протокол USB;

На боковых панелях размещены:

4 - вентиляционные отверстия;



На задней панели установлены:

1 - Выключатель питания «Питание».

2 - Разъем для подключения сетевого кабеля 1;

3 - Разъем для подключения сетевого кабеля 2(опционально);

4 – Кнопка сброса настроек «Reset»

5 - Разъем типа RJ45 для сети Ethernet «LAN» 2(опционально);

6 - Разъем типа RJ45 для сети Ethernet «LAN» 1;

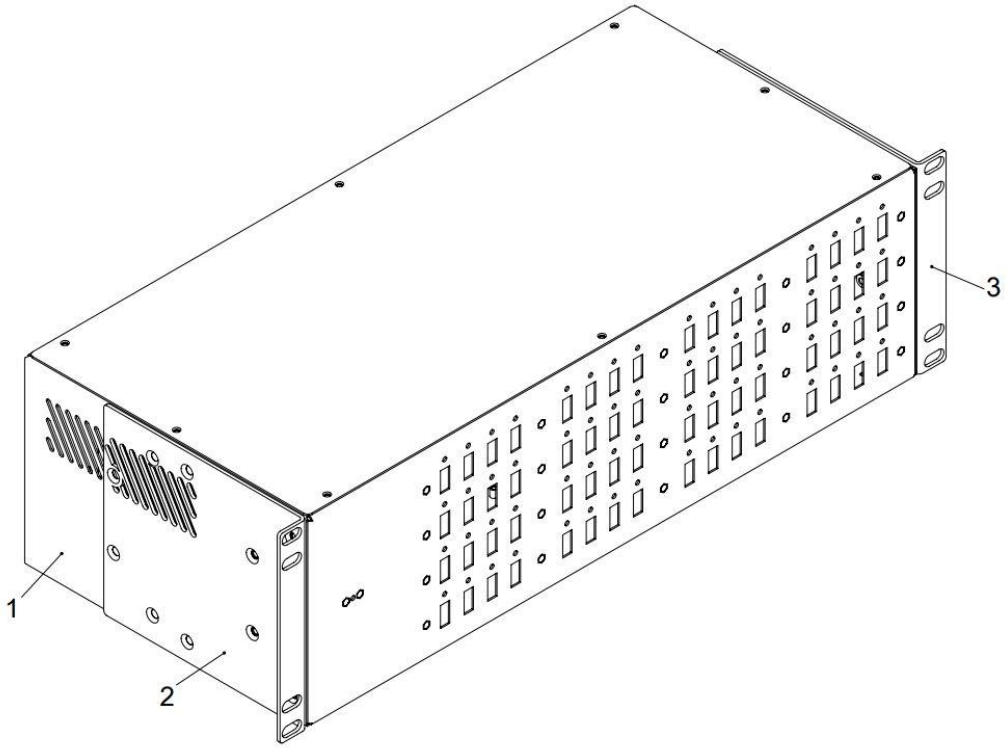
По углам нижней панели концентратора имеется четыре отверстия для монтажа приборных ножек для его установки на поверхность (стол).

В комплекте с устройством поставляются крепления в стойку/шкаф 19” с возможностью крепления в двух положениях.

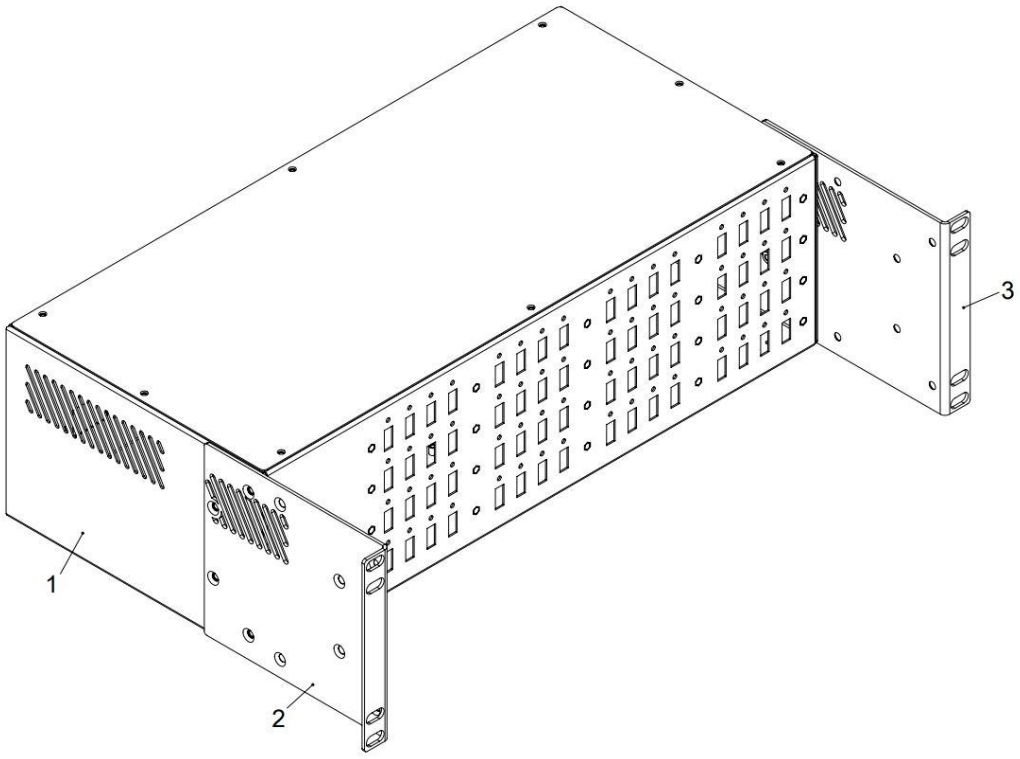
На рис:

1 – Устройство;

2,3 – Крепления в стойку/шкаф 19”;



Сборка устройства для крепления в стойку 19”.



Сборка устройства для крепления в шкаф 19”.

1.6.3 МОДУЛЬ ЗАЩИТЫ ПОДКЛЮЧАЕМЫХ USB УСТРОЙСТВ УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

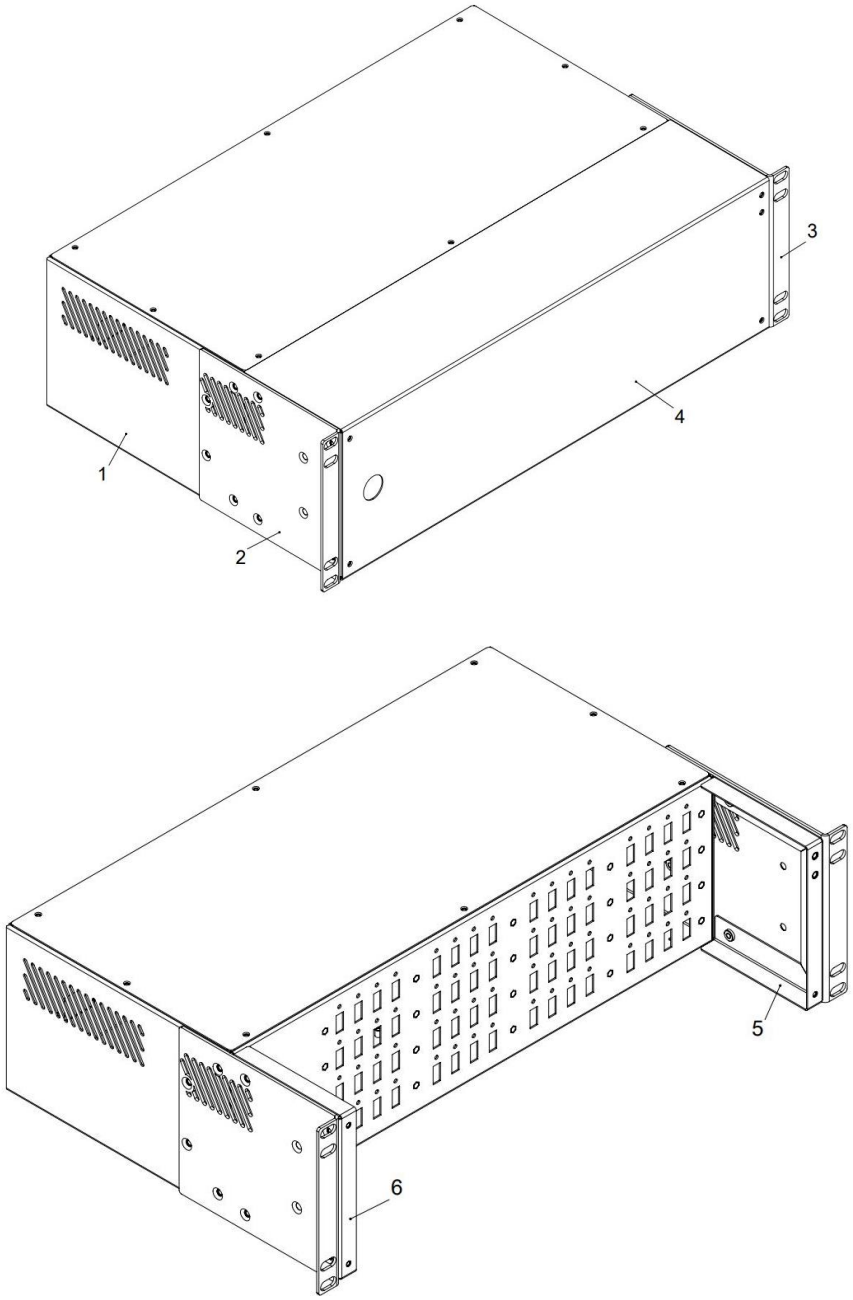
Модуль защиты подключаемых USB устройств управляемого USB over IP концентратора поставляется отдельно (опционально). В стандартную комплектацию не входит.

Модуль предназначена для защиты подключаемых USB устройств от повреждения и физического доступа. Включает в себя дополнительное крепление для крышки и защитную крышку. На крышке предусмотрена возможность пломбировки.

Внешний вид.:

4 – Защитная крышка;

5,6 – Крепления модуля защиты.



1.6.4 ЭКСПЛУАТАЦИОННЫЕ ОГРАНИЧЕНИЯ И РЕКОМЕНДАЦИИ

Концентратор обеспечивает непрерывную круглосуточную работу и является восстанавливаемым и обслуживаемым.

Концентратор сохраняет работоспособность при воздействии:

- повышенной температуры окружающей среды до +50°С;
- пониженной температуры окружающей среды не ниже - 5°С;
- повышенной относительной влажности воздуха до 98% при температуре плюс 25°С;
- синусоидальной вибрации в диапазоне частот от 10 до 55 Гц при амплитуде смещения до 0,35 мм (в любом направлении) в соответствии с требованиями ГОСТ 12997.

1.6.5 МЕРЫ БЕЗОПАСНОСТИ

При эксплуатации прибора следует соблюдать «Межотраслевые правила по охране труда (правила безопасности) при эксплуатации электроустановок».

Класс безопасности - I по ГОСТ 12.2.007.0-75

Конструкция прибора обеспечивает степень защиты IP 20 по ГОСТ 14254-96.

Источниками опасности прибора являются цепи сетевого напряжения ~220В, контакты ~220В разъёма подключения кабеля питания и встроенный преобразователь напряжения.

Прибор устанавливается горизонтально на столах или других конструкциях, в стойку 19`, в местах, где отсутствует доступ посторонних лиц.

Установку (снятие), монтаж, ремонт производить при отключенном сетевом напряжении ~220В от прибора.

Не рекомендуется закрывать вентиляционные отверстия концентратора на боковых панелях.

1.6.6 ПОДГОТОВКА УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА К РАБОТЕ

Подготовка концентратора к использованию включает в себя следующие операции:

- после распаковки, визуально проверить, нет ли на концентраторе повреждений;
- разместить концентратор на устойчивой, ровной поверхности (столе) или закрепить в стойке 19";
- подключить шнур питания на задней панели концентратора;
- подключить вилку сетевого шнура к сети 220В 50 Гц;
- подключить к USB-портам, расположенным на передней панели прибора, устройства, поддерживающие протокол USB;
- подключить прибор к сети Ethernet;
- включить питание.

Не включайте концентратор, если его температура ниже комнатной! (Это может возникнуть при перевозке концентратора в холодное время года). Дайте концентратору нагреться до комнатной температуры, прежде чем включать его.

1.6.7 РАБОТА УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА

Для работы с USB устройством, подключенным к управляемому USB over IP концентратору, необходимо:

1. Включить USB устройство (удаленно подать питание на устройство USB);
2. Подключить USB устройство к своему компьютеру (ноутбуку, планшету, телефону и т.п.).

Включение и отключение USB устройств, подключенных к управляемому USB over IP концентратору возможно (включение и отключение USB входов устройства):

- Через WEB интерфейс;
- С помощью планировщика задач и назначенных заданий;
- С помощью утилиты управления устройством (скриптами, из командной строки или своего приложения).

Подключение и отключение USB устройств, подключенных к управляемому USB over IP концентратору возможно:

- Через клиентское приложение, работающее в графическом режиме или в виде службы;
- С помощью API (скриптами, из командной строки или своего приложения).

Для использования, управляемого USB over IP концентратора, необходимо:

1. Подключить устройство к LAN (через Ethernet или WiFi) и произвести его настройку.
2. На каждом компьютере, к которому необходимо пробросить USB устройство запустить программное обеспечение DistKontrolUSB Client, работающее под управлением версий Linux, Windows, OSX.
3. Настройка и управление устройством подключения USB по сети осуществляется через Web интерфейс.
4. Настройка клиентского компьютера проста и интуитивно понятна. DistKontrolUSB Client работает под управлением версий Linux, Windows, а также OSX. Клиент позволяет интуитивно понятного и простого подключать и отключать удаленные устройства USB. DistKontrolUSB Client не требует установки. Клиент может запускаться в качестве сервиса.

1.7 ПЛОМБИРОВАНИЕ

После проведения приемо-сдаточных испытаний на предприятии-изготовителе прибор пломбируется.

Устанавливаемые пломбы (печати) должны исключать возможность несанкционированного внесения изменений в электрическую принципиальную схему прибора. Пломбы (печати) устанавливаются на приборе таким образом, чтобы исключить возможность снятия крышки прибора без повреждения пломбы (печати).

1.8 УПАКОВКА

Готовой продукцией считается прибор, принятый представителем технического контроля и упакованный в потребительскую тару.

2 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

2.1 ОБЩИЕ ПОЛОЖЕНИЯ

Техническое обслуживание прибора проводится по планово-предупредительной системе и осуществляется Потребителем. Персонал, обслуживающий данные изделия, должен иметь группу по электробезопасности не ниже III.

Техническое обслуживание заключается в периодическом (не реже одного раза в год) 6

- внешнем осмотре концентратора, с удалением пыли мягкой тканью;
- проверке работоспособности концентратора.

При техническом обслуживании должны соблюдаться требования техники безопасности, а также требования ГОСТ 12.1.006, ГОСТ 12.1.019, ГОСТ 12.2.003, «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

2.2 ПРОВЕРКА РАБОТОСПОСОБНОСТИ УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА

Для проверки прибора необходимо к каждому из портов подключить USB флеш-накопитель с записанными на него произвольными файлами, и, подключив этот накопитель к ПК посредством WEB-интерфейса (индикатор активности порта должен гореть), произвести чтение файла. Возможность чтения файла свидетельствует об исправности проверяемого порта. После отключения порта индикатор включения порта должен погаснуть.

Примечание: в случае отсутствия необходимого количества флеш-накопителей можно производить указанные операции с портами последовательно.

3 КОНСЕРВАЦИЯ И ХРАНЕНИЕ УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА

3.1 КОНСЕРВАЦИЯ

Консервация прибора при длительном хранении не предусматривается.

3.2 ХРАНЕНИЕ, ТРАНСПОРТИРОВКА И УТИЛИЗАЦИЯ

Хранение прибора рекомендуется производить в отапливаемых складских помещениях. В помещениях не должно быть паров кислот, щелочей, агрессивных газов и других вредных примесей, вызывающих коррозию.

Гарантийный срок хранения в отапливаемых складских помещениях в потребительской таре – не менее 3 лет.

Транспортировка прибора может осуществляться любыми видами автомобильного, железнодорожного транспорта в закрытых кузовах (контейнерах, вагонах).

Условия транспортировки должны соответствовать условиям хранения 5 по ГОСТ 15150-69.

После транспортировки прибор перед включением должен быть выдержан в нормальных условиях не менее 12 часов.

Специальных требований к утилизации прибора не предъявляется.

4 WEB ИНТЕРФЕЙС УПРАВЛЕНИЯ DISTKONTROLUSB

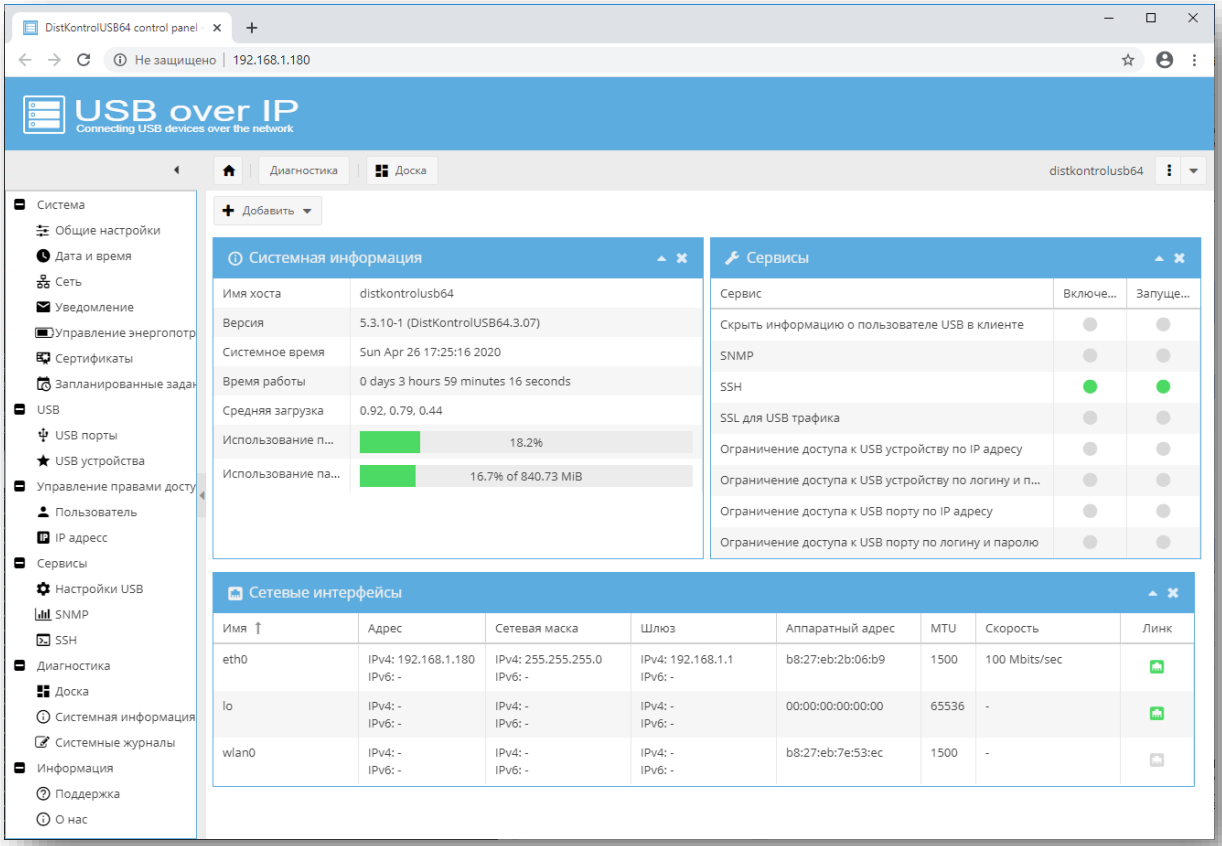
4.1 ВХОД В WEB ИНТЕРФЕЙС И НАЧАЛЬНЫЙ ЭКРАН

Управление USB over IP концентратором осуществляется через мульти язычный WEB интерфейс администратора.

После авторизации доступно управление настройками.

Вид главной страницы можно настроить, добавив или убрав нужные панели.

Вид WEB интерфейса управления настройками устройства подключения USB по сети:



По умолчанию устройство подключения USB по сети имеет:

Статический IP адрес – 192.168.1.180

Логин к панели WEB интерфейса – admin

Пароль к панели WEB интерфейса – admin

Порт подключения клиентов – 6565 (по умолчанию)

SSL порт подключения клиентов – 6564 (при включенном режиме)

Интерфейс WiFi (wlan0) – отключен

Внимание!!! При некорректном вводе пароля до 4 раз, пользователь, для которого были попытки ввода, блокируется на 3 минуты. Каждый последующий ввод, даже корректного пароля, обновляет таймер блокировки.

4.2 СИСТЕМА

4.2.1 ОБЩИЕ НАСТРОЙКИ

В данном разделе находятся настройки Web интерфейса.

SSL настраивается для Web интерфейса, для USB трафика см. раздел «Параметры клиентского приложения»

Внимание!!! При отключении, ранее настроенного шифрования, требуется очистить кэш браузера, так как некоторые браузеры кэшируют переадресацию с http на https.

4.2.2 ДАТА И ВРЕМЯ

По умолчанию используется NTP сервер. Для ручного ввода времени необходимо отключить «Использование сервера NTP». Функция «Обновить сейчас» доступна только при ручной установки времени.

В разделе Информация текущее время статично, загружается в момент открытия настройки «Дата и время».

4.2.3 СЕТЬ

4.2.3.1 ОБЩИЙ

Имя хоста – имя которое будет отображено в клиенте DistKontrolUSB. Рекомендуется изменить при нескольких концентраторах в сети. При наличии несколько сетевых интерфейсов, рекомендуется добавлять концентратор по имени хоста. В этом случае независимо от активного интерфейса устройство будет отображено в клиенте.

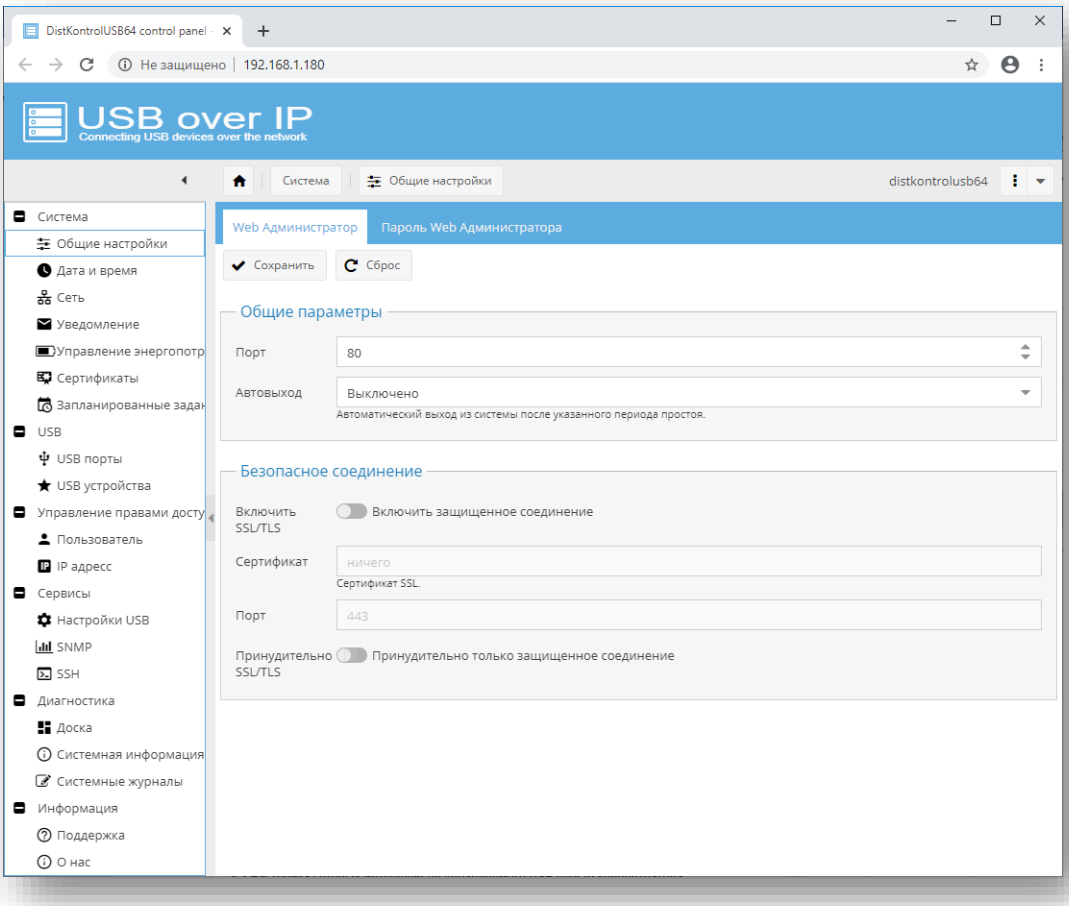
Доменное имя – добавляет имя домена 2 и более уровня. Не влияет на подключение к домену, используется для графического отображения в клиентском приложении.

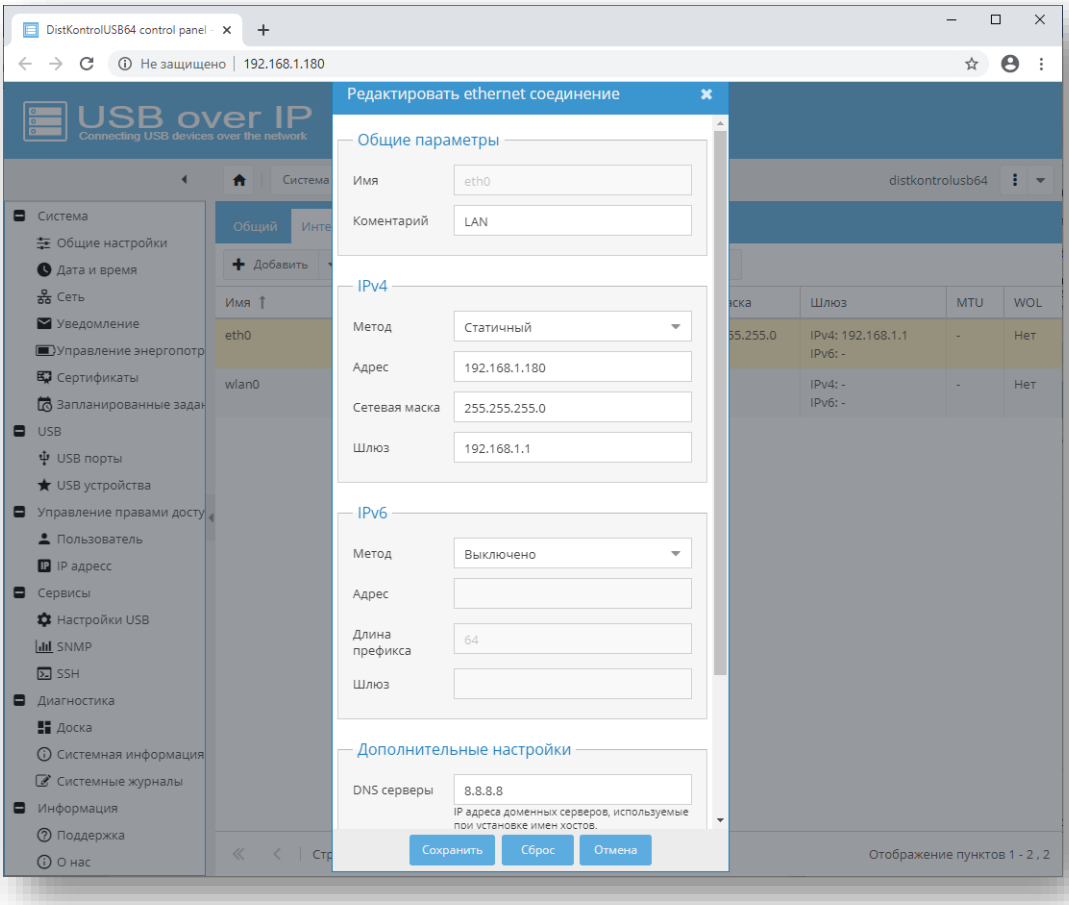
4.2.3.2 ИНТЕРФЕЙСЫ

Для начала работы необходимо изменить IP адрес устройства и пароль WEB интерфейса.

IP адрес меняется при двойном клике на соответствующем сетевом интерфейсе (страница Сеть - Интерфейсы). Возможно, как совместное использование интерфейсов LAN(eth0) и WiFi(wlan0), так и самостоятельное использование любого из интерфейсов. При использовании только одного сетевого интерфейса, второй рекомендуется отключать.

На странице общих настроек можно изменить пароль для доступа к WEB интерфейсу, порт WEB интерфейса.

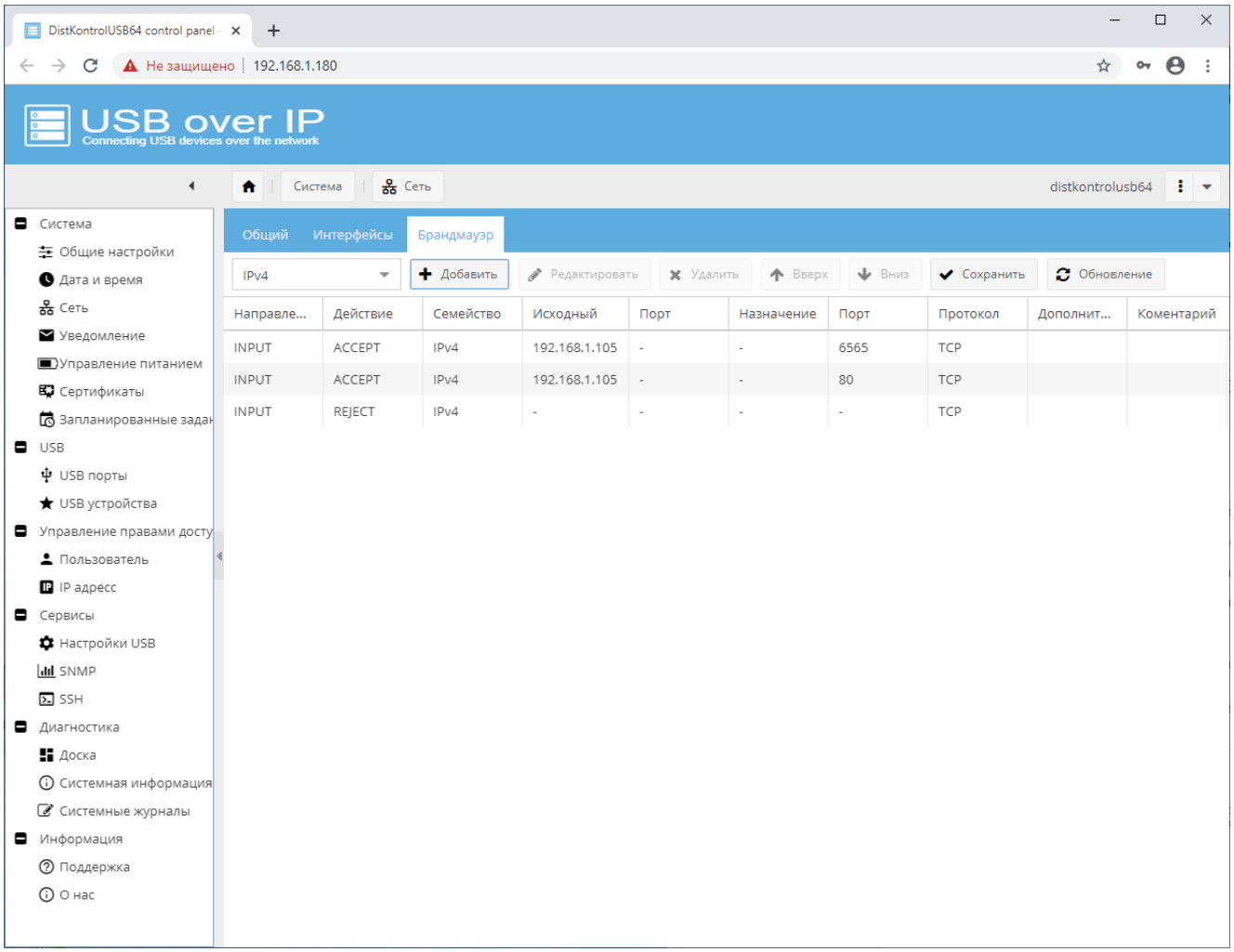

DistKontrolUSB64 control panel
Не защищено | 192.168.1.180
USB over IP
Connecting USB devices over the network
Система
Общие настройки
distkontrolusb64
Web Администратор
Пароль Web Администратора
Сохранить
Сброс
Общие параметры
Порт
80
Автовыход
Выключено
Автоматический выход из системы после указанного периода простоя.
Безопасное соединение
Включить SSL/TLS
Включить защищенное соединение
Сертификат
ничего
Сертификат SSL.
Порт
443
Принудительно SSL/TLS
Принудительно только защищенное соединение
Система
Общие настройки
Дата и время
Сеть
Уведомление
Управление энергопотр
Сертификаты
USB
USB порты
USB устройства
Управление правами досту
Пользователь
IP адресс
Сервисы
Настройки USB
SNMP
SSH
Диагностика
Доска
Системная информация
Системные журналы
Информация
Поддержка
О нас


DistKontrolUSB64 control panel
Не защищено | 192.168.1.180
USB over IP
Connecting USB devices over the network
Редактировать ethernet соединение
Общие параметры
Имя
eth0
Коментарий
LAN
IPv4
Метод
Статичный
Адрес
192.168.1.180
Сетевая маска
255.255.255.0
Шлюз
192.168.1.1
IPv6
Метод
Выключено
Адрес
Длина префикса
64
Шлюз
Дополнительные настройки
DNS серверы
8.8.8.8
IP адреса доменных серверов, используемые при установке имен хостов.
Сохранить
Сброс
Отмена
Добавить
Имя
Шлюз
MTU
WOL
eth0
IPv4: 192.168.1.1
IPv6: -
Нет
wlan0
IPv4: -
IPv6: -
Нет
Отображение пунктов 1 - 2 , 2

Для создания соединения Bond, необходимо удалить все интерфейсы, которые будут участвовать в соединении. При удалении интерфейса eth0, IP адрес устройства станет динамическим. После применения настроек, зайдите в Web интерфейс по новому адресу и настройте bond соединения добавив все необходимые интерфейсы.

4.2.3.3 БРАНДМАУЭР

Брандмауэр концентратора работает на базе iptables. Он может быть полезен, если вам необходимо полностью исключить доступ к концентратору каким-то компьютерам в локальной сети. Или предоставить доступ только с определенных компьютеров. Можно создать соответствующие правила в таблице фильтров.



Например, требуется предоставить доступ к концентратору (WEB интерфейсу - порт 80 и USB устройствам – порт 6565) только с одного компьютера в локальной сети с IP 192.168.1.105.

Необходимо (см. скриншот страницы выше):

1. Разрешить доступ с IP 192.168.1.105 к концентратору для клиентского приложения.
2. Разрешить доступ с IP 192.168.1.105 к web интерфейсу концентратора.
3. Разрешить доступ с localhost 127.0.0.1
4. Все остальные соединения запретить.

Последовательность правил важна. В результате - со всех кроме указанного в правилах IP адреса, в клиенте концентратор будет отсутствовать.

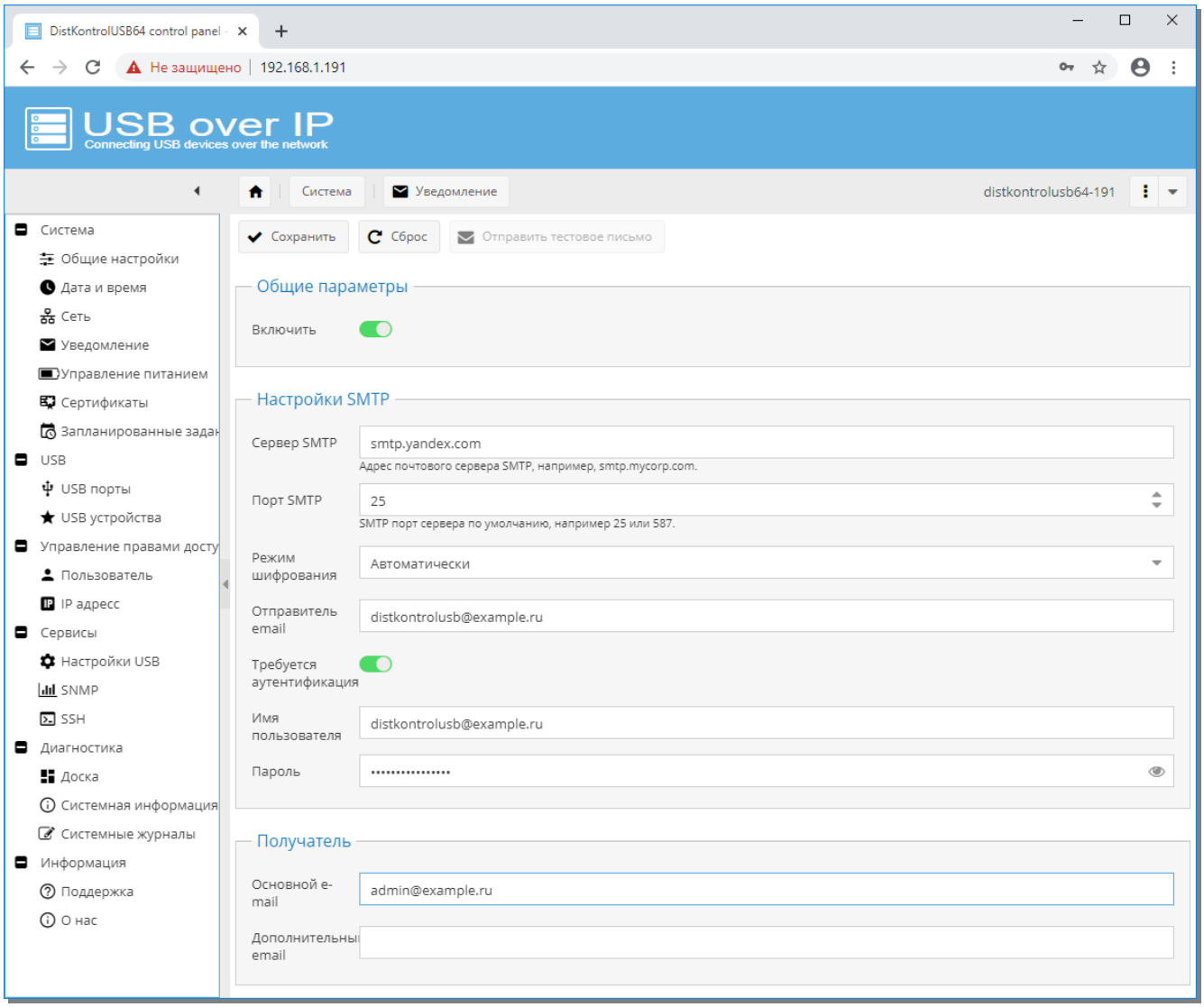
Если необходимо закрыть доступ только одному IP адресу в локальной сети, то во всех правилах поменять на противоположное «Действие»

ВНИМАНИЕ!!! Внимательно настраивайте правила, не закройте доступ к WEB интерфейсу концентратора (для восстановления контроля над ним потребуется сброс настроек, управляемого USB over IP концентратора в исходное состояние)

При настройке рекомендуется временно разрешить для определенного IP и закрыть для всех, например, 22 или 6565 порт на устройстве, и только убедившись в корректном вводе правил, уже порт 80.

4.2.4 УВЕДОМЛЕНИЕ

При необходимости, можно включить отправку уведомлений на электронную почту. Настройка системы уведомлений осуществляется на странице веб интерфейса концентратора Система-Уведомления



Уведомления о действиях пользователей высылаются на почтовые адреса, указанные в их профиле. Уведомление о назначенных заданиях – на адрес, указанный в профиле пользователя usbcontrol.

Отправка уведомлений осуществляется:

- При успешном входе в веб интерфейс управления концентратора
- При неправильном вводе логина или пароля для входа в веб интерфейс управления концентратора
- При блокировке входа в веб интерфейс управления концентратора
- Служебная информация о состоянии концентратора

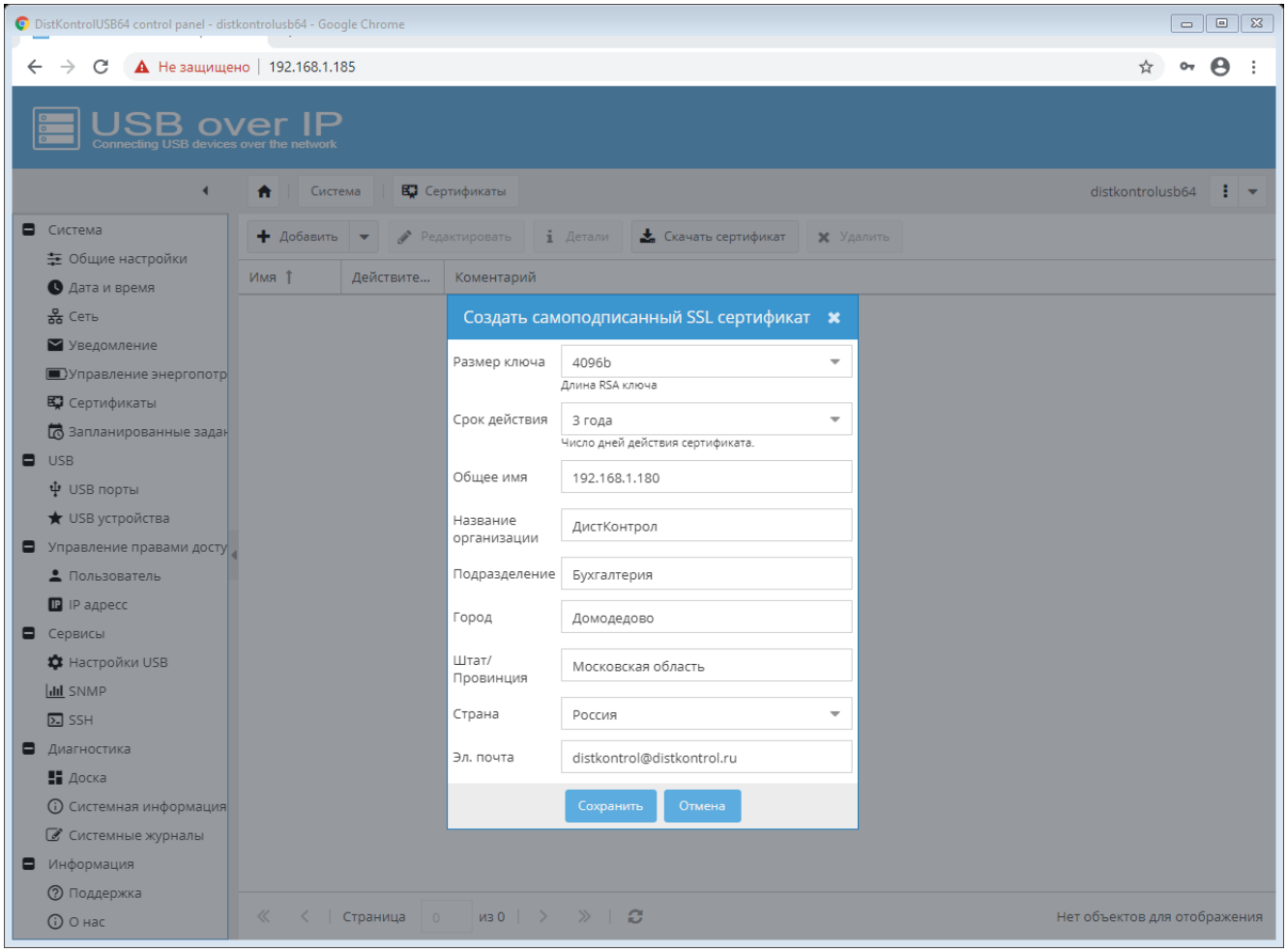
Веб интерфейс управления концентратора имеет защиту от перебора паролей для входа. При пятикратном не правильном вводе пароля или имени пользователя осуществляется блокировка входа в интерфейс управления на 3 мин. Далее блокировка на 3 мин при каждом не правильном вводе учетных данных, до правильного ввода. При блокировке входа высылается уведомление на основной e-mail, если включено и настроено уведомление.

4.2.5 УПРАВЛЕНИЕ ЭНЕРГОПОТРЕБЛЕНИЕМ

В данном разделе можно настроить задачу на перезагрузку и выключения концентратора.

4.2.6 СЕРТИФИКАТЫ

Управляемый USB over IP концентратор поддерживает импорт и создание самоподписанных сертификатов SSL/SSH. Управление сертификатами осуществляется на странице «Сертификаты».



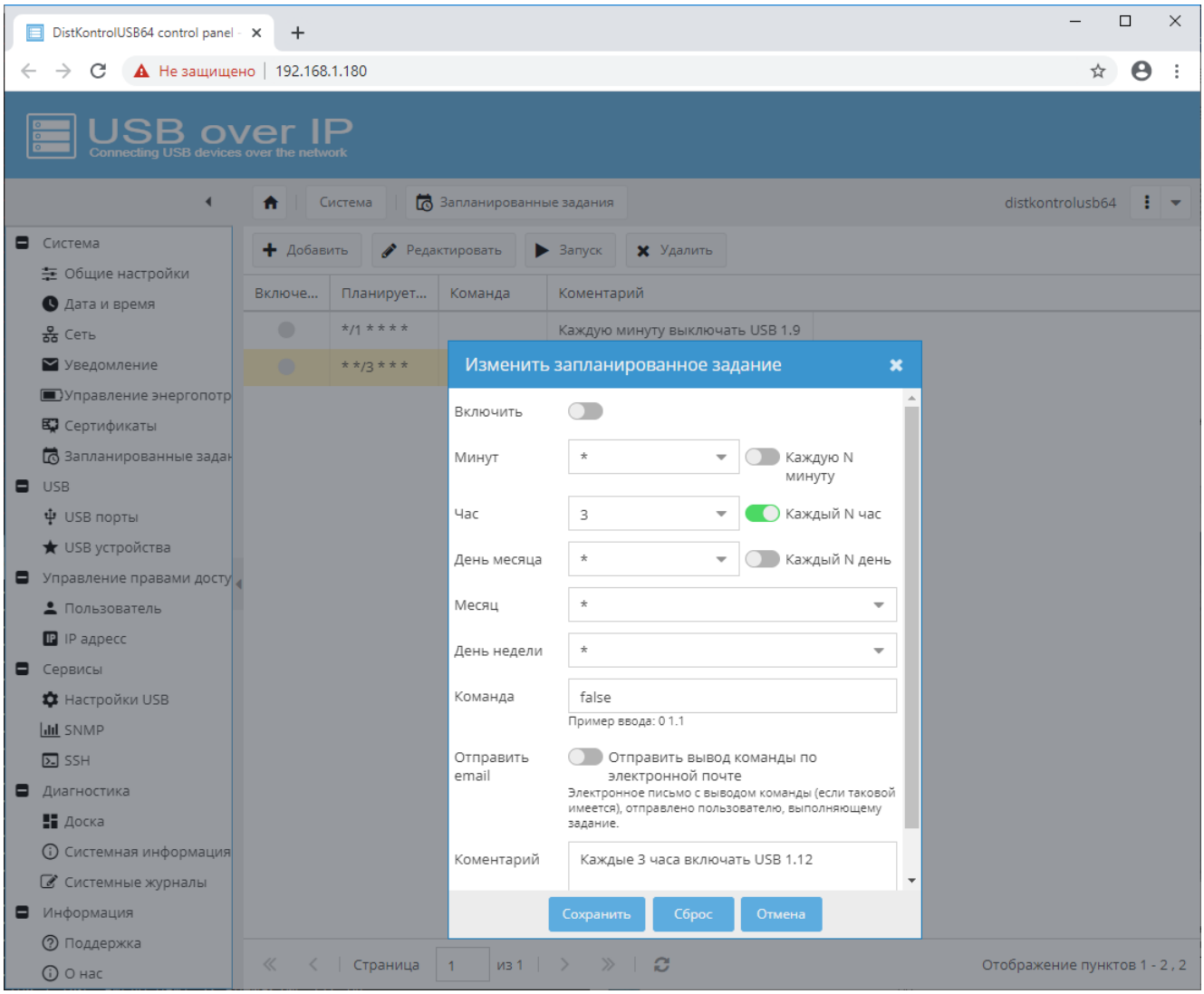
Безопасное соединение для WEB интерфейса можно включить на странице «Общие настройки». Там же можно включить принудительное использование только безопасного соединения для доступа к WEB интерфейсу управляемого USB over IP концентратора.

Порядок создания и использования сертификатов для шифрования трафика от USB устройств подробно описан в разделе «Параметры клиентского приложения»

Брандмауэр управляемого USB over IP концентратора позволяет обеспечить дополнительную безопасность использования DistKontrolUSB в сети и гибко настроить доступ к нему

> **Примечание**: устройство должно корректно получать время по NTP (Система - Дата и время)

4.2.7 ЗАПЛАНИРОВАННЫЕ ЗАДАНИЯ



Для создания задания управления USB входами необходимо на странице «Запланированные задания» нажать кнопку «Добавить» заполнить поля задания и нажать кнопку «Сохранить». Созданные задания можно отключать, и они не будут выполняться.

Команда состоит из:

- Команда – usbcontrolapi;
- Признака включения «1» или выключения «0» порта;
- Номера USB порта (от 1.1 до 4.16)

Так же возможно перечисление нескольких портов и/или указания группы портов:

"0.0" - от 1.1 до 4.16;
"1.0" - от 1.1 до 1.16;
"2.0" - от 2.1 до 2.16;
"3.0" - от 3.1 до 3.16;
"4.0" - от 4.1 до 4.16.

Примеры команд:

```
usbcontrolapi 0 1.9          (Выключить USB 1.9)
usbcontrolapi 1 1.12         (Включить USB 1.12)
usbcontrolapi 1 0.0          (Включить USB с 1.1 по 4.16)
usbcontrolapi 1 2.0,3.0      (Включить USB с 2.1 по 3.16)
usbcontrolapi 0 1.0,2.1,2.5,3.8,4.0  (Выключить USB с 1.1 по 1.16, 2.1, 2.5, 3.8, с 4.1 по 4.16)
```

По умолчанию 2 примера созданы, но выключены.

В настройках заданий можно включить отправку уведомлений о результате их выполнения на электронную почту. Задания выполняются от имени пользователя usbcontrol, уведомления будут отправляться на электронную почту, указанную в настройках данного пользователя.

Для создания задания управления перезагрузкой и выключением управляемого USB over IP концентратора необходимо на странице «Управление энергопотреблением» - «Запланированные задания» нажать кнопку «Добавить» заполнить поля задания и нажать кнопку «Сохранить». Созданные задания можно отключать, и они не будут выполняться.

Доступные задания:

1. Перезагрузка управляемого USB over IP концентратора;
2. Выключение управляемого USB over IP концентратора.

В качестве планировщика задач в устройстве используется cron.

Можно дополнительно ознакомиться с ним и crontab, если необходимо более полное понимание работы планировщика.

Формат команд:

.---------------- минута (0 - 59)

| .--------------- час (0 - 23)

| | .------------ день месяца (1 - 31)

| | | .---------- месяц (1 - 12) ИЛИ jan, feb, mar ...

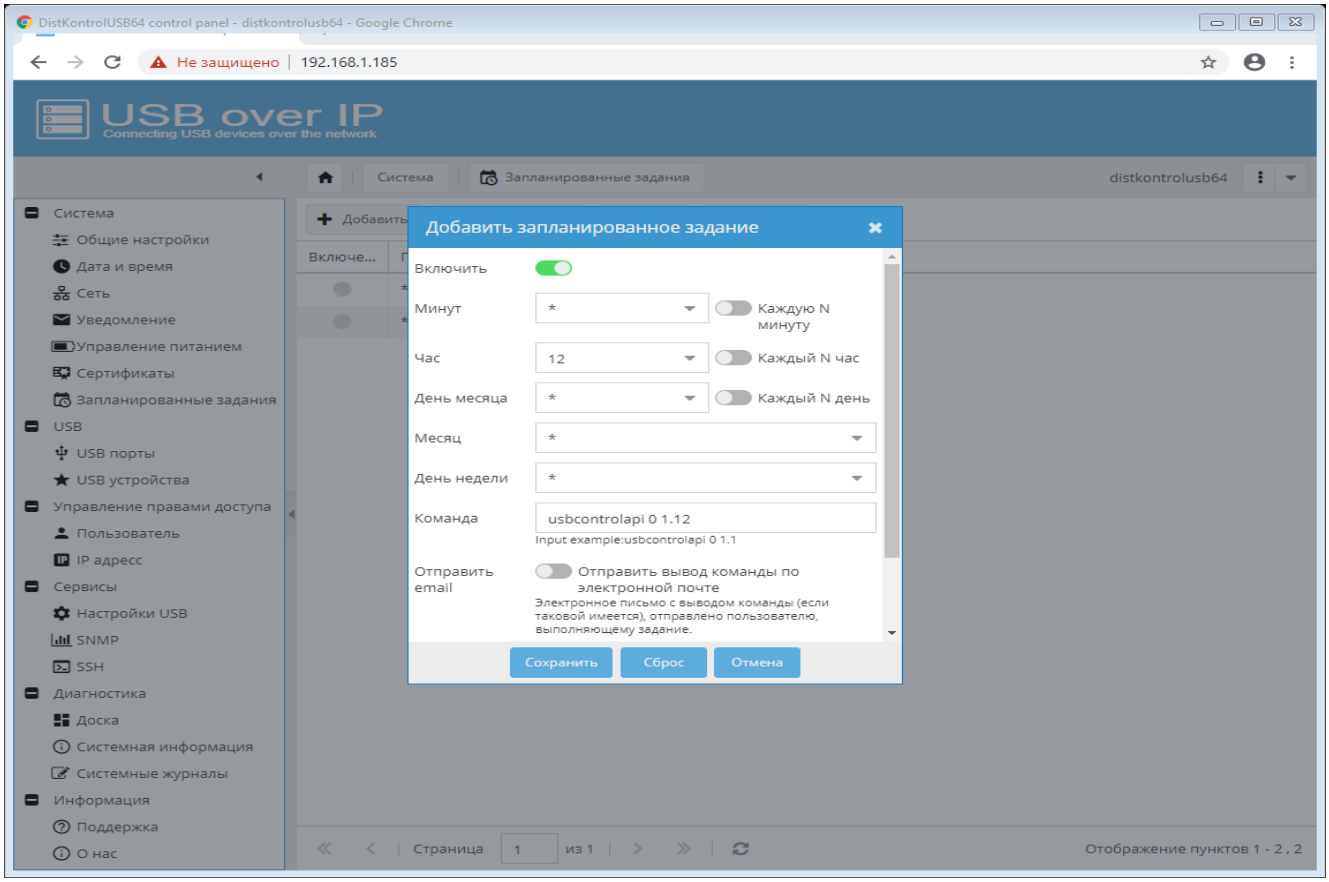
| | | | .-------- день недели (0 - 6) (Воскресенье=0 или 7)

| | | | | * * * * * команда для выполнения

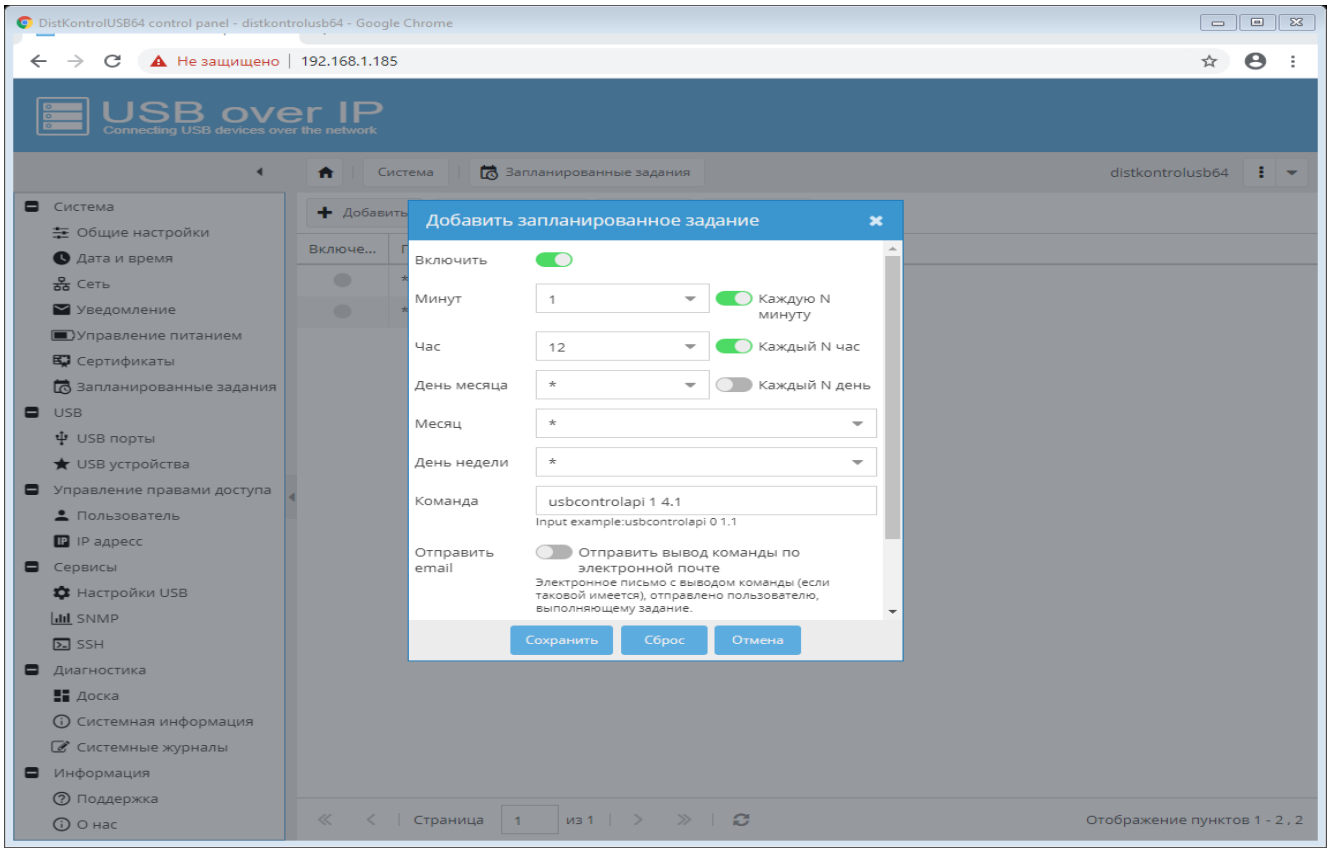
Например, запланировать задание на определенное время (чтобы команда 0 1.12 выполнялась в 7:00ч. 26

> **Примечание**: устройство должно корректно получать время по NTP (Система - Дата и время)

Создаем задание:



В столбце «Планируется» будет: * 7 * * *

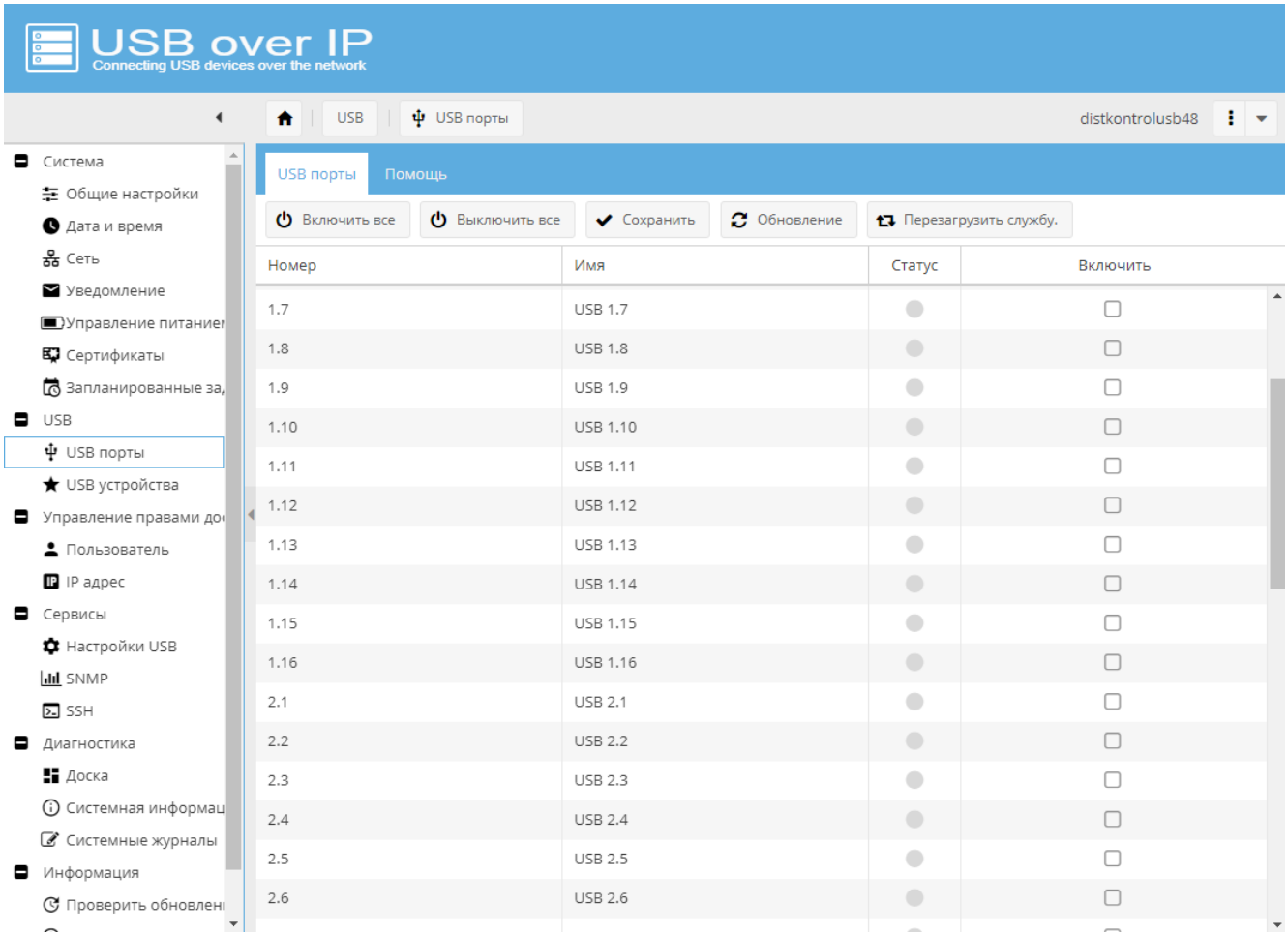


Пример повторения задания через 12:01 ч
В столбце «Планируется» будет: */1 */12 * *

4.3 USB

4.3.1 USB ПОРТЫ

Возможно изменение наименования порта USB. Включение и выключение USB портов управляемого USB over IP концентратора осуществляется кликом по соответствующей кнопке устройства.



Кнопки "Включить все", "Выключить все" управляют всеми доступными портами. Столбец "Имя" для обозначения имен USB портов.

Если "Отображаемое имя" = "DEFAULT" или "default" или "0" сбросит имя по умолчанию.

Для применения изменений, необходимо нажать на кнопку "Сохранить".

Для того, чтобы увидеть внесенные изменения в клиентских приложениях,, необходимо нажать на кнопку "Перезагрузить службу". Служба будет перезапущена.

3.3.2 USB УСТРОЙСТВА

Данный раздел необходим для настройки прав доступа, более подробно см. «Настройки доступа»

По умолчанию добавлено 2 USB устройства для примера. Устройства можно добавлять, редактировать, удалять. Добавление ручное и Автопоиск по подключенным USB устройствам к управляемому USB over IP концентратору. У устройства должен быть уникален один из параметров: Vendor ID, Product ID или Serial №. Рекомендуется добавлять устройства через Автопоиск.

В столбце «Пользователи» указаны пользователи, которым назначены права на данное устройство.

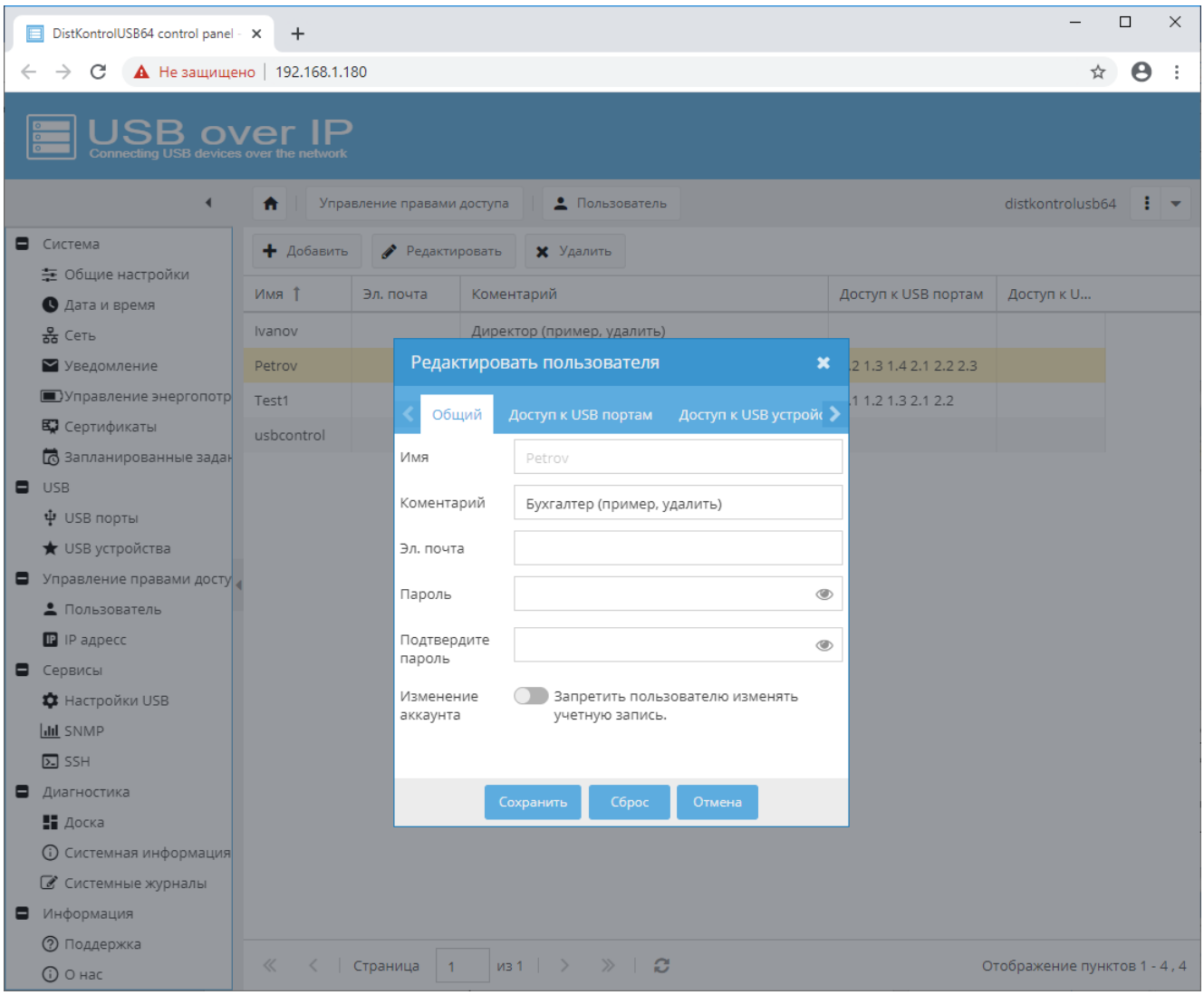
Внимание!!! Некоторые USB устройства могут работать некорректно. В этом случае они будут пропускаться при автопоиске. Возможно некорректное отображение списка поиска. Отключите и повторно включите питание USB порта и повторите поиск устройств.

4.4 УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА

4.4.1 ПОЛЬЗОВАТЕЛЬ

Для ограниченного предоставления прав на включение и отключение USB устройств необходимо на странице «Управление правами доступа» - «Пользователь» создать пользователей управляемого USB over IP концентратора.

ВНИМАНИЕ!!! Имя пользователя может быть введено только на латинской раскладке. Регистр имеет значение!



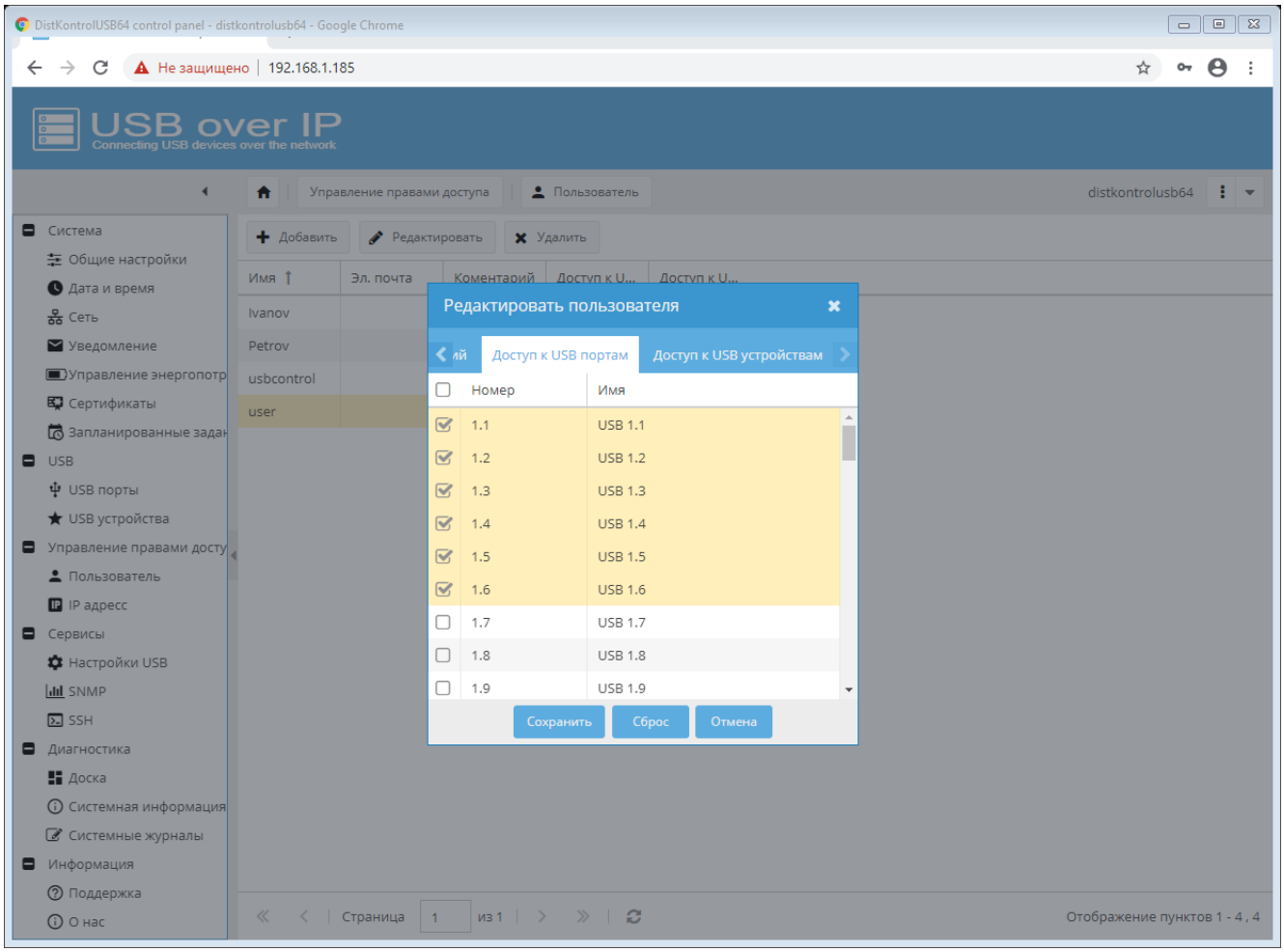
В исходном состоянии на устройстве созданы демонстрационные пользователи (рекомендуется их удалить до начала использования устройства) и пользователь – usbcontrol (рекомендуется поменять пароль, но не удалять пользователя).

Пользователь usbcontrol необходим для поддержания сервисной функции включения и выключения USB портов устройства с помощью утилиты usbcontrol и ssh.

ВНИМАНИЕ!!! При удалении пользователя usbcontrol будет недоступна возможность включать и выключать USB порты устройства с помощью утилиты usbcontrol и ssh. **Восстановление пользователя usbcontrol возможно только сбросом устройства к исходным установкам.**

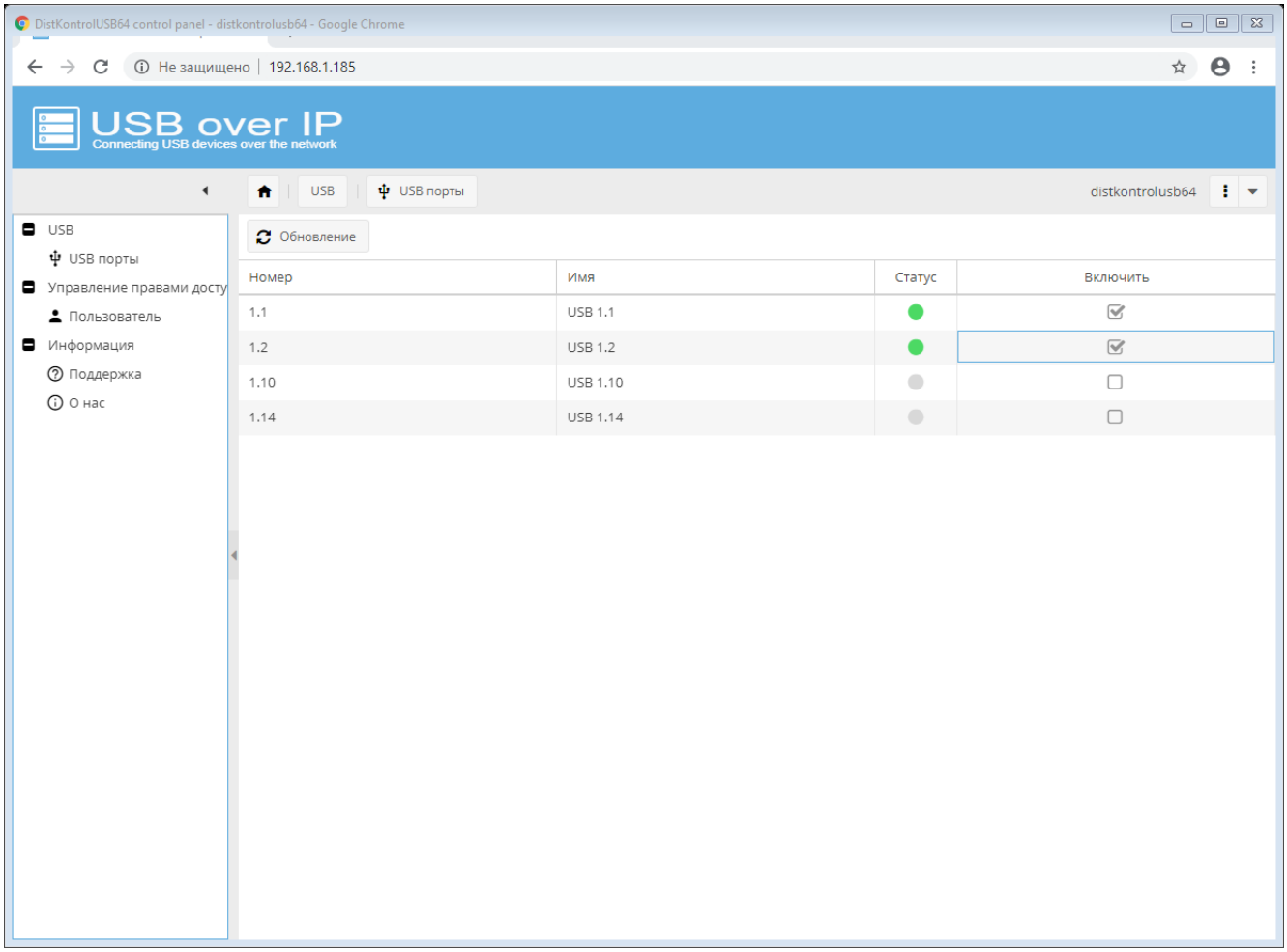
Устройство имеет ряд системных учетных записей создание с которыми одноименных пользователей невозможно. При попытке создания такого пользователя система выдаст соответствующее предупреждение.

При добавлении пользователей на вкладках «Доступ к USB портам» и «Доступ к USB устройствам» можно назначить им права на управление USB входами и права на возможность подключения к USB устройствами, USB портам. Подробнее см. раздел «Ограничение доступа к USB устройствам, USB портам». Редактирование прав и настроек пользователя возможно и после добавления.



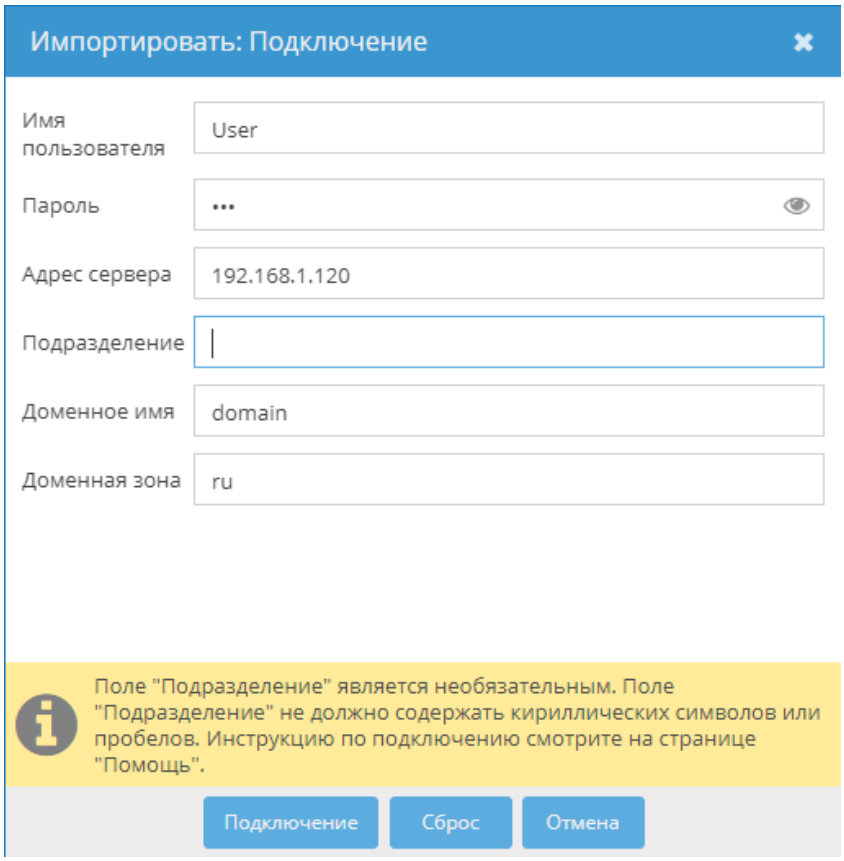
При входе в WEB интерфейс управляемого USB over IP концентратора под правами созданных пользователей им доступно только управление разрешенными входами (портами) USB, изменение пароля и адреса электронной почты для отправки уведомлений. Возможность изменения данных пользователя может быть отключена в настройках.

Для управления (включения и выключения) USB входов DistKontrolUSB пользователю доступны только назначенные входы и в WEB интерфейсе пользователя на странице «Пользователь» будут отображены только те входы, к которым пользователю предоставлены права на управление. См. раздел настройки ограничений доступа.


DistKontrolUSB64 control panel - distkontrolusb64 - Google Chrome
Не защищено | 192.168.1.185
USB over IP
Connecting USB devices over the network
USB
USB порты
distkontrolusb64
USB
USB порты
Управление правами досту
Пользователь
Информация
Поддержка
О нас
Обновление
Номер
Имя
Статус
Включить
1.1
USB 1.1
1.2
USB 1.2
1.10
USB 1.10
1.14
USB 1.14

Импорт пользователей из Active Directory (AD).

1.Подключение:



Введите корректные данные для подключения к вашему AD.

Имя пользователя - пользователь должен иметь доступ к получению списка пользователей.

Пароль - пароль пользователя в AD.

Адрес сервера - IP адрес сервера AD.

Подразделение - подразделение в AD из которой будут выгружены имена пользователей.

Поле "Подразделение" является необязательным.

Поле "Подразделение" не должно содержать кириллических символов или пробелов.

Доменное имя - имя домена вашей сети, например "myad".

Доменная зона - зона вашей сети, например "com" или "local".

Доменные имя и зона будут выглядеть как "myad.local".

Нажмите кнопку "Подключение" для перехода к следующему шагу.

Если вы ввели некорректные данные, вы получите соответствующее уведомление системы.

2.Выбор пользователей:

Выберите из списка тех пользователей, которых необходимо добавить.

Добавленные пользователи будут иметь случайные пароли.

У пользователей будут настройки по умолчанию.

Нажмите кнопку "Импортировать" для перехода к следующему шагу.

Применять настройки необходимо по завершению следующего шага.

3.Редактирование пользователей:

Нажмите на кнопку "Обновление" для получения актуального списка пользователей.

Отредактируйте всех добавленных пользователей.

Задайте корректный пароль.

Назначьте необходимые права.

Примените настройки.

(Желтое всплывающее окно в верхней части экрана.)

4.4.2 IP АДРЕС

Данный раздел необходим для настройки прав доступа, более подробно см. «Настройки доступа»

По умолчанию добавлено 2 IP адреса для примера. IP можно добавлять, редактировать, удалять. При создании, редактировании устройства выберите семейство IP (IPv4 или IPv6)

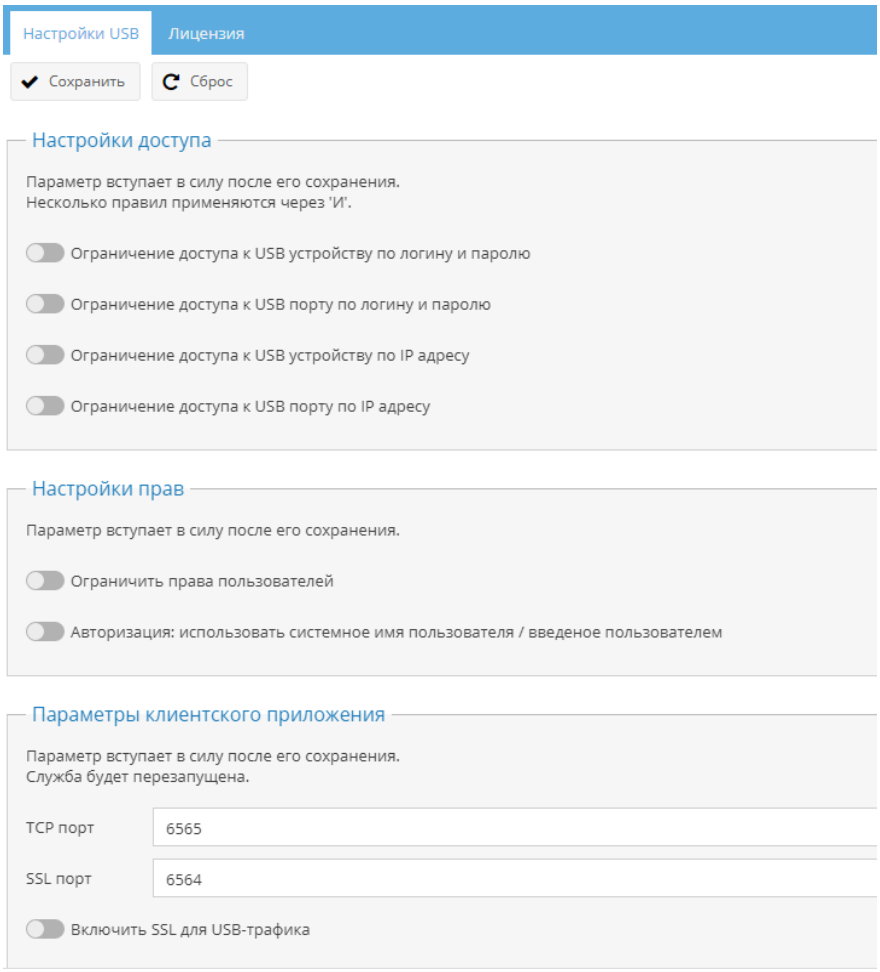
4.5 СЕРВИСЫ

4.5.1 НАСТРОЙКИ USB

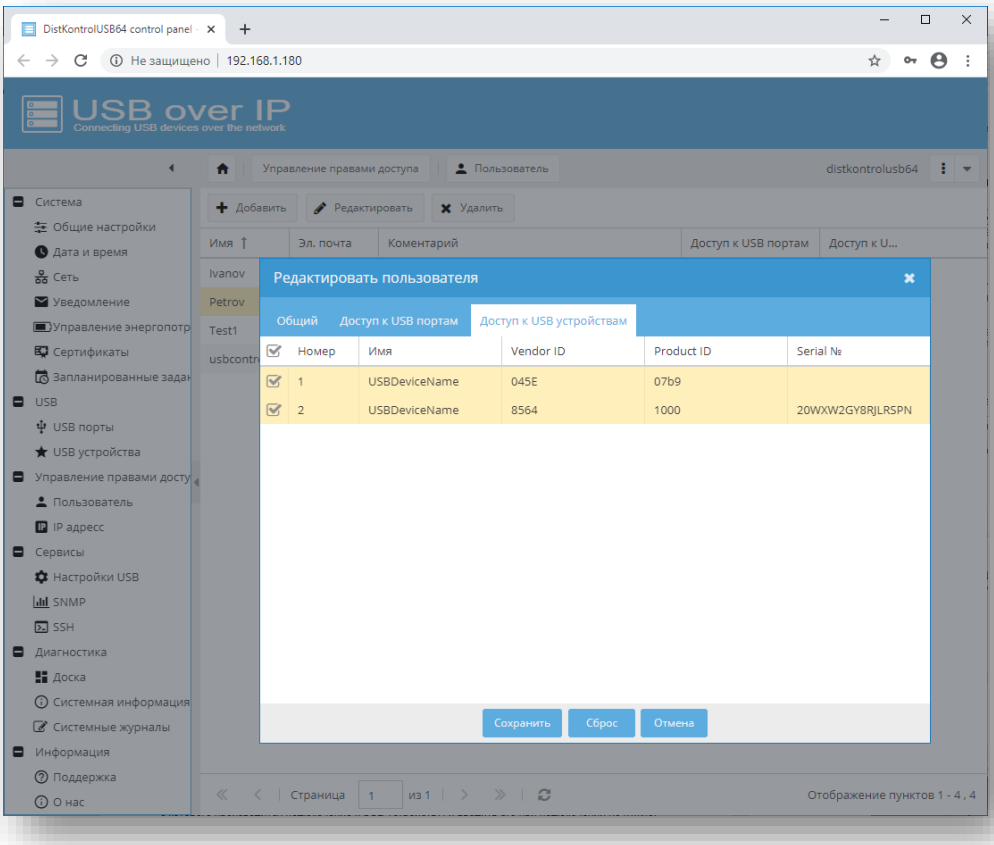
4.5.1.1 НАСТРОЙКИ ДОСТУПА

В управляемом USB over IP концентраторе реализована возможность ограничения доступа пользователей к подключаемым USB устройствам и портам (авторизация для доступа к USB устройствам и/или портам). Предусмотрены четыре способа ограничения:

1. Ограничение доступа к USB устройству по логину и паролю (авторизация по логину и паролю для доступа к USB устройству);
2. Ограничение доступа к USB порту по логину и паролю (авторизация по логину и паролю для доступа к USB порту);
3. Ограничение доступа к USB устройству по IP адресу (авторизация по IP адресу).
4. Ограничение доступа к USB порту по IP адресу (авторизация по IP адресу для доступа к USB порту).



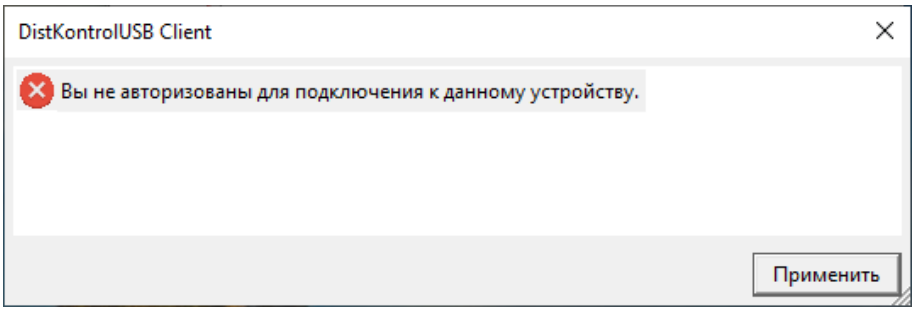
Режимы ограничения включаются на странице WEB интерфейса странице «Управление правами доступа» - «Права доступа». По умолчанию все способы авторизации отключены. Для включения ограничения доступа пользователей к подключаемым USB устройствам необходимо нажать соответствующую кнопку интерфейса.



Режимы ограничения доступа пользователей к USB устройствам (авторизация для доступа к USB устройствам) могут использоваться как независимо друг от друга, так и совместно в целях повышения безопасности использования USB устройств

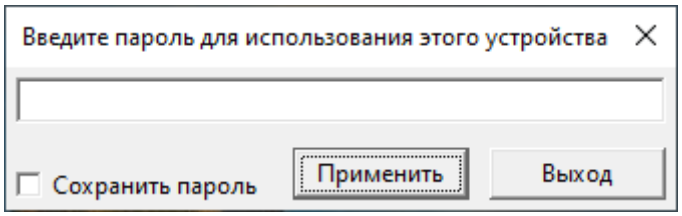
ВНИМАНИЕ!!! При совместном использовании правила применяются через «И». Для предоставления доступа к устройству должны будут выполняться все включенные правила. Настройку правил доступа рекомендуется выполнять по одному правилу, после чего включать совместные режимы ограничения.

При попытке подключения USB устройства, в отсутствии на это прав, пользователю будет выведено соответствующее сообщение:



4.5.1.1.1 ОГРАНИЧЕНИЕ ДОСТУПА К USB УСТРОЙСТВУ ПО ЛОГИНУ И ПАРОЛЮ

При включенном ограничении доступа к USB устройству по логину и паролю – при подключении к USB устройству, пользователю будет предложено ввести пароль для доступа к устройству USB (не порту управляемого USB over IP концентратора, а именно USB устройству, не зависимо от того в какой порт оно подключено). Логин при подключении используется системный (имя текущего пользователя компьютера, с которого производится подключение к USB устройству) и вводить его при подключении не нужно.

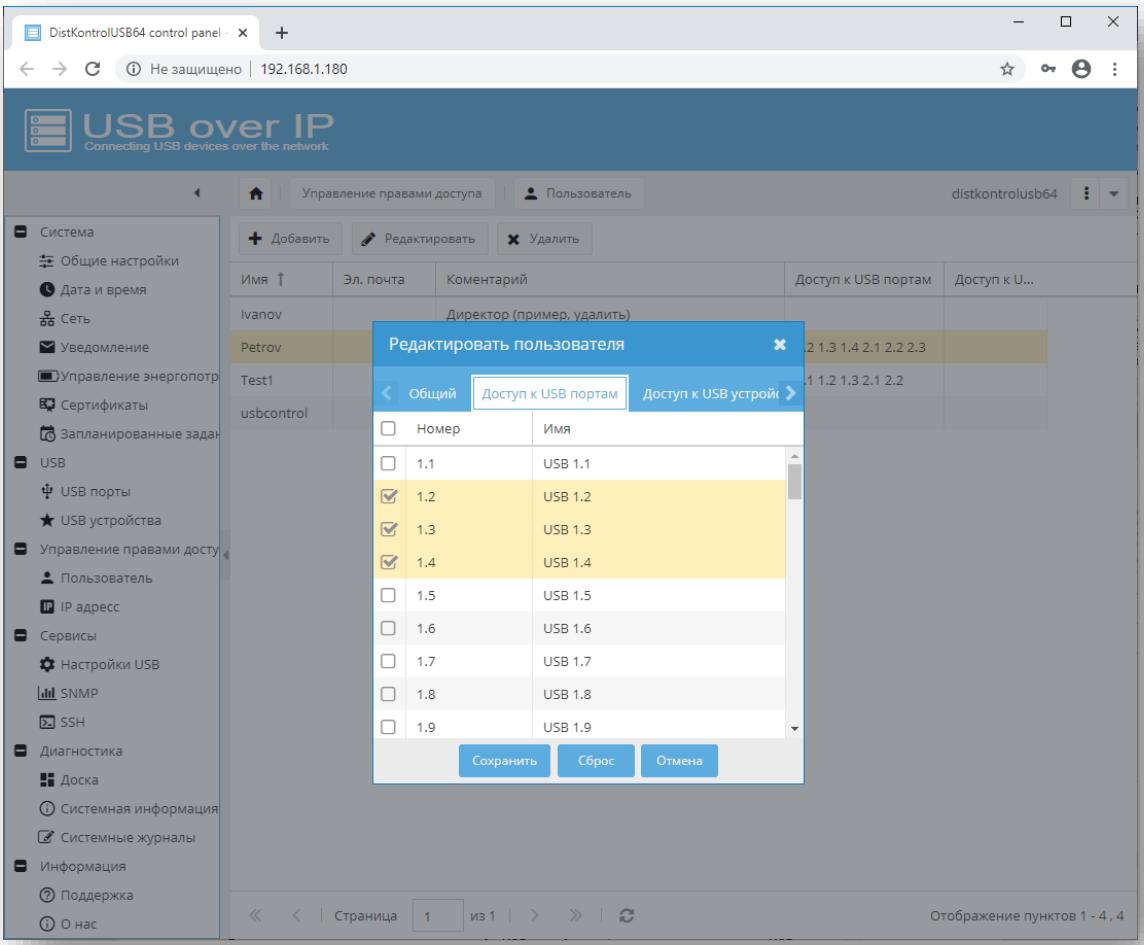


При правильном вводе пароля устройство USB будет подключено к компьютеру пользователя и до перезапуска клиента ввод пароля больше не потребуется даже при отключении и повторном подключении к устройству.

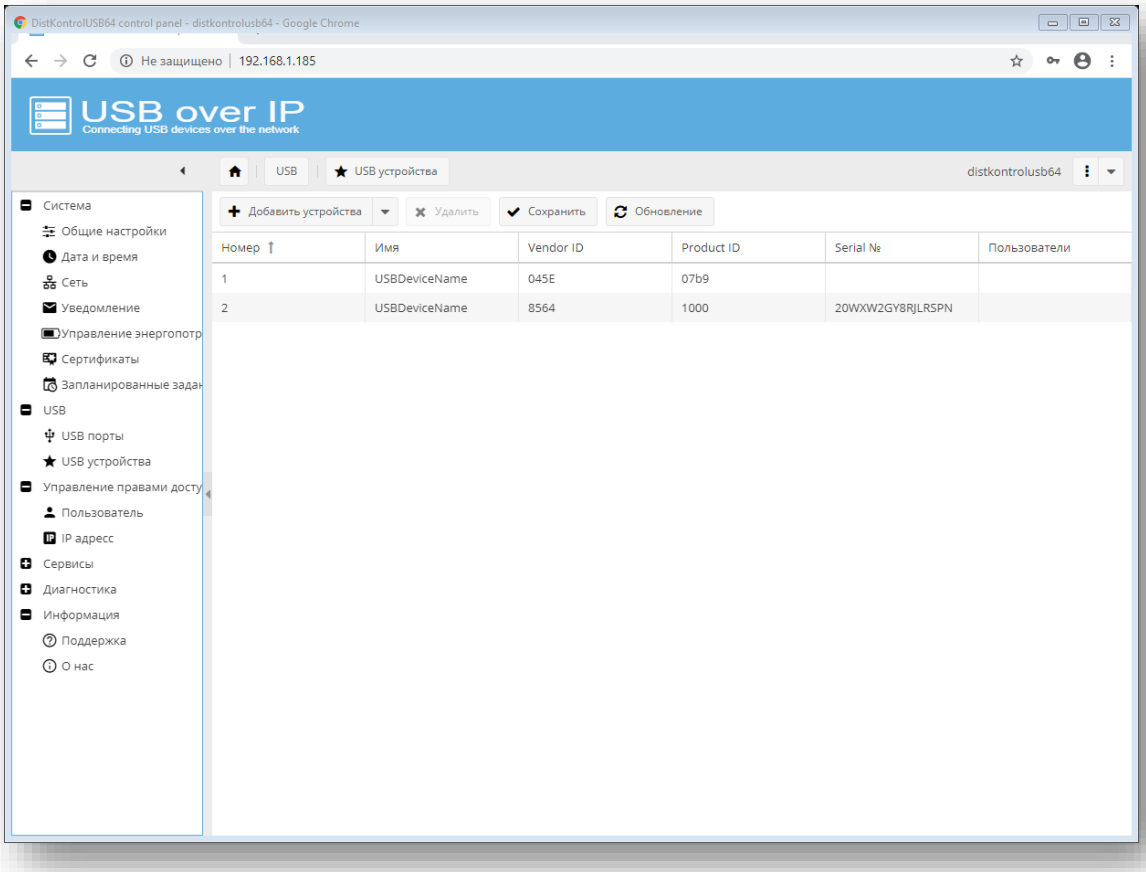
При подключении к USB устройству (порту), при запросе пароля, можно выбрать «Save Password», пароль пользователя будет сохранен и при последующих запусках приложения его ввод не потребуется. В случае, если пароль пользователя будет изменен, то необходимо вначале удалить запомненный пароль из файла настроек пользователя, и при следующем запросе пароля – ввести новый. Для удаления запомненного пароля необходимо закрыть приложение (не свернуть, что является действием по умолчанию при нажатии на крестик в правом верхнем углу интерфейса программы). Внести изменения в файл настроек клиентского приложения см. п. «Настройка клиентского приложения, управляемого USB over IP концентратора» (можно просто удалить файл настроек, для сброса всех настроек клиентского приложения к исходным).

Для настройки режима ограничения доступа к USB устройству по логину и паролю необходимо:

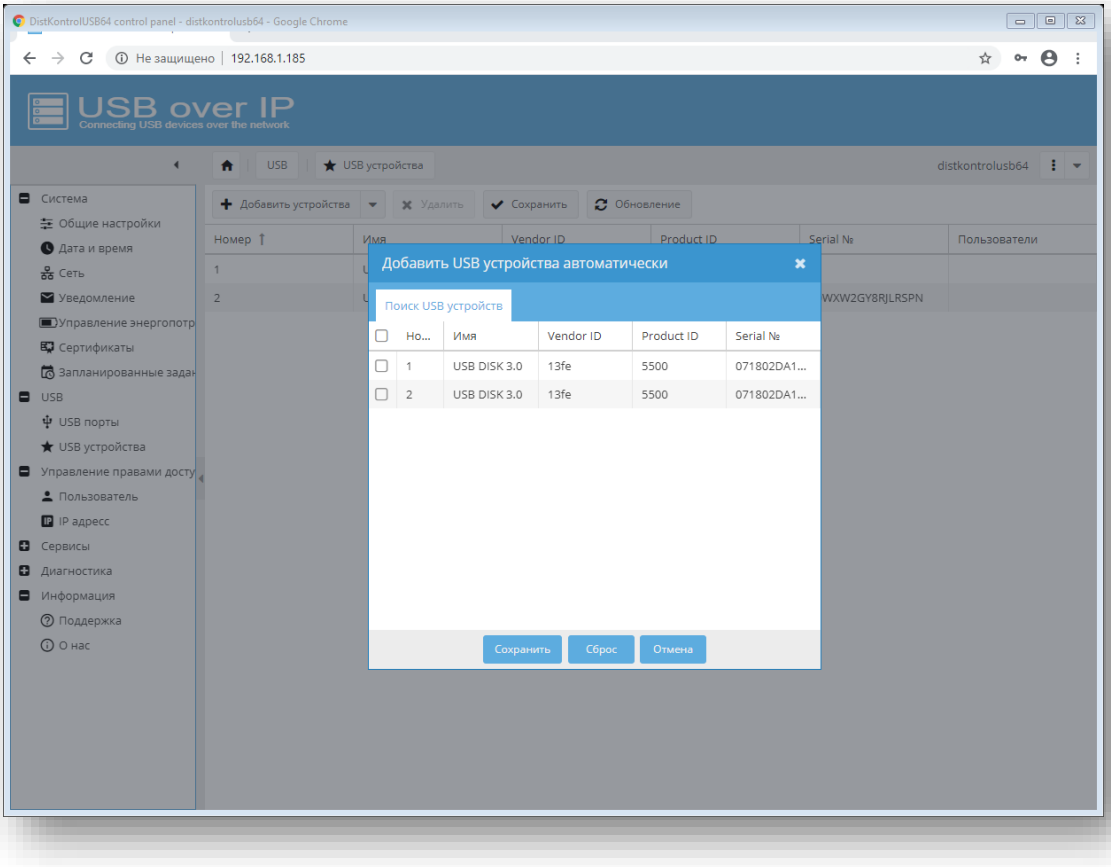
1. На странице WEB интерфейса администратора «Сервисы» - «USB устройства» добавить ВСЕ USB устройства, которые будут использоваться. Устройство работает по принципу: «Запрещено все, что явно не разрешено»



USB устройства можно добавить:



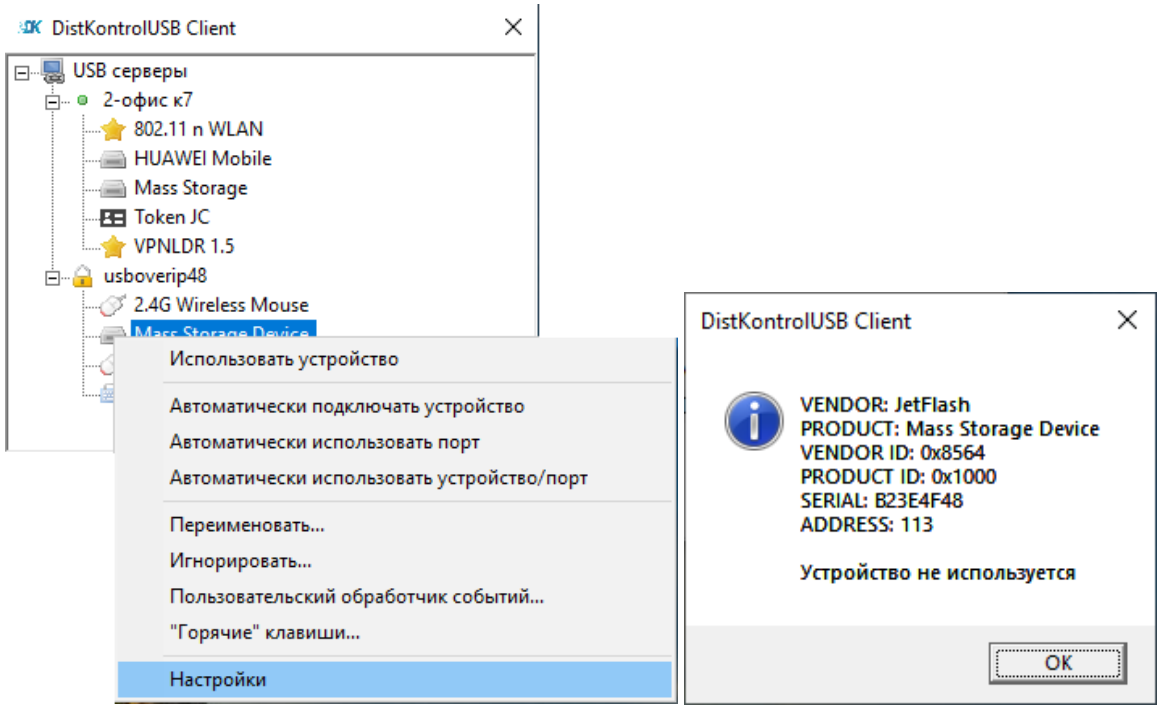
- 1. Из автоматически генерируемого списка подключенных к концентратору USB устройств (включенных на странице «USB входы»). «Добавить устройства» - «Автопоиск». В списке выбрать добавляемые USB устройства и нажать кнопку «Сохранить».



Будет выдан отчет о результате добавления USB устройств в список.

- 2. Вручную:

Для добавления USB устройств вручную, необходимо знать их VendorID, ProductID и Serial №. Их можно посмотреть в клиенте



или на странице WEB интерфейса администратора «Диагностика» - «Системные журналы» в стоке вида:

Sep 25 22:56:28 USBoverIP64: Authorizing parameters -> '8564' '1000' Ivanov (Ivanov)' '192.168.1.5' '05KVOF66TU4IHDTZ' "

VendorID - 8564

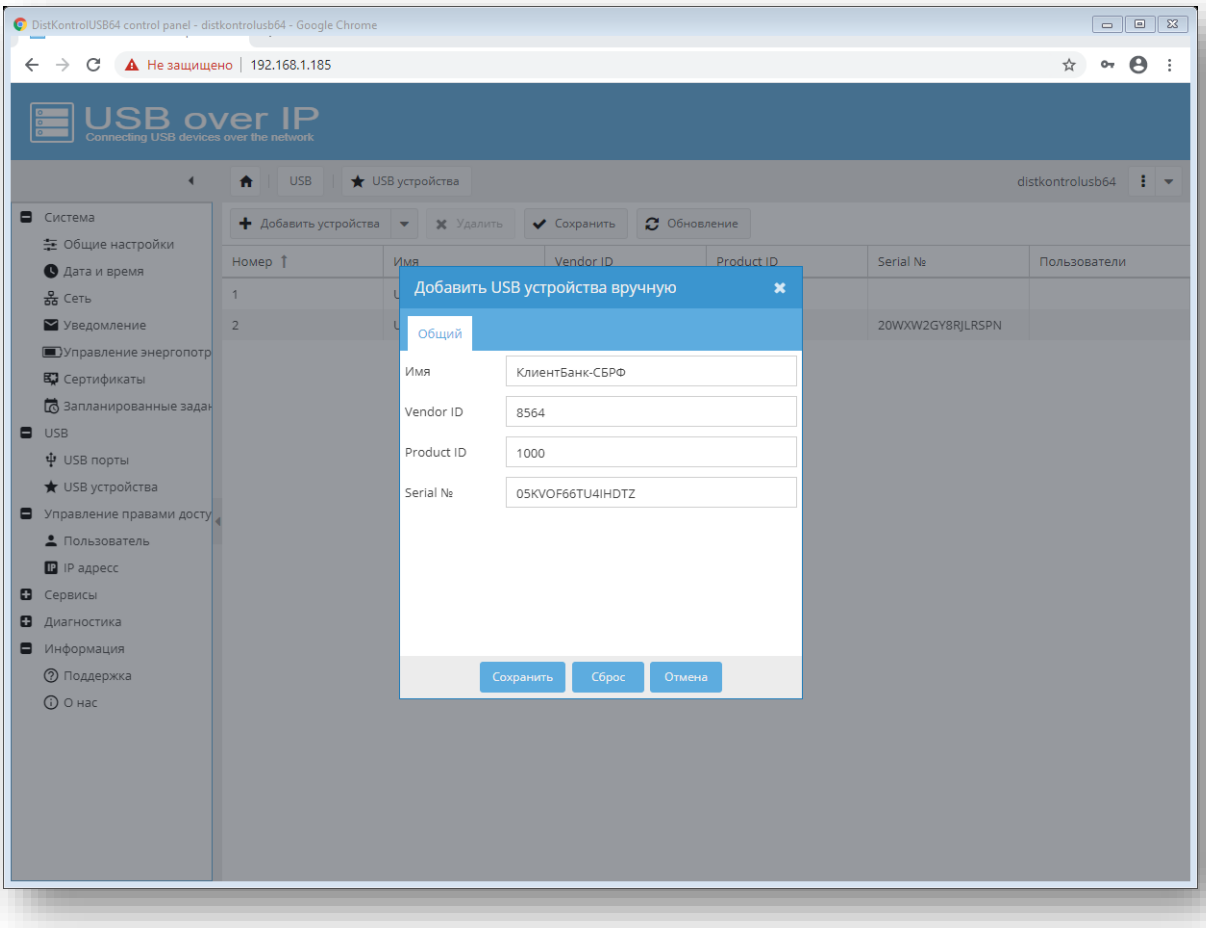
ProductID – 1000

Serial №. - '05KVOF66TU4IHDTZ'

VendorID и ProductID и Serial № должны содержать только цифры и латинские буквы.

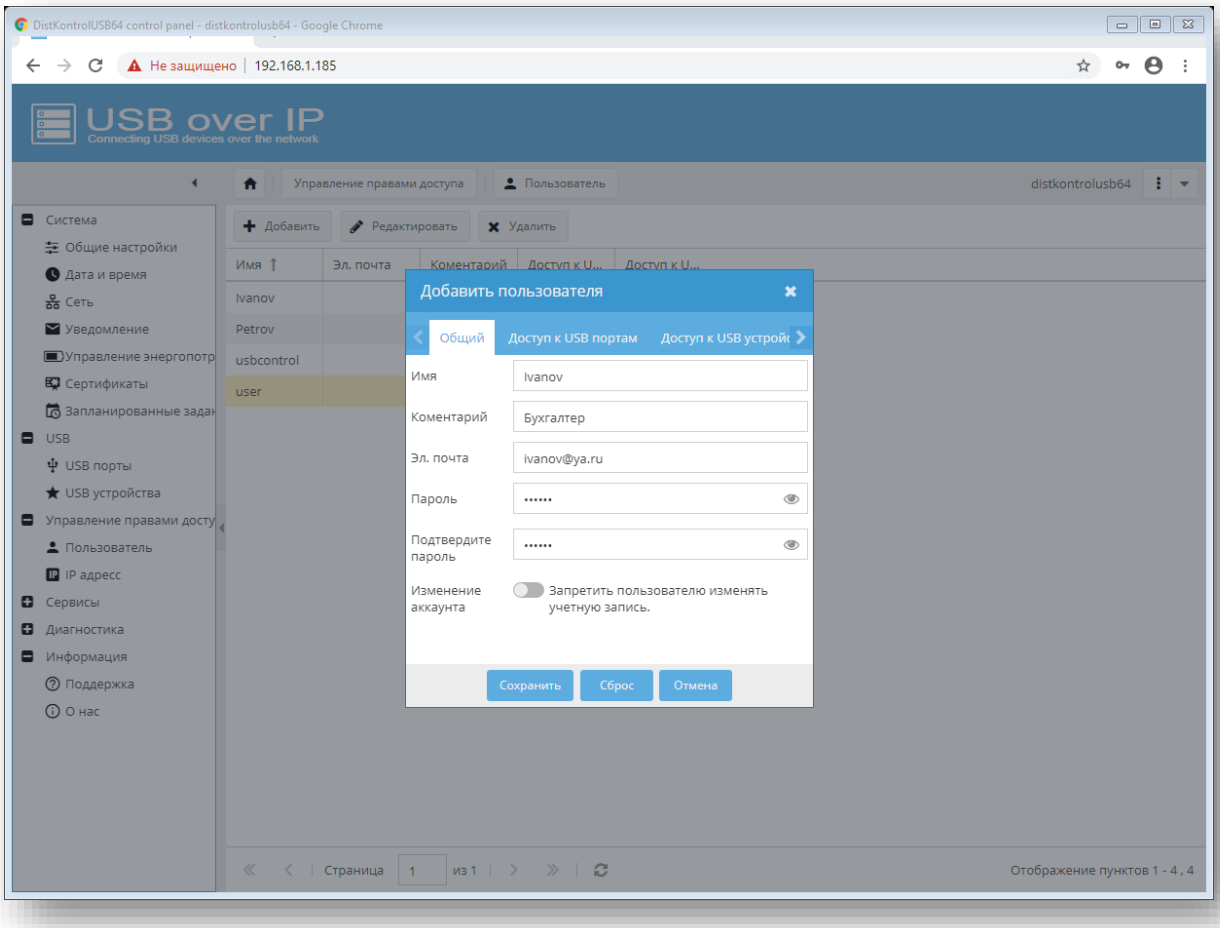
«Добавить устройства» - «Добавить вручную»

В дальнейшем возможно удаление и редактирование информации о USB устройстве:



В заводской настройке изделия созданы примеры ключей, которые можно удалить или отредактировать для использования DistKontrolUSB.

2. На странице «Управление правами доступа» - «Пользователь» добавить пользователей.

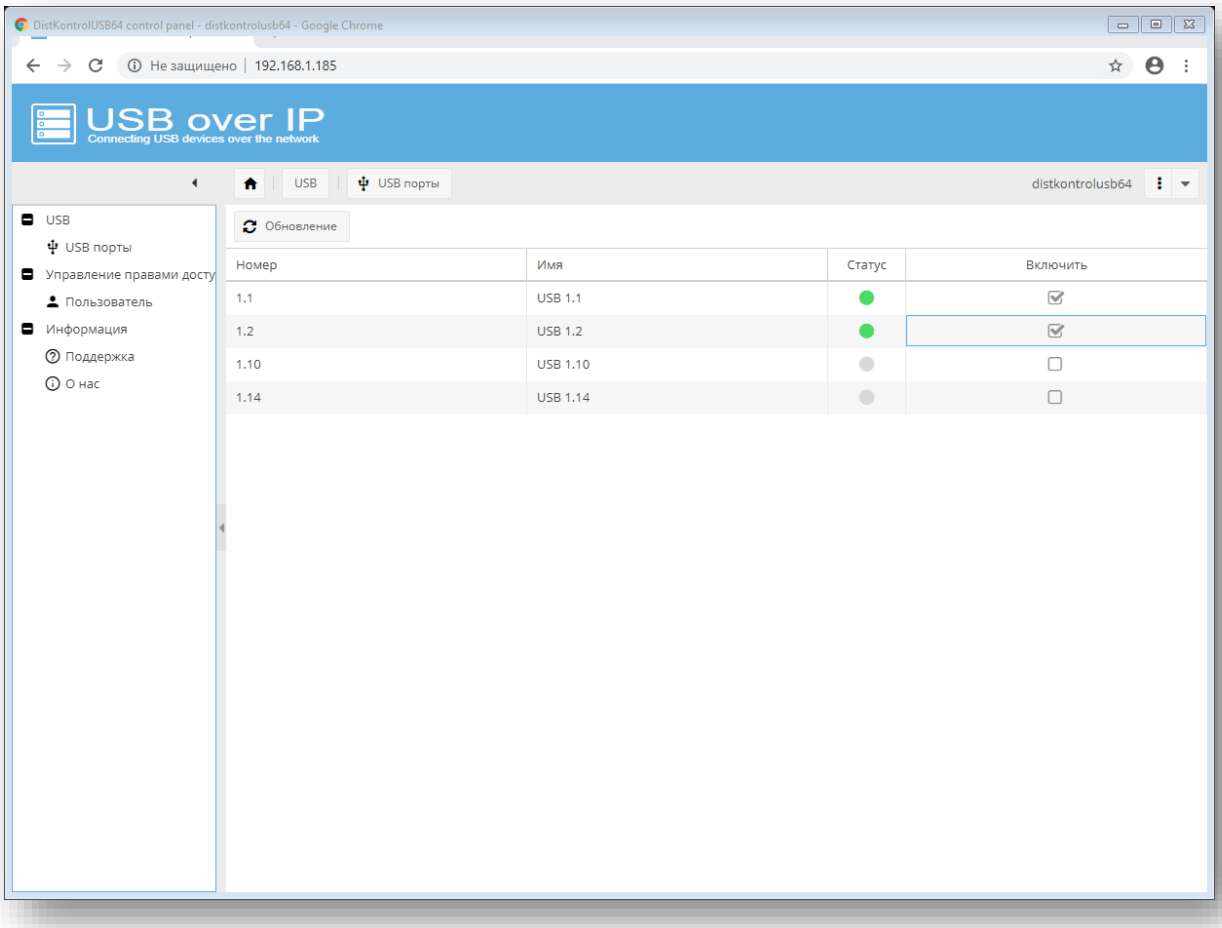


Имена пользователей должны СОВПАДАТЬ с системным именем пользователя (имя текущего пользователя компьютера, с которого производится подключение к USB устройству). При необходимости его так же можно посмотреть (после попытки подключения к USB устройству) в системном журнале. См. пример выше. Email и пароль пользователя – любые. Рекомендуется использовать сложные пароли.

3. На вкладках «Доступ к USB портам», «Доступ к USB устройству» назначить пользователю права доступа к USB портам и/или USB устройствам. Нажать кнопку «Сохранить» в диалоговом окне.

При назначении прав во вкладке «Доступ к USB портам», пользователю будет доступно управление питанием USB портами через WEB интерфейс и подключение USB устройств в выбранных портах. Если ни одного порта не назначено, пользователь получит соответствующие уведомление об отсутствии прав на управление портами.

При подключении USB устройств пользователю будут доступны для подключения только назначенные USB устройства и (или) USB устройства, подключенные к разрешенным портам. При попытке подключения USB устройств, не назначенных пользователю, в клиентском приложении будет выдаваться сообщение об отсутствии прав доступа к USB устройству.


DistKontrolUSB64 control panel - distkontrolusb64 - Google Chrome
Не защищено | 192.168.1.185
USB over IP
Connecting USB devices over the network
USB
USB порты
distkontrolusb64
USB
USB порты
Управление правами досту
Пользователь
Информация
Поддержка
О нас
Обновление
Номер
Имя
Статус
Включить
1.1
USB 1.1
1.2
USB 1.2
1.10
USB 1.10
1.14
USB 1.14

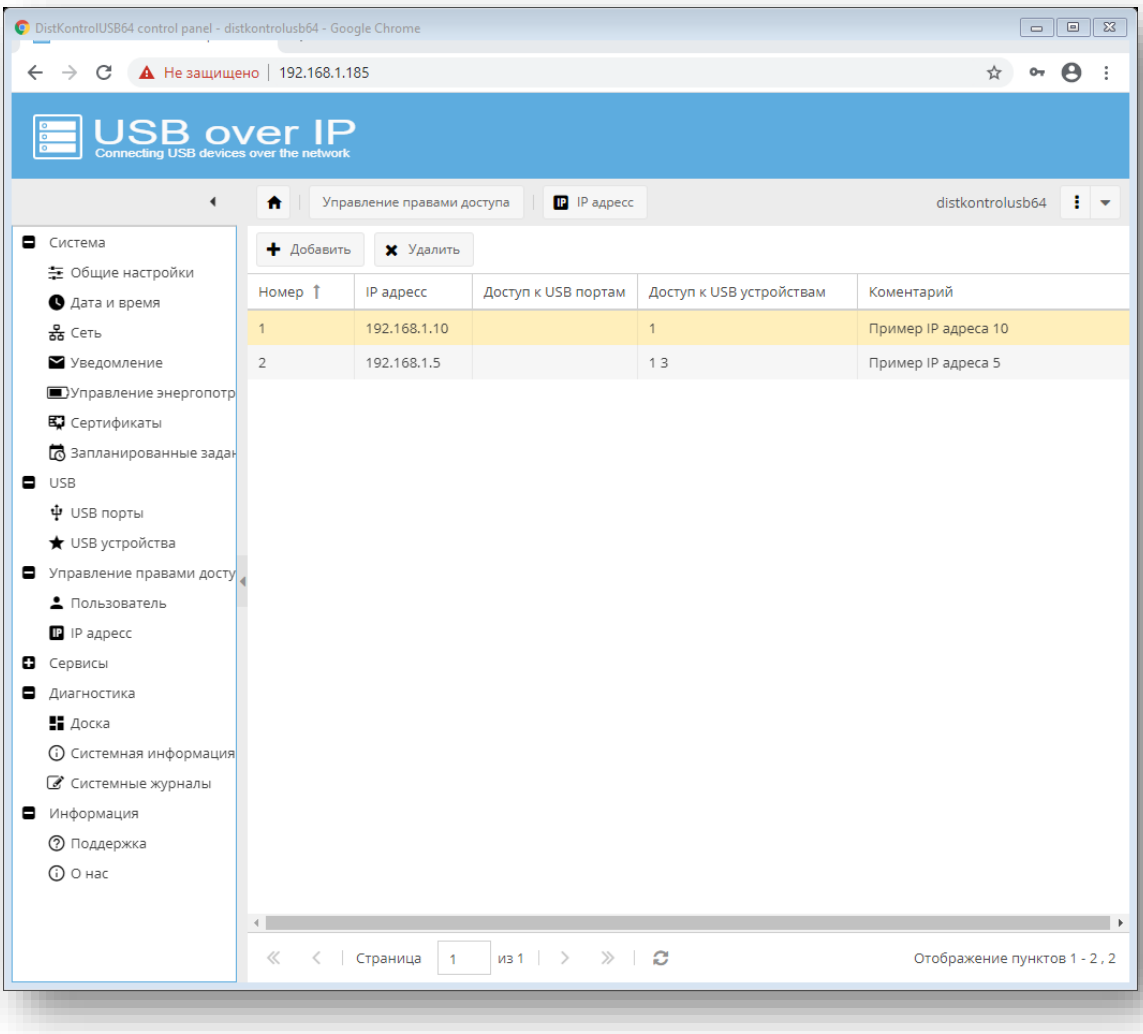
4.5.1.1.2 ОГРАНИЧЕНИЕ ДОСТУПА К USB ПОРТУ ПО ЛОГИНУ И ПАРОЛЮ

При включенном ограничении доступа к USB порту по логину и паролю – при подключении к USB устройству, пользователю будет предложено ввести пароль для доступа к устройству USB. Логин при подключении используется системный (имя текущего пользователя компьютера, с которого производится подключение к USB устройству) и вводить его при подключении не нужно. Не зависимо от того какое устройство USB подключено к порту, если пользователю разрешено использовать USB порт, ему будет предоставлен доступ к USB устройству.

Настройка прав доступа к порту подробно описана предыдущем параграфе

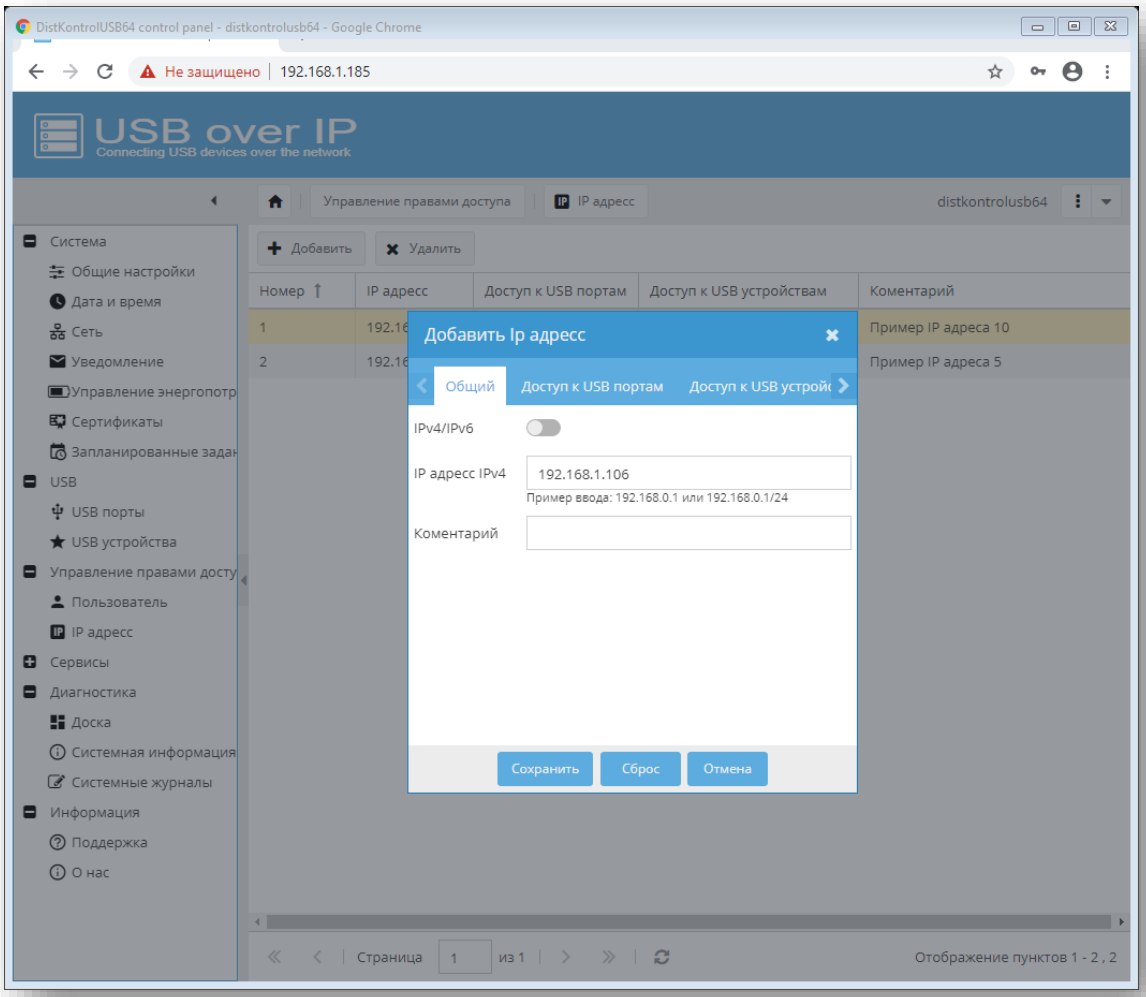
4.5.1.1.3 ОГРАНИЧЕНИЕ ДОСТУПА К USB УСТРОЙСТВУ ПО IP АДРЕСУ

При включенном ограничении доступа к USB устройству по IP адресу – подключение пользователем USB устройства будет возможно только с IP адреса с правом доступа к устройству USB (не порту управляемого USB over IP концентратора, а именно USB устройству, не зависимо от того в какой порт оно подключено).



Для настройки режима необходимо:

1. На странице WEB интерфейса администратора «Управление правами доступа» - «IP адреса» добавить **ВСЕ** IP адреса, которые будут использоваться. Устройство работает по принципу: «Запрещено все, что явно не разрешено».



Возможно добавление и удаление информации. При добавлении необходимо назначить все необходимые права во вкладках «Доступ к USB портам», «Доступ к USB устройству». Редактирование не возможно.

Для ввода доступны IP адреса формата 192.168.1.1. Если необходимо добавить формат IPv6, включите переключатель IPv4/IPv6.

4.5.1.1.4 ОГРАНИЧЕНИЕ ДОСТУПА К USB ПОРТУ ПО IP АДРЕСУ

При включенном ограничении доступа к USB порту по IP адресу – подключение пользователем USB устройства будет возможно только с IP адреса с правом доступа к порту USB (не USB устройству, а именно USB порту управляемого USB over IP концентратора, не зависимо от того какое USB устройство к нему подключено).

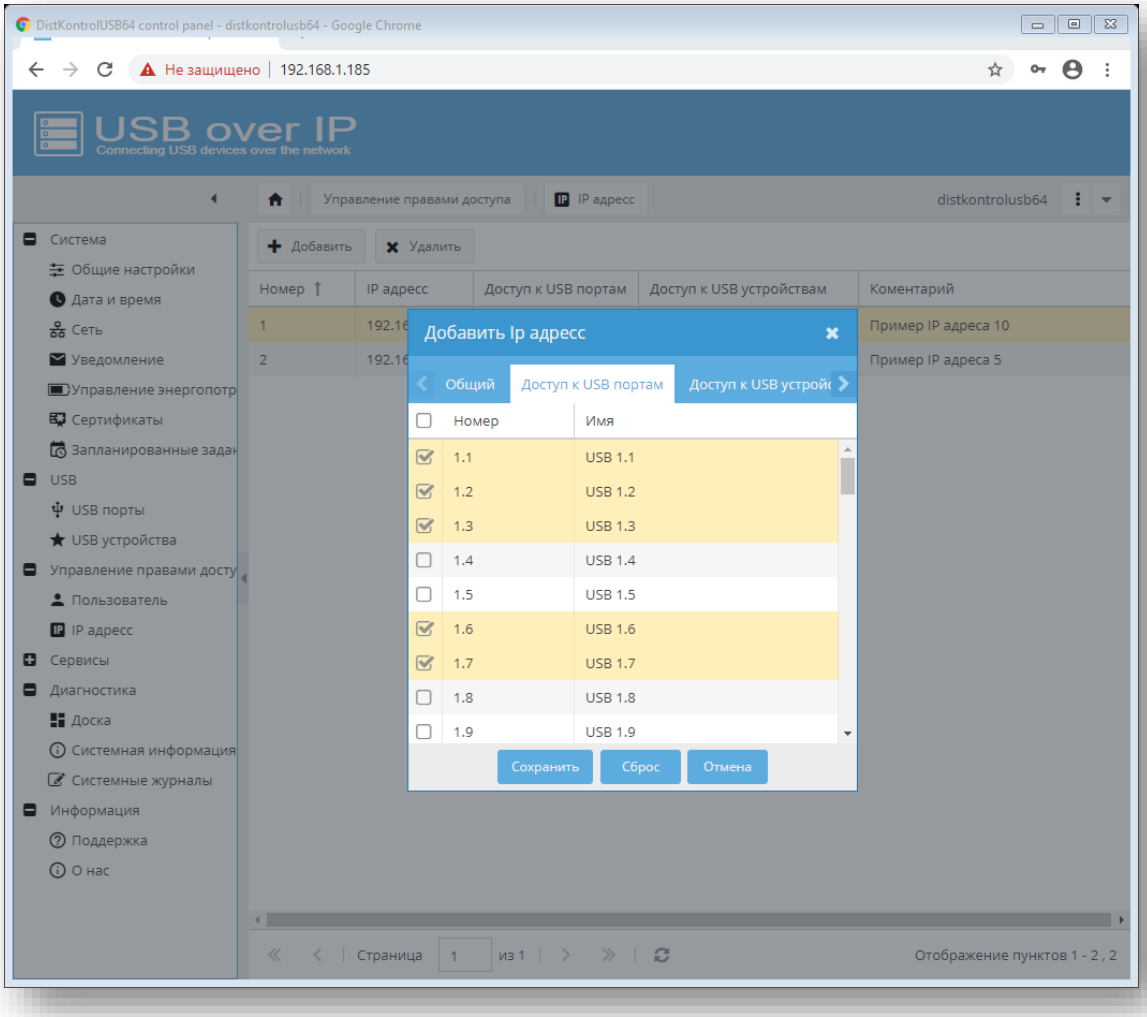
Для настройки режима необходимо:

1. На странице WEB интерфейса администратора «Управление правами доступа» - «IP адреса» добавить **ВСЕ** IP адреса, которые будут использоваться. Устройство работает по принципу: «Запрещено все, что явно не разрешено».

Возможно добавление и удаление информации. При добавлении необходимо назначить все необходимые права во вкладках «Доступ к USB портам», «Доступ к USB устройству». Редактирование не возможно.

Для ввода доступны IP адреса формата 192.168.1.1. Если необходимо добавить формат IPv6, включите переключатель IPv4/IPv6.

В вкладке «Доступ к USB устройствам» необходимо отметить USB устройства, к которым пользователю будет разрешен.



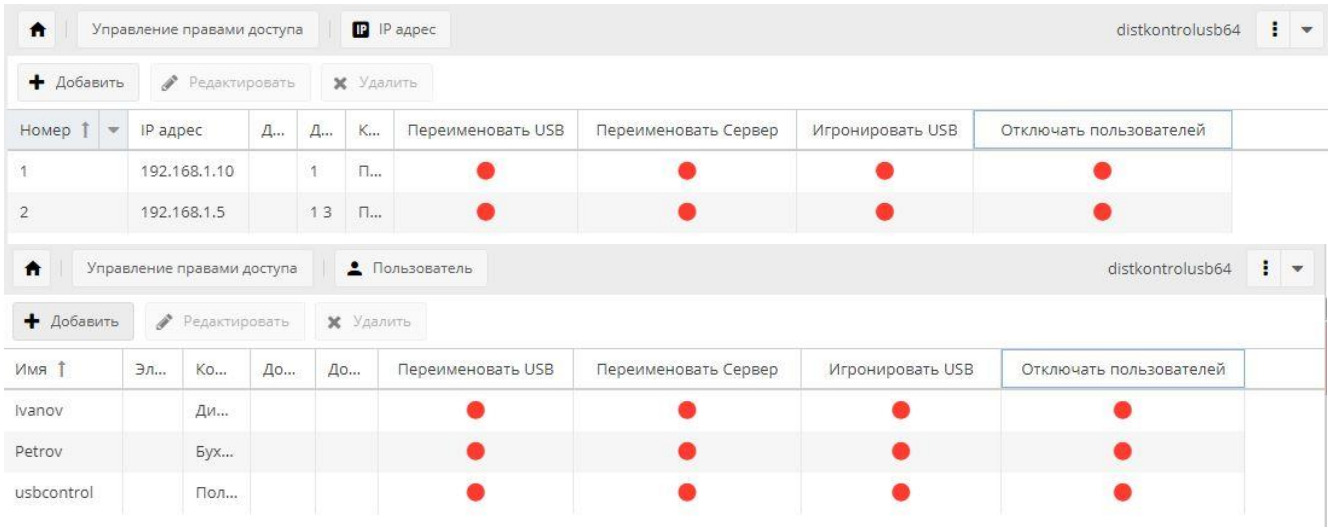
Аналогично, во вкладке «Доступ к USB портам» отметить USB порты (входы) к которым пользователю будет разрешен.

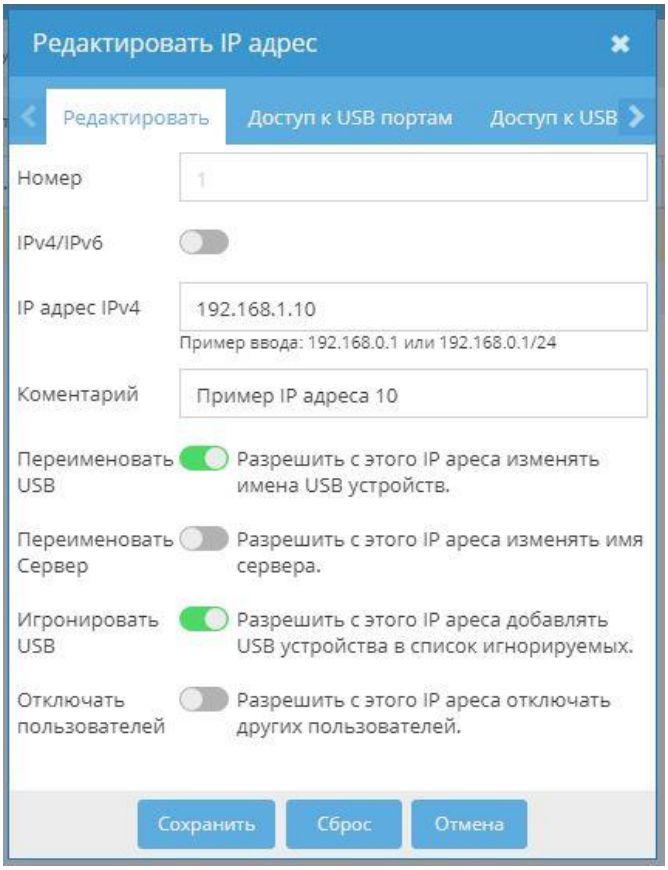
Для завершения создания нажать на кнопку «Сохранить» в диалоговом окне.

4.5.1.2 НАСТРОЙКИ ПРАВ

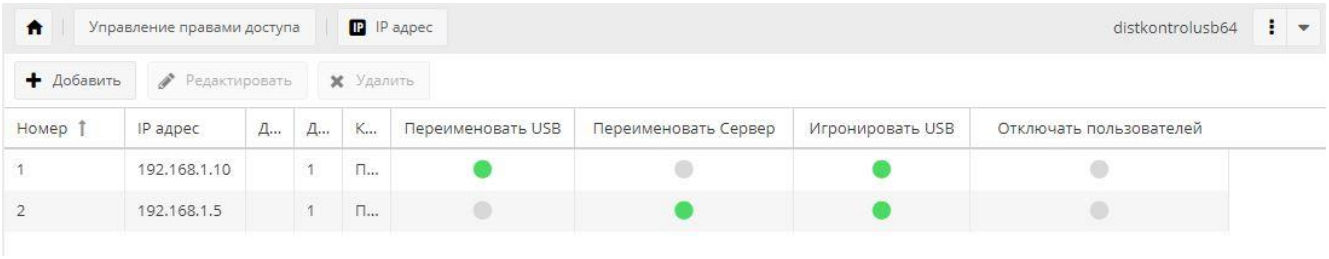
Опция «Ограничить права пользователей» по умолчанию отключена. В интерфейсе все права обозначены красным маркером. Все пользователи имеют права:

- изменение имени USB устройства;
- изменение имени концентратора;
- добавление USB устройств в список игнорируемых;
- отключение других пользователей в клиентском приложении DistKontrolUSB Client (при запуске клиентского приложения с параметром -a).





При активации данной опции, права на использования вышеперечисленных опций будут определяться из настроек прав пользователей и IP адресов. Разрешенные действия будут помечены зеленым маркером, не разрешенные серым.



Разрешения для пользователей и IP адресов работают по правилу «ИЛИ»

Пример 1:

Включили опцию «Ограничить права пользователей»

Пользователю Ivanov не разрешили ни одного из правил

IP адресу 192.168.1.10 разрешили изменять имя USB устройства

Пользователь Ivanov не сможет изменять имя USB устройства, если его IPадрес не будет 192.168.1.10

Любой пользователь с адресом 192.168.1.10 сможет изменять имя USB устройства.

Пример 2:

Включили опцию «Ограничить права пользователей»

Пользователю Ivanov разрешили отключать других пользователей

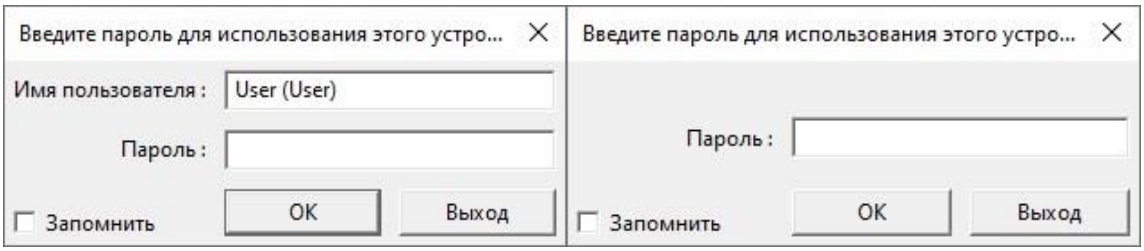
IP адресу 192.168.1.10 разрешили изменять имя сервера

Пользователь Ivanov сможет отключать других пользователей, если его IPадрес 192.168.1.10 он так же сможет изменять имя сервера.

Все пользователи с адресом 192.168.1.10 смогут изменять имя сервера.

Опция «Авторизация: использовать системное имя пользователя / введённое пользователем» по умолчанию “использовать системное имя пользователя”. Окно с запросом пароля будет выводится только при включенных ограничениях прав доступа по логину и паролю.

При активации, у пользователя будет возможность вводить логин отличный от системного во время подключения USB устройства.



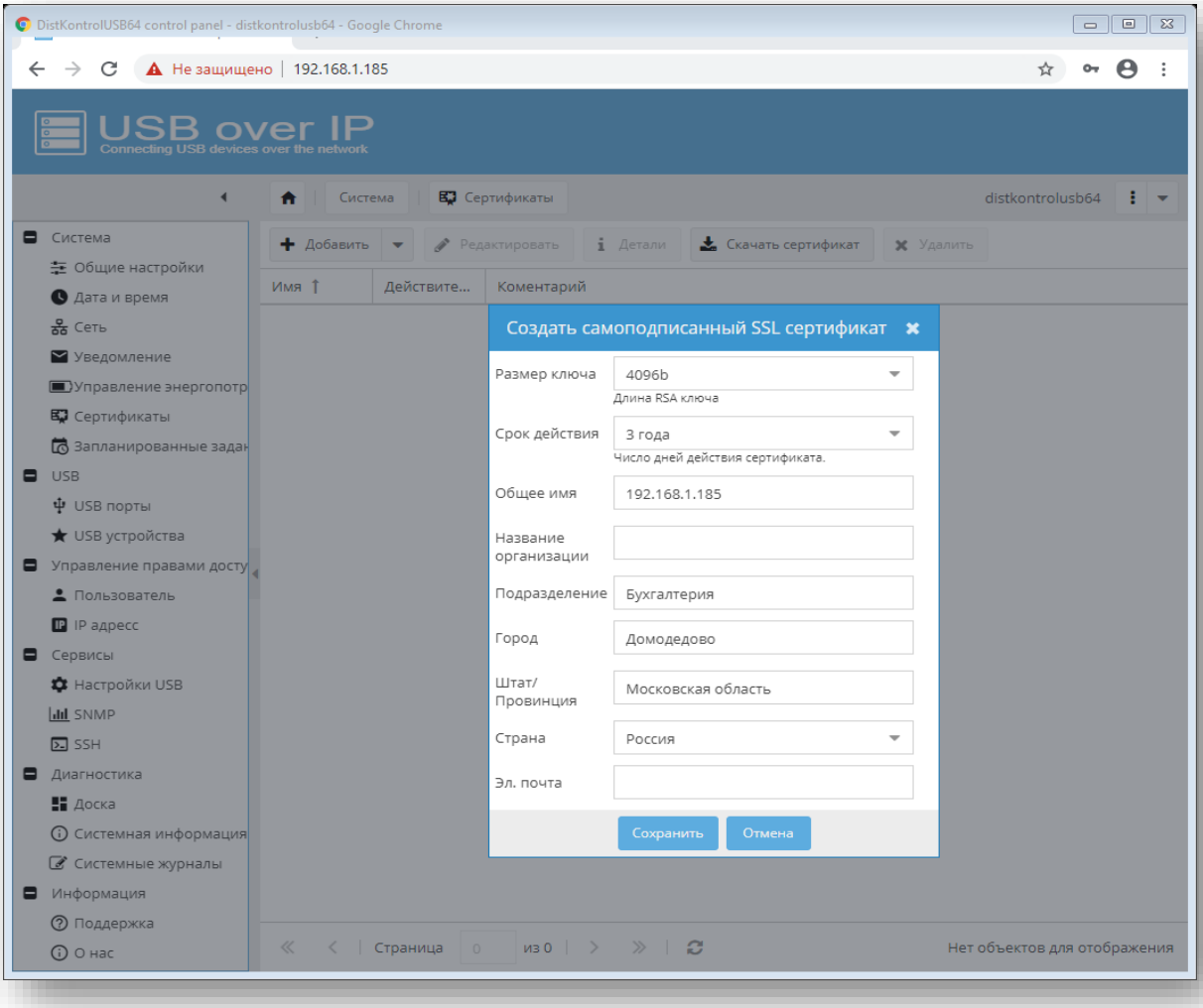
4.5.1.3 ПАРАМЕТРЫ КЛИЕНТСКОГО ПРИЛОЖЕНИЯ

Управляемый USB over IP концентратор поддерживает протокол защищенных сокетов (SSL) для связи клиент / сервер. Это полезно при совместном использовании USB-устройств через Интернет, чтобы обеспечить лучшую защиту от прослушивания. Возможно использование коммерческих или самоподписанных сертификатов.

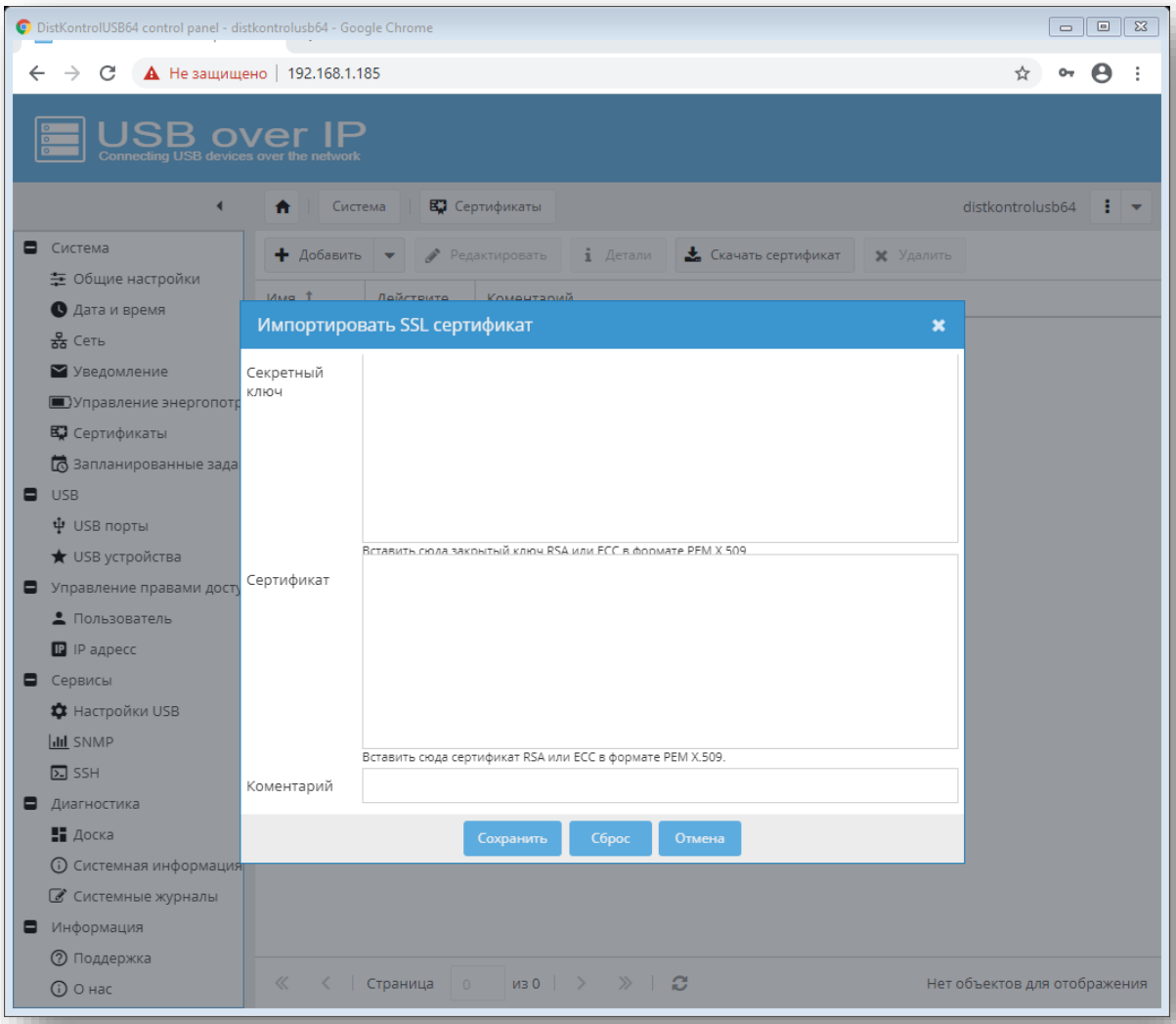
Включение режима осуществляется на странице «Сервисы» - «Настройки USB» - «Включить SSL для USB трафика». После включения режима и (или) добавления сертификатов необходима перезагрузка устройства для вступления изменений в силу.

Создайте самоподписанный сертификат сервера (или купите его в Центре сертификации). Также Вы можете использовать самоподписанный сертификат DistKontrolUSB. Его можно скачать на странице: «Система» - «Сертификаты» - «SSL» - «Скачать сертификат» или «Информация» - «Поддержка» - «Самоподписанный сертификат DistKontrolUSB» При настройке устройства рекомендуется сначала использовать его. Далее использовать коммерческий или создать свой самоподписанный сертификат.

Создать свой самоподписанный сертификат можно в WEB интерфейсе устройства на странице: «Система» - «Сертификаты» - «SSL» выбрать «Добавить» - «Создать»



Возможен импорт имеющегося сертификата. (необходимы: приватный RSA ключ в формате X.509 PEM и RSA сертификат X.509 в PEM формате), для этого выбрать «Добавить» - «Импортировать»



При создании нескольких сертификатов SSL, для шифрования USB трафика **будет использоваться последний созданный (импортированный)**. Сертификат для клиентского приложения можно скачать на странице: «Система» - «Сертификаты» - «SSL» - «Скачать сертификат» или «Информация» - «Поддержка» - «Самоподписанный сертификат DistKontrolUSB». Он будет обновлен и **соответствует последнему созданному (импортированному).**

ВНИМАНИЕ!!! Для шифрования трафика, устройство использует OpenSSL. При необходимости создания сертификата вне устройства, рекомендуем генерировать его при помощи OpenSSL:

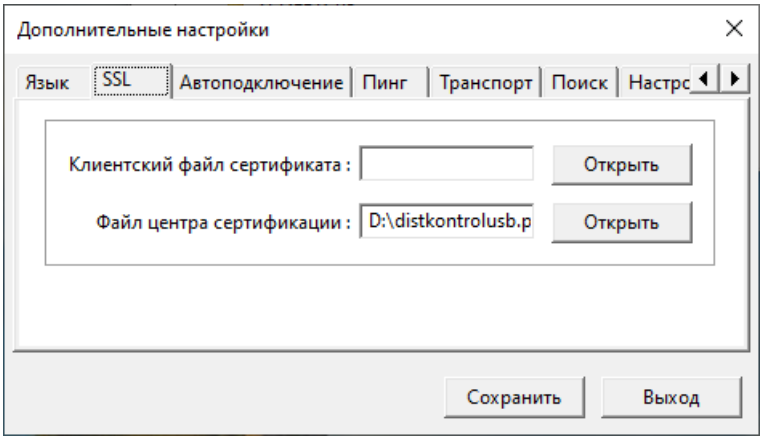
openssl genrsa -out usb.key 2048

openssl req -new -x509 -days 3650 -key usb.key -out usb.crt

openssl x509 -in usb.crt -out usb.pem -outform PEM

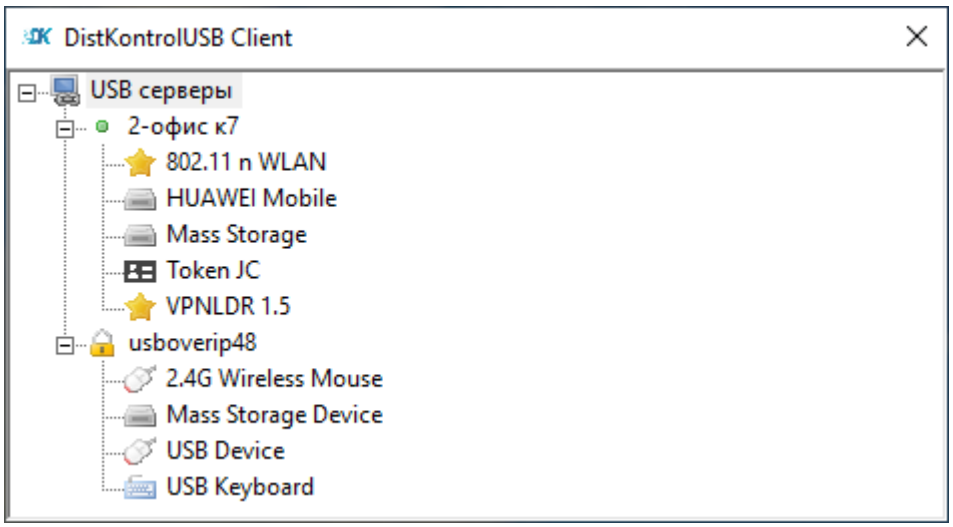
В клиентском приложении кликнете правой кнопкой мыши «USB Hubs» - «Advancent Settings». На вкладке «SSL» в строке «Sertificate Authority File» нажмите «Browse» и выберите Ваш сертификат pem. Нажмите «Save» и согласитесь с перезапуском клиентского приложения.

ВНИМАНИЕ!!! На ряде OS для корректной работы в пути к сертификату не должно быть кириллицы. Рекомендуется использовать латиницу для названий папок с местом хранения сертификата.



После настройки, клиент автоматически подключается к управляемому USB over IP концентратору с использованием TLSv1.2 через порт SSL по умолчанию 6564. Если вы не используете «Автоматический поиск», вам необходимо в меню «Specify Hubs» ввести адрес управляемого USB over IP концентратора и указать порт 6564.

После успешного подключения клиентского приложения к DustKontrolUSB, устройство в клиенте будет отображаться с соответствующим значком.



Порт SSL может быть изменен в WEB интерфейсе. Если Вы хотите использовать порт отличный от порта ssl по умолчанию будет необходимо внести изменения в INI-файл с настройками клиента. Закройте клиентское приложение. Отредактируйте INI-файл для клиента и добавьте строку под

```
[General]
……
SSLPort = 5554  (установленный в WEB интерфейсе порт SSL)
```

затем запустите клиент. Теперь клиент будет ожидать, что соединение через порт 5554 будет использовать ssl.

4.5.1.4 ОЧИСТКА И СБРОС

В ряде случаев возникает необходимость запрета использования USB устройства. Это возможно сделать из клиентского приложения. Кликнете правой кнопкой мыши на соответствующем USB устройстве и выберете «Ignore». Если у USB устройства есть серийный номер будет предложено добавить в список не используемых только это устройство или все с аналогичными VendorID и ProductID.

Очистка списка не используемых устройств USB осуществляется в WEB интерфейсе управляемого USB over IP концентратора на странице «Сервисы» - «Настройки USB» - «Очистить список игнорируемых устройств». После очистки списка не используемых устройств необходима перезагрузка устройства.

В клиентском приложении возможно переименовать USB устройства. Правой кнопкой мыши по устройству вызовите окно – Переименовать. Введите желаемое имя – Нажмите Ок. Изменение имени увидят все пользователи.

В WEB интерфейсе устройства на странице «Сервисы» - «Настройки USB» - «Сбросить имя USB-устройств на исходные», возможно сбросить имена на исходные. При сбросе служба будет перезапущена.

Для сброса всех настроек клиентского приложения, в WEB интерфейсе устройства на странице «Сервисы» - «Настройки USB» - «Сбросить параметры службы USB over IP на исходные.» При сбросе служба будет перезапущена.

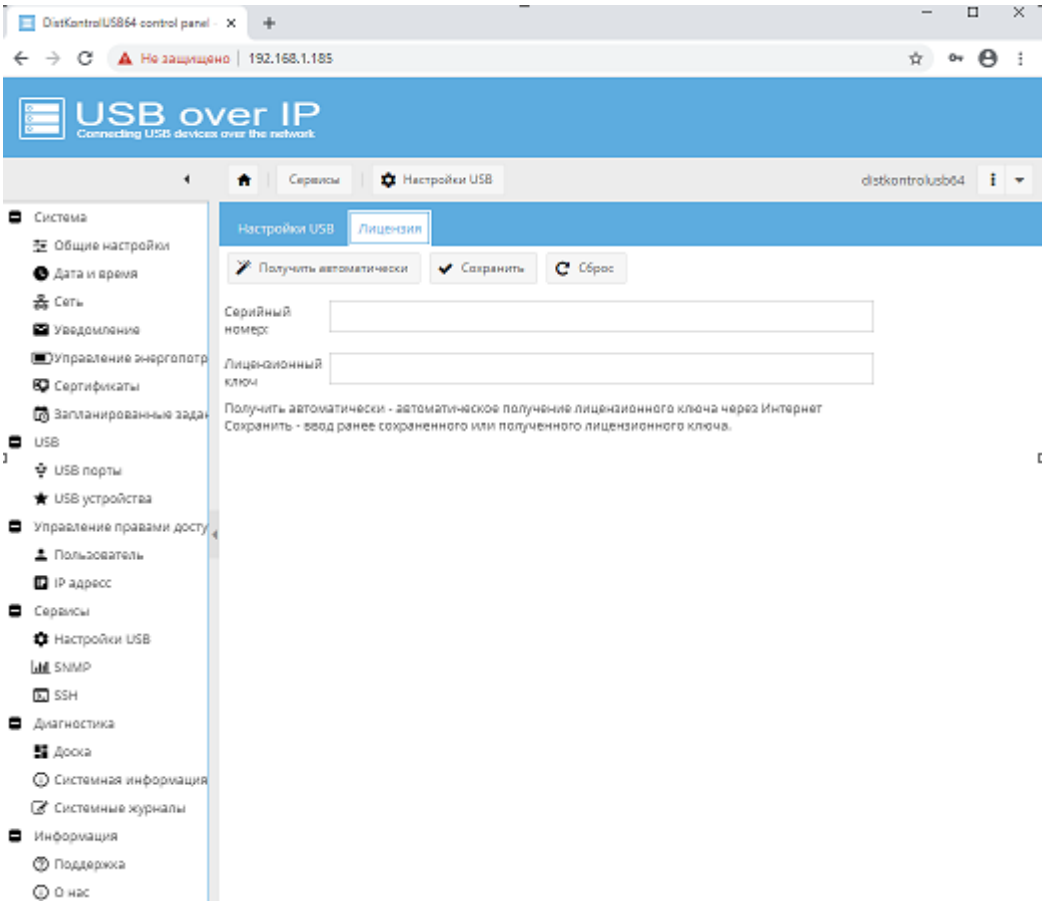
Будут сброшены номера портов, настройки ssl и отображения скрытых устройств, имена и скрытие устройств.

4.5.1.5 ЛИЦЕНЗИЯ

После сброса устройства к исходным установкам или обновления необходимо включить устройство и дождаться его загрузки. Об окончании загрузки свидетельствует появление устройства, а клиентском приложении и доступность WEB интерфейса устройства.

После загрузки необходимо ввести лицензионный ключ к ПО. Его можно ввести любым их трех способов:

1. В WEB интерфейсе концентратора автоматически – нажав на кнопку «Получить автоматически» на странице «Сервисы» - «Настройки USB» - «Лицензия». Ключ будет получен автоматически (у концентратора должен быть доступ к сети интернет) и ни какие дополнительные действия не потребуются.



2. В WEB интерфейсе концентратора вручную - ввести ранее сохраненный или полученный лицензионный ключ и нажать на кнопку «Сохранить».

3. Через клиентское приложение вручную. Для ввода лицензионного ключа необходимо, запустив клиентское приложение кликнуть правой кнопкой мыши по «USB Hubs» в клиенте, выбрать «License» - «Enter License» и в открывшемся окне вставить полученный ключ и нажать «OK».

Для ручного ввода лицензионного ключа:

1. Его можно скопировать и сохранить на странице «Лицензия» до обновления или сброса концентратора к заводским настройкам.

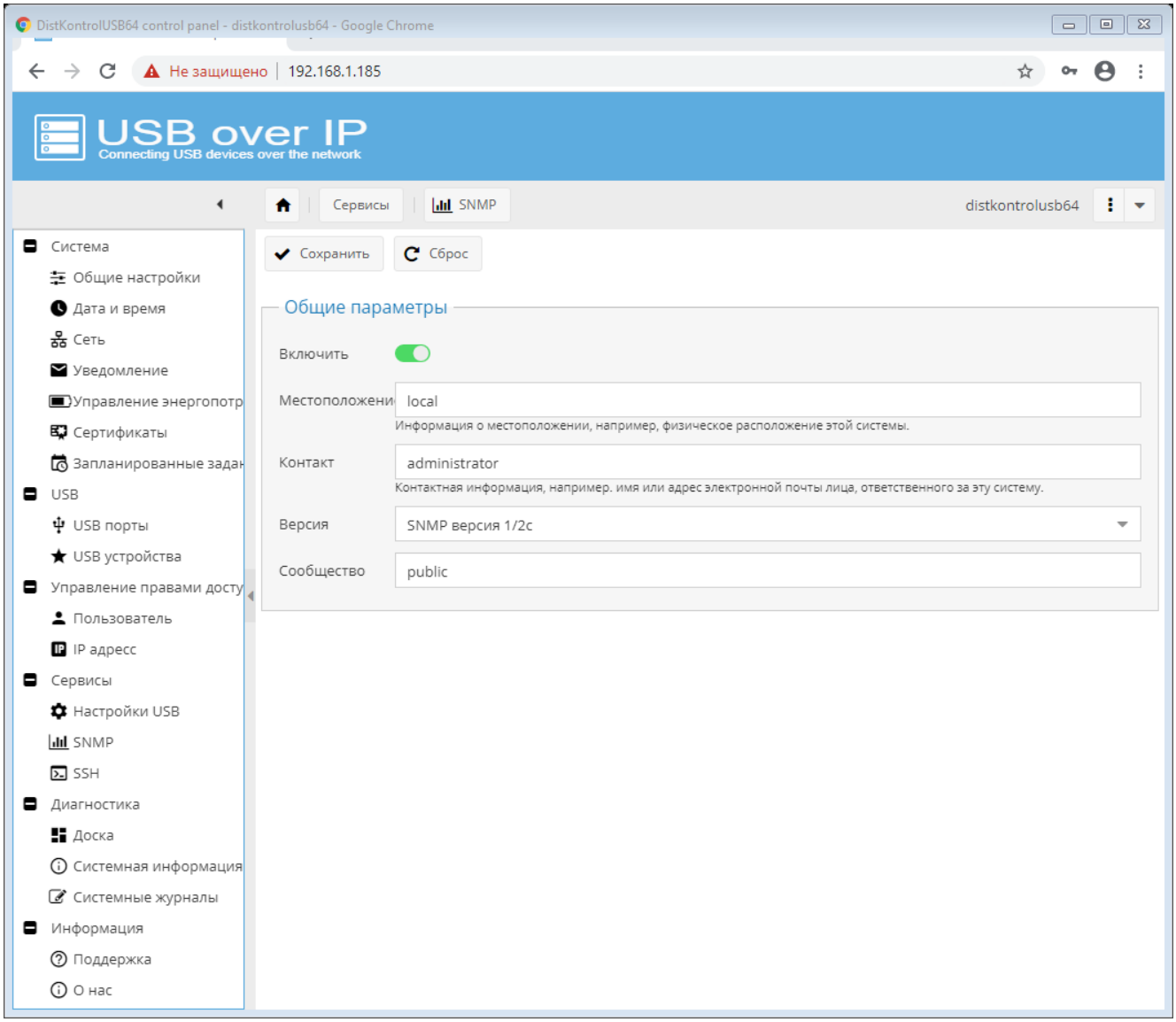
2.Запросить по электронной почте support@distkontrol.ru , указав заводской номер изделия.

Заводской номер изделия можно посмотреть, на странице «Сервисы» - «Настройки USB» - «Лицензия» или, запустив клиентское приложение. Кликнуть правой кнопкой мыши по имени устройства в клиенте, выбрать пункт меню «Properties» и скопировать из строки «SERIAL NUMBER» (РЕКОМЕНДУЕТСЯ) или в паспорте устройства (на последней странице внизу).

4.5.2 SNMP

Управляемый USB over IP концентратор поддерживает SNMP версий 1, 2c, 3. Поддержка SNMP позволяет легко обеспечить мониторинг состояния концентратора и USB входов с помощью различных систем мониторинга. Например, Zabbix, Nagios и т.д.

В заводской настройке SNMP (Simple Network Management Protocol) отключен. Включение и настройка протокола осуществляется на странице «Сервисы» - «SNMP».



Для настройки SNMP версий 1, 2c:

Элемент	Описание
Включить	Выберите, будет ли концентратор использовать SNMP.
Местоположение	Информация о местоположении, например, физическое расположение этой системы. Может содержать до 64 символов.
Контактное лицо	Контактная информация, например, имя или адрес электронной почты лица, ответственного за эту систему. Может содержать до 64 символов.
Версия	Используемая версия SNMP
Сообщества	Введите имя сообщества для аутентификации запросов. Может содержать до 32 символов. (Может использоваться в качестве пароля)

Для настройки SNMP версии 3 дополнительно необходимо задать:

- Имя пользователя,
- Уровень безопасности. Эта функция безопасности позволяет устанавливать аутентификацию на основе требований пользователя. 3 уровня аутентификации:
    - NoAuthNoPriv: пользователи, которые используют этот режим / уровень, не имеют аутентификации и не имеют конфиденциальности при отправке / получении сообщений.
    - AuthNoPriv: этот уровень требует от пользователя аутентификации, но не будет шифрования отправленных / полученных сообщений.
    - AuthPriv: Наконец, самый безопасный уровень, в котором требуется аутентификация, и отправленные / полученные сообщения зашифрованы.
- Тип аутентификации и Пароль пользователя (при выборе уровня безопасности с аутентификацией),
- Тип конфиденциальности (шифрования данных) и Пароль (при выборе уровня безопасности с конфиденциальностью).

Список OID (Object Identifier) для получения информации

о состояния управляемого USB over IP концентратора по SNMP:

OID (Object Identifier)	Параметр	Примечания
.1.3.6.1.4.1.2021.9.12.1	Температура CPU	
.1.3.6.1.4.1.2021.9.12.2	CPU Load	
.1.3.6.1.4.1.2021.10.1.3.1	1 minute CPU Load	
.1.3.6.1.4.1.2021.10.1.3.2	5 minute CPU Load	
.1.3.6.1.4.1.2021.10.1.3.3	15 minute CPU Load	

.1.3.6.1.4.1.2021.11.11.0	Idle CPU time (%)	
.1.3.6.1.4.1.2021.4.6.0	Total RAM used	
.1.3.6.1.4.1.2021.4.11.0	Total RAM Free	
.1.3.6.1.2.1.25.1.1.0	Uptime устройства	
.1.3.6.1.4.1.2021.20.1.1	Состояние USB порта 1.1	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.2	Состояние USB порта 1.2	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.3	Состояние USB порта 1.3	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.4	Состояние USB порта 1.4	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.5	Состояние USB порта 1.5	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.6	Состояние USB порта 1.6	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.7	Состояние USB порта 1.7	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.8	Состояние USB порта 1.8	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.9	Состояние USB порта 1.9	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.10	Состояние USB порта 1.10	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.11	Состояние USB порта 1.11	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.12	Состояние USB порта 1.12	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.13	Состояние USB порта 1.13	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.14	Состояние USB порта 1.14	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.15	Состояние USB порта 1.15	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.1.16	Состояние USB порта 1.16	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.1	Состояние USB порта 2.1	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.2	Состояние USB порта 2.2	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.3	Состояние USB порта 2.3	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.4	Состояние USB порта 2.4	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.5	Состояние USB порта 2.5	Включен/выключен (1/0)

.1.3.6.1.4.1.2021.20.2.6	Состояние USB порта 2.6	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.7	Состояние USB порта 2.7	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.8	Состояние USB порта 2.8	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.9	Состояние USB порта 2.9	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.10	Состояние USB порта 2.10	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.11	Состояние USB порта 2.11	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.12	Состояние USB порта 2.12	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.13	Состояние USB порта 2.13	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.14	Состояние USB порта 2.14	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.15	Состояние USB порта 2.15	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.2.16	Состояние USB порта 2.16	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.1	Состояние USB порта 3.1	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.2	Состояние USB порта 3.2	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.3	Состояние USB порта 3.3	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.4	Состояние USB порта 3.4	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.5	Состояние USB порта 3.5	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.6	Состояние USB порта 3.6	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.7	Состояние USB порта 3.7	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.8	Состояние USB порта 3.8	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.9	Состояние USB порта 3.9	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.10	Состояние USB порта 3.10	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.11	Состояние USB порта 3.11	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.12	Состояние USB порта 3.12	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.13	Состояние USB порта 3.13	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.14	Состояние USB порта 3.14	Включен/выключен (1/0)

.1.3.6.1.4.1.2021.20.3.15	Состояние USB порта 3.15	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.3.16	Состояние USB порта 3.16	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.1	Состояние USB порта 4.1	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.2	Состояние USB порта 4.2	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.3	Состояние USB порта 4.3	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.4	Состояние USB порта 4.4	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.5	Состояние USB порта 4.5	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.6	Состояние USB порта 4.6	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.7	Состояние USB порта 4.7	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.8	Состояние USB порта 4.8	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.9	Состояние USB порта 4.9	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.10	Состояние USB порта 4.10	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.11	Состояние USB порта 4.11	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.12	Состояние USB порта 4.12	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.13	Состояние USB порта 4.13	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.14	Состояние USB порта 4.14	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.15	Состояние USB порта 4.15	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.4.16	Состояние USB порта 4.16	Включен/выключен (1/0)

4.5.2.1 ПРИМЕРЫ ПРОВЕРКИ НАСТРОЙКИ SNMP УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

Перед настройкой системы мониторинга рекомендуется убедиться в корректности получения данных с устройства. Должен быть открыт порт 161/TCP.

Пример для Linux, с помощью snmpget (должна быть установлена).

Вводим:

```
snmpget -v 2c 192.168.1.180 -c public .1.3.6.1.4.1.2021.9.12.1
```

или (в зависимости от выбранной версии SNMP)

```
snmpget -v3  -l authPriv -u user1 -a MD5 -A "12345678"  -x DES -X "12345678" 192.168.1.180
.1.3.6.1.4.1.2021.9.12.1
```

Получаем:

iso.3.6.1.4.1.2021.9.12.1 = INTEGER: 52

Пример для Windows, с помощью SnmpGet (должна быть установлена):

```
SnmpGet.exe -r:192.168.1.180 -t:10 -c:"public" -o:.1.3.6.1.4.1.2021.9.12.1
```

или (в зависимости от выбранной версии SNMP)

```
SnmpGet.exe -r:192.168.1.180 -v:3 -sn:user1 -ap:MD5 -aw:12345678 -pp:DES -pw:12345678 -o:
.1.3.6.1.4.1.2021.9.12.1
```

Получаем:

SnmpGet v1.01 - Copyright (C) 2009 SnmpSoft Company

[More useful network tools on http://www.snmpsoft.com]

OID=.1.3.6.1.4.1.2021.9.12.1

Type=Integer

Value=52

4.5.2.2 ПРИМЕР НАСТРОЙКИ ZABBIX ДЛЯ МОНИТОРИНГА СОСТОЯНИЯ УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

Для начала мониторинга состояния, управляемого USB over IP концентратора и его USB входов по SNMP с помощью системы мониторинга Zabbix, должны быть выполнены следующие шаги:

Шаг 1

Создайте узел сети для устройства.

Введите IP адрес. Нажмите на «Добавить» для сохранения узла сети.

Шаг 2

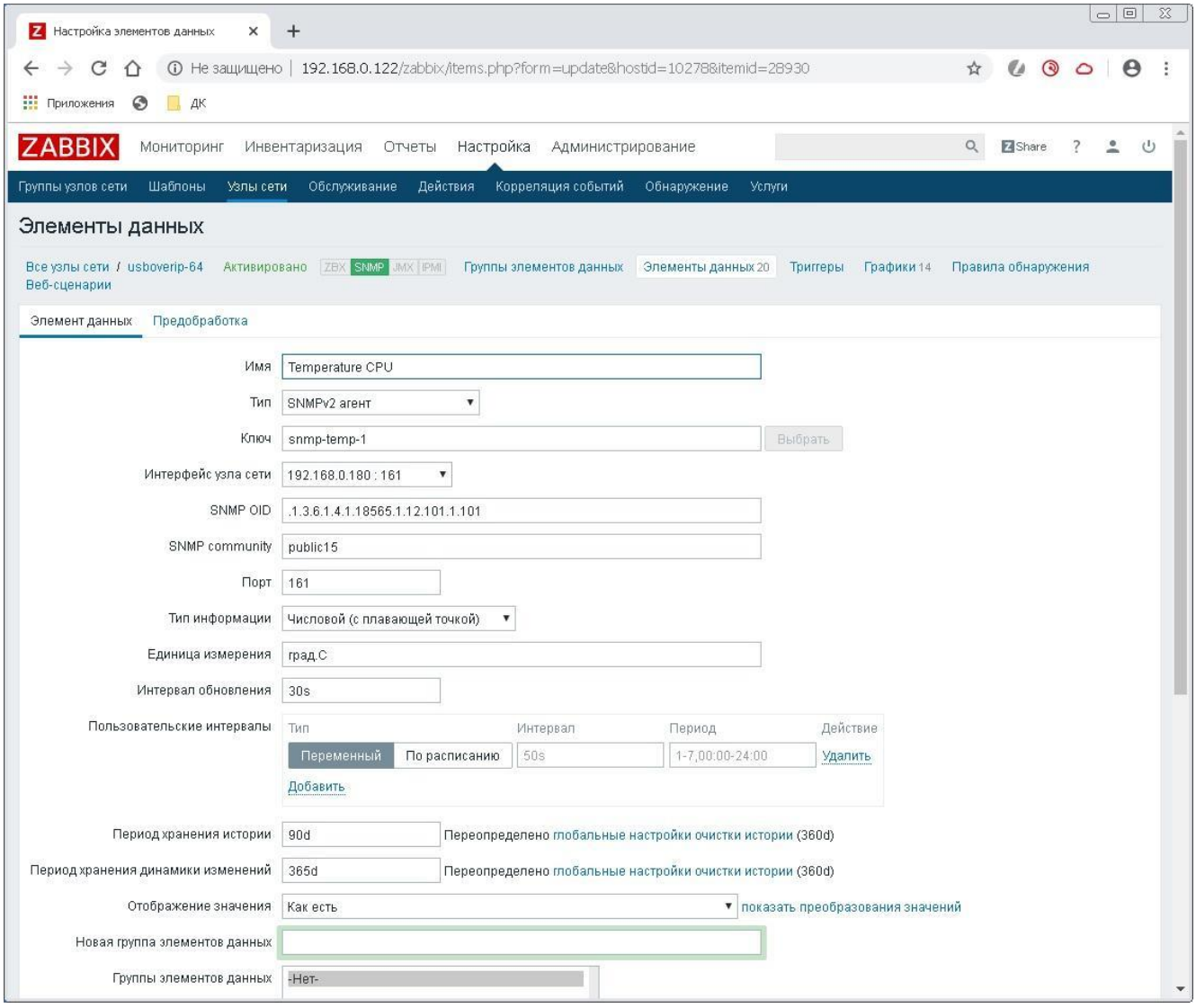
В руководстве пользователя уточните SNMP OID элемента данных, который вы хотите наблюдать.

Шаг 3

Создайте элемент данных для мониторинга.

В Zabbix нажмите на Элементы данных, выберите созданный ранее узел сети SNMP. Введите простое описание на русском языке (или английском) в поле 'Описание' в диалоге нового элемента данных. Убедитесь, что в поле «Узел сети» находится ваш концентратор и измените поле «Тип» в значение «SNMPv* агент». Введите «community» (обычно public) и укажите числовой OID, который вы получили ранее, в поле «SNMP OID», например: .1.3.6.1.4.1.2021.9.12.1

Введите «Порт SNMP» - 161 и «Ключ» - что-то осмысленное, например, SNMP-Temperature. Установите «Тип информации» в значение равное Числовой (с плавающей точкой). Выберите множитель, если желаете, и укажите «Интервал обновления», и «Хранение истории», если вы хотите, чтобы значения параметров отличались от умолчаний.



Все обязательные поля ввода отмечены красной звёздочкой.

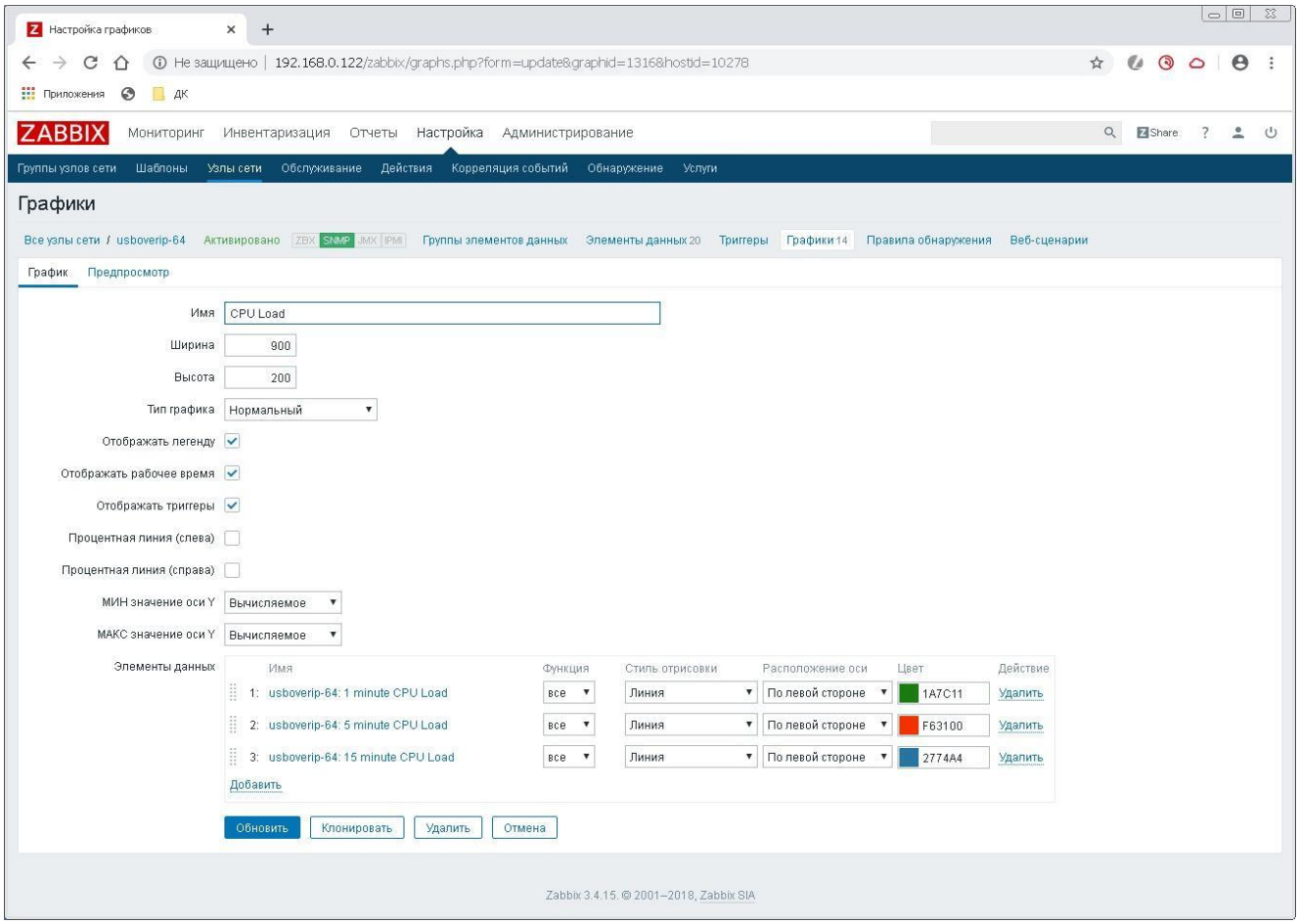
Сохраните элемент данных и перейдите в Мониторинг → Последние данные, чтобы увидеть данные SNMP.

Обратите внимание на специфичные опции доступные только для SNMPv3 элементов данных. В случае некорректных учётных данных SNMPv3 (имя безопасности, протокол/фраза-пароль аутентификации, протокол безопасности) Zabbix получит ERROR от net-snmp, за исключением ошибочного Фразы-пароль безопасности, в этом случае Zabbix получит ошибку ВРЕМЕНИ ОЖИДАНИЯ от net-snmp.

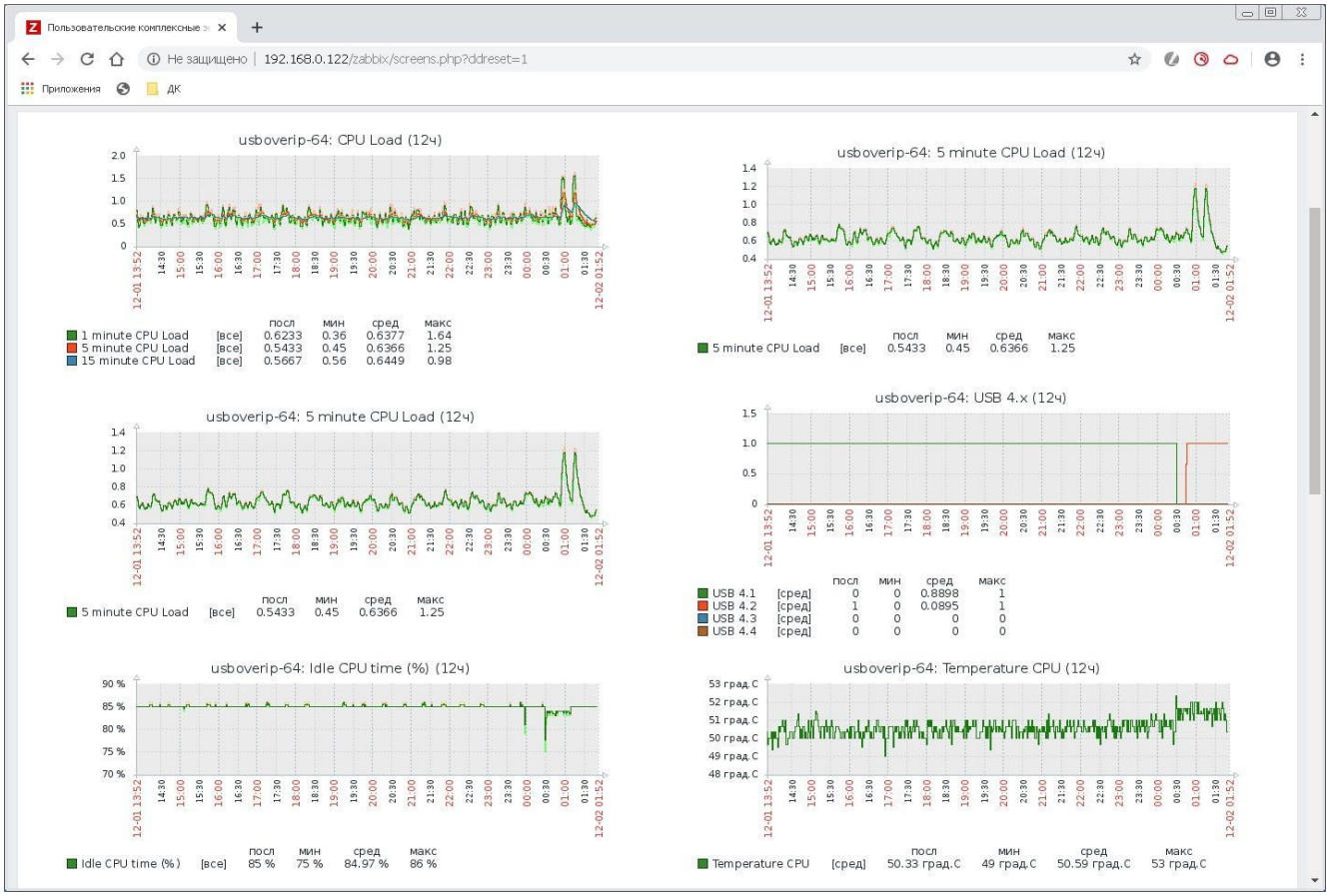
При изменениях в Протокол аутентификации, Фраза-пароль аутентификации, Протокол безопасности или Фраза-пароль безопасности, чтобы эти изменения применились, необходимо перезапустить сервер.

Шаг 4

Далее создаем графики для необходимых элементов данных.



Шаг 5. Далее создаем комплексные экраны:



4.5.3 SSH

SSH используется для работы с утилитой UsbControl. Более подробно по работе с утилитой можно ознакомиться в разделе «Краткая инструкция по использованию утилиты управления портами управляемого USB over IP концентратора»

4.6 ДИАГНОСТИКА

4.6.1 ДОСКА

Доска с информацией. Возможно добавлять, скрывать, закрывать, изменять размер, а также перетаскивать окна. Является начальной страницей при входе в Web интерфейс.

4.6.2 СИСТЕМНАЯ ИНФОРМАЦИЯ

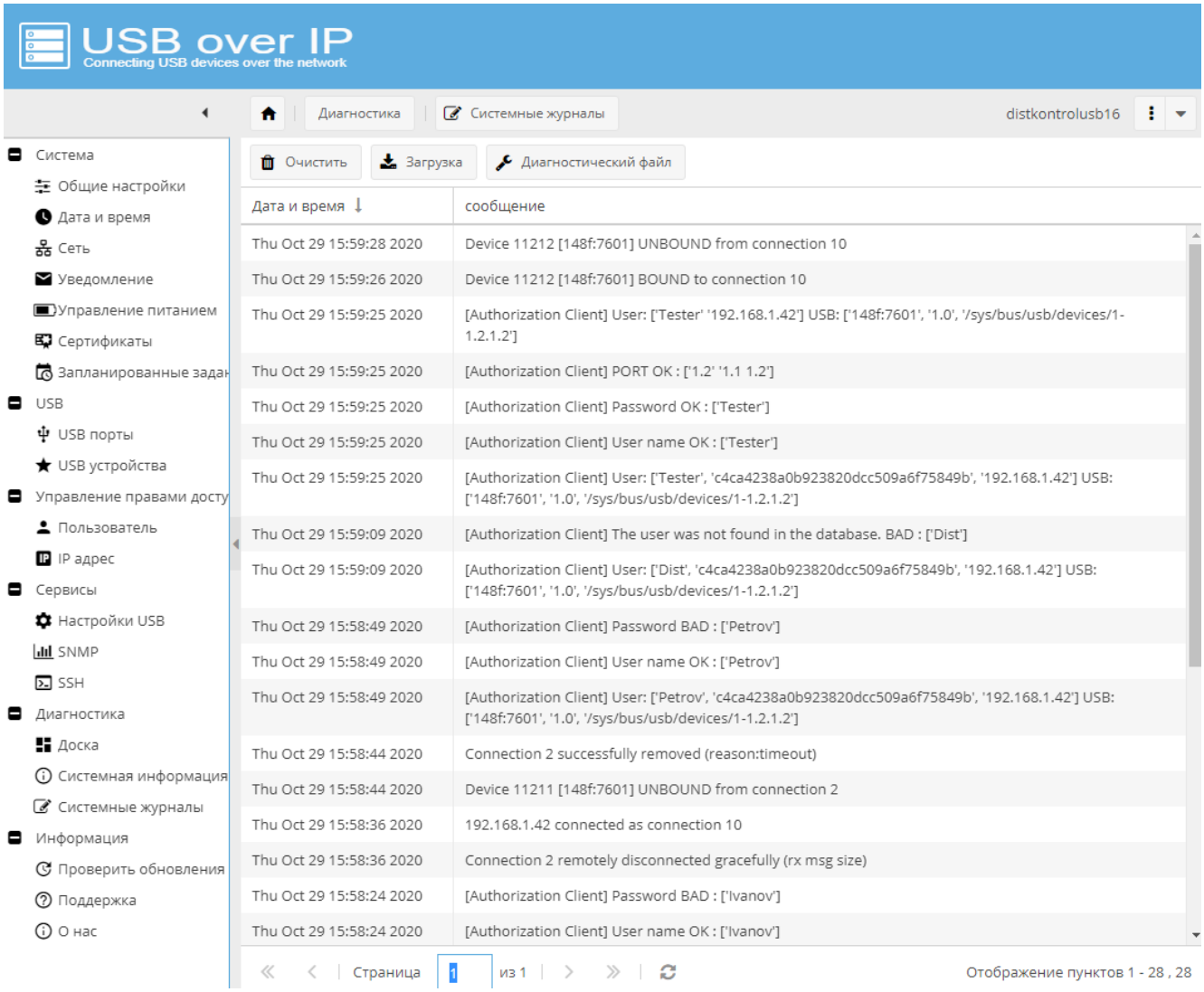
В данном разделе представлена информация о версии прошивки, системное время, параметры нагрузки CPU и RAM.

4.6.3 СИСТЕМНЫЙ ЖУРНАЛ

Просмотр системного журнала возможен на странице WEB интерфейса администратора «Диагностика» - «Системные журналы».

В журнале хранится вся информация о подключениях и отключениях как USB входов (портов) DistKontrolUSB, так и любого из USB устройств, а также попытках не правильного ввода пароля. Так же записываются изменения настроек концентратора и прочая служебная информация.

Диагностический файл необходим при обращении в техническую поддержку.



В строке [Connect Client] -> отображаются параметры подключения USB устройства пользователем в следующей последовательности:

User: Логин пользователя

Pswd: Пароль пользователя (MD5 hash) (в случае ввода пароля)

IP: IP адрес пользователя

Port: USB порт

Name: Псевдоним USB устройства (в случае если устройство переименовывалось)

V_ID: VENDOR_ID USB устройства

P_ID: PRODUCT_ID USB устройства

Serial: SERIAL № USB устройства

Path: Текущий номер USB устройства используемый пользователем (внутренний служебный)

Строка записывается в журнал при каждом подключении клиентом USB устройства, независимо от режима доступа к USB устройствам.

4.6.3.1 СООБЩЕНИЯ СИСТЕМЫ АВТОРИЗАЦИИ

Авторизация по логину и паролю для доступа к USB устройству.

[Authorization Client] The user ‘ИМЯ’ was not found in the database – Пользователь не найден в базе концентратора.

[Authorization Client] The user ' ИМЯ ' found - Пользователь найден в базе концентратора.

[Authorization Client] Password OK (или BAD) – Не успешная (или успешная) проверка имени пользователя и пароля для подключения к USB устройству. В квадратных скобках Имя пользователя, от которого производится подключение.

[Authorization Client] The USB device was not found in the database - Подключаемое USB устройство отсутствует в списке USB устройств.

[Authorization Client] The user 'ИМЯ' does not have permission to connect USB devices. – Пользователь не имеет ни одного разрешенного USB устройства.

[Authorization Client] DEVICE OK (или BAD) – Не успешная (или успешная) проверка разрешения пользователю использовать подключаемое USB устройство. В квадратных скобках первый параметр № USB устройства к которому производится подключение, второй – перечень разрешенных для пользователя USB устройств.

Авторизация по логину и паролю для доступа к USB порту концентратора.

[Authorization Client] The user ‘ИМЯ’ was not found in the database – Пользователь не найден в базе концентратора.

[Authorization Client] The user ' ИМЯ ' found - Пользователь найден в базе концентратора.

[Authorization Client] Password OK (или BAD) – Не успешная (или успешная) проверка имени пользователя и пароля для подключения к USB устройству. В квадратных скобках Имя пользователя, от которого производится подключение.

[Authorization Client] PORT OK (или BAD) – Не успешная (или успешная) проверка разрешения пользователю пользоваться подключаемым портам. В квадратных скобках первый параметр номер порта, к которому производится подключение, второй – перечень разрешенных для данного пользователя портов.

Авторизация по IP адресу для доступа к USB устройству.

[Authorization Client] The IP 'IP адрес' not found in the database – IP адрес не найден в базе концентратора.

[Authorization Client] The IP 'IP адрес' found - IP адрес найден в базе концентратора.

[Authorization Client] DEVICE OK (или BAD) – Не успешная (или успешная) проверка разрешения подключения USB устройств с данного IP. В квадратных скобках первый параметр номер USB устройства из списка USB устройств, второй – список USB устройств, разрешенных для данного IP.

Авторизация по IP адресу для доступа к USB порту концентратора.

[Authorization Client] The IP 'IP адрес' not found in the database – IP адрес не найден в базе концентратора.

[Authorization Client] The IP 'IP адрес' found - IP адрес найден в базе концентратора.

[Authorization Client] PORT OK (или BAD) – Н Не успешная (или успешная) проверка разрешения подключения USB порта с данного IP. В квадратных скобках первый параметр номер USB порта к которому производится подключение, второй – перечень разрешенных портов для данного IP.

BOUND to connection X - Успешное подключение USB устройства;

UNBOUND from connection X - Успешное отключение USB устройства.

4.6.3.2 СООБЩЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПИТАНИЕМ USB УСТРОЙСТВ

[USB PORTS]//Control port// USER: Petrov USB in: 2.3 STATUS: turnOn (turnoff) – Включение (выключение) USB порта 2.3 пользователем « Petrov »

4.6.3.3 ПРОЧИЕ СООБЩЕНИЯ

Все сообщения в системном журнале управляемого USB over IP концентратора записываются с датой и временем. Для корректной работы службы времени устройства, она должна быть настроена в разделе «Система» - «Дата и время».

Так же в системном журнале управляемого USB over IP концентратора записывается прочая служебная информация о работе устройства.

Возможна очистка журнала и его загрузка на компьютер пользователя для последующего хранения и анализа.

Таким образом, при анализе сообщений системного журнала можно диагностировать различные проблемы при ограничении доступа к USB устройствам и портам для ее настройки требуемым образом.

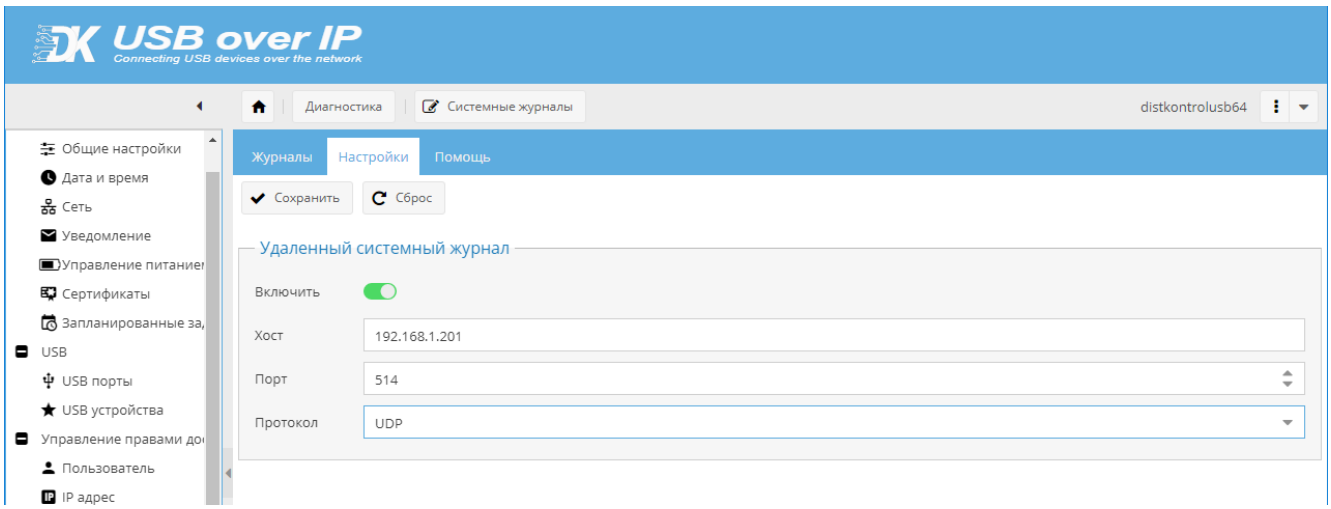
Общая структура сообщений:

[USB Settings] Restricting access to the USB port by login and password – DISABLED:

- [USB Settings] – Лог раздела «Настройки USB»
- Restricting access to the USB port by login and password – название измененного параметра
- DISABLED – статус параметра.

4.6.4 УДАЛЕННЫЙ СИСТЕМНЫЙ ЖУРНАЛ

В концентраторе предусмотрена возможность отправки журнала (syslog) на удаленный сервер. Включение опции и ее настройка осуществляются на странице WEB интерфейса администратора «Диагностика» - «Системные журналы» - «Настройки».



Для настройки перенаправления журналов на сторонний сервер со стороны концентратора достаточно включить отправку журнала, указать хост порт и протокол.

В сети вам необходимо иметь настроенный действующий сервер приема логов.

Пример настройки удаленного сервера Linux на базе Debian:

Все команды выполняются под пользователем root

1. Установка программы:

```
apt-get install -y syslog-ng
```

2. Создадим файл конфигурации:

```
nano /etc/syslog-ng/conf.d/input.conf
```

3. Добавляем настройки в файл:

```
source s_udp { udp(ip(0.0.0.0) port(514)); };
destination d_dku-64 { file("/var/log/dku-64-logs/logs.log"); };
filter f_dku-64 { netmask("192.168.1.180/255.255.255.255"); };
log { source(s_udp); filter(f_dku); destination(d_dku); };
```

Если IP адрес отличается от настроек по умолчанию, измените настройки filter.

4. Создаём каталог для хранения логов:

```
mkdir /var/log/dku-64-logs/
```

5. Запускаем syslog-ng и добавляем в автозагрузку:

```
systemctl start syslog-ng
systemctl enable syslog-ng
```

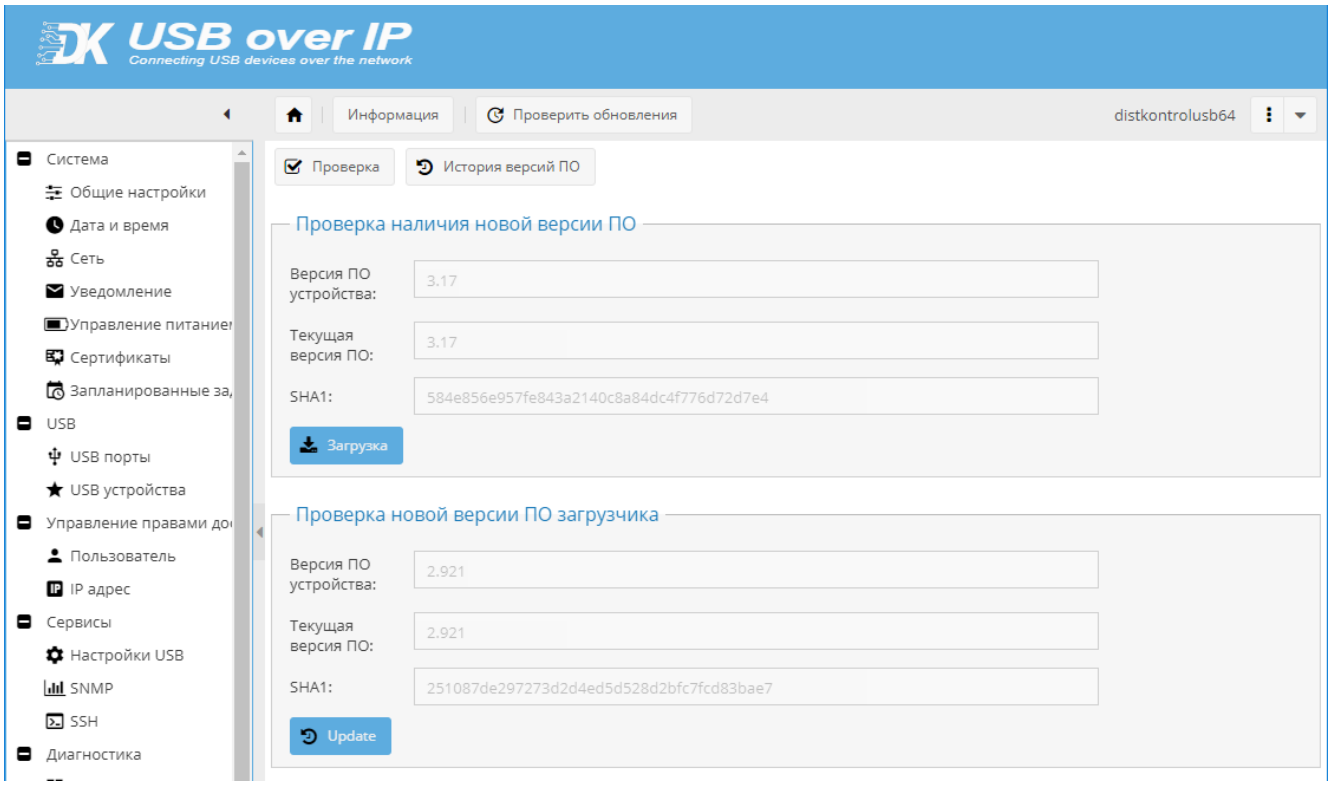
4.7 ИНФОРМАЦИЯ

4.7.1 ПРОВЕРИТЬ ОБНОВЛЕНИЯ

Страница позволяет:

1. Проверить наличие новой версии ПО концентратора и, при наличии, скачать его для обновления через флеш носитель.
2. Проверить наличие новой версии ПО загрузчика концентратора, и при наличии, установить его.

Для работы опций требуется доступ концентратора в интернет.



Для проверки наличия обновлений, необходимо нажать на кнопку «Проверка»

Кнопка «Загрузка» - позволяет скачать последнею доступную версию ПО для обновления концентратора с флеш носителя. Подробнее см. «Обновление ПО».

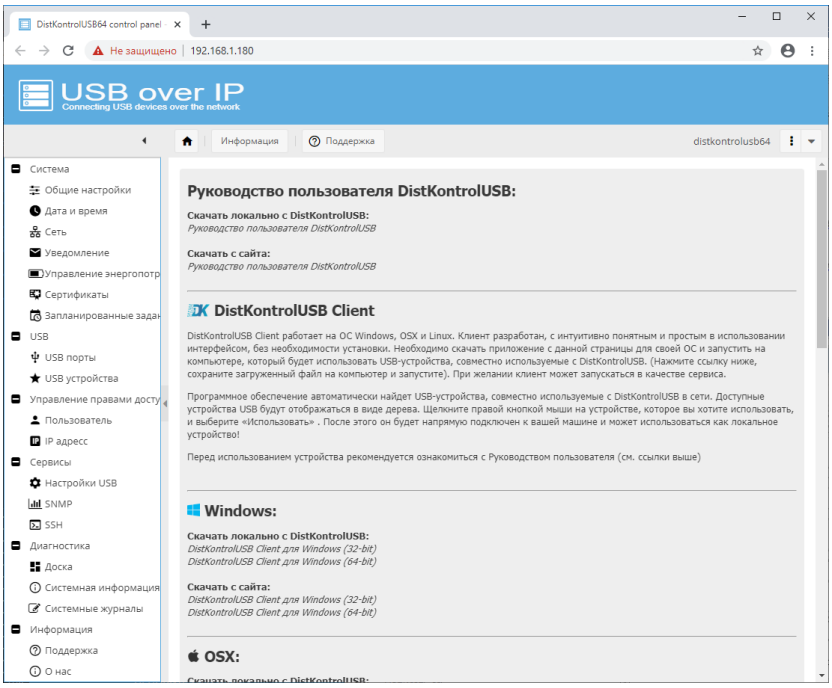
Кнопка «Обновление» - позволяет скачать последнею доступную версию загрузчика ПО концентратора и установить ее. После обновления концентратор необходимо перезагрузить.

Кнопка «История версий ПО» - открывает страницу с историей изменений в новом окне.

«SHA1» - контрольная сумма файла прошивки.

4.7.2 ПОДДЕРЖКА

В данном разделе можно скачать Руководство пользователя, а также клиент DistKontrolUSB под вашу операционную систему. Скачивание доступно локально и с сайта через интернет.



4.7.3 О НАС

Контактная информация.

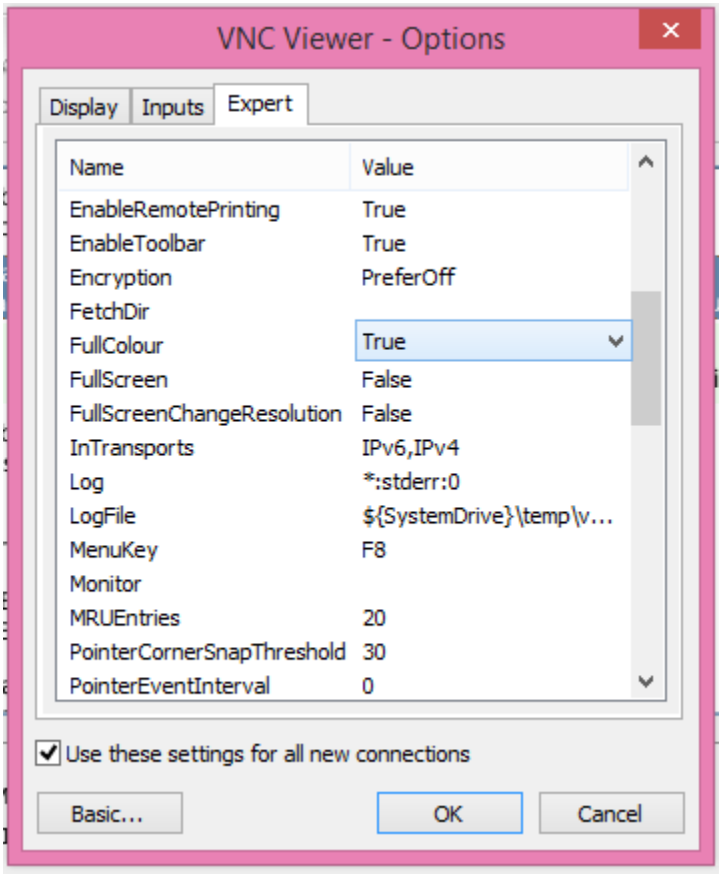
4.8 СБРОС НАСТРОЕК, УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА В ИСХОДНОЕ СОСТОЯНИЕ.

Выполнить сброс настроек возможно двумя способами:

1. С помощью аппаратной кнопки «Reset», расположенной с тыльной части устройства. Для сброса необходимо выключить концентратор, нажать на кнопку «Reset» и, не отпуская кнопку, подать питание на устройство. Через 20 секунд можно отпустить кнопку «Reset». Устройство сброшено до заводских установок.

2. Для сброса настроек USB over IP к исходным установкам необходимо установить любой клиент VNC.

Клиент VNC, который вы используете, должен запросить 24-разрядный цвет (режим палитры цветов*not* 256). TightVNC и krdc работают нормально по умолчанию, для RealVNC убедитесь, что вы включили полный Цвет в настройках:



Использование клиента VNC, который запрашивает неправильное количество цветов, приведет к сбою приложения (отображение “оболочки аварийного восстановления” на экране).

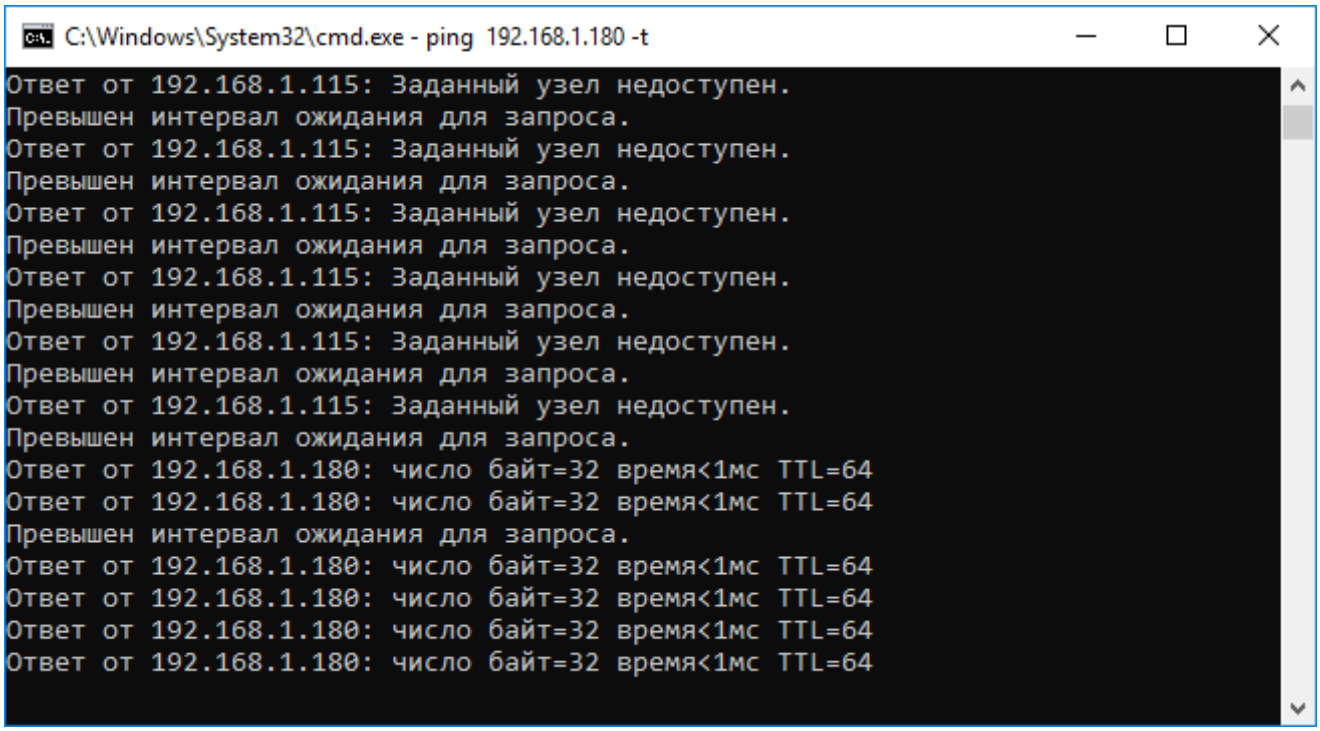
Подключение для сброса настроек возможно в течении 20 с после подачи питания на USB over IP. Рекомендуется в командной строке выполнить команду:

```
ping -t 192.168.1.180
```

и дождаться появления ответа от USB over IP. Затем вы можете запустить клиентскую программу VNC на обычном компьютере и подключиться к устройству по IP-адресу 192.168.1.180

ВНИМАНИЕ!!! Для сброса настроек и обновления концентратора подключатся необходимо именно по IP-адресу 192.168.1.180, независимо от установленного для основного ПО адреса.

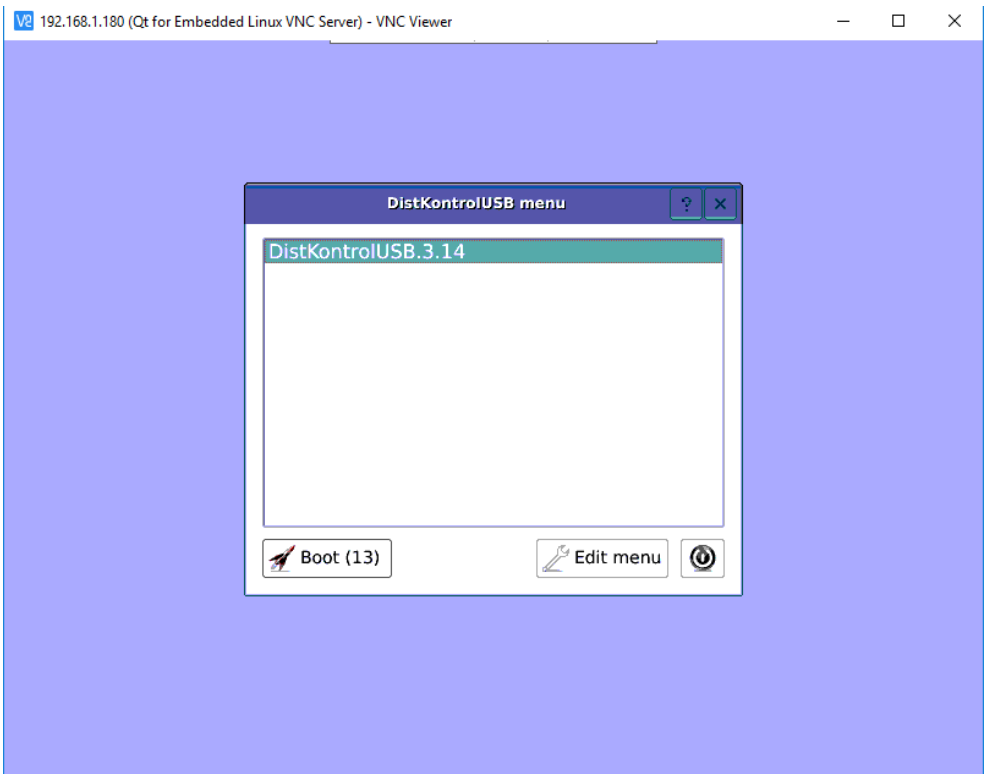
Подключение должно быть выполнено в течении 20 с или устройство продолжит нормальную загрузку для работы в штатном режиме, подключение к нему уже будет невозможно до повторной перезагрузки.



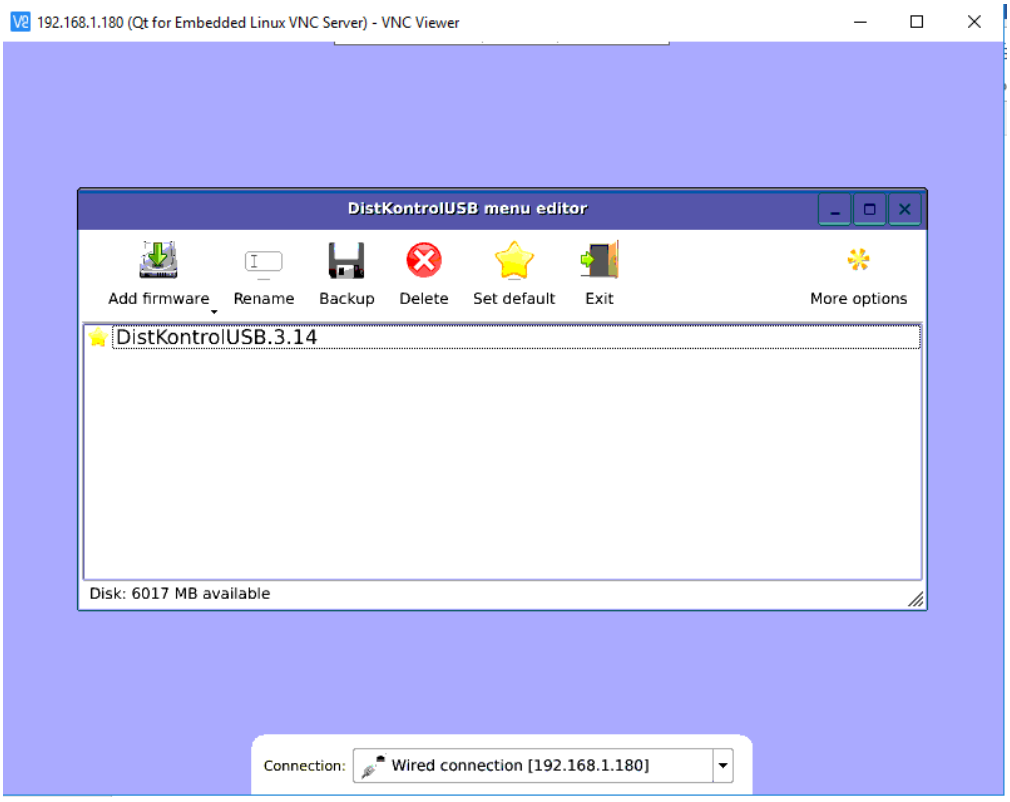
Для сброса настроек необходимо:

Последовательно в меню загрузки и восстановления USBoverIP выбрать:

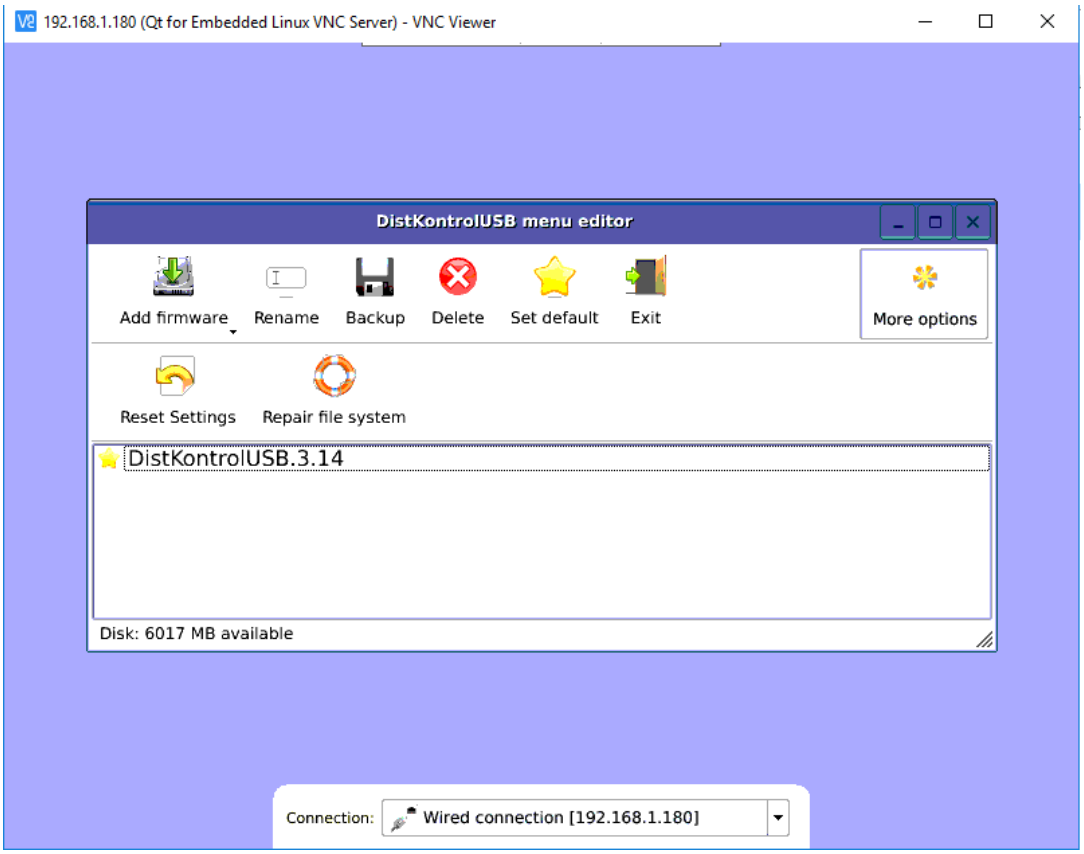
a. «Edit menu»



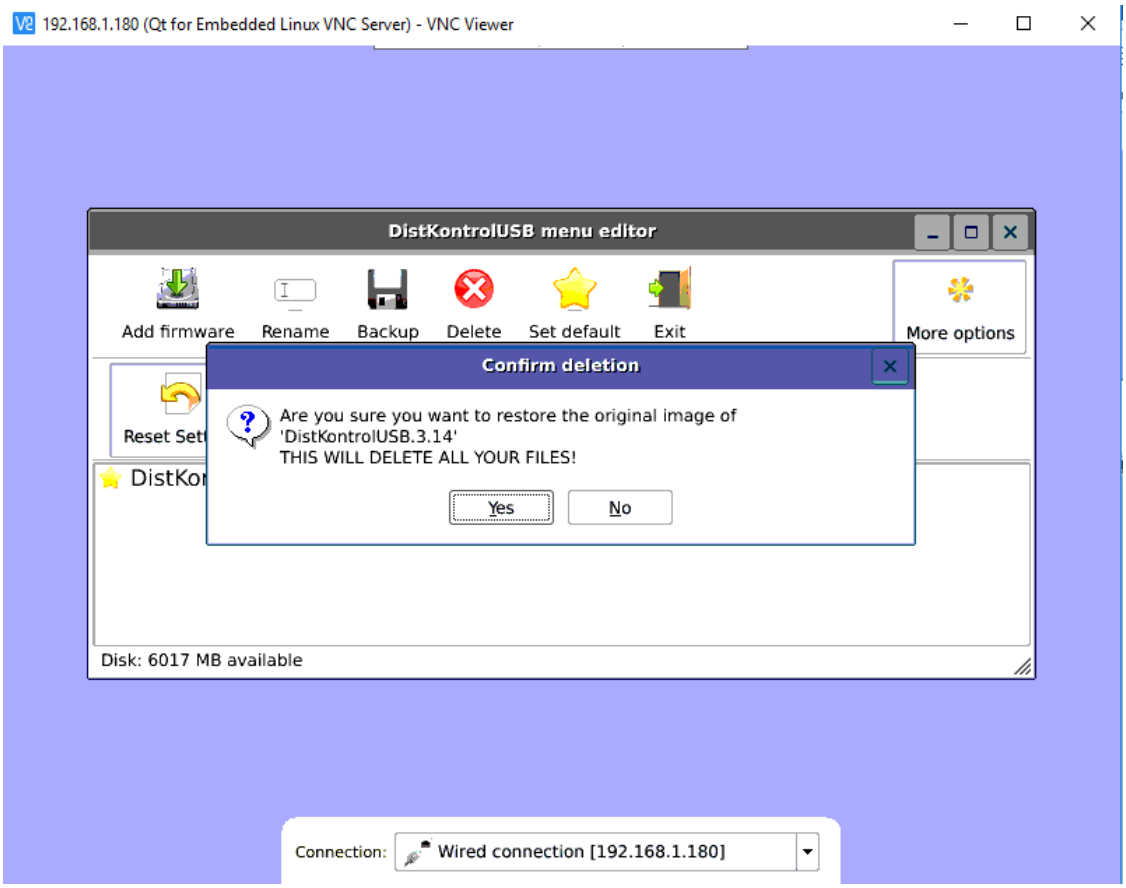
b. «More options»



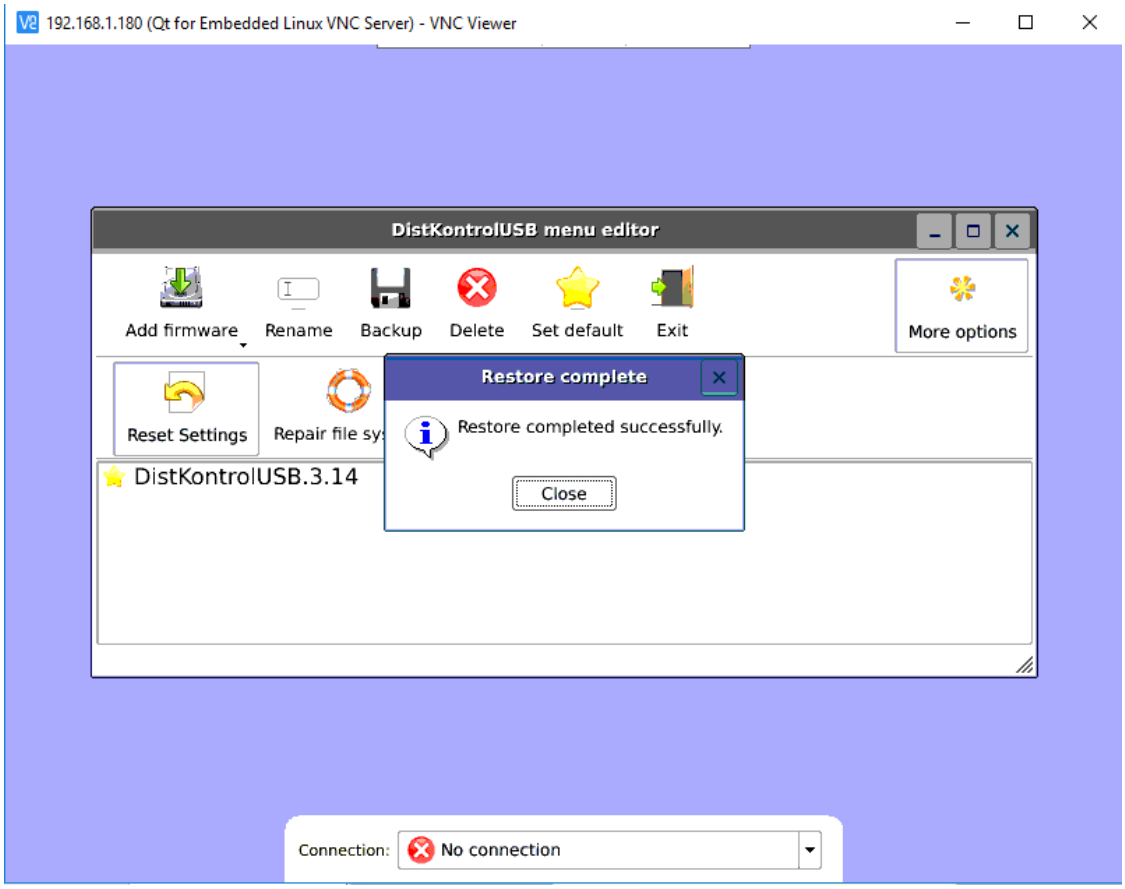
c. «Reset Settings»


192.168.1.180 (Qt for Embedded Linux VNC Server) - VNC Viewer
DistKontrolUSB menu editor
Add firmware
Rename
Backup
Delete
Set default
Exit
More options
Reset Settings
Repair file system
DistKontrolUSB.3.14
Disk: 6017 MB available
Connection:
Wired connection [192.168.1.180]

d. «Yes»


192.168.1.180 (Qt for Embedded Linux VNC Server) - VNC Viewer
DistKontrolUSB menu editor
Add firmware
Rename
Backup
Delete
Set default
Exit
More options
Confirm deletion
Are you sure you want to restore the original image of
'DistKontrolUSB.3.14'
THIS WILL DELETE ALL YOUR FILES!
Yes
No
Disk: 6017 MB available
Connection:
Wired connection [192.168.1.180]

e. «Close» и «Exit»



ВНИМАНИЕ!!! После сброса устройства к исходным установкам и обновления, первая загрузка устройства может осуществляться порядка 5 мин.

После сброса устройства к исходным установкам и обновления потребуется ввод лицензионного ключ к ПО управляемого USB over IP концентратора по изложенной в разделе Лицензия.

4.9 ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

ВНИМАНИЕ!!! При обновлении программного обеспечения, управляемого USB over IP концентратора его настройки, не сохраняются и сбрасываются к исходным. Необходимо, до обновления устройства, выполнить экспорт настроек и их импорт после обновления (см. раздел «Сохранение и восстановление настроек» руководства) или осуществить повторную настройку устройства, при этом потребуется ввод лицензионного ключа к ПО управляемого USB over IP концентратора по методике, изложенной в разделе «Лицензия».

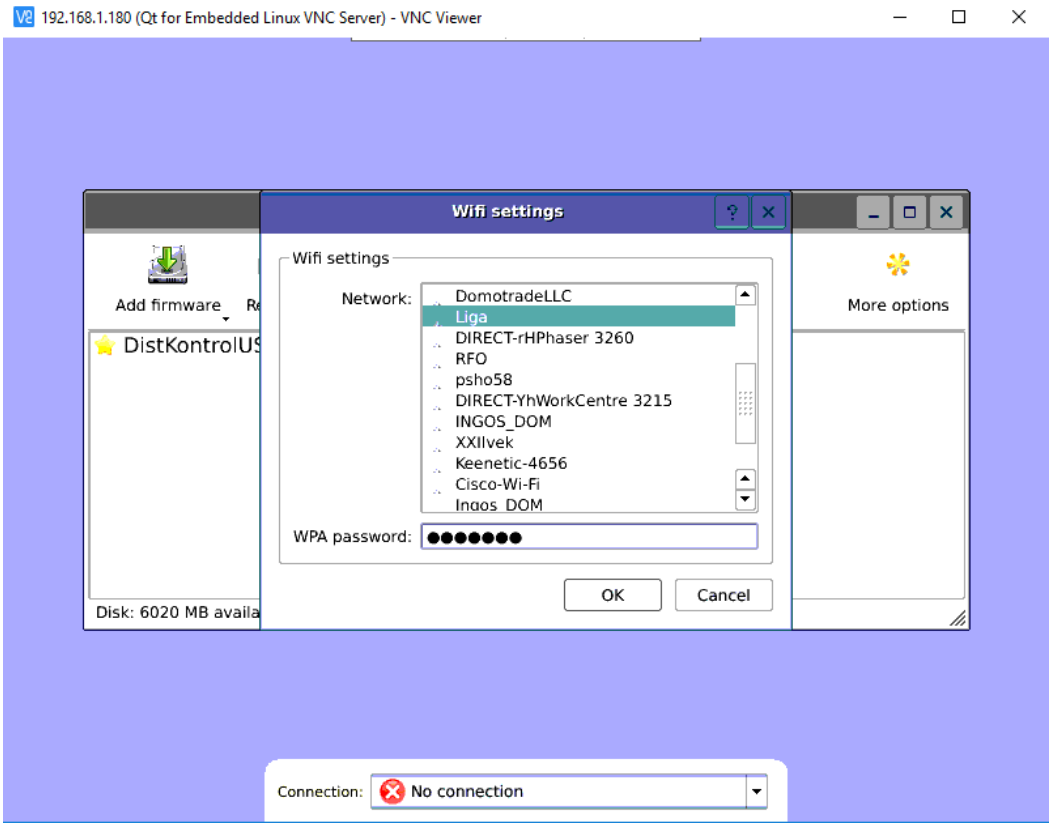
Для обновления программного обеспечения, управляемого USB over IP концентратора необходимо подключиться к нему с помощью VNC по изложенной выше методике.

Обновление возможно двумя способами:

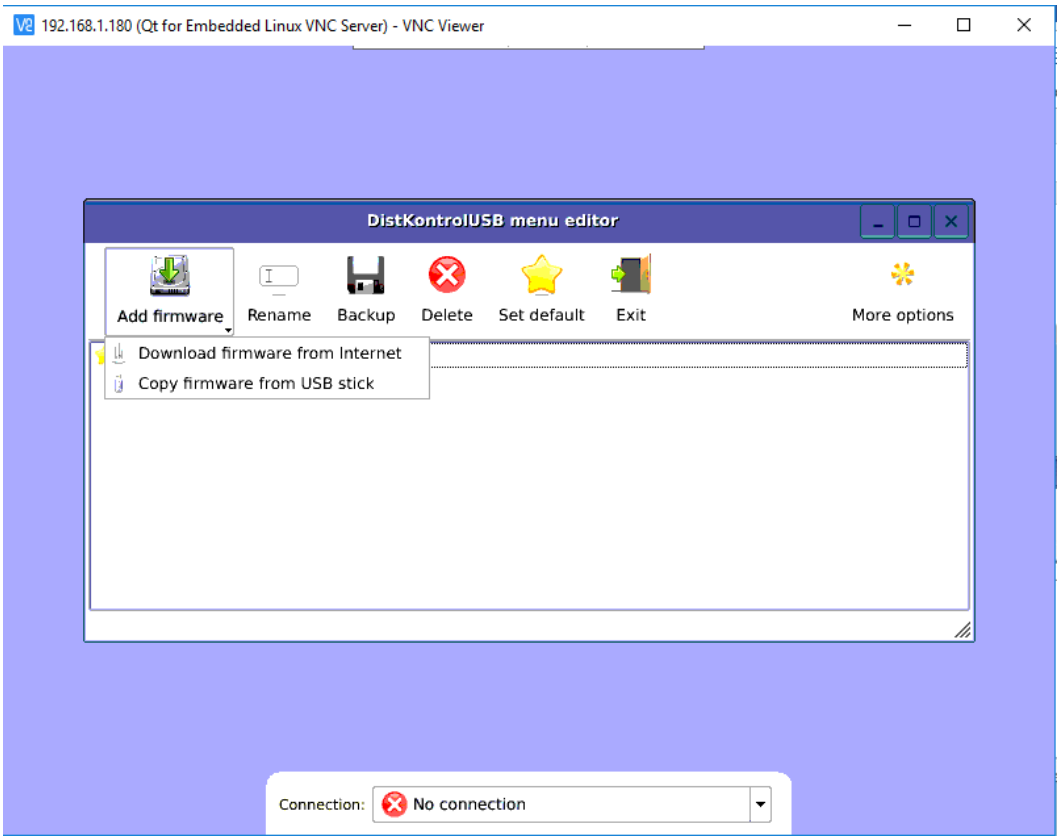
1. Через интернет (рекомендуемый способ обновления).

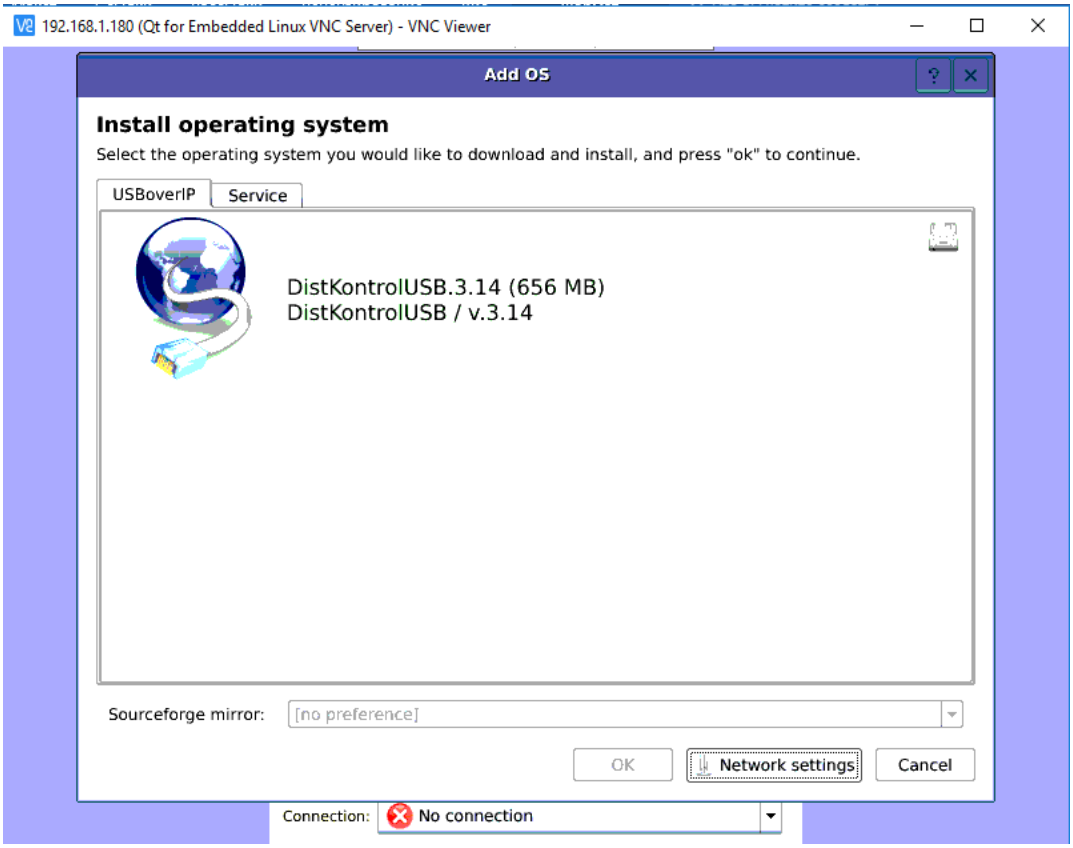
2. С флеш носителя.

1. Для обновления через интернет необходимо обеспечить доступ к глобальной сети с адреса 192.168.1.180 по LAN устройства. Также возможно обновление ПО по WiFi. Для подключения к WiFi необходимо кликнуть по надписи «Wired connection» внизу экрана, выбрать сеть из списка доступных и ввести пароль.

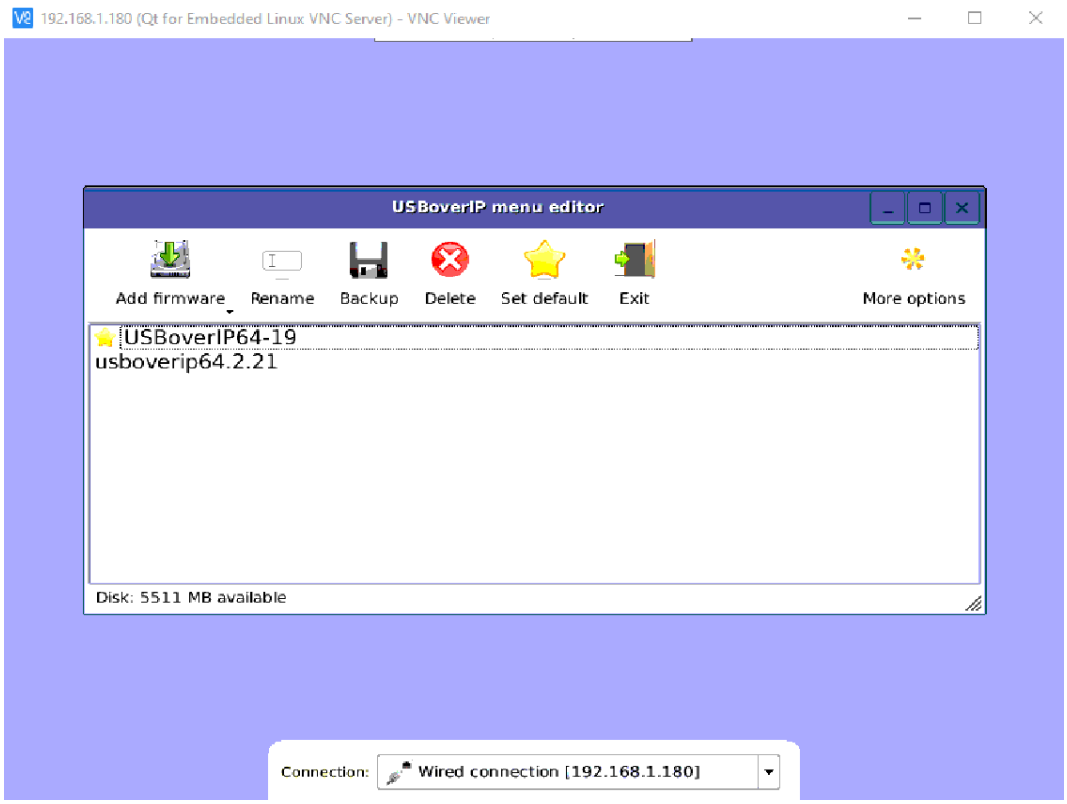


Для начала обновления необходимо последовательно в меню загрузки и восстановления USBoverIP выбрать: «Edit menu» - «Add firmware» и выбрать соответствующий пункт подменю.





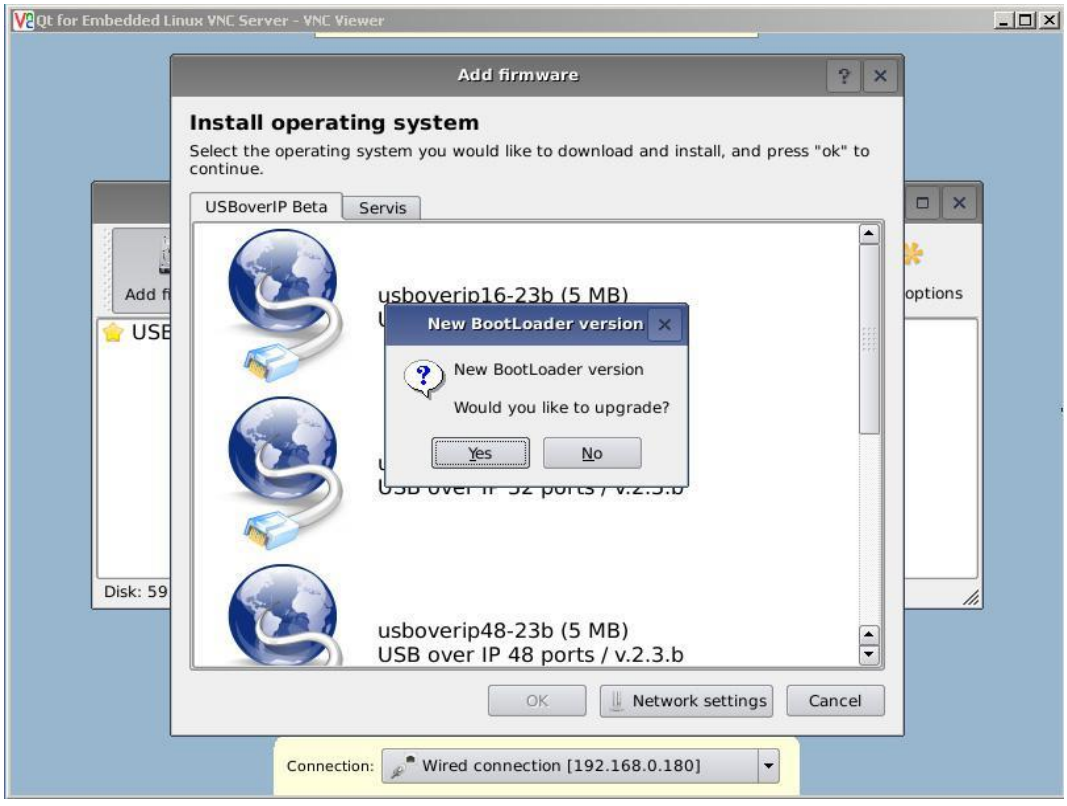
Далее выбрать версию ПО и нажать кнопку OK. Новая версия ПО будет загружена и установлена на устройство.



В случае, если при обновлении устройства вы видите сообщение о наличии новой версии загрузчика, то вначале необходимо произвести обновление ПО загрузчика, нажав на кнопку «YES». Обновление загрузчика возможно только через интернет.

После обновления загрузчика выполните обновление основного ПО устройства.

Если Вы не планируете производить обновление основного ПО концентратора, то обновлять загрузчик не рекомендуется.



2. При плохом канале интернет возможно обновление основного ПО управляемого USB over IP концентратора с помощью флеш носителя.

Для обновления ПО с флеш носителя необходимо:

- Скачать новую версию ПО на странице «Информация» - «Проверить обновления» или по ссылке.
- При обновлении с флеш носителя проверка контрольной суммы файла прошивки не производится. Необходимо самостоятельно проверить контрольную сумму скаченного файла с указанной на странице загрузки обновления.
- Записать на флеш носитель ПО (рекомендуется использовать носители объемом 4 - 16Гб) и подключить носитель в USB порт 1.1. Порт включается автоматически при входе в меню редактирования.
- Для вызова подменю кликнуть **и удержать** кнопку «Add firmware». При выборе соответствующего пункта подменю «Add firmware» откроется диалоговое окно выбора ПО. Необходимо выбрать на флеш носителе записанную версию ПО и нажать кнопку «Open».
- Новая версия ПО будет скопирована и установлена на устройство.

После установки вы увидите новый пункт в списке установленного ПО. Для использования новой версии ПО необходимо выбрать его в меню и нажать на кнопку «Set default», далее «Exit». Будет произведена перезагрузка устройства с новой версией ПО.

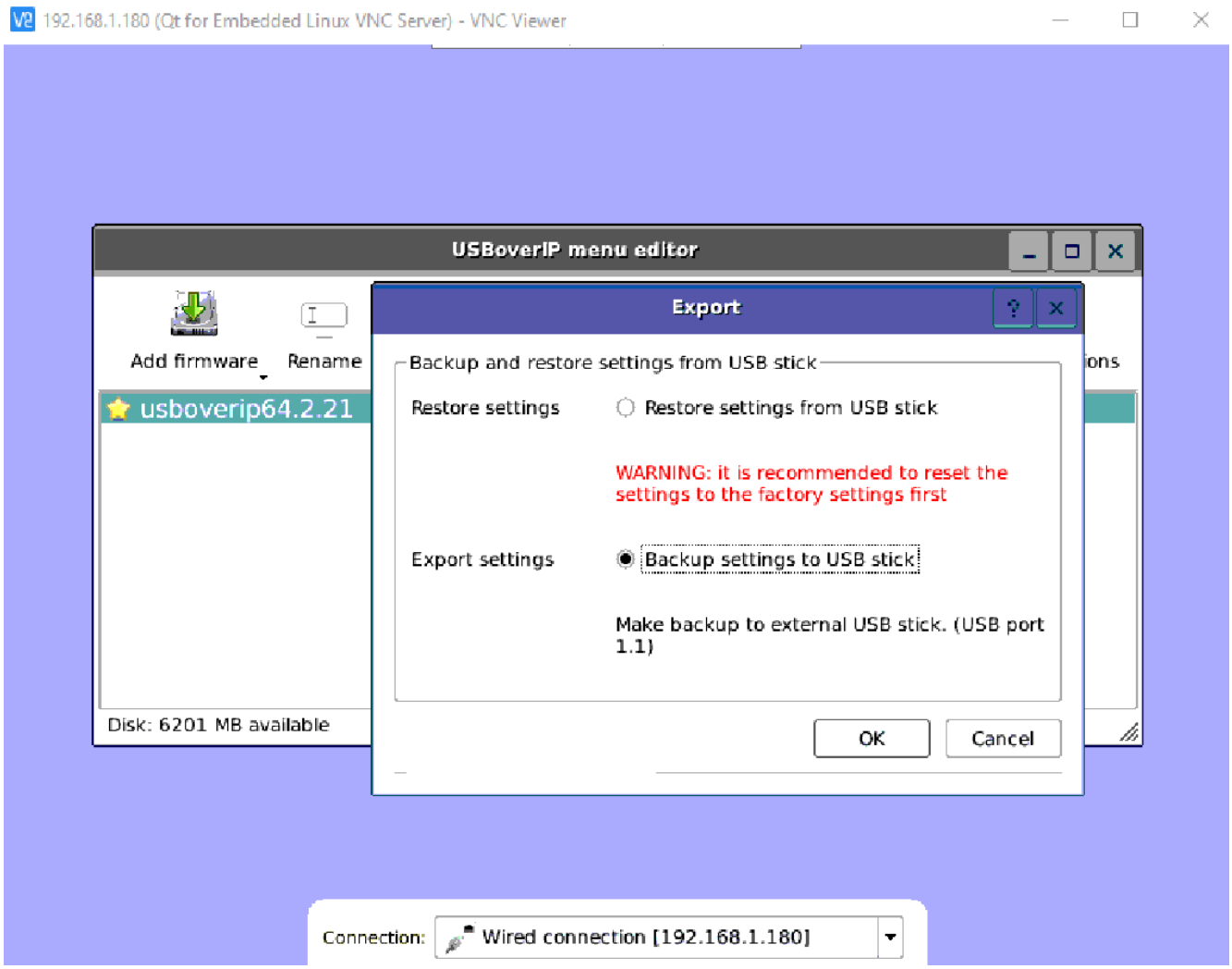
Дополнительно в меню редактирования доступны возможности переименования и удаления не нужных версий ПО.

4.10 СОХРАНЕНИЕ И ВОССТАНОВЛЕНИЕ НАСТРОЕК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

ВНИМАНИЕ!!! Сохранения настроек программного обеспечения, управляемого USB over IP концентратора или их восстановления возможно для версий ПО не ниже 2.21. При необходимости, удаление импортированных настроек, осуществляется простым сбросом настроек управляемого USB over IP концентратора в исходное состояние. Подробнее в «Сброс настроек, управляемого USB over IP концентратора в исходное состояние.»

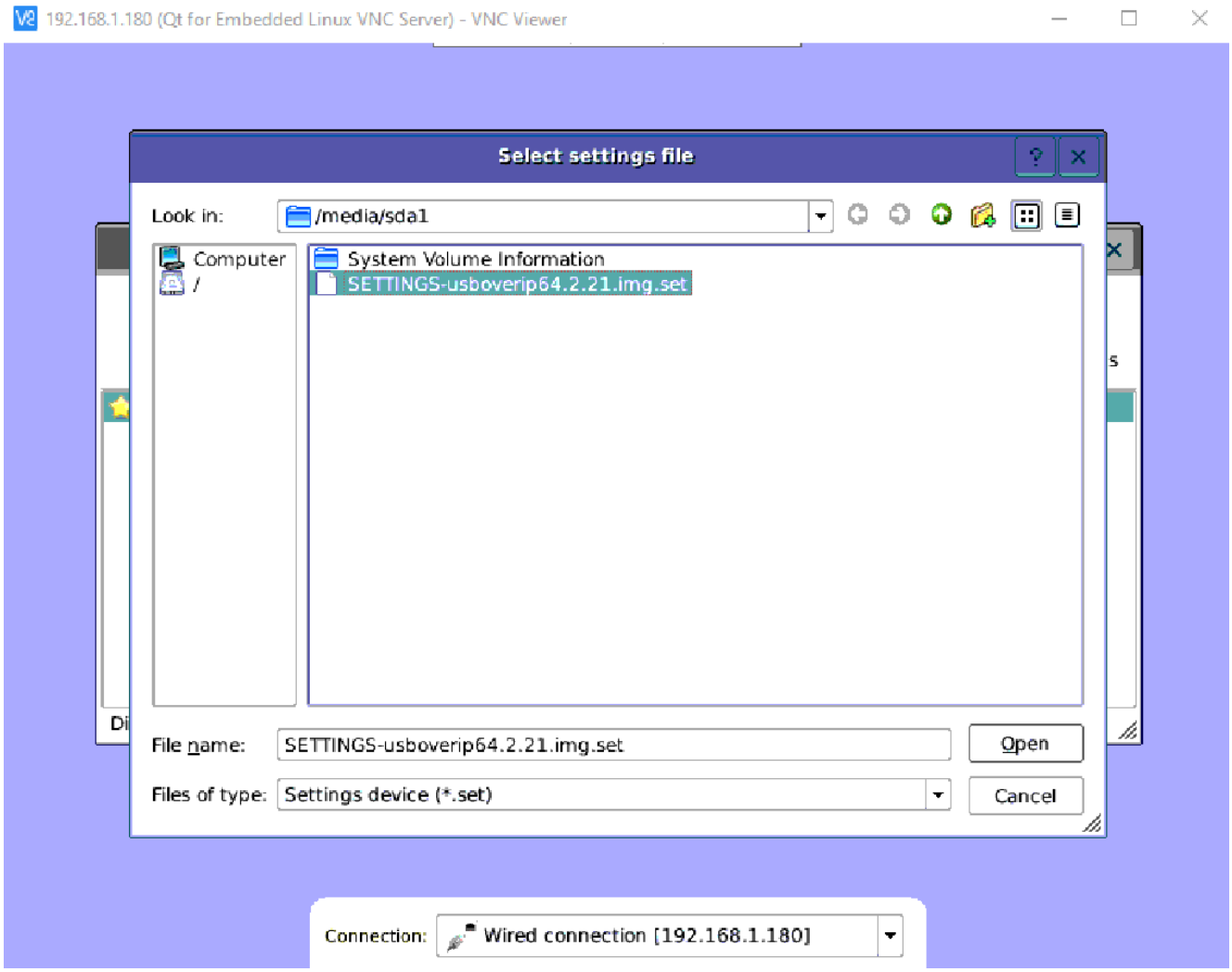
Для сохранения настроек программного обеспечения, управляемого USB over IP концентратора **или их восстановления** необходимо подключиться к концентратору с помощью VNC по изложенной выше методике. В USB порт 1.1 концентратора необходимо подключить флеш носитель (рекомендуется использовать носители объемом 4 - 16Гб) отформатированный в FAT32. Порт включается автоматически при входе в меню редактирования.

Для сохранения настроек программного обеспечения, управляемого USB over IP концентратора необходимо кликнуть кнопку меню «Backup». В открывшемся окне экспорта выбрать «Backup settings to USB stick» и нажать кнопку меню «ОК». Далее подтвердить экспорт настроек и дождаться завершения операции.



Перед восстановлением настроек программного обеспечения, управляемого USB over IP концентратора рекомендуется осуществить сброс настроек управляемого USB over IP концентратора в исходное состояние по методике, изложенной в п. 4.18 Руководства.

Для восстановления настроек программного обеспечения, управляемого USB over IP концентратора необходимо кликнуть по названию прошивки, в которую необходимо экспортировать настройки, далее кликнуть кнопку меню «Backup». В открывшемся окне экспорта выбрать «Restore settings from USB stick» и кликнуть кнопку меню «OK». Далее выбрать файл настроек и дождаться завершения операции.



После завершения восстановления настроек программного обеспечения, управляемого USB over IP концентратора кликнуть кнопку меню «Exit» для перезагрузки концентратора.

4.11 АППАРАТНАЯ ПЕРЕЗАГРУЗКА УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

Для перезагрузки концентратора нажмите и удерживайте кнопку «Reset», расположенную с тыльной стороны устройства, в течении 5 секунд. Концентратор будет корректно перезагружен.

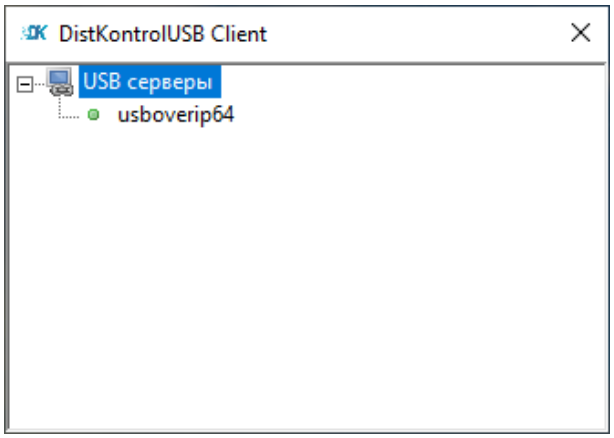
5 КЛИЕНТ DISTKONTROLUSB

5.1 УСТАНОВКА КЛИЕНТА DISTKONTROLUSB

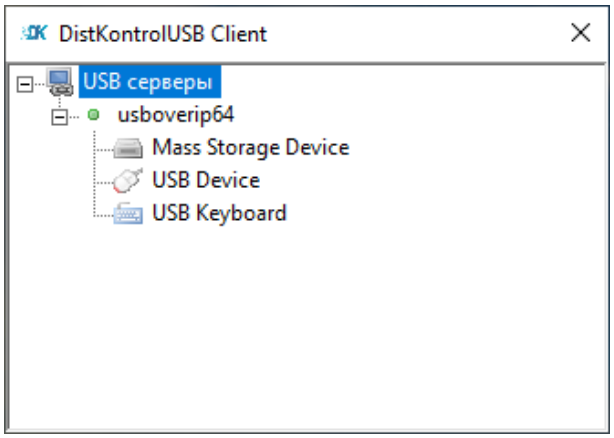
Клиент USB можно скачать с самого устройства подключения USB по сети или с сайта (ссылки на странице Информация - Поддержка).

Необходимо скачать и запустить соответствующее ПО.

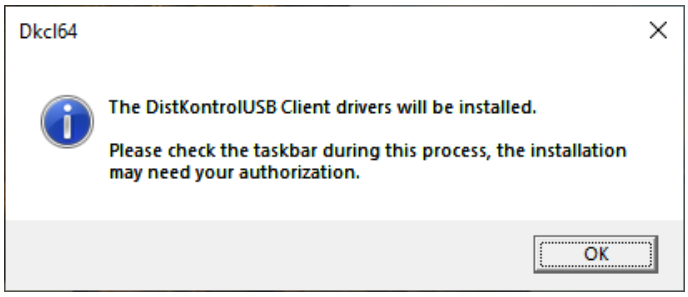
Во время установки появится уведомление центра безопасности Windows. Необходимо разрешить приложению внесение изменений.



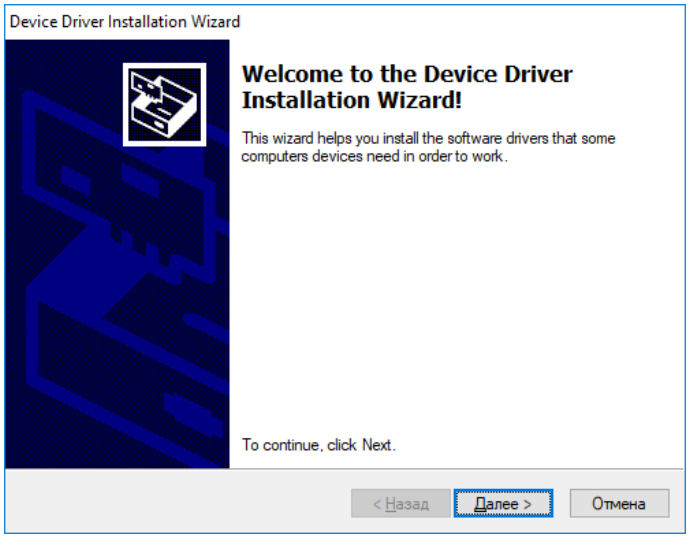
При подключении к USB over IP USB устройств они будут видны в клиенте и их будет можно подключить к компьютеру:



При первом подключении к USB устройству будет предложена установка драйвера USB over IP:



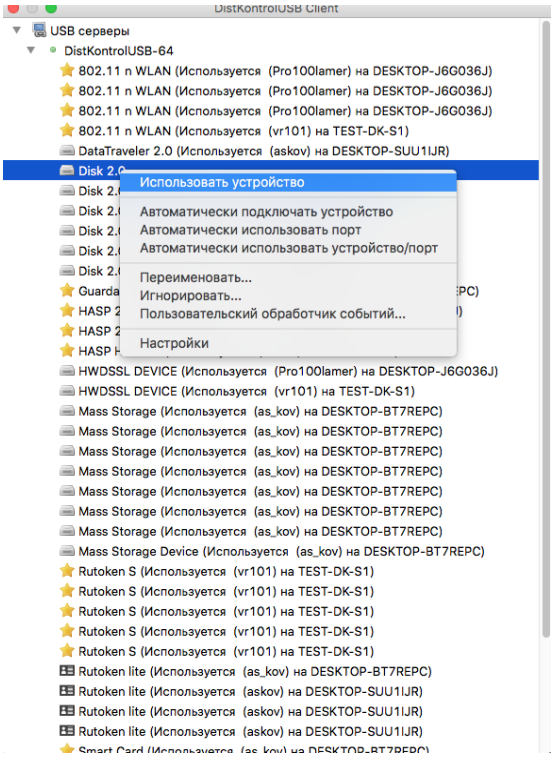
Во время установки появится уведомление центра безопасности Windows. Необходимо разрешить приложению внесение изменений.



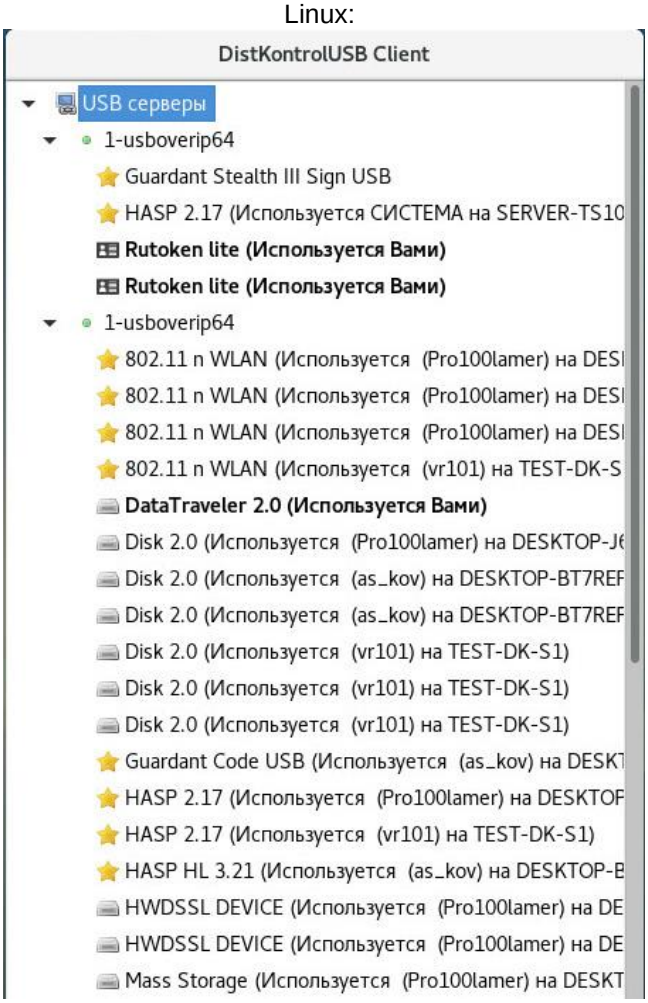
Нажать «Установить».

После запуска отобразится окно USB клиента.

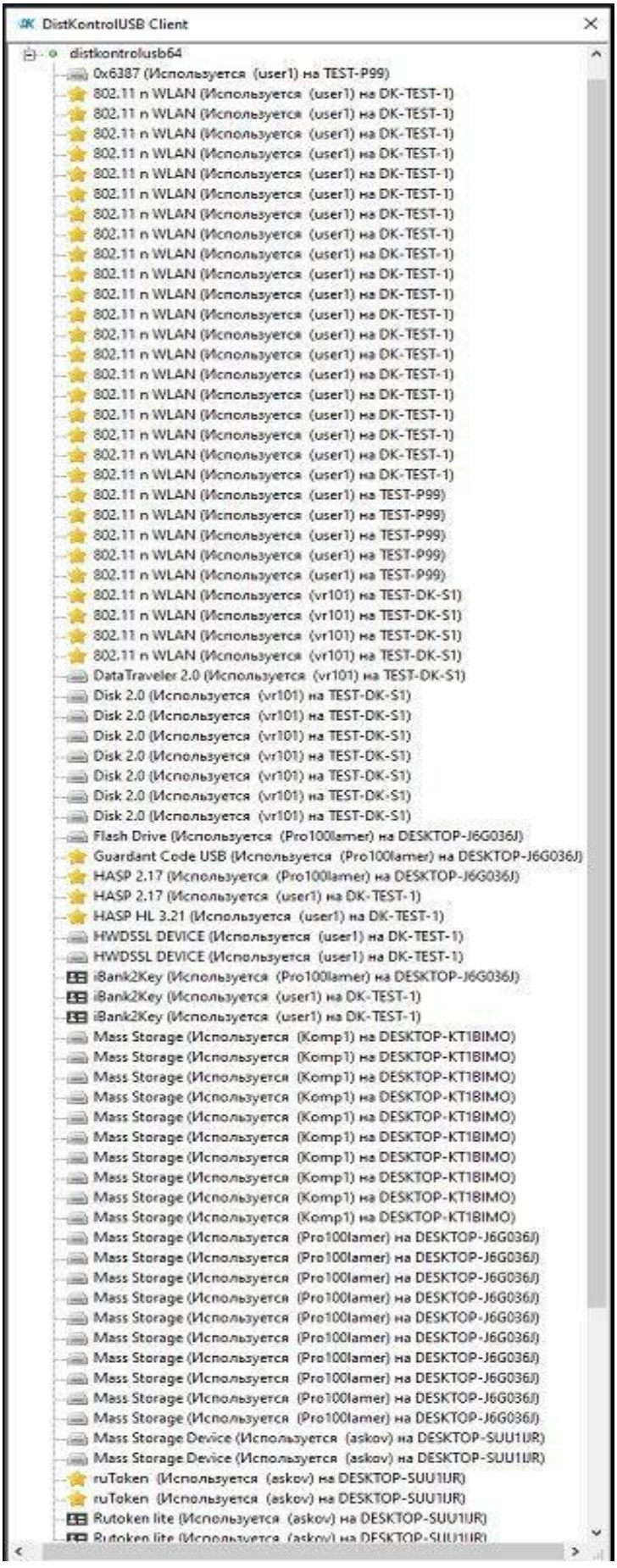
Программное обеспечение автоматически найдет USB-устройства, совместно используемые серверами в сети. Доступные устройства USB будут отображаться в виде дерева. Щелкните правой кнопкой мыши на устройстве, которое вы хотите использовать, и выберите «Использовать». После этого он будет напрямую подключен к вашему компьютеру (машине) и может использоваться как локальное устройство.


DistKontrolUSB Client
USB серверы
DistKontrolUSB-64
802.11 n WLAN (Используется (Pro100lamer) на DESKTOP-J6G036J)
802.11 n WLAN (Используется (Pro100lamer) на DESKTOP-J6G036J)
802.11 n WLAN (Используется (Pro100lamer) на DESKTOP-J6G036J)
802.11 n WLAN (Используется (vr101) на TEST-DK-S1)
DataTraveler 2.0 (Используется (askov) на DESKTOP-SUU1IJR)
Использовать устройство
Автоматически подключать устройство
Автоматически использовать порт
Автоматически использовать устройство/порт
Переименовать...
Игнорировать...
Пользовательский обработчик событий...
Настройки
HWDSSL DEVICE (Используется (Pro100lamer) на DESKTOP-J6G036J)
HWDSSL DEVICE (Используется (vr101) на TEST-DK-S1)
Mass Storage (Используется (as_kov) на DESKTOP-BT7REPC)
Mass Storage Device (Используется (as_kov) на DESKTOP-BT7REPC)
Rutoken S (Используется (vr101) на TEST-DK-S1)
Rutoken lite (Используется (as_kov) на DESKTOP-BT7REPC)
Rutoken lite (Используется (askov) на DESKTOP-SUU1IJR)

Linux:

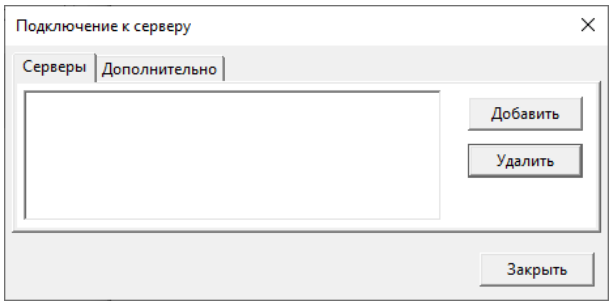

DistKontrolUSB Client
USB серверы
1-usboverip64
Guardant Stealth III Sign USB
HASP 2.17 (Используется СИСТЕМА на SERVER-TS10
Rutoken lite (Используется Вами)
Rutoken lite (Используется Вами)
1-usboverip64
802.11 n WLAN (Используется (Pro100lamer) на DES
802.11 n WLAN (Используется (Pro100lamer) на DES
802.11 n WLAN (Используется (Pro100lamer) на DES
802.11 n WLAN (Используется (vr101) на TEST-DK-S
DataTraveler 2.0 (Используется Вами)
Disk 2.0 (Используется (Pro100lamer) на DESKTOP-J6
Disk 2.0 (Используется (as_kov) на DESKTOP-BT7REF
Disk 2.0 (Используется (as_kov) на DESKTOP-BT7REF
Disk 2.0 (Используется (vr101) на TEST-DK-S1)
Disk 2.0 (Используется (vr101) на TEST-DK-S1)
Disk 2.0 (Используется (vr101) на TEST-DK-S1)
Guardant Code USB (Используется (as_kov) на DESKT
HASP 2.17 (Используется (Pro100lamer) на DESKTOP
HASP 2.17 (Используется (vr101) на TEST-DK-S1)
HASP HL 3.21 (Используется (as_kov) на DESKTOP-B
HWDSSL DEVICE (Используется (Pro100lamer) на DE
HWDSSL DEVICE (Используется (Pro100lamer) на DE
Mass Storage (Используется (Pro100lamer) на DESKT

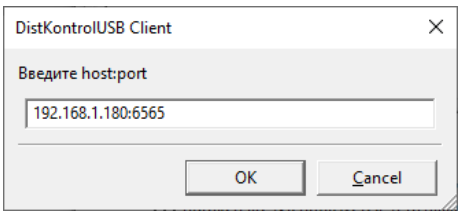
Windows:


DistKontrolUSB Client
distkontrolusb64
0x6387 (Используется (user1) на TEST-P99)
802.11 n WLAN (Используется (user1) на DK-TEST-1)
802.11 n WLAN (Используется (user1) на TEST-P99)
802.11 n WLAN (Используется (vr101) на TEST-DK-S1)
DataTraveler 2.0 (Используется (vr101) на TEST-DK-S1)
Disk 2.0 (Используется (vr101) на TEST-DK-S1)
Flash Drive (Используется (Pro100lamer) на DESKTOP-J6G036J)
Guardant Code USB (Используется (Pro100lamer) на DESKTOP-J6G036J)
HASP 2.17 (Используется (Pro100lamer) на DESKTOP-J6G036J)
HASP 2.17 (Используется (user1) на DK-TEST-1)
HASP HL 3.21 (Используется (user1) на DK-TEST-1)
HWDSSL DEVICE (Используется (user1) на DK-TEST-1)
iBank2Key (Используется (Pro100lamer) на DESKTOP-J6G036J)
iBank2Key (Используется (user1) на DK-TEST-1)
Mass Storage (Используется (Komp1) на DESKTOP-KT1BIMO)
Mass Storage (Используется (Pro100lamer) на DESKTOP-J6G036J)
Mass Storage Device (Используется (askov) на DESKTOP-SUU1IJR)
ruToken (Используется (askov) на DESKTOP-SUU1IJR)
Rutoken lite (Используется (askov) на DESKTOP-SUU1IJR)

DistKontrolUSB Client для Linux устройства аппаратного подключения USB по сети использует встроенный драйвер usbip для Linux. (Рекомендуется использовать ядро (4.9+) для максимальной совместимости).

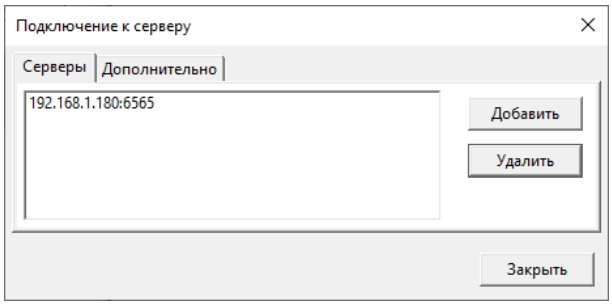
Адрес управляемого USB over IP концентратора можно указать (для использования, например, в глобальной сети), для этого правой кнопкой мыши нажать на USB Hubs и выбрать Specify Hubs.





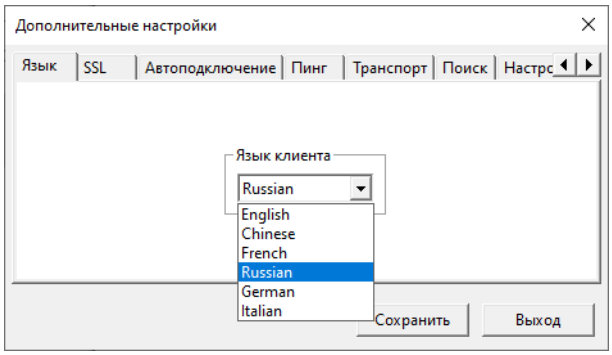
В окне Specify Hubs нажать Add.

Ввести настройки сервера в формате адрес:порт и нажать OK. Порт: 6565 (6564 при использовании SSL). Здесь необходимо указать IP-адрес концентратора.



В окне Specify Hubs нажать Close.

Интерфейс клиента мультиязычный. Для выбора В клиенте:
1. Клик правой кнопкой мыши на USB Habs -> Advanced Setting
2. На вкладке Lenguage выбрать язык интерфейса -> Save

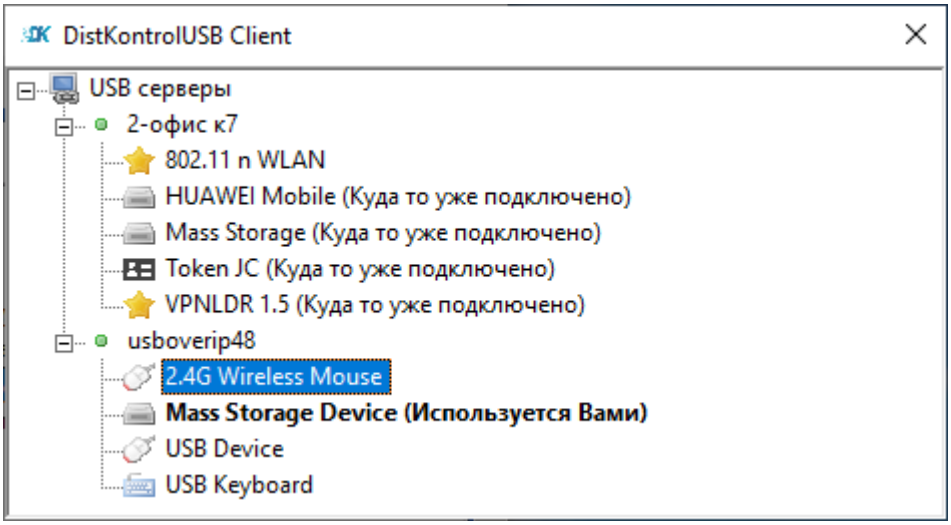


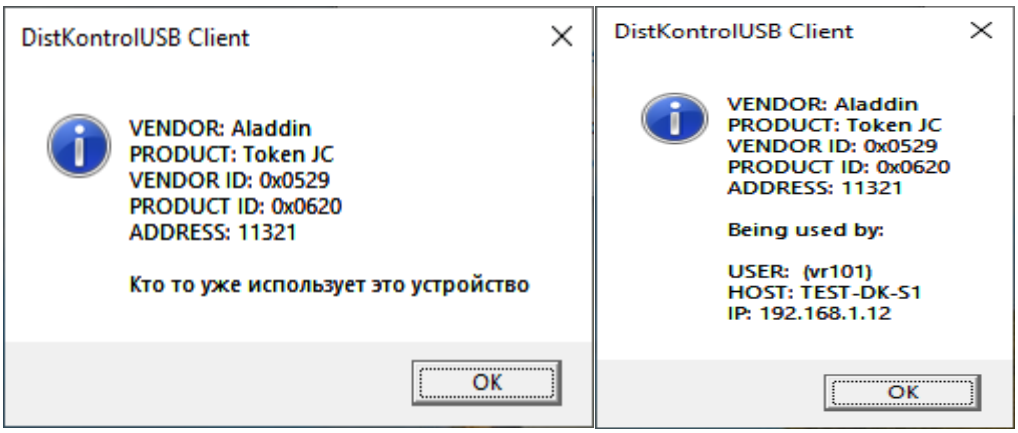
5.2 НАСТРОЙКА КЛИЕНТА DISTKONTROLUSB

5.2.1 УПРАВЛЕНИЕ ОТОБРАЖЕНИЕМ ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЯХ USB УСТРОЙСТВ

Управляемый USB over IP концентратор позволяет включать и выключать отображение информации в клиентском приложении о пользователях, использующих USB устройства.

По умолчанию отображение информации включено. В примере ниже, на USBoverIP64 концентраторе отображение информации включено, на USBoverIP32 концентраторе выключено.





Управление отображением информации о пользователях USB устройств осуществляется в WEB интерфейсе устройства на странице «Сервисы» - «Настройки USB» - «Скрывать информацию о пользователях USB в клиенте» (Для применения, включить и сохранить)

5.2.2 ИЗМЕНЕНИЕ ИМЕНИ USB УСТРОЙСТВА В КЛИЕНТСКОМ ПРИЛОЖЕНИИ.

В клиентском приложении возможно переименовать USB устройства. Правой кнопкой мыши по устройству вызовите окно – Переименовать. Введите желаемое имя – Нажмите Ок. Изменение имени увидят все пользователи. Имя устройства по умолчанию задается по номеру USB порта.

Для ограничения прав на переименования USB устройств настройте права: «Настройки прав»

В WEB интерфейсе устройства на странице «Сервисы» - «Настройки USB» - «Сбросить имя USB-устройств на исходные», возможно сбросить имена на исходные. При сбросе служба будет перезапущена.

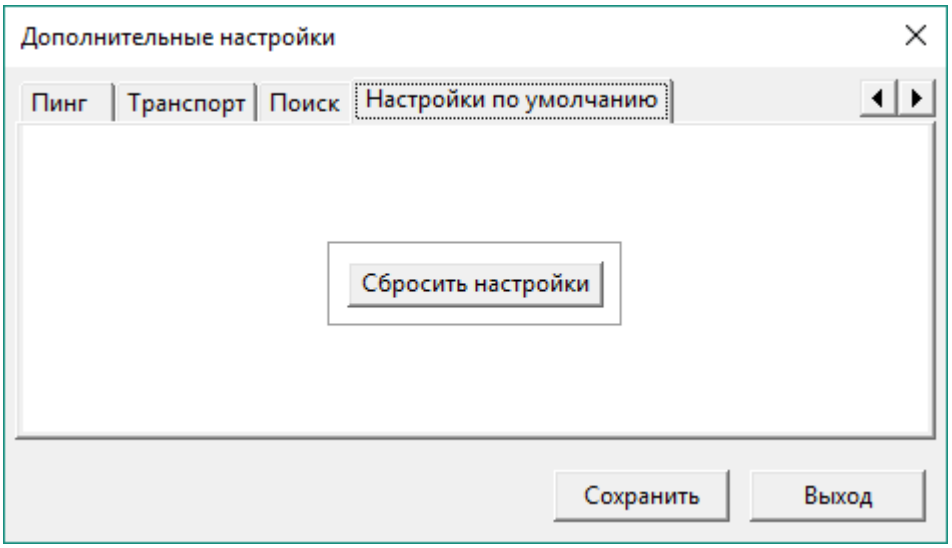
5.2.3 НАСТРОЙКА МЕНЮ КЛИЕНТСКОГО ПРИЛОЖЕНИЯ DISTKONTROLUSB

Клиент сохраняет все свои параметры в одном текстовом файле

Windows: c:\Users\Username\AppData\Roaming\dkcl.ini
OSX : /Users/Username/Library/Preferences/ dkcl Preferences
Linux: ~/. dkcl

Этот файл обновляется при изменении настоек. При первом запуске клиент создает файл конфигурации по умолчанию.

Для сброса ранее сохранённого пароля, необходимо сбросить настройки клиента. Правой кнопкой мыши по “USB серверы” – “Дополнительные настройки”. Вкладка “Настройки по умолчанию” расположена в самом конце.



5.2.4 СБРОС НАСТРОЕК КЛИЕНТСКОГО ПРИЛОЖЕНИЯ DISTKONTROLUSB

Для сброса всех настроек клиентского приложения, в WEB интерфейсе устройства на странице «Сервисы» - «Настройки USB» - «Сбросить параметры службы USB over IP на исходные.» При сбросе служба будет перезапущена.

Будут сброшены номера портов, настройки ssl и отображения скрытых устройств, имена и скрытие устройств.

5.3 ЗАПУСК КЛИЕНТА DISTKONTROLUSB, В КАЧЕСТВЕ СЛУЖБЫ (ДЕМОНА)

В USB-клиент может работать как обычное приложение или в качестве службы (демона). Запуск клиента в качестве службы позволяет совместно использовать устройства, не требуя входа пользователя в систему, клиент будет работать в фоновом режиме непрерывно.

При установке клиента USB в качестве службы он автоматически запускается при загрузке операционной системы и автоматически подключается к любым указанным вами устройствам. Журнал Сообщений можно просмотреть в средстве просмотра событий (под Windows), Console Viewer (под OSX) или tail /var/log/syslog (под Linux).

Чтобы установить USB клиента в качестве службы Windows или OSX:

Щелкните правой кнопкой «USB Hubs->Install Client as a Sevice» (если сервис уже установлен, будет доступно - Uninstall Client Service).

Будет установлен клиент DistKontrolUSB в качестве службы.

При повторном запуске клиента он будет взаимодействовать с запущенной службой в фоновом режиме.

Можно выйти из клиента, и служба клиента будет продолжать работать как обычно в фоновом режиме.

Чтобы установить на USB клиента как демон в Linux необходимо запустить клиент с параметром -n. Это позволит запустить его в режиме демона.

Например: для запуска клиента в фоновом режиме под Ubuntu/Debian используйте:

```
sudo ./dkclientx86_64 -n
```

Для запуска в консольном режиме от имени не привилегированного пользователя демону не нужно использовать sudo, просто запустите в командной строке.

```
./dkclientx86_64 -t "HELP"
```

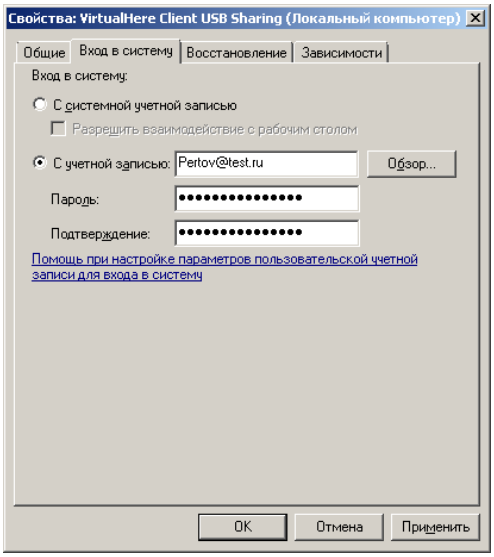
По умолчанию служба запускается от имени пользователя «Система».

Так как режим службы предназначен для фоновой работы (демон), то управление устройств осуществляется не через графический интерфейс клиентского приложения, а с помощью bat файлов (скриптов).

Графический интерфейс, при работе клиента в режиме службы, имеет ограниченный функционал и предназначен в основном для мониторинга подключенных USB устройств.

В терминальном режиме графический интерфейс может быть запущен только для одного из пользователей.Авторизация от имени пользователя возможна двумя способами:

1. Запустить службу от имени пользователя, от которого будет производится подключение USB-устройств:




```
dkcl64.exe -t "USE,USBoverIP64.114,pssword"
```

(pssword - пароль пользователя от имени, которого запущена служба)

2. Указывать в bat файлах, при подключении USB-устройств, соответствующие параметры:

```
dkcl64.exe -t "USE,USBoverIP64.114,user\pssword"
```

(user – имя пользователя **(регистр имеет значение)**, pssword - пароль пользователя)

Запуск клиента в качестве службы имеет дополнительные разрешения (аналогично запуску в графическом режиме с параметром -a). Это удобно, когда пользователям необходимо предоставить возможность отключать используемые другими USB устройства.

Для ограничения прав на отключения пользователей настройте права: «Настройки прав»

5.4 УПРАВЛЕНИЕ КЛИЕНТОМ DISTKONTROLUSB СКРИПТАМИ ИЛИ ИЗ КОМАНДНОЙ СТРОКИ

Клиент USB может управляться скриптами или из командной строки. Это полезно, когда:

- Вы хотите управлять клиентом при запуске в качестве службы
- Вы хотите управлять клиентом только через консольный сеанс, например, ssh
- Вы хотите создать собственный графический интерфейс
- Вы хотите управлять с помощью пакетного файла (Windows) или bash (OSX/Linux) скрипта

Запустите клиент с аргументом -t HELP, чтобы получить список доступных команд.

```
C:\Users\user1> dkcl64.exe -t help


List devices:
   "LIST"
Get the detailed full client state as an XML Document:
   "GET CLIENT STATE"
Use a device:
   "USE,<address>[,password]"
Stop using a device:
   "STOP USING,<address>"
Stop using all devices on all clients:
   "STOP USING ALL"
Stop using all devices just for this client:
   "STOP USING ALL LOCAL"
Rename server:
   "SERVER RENAME,<hubaddress:port>,<new name>"
Turn auto-use all devices on:
   "AUTO USE ALL"
Turn Auto-use all devices on this hub on/off:
   "AUTO USE HUB,<server name>"
Turn Auto-use any device on this port on/off:
   "AUTO USE PORT,<address>"
Turn Auto-use this device on any port on/off:
   "AUTO USE DEVICE,<address>"
Turn Auto-use this device on this port on/off:
```

```
   "AUTO USE DEVICE PORT,<address>"
Clear all auto-use settings:
   "AUTO USE CLEAR ALL"
```

```
Manually specify a hub to connect to:
   "MANUAL HUB ADD,<address>[:port]"
Remove a manually specified hub:
   "MANUAL HUB REMOVE,<address>[:port]"
Remove all manually specified hubs:
   "MANUAL HUB REMOVE ALL"
List manually specified hubs:
   "MANUAL HUB LIST"
Clear client log:
   "CLEAR LOG"
Set a custom device event:
   "CUSTOM EVENT,<address>,<event>"
Turn auto-find off:
   "AUTOFIND"
Shutdown the client:
   "EXIT"
Help:
   "HELP"
```

При успешном выполнении возвращается "OK",

Если сервер не существует, или адрес недействителен - "ошибка: ошибка строка".

Например, в Windows:

Убедитесь, что клиент уже работает в обычном режиме как приложение (отображается в виде зеленого значка USB на панели задач) или как фоновая служба.

```
C:\Users\user1> dkcl64.exe -t list
DistKontrolUSB Client IPC, below are the available devices:
(Value in brackets = address, * = Auto-Use)
USBoverIP16-1 (USBoverIP16:6565)
  --> Mass Storage Device (USBoverIP16.114)
  --> USB Optical Mouse (USBoverIP16.113)
  --> USB Keyboard (USBoverIP16.115)
USBoverIP16 (USBoverIP16:6565)
  --> 3-v3.3 (USBoverIP16.1123)
  --> 2-TokenJC (USBoverIP16.1122)
  --> 1-SmartCard (USBoverIP16.1121)
  --> 10-RutokenLite (USBoverIP16.1143)
  --> 9-RutokenLite (USBoverIP16.1142)
  --> 8-RutokenS (USBoverIP16.1141)
```

```
  --> 14-RutokenS (USBoverIP16.11444)
  --> 13-RutokenS (USBoverIP16.11443)
  --> 12-ruToken (USBoverIP16.11442)
  --> 11-RutokenLite (USBoverIP16.11441)
Auto-Find currently on
Auto-Use All currently off
Reverse Lookup currently off
DistKontrolUSB Client not running as a service
C:\Users\user1>
```

Из этого отчета вы можете видеть клиент подключен к двум USBoverIP концентраторам и имеет 13 подключенных устройств.

Например, 2-TokenJC, подключен к USBoverIP16 по адресу USBoverIP16.1122, чтобы использовать его необходимо в командной строке выполнить

dkcl64.exe -t "USE, USBoverIP16.1122"

и увидеть ответ “OK” в консоли.

Чтобы остановить использование USB-накопителя

dkcl64.exe -t "STOP USING, USBoverIP16.1122"

Чтобы автоматически использовать любое устройство, подключенное к компьютеру:

dkcl64.exe -t "AUTO USE HUB, USBoverIP16:6565"

5.5 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ПРИ РАБОТЕ С КЛИЕНТОМ DISTKONTROLUSB

Клиент управляемого USB over IP концентратора имеет несколько аргументов командной строки, описанных ниже. Чтобы использовать их в Windows, просто вызовите dkcl32.exe <argument> или dkcl64.exe <argument>, в OSX вы должны вызвать непосредственно /Applications/DistKontrolUSB/ DistKontrolUSB.app/Contents/MacOS/dkcl <argument>, в Linux - dkclt64, или dkclientx86_64.

Перечень и назначение аргументов:

-h Справка по командной строке.

-l=<path> Файл для регистрации всех сообщений (вместо регистрации в окне Системные Сообщения.

-c Файл конфигурации для использования вместо файла по умолчанию.

-a Запуск клиент в режиме администратора. Это позволяет клиенту отключать других пользователей от устройств удаленно.

-d установка драйверы клиента и завершение работы. Этот аргумент полезен для выполнения установки в масштабах предприятия по сети через Microsoft Systems Management Server. (При использовании этого аргумента необходимы права администратора).

-x Извлечение драйверов. Это полезно для ручной установки драйверов в Windows XP Embedded.

-i Под Windows и OSX установка клиента в качестве сервиса, (При использовании этого аргумента необходимы права администратора).

-b То же, что и аргумент -i, но установит клиент как сервис с включенным автопоиском устройств по умолчанию.

-u Удаление службы клиента (При использовании этого аргумента необходимы права администратора).

-y Удалить все драйверы USB клиента (если таковые имеются) (При использовании этого аргумента необходимы права администратора).

-t Отправить команду работающему клиенту.

-r=<file> При использовании с аргументом t/x / i / u / d, будет перенаправлять выходные данные в файл, указанный после аргумента. Это полезно для анализа результатов в пакетных файлах в Windows.

5.6 ПРИМЕРЫ УПРАВЛЕНИЯ КЛИЕНТОМ DISTKONTROLUSB ДЛЯ WINDOWS И LINUX

5.6.1 АЛГОРИТМ СОЗДАНИЯ ПАКЕТНОГО ФАЙЛА УПРАВЛЕНИЯ КЛИЕНТОМ ДЛЯ WINDOWS

Запускаем dkcl64.exe как службу или в графическом интерфейсе в Windows.

Запускаем командную строку, переходим в каталог программы.
Набираем

```
dkcl64.exe -t "LIST"
```

Копируем адрес устройства (то, что в скобках).
Например он - USBoverIP16.115, тогда
Для подключения USB устройства

```
dkcl64.exe -t "USE,USBoverIP16.115"
```

Для отключения USB устройства

```
dkcl64.exe -t "STOP USING,USBoverIP16.115"
```

(адрес USB устройства вводится без пробела после запятой)
Для подключения USB порта

```
dkcl64.exe -t "AUTO USE PORT,USBoverIP16.115"
```

Для отключения USB порта

```
dkcl64.exe -t "STOP USING,USBoverIP16.115"
dkcl64.exe -t "AUTO USE CLEAR ALL"
```

(адрес USB устройства вводится без пробела после запятой)

5.6.2 АЛГОРИТМ УСТАНОВКИ И НАСТРОЙКИ ДЕМОНА ДЛЯ LINUX

Пример установки и настройки (для подключения USB устройств с SSL шифрование и авторизацией) **консольного клиента USB over IP концентратора** в качестве демона на Debian (Ubuntu):

Клиента USB over IP концентратора для Linux использует встроенный драйвер Linux usbip. В большинстве версий Linux он включен по умолчанию. Рекомендуется использовать последнее ядро (4.9+) для максимальной совместимости.

Пользователь должен иметь разрешение на sudo для запуска демона. Команды управления демоном выполняются без sudo. (подключаемся по ssh к ОС, создаем пользователя, добавляем его в группу sudo).

IP адрес концентратора 192.168.1.180 из примера - замените на адрес Вашего устройства, пользователя «testuser» и пароль «pass» на соответствующие Ваши.

Скачиваем с концентратора сертификат и консольный клиент:

```
wget --no-check-certificate http:// 192.168.1.180/client /distkontrolusb.pem
wget --no-check-certificate http://192.168.1.180/client/dkclientx86_64
```

Устанавливаем права на клиента и запускаем его в качестве демона:

```
chmod +x ./dkclientx86_64
sudo ./dkclientx86_64 -n
```

Добавляем IP адрес концентратора:

```
./dkclientx86_64 -t 'MANUAL HUB ADD, 192.168.1.180:6565'
./dkclientx86_64 -t 'list'
```

Далее настроим SSL и авторизацию. Включаем SSL шифрование, ограничение доступа к USB порту по логину и паролю и добавляем пользователя в WEB интерфейсе концентратора (см. соответствующие разделы инструкции).

Добавляем в конфигурационный файл клиента путь к сертификату (пользователя «testuser» замените на имя Вашего пользователя):

```
echo "[General]" >> ./.dkcl
echo "SSLCAFile=/home/testuser/distkontrolusb.pem" >> ./.dkcl
cat ./.dkcl
```

Проверяем, в выводе должны присутствовать строки:

```
…..
[Settings]
ManualHubs=192.168.1.180:6564
[General]
SSLCAFile=/home/ testuser /distkontrolusb.pem
.....
```

Перезапускаем демона:

```
sudo ps aux | grep [v]hc
```

Видим:

```
testuser   6345  0.0  1.0  13624 10432 ?        Ssl  17:25   0:00 ./dkclientx86_64 -n
```

Вводим:

```
sudo kill -9 6345
sudo ./dkclientx86_64 –n
```

Проверяем:

```
./dkclientx86_64 -t 'list'
```

Должно быть;

```
DistKontrolUSB Client IPC, below are the available devices:
(Value in brackets = address, * = Auto-Use)
usboverip64 (usboverip64:6565)
 --> Guardant Stealth III Sign USB  (usboverip64.11512)
 --> DataTraveler 410 (usboverip64.11511)
Auto-Find currently on
Auto-Use All currently off
Reverse Lookup currently off
Reverse SSL Lookup currently off
DistKontrolUSB Client is running as a service
```

Подключаем USB-устройство, доступ к порту, которого разрешен для пользователя testuser со стороны устройства:

```
./dkclientx86_64 -t "USE,usboverip64.11512,pass"
```

В выводе должны увидеть:

```
OK
```

USB устройство подключено к ОС с SSL шифрованием и ограничением доступа к USB порту управляемого USB over IP концентратора по логину и паролю.

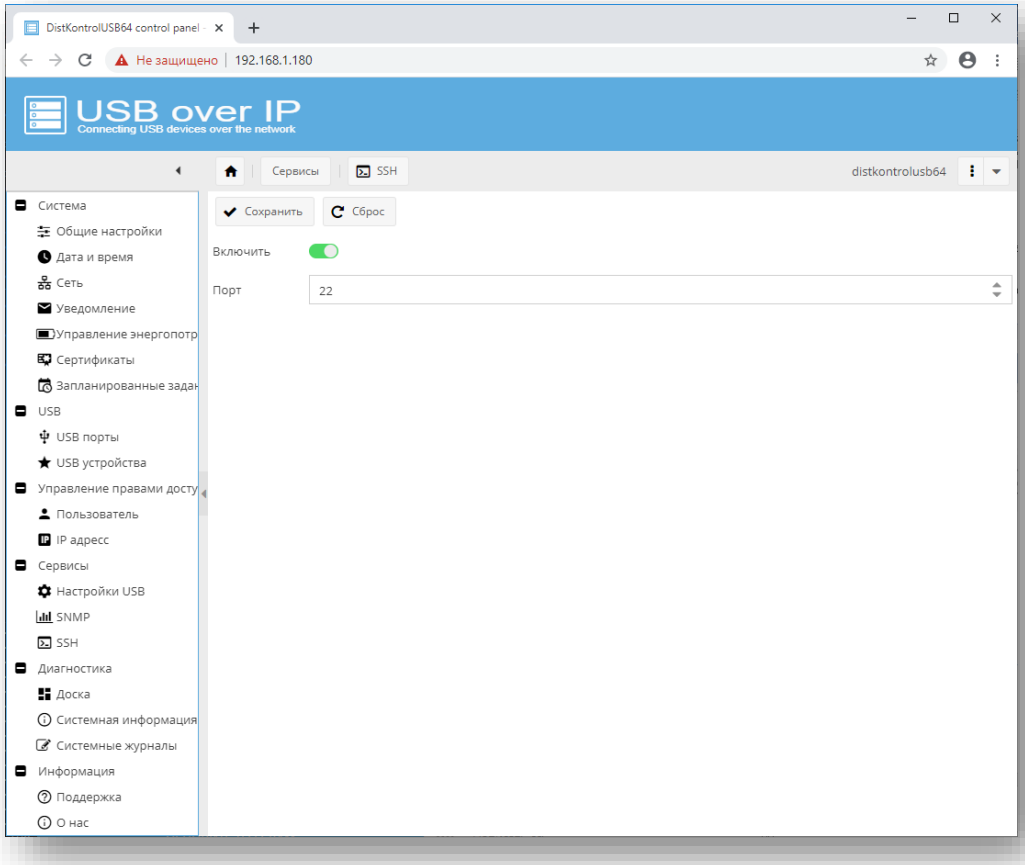
Если в выводе:

```
FAILED
```

Смотрим результат попытки подключения в WEB интерфейсе устройства (подробнее см. Сообщения системы авторизации в разделе Просмотр системного журнала DistKontrolUSB). Анализируем, что сделано не так, вносим коррективы.

6 КРАТКАЯ ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ УТИЛИТЫ УПРАВЛЕНИЯ ПОРТАМИ УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА

Для использования утилиты необходимо включить «API SSH» на странице «Сервисы» - «Настройки USB». Утилита работает с 22 портом.



Общий формат запуска утилиты:

```
usbcontrol.exe ipaddress status UsbPort  pass
```

Все аргументы разделяются пробелами.

В случае запуска утилиты без параметров (без аргументов) на экран будет выведена краткая справка на английском языке.

Описание аргументов:

1) ipaddress - IP-адрес(или сетевое имя) устройства к которому необходимо подключиться;

2) status - "0" или "1". 0 - Выключить USB порт. 1 - Включить USB порт.

3) UsbPort - номер USB порта который необходимо включить/выключить (от 1.1 до 4.16);

4) pass - пароль пользователя usbcontrol (задается в WEB интерфейсе: Управление правами доступа - Пользователь - usbcontrol)

Пример:

```
usbcontrol.exe 192.168.1.180 1 3.12 TestPass
```

(Включить USB порт № 3.12)

Пример запуска в bat файле: см. usbcontrol.bat

ВНИМАНИЕ!!! Пароль пользователя usbcontrol передается на устройство безопасным способом, но его хранение в файлах скриптов управления не безопасно. Необходимо принимать дополнительные меры по обеспечению безопасности используемых Вами скриптов, приложений и т.д.

Так же возможно самостоятельна написать скрипт управления портами USB по ssh. Подключение возможно от пользователя «usbcontrol». Пароль задается при редактировании прав пользователя. Доступны команды:

```
q  (выход)
usbcontrolapi status UsbPort
```

Описание аргументов:

1) status - "0" или "1". 0 - Выключить USB порт. 1 - Включить USB порт.

2) UsbPort - номер USB порта который необходимо включить/выключить (от 1.1 до 4.16);

Пример:

```
usbcontrol@192.168.1.180's password:
> ucbcontrol-api 1 3.15
Status OK. USB port: 3.16 Status: 1
```

7 ВАРИАНТ ИСПОЛЬЗОВАНИЯ, УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

Управляемый USB over IP концентратор не является абсолютный средством обеспечения безопасности при подключении USB устройств по сети. Необходимо его использование сочетать с дополнительными организационными и техническими мерами обеспечения информационной безопасности.

Возможный сценарий использования:

Задача: организация доступа к USB устройствам:

- из региональных офисов (условно NET №1 …… NET № N),
- для ограниченного ряда компьютеров и ноутбуков, подключающих USB устройства через глобальную сеть,
- для пользователей, опубликованных на терминальных серверах приложений.

1. Организационные меры безопасности.

Управляемый USB over IP концентратор установлен в качественно закрывающийся на ключ серверный шкаф. Физический доступ к нему упорядочен (СКД в само помещение, видеонаблюдение, ключи и права доступа у строго ограниченного круга лиц).

Все используемые в организации USB устройства условно разделены на 3 группы:

- Критичные. Финансовые ЭЦП – используются в соответствии с рекомендациями банков (не через USB over IP)
- Важные. ЭЦП для торговых площадок, услуг, ЭДО, отчетности и т.д., ряд ключей для ПО — используются с применением управляемого USB over IP концентратора.

- Не критичные. Ряд ключей для ПО, камеры, ряд флеш носителей и дисков с не критичной информацией, USB модемы — используются с применением управляемого USB over IP концентратора.

2. Технические меры безопасности.

Сетевой доступ к управляемому USB over IP концентратору предоставляется только внутри изолированной подсети. Доступ в изолированную подсеть предоставляется:

- с фермы терминальных серверов,
- по VPN (сертификат и пароль) ограниченному количеству компьютеров и ноутбуков, по VPN им выдаются постоянные адреса,
- по VPN туннелям, соединяющим региональные офисы.

На самом управляемом USB over IP концентраторе DistKontrolUSB с использованием его штатных средств настроены функции:

- Для доступа к USB устройствам USB over IP концентратора используется шифрование (на концентраторе включено шифрование SSL).
- Настроено «ограничение доступа к USB устройствам по IP адресу». В зависимости от IP адреса пользователю предоставляется или нет доступ к назначенным USB устройствам.
- Настроено «Ограничение доступа к USB порту по логину и паролю». Соответственно пользователям назначены права на доступ к USB устройствам, т.к. все USB ключи подключены к USB over IP концентратору стационарно и из порта в порт не переставляются.
- Физическое включение и выключение USB портов осуществляется:
    - Для ключей от программного обеспечения и ЭДО — с помощью планировщика задач и назначенных заданий концентратора (ряд ключей запрограммировали на включение в 9.00 и отключение в 18.00, ряд с 13.00 до 16.00);
    - Для ключей от торговых площадок и ряда программного обеспечения – имеющими разрешение пользователями через WEB интерфейс;
    - Камеры, ряд флеш носителей и дисков с не критичной информацией – включены всегда.

8 ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

8.1 ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ ПО НАСТРОЙКЕ USB OVER IP КОНЦЕНТРАТОРА.

Интересует возможность работы устройства с ключами на нескольких ВМ и ПК – одновременно (Возможно ли одновременное подключение usb устройства к двум компьютерам).

К концентратору одновременно может быть подключено любое количество компьютеров. Использование одного usb устройства одновременно несколькими хостами не допускает протокол USB. Т.е. в одну единицу времени одним портом может пользоваться один компьютер, при этом пользоваться концентратором могут неограниченное количество компьютеров. Ограничения заложены в самом протоколе (спецификации) USB.

Например, пользователь 1 подключил порт 1.1 для того, чтобы пользователь 2 подключил порт 1.1, необходимо пользователю 1 отключить порт 1.1. Если пользователю 2 необходимо подключить порт 1.2, он может это сделать, не мешая работе пользователя 1.

Какое максимальное количество USB устройств можно подключить к одному компьютеру, ноутбуку.

К одному хосту теоретически можно подключить максимум 127 usb устройств, включая сами хабы и внутренние USB устройства. Ограничено спецификациями USB и разрядностью шины. На практике, в зависимости от оборудования и операционной системы может быть значительно меньше.

Какое максимальное количество USB устройств можно подключить к концентратору DistkontrolUSB.

Концентратор сертифицирован для работы с заявленным в зависимости от модели (количества USB портов 16, 32, 48, 64) количеством USB устройств. При определенных обстоятельствах, стандартная модель концентратора может работать с 120 usb устройствами. Возможно изготовление специализированной модели концентратора с поддержкой подключения до 150 или 230 usb устройств.

Получили устройство. При подключении управляемого USBoverIP концентратора патчкордом к ноутбуку он не пингуется и нельзя зайти в WEB интерфейс.

Подключите устройство и ноутбук через сетевой коммутатор.

Получили устройство. Почему я не могу подключить USB-устройство по сети к своему компьютеру через управляемый USB over IP концентратор DistKontrolUSB?

Убедитесь, что USB-устройство исправно функционирует при подключении к компьютеру через USB-кабель. Если для USB-устройства, такого как USB-принтер или многофункциональное устройство, необходим драйвер, убедитесь, что он был установлен на используемом компьютере. Перезагрузка компьютера после установки драйвера USB-устройства также может помочь. Несмотря на то, что управляемый USB over IP концентратор может работать с очень широким спектром USB-устройств, не гарантируется его работоспособность с абсолютно всеми USB устройствами.

Получили устройство. В комплекте только паспорт на изделие. Где можно найти инструкцию?

Всю документацию и ПО можно скачать с сайта.

Управляемый USB over IP концентратор. Руководство пользователя

Управляемый USB over IP концентратор. Буклет

Управляемый USB over IP концентратор. Паспорт

Управляемый USB over IP концентратор. Сертификат соответствия ГОСТ Р

Управляемый USB over IP концентратор. Сертификат соответствия требованиям пожарной безопасности

Управляемый USB over IP концентратор. Нотификация Центра по лицензированию, сертификации и защите государственной тайны ФСБ России

Управляемый USB over IP концентратор. Отчет о внесении в Единый реестр нотификаций Центром по лицензированию, сертификации и защите государственной тайны ФСБ России

Управляемый USB over IP концентратор. Евразийская Экономическая Комиссия. Единый реестр нотификаций о характеристиках шифровальных (криптографических) средств и товаров, их содержащих

Управляемый USB over IP концентратор. Декларация о соответствии требованиям ЕАС

Управляемый USB over IP концентратор. РОСАККРЕДИТАЦИЯ

Управляемый USB over IP концентратор. Цены

Управляемый USB over IP концентратор. Оплата и доставка

Получили устройство. В комплекте только паспорт на изделие, но в нём не указан заводской IP адрес устройства и логин/пароль. Где мне их можно найти?

По умолчанию устройство подключения USB по сети имеет:

Статический IP адрес – 192.168.1.180

Логин к панели WEB интерфейса – admin

Пароль к панели WEB интерфейса – admin

Порт подключения клиентов – 6565 (по умолчанию)

SSL порт подключения клиентов – 6564 (при включенном режиме)

Интерфейс WiFi (wlan0) – отключен

Получили устройство. Почему после установки я не вижу никаких серверов в списке клиента управляемого USB over IP концентратора DistKontrolUSB?

Убедитесь, что управляемый USB over IP концентратор корректно подключен к сети. Некоторые антивирусные программы также могут использовать межсетевой экран, не позволяющий программе настройки управляемого USB over IP получить доступ к сети. Убедитесь, что клиентское приложение управляемого USB over IP концентратора не блокируется антивирусной программой.

Проблема при работе с ключами СберБанка VPN-Key-TLS в терминальной сессии. Ключ подключен к USBoverIP концентратору, на клиентской машине (виртуальная машина на Windows) он виден, но после запуска выдаёт следующую ошибку: "ошибка не удается открыть infocrypt hwdssl device"

Система работы с токенами VPN-Key-TLS предусматривает защиту от удаленного обращения к ключу, поэтому если попытаться запустить ключ из удаленного рабочего стола (когда ключ вставлен в сервер, а запустить его пытается клиент RDP), то будет выдаваться эта ошибка, и ключ работать не будет.

Выходы:

1. Подключать ключ к клиенту по usboverip и после этого подключаться к серверу терминалов.

2. Или использовать не RDP, а программы типа VNC, Radmin и подобные для консольного доступа.

Для Вашей схемы подключения VPN-Key-TLS рекомендуем:

1. Подключить ключ по USB over IP к ПК клиента (в свойствах подключения разрешить подключение портов и дисков (или диска Infocrypt HWDSSL)).

2. Подключиться к серверу по RDP

3. Открыть диск соответствующий диску Infocrypt HWDSSL

4. Запустить start.exe

Процесс подключения или его часть можно автоматизировать скриптом:

1. Подключаемся к серверу VPN.

2. Включаем питание USB порта.

3. Подключаем ключ

4. Подключаемся к серверу RDP

5. Работаем

6. По завершении сессии RDP отключаем питание USB порта.

Так же, для обеспечения безопасности, рекомендуется принять дополнительные меры (VPN канал, авторизация и т.д.)

Проблема при подключении ключа СберБанка VPN-Key-TLS в консольной сессии.

1. Удалите на сервере (компьютере) все драйвера токена

2. Перезагрузите сервер (компьютер)

3. Подключите к серверу (компьютеру) токен через USB over IP

4. Произведите установку драйверов

Токен Сбербанка имеет некоторое кол-во проблем с ОС, но именно с ОС. Как правило, хватает описанных выше действий.

Дополнительно см.:

https://www.amicon.ru/forum/threads/vpn-key-tsl-%D0%B8-win10.1921/

При подключении через концентратор DistKontrolUSB устройства USB, сможет ли ОДНОВРЕМЕННО работать несколько компьютеров с ним?

Одновременно работать нескольким устройствам (ПК) с одним устройством USB невозможно. Протокол USB 2.0 этого не допускает.

Ключ может быть доступен любому кол-ву ПК и переключаться между ними вручную или автоматизировано.

Как использовать один сертификат SSL на нескольких концентраторах?

В разделе «Система» - «Сертификаты» необходимо ИМПОРТИРОВАТЬ сертификат на все концентраторы как указано в инструкции «Параметры клиентского приложения».

Скаченный сертификат с любого устройства будет работать для всех устройств, на которых импортирован один и тот же сертификат.

8.2 ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ ПО НАСТРОЙКЕ КЛИЕНТСКОГО ПРИЛОЖЕНИЯ USB OVER IP КОНЦЕНТРАТОРА.

1. При включенной авторизации не запрашивается пароль для подключения к USB устройству (порту). В системном журнале результат подключения записывается:

```
…
…. logger: Password AUTH_DEVICE (или AUTH_PORT) OK: …
….
```

При подключении к USB устройству (порту) в клиентском приложении поставлена галочка «Запомнить пароль», см. п. «Настройка клиентского приложения, управляемого USB over IP концентратора»

2. При включенной авторизации, устройства USB видны в клиентском приложении, но при подключении они не подключаются. В системном журнале результат подключения записывается:

```
…
…. logger: Password AUTH_DEVICE BAD (или AUTH_PORT): …
….
```

При подключении к USB устройству (порту) в клиентском приложении поставлена галочка «Запомнить пароль» и произведено подключение к USB устройству. Далее пароль пользователя был изменен, но автоматически передается старый. Необходимо закрыть приложение (не свернуть, что является действием по умолчанию при нажатии на “крестик” в правом верхнем углу интерфейса программы). Внести изменения в файл настроек клиентского приложения см. п. «Настройка клиентского приложения управляемого USB over IP концентратора» (можно просто удалить файл настроек для сброса всех настроек клиентского приложения к исходным) Если необходимо удалить запомненный пользователем пароль, то нужно удалить из файла строку вида (будет отличаться после знака «равно»):

```
[General]
...
PresavedPasswords=000000006c9449a7.11212,11111
...
```

3. Клиентское приложение не работает на ОС Linux. Выдается сообщение: "USBIP client drivers are not available, you will have to compile/install your own from the linux kernel source"

Наиболее вероятно, в ядре отсутствует usbip.

Проверить можно:

```
modprobe vhci_hcd
...
lsmod | grep vhci
```

Большинство версий Linux уже скомпилированы с usbip, однако иногда требуется перекомпиляция ядра с их поддержкой. (make menuconfig и выбрать Drivers - >USBIP проверить включено ли, а затем пересобрать ядро kernel make)

4. Можно ли настроить меню клиента? В клиентском приложении не нужен какой-то пункт меню.

Да, можно. Клиент сохраняет все свои параметры в одном текстовом файле:

Windows: c:\Users\Username\AppData\Roaming\dkcl.ini

OSX : /Users/Username/Library/Preferences/dkcl Preferences

Linux: ~/.dkcl

Этот файл обновляется при изменении настоек и обычно не должны быть изменены конечным пользователем. При первом запуске клиент создает файл конфигурации по умолчанию. Для скрытия элементов меню в клиенте необходимо:

1. Выйти из клиента.

2. Отредактировать файла c:\Users\\AppData\Roaming\dkcl.ini (для Windows)

3. В [General] разделе добавить строку HideMenuItems и указать точное название пунктов меню,разделенных запятыми, которые должны быть скрыты.

```
[General]
...
HideMenuItems=Specify Hubs...,Install Client as a Service,ServerMenu^Properties,DeviceMenu^Properties
...
```

5. Можно ли добавить номера портов в список устройств клиентского приложения? Сейчас, если подключено несколько устройств (особенно одного наименования), то очень неочевидно какое устройство нужно использовать конкретному клиенту

Да. Переименовываете (подключая поочередно) USB устройства и сможете использовать просто названия (при желании в названии можно использовать номера портов).

6. Не получается переименовать USB устройство в клиентском приложении.

Обновите ПО устройства до последней актуальной версии. Скачайте последнюю версию клиента с сайта. Ссылки для скачивания доступны в Web интерфейсе в разделе “Поддержка”

7. Как запустить DistKontrolUSB Client в виде сервиса systemctl (Debian 9+ / Ubuntu 18.04 Server+) при старте системы

1. SSH к вашей ОС

wget http://www.distkontrol.ru/usbclient/dkclientx86_64

(или wget http://www.distkontrol.ru/usbclient/dkclienti386 в зависимости от разрядности ОС)

2. sudo chmod +x ./dkclientx86_64

3. sudo mv dkclientx86_64 /usr/sbin

4. Создайте текстовый файл

nano /etc/systemd/system/dkclient.service

со следующим содержимым:

```
[Unit]
Description=DistKontrolUSBClient
Requires=networking.service (или Requires=NetworkManager.service в зависимости от ОС)
After=networking.service (или After=NetworkManager.service в зависимости от ОС)
[Service]
ExecStartPre=/bin/sh -c 'logger DistKontrolUSBClient settling...;sleep 1s;logger DistKontrolUSBClient settled'
ExecStart=/usr/sbin/dkclientx86_64
Type=idle
[Install]
WantedBy=multi-user.target
```

5. systemctl daemon-reload

6. systemctl enable dkclient

7. systemctl start dkclient

Проверяем:

```
/usr/sbin/dkclientx86_64 -t 'MANUAL HUB ADD,192.168.1.180:6565'
/usr/sbin/dkclientx86_64 -t 'list'
/usr/sbin/dkclientx86_64 -t 'AUTO USE HUB,distkontrolusb64'
```

8. DistKontrolUSB Client у нас запускается как служба, как настроить автоподключение USB устройств по порту.

РЕКОМЕНДУЕМЫЙ ВАРИАНТ ИСПОЛЬЗОВАНИЯ №1.

Запуская клиентское приложение как службу, Вы используете его в многопользовательском режиме.

При использовании клиента в режиме службы подключение USB устройств рекомендуется осуществлять с помощью командной строки (bat файлов, скриптов).

В этом случае, используйте консольные команды для подключения к USB устройствам.

Например:

```
dkcl64.exe -t "USE,distkontrolusb48.31434,User1\pass"
```

Список примеров команд можно посмотреть в разделе инструкции: УПРАВЛЕНИЕ КЛИЕНТОМ DISTKONTROLUSB СКРИПТАМИ ИЛИ ИЗ КОМАНДНОЙ СТРОКИ.

Графический интерфейс, при работе клиента в режиме службы, имеет ограниченный функционал и предназначен в основном для мониторинга подключенных USB устройств.

В терминальном режиме графический интерфейс может быть запущен только для одного из пользователей.

Скриптами Вы сможете подключать USB устройства от различных произвольных пользователей, управлять питанием USB устройств.

ВОЗМОЖНЫЙ ВАРИАНТ ИСПОЛЬЗОВАНИЯ №2 (С подключением под текущим логином).

Для этого:

1. Выключите режим авторизации с вводимым логином и паролем. (по умолчанию выключено)

(Сервисы - Настройки USB - Настройки прав - Авторизация: использовать системное имя пользователя / введённое пользователем - ОТКЛЮЧИТЬ (должно стать серым) сохранить.

2. Запустите клиент

3. Последовательно подключить нужные USB устройства с сохранением пароля (сохранятся текущие системный логин пользователя и его пароль)

4. Отключить USB устройства в клиенте

5. Установить клиент как службу

6. Повторно запустите клиент

7. Поставьте галочки "Автоподключения по порту" для требуемых USB устройств (логин и пароль для подключения каждого из них должны были быть сохранены на шаге 3)

8. Закройте клиент

9. Перезапустите службу и убедитесь, что автоподключение работает.

ВОЗМОЖНЫЙ ВАРИАНТ ИСПОЛЬЗОВАНИЯ №3 (С произвольным логином).

Для этого:

1. Для сохранения, требуемого для автоподключения логина и пароля, включите режим авторизации с вводимым логином и паролем.

(Сервисы - Настройки USB - Настройки прав - Авторизация: использовать системное имя пользователя / введённое пользователем - ВКЛЮЧИТЬ (должно стать зеленым), сохранить.

2. Запустите клиент

3. Последовательно подключить нужные USB устройства с сохранением логина и пароля

4. Отключить USB устройства в клиенте

5. Установить клиент как службу

6. Выключите режим авторизации с вводимым логином и паролем.

(Сервисы - Настройки USB - Настройки прав - Авторизация: использовать системное имя пользователя / введённое пользователем - ОТКЛЮЧИТЬ (должно стать серым) сохранить.

7. Повторно запустите клиент

8. Поставьте галочки "Автоподключения по порту" для требуемых USB устройств (логин и пароль для подключения каждого из них должны были быть сохранены на шаге 3)

9. Закройте клиент

10. Перезапустите службу и убедитесь, что автоподключение работает.

Дополнительно см.:

http://distkontrol.ru/index.php/faq-usboverip