

Управляемый USB over IP концентратор

DistKontrolUSB

(Устройство подключения USB по сети)

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Версия 4.08.11

Оглавление

1	Общая информация.....	5
1.1	Назначение прибора	5
1.2	Модельный ряд управляемых USB over IP концентраторов	5
1.3	Область применения управляемых USB over IP концентраторов	6
1.4	Технические характеристики управляемых USB over IP концентраторов.....	8
1.5	Комплект поставки управляемого USB over IP концентратора.....	10
1.6	Устройство и работа управляемого USB over IP концентратора.....	10
1.6.1	Габаритные размеры управляемых USB over IP концентраторов (в 19" стойку).....	10
1.6.2	Устройство прибора	11
1.6.3	Модуль защиты подключаемых USB устройств управляемого USB over IP концентратора.....	14
1.6.4	Эксплуатационные ограничения и рекомендации	15
1.6.5	Меры безопасности	15
1.6.6	Подготовка управляемого USB over IP концентратора к работе.....	15
1.6.7	Работа управляемого USB over IP концентратора	16
1.7	Пломбирование	16
1.8	Упаковка	16
2	Техническое обслуживание.....	17
2.1	Общие положения.....	17
2.2	Проверка работоспособности управляемого USB over IP концентратора	17
3	Консервация и хранение управляемого USB over IP концентратора.....	17
3.1	Консервация	17
3.2	Хранение, транспортировка и утилизация.....	17
4	Web интерфейс управления DistKontrolUSB.....	18
4.1	Вход в Web интерфейс и начальный экран	18
4.2	Система	19
4.2.1	Общие настройки	19
4.2.2	Дата и время	20
4.2.3	Сеть.....	21
4.2.4	Уведомление.....	24
4.2.5	Управление энергопотреблением.....	26
4.2.6	Сертификаты	27
4.2.7	Запланированные задания.....	29
4.3	USB.....	32
4.3.1	USB порты	32
4.3.2	Типы USB устройств	33
4.4	Управление правами доступа	34

4.4.1 Пользователь	34
4.4.2 IP адрес	38
4.4.3 Группы	38
4.5 Сервисы	55
4.5.1 SNMP	55
4.5.2 SSH	64
4.6 Диагностика	64
4.6.1 Доска	64
4.6.2 Системная информация	64
4.6.3 Системный журнал	64
4.6.4 Сброс и восстановление	70
4.7 Информация	71
4.7.1 Проверить обновление	71
4.7.2 Поддержка	71
4.7.3 О нас	72
4.8 Сброс настроек, управляемого USB over IP концентратора в исходное состояние	73
4.9 Обновление программного обеспечения управляемого USB over IP концентратора	78
4.10 Сохранение и восстановление настроек программного обеспечения, управляемого USB over IP концентратора	83
4.11 Аппаратная перезагрузка управляемого USB over IP концентратора	85
5 Клиент DistKontrolUSB	86
5.1 Установка клиента DistKontrolUSB	86
5.2 Настройка клиента DistKontrolUSB	91
5.2.1 Управление отображением информации о пользователях USB устройств	91
5.2.2 Настройка меню клиентского приложения DistKontrolUSB	91
5.2.3 Сброс настроек клиентского приложения DistKontrolUSB	92
5.2.4 Комбинации клавиш клиентского приложения DistKontrolUSB	92
5.3 Запуск клиента DistKontrolUSB, в качестве службы (демона)	93
5.4 Управление клиентом DistKontrolUSB скриптами или из командной строки	94
5.5 Дополнительные возможности при работе с клиентом DistKontrolUSB	98
5.6 Примеры управления клиентом DistKontrolUSB для Windows и Linux	99
5.6.1 Алгоритм создания пакетного файла управления клиентом для Windows	99
5.6.2 Алгоритм установки и настройки демона для Linux	100
6 Краткая инструкция по использованию утилиты управления портами управляемого USB over IP концентратора	103
7 Вариант использования, управляемого USB over IP концентратора	105
8 Часто задаваемые вопросы	106

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;

1.1 НАЗНАЧЕНИЕ 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 обеспечить 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 Wireless				
Порт Ethernet	1 x 10/100/1000 Mb	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)				
Индикация LEDs	Питание, LAN порт статус	Питание, LAN порт статус, наличие питания порта USB-устройства			
Питание	Встроенный блок питания 220В 50 Гц, 15 Вт	Встроенный блок питания 220В 50 Гц, 75 Вт	Встроенный блок питания 220В 50 Гц, 100 Вт	Встроенный блок питания 220В 50 Гц, 150 Вт	Встроенный блок питания 220В 50 Гц, 300 Вт
	(опционально: Второй блок питания в режиме резервирования питания или блока питания)				
Программное управление режимами резервирования питания. (Опционально при наличии второго блока питания)	-	<p>- Резервирование питания. (Всегда работает 2 блока питания, при пропадании питания на входе одного БП или при выходе из строя БП, устройство продолжает работать без перезагрузки).</p> <p>- Резервирование Блока питания. (Всегда работает 1 БП. При пропадании питания на входе работающего БП или при его выходе из строя, включается 2-ой БП. При переключении устройство будет перезагружено.).</p>			
Поддержка USB	USB 3.0, 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			
Номинальный ток нагрузки на порт USB	-	0,5 А			
Предельный ток нагрузки на порт USB	-	0,9 А			
Температура окружающей среды	0°C до +50°C				
Относительная влажность воздуха	не более 80% (при температуре +35°C и ниже)				
Поддержка операционных систем	Windows® Server 2016/2019/2022, Windows® 10,11 Linux (ядро не ниже 4.9+) OSX (10.9.5-10.13 , 12 Monterrey)				

Модель	DistKontrolUSB-4	DistKontrolUSB-16	DistKontrolUSB-32	DistKontrolUSB-48	DistKontrolUSB-64
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			
Размеры в Unit	-	1	2	3	3
Безопасность	https, ssl				
Шифрование трафика USB	есть				
Встроенный брандмауэр	есть				
Ограничение по IP для подключения USB устройства	есть				
Ограничение по IP для подключения USB порта	есть				
Авторизация для подключения USB устройства	есть				
Авторизация для подключения USB порта	есть				
Групповые политики доступа	нет	есть (до 16 групп доступа)			
Управление видимостью USB устройств для пользователей	нет	есть (до 16 групп видимости)			
Модуль защиты подключаемых USB устройств	нет	(опционально: есть)			
Резервирование питания	нет	(опционально: есть)			
Отказоустойчивость Ethernet портов	нет	(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

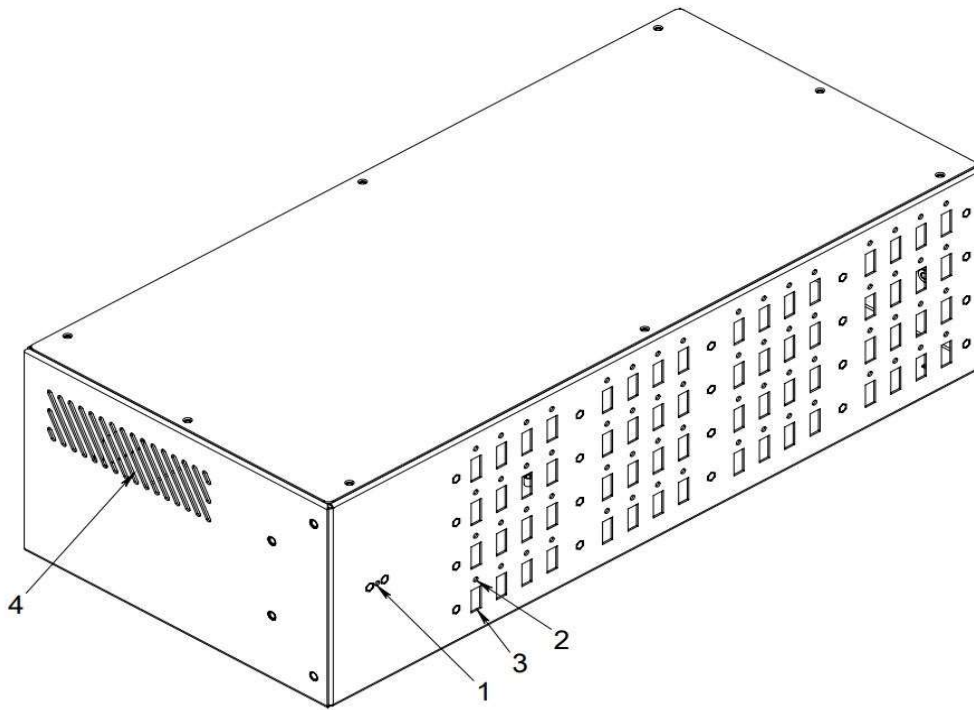
1.6 УСТРОЙСТВО И РАБОТА УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА

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".

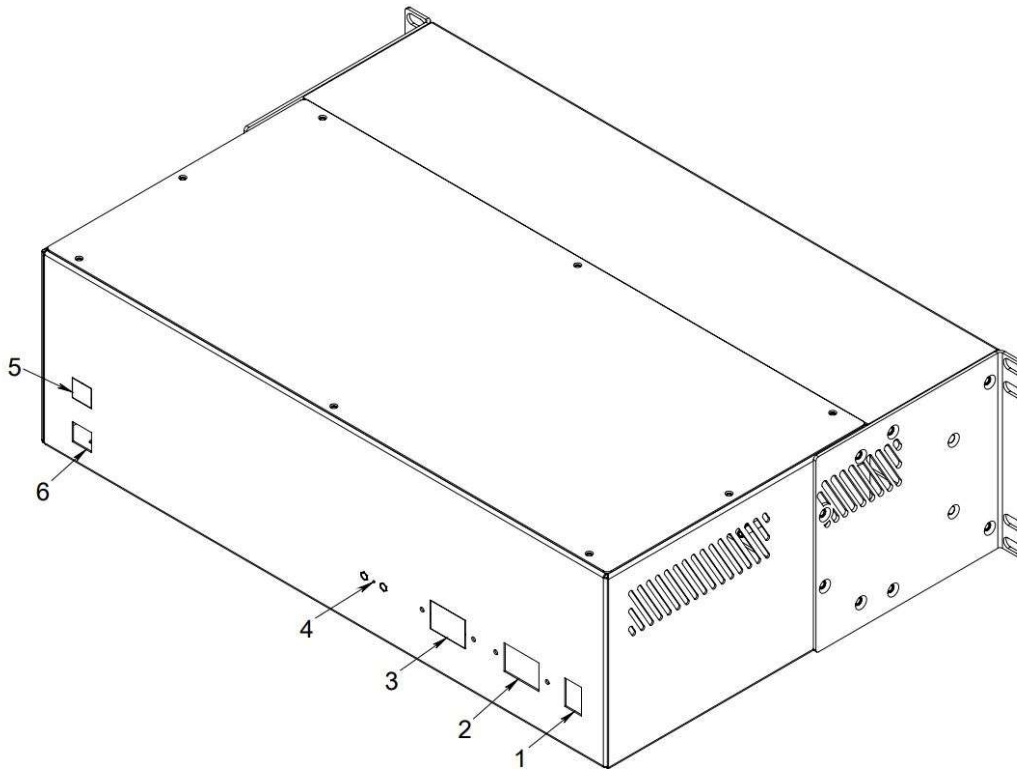


На передней панели расположены:

- 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:

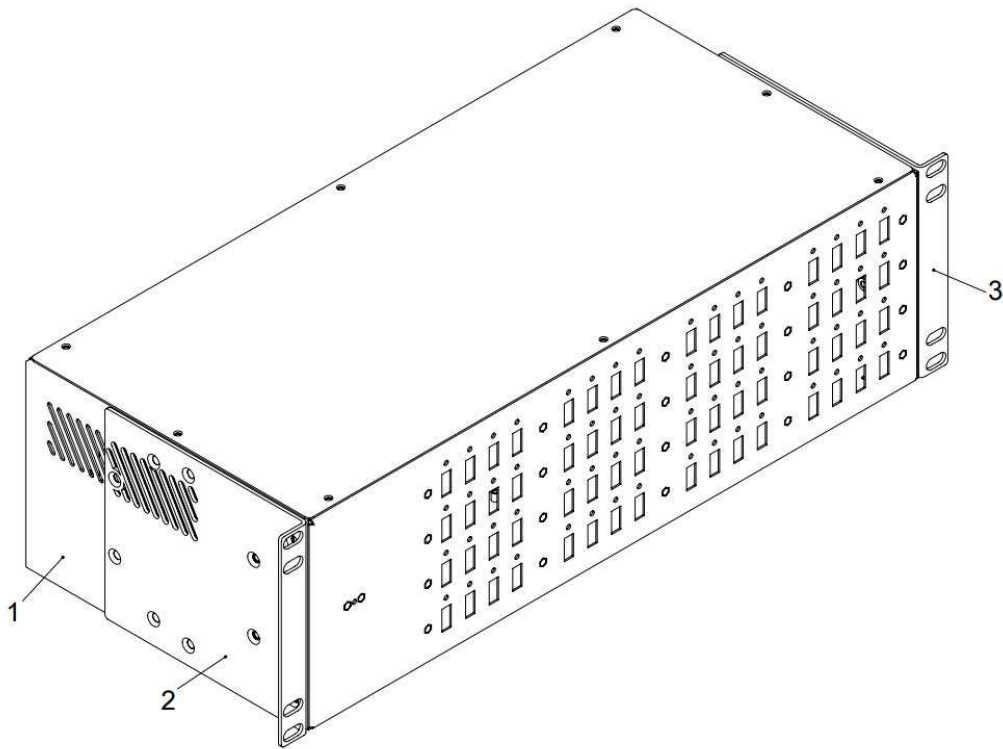
- 1 - Выключатель питания «Питание».
- 2 - Разъем для подключения сетевого кабеля 1;
- 3 - Разъем для подключения сетевого кабеля 2(опционально);
- 4 – Кнопка сброса настроек «Reset»
- 5 - Разъем типа RJ45 для сети Ethernet «LAN» 2(опционально);
- 6 - Разъем типа RJ45 для сети Ethernet «LAN» 1;

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

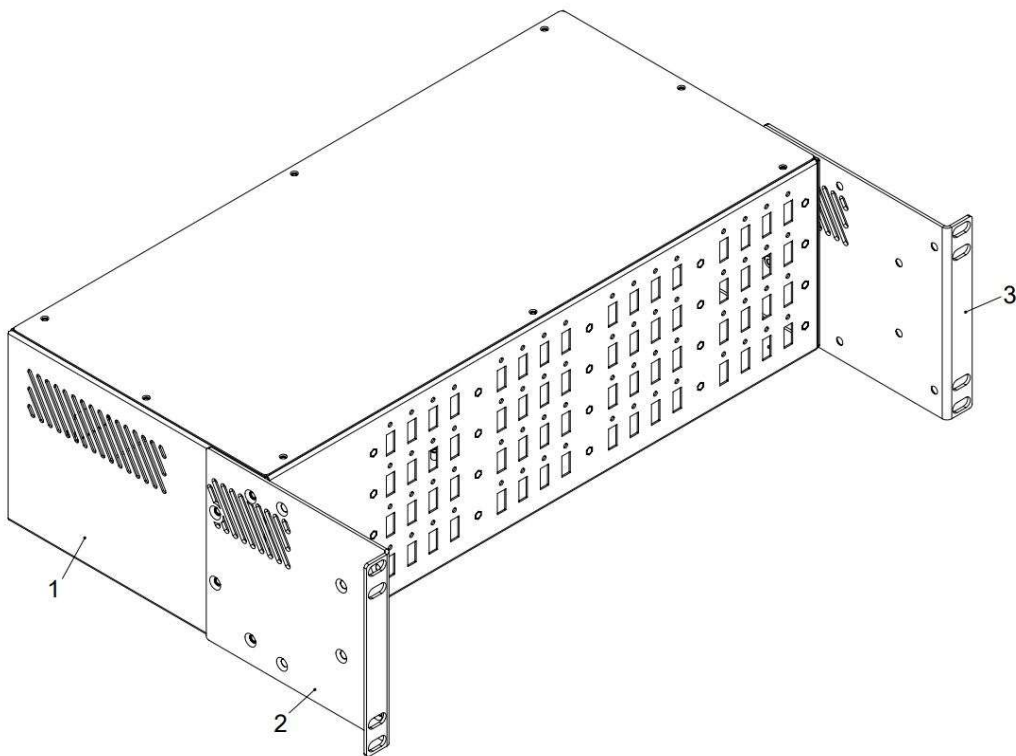
В комплекте с устройством поставляются крепления в стойку/шкаф 19" с возможностью крепления в двух положениях.

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.

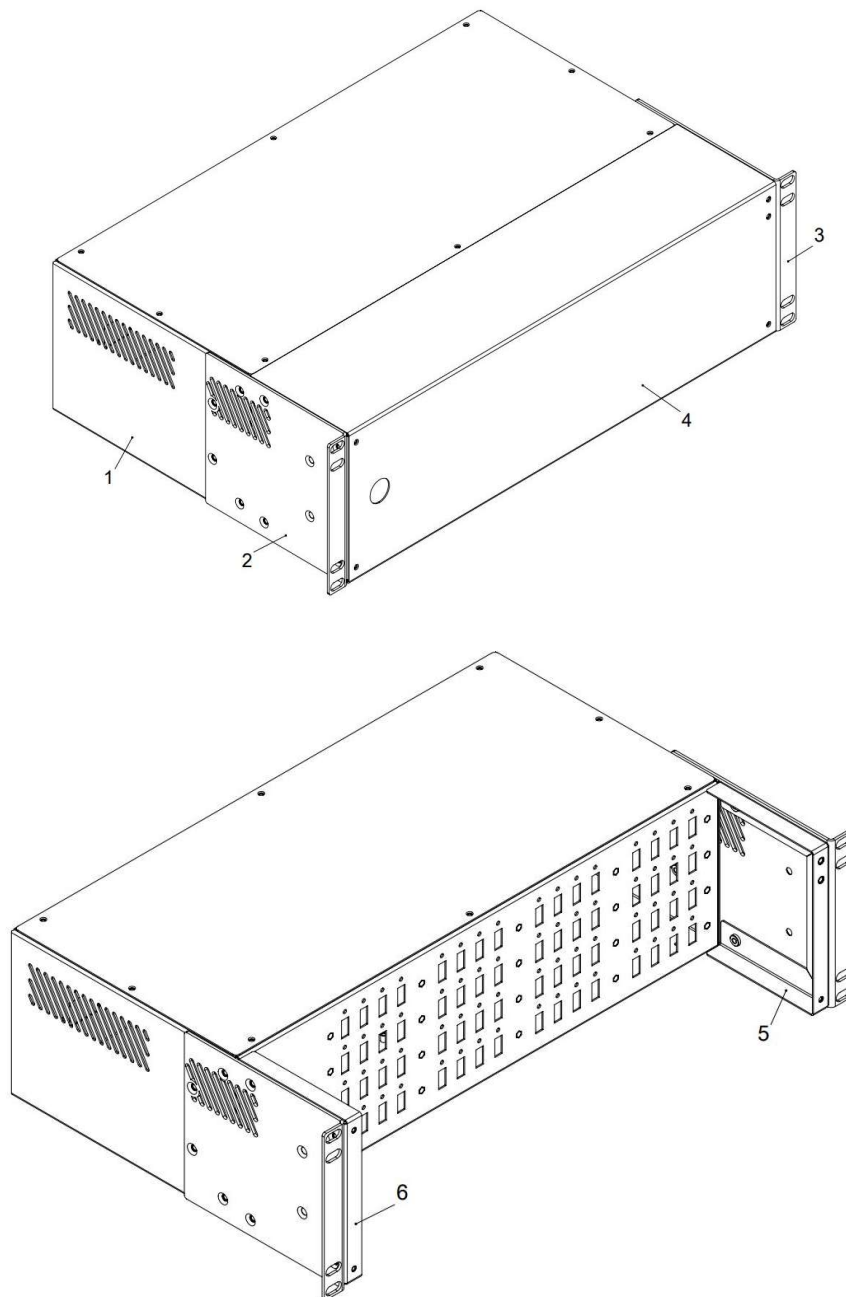
Модуль защиты подключаемых USB устройств управляемого USB over IP концентратора поставляется отдельно (опционально). В стандартную комплектацию не входит.

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°C;
- пониженной температуры окружающей среды не ниже - 5°C;
- повышенной относительной влажности воздуха до 98% при температуре плюс 25°C;
- 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 USB 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.

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

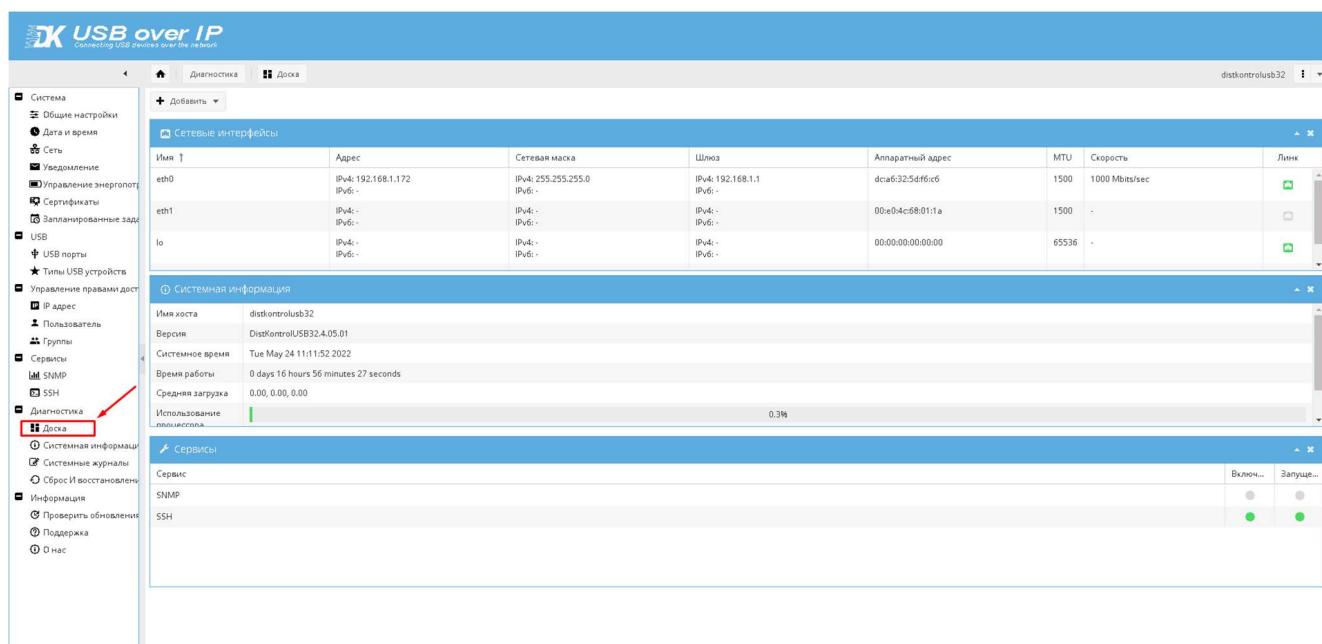
4.1 ВХОД В WEB ИНТЕРФЕЙС И НАЧАЛЬНЫЙ ЭКРАН

Управление USB over IP концентратором осуществляется через мультязычный 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 DistKontrolUSB имеет следующие сетевые настройки:

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 3 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

4.2.1.1 WEB АДМИНИСТРАТОР

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.

Внимание!!! Пользователь может изменить порты http с 80 на произвольный, https с 443 на произвольный, ssh с 22 на произвольный. При изменении данных портов, будьте внимательны, они не должны совпадать с любым из портов [групп USB концентратора](#). При некорректном назначении данных портов можно потерять доступ к WEB интерфейсу администрирования. Для восстановления доступа потребуется полный [сброс устройства к заводским настройкам](#).

4.2.1.2 ПАРОЛЬ WEB АДМИНИСТРАТОРА

В данном разделе возможно изменить пароль пользователя admin.

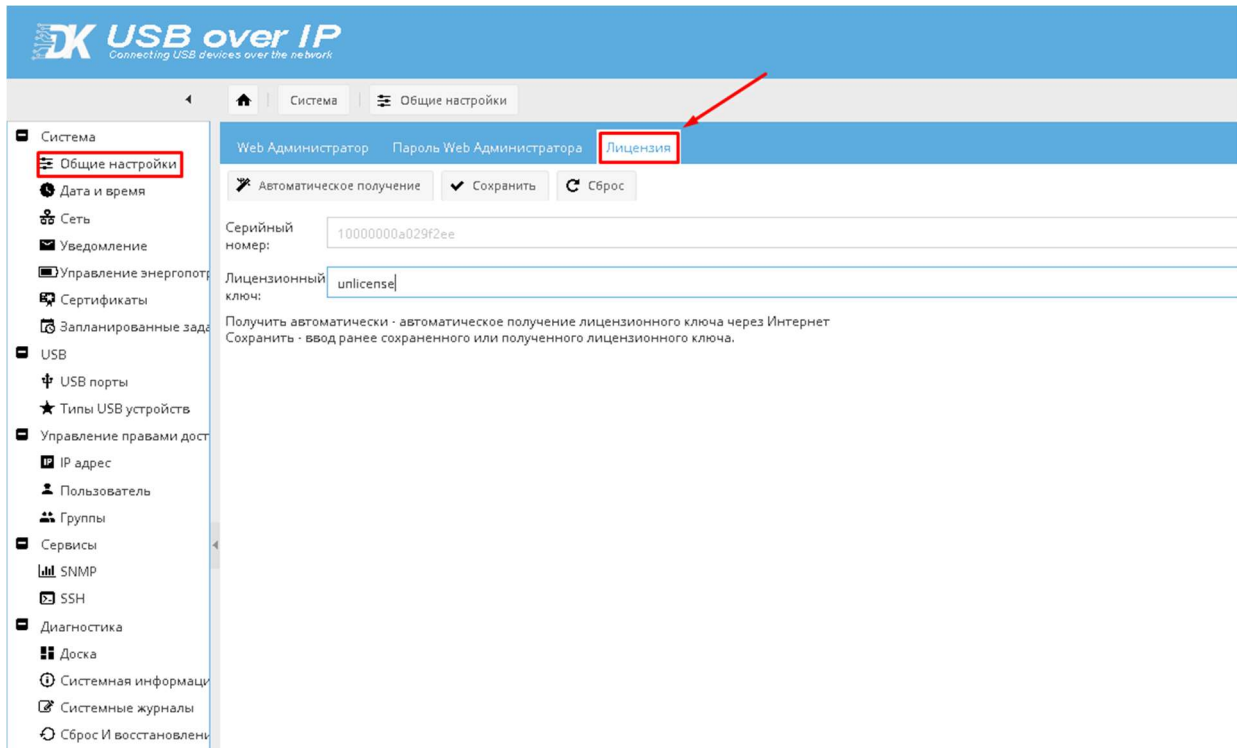
Внимание!!! При утере пароля, потребуется [сброс настроек, управляемого USB over IP концентратора в исходное состояние](#)

4.2.1.3 ЛИЦЕНЗИЯ

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

После загрузки необходимо ввести лицензионный ключ к ПО. Его можно ввести любым из двух способов:

1. (Потребуется доступ к интернету на концентраторе DistKontrolUSB) В WEB интерфейсе концентратора автоматически – нажав на кнопку «Получить автоматически» на странице «Система» - «Общие настройки» - «Лицензия». Ключ будет получен автоматически и ни какие дополнительные действия не потребуются.



2. (доступ к интернету не потребуется) В WEB интерфейсе концентратора вручную - ввести ранее сохраненный или полученный лицензионный ключ и нажать на кнопку «Сохранить».

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 WEB интерфейса «Система» - «Общие настройки» - «Лицензия» или, в паспорте устройства (на последней странице внизу).

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 установке времени.

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

Внимание!!! В случае изменения NTP сервера, необходима перезагрузка устройства.

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.

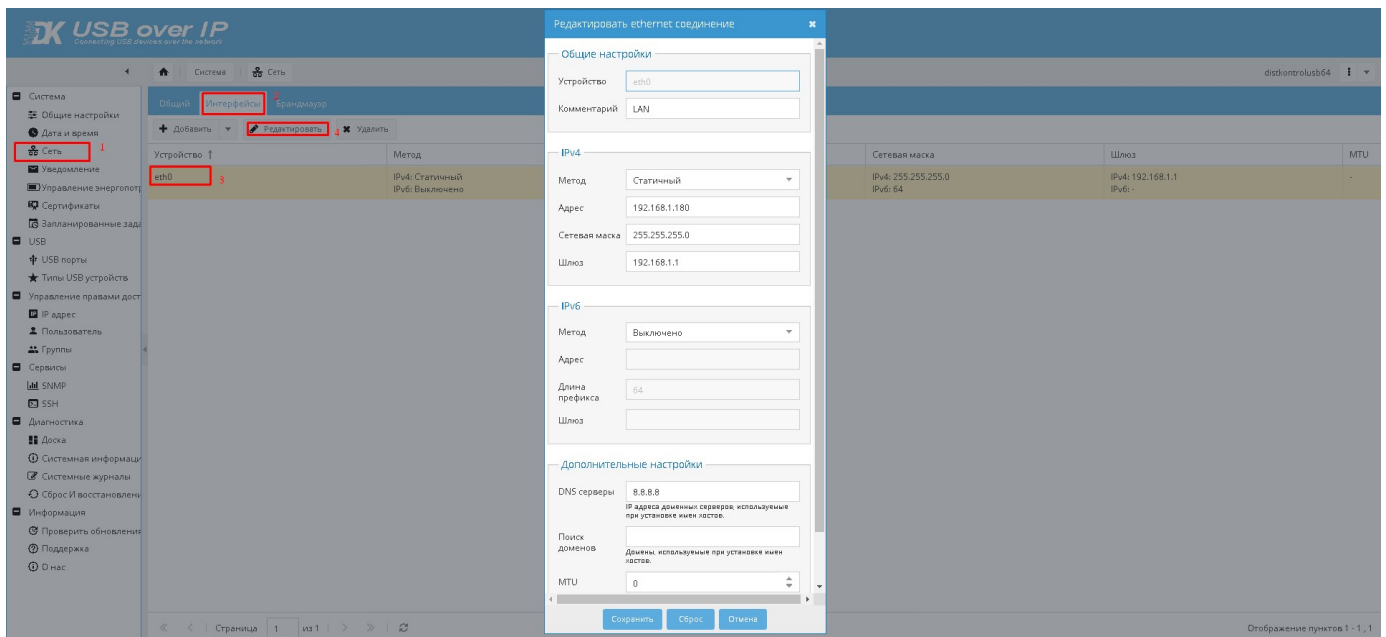
Доменное имя – добавляет имя домена 2 и более уровня. Не влияет на подключение к домену, используется для графического отображения в клиентском приложении.

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 [«Общие настройки»](#) можно изменить пароль для доступа к WEB интерфейсу, порт WEB интерфейса.



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.

Для настройки соединения необходимо, по крайней мере, два физических сетевых интерфейса. Веб - интерфейс позволяет выбрать менее двух. Это сделано специально для целей конфигурации. Рабочий процесс для двух сетевых карт выглядит следующим образом:

- Если основной сетевой адаптер уже работает с помощью установщика, настройте его через веб-интерфейс как статический. Если установлено как статическое, используя тот же IP-адрес, указанный DHCP, не должно быть необходимости повторно входить в веб-интерфейс.
- Выберите второй доступный сетевой адаптер, выберите режим подключения, заполните поле IP и значения маски подсети, оставьте шлюз и DNS пустыми. Сохраните и нажмите применить.
- Выйдите из системы и получите доступ к Web интерфейсу, используя новый IP-адрес, назначенный созданному bond интерфейсу.
- Теперь выберите основной интерфейс, настроенный через веб-интерфейс на первом шаге, и удалите его. Сохраните и нажмите применить.
- Выберите вновь созданный интерфейс связи, нажмите "Изменить", теперь для выбора должна быть доступна физическая сетевая карта, удаленная с предыдущего шага. Сохраните и нажмите применить.
- Теперь панель мониторинга должна отображать информацию об bond интерфейсе (включая скорость).

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.

Направление	Действие	Семейство	Исходный	Порт	Назначение	Порт	Протокол	Дополнительные опции	Комментарий
INPUT	ACCEPT	IPv4	192.168.1.105	-	-	6565	TCP		
INPUT	ACCEPT	IPv4	192.168.1.105	-	-	80	TCP		
INPUT	REJECT	IPv4	-	-	-	-	TCP		

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 адреса и закрыть для всех остальных только, например, **22** или **6565** порт на устройстве, и только убедившись в корректном вводе правил, уже закрывать 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

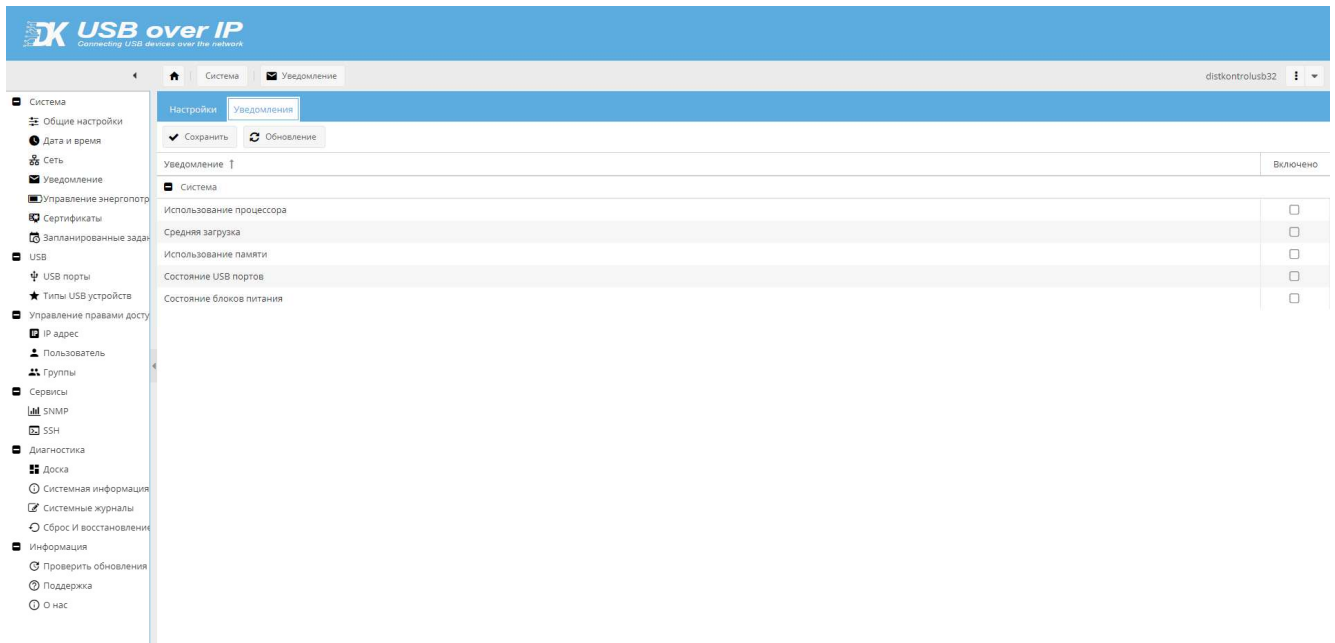
The screenshot shows the 'Уведомление' (Notification) settings page. The left sidebar contains a menu with 'Уведомление' highlighted. The main content area is divided into sections: 'Общие настройки' (General settings) with a 'Включить' (Enable) toggle switch; 'Настройки SMTP' (SMTP settings) with fields for 'Сервер SMTP' (smtp.mail.ru), 'Порт SMTP' (465), 'Режим шифрования' (SSL/TLS), 'Отправитель email' (distkontrol@example.ru), and 'Требуется аутентификация' (Authentication required) toggle; and 'Получатель' (Recipient) with fields for 'Основной e-mail' (admin@example.ru) and 'Дополнительный email'.

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 трехкратном 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.

Пункт меню «Уведомления» предназначен для настройки необходимых Вам сообщений по e-mail.



Уведомления приходят в том случае если:

«Использование процессора» более 95% за 10 циклов подряд

«Средняя загрузка» более 2 за 1 минуту, более 1.5 за 5 минут, более 1 за 15 минут

«Использование памяти» более 90%

«Состояние портов» - при изменении состояния порта

«Состояние блоков питания» - при изменении состояния блока питания (при аппаратном наличии второго блока питания).

Примечание: При восстановлении настроек или же при обновлении ПО с последующим восстановлением необходимо в настройке уведомлений ввести пароль пользователя заново (удалить из заполненного поля пароль, сохранить, ввести корректный пароль и сохранить его).

4.2.5 УПРАВЛЕНИЕ ЭНЕРГОПОТРЕБЛЕНИЕМ

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

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

Доступные задания:

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

Существует возможность переключения режимов резервирования питания. Данная возможность присутствует только в модификации устройства с двумя блоками питания и версиях ПО не старше 4.05.

Управления режимами резервирования происходит на странице «Управление энергопотреблением» - «Режимы питания».

По умолчанию уставлен режим резервирования питания для повышения отказоустойчивости USB over IP концентратора (Всегда работает 2 блока питания, при пропадании питания на входе одного БП или при выходе из строя БП, устройство продолжает работать без перезагрузки).

Возможно переключить в режим резервирования блока питания для повышения отказоустойчивости USB over IP концентратора. (Всегда работает 1 БП. При пропадании питания на входе работающего БП или при его выходе из строя, включается 2-ой БП. При переключении устройство будет перезагружено).

Также в данном разделе существует возможность отслеживания актуального состояния блока питания.

Для отображения актуального состояния блока питания после переключения режима резервирования необходимо обновить страницу.

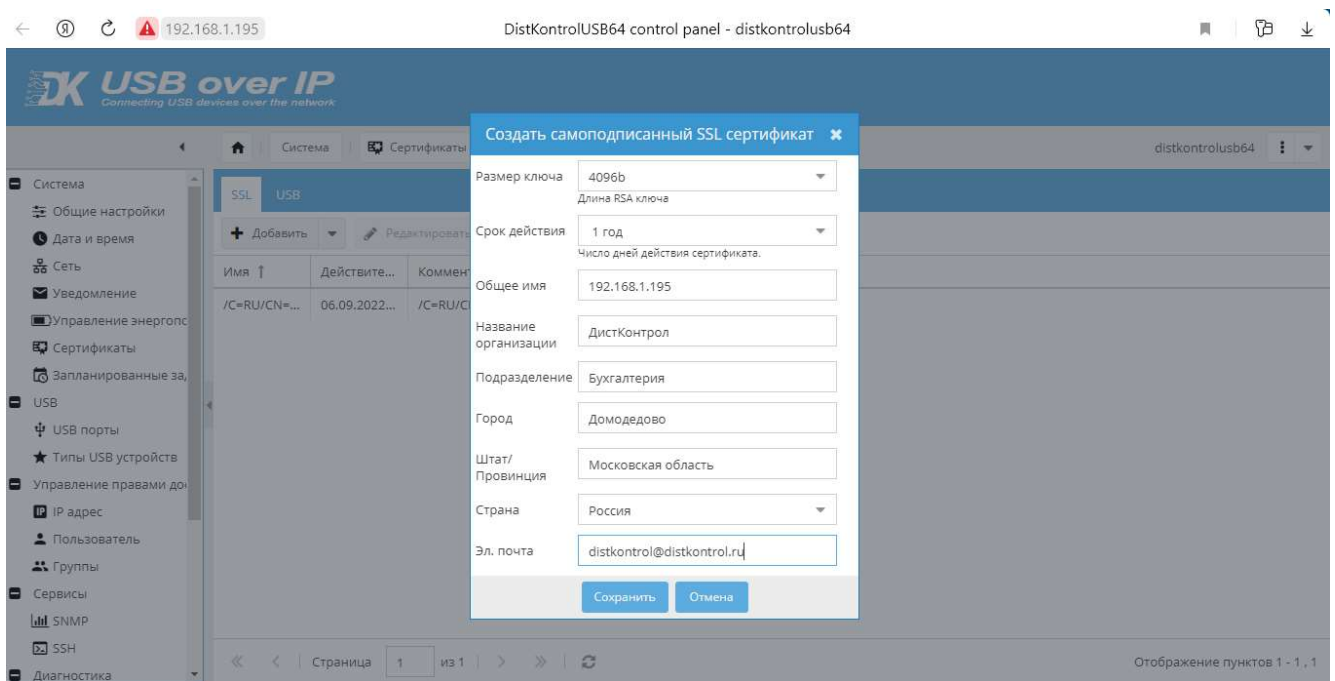
4.2.6 СЕРТИФИКАТЫ

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

По умолчанию USB over IP концентратор имеет два вида сертификатов.

1. SSL сертификат
2. Сертификат SSL для трафика USB-устройств

SSL сертификат предназначен для настроек безопасного соединения.



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.

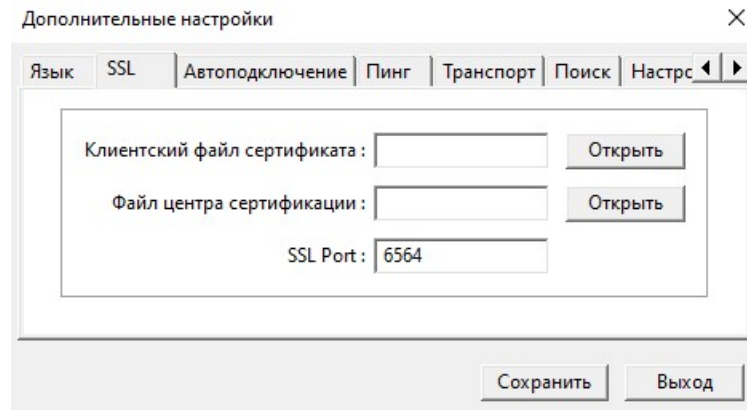
Примечание: устройство должно корректно получать время по NTP (Система - Дата и время)

В случае необходимости использовать сертификат SSL для трафика USB-устройств необходимо перейти на вкладку «USB» - создать сертификат - назначить его той [группе](#), в которой он будет использоваться.

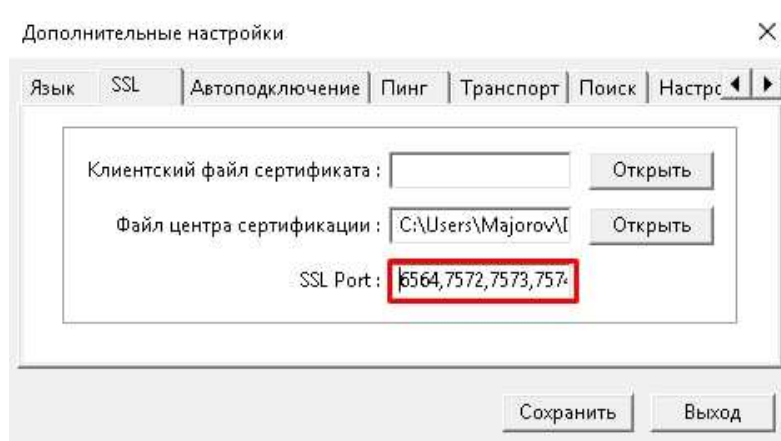
После назначения сертификата группе:

В клиентском приложении кликните правой кнопкой мыши «USB серверы» - «Дополнительные настройки». На вкладке «SSL» в строке «Файл центра сертификации» нажмите «Открыть» и выберите Ваш сертификат *.pem.

Укажите необходимый порт.

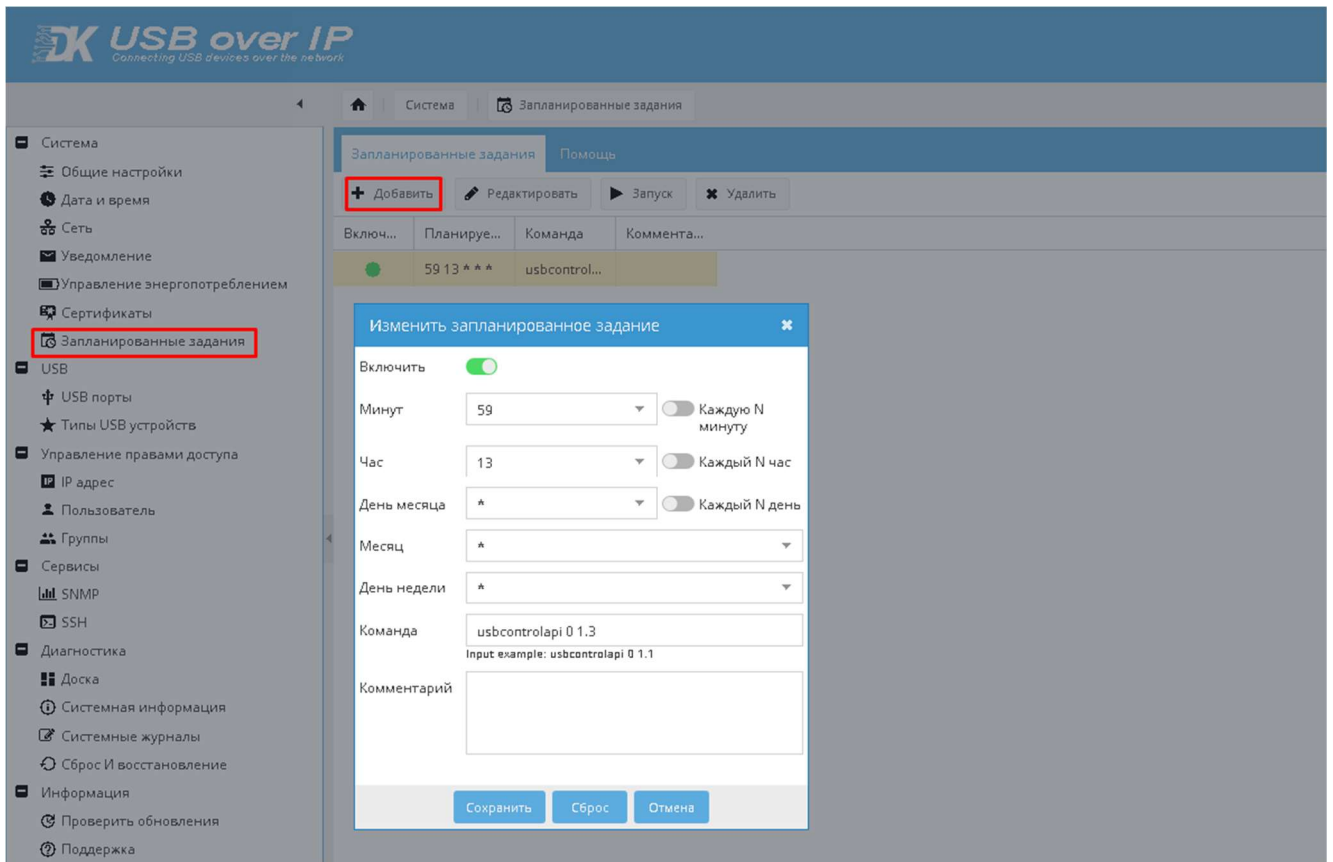


В случае использования нескольких групп с разными SSL сертификатами необходимо скачать все сертификаты, открыть в текстовом редакторе и объединить в один файл сертификации. Порты в данном случае указываются через запятую.



Нажмите «Сохранить» и согласитесь с перезапуском клиентского приложения.

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:

<code>usbcontrolapi 0 1.9</code>	(Выключить USB 1.9)
<code>usbcontrolapi 1 1.12</code>	(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)
```

Доступные задания:

1. Включить питание для конкретного USB порта
2. Включить питание для конкретного ряда USB портов
3. Включить питание для всех USB портов
4. Отключить питание для конкретного USB порта
5. Отключить питание для конкретного ряда USB портов
6. Отключить питание для всех USB портов

В качестве планировщика задач в устройстве используется cron.

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

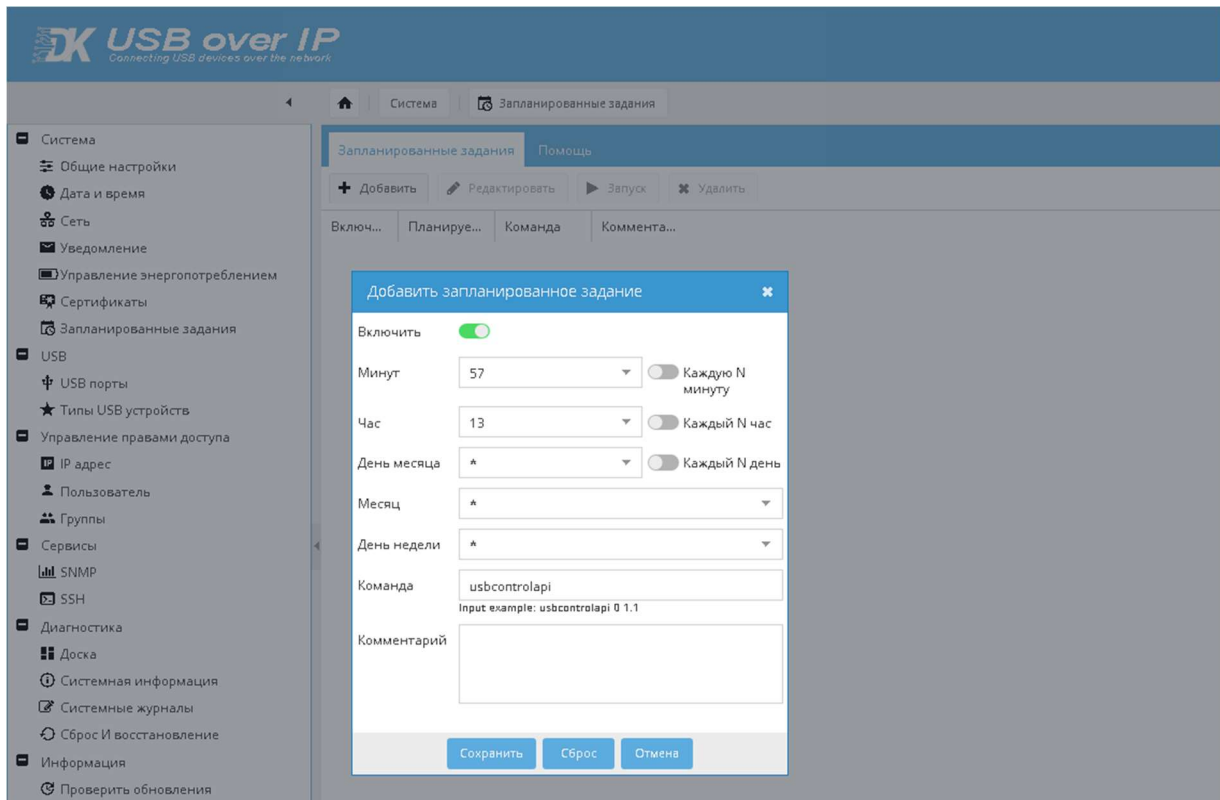
Формат команд:

```
.----- 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

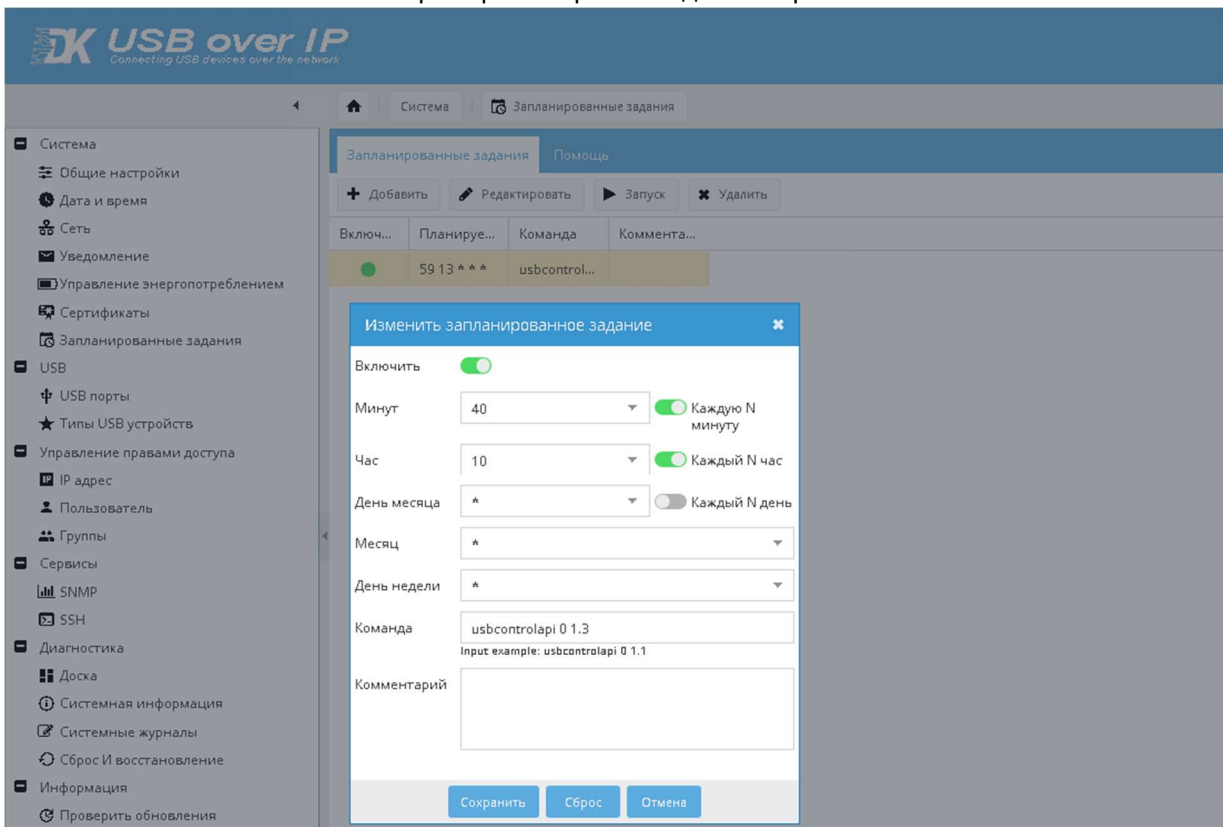
Примечание: устройство должно корректно получать время по NTP (Система - Дата и время)

Создаем задание:



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

Пример повторения задания через 12:01 ч



В столбце «Планируется» будет: */40 */10 * *

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.

The screenshot shows the 'USB over IP' web interface. The main content area displays a table of USB ports. The table has the following columns: 'Номер' (Number), 'Имя' (Name), 'Статус' (Status), and 'Включить' (Enable). The 'Включить' column contains checkboxes. The 'Статус' column contains green circles for active ports and grey circles for inactive ports. The 'Имя' column contains names like 'USB 1.01' through 'USB 1.15'. Above the table are buttons for 'Включить все', 'Выключить все', 'Сброс Имен', and 'Сохранить'. The sidebar menu on the left includes 'Система', 'Общие настройки', 'Дата и время', 'Сеть', 'Уведомление', 'Управление энергоп', 'Сертификаты', 'Запланированные з', 'USB', 'USB порты', 'Типы USB устройств', 'Управление правами д', 'IP адрес', 'Пользователь', 'Группы', 'Сервисы', 'SNMP', 'SSH', 'Диагностика', 'Доска', 'Системная информ', 'Системные журнал', and 'Сброс И восстановл'.

Номер	Имя	Статус	Включить
1.1	USB 1.01	●	<input checked="" type="checkbox"/>
1.2	USB 1.02	●	<input checked="" type="checkbox"/>
1.3	USB 1.03	●	<input checked="" type="checkbox"/>
1.4	USB 1.04	●	<input checked="" type="checkbox"/>
1.5	USB 1.05	●	<input type="checkbox"/>
1.6	USB 1.06	●	<input type="checkbox"/>
1.7	USB 1.07	●	<input type="checkbox"/>
1.8	USB 1.08	●	<input checked="" type="checkbox"/>
1.9	USB 1.09	●	<input checked="" type="checkbox"/>
1.10	USB 1.10	●	<input checked="" type="checkbox"/>
1.11	USB 1.11	●	<input checked="" type="checkbox"/>
1.12	USB 1.12	●	<input checked="" type="checkbox"/>
1.13	USB 1.13	●	<input checked="" type="checkbox"/>
1.14	USB 1.14	●	<input checked="" type="checkbox"/>
1.15	USB 1.15	●	<input checked="" type="checkbox"/>

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".

4.3.2 ТИПЫ USB УСТРОЙСТВ

Данный раздел необходим для настройки прав доступа, более подробно см. [«Настройки доступа»](#)

Типы 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.

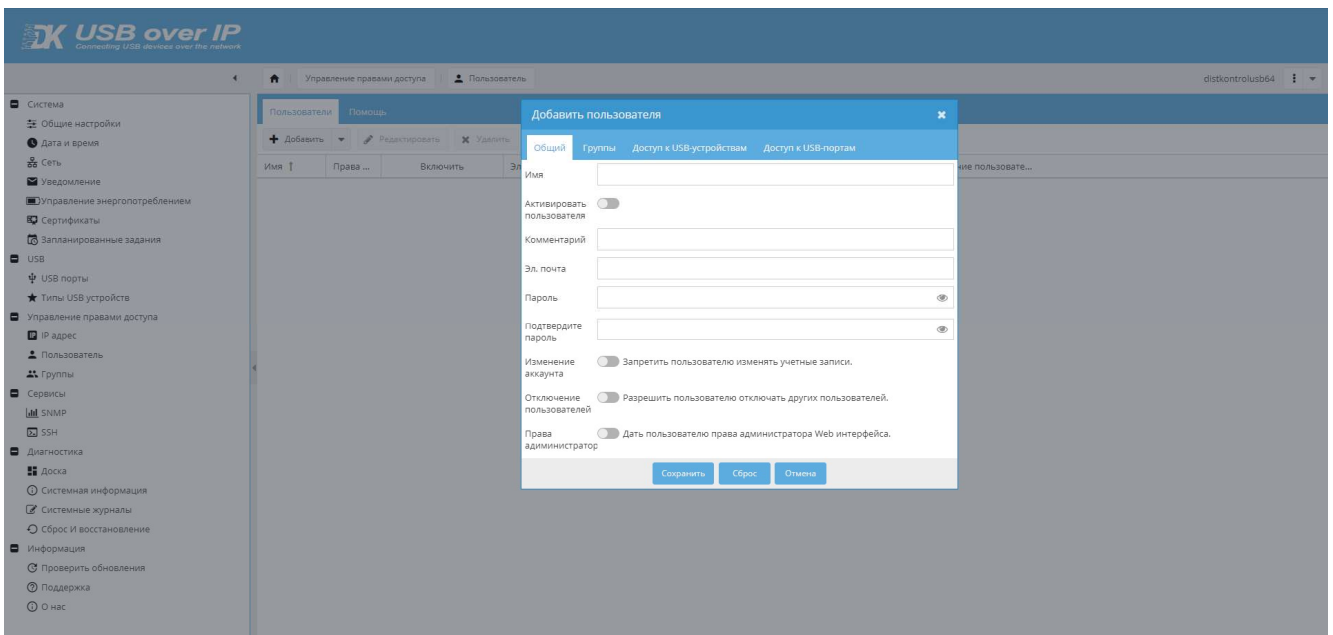
4.4 УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА

4.4.1 ПОЛЬЗОВАТЕЛЬ

Для корректной настройки групп, ограниченного предоставления прав на включение и отключение USB устройств необходимо на странице «Управление правами доступа» - «Пользователь» создать пользователей управляемого USB over IP концентратора, активировать, дать доступ к необходимым портам и устройствам и добавить в группу.

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

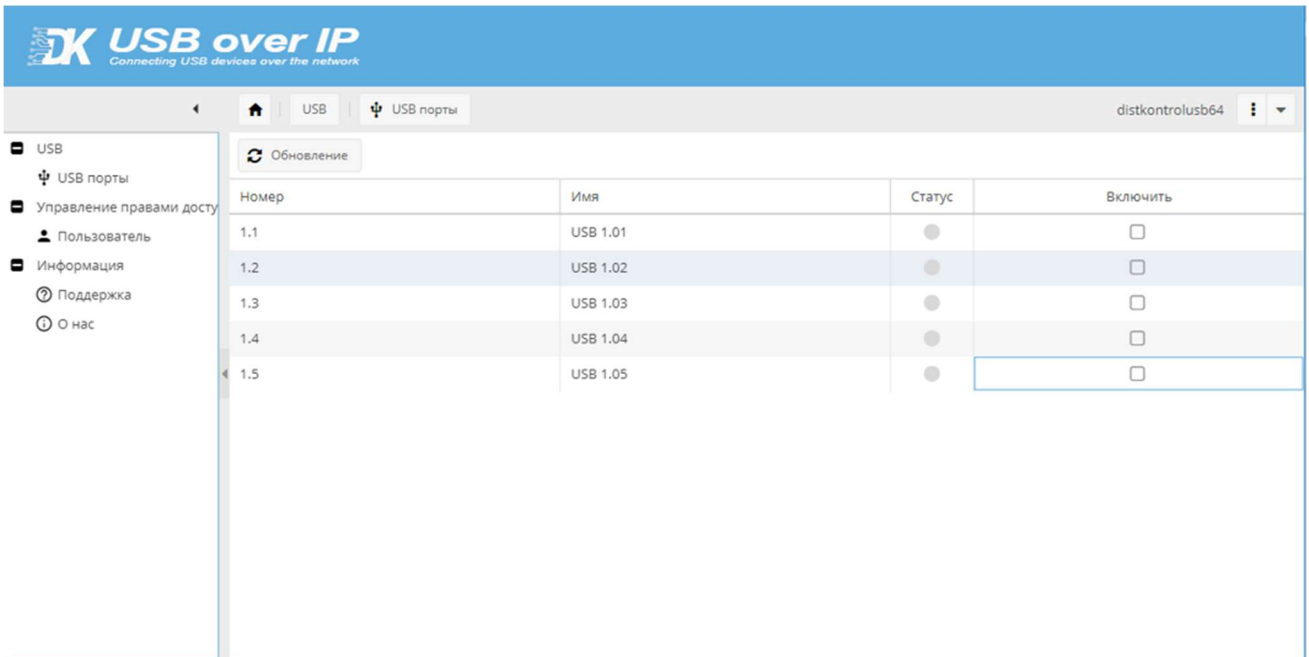
Регистр имеет значение!



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

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 входы, назначенные его группам и в WEB интерфейсе пользователя на странице «USB порты» будут отображены только те входы, к которым пользователю предоставлены права на управление. См. раздел [настройки ограничений доступа](#).



Импорт пользователей из Active Directory (AD).

1.Подключение:

Импортировать: Подключение
✕

Имя пользователя

Пароль

Адрес сервера

Подразделение

Доменное имя

Доменная зона

i

Поле "Подразделение" является необязательным. Поле "Подразделение" не должно содержать кириллических символов или пробелов. Инструкцию по подключению смотрите на странице "Помощь".

Подключение
Сброс
Отмена

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".

В случае использования домена 3-го уровня (Например: "myad.ad.com") для корректной работы необходимо ввести "myad.ad" в Доменное имя.

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.)

4.4.1.1 ОТКЛЮЧЕНИЕ ПОДКЛЮЧЕННОГО ПОЛЬЗОВАТЕЛЯ

Отключение подключенных пользователей к USB-устройству может осуществляться несколькими способами:

- Путем отключения питания с определенного USB-порта (см. [«USB порты»](#), [«Утилита USBControl»](#))
- Предоставлением прав пользователю на отключение других пользователей (требуется запуск клиентского приложения с параметром –а см. [«Дополнительные возможности при работе с клиентским приложением»](#))
- Предоставлением прав IP-адресу на отключение других пользователей (требуется запуск клиентского приложения с параметром –а см. [«Дополнительные возможности при работе с клиентским приложением»](#))

ВНИМАНИЕ!!! Имя пользователя, введённое в WEB-интерфейсе, ДОЛЖНО СОВПАДАТЬ с именем учетной записи системы, с которой происходит отключение подключенных к USB-порту пользователей.

Пользователь может выключить питание на к USB-порту или отключать подключённых пользователей, только с тех USB-портов, которые ему назначены в разделе «Пользователи», вкладка «Доступ к USB-портам».

Пример настройки отключения пользователей:

1. В разделе «Пользователи» создаем пользователя, имя которого будет совпадать с именем системы (например, имя моей учетной записи “Petrov”, следовательно, имя пользователя должно быть “Petrov”).
2. Даю пользователю соответствующие права на “управление питанием USB-портов” и “отключение других пользователей”
3. Во вкладке «Доступ к USB-портам» указываю USB-порты, к которым пользователь может подключать USB-устройства, управлять их питанием, а также отключать других пользователей, если те подключились к назначенным USB-портам пользователя “Petrov”.
4. Запустить клиентское приложение Distkontrol Client с параметром запуска –а (см. [«Дополнительные возможности при работе с DistkontrolUSB Client»](#))
5. После чего, в клиентском приложении, можно отключить уже подключенных пользователей.

4.4.2 IP АДРЕС

Данный раздел необходим для настройки прав доступа, более подробно см. [«Настройки доступа»](#)

IP можно добавлять, редактировать, удалять. При создании, редактировании устройства выберите семейство IP (IPv4 или IPv6)

4.4.3 ГРУППЫ

Данный раздел необходим для настройки групп USB портов. Существует 16 групп, в которые можно добавить пользователей, настроить права доступа для группы, настроить видимость USB-портов.

Имя ↑	Коммента...	Участники	Статус	Скрыть...	Устрой...	ПортУЛ...	Устрой...	ПортUP	Тип авториз...	Порт	Видимость USB-портов
Group01			●	●	●	●	●	●	System user	6565	All ports
Group02			●	●	●	●	●	●	System user	6602	
Group03			●	●	●	●	●	●	System user	6603	
Group04			●	●	●	●	●	●	System user	6604	
Group05			●	●	●	●	●	●	System user	6605	
Group06			●	●	●	●	●	●	System user	6606	
Group07			●	●	●	●	●	●	System user	6607	
Group08			●	●	●	●	●	●	System user	6608	
Group09			●	●	●	●	●	●	System user	6609	
Group10			●	●	●	●	●	●	System user	6610	
Group11			●	●	●	●	●	●	System user	6611	
Group12			●	●	●	●	●	●	System user	6612	
Group13			●	●	●	●	●	●	System user	6613	
Group14			●	●	●	●	●	●	System user	6614	
Group15			●	●	●	●	●	●	System user	6615	

В данном разделе для пользователя возможно настроить отображение только доступных ему USB-портов. Для этого:

1. Необходимо создать SSL сертификат для трафика USB устройств и добавить его в группу.
2. Скачать данный сертификат и добавить в DistKontrolUSB Client.
3. Добавить сервер в DistKontrolUSB Client с указанием SSL порта(по умолчанию для Group1: 6564). Для корректного отображения нескольких групп USB устройств необходимо добавить все используемые сервера с указанием [SSL порта](#), указанного в настройках группы
4. В Web-интерфейсе добавить пользователя, активировать его и добавить в группу, к которой у пользователя будет доступ, дать доступ к необходимым устройствам\портам.
5. В разделе «Группы» - открыть настройки группы, перевести ползунки «Включить», «Включение SSL для USB-трафика» в активное состояние.
6. При необходимости установить настройки прав доступа, более подробно см. [«Настройки доступа»](#)
7. Включить в список видимости необходимые USB-порты.
8. Сохранить настройки, включить порты.

В случае необходимости разделения USB устройств между пользователями, настройте другую группу в том же порядке.

Для корректного отображения нескольких групп USB устройств в DistKontrolUSB Client необходимо добавить все используемые сервера с указанием SSL порта, указанного в настройках группы (по умолчанию Group2:7572, Group3:7573, Group4:7574 и т.д.).

Для сброса настроек - необходимо выбрать нужную группу и сбросить настройки.

ВНИМАНИЕ!!! В исходном состоянии все USB-порты будут добавлены в «Group1», для того чтобы увидеть порты в другой группе необходимо в первой группе назначить только необходимые порты, оставшиеся порты станут доступны в других группах.

В случае необходимости настроить для каждого устройства доступ определенным пользователям видимость всех портов необходимо оставить в «Group1», создать пользователей разграничить права на доступ к определенным устройствам\портам, добавить всех пользователей в группу, включить ограничения в настройках группы.

4.4.3.1 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).

Редактировать группу

Настройки Общий **Настройки доступа** Участники Видимость USB-портов

Настройки доступа

Этот параметр вступает в силу после его сохранения.
Несколько правил применяются через 'И'.

- Ограничение доступа к USB устройству по логину и паролю
- Ограничение доступа к USB порту по логину и паролю
- Ограничение доступа к USB устройству по IP адресу
- Ограничение доступа к USB порту по IP адресу

Настройки прав

Этот параметр вступает в силу после его сохранения.

- Авторизация: использовать системное имя пользователя / введенное пользователем

Сохранить Сброс Отмена

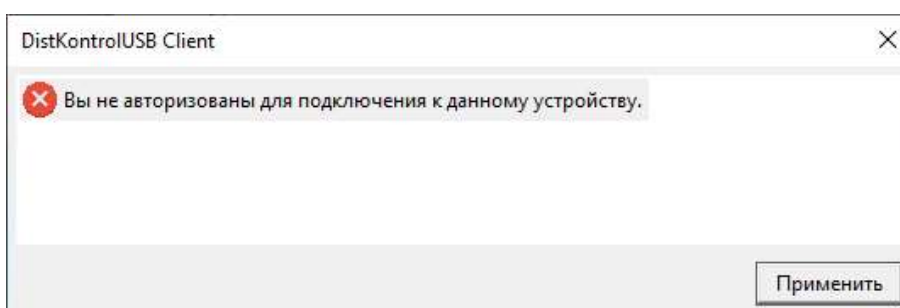
Режимы ограничения включаются на странице WEB интерфейса странице «Управление правами доступа» - «Группы» - «Настройки доступа». По умолчанию все способы авторизации отключены. Для включения ограничения доступа пользователей к подключаемым USB устройствам необходимо нажать соответствующую кнопку интерфейса.

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!!! Настройки доступа настраиваются для каждой группы отдельно.

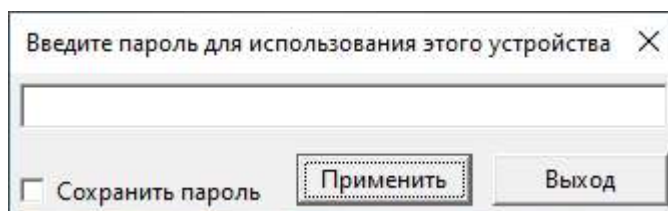
ВНИМАНИЕ!!! При совместном использовании правила применяются через «И». Для предоставления доступа к устройству должны будут выполняться все включенные правила. Настройку правил доступа рекомендуется выполнять по одному правилу, после чего включать совместные режимы ограничения.

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



4.4.3.1.1 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.

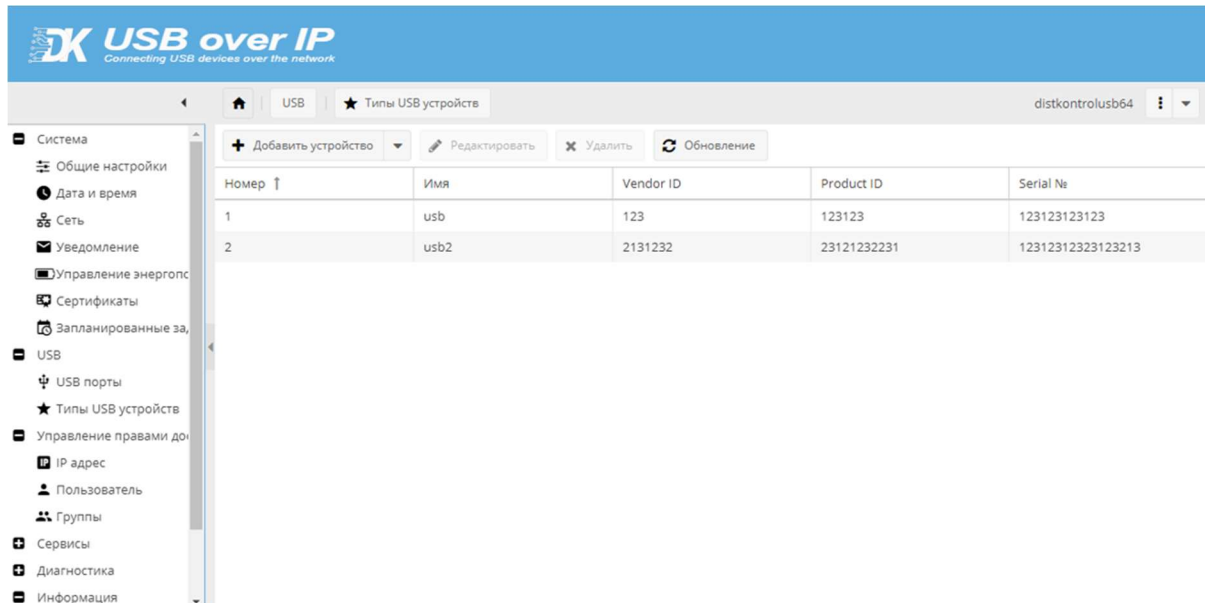


При правильном вводе пароля устройство USB будет подключено к компьютеру пользователя и до перезапуска клиента ввод пароля больше не потребуется даже при отключении и повторном подключении к устройству.

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).

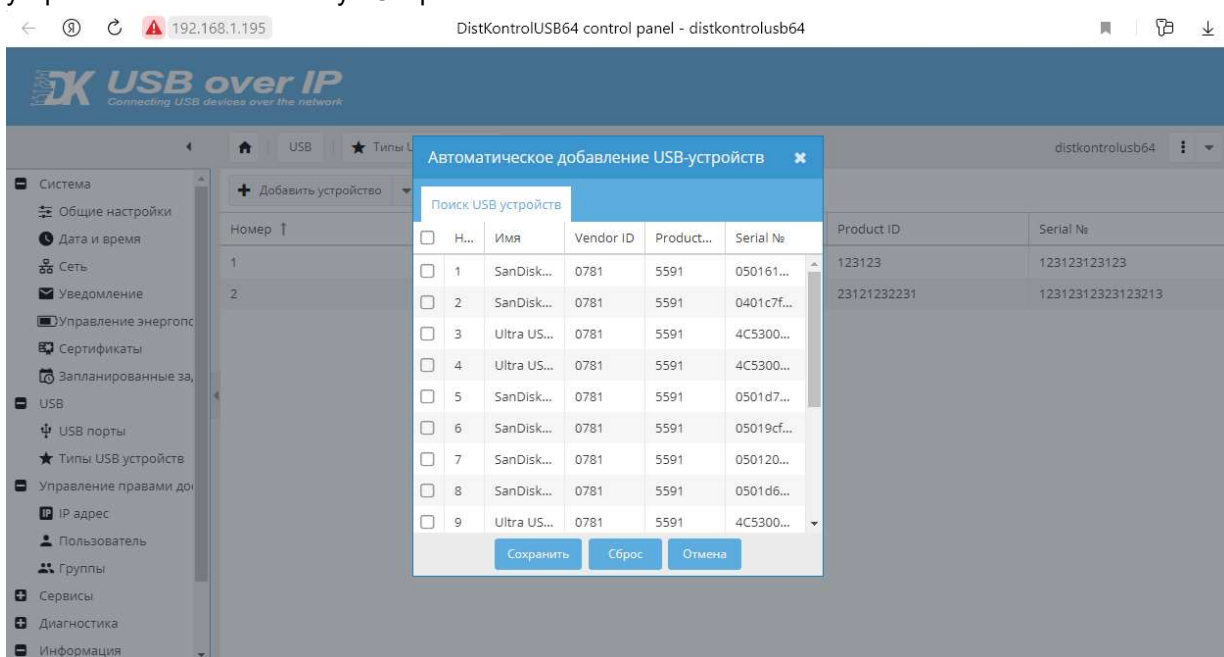
Для настройки режима ограничения доступа к USB устройству по логину и паролю необходимо:

1. На странице WEB интерфейса администратора «Сервисы» - «Типы USB устройств» добавить BCE USB устройства, которые будут использоваться. Устройство работает по принципу: «Запрещено все, что явно не разрешено»
- 2.



USB устройства можно добавить:

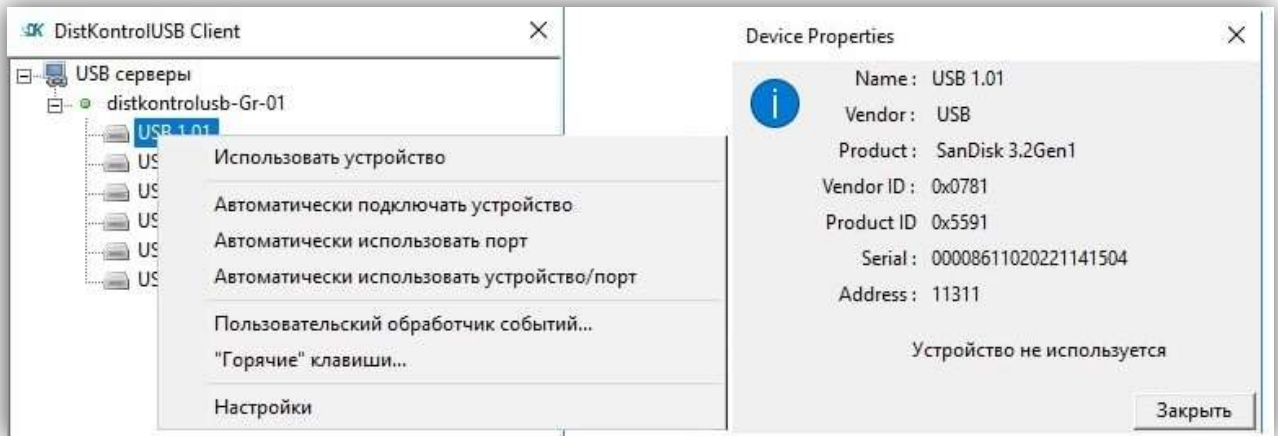
1.1 Из автоматически генерируемого списка подключенных к концентратору USB устройств (включенных на странице «USB входы»). «Добавить устройства» - «Автопоиск». В списке выбрать добавляемые USB устройства и нажать кнопку «Сохранить».



Будет выдан отчет о результате добавления USB устройств в список.

1.2 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 строке вида:

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

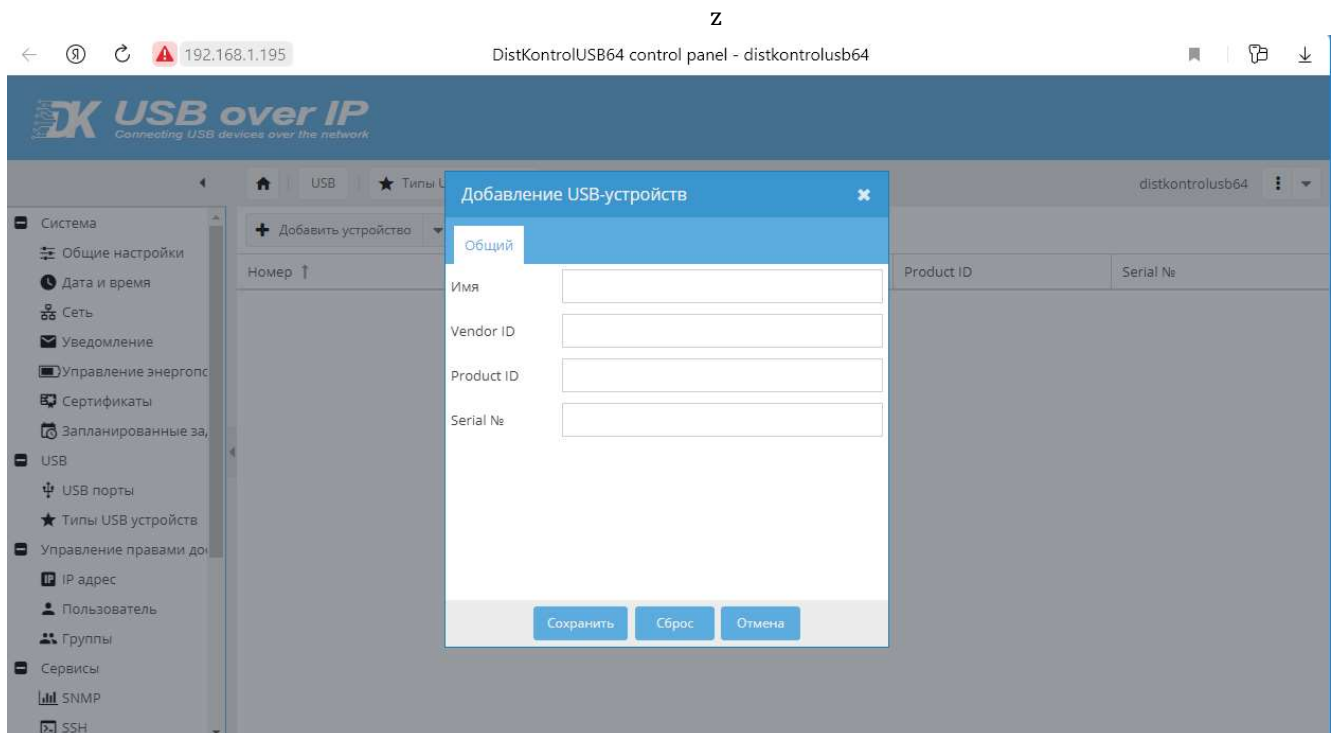
VendorID - 8564

ProductID – 1000

Serial №. - '05KVOF66TU4IHDTZ'

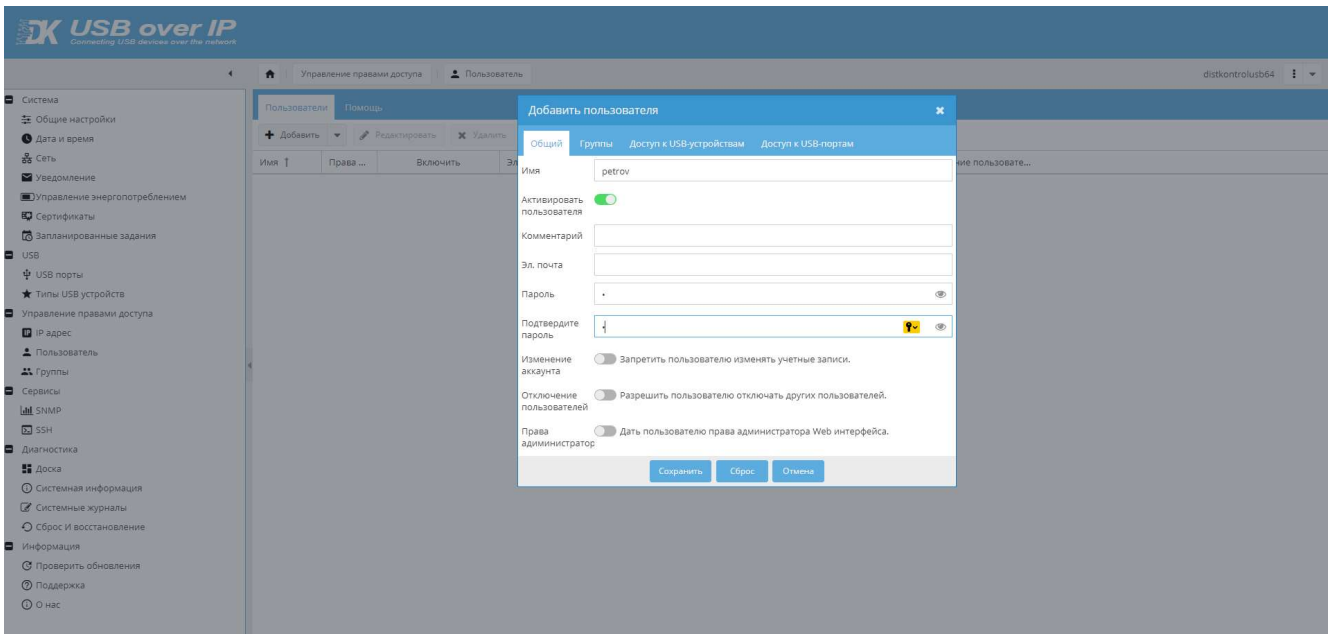
VendorID и ProductID и Serial № должны содержать только цифры и латинские буквы.

«Добавить устройства» - «Добавить вручную»



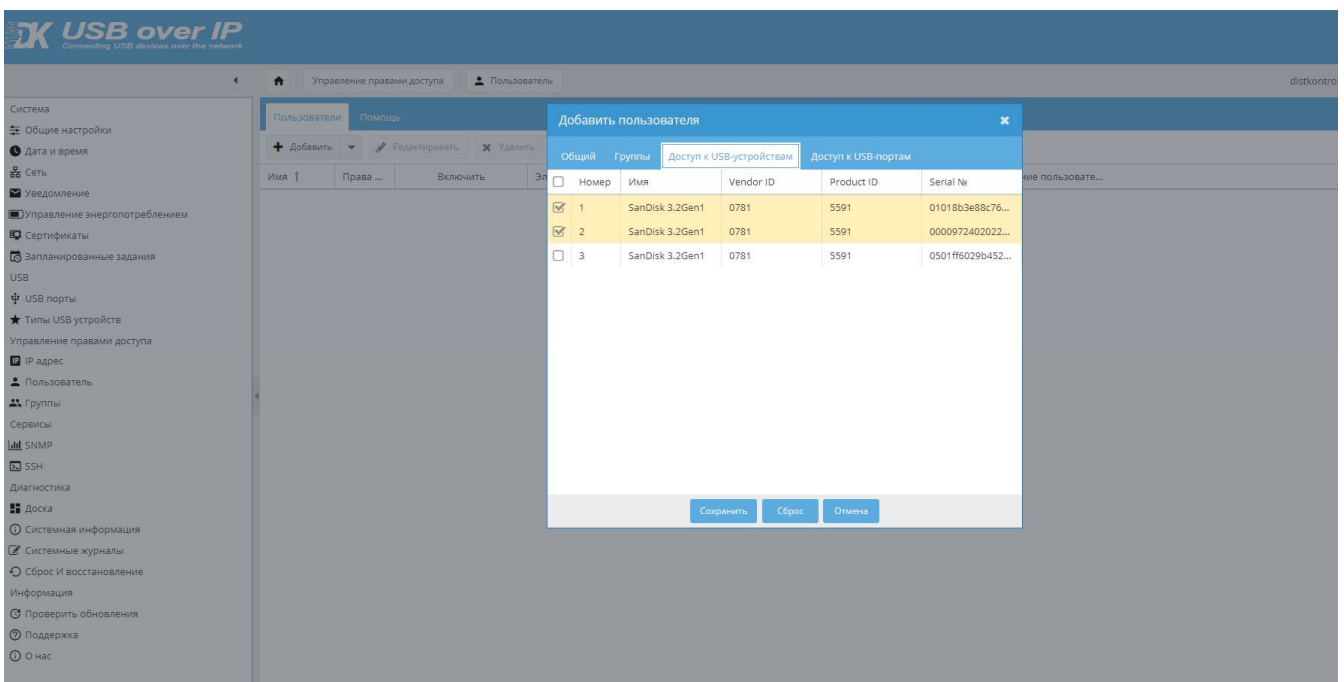
В дальнейшем возможно удаление и редактирование информации о USB устройстве:

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 вкладке «Группы» добавить пользователя в настраиваемую группу. Добавить пользователю необходимые устройства. Нажать кнопку «Сохранить» в диалоговом окне.



4. Настроить в группе видимость необходимых портов. При назначении прав пользователю будет доступно подключение USB устройств (к которым был назначен доступ при создании) в видимых портах. Если ни одного устройства не назначено, пользователь получит соответствующее уведомление об отсутствии прав на управление портами.

При подключении USB устройств пользователю будут доступны для подключения только назначенные ему устройства. При попытке подключения USB устройств, не назначенных пользователю, в клиентском приложении будет выдаваться сообщение об отсутствии прав доступа к USB устройству.

4.4.3.1.2 ОГРАНИЧЕНИЕ ДОСТУПА К USB ПОРТУ ПО ЛОГИНУ И ПАРОЛЮ

При включенном ограничении доступа к USB порту по логину и паролю – при подключении к USB порту, пользователю будет предложено ввести пароль для доступа к USB порту. 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 устройству подробно описана предыдущем параграфе

4.4.3.1.3 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.

← 192.168.1.195 DistKontrolUSB64 control panel - distkontrolusb64

DK USB over IP

Connecting USB devices over the network

Управление правами доступа IP адрес distkontrolusb64

- Система
- USB
 - USB порты
 - Типы USB устройств
- Управление правами досту
 - IP адрес**
 - Пользователь
 - Группы
- Сервисы
- Диагностика
- Информация
 - Проверить обновления
 - Поддержка
 - О нас

+ Добавить ✎ Редактировать ✕ Удалить

Номер ↑	IP адрес	Доступ к U...	Доступ к U...	Комментарий	Отключение пользо...
1	192.168.1.5			Пример IP-адреса 5	●
2	192.168.1.10			Пример IP-адреса 10	●

« < | Страница 1 из 1 | > » ↻

Отображение пунктов 1 - 2, 2

4.4.3.1.4 ОГРАНИЧЕНИЕ ДОСТУПА К USB ПОРТУ ПО IP АДРЕСУ

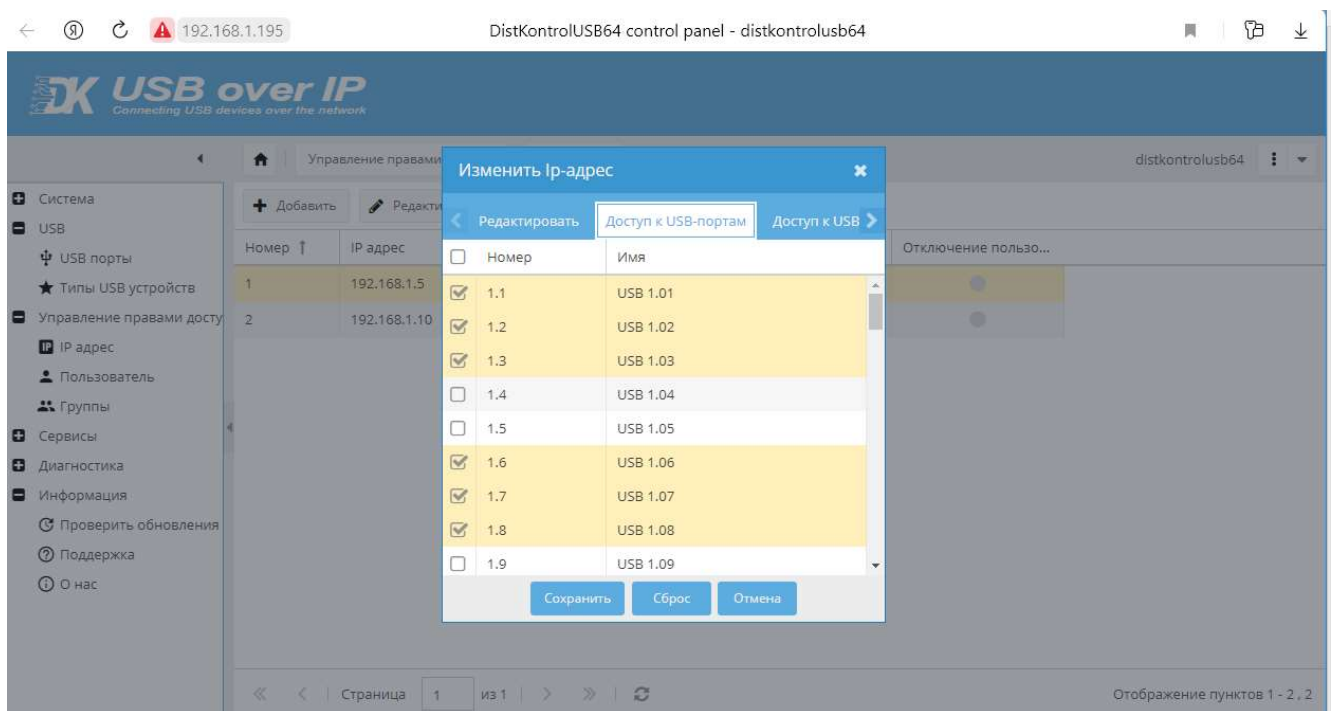
При включенном ограничении доступа к USB порту по IP адресу – подключение пользователем USB устройства будет возможно только с IP адреса с правом доступа к порту USB (не USB устройству, а именно USB порту управляемого USB over IP концентратора, не зависимо от того какое USB устройство к нему подключено).

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 невозможно.

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.

4.4.3.2 НАСТРОЙКИ ПРАВ

Настройка прав зависит от выбранной настройки доступа. В случае выбора «Ограничение прав по логину и паролю», необходимо создать пользователя и назначить ему права. Права пользователю задаются при создании, по умолчанию все права отключены. В интерфейсе все права обозначены зеленым или серым маркером в зависимости от состояния.

Всем новым пользователям можно дать права:

- дать пользователю права администратора Web интерфейса;
- изменение имени USB устройства;
- назначить пользователя определенной группе;
- дать доступ к определенным USB-устройствам;
- дать доступ к определенным USB-портам;
- отключение других пользователей в клиентском приложении DistKontrolUSB Client (при запуске клиентского приложения с параметром -a).

Добавить пользователя
✕

Общий
Группы
Доступ к USB-устройствам
Доступ к USB-портам

Имя

Активировать пользователя

Комментарий

Эл. почта

Пароль 👁

Подтвердите пароль 👁

Изменение аккаунта Запретить пользователю изменять учетные записи.

Отключение пользователей Разрешить пользователю отключать других пользователей.

Права администратор Дать пользователю права администратора Web интерфейса.

Сохранить
Сброс
Отмена

Пользователи								
Помощь								
+ Добавить ✎ Редактировать ✕ Удалить								
Имя ↑	Права админ...	Включить	Эл. почта	Комментарий	Группы	Доступ к USB-п...	Доступ к USB-устрой...	Отключение пользовате...
petrov	●	●	petrov@ya...	Директор	Group01	1.1 1.2 1.3 1.4 1...	1 2 3	●

В случае выбора «Ограничение прав IP адресу», необходимо создать IP адрес и назначить ему права.

Номер ↑	IP адрес	Доступ к U...	Доступ к USB-устро...	Комментарий	Отключение пользов...
1	192.168.1.180	1.1 1.2 1.3 ...			●

Возможно задать только отключение других пользователей в клиентском приложении DistKontrolUSB Client (при запуске клиентского приложения с параметром -a)

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

Пример 1:

Пользователю Ivanov не разрешили ни одного из правил

IP адресу 192.168.1.10 разрешили отключать другого пользователя

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 отключать другого пользователя.

Опция «Авторизация: использовать системное имя пользователя / введённое пользователем» по умолчанию «использовать системное имя пользователя». Окно с запросом пароля будет выводиться только при включенных ограничениях [прав доступа](#) по логину и паролю.

Редактировать группу

Настройки Общий **Настройки доступа** Участники Видимость USB-портов

Настройки доступа

Этот параметр вступает в силу после его сохранения.
Несколько правил применяются через 'И'.

- Ограничение доступа к USB устройству по логину и паролю
- Ограничение доступа к USB порту по логину и паролю
- Ограничение доступа к USB устройству по IP адресу
- Ограничение доступа к USB порту по IP адресу

Настройки прав

Этот параметр вступает в силу после его сохранения.

- Авторизация: использовать системное имя пользователя / введённое пользователем

Сохранить Сброс Отмена

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

The image displays two side-by-side Windows login dialog boxes. Both have the title "Введите пароль для использования этого устро...".

The left dialog box contains the following elements:

- Имя пользователя: User (User)
- Пароль: [empty field]
- Запомнить
- ОК
- Выход

The right dialog box contains the following elements:

- Имя пользователя: [empty field]
- Пароль: [empty field]
- Запомнить
- ОК
- Выход

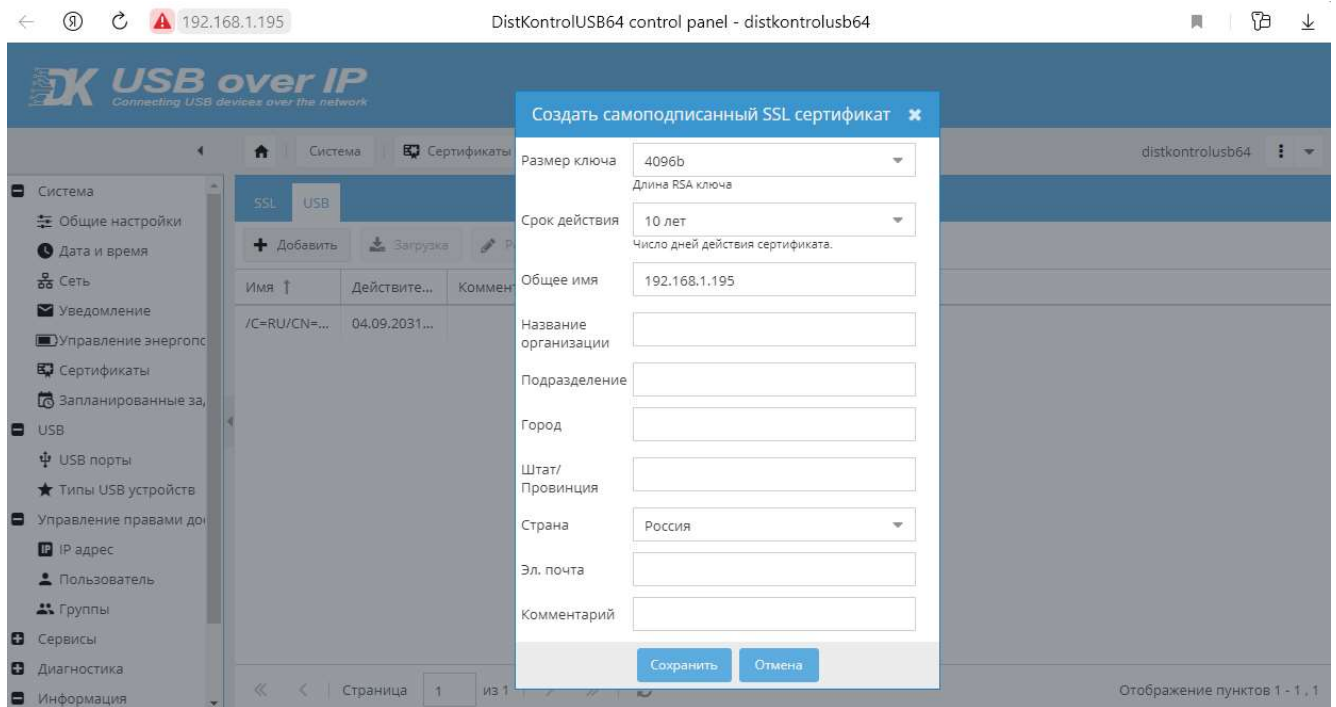
4.4.3.3 ПАРАМЕТРЫ КЛИЕНТСКОГО ПРИЛОЖЕНИЯ

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.

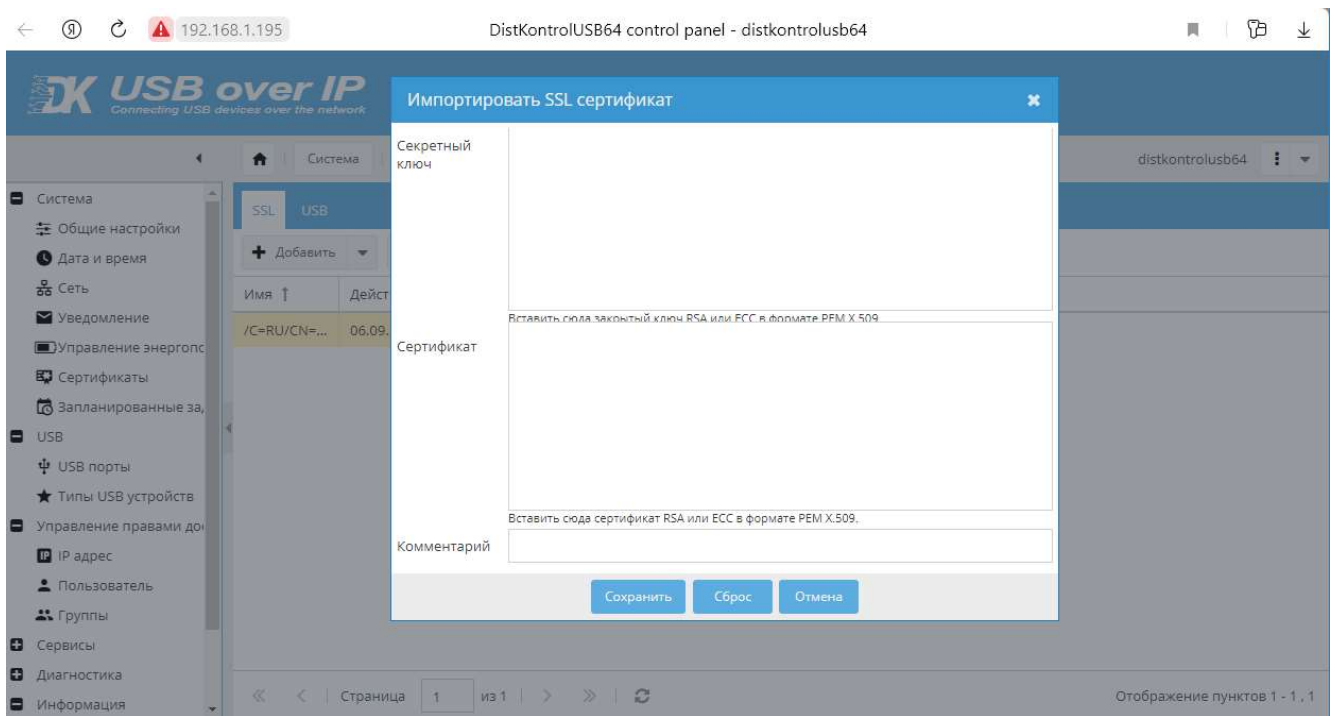
Включение режима осуществляется на странице «Группы» - «Настройки»- «Включить SSL для USB трафика». После включения режима и (или) добавления сертификатов необходима перезагрузка устройства для вступления изменений в силу.

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», далее необходимо созданному сертификату добавить группу, в которой он будет использоваться.



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»



Сертификат для клиентского приложения можно скачать на странице: «Система» - «Сертификаты» - «USB» - «Скачать сертификат».

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

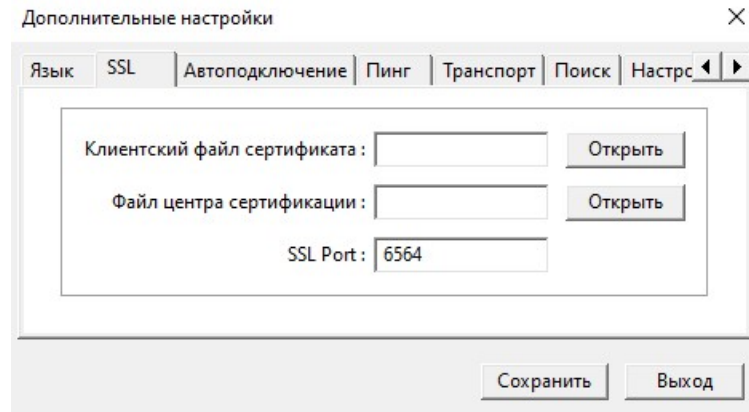
```
openssl genrsa -out usb.key 2048
```

```
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 кликните правой кнопкой мыши «USB серверы» - «Дополнительные настройки». На вкладке «SSL» в строке «Файл центра сертификации» нажмите «Открыть» и выберите Ваш сертификат *.pem. Нажмите «Сохранить» 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 DustKontrol USB, устройство в клиенте будет отображаться с соответствующим значком.



4.4.3.4 ОЧИСТКА И СБРОС

В ряде случаев возникает необходимость запрета использования USB устройства. Это возможно сделать из клиентского приложения. Кликните 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 «Группы» - «Сброс группы». После очистки списка не используемых устройств необходима перезагрузка устройства.

В WEB интерфейсе устройства на странице «USB порты» возможно переименовать USB порты. Двойным кликом по названию порта. Введите желаемое имя – Нажмите Сохранить. Изменение имени увидят все пользователи.

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

Для сброса всех настроек группы клиентского приложения, в WEB интерфейсе устройства на странице на странице «Группы» - «Сброс группы». При сбросе служба будет перезапущена.

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

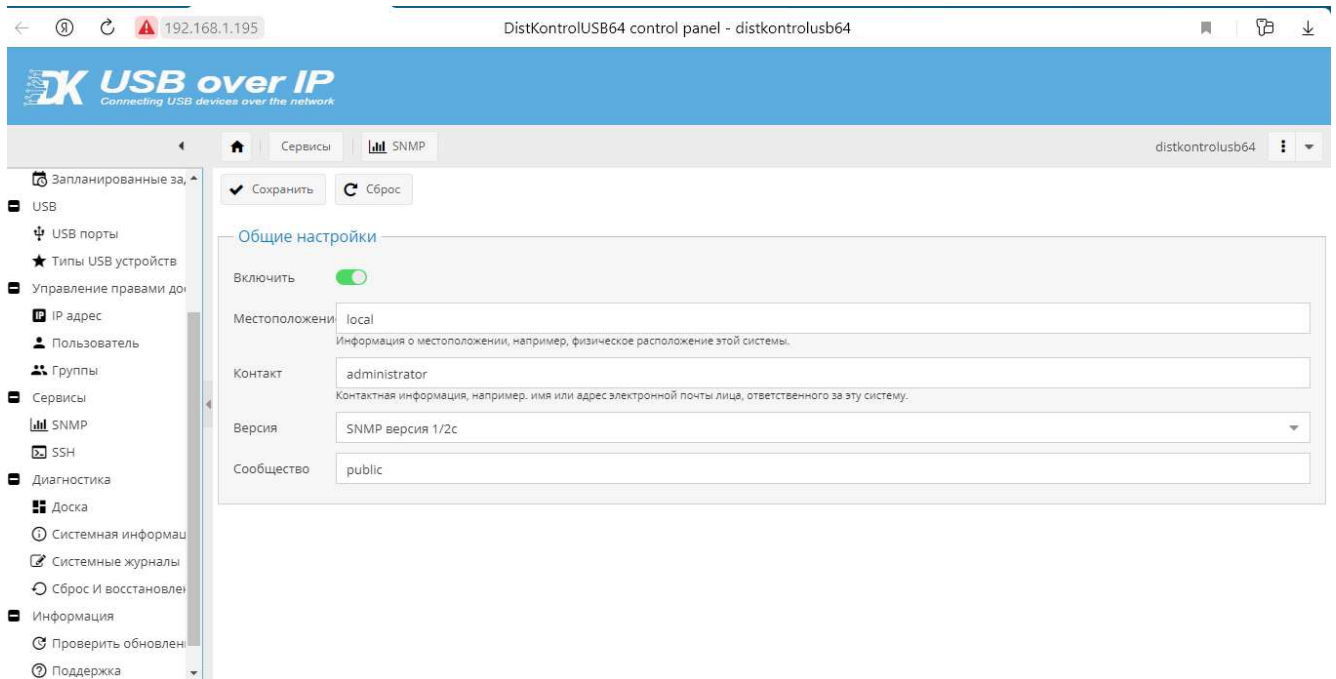
Также возможен [сброс устройства к заводским настройкам](#).

4.5 СЕРВИСЫ

4.5.1 SNMP

Управляемый USB over IP концентратор поддерживает SNMP версий 1, 2с, 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».



The screenshot displays the web interface of the DistKontrolUSB64 control panel. The browser address bar shows the IP address 192.168.1.195 and the page title "DistKontrolUSB64 control panel - distkontrolusb64". The interface features a blue header with the "DK USB over IP" logo and the tagline "Connecting USB devices over the network". Below the header, a navigation menu includes "Сервисы" (Services) and "SNMP". The main content area is titled "Общие настройки" (General settings) and contains the following configuration options:

- Включить** (Enable): A toggle switch that is currently turned on (green).
- Местоположение** (Location): A text input field containing "local". Below the field is a descriptive note: "Информация о местоположении, например, физическое расположение этой системы." (Location information, for example, the physical location of this system.)
- Контакт** (Contact): A text input field containing "administrator". Below the field is a descriptive note: "Контактная информация, например, имя или адрес электронной почты лица, ответственного за эту систему." (Contact information, for example, the name or email address of the person responsible for this system.)
- Версия** (Version): A dropdown menu currently set to "SNMP версия 1/2с" (SNMP version 1/2c).
- Сообщество** (Community): A text input field containing "public".

At the top of the configuration area, there are two buttons: "Сохранить" (Save) and "Сброс" (Reset). On the left side of the interface, a sidebar menu lists various system management options, including "USB", "USB порты", "Типы USB устройств", "Управление правами доступа", "IP адрес", "Пользователь", "Группы", "Сервисы", "SSH", "Диагностика", "Доска", "Системная информация", "Системные журналы", "Сброс и восстановление", "Информация", "Проверить обновления", and "Поддержка".

Для настройки SNMP версий 1, 2с:

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 состоянии управляемого USB over IP концентратора по SNMP:

OID (Object Identifier)	Параметр	Примечания
.1.3.6.1.2.1.1.5.0	Имя хоста DistKontrolUSB	
.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	

.1.3.6.1.4.1.2021.20.5.1	Состояние блока питания 1	Включен/выключен (1/0)
.1.3.6.1.4.1.2021.20.5.2	Состояние блока питания 2	Включен/выключен (1/0)
.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)

.1.3.6.1.4.1.2021.20.3.12	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)

4.5.1.1 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
```

4.5.1.2 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.

Настройка элементов данных

192.168.0.122/zabbix/items.php?form=update&hostid=10278&itemid=26930

ZABBIX Мониторинг Инвентаризация Отчеты Настройка Администрирование

Группы узлов сети Шаблоны Узлы сети Обслуживание Действия Корреляция событий Обнаружение Услуги

Элементы данных

Все узлы сети / usboverip-64 Активировано ZBX SNMP MMX IPMI Группы элементов данных: Элементы данных 20 Триггеры Графики 14 Правила обнаружения Веб-сценарии

Элемент данных Предобработка

Имя: Temperature CPU

Тип: SNMPv2 агент

Ключ: snmp-temp-1

Интерфейс узла сети: 192.168.0.180:161

SNMP OID: .1.3.6.1.4.1.18565.1.12.101.1.101

SNMP community: public15

Порт: 161

Тип информации: Числовой (с плавающей точкой)

Единица измерения: град.С

Интервал обновления: 30s

Тип	Интервал	Период	Действие
<input checked="" type="checkbox"/> Переменный	<input type="text" value="По расписанию"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00:24:00"/>

Период хранения истории: 90d Переопределено глобальные настройки очистки истории (360d)

Период хранения динамики изменений: 365d Переопределено глобальные настройки очистки истории (360d)

Отображение значения: Как есть

Новая группа элементов данных:

Группы элементов данных:

Все обязательные поля ввода отмечены красной звездочкой.

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.

Настройка графиков

Не защищено | 192.168.0.122/zabbix/graphs.php?form=update&graphid=1316&hostid=10278

ZABBIX Мониторинг Инвентаризация Отчеты Настройка Администрирование

Группы узлов сети Шаблоны Узлы сети Обслуживание Действия Корреляция событий Обнаружение Услуги

Графики

Все узлы сети / usboverip-64 Активировано ZBX SAMP JMX RMI Группы элементов данных Элементы данных 20 Триггеры Графики14 Правила обнаружения Веб-сценарии

График Предпросмотр

Имя: CPU Load

Ширина: 900

Высота: 200

Тип графика: Нормальный

Отображать легенду:

Отображать рабочее время:

Отображать триггеры:

Процентная линия (слева):

Процентная линия (справа):

МИН значение оси Y: Вычисляемое

МАКС значение оси Y: Вычисляемое

Элементы данных	Имя	Функция	Стиль отрисовки	Расположение оси	Цвет	Действие
1:	usboverip-64: 1 minute CPU Load	все	Линия	По левой стороне	1A7C11	Удалить
2:	usboverip-64: 5 minute CPU Load	все	Линия	По левой стороне	F63100	Удалить
3:	usboverip-64: 15 minute CPU Load	все	Линия	По левой стороне	2774A4	Удалить

Добавить

Обновить Клонировать Удалить Отмена

Zabbix 3.4.15 © 2001–2018, Zabbix SIA

Шаг 5. Далее создаем комплексные экраны:

Пользовательские комплексные экраны

Не защищено | 192.168.0.122/zabbix/screens.php?ddreset=1

usboverip-64: CPU Load (12ч)

	посл	мин	сред	макс
1 minute CPU Load [все]	0.62333	0.36	0.63777	1.64
5 minute CPU Load [все]	0.54433	0.45	0.63666	1.25
15 minute CPU Load [все]	0.56667	0.56	0.64444	0.98

usboverip-64: 5 minute CPU Load (12ч)

	посл	мин	сред	макс
5 minute CPU Load [все]	0.54433	0.45	0.63666	1.25

usboverip-64: 5 minute CPU Load (12ч)

	посл	мин	сред	макс
5 minute CPU Load [все]	0.54433	0.45	0.63666	1.25

usboverip-64: USB 4.x (12ч)

	посл	мин	сред	макс
USB 4.1 [сред]	0	0	0.8898	1
USB 4.2 [сред]	1	0	0.0895	0
USB 4.3 [сред]	0	0	0	0
USB 4.4 [сред]	0	0	0	0

usboverip-64: Idle CPU time (%) (12ч)

	посл	мин	сред	макс
Idle CPU time (%) [все]	85%	75%	84.97%	86%

usboverip-64: Temperature CPU (12ч)

	посл	мин	сред	макс
Temperature CPU [сред]	50.33 град.С	49 град.С	50.59 град.С	53 град.С

4.5.2 SSH

SSH используется для управления питанием портов и 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»](#)

4.5.2.1 НАСТРОЙКИ SSH

На странице «Настройки» возможно изменить стандартный порт. Также возможно управлять включением и выключением данного функционала.

4.5.2.2 ПАРОЛЬ

На странице «Пароль» возможно задать/изменить пароль для пользователя UsbControl. Это необходимо сделать при первом же использовании утилиты. В пароле можно использовать все спецсимволы(кроме одинарной кавычки).

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».

4.6.3.1 ЖУРНАЛЫ

На странице журналы 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.

Существует фильтрация сообщений на сообщения, присылаемые системой и e-mail сообщения (настраивается в выпадающем списке). Также существует возможность очистить журнал с помощью кнопки «Очистить».

Кнопки «Загрузка» и «Диагностический файл» предназначены для загрузки системной информации при обращении в техническую поддержку.

Дата и время ↓	сообщение
Thu Oct 29 15:59:28 2020	Device 11212 [148f:7601] UNBOUND from connection 10
Thu Oct 29 15:59:26 2020	Device 11212 [148f:7601] BOUND to connection 10
Thu Oct 29 15:59:25 2020	[Authorization Client] User: ['Tester' '192.168.1.42'] USB: ['148f:7601', '1.0', '/sys/bus/usb/devices/1-1.2.1.2']
Thu Oct 29 15:59:25 2020	[Authorization Client] PORT OK : ['1.2' '1.1 1.2']
Thu Oct 29 15:59:25 2020	[Authorization Client] Password OK : ['Tester']
Thu Oct 29 15:59:25 2020	[Authorization Client] User name OK : ['Tester']
Thu Oct 29 15:59:25 2020	[Authorization Client] User: ['Tester', 'c4ca4238a0b923820dcc509a6f75849b', '192.168.1.42'] USB: ['148f:7601', '1.0', '/sys/bus/usb/devices/1-1.2.1.2']
Thu Oct 29 15:59:09 2020	[Authorization Client] The user was not found in the database. BAD : ['Dist']
Thu Oct 29 15:59:09 2020	[Authorization Client] User: ['Dist', 'c4ca4238a0b923820dcc509a6f75849b', '192.168.1.42'] USB: ['148f:7601', '1.0', '/sys/bus/usb/devices/1-1.2.1.2']
Thu Oct 29 15:58:49 2020	[Authorization Client] Password BAD : ['Petrov']
Thu Oct 29 15:58:49 2020	[Authorization Client] User name OK : ['Petrov']
Thu Oct 29 15:58:49 2020	[Authorization Client] User: ['Petrov', 'c4ca4238a0b923820dcc509a6f75849b', '192.168.1.42'] USB: ['148f:7601', '1.0', '/sys/bus/usb/devices/1-1.2.1.2']
Thu Oct 29 15:58:44 2020	Connection 2 successfully removed (reason:timeout)
Thu Oct 29 15:58:44 2020	Device 11211 [148f:7601] UNBOUND from connection 2
Thu Oct 29 15:58:36 2020	192.168.1.42 connected as connection 10
Thu Oct 29 15:58:36 2020	Connection 2 remotely disconnected gracefully (rx msg size)
Thu Oct 29 15:58:24 2020	[Authorization Client] Password BAD : ['Ivanov']
Thu Oct 29 15:58:24 2020	[Authorization Client] User name OK : ['Ivanov']

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

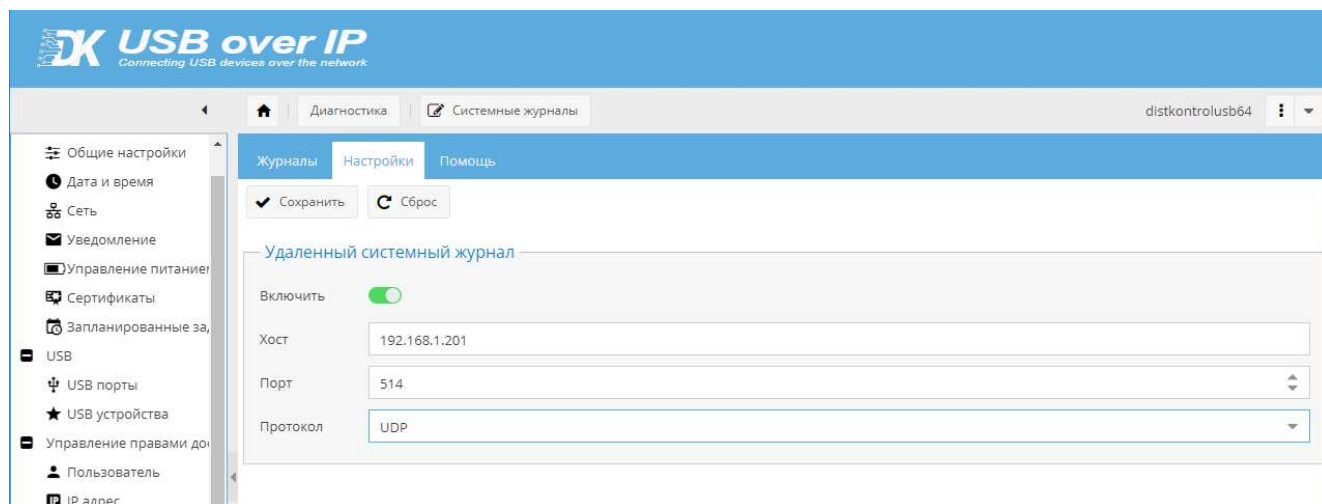
Path: Текущий номер USB устройства используемый пользователем (внутренний служебный)

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

4.6.3.2 НАСТРОЙКИ

На странице «Настройки» возможно настроить 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
```

4.6.3.3 ПОМОЩЬ

На странице «Помощь» описан пример настройки удаленного сервера.

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
```

4.6.3.4 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) – 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.

4.6.3.5 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 »

4.6.3.6 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:

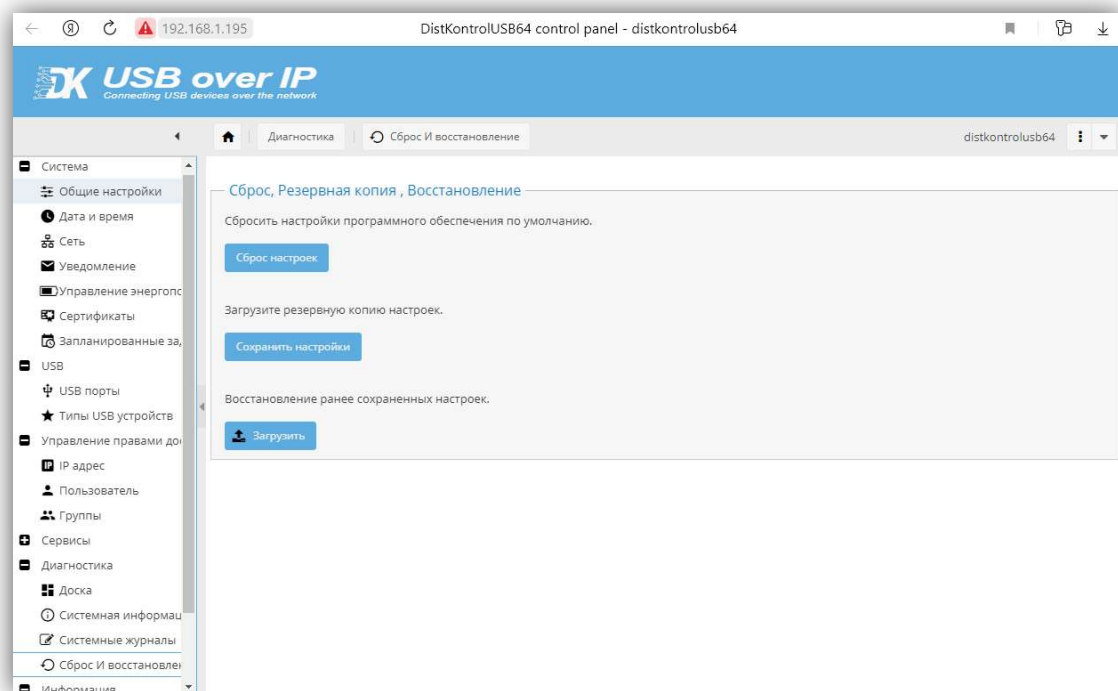
[USB Settings] Restricting access to the USB port by login and password – DISABLED:

- [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 СБРОС И ВОССТАНОВЛЕНИЕ

Страница позволяет:

1. Произвести сброс настроек программного обеспечения до состояния по умолчанию.
2. Загрузить резервную копию настроек.
3. Восстановить ранее сохраненные настройки.



Сброс настроек программного обеспечения к параметрам по умолчанию осуществляется нажатием на кнопку «Сброс настроек», в появившемся окне будет необходимо подтвердить сброс.

Сохранить имеющиеся настройки ПО возможно нажатием кнопки «Сохранить настройки», далее необходимо подтвердить загрузку копии.

Восстановить настройки ПО возможно нажатием на кнопку «Загрузить». После чего выбрать сохраненный файл настроек. После загрузки файла устройство будет перезагружено.

Внимание!!! Восстановление настроек с v.2 до v.3 а также с v.3 до v.4 невозможно. Если необходимо произвести данные действия в рамках одной версии воспользуйтесь [VNC](#) или же обновите ПО до актуальной версии. Перенос настроек и Восстановление возможно начиная с v.4 в рамках одного серийного устройства. При переименовании файла настроек не используйте пробелы.

Внимание!!! Сброс настроек происходит на той версии ПО, которая стоит по умолчанию. Если через подключение по VNC загрузка будет произведена на другую версию, не имеющую статуса "Set default", то при попытке сброса настроек в WEB интерфейсе сбросятся настройки на той версии, у которой статус "Set default").

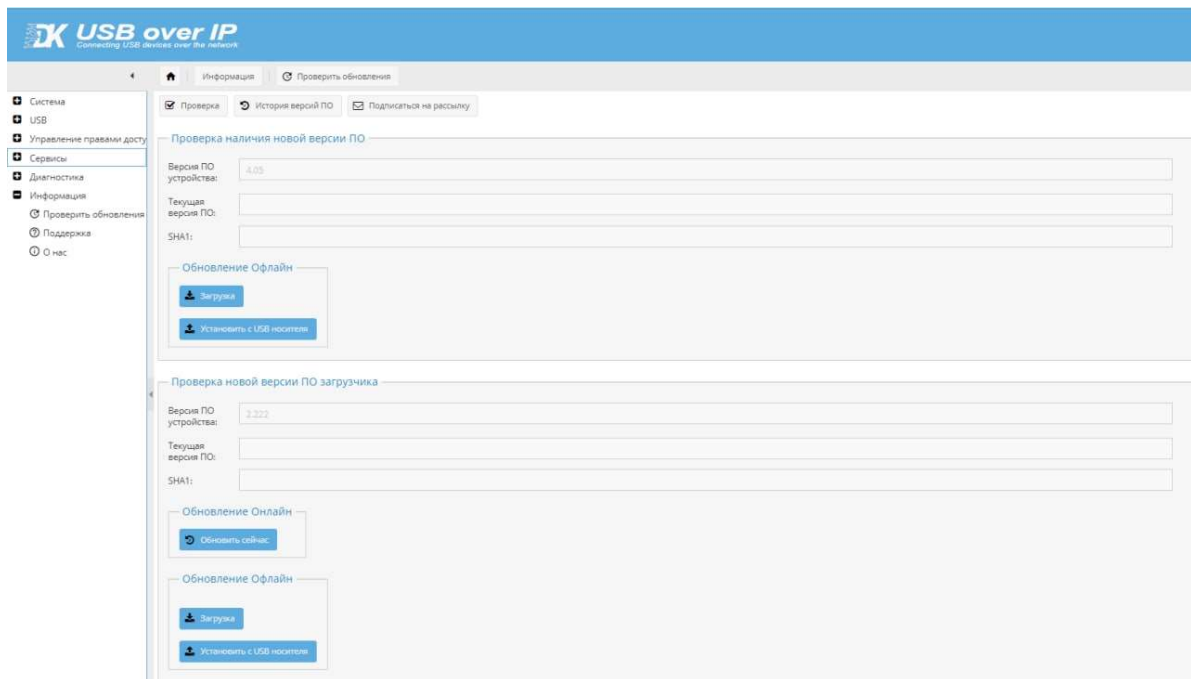
4.7 ИНФОРМАЦИЯ

4.7.1 ПРОВЕРИТЬ ОБНОВЛЕНИЕ

Данный пункт меню позволяет:

1. Проверить наличие новой версии ПО концентратора и, при наличии, скачать его для обновления через USB накопитель.
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 **«История версий ПО»** - открывает страницу с историей изменений в новом окне.

Кнопка **«Подписаться на рассылку»** - о выходе новых продуктов и обновлений.

Кнопка **«Загрузка»** - позволяет скачать последнюю доступную версию ПО для обновления концентратора с USB накопителя. Подробнее см. [«Обновление ПО»](#).

Кнопка **«Установить с USB накопителя»** - устанавливает обновление с USB накопителя находящегося в порту 1.1 .

«SHA1» - контрольная сумма файла прошивки.

ВНИМАНИЕ!!! Не выключайте питание до завершения обновления, выключение питания может вызвать сбой в устройстве, дальнейшее исправление сбоя будет возможно только в сервисном центре.

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.

The screenshot shows a web browser window displaying the DistKontrolUSB website. The page title is "Руководство пользователя DistKontrolUSB:". The left sidebar contains a navigation menu with categories like "Система", "USB", "Диагностика", and "Информация". The "Поддержка" (Support) option is highlighted. The main content area provides instructions for downloading the user manual and the DistKontrolUSB Client for Windows and OSX. It includes links for local and online downloads and a brief description of the client's functionality.

USB over IP
Connecting USB devices over the network

Информация | Поддержка

distkontrolusb64

Руководство пользователя DistKontrolUSB:

Скачать локально с DistKontrolUSB:
Руководство пользователя DistKontrolUSB
DistKontrolUSB user's guide EN

Скачать с сайта:
Руководство пользователя DistKontrolUSB
DistKontrolUSB user's guide EN

DistKontrolUSB Client

DistKontrolUSB Client работает на ОС Windows, OSX и Linux. Клиент разработан с интуитивно понятным и простым в использовании интерфейсом без необходимости установки. Необходимо скачать приложение с данной страницы для своей ОС и запустить на компьютере, который будет использовать USB-устройства, совместно используемые с DistKontrolUSB. (Нажмите ссылку ниже, сохраните загруженный файл на компьютер и запустите). При желании клиент может запускаться в качестве сервиса.

Программное обеспечение автоматически найдет USB-устройства, совместно используемые с DistKontrolUSB 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 вашей машине и может использоваться как локальное устройство!

Перед использованием устройства рекомендуется ознакомиться с Руководством пользователя (см. ссылки выше)

Windows:

Скачать локально с DistKontrolUSB:
DistKontrolUSB Client для Windows (32-bit)
DistKontrolUSB Client для Windows (64-bit)

Скачать с сайта:
DistKontrolUSB Client для Windows (32-bit)
DistKontrolUSB Client для Windows (64-bit)

OSX:

Скачать локально с DistKontrolUSB:
DistKontrolUSB Client для OSX 10.9.5 / 10.10 / 10.12 / 10.13 / 10.14* (* поддержка некоторых USB-устройств)
DistKontrolUSB Client для MacOS (Silicon M1 & Intel) 12 Monterey (На данный момент нет изохранной поддержки, например, веб-камеры / микрофонов, но другие устройства должны работать)

Скачать с сайта:
DistKontrolUSB Client для OSX 10.9.5 / 10.10 / 10.12 / 10.13 / 10.14* (* поддержка некоторых USB-устройств)
DistKontrolUSB Client для MacOS (Silicon M1 & Intel) 12 Monterey (На данный момент нет изохранной поддержки, например, веб-камеры / микрофонов, но другие устройства должны работать)

4.7.3 О НАС

Данный пункт меню содержит необходимую контактную информацию о нас.

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

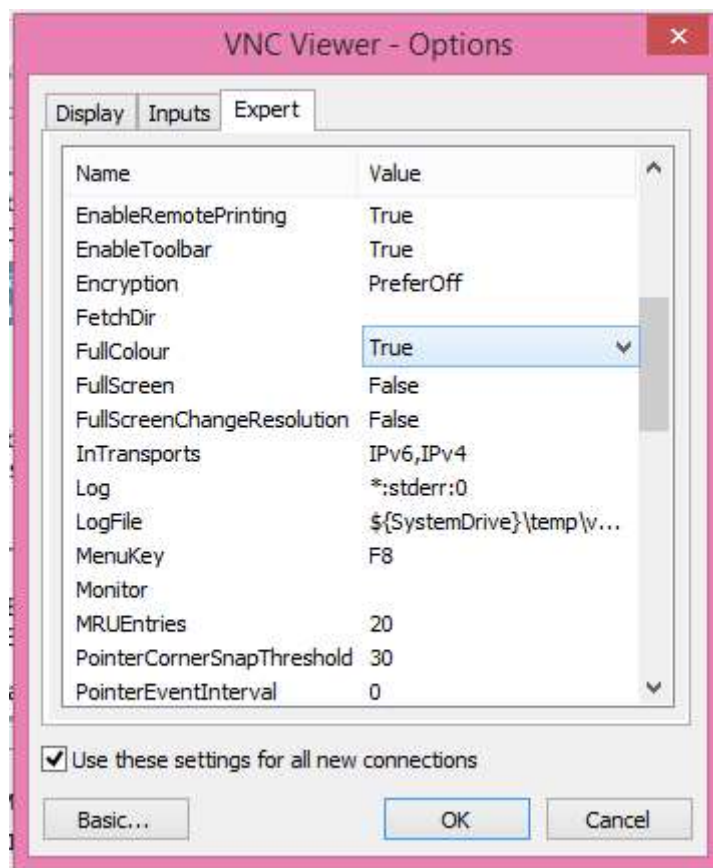
Выполнить сброс настроек возможно тремя способами:

1. [Через WEB-интерфейс устройства.](#)

2. 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.

3. 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 krds 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).

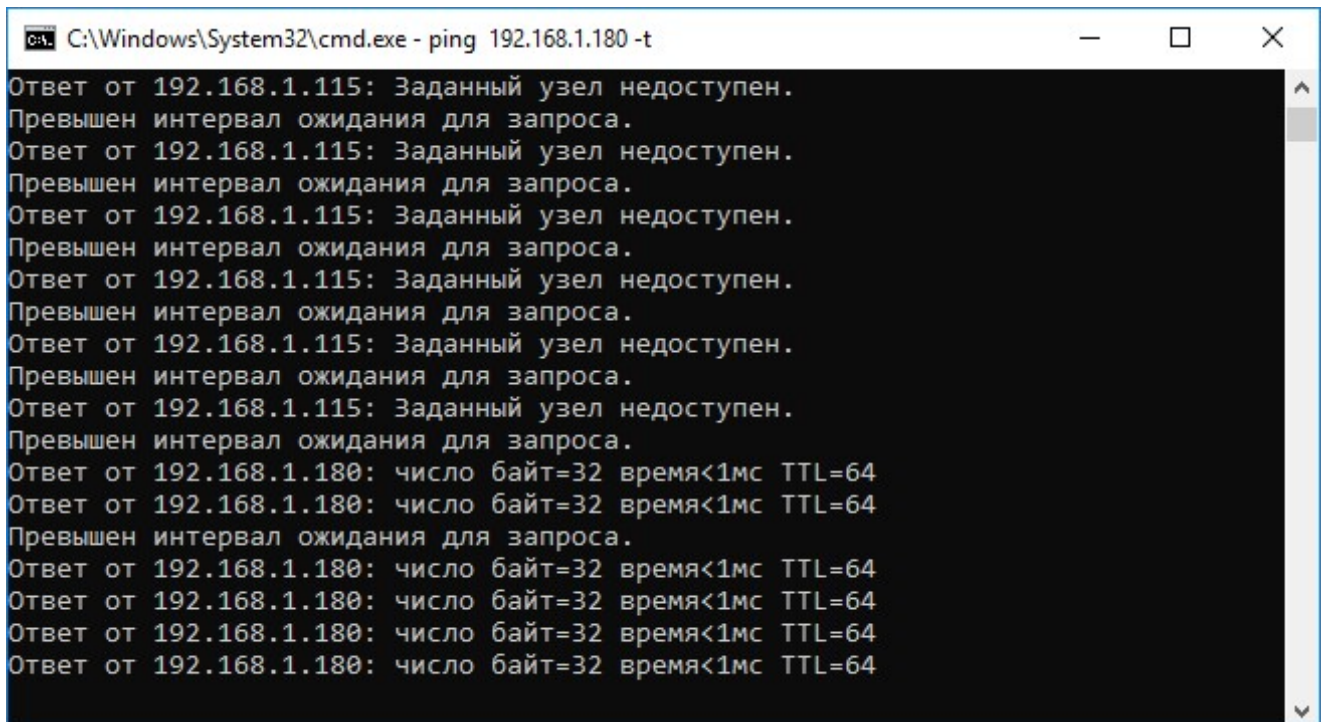
Подключение для сброса настроек возможно в течении 20 с после подачи питания на USB over IP. Рекомендуется в командной строке выполнить команду:

```
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 подключаться 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.

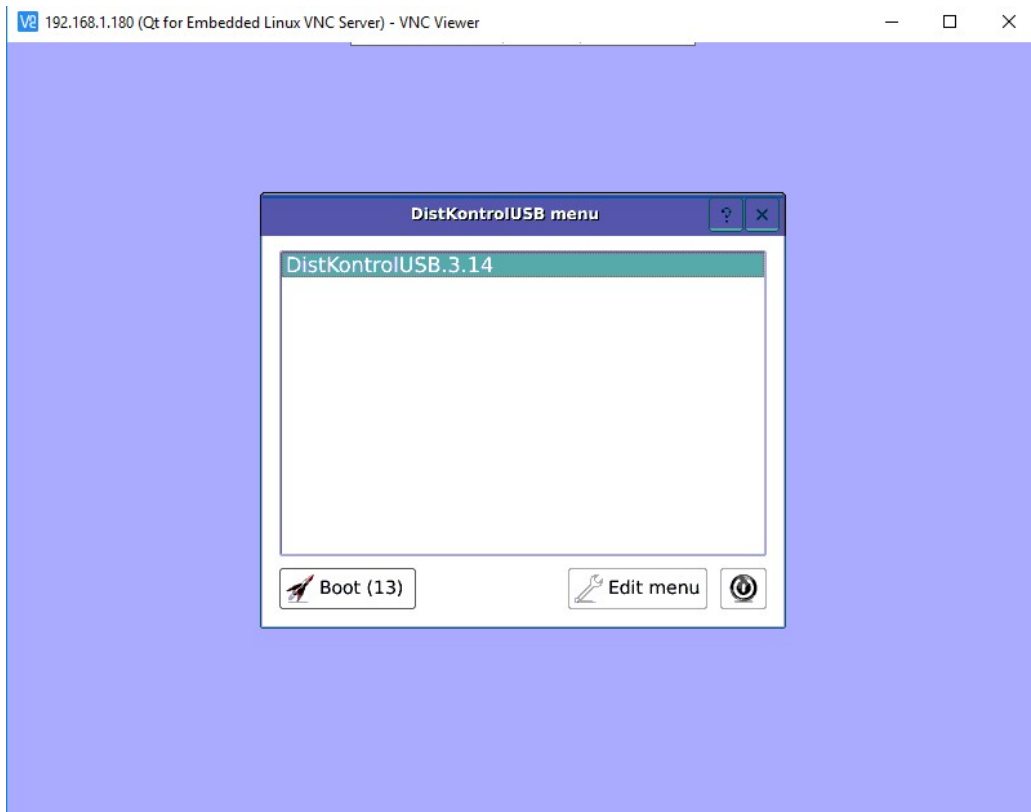


```
C:\Windows\System32\cmd.exe - ping 192.168.1.180 -t
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.180: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.180: число байт=32 время<1мс TTL=64
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.180: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.180: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.180: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.180: число байт=32 время<1мс TTL=64
```

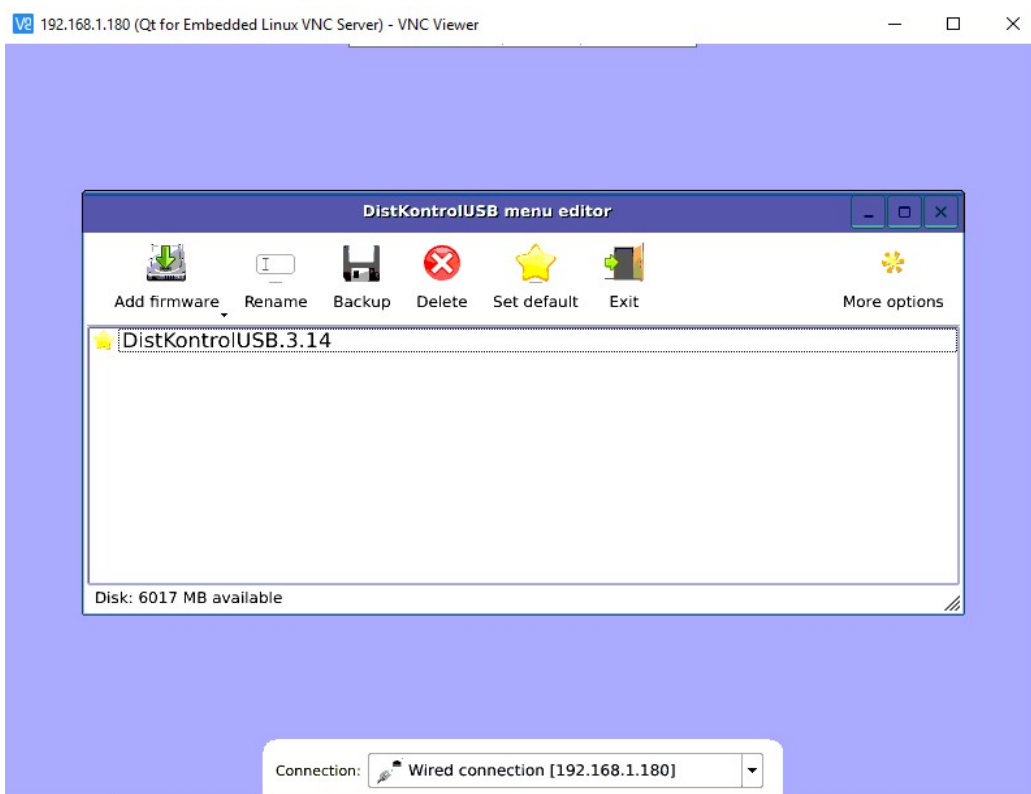
Для сброса настроек необходимо:

Последовательно в меню загрузки и восстановления USBoverIP выбрать:

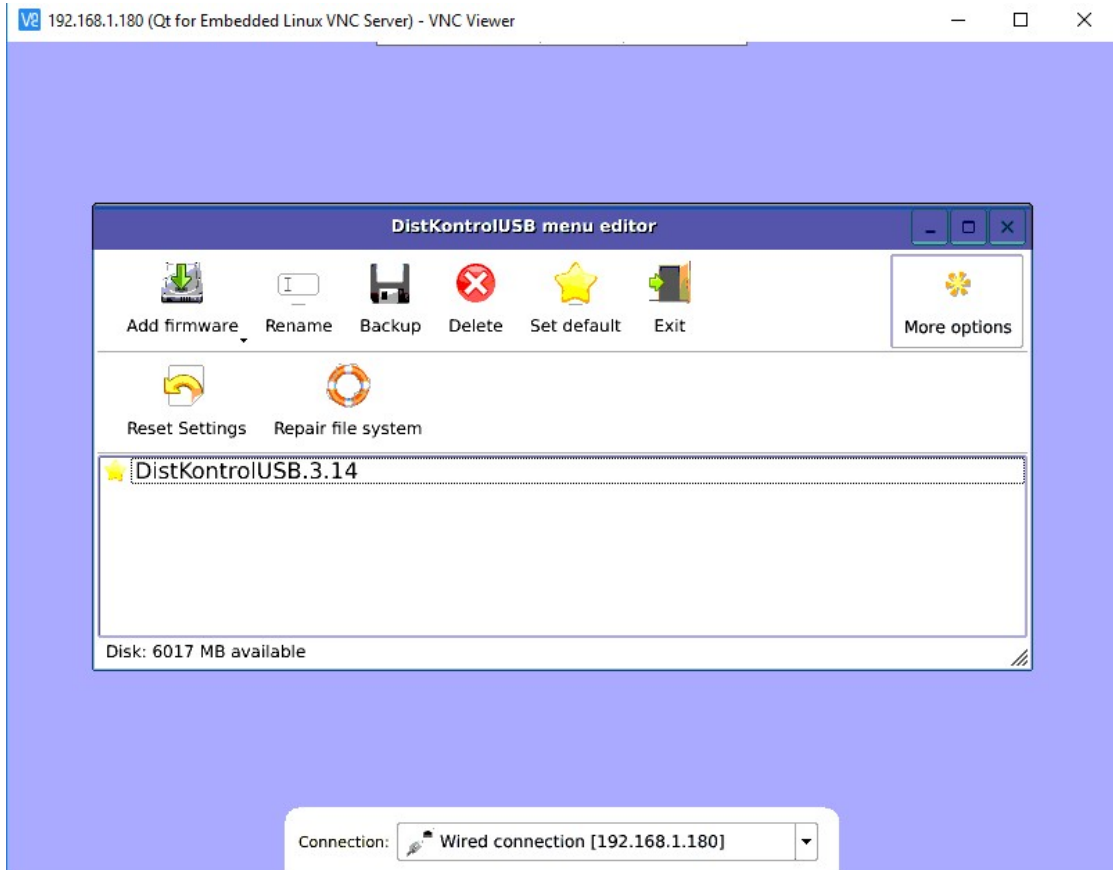
a. «Edit menu»



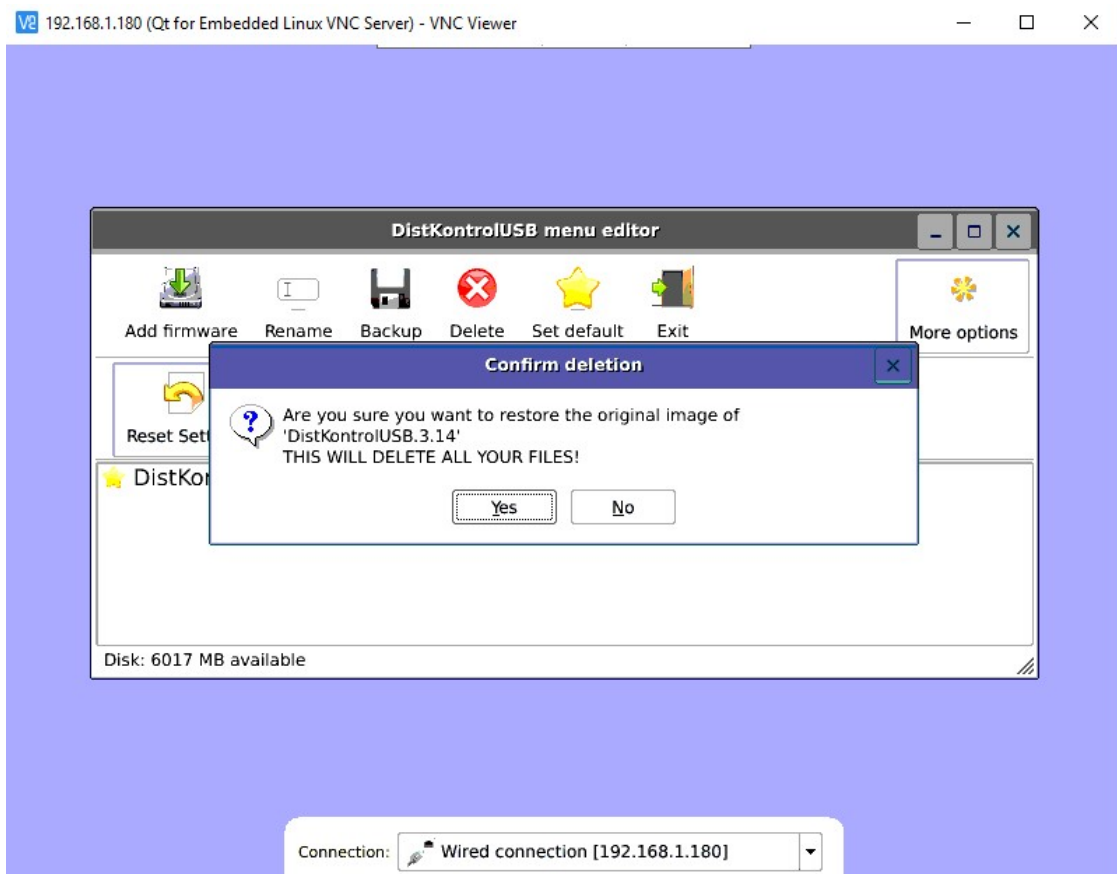
b. «More options»



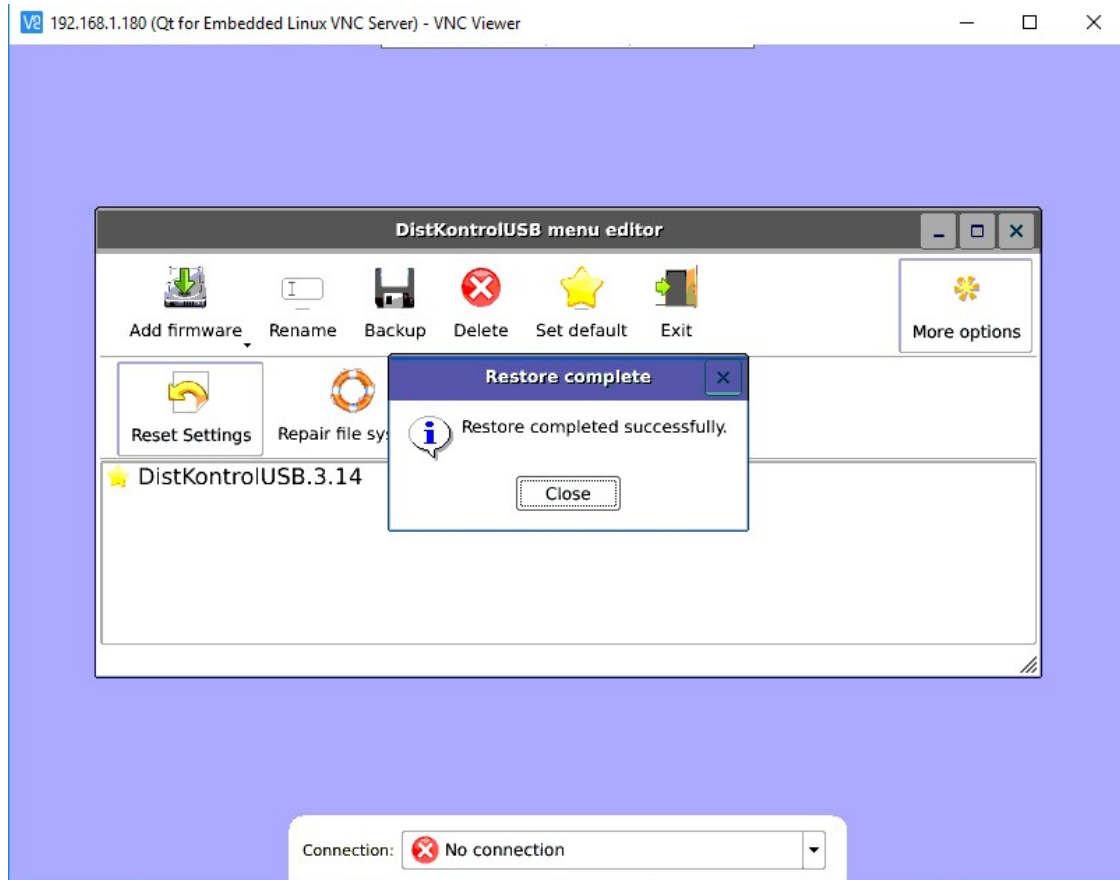
c. «Reset Settings»



d. «Yes»



е. «Close» и «Exit»



Внимание!!! Сброс настроек происходит на той версии ПО, которая стоит по умолчанию. Если через подключение по VNC загрузка будет произведена на другую версию, не имеющую статуса "Set default", то при попытке [сброса настроек в WEB интерфейсе](#) сбросятся настройки на той версии, у которой статус "Set default").

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 ключа к ПО управляемого USB over IP концентратора по изложенной в разделе [Лицензия](#).

4.9 ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УПРАВЛЯЕМОГО USB OVER IP КОНЦЕНТРАТОРА.

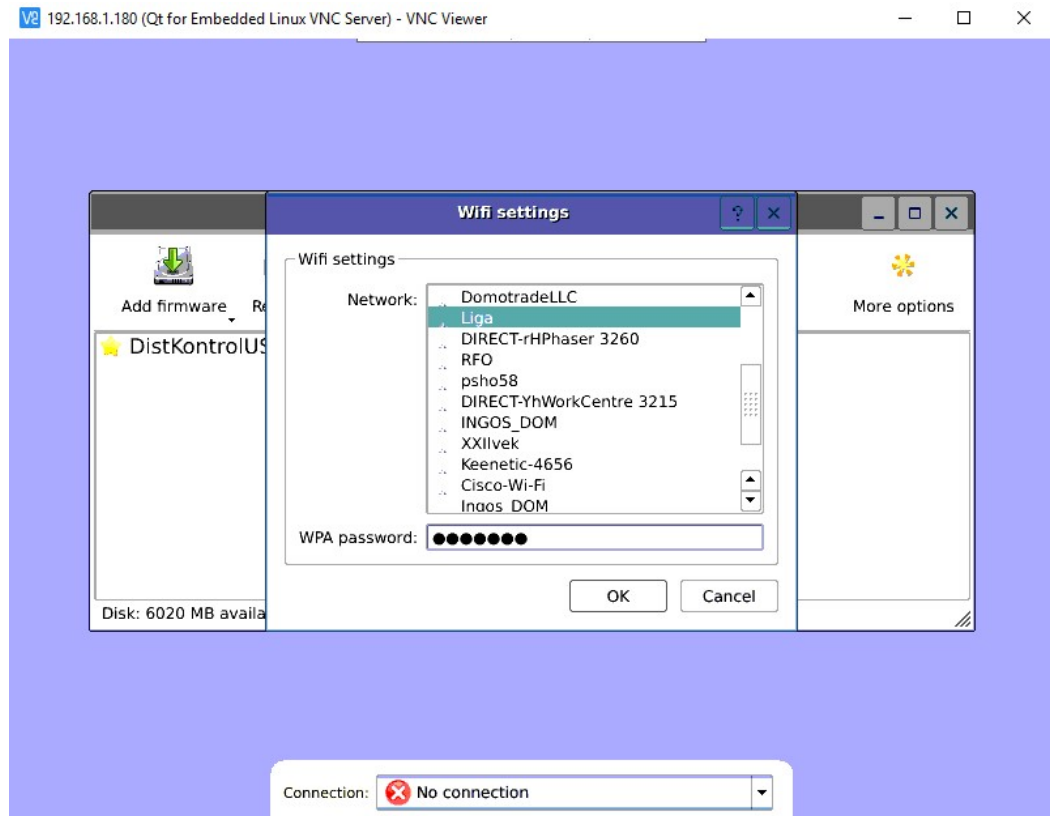
ВНИМАНИЕ!!! При обновлении программного обеспечения, управляемого USB over IP концентратора его настройки, не сохраняются и сбрасываются к исходным. Необходимо, до обновления устройства, выполнить экспорт настроек и их импорт после обновления (см. раздел [«Сохранение и восстановление настроек»](#) руководства) 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.

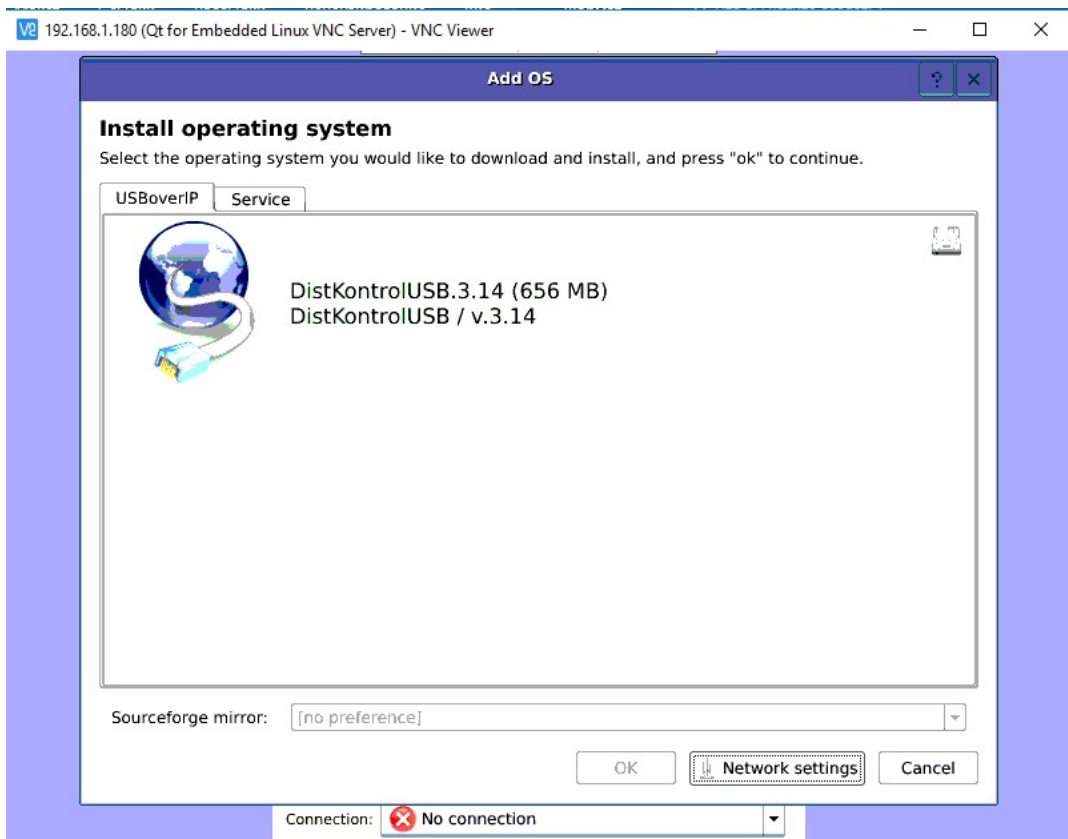
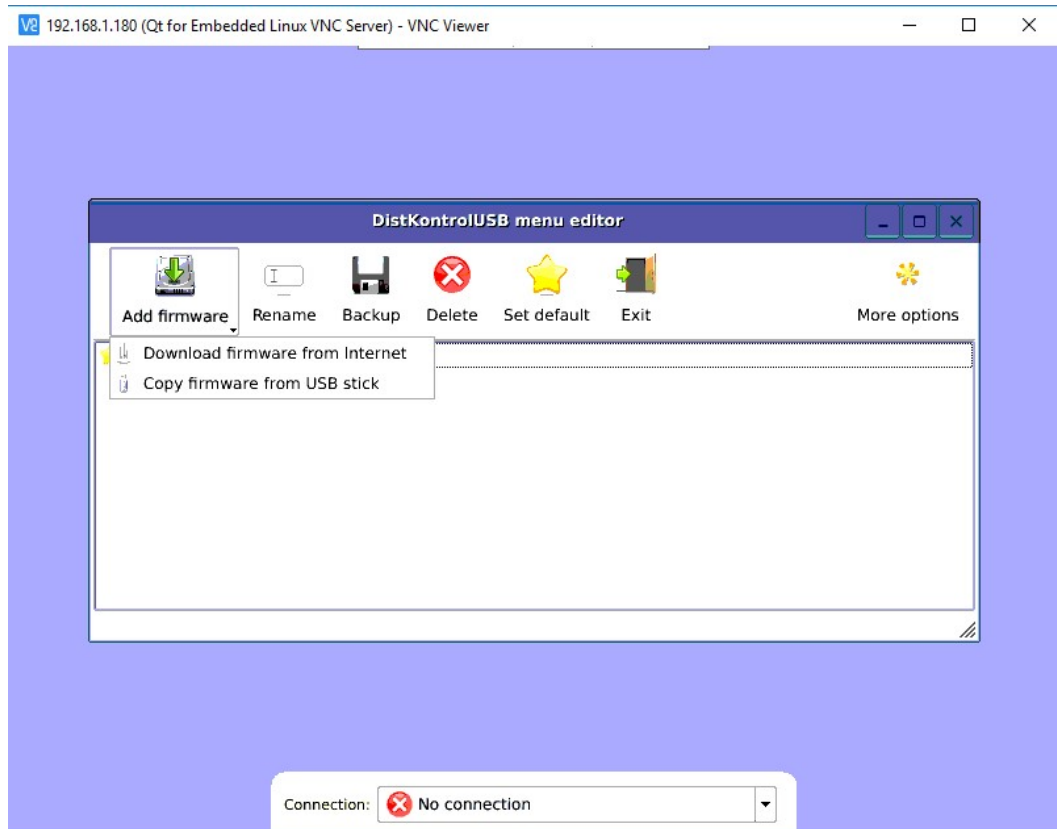
Обновление возможно двумя способами:

1. Через интернет (рекомендуемый способ обновления).
2. С флэш носителя.

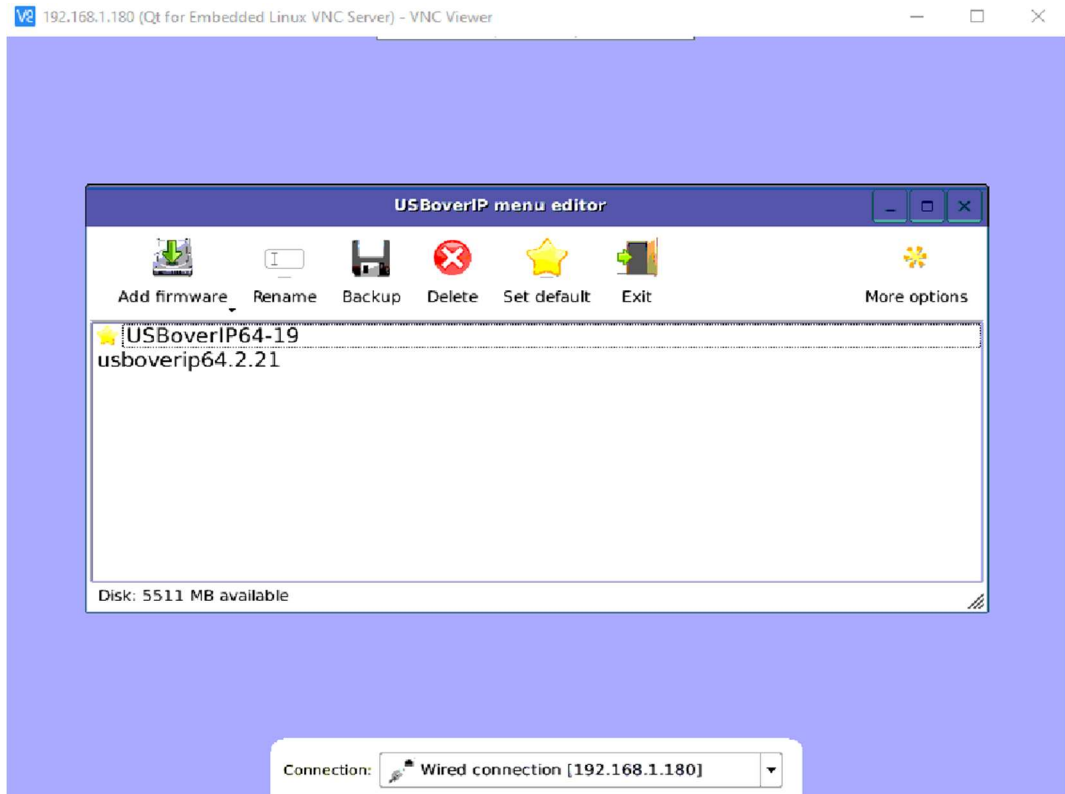
1. Для обновления через интернет необходимо обеспечить доступ к глобальной сети с адреса 192.168.1.180 по LAN устройства. Также возможно обновление ПО по WiFi. Для подключения к WiFi необходимо кликнуть по надписи «Wired connection» внизу экрана, выбрать сеть из списка доступных и ввести пароль.



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



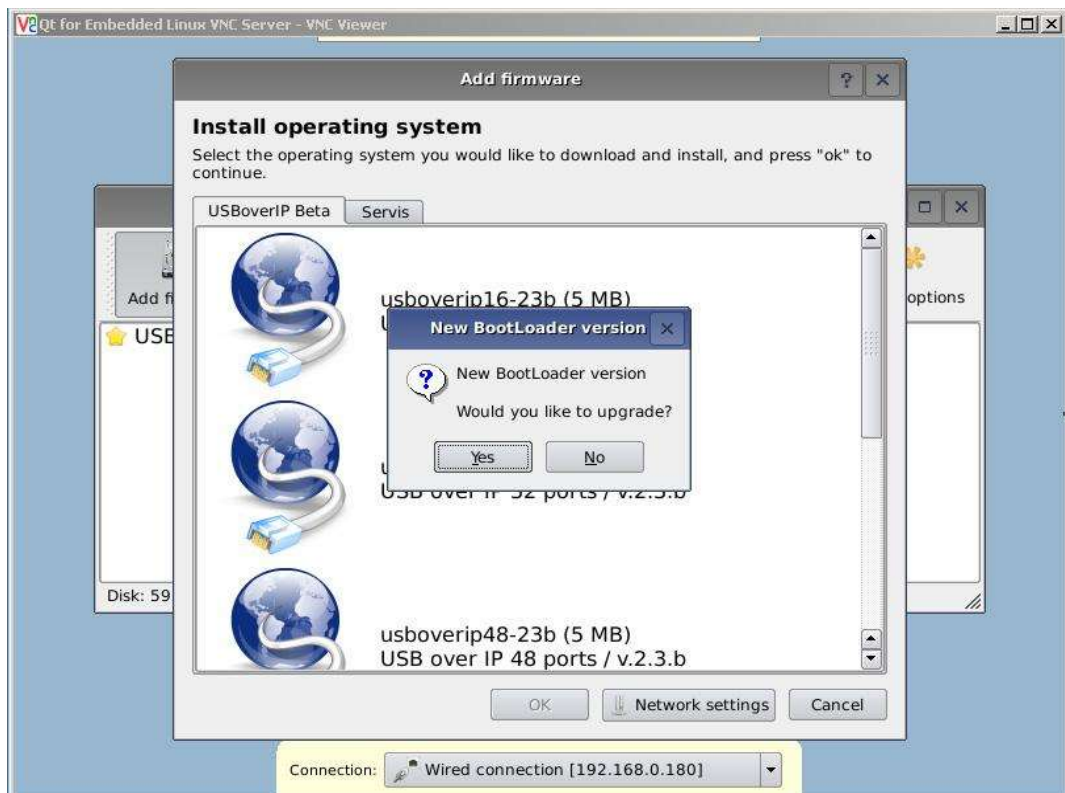
Далее выбрать версию ПО и нажать кнопку ОК. Новая версия ПО будет загружена и установлена на устройство.



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 предварительно отформатировав в его файловой системе **FAT32**. (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.

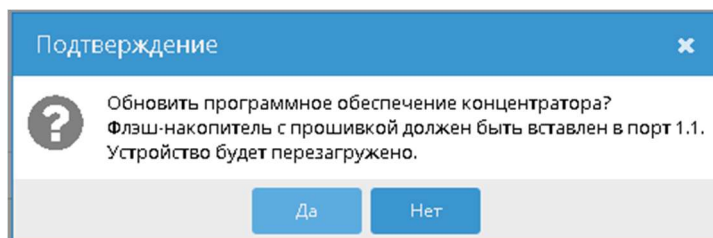
После установки вы увидите новый пункт в списке установленного ПО. Для использования новой версии ПО необходимо выбрать его в меню и нажать на кнопку «Set default», далее «Exit». Будет произведена перезагрузка устройства с новой версией ПО.

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

3. Обновление через в Web интерфейс – **«Установить»** .

Необходимо подготовить **USB Flash** накопитель для обновления ,предварительно отформатировав в его файловой системе **FAT32**. (рекомендуется использовать носители объемом 4 - 16Гб)

Записать образ *.img на USB носитель и подключить в **порт 1.1**



Нажав на кнопку **«Установить»** вы увидите сообщение если все условия выполнены будет произведено обновление программного обеспечения.

4. Обновление через в Web интерфейс [новой версии ПО загрузчика](#).

The screenshot displays a web interface titled "Проверка новой версии ПО загрузчика". It contains several input fields: "Версия ПО устройства:" with the value "2.222", "Текущая версия ПО:" (empty), and "SHA1:" (empty). Below these are two sections for updates. The "Обновление Онлайн" section contains a blue button labeled "Обновить сейчас" with a circular arrow icon. The "Обновление Офлайн" section contains two blue buttons: "Загрузка" with a download icon and "Установить с USB носителя" with a USB drive icon.

Обновление возможно двумя способами:

- 1) Онлайн(концентратор имеет доступ к сети Интернет) - Кнопка «Обновить сейчас».
- 2) Офлайн(у концентратора нет доступа к сети Интернет) - Кнопка «Загрузка» - загрузить обновление в виде файла.

Кнопка «Установить с USB носителя» - находящемся в порту 1.1 устройства с предварительно загруженным файлом обновления.

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

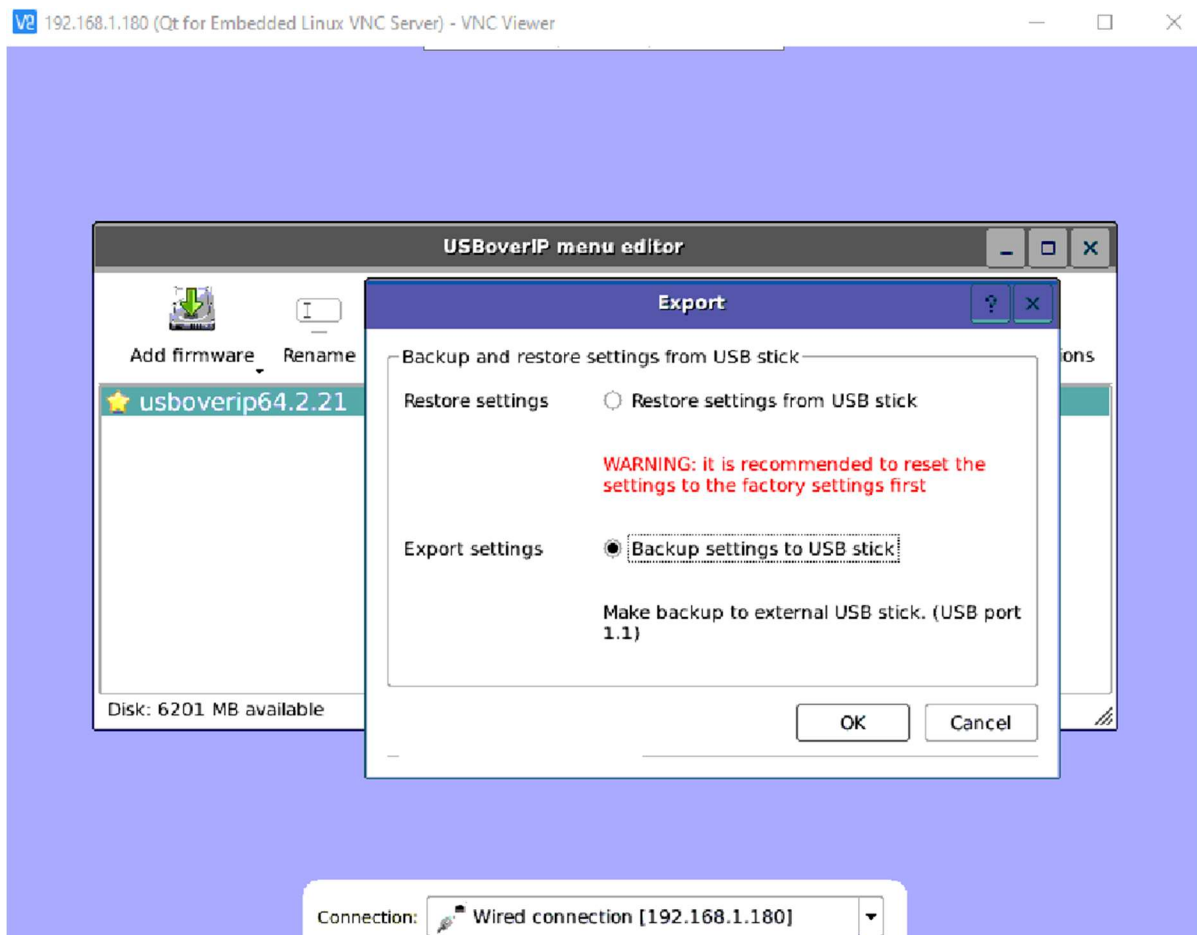
ВНИМАНИЕ!!! Сохранения настроек программного обеспечения, управляемого USB over IP концентратора или их восстановления возможно для версий ПО не ниже 2.21. При необходимости, удаление импортированных настроек, осуществляется простым сбросом настроек управляемого USB over IP концентратора в исходное состояние.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

Существует два способа сохранения и восстановления настроек программного обеспечения:

1. Через **Web** интерфейс устройства.
2. Через **VNC**.

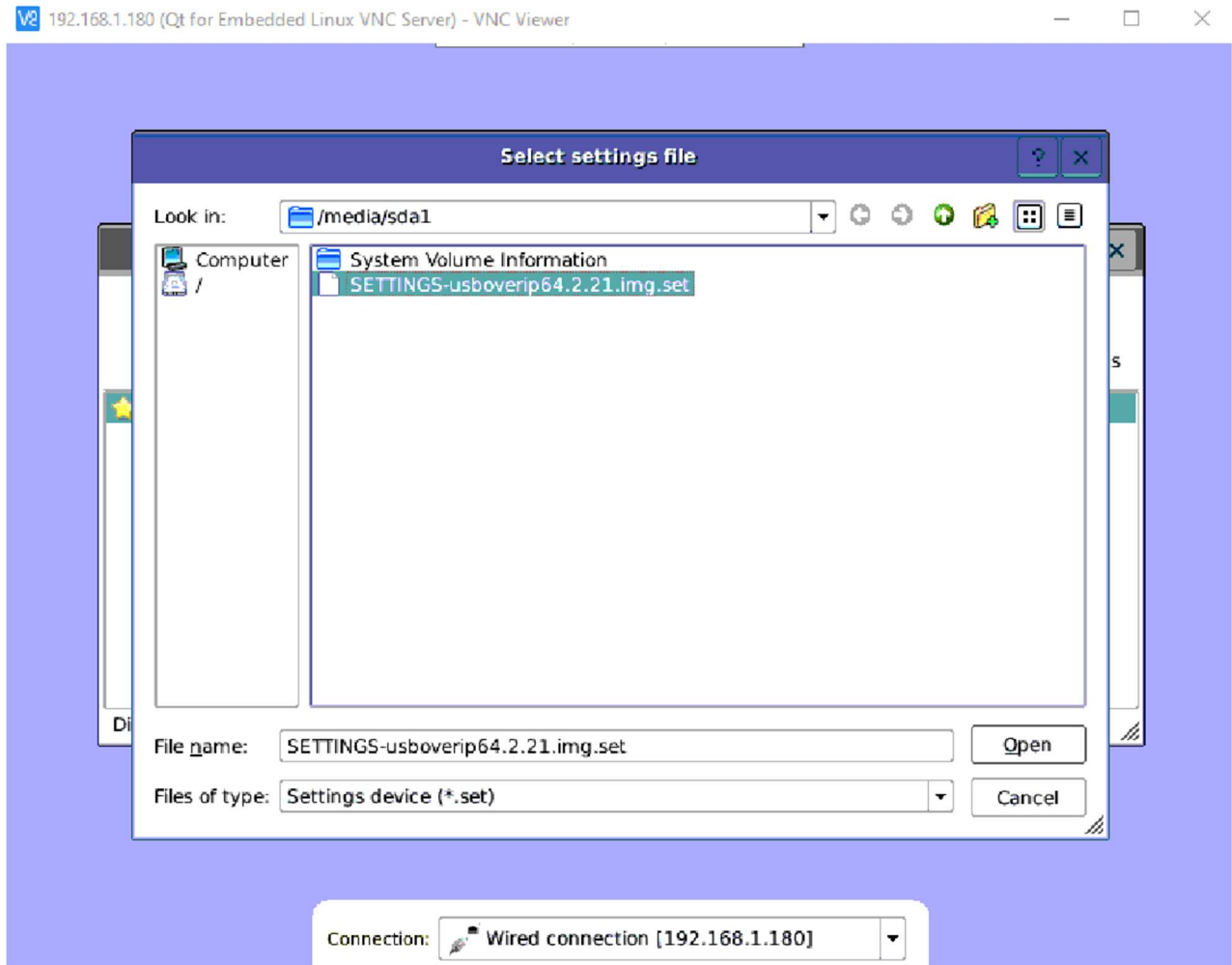
Для сохранения настроек программного обеспечения, управляемого USB over IP концентратора **или их восстановления** через VNC необходимо подключиться к концентратору с помощью VNC по изложенной выше методике. В USB порт 1.1 концентратора необходимо подключить флеш носитель (рекомендуется использовать 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 «OK». 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

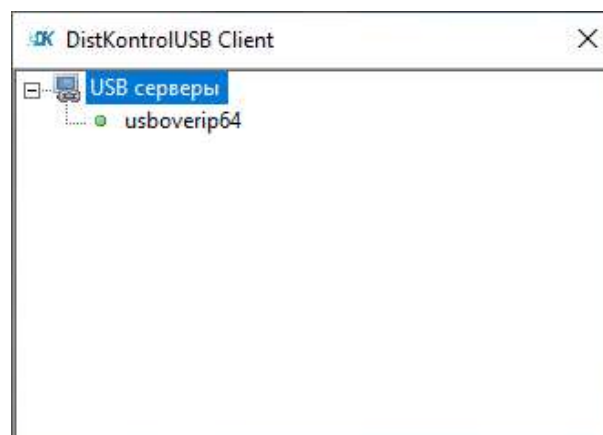
5 КЛИЕНТ DISTKONTROLUSB

5.1 УСТАНОВКА КЛИЕНТА DISTKONTROLUSB

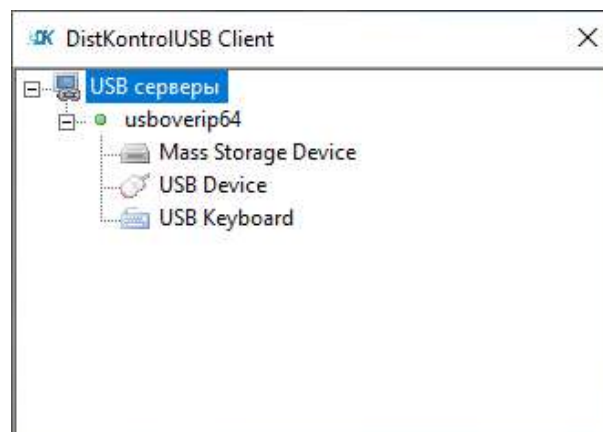
Клиент USB можно скачать с самого устройства подключения USB по сети или с сайта (ссылки на странице Информация - Поддержка).

Необходимо скачать и запустить соответствующее ПО.

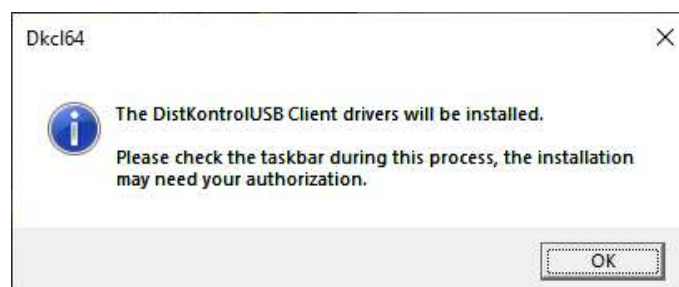
Во время установки появится уведомление центра безопасности Windows. Необходимо разрешить приложению внесение изменений.



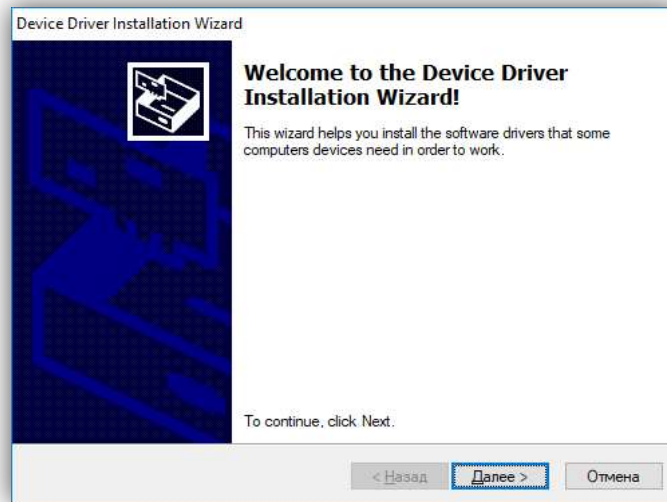
При подключении к USB over IP USB устройств они будут видны в клиенте и их будет можно подключить к компьютеру:



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.

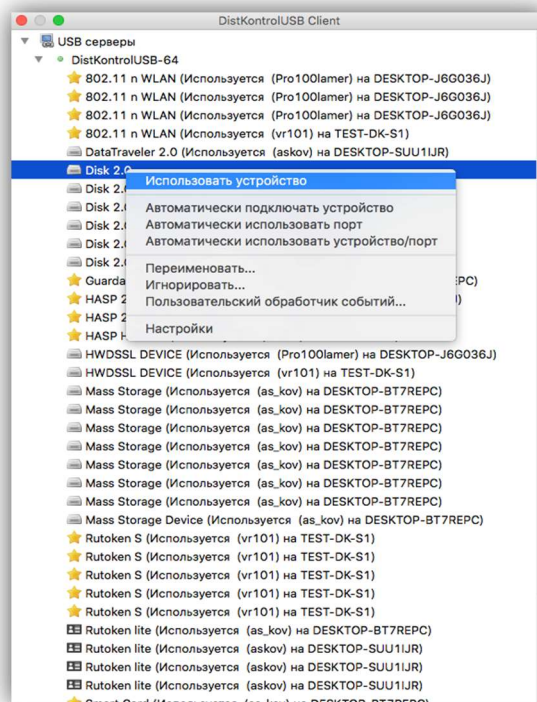


Нажать «Установить».

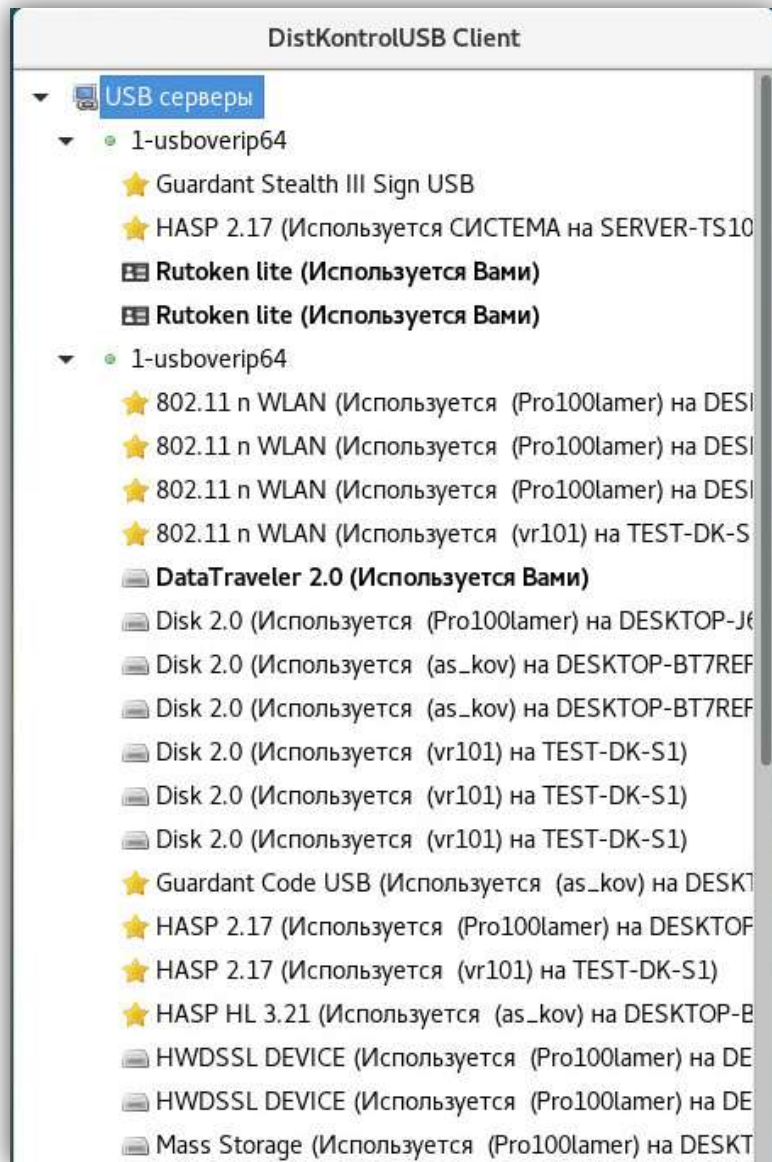
После запуска отобразится окно USB клиента.

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.

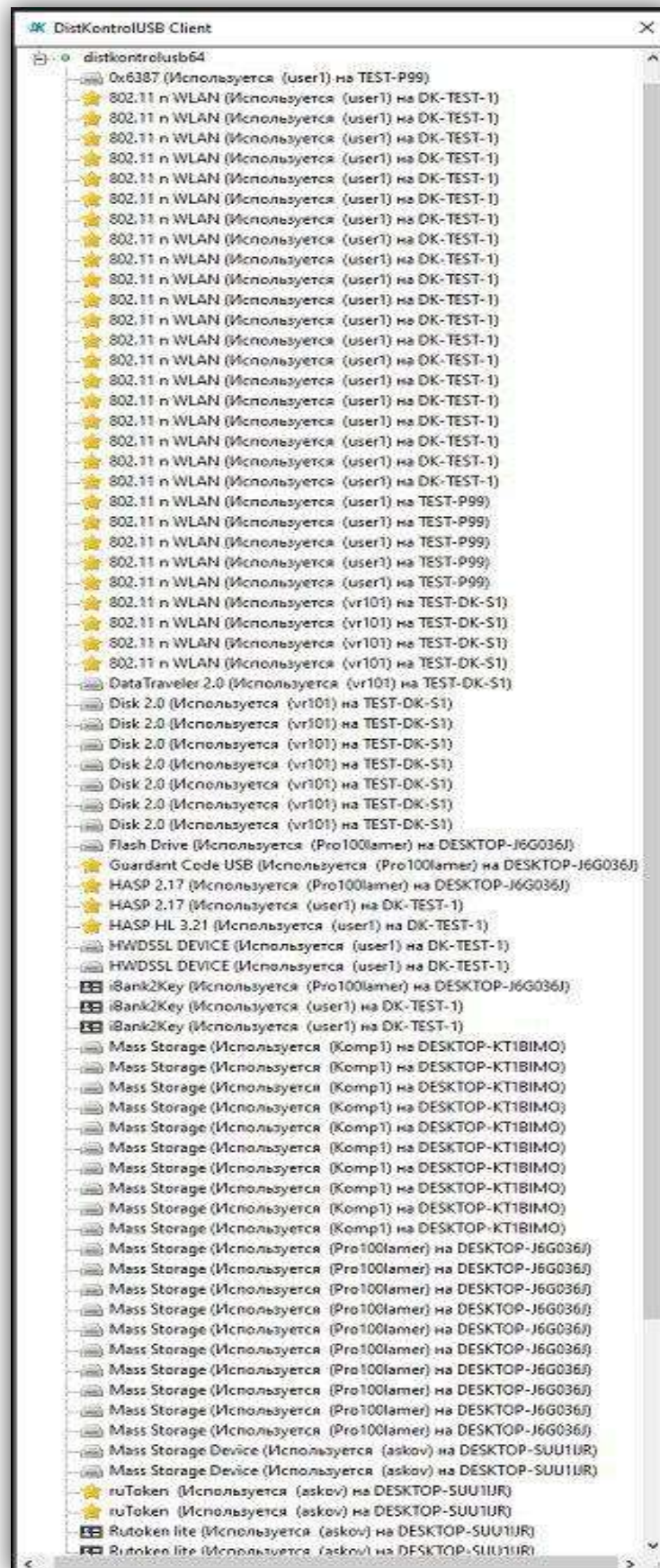
OSX:



Linux:

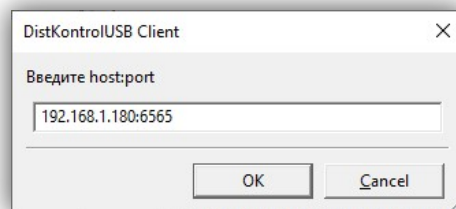
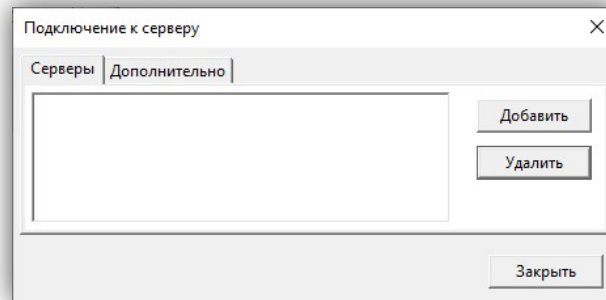


Windows:



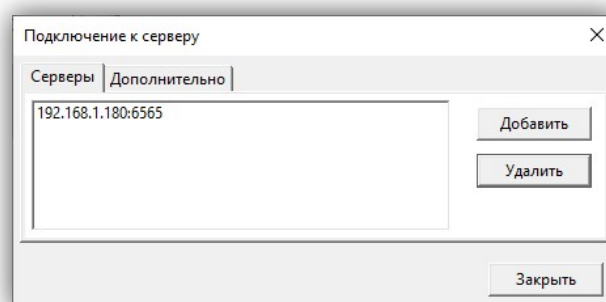
DistKontrolUSB Client для Linux устройства аппаратного подключения USB по сети использует встроенный драйвер usbip для Linux. (Рекомендуется использовать ядро (4.9+) для максимальной совместимости).

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.

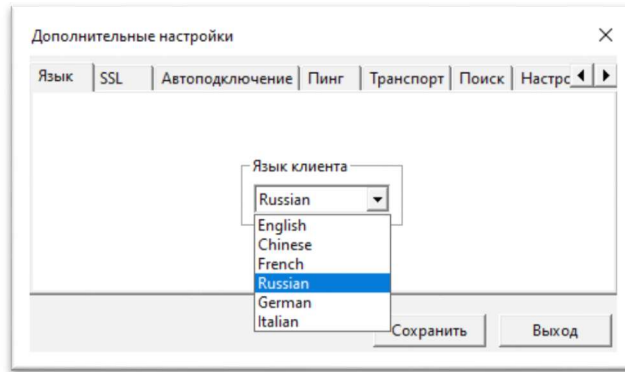
Ввести настройки сервера в формате адрес:порт и нажать OK. Порт: 6565 (6564 при использовании SSL). Здесь необходимо указать IP-адрес концентратора.



В окне Specify Hubs нажать Close.

Интерфейс клиента мультиязычный. Для выбора В клиенте:

1. Клик правой кнопкой мыши на USB Hubs -> Advanced Setting
2. На вкладке Language выбрать язык интерфейса -> Save

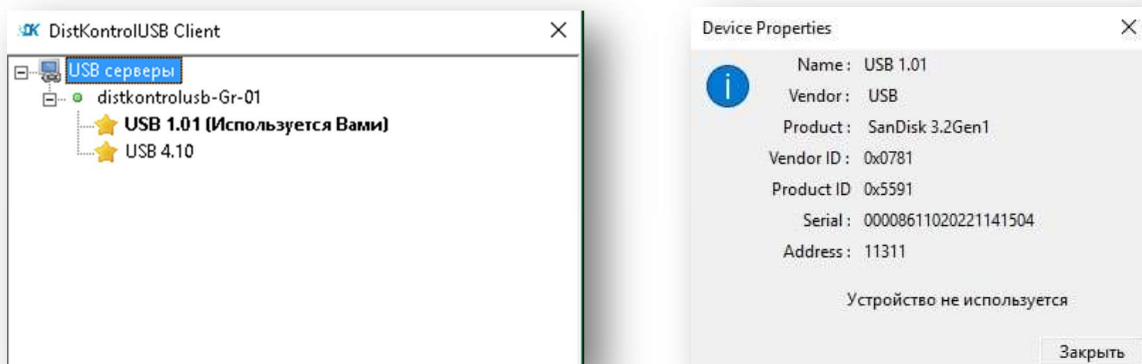


5.2 НАСТРОЙКА КЛИЕНТА DISTKONTROLUSB

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 НАСТРОЙКА МЕНЮ КЛИЕНТСКОГО ПРИЛОЖЕНИЯ DISTKONTROLUSB

Клиент сохраняет все свои параметры в одном текстовом файле

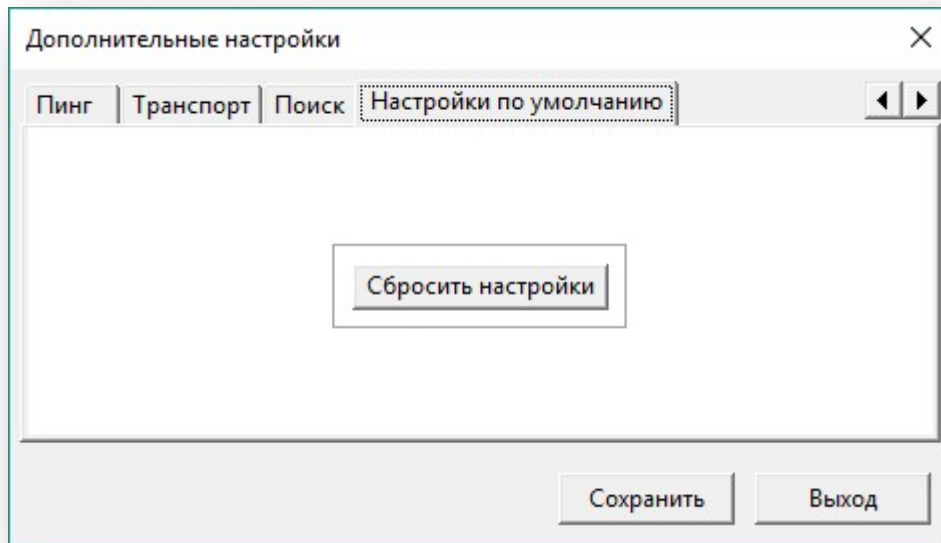
Windows: c:\Users\Username\AppData\Roaming\dkcl.ini

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

Linux: ~/. dkcl

Этот файл обновляется при изменении настроек. 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.



5.2.3 СБРОС НАСТРОЕК КЛИЕНТСКОГО ПРИЛОЖЕНИЯ DISTKONTROLUSB

Для сброса всех настроек клиентского приложения, необходимо сбросить настройки клиента. Правой кнопкой мыши по “USB серверы” – “Дополнительные настройки”. Вкладка “Настройки по умолчанию” расположена в самом конце.

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

5.2.4 КОМБИНАЦИИ КЛАВИШ КЛИЕНТСКОГО ПРИЛОЖЕНИЯ DISTKONTROLUSB

Для удаления сохраненных паролей клиентского приложения необходимо воспользоваться комбинацией клавиш.

- 1)Нажмите SHIFT+F9 удаление сохраненного пароля выбранного порта.
- 2)Нажмите SHIFT+F8 удаление всех сохраненных паролей для всех 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"
```

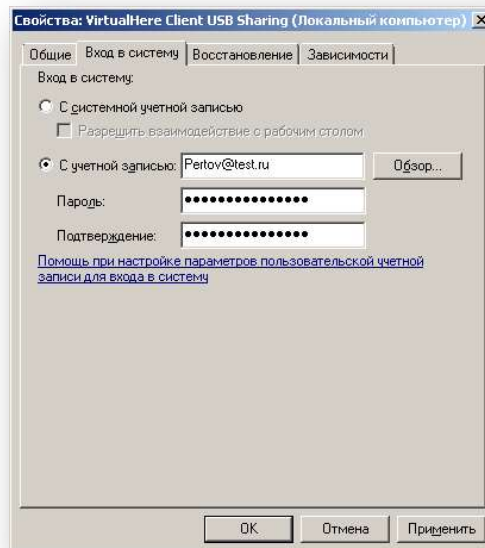
По умолчанию служба запускается от имени пользователя «Система».

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).

`-s` 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.

Путь до сертификата для USB трафика возможно посмотреть в Web-интерфейсе в Разделе «Система» - «Сертификаты» вкладка «USB». Необходимо открыть настройки сертификата и скопировать путь.

Скачиваем с концентратора сертификат и консольный клиент:

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

/client/*****.pem – Необходимо указать путь до сертификата скопированный в Web-интерфейсе.

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 [d]kc
```

Видим:

```
root 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"
```

Для автоматического использования USB-порта:

```
./dkclientx86_64 -t " AUTO USE PORT,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.

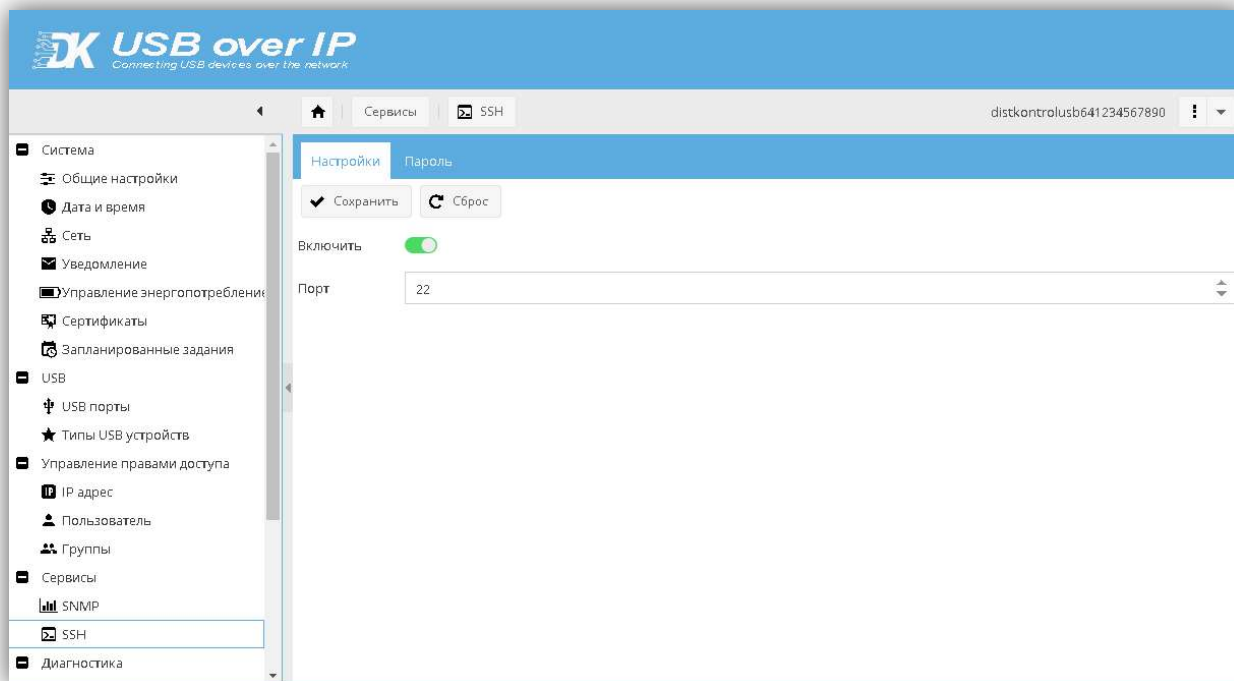
Если в выводе:

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 самостоятельно 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:  
> usbcontrol-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 абсолютным 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

Ответы на большинство вопросов по использованию **управляемого USB over IP концентратора DistKontrolUSB** и клиентского приложения **DistKontrolUsb Client** и их настройке изложены в [Базе знаний](#).